

# 群晖 Let's Encrypt 泛域名证书自动更新

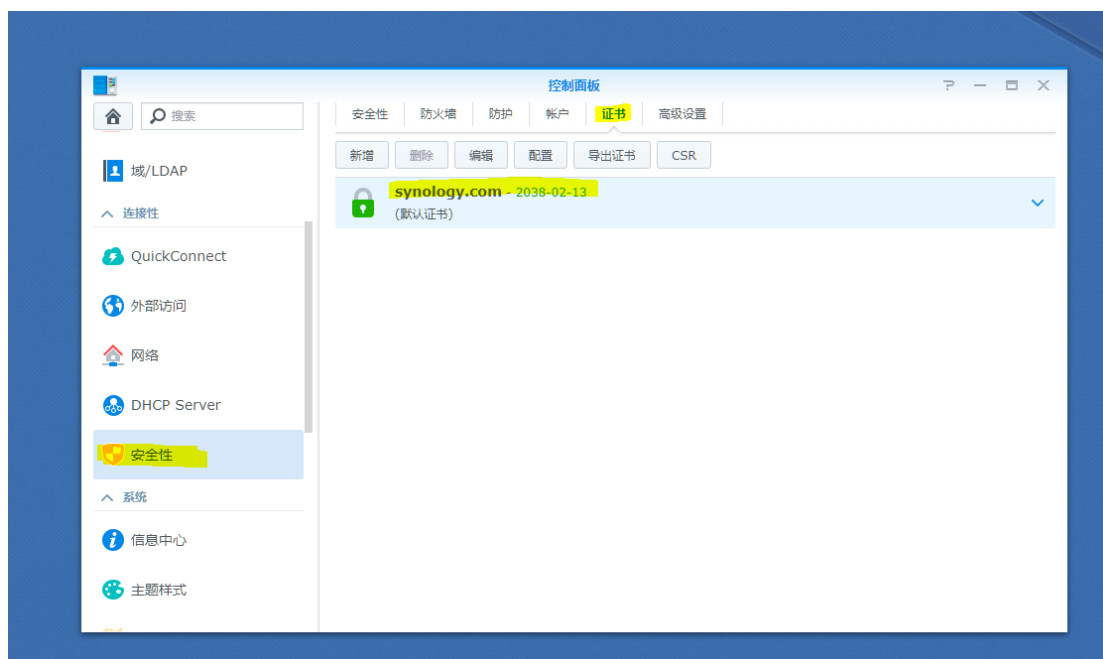
原文地址: <http://www.up4dev.com/2018/05/29/synology-ssl-wildcard-cert-update/>

曾经写过一篇文章介绍如何在群晖的 NAS 通过 acme 协议更新 Let's Encrypt 的 HTTPS 证书。目前 acme 协议版本更新, 开始支持泛域名(wildcard), 也就是说, 可以申请一个类似 \*.domain.com 的单一证书, 就可以适配 abc.domain.com, xyz.domain.com 这类的子域名, 而不需要单独为每个子域名申请证书了。

`acmesh-official/acme.sh` 工具已经支持新的协议, 我这篇文章就是在这个工具的基础上, 实现泛域名的自动更新。为了减少复杂度, 我编写了一个一键更新的懒人脚本, 来帮助没有时间了解详细原理的同学快速部署。

## 1. 准备工作

因为我介绍的方法是一键替换群晖的默认证书, 所以, 为了防止意外, 最好保证你的证书列表里只有一条记录, 即默认证书那一条。实际上因为支持了泛域名证书, 基本上这一条记录就足够用了(当然, 如果你要管理多个域名, 可能本文的方法并不适用)。开始工作前你的证书列表大概应该是这个样子:



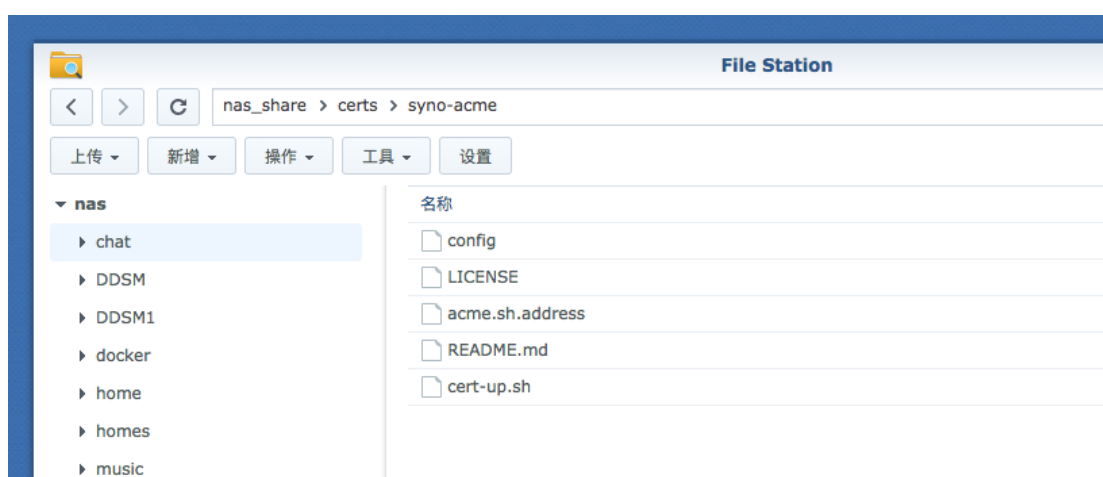
## 2. 下载一键更新脚本

这是一键脚本的项目地址：[andyzhshg/syno-acme](https://github.com/andyzhshg/syno-acme)。

如果你对项目本身不感兴趣，可以直接下载打包好的工具：[syno-acme v0.2.1](#)。

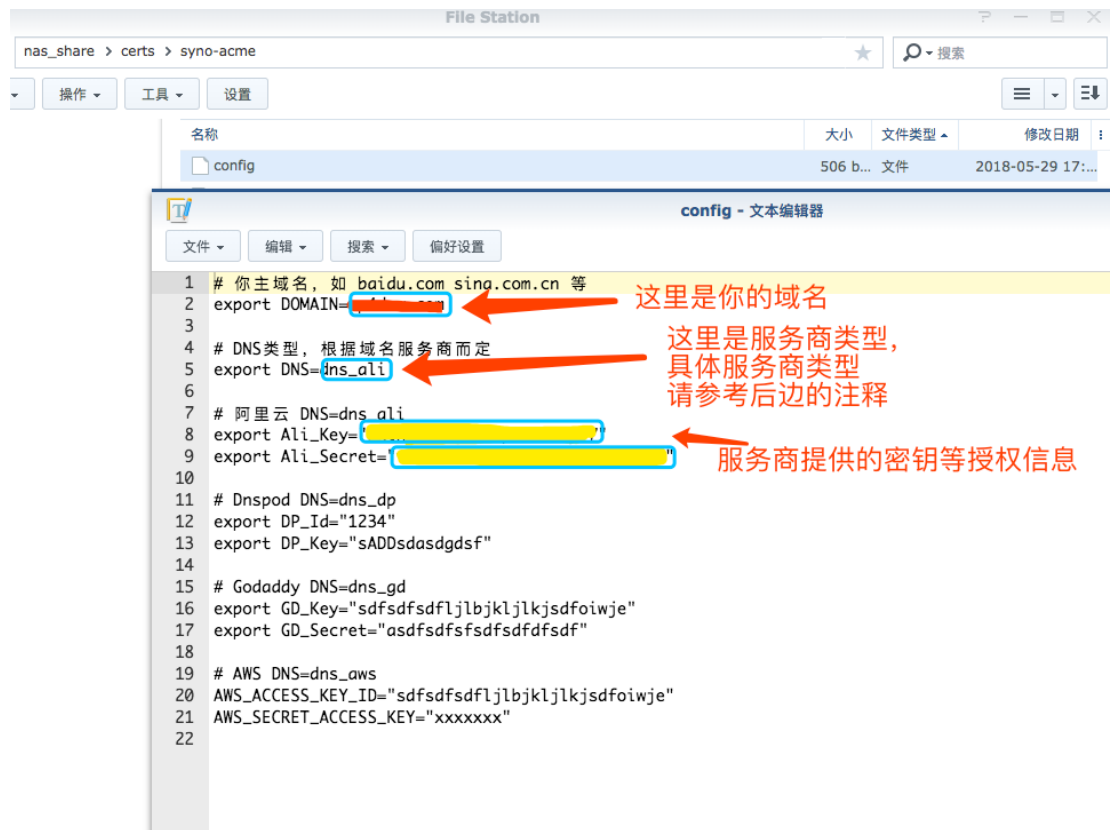
可以通过 File Station 将下载的工具上传到 NAS 的任意目录下，并解压。

解压后大概是这个样子：



### 3. 配置脚本参数

编辑脚本的配置文件 config:



如图所示，需要编辑的几个字段我用蓝框标记出来了。

首先是 DOMAIN，也就是你的域名。

然后是 DNS 的类型，根据服务商的不同，DNS 类型各不相同，比如阿里云（dns\_ali），Dnspod（dns\_dp），Godaddy（dns\_gd）等。

最后要根据不同的域名服务商提供的授权密钥等信息，比如我的域名服务商是阿里云，我需要编辑 Ali\_Key 和 Ali\_Secret 字段，字段的内容需要到域名服务商的管理后台来查看，因为不同的服务商的查看方式不同，请大家根据自己的实际情况去查找。

需要指出的是，我给出的配置文件模板并没有给出所有 acme.sh 支持的域名服务商，大家可以参照 <https://github.com/acmesh-official/acme.sh/tree/master/dnsapi> 来添加自己的配置。一般情况下，这个页面每个文件对应一个域名服务商，比如 `dns_ali.sh` 就是对应阿里云，文件名去掉 `.sh` 扩展名就是 DNS 类型，比如阿里云的 DNS 类型就是 `dns_ali`。打开对应文件，一般都可以在文件的头部找到需要设置的授权信息对应的密钥，比如阿里云的授权密钥所在的位置如下图所示：



```
1 #!/usr/bin/env sh
2
3 Ali_API="https://alidns.aliyuncs.com/"
4
5 #Ali_Key="LTqIA87h0Kdjev5f5"
6 #Ali_Secret="0p5EYueFNq501xnCPzKNbx6K51qPH2"
7
8 #Usage: dns_ali_add _acme-challenge.www.domain.com "XKrxpRBosdIKFzxW_CT3KLZNf6q0HG9i01zxXp5CPBs"
9 dns_ali_add() {
10     fulldomain=$1
11     txtvalue=$2
12
13     Ali_Key="${Ali_Key:-$(readaccountconf mutable Ali_Key)}"
14     Ali_Secret="${Ali_Secret:-$(readaccountconf mutable Ali_Secret)}"
```

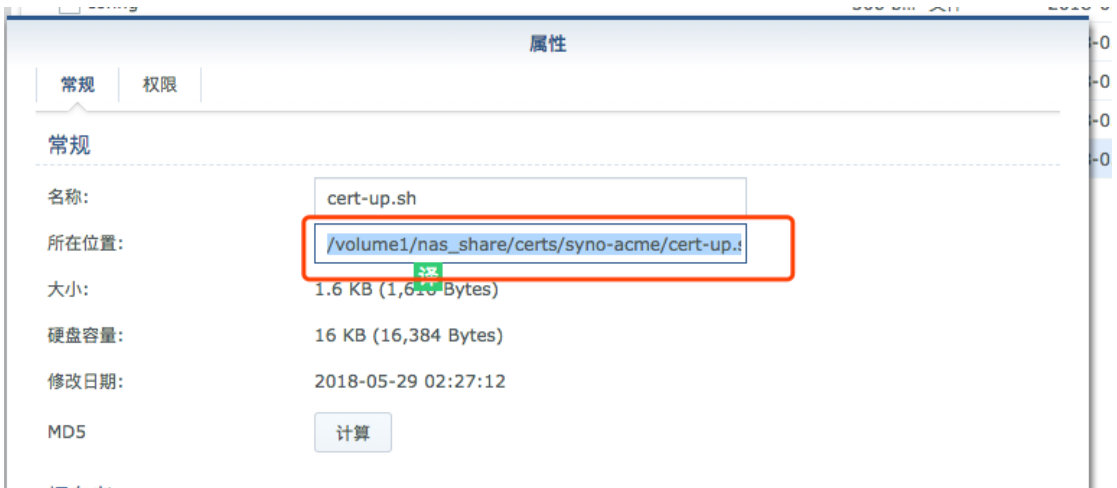
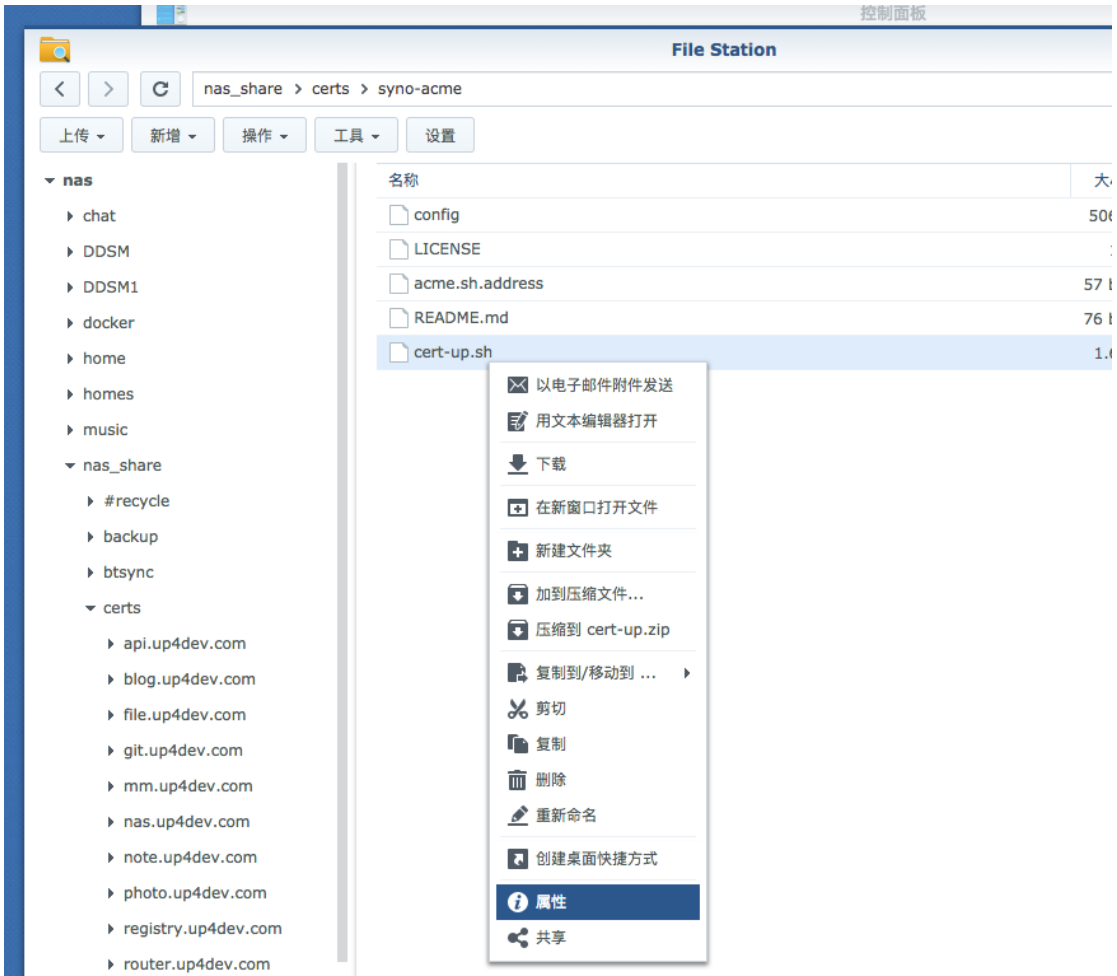
`config` 模板中没有的服务商，请大家自行完善。

[^2018.05.31]: 针对评论区同学提出的 Linode 的 API 生效时间的问题，增加了一个配置参数 `DNS_SLEEP`，出现类似问题的话可以通过修改增大这个参数来解决。

## 4. 配置定时任务

### i. 查找脚本路径

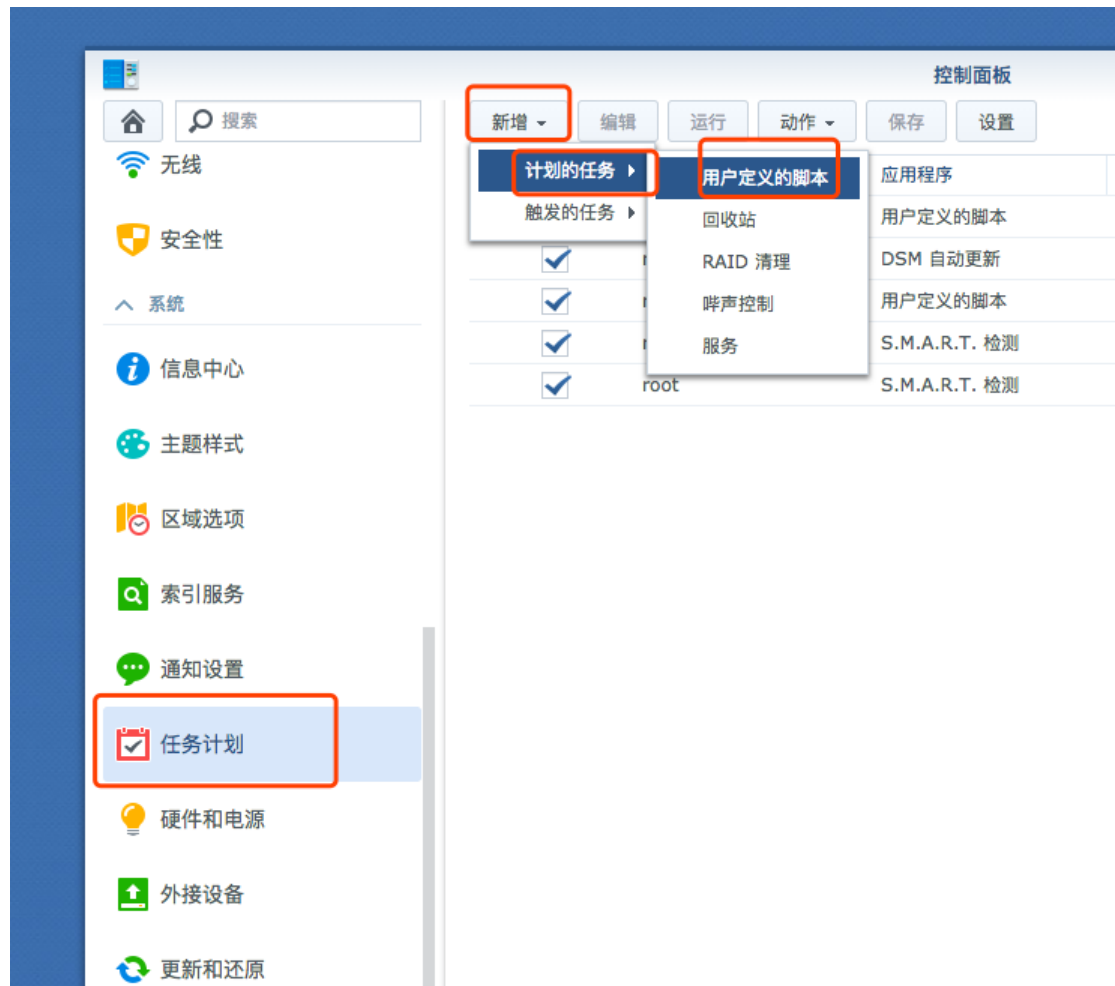
在 File Station 中定位到下载的一键脚本的目录，查看该脚本的绝对路径：



复制完整的绝对路径到剪贴板。

## ii. 创建定时任务

打开 控制面板 / 任务计划 / 新增 / 计划的任务 / 用户自定义的脚本：



设置任务名称和操作用户，需要注意的是这里一定要选择 root：

创建任务

常规

计划

任务设置

一般设置

任务名称:

cet\_update

...

6

用户帐号:

root

▼

☒

已启动

确定

取消

设置计划的时间和周期，这里只支持按月或者年重复，我们只能取按月重复才能满足 Let's Encrypt 至少 3 个月更新一次的要求：

创建任务

常规

计划

任务设置

日期

☐ 在以下天中运行

每天

☒ 在以下日期运行

2018/5/29

每月重复

时间

首次运行时间:

00 : 00

运行频率:

每日一次

最后运行时间:

00:00

确定

取消

设置执行脚本，这里我们将脚本的输出重定向到了一个 `log.txt` 的文件中，以方便后期查看脚本的执行情况：



创建任务

常规

计划

任务设置

通知设置

☐

通过电子邮件发送运行详情 

电子邮件:

admin@example.com


☐

仅在脚本异常终止时发送运行详情

运行命令

用户定义的脚本

```
/volume1/nas_share/certs/syno-acme/cert-up.sh >>  
/volume1/nas_share/certs/syno-acme/log.txt 2>&1|
```



确定

取消

上图红框中的脚本命令为(注意没有换行):

```
/volume1/nas_share/certs/syno-acme/cert-up.sh update >>  
1/volume1/nas_share/certs/syno-acme/log.txt 2>&1
```

具体的路径是步骤 i 中复制的路径。

### iii. 试运行脚本

可以在新建的任务上点击右键立即执行任务:

控制面板						
<div> <span>新增 ▾</span> <span>编辑</span> <span>运行</span> <span>动作 ▾</span> <span>保存</span> <span>设置</span> </div>						
<input checked="" type="checkbox"/> 已启动	拥有者	应用程序	任务名称	动作	下次运行时间	
<input checked="" type="checkbox"/>	root	用户定义的脚本	GitLab2OneDrive	运行: /bin/rsync -av /v...	2018-05-30 04	
<input checked="" type="checkbox"/>	root	DSM 自动更新	DSM Auto Update	下载 DSM 更新	2018-06-04 03	
<input checked="" type="checkbox"/>	root	S.M.A.R.T. 检测	Auto S.M.A.R.T. Test	对所有的硬盘进行快速检测	2018-06-20 00	
<input checked="" type="checkbox"/>	root	用户定义的脚本	cet_update	运行: /volume1/nas_sh...	2018-06-29 00	
<input checked="" type="checkbox"/>	root	S.M.A.R.T. 检测	Auto S	对所有的硬盘进行完整检测	2018-11-04 00	

编辑
删除
运行

这样脚本就会运行，自动更新证书，并重启 web 服务器加载新的脚本。以后，NAS 会每隔一个月执行一次该脚本，自动更新证书。

## iv. 回滚

脚本里提供了回滚命令，可以通过 ssh 登录到 nas，定位到对应目录，执行如下命令回滚证书目录到备份的状态：

```
1/volume1/nas_share/certs/syno-acme/cert-up.sh revert
```

## 总结

这个一键脚本的特点是最大限度的触碰系统文件，仅 `/usr/syno/etc/certificate/_archive` 目录会被更改。`acme.sh` 工具随用随时下载，保持最新，用完即删除，不占用磁盘空间。

这基本就是本文的全部了，如果大家使用中遇到问题，可以在这里留言或者到 <https://github.com/andyzhshg/syno-acme/issues> 提 issue。