三步搞定自签名 https 证书以及自动更新

作者：yuanhenglizhen
原文链接：https://ld246.com/article/1531902759191
来源网站：链滴

第一步.安装certbot

```
yum install certbot -y
```

第二步.生成https签名证书

```
certbot certonly -w /home/wwwroot/blog.mufengs.com -d blog.mufengs.com
```

如图所示

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log

How would you like to authenticate with the ACME CA?
-------------------------------------------------------------------------------
1: Spin up a temporary webserver (standalone)
2: Place files in webroot directory (webroot)
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Plugins selected: Authenticator standalone, Installer None
Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for blog.mufengs.com
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/blog.mufengs.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/blog.mufengs.com/privkey.pem
   Your cert will expire on 2018-10-16. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

[root@vultr blog.mufengs.com]# ll
```

第三步.配置nginx

```
ssl_prefer_server_ciphers on;

ssl_certificate /etc/letsencrypt/live/blog.mufengs.com/fullchain.pem;

ssl_certificate_key /etc/letsencrypt/live/blog.mufengs.com/privkey.pem;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EEC
H+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECD
 EDH+aRSA !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4";

keepalive_timeout 70;

ssl_session_cache shared:SSL:10m;

ssl_session_timeout 10m;
```

```
server {
    listen 80;
    server_name blog.mufengs.com; # 配置为你自己的域名
  rewrite ^(.*)$  https://$host$1 permanent;
    #location / {
    #    proxy_pass http://pipe$request_uri;
    #    proxy_set_header  Host $host:$server_port;
    #    proxy_set_header  X-Real-IP  $remote_addr;
    #    client_max_body_size  10m;
    #}
}


server {
        listen 443;
        ssl on;
        server_name blog.mufengs.com;
        ssl_prefer_server_ciphers on;
        ssl_certificate /etc/letsencrypt/live/blog.mufengs.com/fullchain.pem;
        ssl_certificate_key /etc/letsencrypt/live/blog.mufengs.com/privkey.pem;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA !aNULL !eNULL !LOW
!3DES !MD5 !EXP !PSK !SRP !DSS !RC4";
        keepalive_timeout 70;
        ssl_session_cache shared:SSL:10m;
        ssl_session_timeout 10m;
  location / {
        proxy_pass http://pipe$request_uri;
        proxy_set_header  Host $host:$server_port;
        proxy_set_header  X-Real-IP  $remote_addr;
        client_max_body_size  10m;
    }
}
```

尴尬说错了 四步

第四步.将自动更新加到定时任务中

0 3 * * 2,4,6 certbot renew -q –pre-hook "service nginx stop" –post-hook "service nginx start"