链滴

运维 -- 网站配置 HTTPS

作者：james
原文链接：https://ld246.com/article/1507562788905
来源网站：链滴

配置https

1. 获取证书

- Let's Encrypt是一个免费CA： 官网
- 使用手册： https://letsencrypt.org/how-it-works/
- 使用该网站有许多客户端工具，我使用的是： https://www.sslforfree.com/
  - ++按照提示来做就可以了++

2.0 安装证书

- 参考： How to install SSL certificates

2. 给Nginx配置https协议：

- 注意如果Nginx是编译安装的，需要安装模块ngx_http_ssl_module。如果不安装，则有以下错误：

```
/ # nginx -t -c /nginxssl.conf
nginx: [emerg] unknown directive "ssl" in /nginxssl.conf:42
nginx: configuration file /nginxssl.conf test failed
```

- 需要配置的部分就是以下部分：

```
server {
  listen 443;
  ssl on; //必须安装ngx_http_ssl_module模块
  ssl_certificate cert.pem; //证书文件
  ssl_certificate_key key.pem; //证书对应的私钥文件
  ssl_session_timeout 5m;
  ssl_protocols SSLv2 SSLv3 TLSv1;
  ssl_ciphers HIGH:!aNULL:!MD5;
  ssl_prefer_server_ciphers on;

  access_log logs/access.log;
  error_page 404 = @notfound;
  location / {
    root /website_files;
    default_type "text/html";
    try_files $uri $uri.html $uri/index.html index.html;
  }
 }
```

- 官网给出的教程： 教程
- 操作便利的一个教程： 给Nginx配置一个自签名的SSL证书
- 检测配置文件没问题后重新读取 Nginx 即可:

```
nginx -t && nginx -s reload
[root@bwh nginx]# nginx -t
```

```
nginx: [emerg] PEM_read_bio_X509_AUX("/etc/nginx/cert_chain.crt") failed (SSL: error:0906D0
6:PEM routines:PEM_read_bio:bad end line)
nginx: configuration file /etc/nginx/nginx.conf test failed
[root@bwh nginx]# nginx -t
nginx: [emerg] SSL_CTX_use_PrivateKey_file("/etc/nginx/private.key") failed (SSL: error:0B0800
4:x509 certificate routines:X509_check_private_key:key values mismatch)
nginx: configuration file /etc/nginx/nginx.conf test failed
```

-

- 默认是 SHA-1 形式，而现在主流的方案应该都避免 SHA-1，为了确保更强的安全性，我们可以采迪菲 - 赫尔曼密钥交换。参考：Nginx 配置 SSL 证书 + 搭建 HTTPS 网站教程的后半部分。
- HTTPS服务器优化：参考： HTTPS服务器优化后半部分

3. 给Tomcat配置HTTPS协议：

- 参考： Java Web教程：Tomcat的https连接器
-

4. 给浏览器配置自签名证书，来信任指定网站

- 由于https证书是自签名的，配置了域名，浏览器前端调用文件上传的时候总是需要自己手动点击任以后才能接口调通，显然不适合客户使用。于是需要把自己颁发的根证书添加到系统信任证书列表，参考下面的文章：
- 给Mac的chrome配置自签名证书