http与https的区别

阿里云、腾讯云免费一年ssl证书

Encryp免费证书

1、Let's Encrypt是国外一个公共的免费SSL项目，由 Linux 基金会托管，它的来头不小，由Mozilla、思科、Akamai、IdenTrust和EFF等组织发起，目的就是向网站自动签发和管理免费证书，以便加速互联网由HTTP过渡到HTTPS。

官方网站：

https://letsencrypt.org/

1、安装Let's Encrypt前的准备工作

```
#检查系统是否安装git,如果已经自带有git会出现git版本号，没有则需要我们自己安装
git --version
#git 安装
yum install git
#检查Python的版本是否在2.7以上
python -V //2.6版本
#安装python所需的包
yum install zlib-devel bzip2-devel openssl-devel ncurses-devel sqlite-devel

#获取到Python
cd /usr/local/src
wget https://www.python.org/ftp/python/2.7.12/Python-2.7.12.tar.xz
#解压Python2.7.12
tar -zxvf Python-2.7.12.tar.xz
#编译python
cd Python-2.7.12/
./configure --prefix=/usr/local/python2.7
make && make install
#建立链接
ln -s /usr/local/python2.7/bin/python2.7 /usr/local/bin/python
```

```
#解决系统 Python 软链接指向 Python2.7 版本后，因为yum是不兼容 Python 2.7的，所需要指定 yum 的Python版本
# vi /usr/bin/yum
将头部的
#!/usr/bin/python
改成
#!/usr/bin/python2.6.6
```

2.获取Let's Encrypt免费SSL证书

```
#获取letsencrypt
git clone https://github.com/letsencrypt/letsencrypt
#进入letsencrypt目录
cd letsencrypt
```

生成证书

1.服务器80端口不能被占用

2.l.funet8.com域名需要解析到此服务器。

```
./letsencrypt-auto certonly --standalone --email star@funet8.com -d l.funet8.com -d l2.funet8.com
./certbot-auto certonly --standalone --email star@funet8.com -d l.funet8.com
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for l.funet8.com
Cleaning up challenges
Problem binding to port 80: Could not bind to IPv4 or IPv6.

IMPORTANT NOTES:
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
```

```
[root@vpn letsencrypt]# ./certbot-auto certonly --standalone --email star@funet8.com -d l.funet8.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for l.funet8.com
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/l.funet8.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/l.funet8.com/privkey.pem
   Your cert will expire on 2019-08-11. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot-auto
   again. To non-interactively renew *all* of your certificates, run
   "certbot-auto 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
```

l.funet8.com.zip
6.9KB

获取帮助：

```
./letsencrypt-auto --help all

run：获取和安装证书
certonly：获取证书
certificates：查看和--cert-name指定的名称匹配的证书信息
renew：更新快要过期的证书
delete：删除证书
```

letsencrypt简介

letsencrypt客户端插件的功能包括两个部分：认证和安装。

认证插件通过certonly命令启用，认证功能用于确认你是域名的所有者，并为你的域名获取证书，证书被放置在你的域名所在服务器的/etc/letsencrypt/live/[domain]目录。如果你一次性对多个域名进行认证，则这些域名将共用一个证书文件。

3.Let's Encrypt免费SSL证书获取与应用

在完成Let's Encrypt证书的生成之后，我们会在"/etc/letsencrypt/live/l.funet8.com/"域名目录下有4个文件就是生成的密钥证书文件。

```
cert.pem - Apache服务器端证书
chain.pem - Apache根证书和中继证书
fullchain.pem - Nginx所需要ssl_certificate文件
privkey.pem - 安全证书KEY文件
```

如果我们使用的Nginx环境，那就需要用到fullchain.pem和privkey.pem两个证书文件，在部署Nginx的时候需要用到。在Nginx环境中，只要将对应的ssl_certificate和ssl_certificate_key路径设置成我们生成的2个文件就可以。

```
#打开linux配置文件，找到HTTPS 443端口配置的server
 ssl_certificate /etc/letsencrypt/live/l.funet8.com/fullchain.pem;
 ssl_certificate_key /etc/letsencrypt/live/l.funet8.com/privkey.pem;
```

4.解决Let's Encrypt免费SSL证书有效期问题

Let's Encrypt默认是90天免费，需要手工或者自动续期才可以继续使用。

自动提交续费，需要更新pem文件。

```
 ./letsencrypt-auto certonly --renew-by-default --email star@funet8.com -d l.funet8.com
```

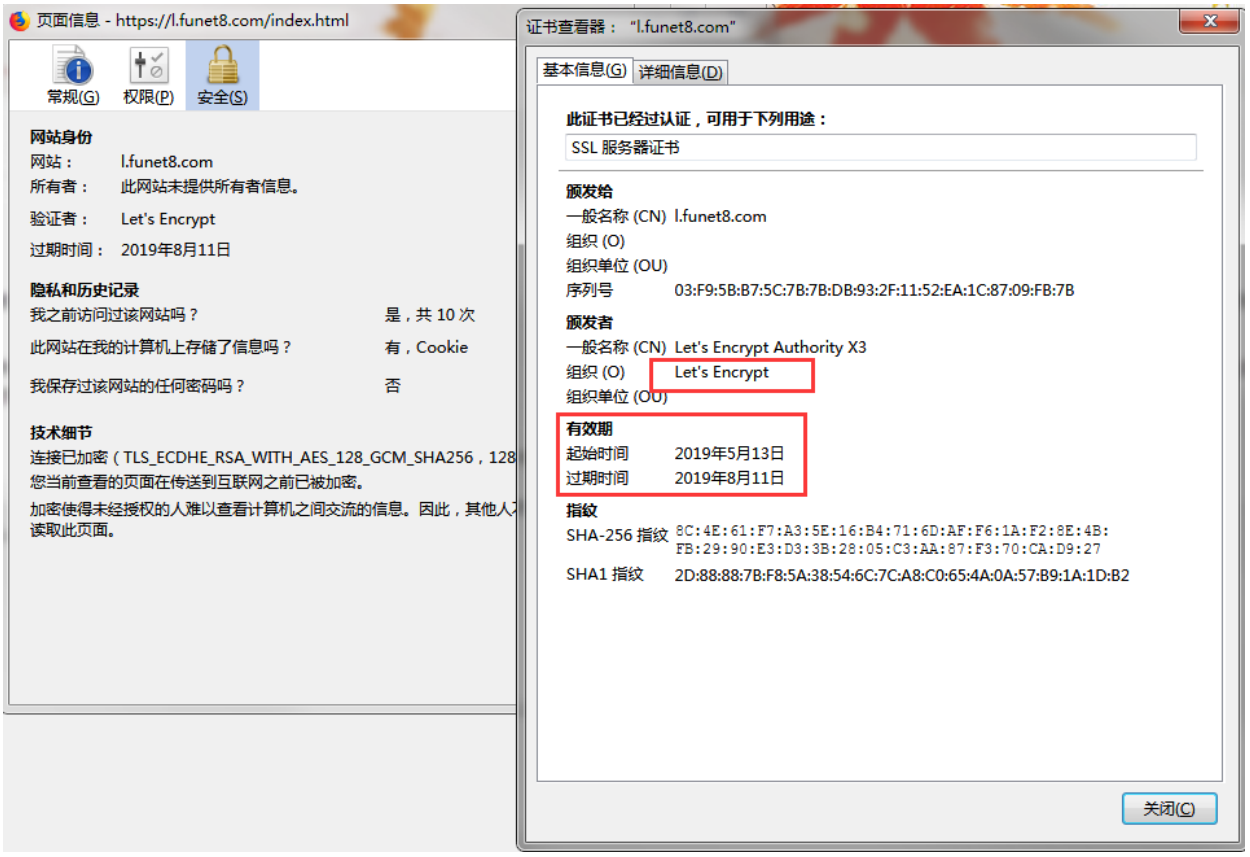
5.nginx配置站点

```
###############l.funet8.com#############################
server {
 listen 443;
 server_name l.funet8.com;
 access_log /data/wwwroot/log/ssl_l.funet8.com-access.log ;
 error_log /data/wwwroot/log/ssl_l.funet8.com-nginx-error.log;
 root /data/wwwroot/web/l.funet8.com/;

 ssl on;
  ssl_certificate /data/wwwroot/web/cert/l.funet8.com/cert.pem;
  ssl_certificate_key /data/wwwroot/web/cert/l.funet8.com/privkey.pem;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers ALL:!DH:!EXPORT:!RC4:+HICH:+MEDIUM:!LOW:!aNULL:!eNULL;

  location / {
  index index.html index.htm index.php;
  }
  location ~ .*\.(php|php5)?$ {
  proxy_pass http://centos6_httpd_php56:8080;
  proxy_redirect off;
  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
```

```
23    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
24    }
25    #静态文件缓存
26    include /etc/nginx/conf.d/static_cache.conf;
27
28  }
```



Redhat或CentOS 6可能需要配置EPEL软件源，Python需要2.7版本以上。

https://www.cnblogs.com/cheyunhua/p/9413935.html