

# Hello World

Just So So ...

[首页](#)[关于本站](#)[友情链接](#)

## 用acme.sh脚本申请证书并自动续更

作者: [毕世平](#) | 时间: 2019-11-14 | 分类: [vps](#), [acme证书](#)

前言: [acme.sh](#) 脚本实现了 [acme](#) 协议, 可以从 [letsencrypt](#) 生成免费的证书, 并且支持手动发行免费的通配符证书, 这对广大个人站长无疑是个很大的福利。

本文则主要介绍使用 [acme.sh](#) 脚本搭配 [Cloudflare](#) 的 [Global API Key](#) 来为托管在 [Cloudflare](#) 上的域名申请证书, 并实现到期自动续订的步骤。

本文参考: <https://github.com/Neilpang/acme.sh/wiki/%E8%AF%B4%E6%98%8E>

## 一、安装acme.sh脚本

### 1.1 执行下面的命令

```
apt-get update && apt-get -y install socat //安装socat
```

```
wget -qO- get.acme.sh | bash //安装脚本
```

```
source ~/.bashrc //让环境变量生效, 以后无论在哪个路径, 直接使用acme.sh
```

说明: root用户和非root用户都可以安装使用, 安装过程不污染已有的系统任何功能和文件, 所有的修改都限制在安装目录中。

### 1.2 安装过程及安装目录解释 (嫌麻烦可以跳过)

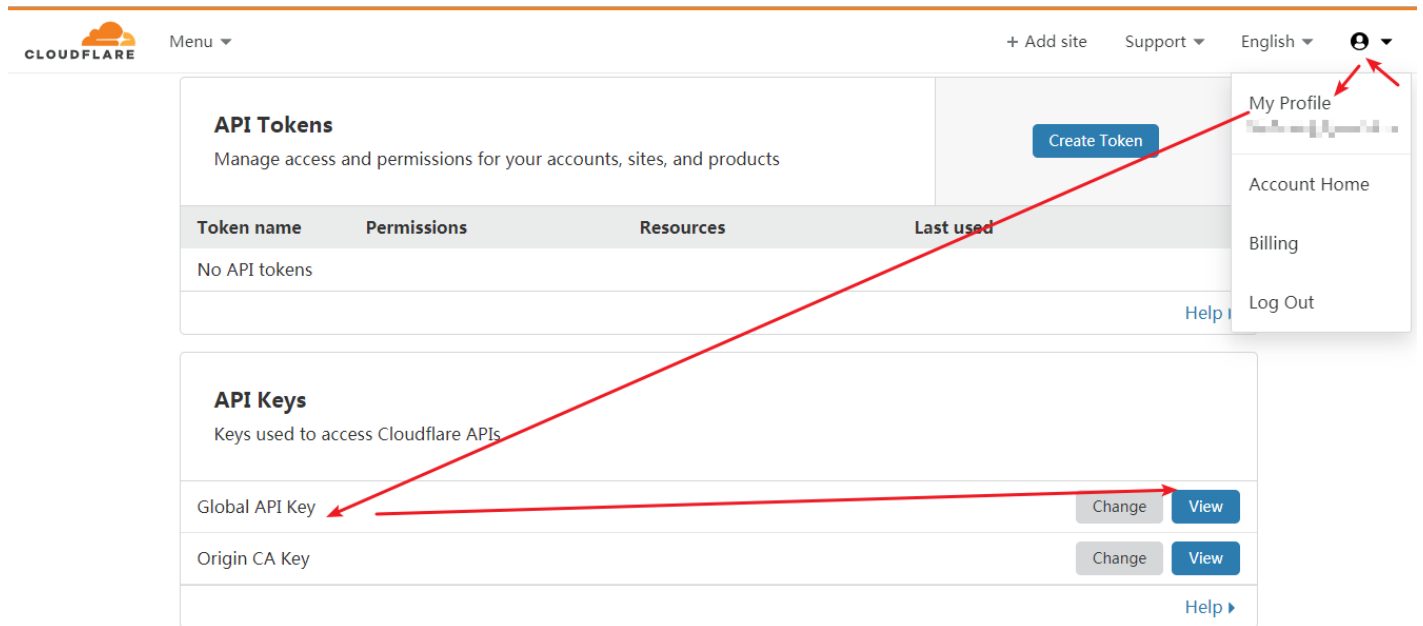
- 先把 [acme.sh](#) 安装到你的 `/home/user/.acme.sh` 目录下, root用户则安装到 `/root/.acme.sh` 目录下。
- 创建一个bash的alias, 方便你的使用: `alias acme.sh=~/.acme.sh/acme.sh`
- 它会自动在 `.bashrc` 的最后添加环境变量, `"/home/user/.acme.sh/acme.sh.env"`, 如果是root用户, 则为 `"/root/.acme.sh/acme.sh.env"`, 你需要 `source ~/.bashrc` 命令使环境变量生效, 以后就可以直接使用 [acme.sh](#) 命令了。
- 自动为你创建crontabjob任务, 每天0:00自动检测所有的证书, 如果快过期了需要更新, 则会自动更新证书。
- 更高级的证书安装选项请参考: <https://github.com/Neilpang/acme.sh/wiki/How-to-install>

## 二、到Cloudflare那里拿到Global API Key

### 2.1 注册Cloudflare账号并添加域名

这个就不用多做介绍了吧, 注意要在域名注册商那里把域名的NS权限交由Cloudflare来解析, 才能添加上域名, 之后添加A记录, 假设域名是 `mydomain.me`, Name填 `@` 或者 `www`, Content填你的 [VPS IP](#), TTL默认, CDN云朵可以开启也可以不开启。

## 2.2 获取Global API Key



按照图示操作复制此Key即可，注意保存在安全位置。

## 三、配置证书(dns+cf api验证)

### 3.1 配置条件

```
export CF_Key="slfjksjffjfjfhfkhjfhfksjf" //此处替换成你自己的Key
export CF_Email="yourcloudflare@gmail.com" //此处填写你注册Cloudflare使用的邮箱账号
```

### 3.2 申请颁发ECC证书

```
acme.sh --issue --dns dns_cf -d mydomain.me -k ec-256
```

**说明：**上面的CF\_Key和CF\_Email在执行这一步之后将被保存到 `/root/.acme.sh/account.conf` 文件中，在需要时会被重新使用。域名套CDN状态下也可以申请成功证书。

关于更详细的api用法，请参考：<https://github.com/Neilpang/acme.sh/blob/master/dnsapi/README.md>

### 3.3 复制/安装证书

**注意：**默认生成的证书都放置在 `~/.acme.sh/mydomain.me_ecc` 目录下，请不要直接使用这目录下的文件，因为这里属于内部文件，且将来目录结构可能会变化。

正确的使用方法如下（假定在 `/root/ssl` 目录下放置证书）：

```
acme.sh --installcert -d mydomain.me --fullchain-file /root/ssl/web.cer --key-file /root/ssl/web.key --ecc
```

**值得注意的是：**这里指定的所有参数会被自动记录下来，并且在证书自动更新以后会被再次调用。

## 四、更新证书

关于从Letsencrypt申请到的证书，有效期为90天，脚本会每60天自动更新证书，你无须进行任何操作，今后可能会缩短这个时间，不过都是自动的，你不用关心。

## 五、更新acme.sh脚本

目前由于acme协议和letsencrypt CA都在频繁的更新，因此 `acme.sh` 脚本呢也经常更新以保持同步。

### 5.1 升级acme.sh到最新版

```
acme.sh --upgrade
```

### 5.2 如果你不想手动升级，可以开启自动升级：

```
acme.sh --upgrade --auto-upgrade
```

### 5.3 你也可以随时关闭脚本的自动更新

```
acme.sh --upgrade --auto-upgrade 0
```

## 六、定时任务

### 6.1 安装crontab

```
apt-get update && apt-get -y install cron
```

### 6.2 设置定时任务

如果你是用的lamp搭建的网站，并在lamp add添加站点过程中手动指定了证书的位置为 `/root/ssl`，证书：`/root/ssl/web.cer` 和key：`/root/ssl/web.key`，那么你可以设置定时任务定时自动将证书放到这里。

```
crontab -e //编辑定时任务
```

```
0 3 15 */2 * acme.sh --installcert -d mydomain.me --fullchain-file /root/ssl/web.cer --key-file /root/ssl/web.key
```

**说明：**这是设置每隔2个月在15号的3:00安装证书和key到 `/root/ssl` 目录下，并重启apache服务。

标签: [acme](#), [cloudflare](#)

---

## 添加新评论

称呼 \*

Email \*

## 网站

## 内容 \*

上一篇: [用Caddy配合Docker搭建V2Ray的\(vmess+ws\)+tls, 可选套cdn](#)

下一篇: [安装经9seconds重构的mtg代理](#)

© 2019 [Hello World](#). 由 [Typecho](#) 强力驱动.