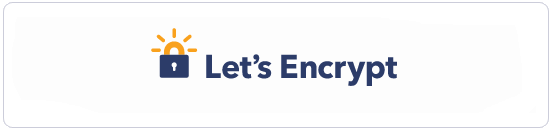
**免费SSL证书Let’s Encrypt安装使用教程：Apache和Nginx配置SSL**



Let's Encrypt是国外一个公共的免费SSL项目，由 Linux 基金会托管，它的来头不小，由Mozilla、思科、Akamai、IdenTrust和EFF等组织发起，目的就是向网站自动签发和管理免费证书，以便加速互联网由HTTP过渡到HTTPS，目前Facebook等大公司开始加入赞助行列。

Let's Encrypt已经得了 IdenTrust 的交叉签名，这意味着其证书现在已经可以被Mozilla、Google、Microsoft和Apple等主流的浏览器所信任，你只需要在Web 服务器证书链中配置交叉签名，浏览器客户端会自动处理好其它的一切，Let's Encrypt安装简单，未来大规模采用可能性非常大。

Let's Encrypt虽然还在测试当中，但是市场需求非常大，已经有非常多的朋友迫不及待地安装并用上了Let's Encrypt。Let's Encrypt向广大的网站提供免费SSL证书，不管是对于网站站长、互联网用户，还是对整个Web互联网，都是非常有利的，它有利于整个互联网的安全。

本篇文章就来为大家讲解一下如何获取Let's Encrypt免费SSL证书，并附上Apache和Nginx的SSL证书配置方法。

**免费SSL证书Let's Encrypt安装使用教程:Apache和Nginx配置方法**

## 一、 安装Let's Encrypt免费SSL准备

### 1、Let's Encrypt官网：

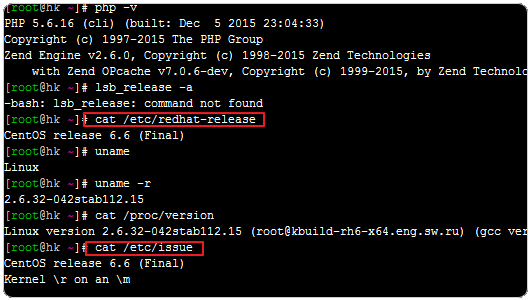
官方网站：https://letsencrypt.org/

项目主页：https://github.com/letsencrypt/letsencrypt

### 2、安装Let's Encrypt脚本依赖环境：（这一部分可以跳过，因为官方提供的Let's Encrypt脚本会自动检测并安装）

# Debianapt-get install git# CentOS 6yum install centos-release-SCL && yum updateyum install python27scl enable python27 bashyum install python27-python-devel python27-python-setuptools python27-python-tools python27-python-virtualenvyum install augeas-libs dialog gcc libffi-devel openssl-devel python-develyum install python-argparse# CentOS 7yum install -y git python27yum install -y augeas-libs dialog gcc libffi-devel openssl-devel python-develyum install python-argparse

### 3、查看自己的VPS主机到底是安装了哪个操作系统版本，可以执行命令：cat /etc/issue 或者 cat /etc/redhat-release。

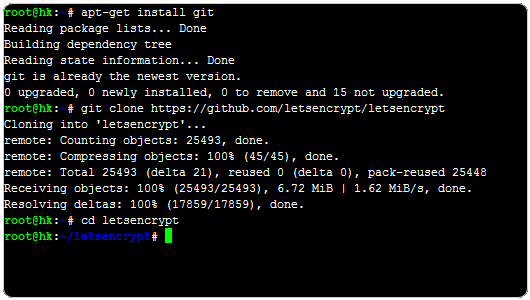


## 二、获取Let's Encrypt免费SSL证书

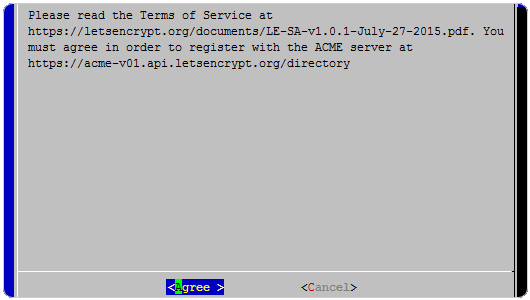
### 1、获取Let's Encrypt免费SSL证书很简单，你只需要执行以下命令，就会自动在你的VPS上生成SSL证书和私钥。

git clone https://github.com/letsencrypt/letsencryptcd letsencrypt./letsencrypt-auto

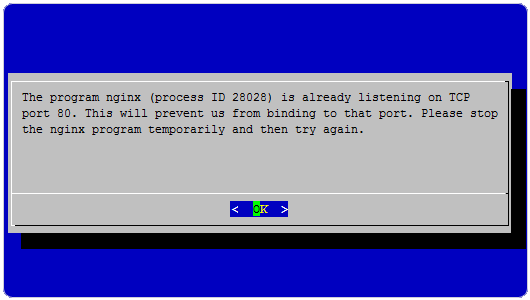
2、经过部落测试，上述代码对于Debian系统支持最好，可以完成自动检测并安装相应的软件。如果你是使用其它的Linux系统，Redhat或CentOS 6可能需要配置EPEL软件源，Python需要2.7版本以上。



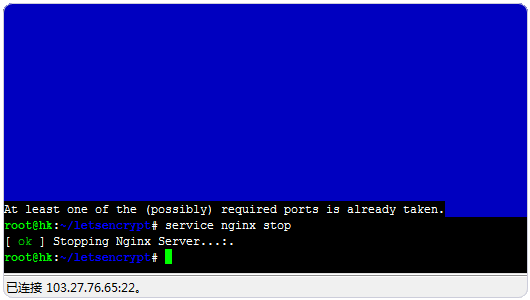
3、执行上述命令后，会弹出对话框，同意用户协议。



4、接着会提示让你关闭Nginx或者Apache。



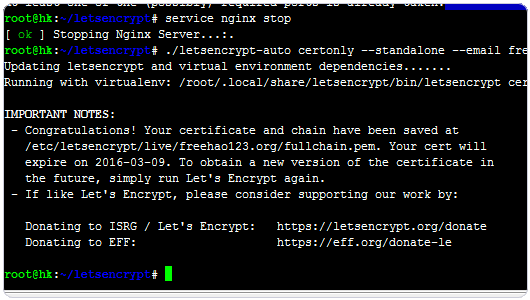
5、Let's Encrypt需要用到80和443端口，所以你需要关闭那些占用这两个端口的应用。



6、当你看以下内容时，就表明你的Let's Encrypt免费SSL证书获取成功了。

IMPORTANT NOTES: - Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/freehao123.org/fullchain.pem. Your cert will expire on 2016-03-09. To obtain a new version of the certificate in the future, simply run Let's Encrypt again. - If like Let's Encrypt, please consider supporting our work by: Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate Donating to EFF: https://eff.org/donate-le

7、见下图：



**注：**相关网站建设技巧阅读请移步到[建站教程](http://www.chinaz.com/web/)频道。

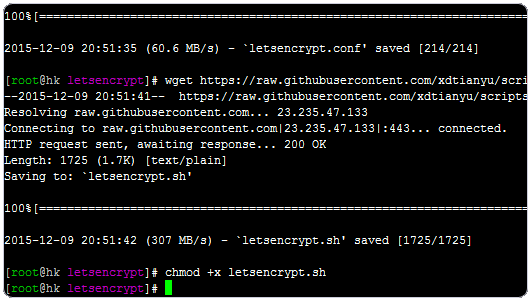
**三、利用脚本快速获取Let's Encrypt SSL证书**

1、嫌上面的麻烦，不妨来试试利用脚本快速获取Let's Encrypt SSL证书，调用 acme\_tiny.py 认证、获取、更新证书，不需要额外的依赖。

1、项目主页：https://github.com/xdtianyu/scripts/tree/master/lets-encrypt

2、下载到本地：

wget https://raw.githubusercontent.com/xdtianyu/scripts/master/lets-encrypt/letsencrypt.confwget https://raw.githubusercontent.com/xdtianyu/scripts/master/lets-encrypt/letsencrypt.shchmod +x letsencrypt.sh

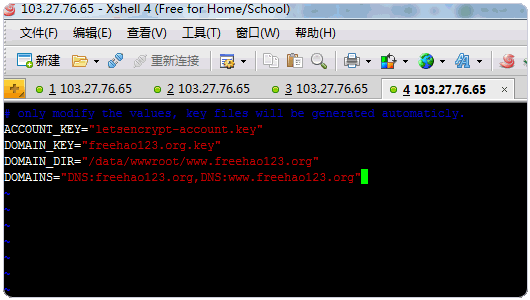


3、配置文件。只需要修改 DOMAIN\_KEY DOMAIN\_DIR DOMAINS 为你自己的信息

ACCOUNT\_KEY="letsencrypt-account.key"DOMAIN\_KEY="freehao123.com.key"DOMAIN\_DIR="/var/www/freehao123.com"DOMAINS="DNS:freehao123.com,DNS:www.freehao123.com"

4、本脚本在Debian下运行正常，但是如果你使用的是CentOS，你还需要修改letsencrypt.sh中openssl.cnf的位置，先找到你的CentOS的openssl.cnf位置。然后打开letsencrypt.sh，将路径/etc/ssl/openssl.cnf替换为你的新路径，例如/etc/pki/tls/openssl.cnf。

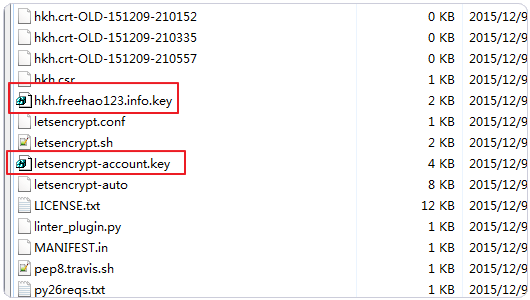
**PS：20151214更新，**该脚本已经更新，现在不需要对CentOS的openssl.cnf进行修改了。感谢ty博主的提醒。



5、执行过程中会自动生成需要的 key 文件。运行：

./letsencrypt.sh letsencrypt.conf

6、注意需要已经绑定域名到 /var/www/www.freehao123.com 目录，即通过 http://freehao123.com http://www.freehao123.com 可以访问到 /var/www/freehao123.com目录，用于域名的验证。



7、正常按照上面的操作即可成功获取到Let's Encrypt SSL证书，不过经过部落测试最大的问题就是“DNS query timed out”，由于域名DNS解析的问题导致无法验证域名从而获取SSL证书不成功。

Traceback (most recent call last): File "/tmp/acme\_tiny.py", line 198, in main(sys.argv[1:]) File "/tmp/acme\_tiny.py", line 194, in main signed\_crt = get\_crt(args.account\_key, args.csr, args.acme\_dir, log=LOGGER, CA=args.ca) File "/tmp/acme\_tiny.py", line 149, in get\_crt domain, challenge\_status))ValueError: hkh.freehao123.info challenge did not pass:   
{u'status': u'invalid', u'validationRecord':   
[{u'url': u'http://hkh.freehao123.info/.well-known/acme-challenge/  
sikHlqvbN4MrWkScgr1oZ9RX-lR1l\_\_Z7FWVLhlYR0Q', u'hostname':   
u'hkh.freehao123.info', u'addressUsed': u'', u'port': u'80',   
u'addressesResolved': None}],   
 u'https://acme-v01.api.letsencrypt.org/acme/challenge/  
5m1su6O5MmJYlGzCJnEUAnvhweAJwECBhEcvsQi5B2Q/1408863', u'token':   
u'sikHlqvbN4MrWkScgr1oZ9RX-lR1l\_\_Z7FWVLhlYR0Q', u'error':   
{u'type': u'urn:acme:error:connection', u'detail': u'DNS query timed out'}, u'type': u'http-01'}

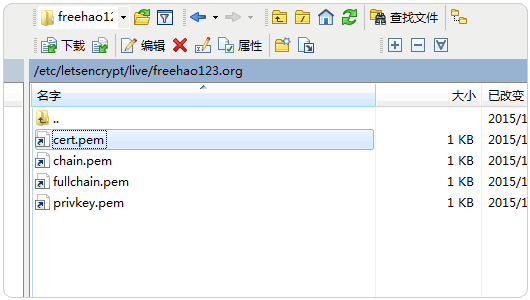
8、经过对比发现，国内的DNSPOD、阿里云DNS、CloudXNS等都会出现Let's Encrypt 验证域名超时的情况，国外的Namecheap DNS、Linode DNS、Domain.com DNS等都是没有问题。



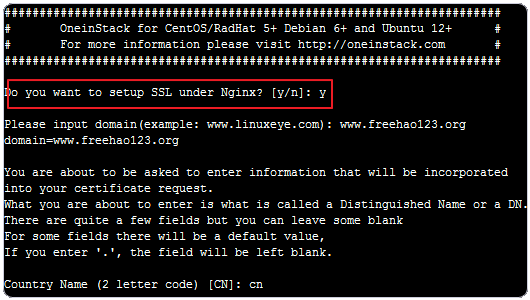
**注：**相关网站建设技巧阅读请移步到[建站教程](http://www.chinaz.com/web/)频道。

**四、 Ngnix配置Let's Encrypt免费SSL**

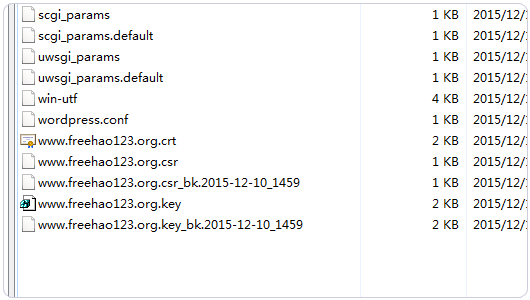
1、注意查看你的Let's Encrypt免费SSL证书保存位置，一般是在/etc/letsencrypt/live/freehao123.com这样的下面。



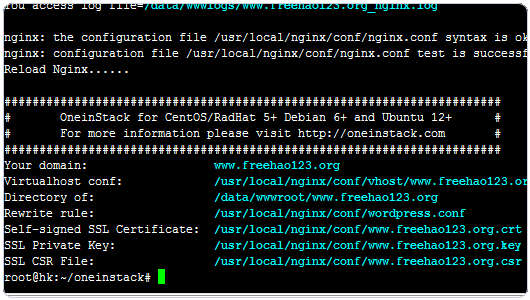
2、fullchain.pem就是公钥，privkey.pem就是私钥。有了这两个文件我们就可以在Ngnix上配置SSL证书了。OneinStack一键工具在创建虚拟主机时可以选择为网站配置SSL。



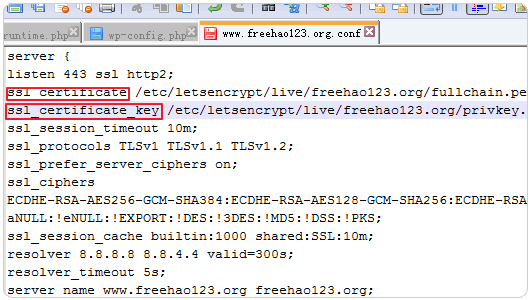
3、如果有用OneinStack，那么最简单的方法就是用fullchain.pem和privkey.pem替代原来生成的CRT和Key文件，这样做的好处就可以保留Ngnix配置的SSL证书路径，只要简单修改引用的公钥和私钥即可。



4、当然，为了后面的操作方便，我们建议保留Let's Encrypt生成的SSL证书，直接在网站的配置中修改SSL证书引用路径。使用VPS主机创建网站时会为网站生成一个.conf文件。



5、这个这个.conf文件，直接替换掉ssl\_certificate和ssl\_certificate路径即可，如下图：



6、OneinStack的Nginx配置SSL证书代码示例：

server {

listen 443 ssl http2;

ssl\_certificate /etc/letsencrypt/live/freehao123.org/fullchain.pem;//改动地方1

ssl\_certificate\_key /etc/letsencrypt/live/freehao123.org/privkey.pem;//改动地方2

ssl\_session\_timeout 10m;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_prefer\_server\_ciphers on;

ssl\_ciphers ECDHE-SHA384:ECDHE-RSA-:ECDHE:!DES:!3DES:!MD5:!DSS:!PKS;

ssl\_session\_cache builtin:1000 shared:SSL:10m;

resolver 8.8.8.8 8.8.4.4 valid=300s;

resolver\_timeout 5s;

server\_name www.freehao123.org freehao123.org;

access\_log /data/wwwlogs/www.freehao123.org\_nginx.log combined;

index index.html index.htm index.php;

include /usr/local/nginx/conf/wordpress.conf;

root /data/wwwroot/www.freehao123.org;

if ($host != www.freehao123.org) {

rewrite ^/(.\*)$ $scheme://www.freehao123.org/$1 permanent;

}

server {

listen 80;

server\_name www.freehao123.org;

rewrite ^/(.\*) https://$server\_name/$1 permanent;

}

7、最后重启Nginx，打开浏览器就可以看到SSL证书已经成功配置好了。



8、对于安装了LNMP的朋友，可以参考以下代码修改自己的Nginx配置。

server

{

listen 443 ssl;  
 //如果需要spdy也可以加上,lnmp1.2及其后版本都默认支持spdy,lnmp1.3 nginx 1.9.5以上版本  
 默认支持http2

server\_name www.freehao123.com; //域名

index index.html index.htm index.php default.html default.htm default.php;

root /home/wwwroot/www.freehao123.com; //网站目录

ssl\_certificate /etc/letsencrypt/live/www.freehao123.com/fullchain.pem; //前面生成的证书

ssl\_certificate\_key /etc/letsencrypt/live/www.freehao123.com/privkey.pem; //前面生成的密钥

ssl\_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_prefer\_server\_ciphers on;

ssl\_session\_cache shared:SSL:10m;

include wordpress.conf; //这个是伪静态

#error\_page 404 /404.html;

location ~ [^/]\.php(/|$)

{

# comment try\_files $uri =404; to enable pathinfo

try\_files $uri =404;

fastcgi\_pass unix:/tmp/php-cgi.sock;

fastcgi\_index index.php;

include fastcgi.conf; //lnmp 1.0及之前版本替换为include fcgi.conf;

#include pathinfo.conf;

}

**五、Apache配置Let's Encrypt免费SSL**

1、首先，我们需要对Apache的配置进行修改，打开 /usr/local/apache/conf/httpd.conf ，查找httpd-ssl将前面的#去掉，然后执行命令（注意将路径换你自己的）：

cat >/usr/local/apache/conf/extra/httpd-ssl.conf<<EOF

Listen 443

AddType application/x-x509-ca-cert .crt

AddType application/x-pkcs7-crl .crl

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

SSLProxyCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

SSLHonorCipherOrder on

SSLProtocol all -SSLv2 -SSLv3

SSLProxyProtocol all -SSLv2 -SSLv3

SSLPassPhraseDialog builtin

SSLSessionCache "shmcb:/usr/local/apache/logs/ssl\_scache(512000)"

SSLSessionCacheTimeout 300

SSLMutex "file:/usr/local/apache/logs/ssl\_mutex"

EOF

2、接着，在你创建的网站的Apache配置的最后</VirtualHost>下面添加上SSL部分的配置文件：

<VirtualHost \*:443>

DocumentRoot /home/wwwroot/www.freehao123.com //网站目录

ServerName www.freehao123.com:443 //域名

ServerAdmin admin@freehao123.com //邮箱

ErrorLog "/home/wwwlogs/www.freehao123.com-error\_log" //错误日志

CustomLog "/home/wwwlogs/www.freehao123.com-access\_log" common //访问日志

SSLEngine on

SSLCertificateFile /etc/letsencrypt/live/www.freehao123.com/fullchain.pem //之前生成的证书

SSLCertificateKeyFile /etc/letsencrypt/live/www.freehao123.com/privkey.pem //之前生成的密钥

<Directory "/home/wwwroot/www.freehao123.com"> //网站目录

SetOutputFilter DEFLATE

Options FollowSymLinks

AllowOverride All

Order allow,deny

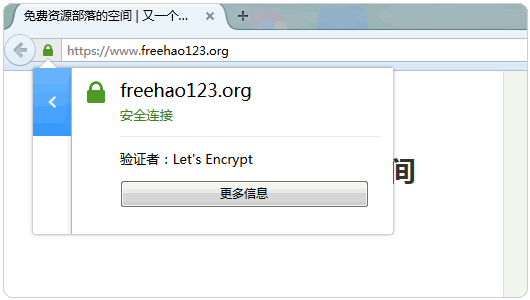
Allow from all

DirectoryIndex index.html index.php

</Directory>

</VirtualHost>

3、最后就是重启Apache，然后打开浏览器就可以看到SSL证书配置成功了。



**六、 Let's Encrypt免费SSL证书续期**

1、Let's Encrypt免费SSL证书有效期是90天，也就是每三个月你就得续期一次。采用官方的方法获取到的免费SSL证书，你不需要更改Apache和Nginx配置代码，执行以下代码即可自动替换证书为新的（注意修改域名和邮箱）：

./letsencrypt-auto certonly --renew-by-default --email freehao123@gmail.com  
 -d freehao123.org -d www.freehao123.org

2、采用上面脚本快速获取Let's Encrypt免费SSL证书的，在90天内再次执行命令即可：./letsencrypt.sh letsencrypt.conf。

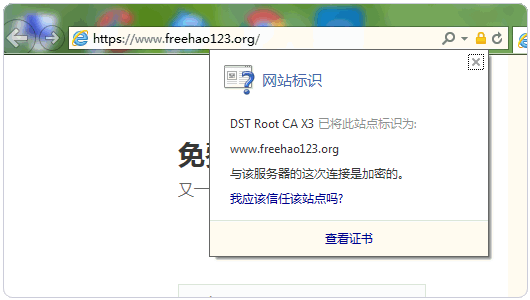


3、cron 定时任务。每个月自动更新一次证书，可以在脚本最后加入 service nginx reload等重新加载服务。

0 0 1 \* \* /etc/nginx/certs/letsencrypt.sh /etc/nginx/certs/letsencrypt.conf >>  
 /var/log/lets-encrypt.log 2>&1

**七、Let's Encrypt免费SSL证书使用小结**

Let's Encrypt免费SSL证书获得方式比较简单，不管采用何种方式，只要能够得到证书和密钥，我们就可以在自己的服务器上配置好SSL。上面讲到了Apache和Nginx的配置方法，如果你有自己的虚拟主机面板，可以直接通过后台添加证书和私钥文件即可。



**注：**相关网站建设技巧阅读请移步到[建站教程](http://www.chinaz.com/web/)频道。