链滴

acme.sh 申请 ssl 证书 体验云端的感觉

作者：yuanhenglizhen

原文链接：https://ld246.com/article/1539067893801

来源网站：链滴

1.环境准备

Centos6.9

Tomcat+nginx

Acme.sh

2.安装acme.sh

下载工具

```
curl https://get.acme.sh | sh
```

执行下面的命令让acme全局生效

```
source ~/.bashrc
```

3.签发证书

生成证书

```
 acme.sh --issue -d wx.123.com  -w  /usr/share/nginx/html --force
```

删掉证书

```
rm -rf /root/.acme.sh/wx.123.com/
```

查看列表

```
acme.sh list
```

```
Main\_Domain    KeyLength  SAN\_Domains  Created                    Renew

wx.ihodoo.com  ""         no          Tue Oct  9 05:05:10 UTC 2018  Sat Dec  8 05:05:10 UTC 2018
```

4.应用证书

新建证书文件夹

```
mkdir -p /etc/nginx/ssl
```

```
acme.sh --install-cert -d wx.123.com --key-file /etc/nginx/ssl/wx.123.com.key  --fullchain-file etc/nginx/ssl/wx.123.com.crt --reloadcmd"service nginx force-reload"
```

加强安全级别

```
openssl dhparam -out /etc/nginx/ssl/dhparam.pem 2048
```

5.修改nginx配置

修改配置文件

vi /etc/nginx/conf.d/123.conf

```
 ssl_dhparam /etc/nginx/ssl/dhparam.pem;

 ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

 ssl_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-G
M-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AE
256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECD
A-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES25
-SHA384:ECDHE-EC

 DSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-S
A:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-R
A-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-     GCM-SHA256:AES256-GCM-SHA384:
ES128-SHA256:AES256-SHA256:AES128-       SHA:AES2

  56-SHA:DES-CBC3-SHA:!DSS';

  ssl_prefer_server_ciphers on;

  ssl_session_cache shared:SSL:50m;

  ssl_session_timeout 1d;
```

此处是证书文件

```
  ssl\_certificate /etc/nginx/ssl/wx.123.com.crt;

  ssl\_certificate\_key /etc/nginx/ssl/wx.123.com.key;
```

开启 HSTS Preload 支持

```
    add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";

    add_header X-Frame-Options SAMEORIGIN;

    add_header X-Content-Type-Options nosniff;

    add_header X-XSS-Protection "1; mode=block";
```

6.测试nginx重启

```
nginx -t

Nginx -s reload
```

7.自动更新证书

手动更新命令

```
acme.sh --cron -f
```

自动更新这边不知道为啥acme自己添加进去了

还有个方式是手动添加

8.其他说明

Let's Encrypt 的证书有效期是 90 天的，你需要定期 renew 重新申请，这部分 acme.sh 以及帮你做，在安装的时候往 crontab 增加了一行每天执行的命令 acme.sh --cron:

```
$ crontab -l

0 0 \* \* \* "/root/.acme.sh"/acme.sh --cron --home "/root/.acme.sh" > /dev/null
```

PS: 下面这段你可以尝试执行一下，看看是否正确

"/root/.acme.sh"/acme.sh --cron --home "/root/.acme.sh"

这样就是正常的:

```
[Fri Dec 23 11:50:30 CST 2016\] Renew: 'wx.123.com'

[Fri Dec 23 11:50:30 CST 2016\] Skip, Next renewal time is: Tue Feb 21 03:20:54 UTC 2017

[Fri Dec 23 11:50:30 CST 2016\] Add '--force' to force to renew.

[Fri Dec 23 11:50:30 CST 2016\] Skipped wx.123.com
```

acme.sh --cron 命令执行以后将会 申请新的证书 并放到相同的文件路径。由于前面执行 --installcert 的时候告知了重新 Nginx 的方法，acme.sh 也同时会在证书更新以后重启 Nginx。

9.遇到的问题

```
acme.sh SSL: error:0906D06C:PEM routines:PEM\_read\_bio:no start line:Expecting: ANY PRIV
TE KE Y error:140B0009:SSL routines:SSL_CTX_use_PrivateKey_file:PEM lib
```

看到上面的报错说明最开的生成证书有问题 需要把证书删掉重新生成