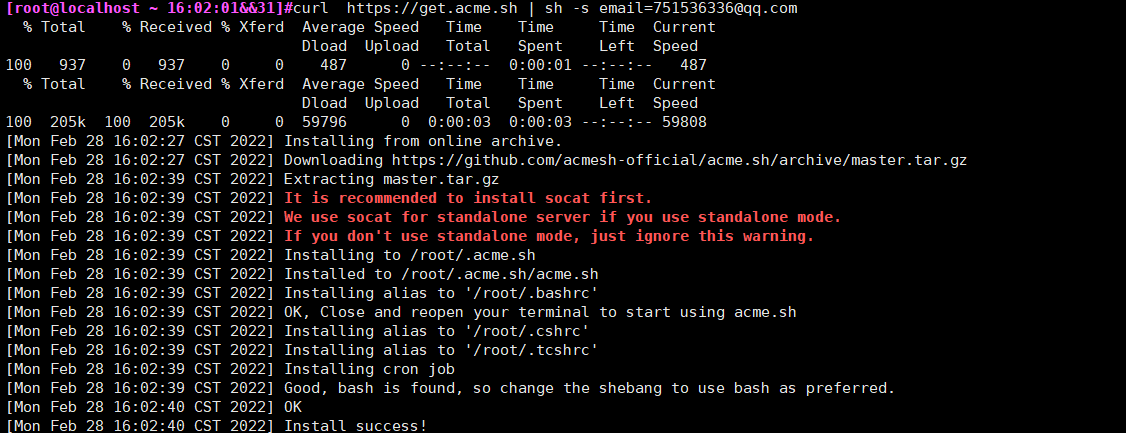
**Let's Encrypt 证书申请及配置**

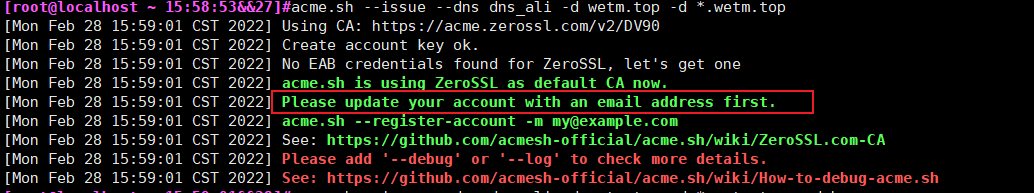
## **一、在线安装**

#yum install openssl

#curl https://get.acme.sh | sh -s [email=751536336@qq.com](mailto:email=751536336@qq.com)

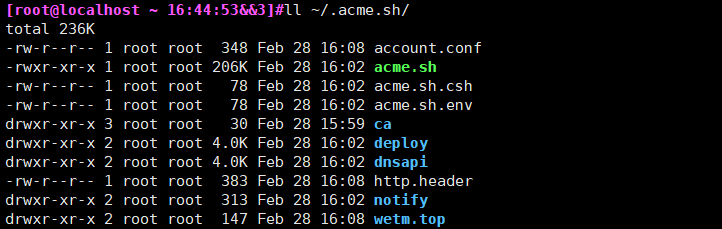


需添加email 否则会不成功



#source ~/.bashrc

home 目录下生成 .acme.sh 文件夹，查看文件夹内容：ls ~/.acme.sh/



## **二、获取证书**

acme.sh强大之处在于，可以自动配置DNS，不用去域名后台操作解析记录了，我的域名是在阿里注册的，下面给出阿里云解析的例子，其他地方注册的请参考这里自行修改：[传送门](https://github.com/Neilpang/acme.sh/wiki/How-to-issue-a-cert)

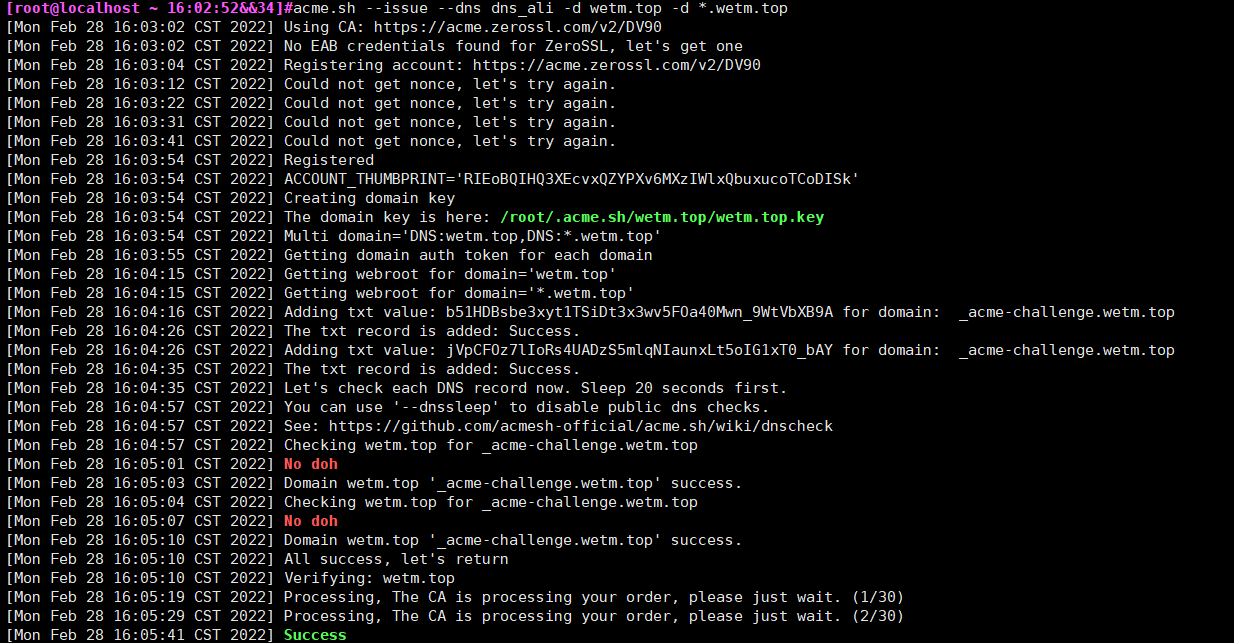
请先前往阿里云后台获取App\_Key跟App\_Secret [传送门](https://ram.console.aliyun.com/manage/ak)，然后执行以下脚本

|  |
| --- |
| # 替换成从阿里云后台获取的密钥  export Ali\_Key="LTAI5tS9jc9rc1p89rezjY2Q"  export Ali\_Secret="otuVHbSqZaHutGNeAKkiUzWueJVvnY"  # 换成自己的域名  acme.sh --issue --dns dns\_ali -d wetm.top -d \*.wetm.top |

#export Ali\_Key="LTAI5tS9jc9rc1p89rezjY2Q"

#export Ali\_Secret="otuVHbSqZaHutGNeAKkiUzWueJVvnY"

#acme.sh --issue --dns dns\_ali -d wetm.top -d \*.wetm.top



|  |
| --- |
| [root@localhost ~ 17:57:01&&11]#acme.sh --issue --dns dns\_ali -d wetm.top -d \*.wetm.top  [Thu Mar 17 17:57:19 CST 2022] Using CA: https://acme.zerossl.com/v2/DV90  [Thu Mar 17 17:57:20 CST 2022] Create account key ok.  [Thu Mar 17 17:57:20 CST 2022] No EAB credentials found for ZeroSSL, let's get one  [Thu Mar 17 17:57:23 CST 2022] Registering account: https://acme.zerossl.com/v2/DV90  [Thu Mar 17 17:57:39 CST 2022] Registered  [Thu Mar 17 17:57:39 CST 2022] ACCOUNT\_THUMBPRINT='KalpVC\_dZK5pa5xQD4OTSm1ozV5d5N7HL8t70uNlf\_o'  [Thu Mar 17 17:57:39 CST 2022] Creating domain key  [Thu Mar 17 17:57:39 CST 2022] The domain key is here: /root/.acme.sh/wetm.top/wetm.top.key  [Thu Mar 17 17:57:39 CST 2022] Multi domain='DNS:wetm.top,DNS:\*.wetm.top'  [Thu Mar 17 17:57:39 CST 2022] Getting domain auth token for each domain  [Thu Mar 17 17:58:05 CST 2022] Getting webroot for domain='wetm.top'  [Thu Mar 17 17:58:05 CST 2022] Getting webroot for domain='\*.wetm.top'  [Thu Mar 17 17:58:05 CST 2022] Adding txt value: jVhKc4gnd8c3fDpgdWpphRD2VQUkJarJnjUNgUTjHZQ for domain: \_acme-challenge.wetm.top  [Thu Mar 17 17:58:28 CST 2022] The txt record is added: Success.  [Thu Mar 17 17:58:28 CST 2022] Adding txt value: UJNVpymcxsCf4cJucsAvLfAJ8o4taqZvD5hizznOsn4 for domain: \_acme-challenge.wetm.top  [Thu Mar 17 17:58:37 CST 2022] The txt record is added: Success.  [Thu Mar 17 17:58:37 CST 2022] Let's check each DNS record now. Sleep 20 seconds first.  [Thu Mar 17 17:58:58 CST 2022] You can use '--dnssleep' to disable public dns checks.  [Thu Mar 17 17:58:58 CST 2022] See: https://github.com/acmesh-official/acme.sh/wiki/dnscheck  [Thu Mar 17 17:58:58 CST 2022] Checking wetm.top for \_acme-challenge.wetm.top  [Thu Mar 17 17:59:03 CST 2022] No doh  [Thu Mar 17 17:59:17 CST 2022] Domain wetm.top '\_acme-challenge.wetm.top' success.  [Thu Mar 17 17:59:17 CST 2022] Checking wetm.top for \_acme-challenge.wetm.top  [Thu Mar 17 17:59:30 CST 2022] No doh  [Thu Mar 17 17:59:33 CST 2022] Domain wetm.top '\_acme-challenge.wetm.top' success.  [Thu Mar 17 17:59:33 CST 2022] All success, let's return  [Thu Mar 17 17:59:33 CST 2022] Verifying: wetm.top  [Thu Mar 17 17:59:40 CST 2022] Processing, The CA is processing your order, please just wait. (1/30)  [Thu Mar 17 17:59:51 CST 2022] Processing, The CA is processing your order, please just wait. (2/30)  [Thu Mar 17 18:00:00 CST 2022] Success  [Thu Mar 17 18:00:00 CST 2022] Verifying: \*.wetm.top  [Thu Mar 17 18:00:08 CST 2022] Processing, The CA is processing your order, please just wait. (1/30)  [Thu Mar 17 18:00:36 CST 2022] Success  [Thu Mar 17 18:00:36 CST 2022] Removing DNS records.  [Thu Mar 17 18:00:36 CST 2022] Removing txt: jVhKc4gnd8c3fDpgdWpphRD2VQUkJarJnjUNgUTjHZQ for domain: \_acme-challenge.wetm.top  [Thu Mar 17 18:00:53 CST 2022] Removed: Success  [Thu Mar 17 18:00:53 CST 2022] Removing txt: UJNVpymcxsCf4cJucsAvLfAJ8o4taqZvD5hizznOsn4 for domain: \_acme-challenge.wetm.top  [Thu Mar 17 18:01:15 CST 2022] Removed: Success  [Thu Mar 17 18:01:15 CST 2022] Verify finished, start to sign.  [Thu Mar 17 18:01:15 CST 2022] Lets finalize the order.  [Thu Mar 17 18:01:15 CST 2022] Le\_OrderFinalize='https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA/finalize'  [Thu Mar 17 18:01:22 CST 2022] Order status is processing, lets sleep and retry.  [Thu Mar 17 18:01:22 CST 2022] Retry after: 15  [Thu Mar 17 18:01:39 CST 2022] Polling order status: https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA  [Thu Mar 17 18:01:46 CST 2022] Order status is processing, lets sleep and retry.  [Thu Mar 17 18:01:46 CST 2022] Retry after: 15  [Thu Mar 17 18:02:02 CST 2022] Polling order status: https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA  [Thu Mar 17 18:02:15 CST 2022] Order status is processing, lets sleep and retry.  [Thu Mar 17 18:02:15 CST 2022] Retry after: 15  [Thu Mar 17 18:02:31 CST 2022] Polling order status: https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA  [Thu Mar 17 18:02:43 CST 2022] Order status is processing, lets sleep and retry.  [Thu Mar 17 18:02:43 CST 2022] Retry after: 15  [Thu Mar 17 18:02:59 CST 2022] Polling order status: https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA  [Thu Mar 17 18:03:07 CST 2022] Order status is processing, lets sleep and retry.  [Thu Mar 17 18:03:07 CST 2022] Retry after: 15  [Thu Mar 17 18:03:24 CST 2022] Polling order status: https://acme.zerossl.com/v2/DV90/order/iXL7KtGRXM\_YI-5bKmUgrA  [Thu Mar 17 18:03:32 CST 2022] Downloading cert.  [Thu Mar 17 18:03:32 CST 2022] Le\_LinkCert='https://acme.zerossl.com/v2/DV90/cert/5csRHsA9vxGF2NYbFFQ4gg'  [Thu Mar 17 18:03:39 CST 2022] Cert success.  -----BEGIN CERTIFICATE-----  MIIGazCCBFOgAwIBAgIQAdsw/yCpJVGBuo3cEoaGQjANBgkqhkiG9w0BAQwFADBL  MQswCQYDVQQGEwJBVDEQMA4GA1UEChMHWmVyb1NTTDEqMCgGA1UEAxMhWmVyb1NT  TCBSU0EgRG9tYWluIFNlY3VyZSBTaXRlIENBMB4XDTIyMDMxNzAwMDAwMFoXDTIy  MDYxNTIzNTk1OVowEzERMA8GA1UEAxMId2V0bS50b3AwggEiMA0GCSqGSIb3DQEB  AQUAA4IBDwAwggEKAoIBAQC8MetdyII3lQja0J4ptEnc7Tq5ICEktnOxGAQtzSX2  6JObIAGrupnDcDst+n1qTdcyjKk28tMJEk9BbUZDMZiTh8Wv0by9TiTcw8CyT8UI  BjTodd79uykubUlyg5qINoPWUaBE6vWFQEvcdd/+qeXx1Y9ubE59tlMUmSCExwJf  VG4KCiyYA9XF/r6OkHliB91gd/D+fD1SWNKtfZf8bjOSzcAjPI8DU8NV4zWrwBh/  XB73Oin3apxsBvxCFuw+CCDrN9nbIPc4NCVAL5POtUGaMATHbTS4jit5oaLPX2U/  pNNaglyPLamNxt/Yee7yKuSVLEyoor+g4XLJ9JrPUgQNAgMBAAGjggKBMIICfTAf  BgNVHSMEGDAWgBTI2XhootkZaNU9ct5fCj7ctYaGpjAdBgNVHQ4EFgQUD6+snosz  Ej4zEKaCBDcRxz5tBTgwDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYD  VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMEkGA1UdIARCMEAwNAYLKwYBBAGy  MQECAk4wJTAjBggrBgEFBQcCARYXaHR0cHM6Ly9zZWN0aWdvLmNvbS9DUFMwCAYG  Z4EMAQIBMIGIBggrBgEFBQcBAQR8MHowSwYIKwYBBQUHMAKGP2h0dHA6Ly96ZXJv  c3NsLmNydC5zZWN0aWdvLmNvbS9aZXJvU1NMUlNBRG9tYWluU2VjdXJlU2l0ZUNB  LmNydDArBggrBgEFBQcwAYYfaHR0cDovL3plcm9zc2wub2NzcC5zZWN0aWdvLmNv  bTCCAQUGCisGAQQB1nkCBAIEgfYEgfMA8QB3AEalVet1+pEgMLWiiWn0830RLEF0  vv1JuIWr8vxw/m1HAAABf5dUQOkAAAQDAEgwRgIhALVqQ+lLQRvvL6hPlDuACkMp  TBf6tpK1D7jtv0SN0JRWAiEA4zjRK46hhhsH1yVTeudrnwfEgsdFqafBSZU+IyjU  yRsAdgBByMqx3yJGShDGoToJQodeTjGLGwPr60vHaPCQYpYG9gAAAX+XVEDUAAAE  AwBHMEUCIDAM25QRpDJwg0RB+Z+tHe+wYjp3Chci4EFqfqYSmikTAiEA5by+A0re  KjD04Er5VnBwymUzkVxL/GST+6c4uXr329owHwYDVR0RBBgwFoIId2V0bS50b3CC  Cioud2V0bS50b3AwDQYJKoZIhvcNAQEMBQADggIBAAFtOw32HV+OER5M+iprBoS5  VrYHdEANJCDf8q9lktQrqEEt17h9udtyDaQlykGWtz3gcesEK4kHHlsS5nhjezPh  TV6FGY/sMlJSLyMvxEhIEdKm06dw2YY4E4nbM+pa2MixOu3zPMlKpA12Wn22nME/  kNHfwc3kfGojPiO3wO+urFM9ohpy6lmRwZM+wAiiHsYUBUoRfBfJwN41VUU2V+bC  DDVGDfmAyoZho48o2lqlfJ503qbN13cS1x830xGqNEWee/zVGero0NO2NwVEhZfl  IfiwY5+nMW1ealkx79qyTSUYF0XDCDSXE+grevR7TfY9wmmoAhGGwaaZR4V8Ylhq  kXkDNdUha2BivUCIFliYslmnAS2K910d/lAR51bSjKD6V3d0ETaoDoTxqeaHNqV5  2hdkscmuMWI4QrPbEtTIQn6xZ7doF+0pF+eMvdEGdjswBaDD/dgJgoeou5DRRCGZ  qVInW8ItLdCke8veAfEpg9PuFTrlFyQaoXkzt3kLJ8RtbsM0qM/Wo33rwbtv0bV+  cR/Rdb7xv2KMLQHClzi4nQa30XiasJPQjtpuJbYsGS4tHQuMt/Dgo4boQJhbkAv6  /T6I68C39bSzhlLwQOWXzIpbJ3Mk6ZlNvF7n4zj+o4wCknMTEmSXahhoTwAWUen9  YFbB7F+17JNU7bXjpuky  -----END CERTIFICATE-----  [Thu Mar 17 18:03:39 CST 2022] Your cert is in: /root/.acme.sh/wetm.top/wetm.top.cer  [Thu Mar 17 18:03:39 CST 2022] Your cert key is in: /root/.acme.sh/wetm.top/wetm.top.key  [Thu Mar 17 18:03:39 CST 2022] The intermediate CA cert is in: /root/.acme.sh/wetm.top/ca.cer  [Thu Mar 17 18:03:39 CST 2022] And the full chain certs is there: /root/.acme.sh/wetm.top/fullchain.cer |

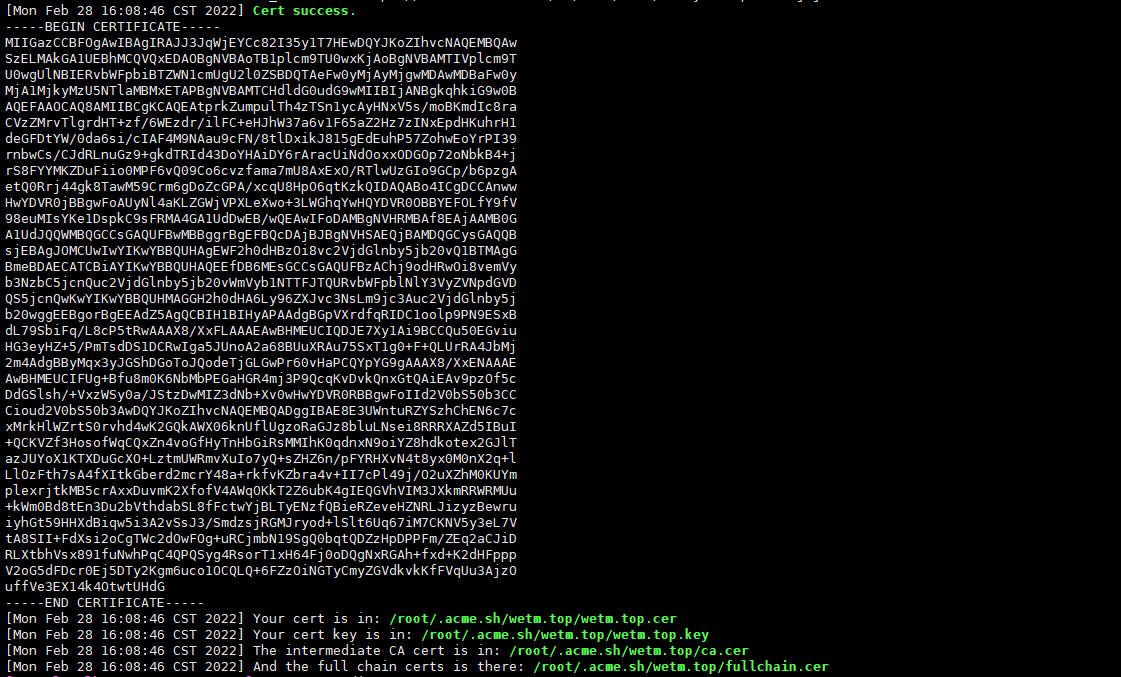
-----END CERTIFICATE-----

[Mon Feb 28 16:08:46 CST 2022] Your cert is in: /root/.acme.sh/wetm.top/wetm.top.cer

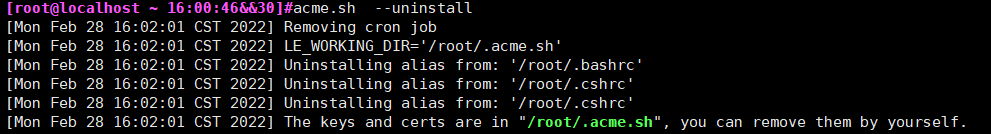
[Mon Feb 28 16:08:46 CST 2022] Your cert key is in: /root/.acme.sh/wetm.top/wetm.top.key

[Mon Feb 28 16:08:46 CST 2022] The intermediate CA cert is in: /root/.acme.sh/wetm.top/ca.cer

[Mon Feb 28 16:08:46 CST 2022] And the full chain certs is there: /root/.acme.sh/wetm.top/fullchain.cer



#acme.sh --uninstall



## **三、更新证书**

目前 Let's Encrypt 的证书有效期是90天，**时间到了会自动更新**，您无需任何操作。 今后有可能会缩短这个时间， 不过都是自动的，不需要您关心。acme.sh安装的时候已经自动添加了一个计划任务每天自动更新证书，更新后重启使用证书的服务。 acme.sh自动添加的计划任务

*#crontab -l | grep acme*



但是，您**也可以强制续签证书**：

acme.sh --renew -d wetm.top --force

## **四、更新 acme.sh**

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

升级 acme.sh 到最新版：

acme.sh --upgrade

如果您不想手动升级,，可以开启自动升级：

acme.sh --upgrade --auto-upgrade

您也可以随时关闭自动更新：

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

## **nginx配置免费证书**

目前 Let's Encrypt 的证书有效期是90天，时间到了会自动更新，您无需任何操作

今后有可能会缩短这个时间， 不过都是自动的，不需要您关心

|  |
| --- |
| server {  listen 443 ssl;  server\_name gitlab.wetm.top;  access\_log /data/nginx/logs/gitlab/access.log main;  charset utf-8;  ssl\_certificate certs/fullchain.cer;  ssl\_certificate\_key certs/wetm.top.key;  ssl\_session\_timeout 5m;  ssl\_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;  ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;  ssl\_prefer\_server\_ciphers on;  location / {  proxy\_redirect http:// https://;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-Ssl on;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  proxy\_pass http://192.168.91.11:10080;  }  } |

<https://blog.csdn.net/qazx123q/article/details/82346221>

<https://blog.csdn.net/qingtian2002/article/details/53691600>

## **六、问题**

使用 Acme.sh 给 SSL 证书自动续期失败，提示Could not get nonce, let's try again的解决方法

<https://www.70ol.com/454.html>

## **七、导出证书**

mkdir -pv /opt/ssl/wetm.top

acme.sh --install-cert -d wetm.top --cert-file /opt/ssl/wetm.top/wetm.top.cert --ca-file /opt/ssl/wetm.top/ca.crt --key-file /opt/ssl/wetm.top/wetm.top.key --fullchain-file /opt/ssl/wetm.top/fullchain.cert

## **八、参考url**

<https://www.jianshu.com/p/1a792f87b6fe>

<https://www.cnblogs.com/sage-blog/p/10302934.html>