



链滴

Solo -- 添加 HTTPS 加密访问协议

作者: [haiyufuer](#)

原文链接: <https://ld246.com/article/1498230805478>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

随着现在网络安全越来越重要，谷歌甚至将非https协议的网站都列为不安全网站。昨天搭建完简单博客系统后，今天突然想着给加个https安全协议。下面是记录了一下操作步骤：

1、修改latke.properties中的 serverScheme 为https,否则单纯修改nginx或者Apache会导致页面布错误。

2、修改nginx配置文件：

1. 添加SSL支持协议

```
ssl_certificate /etc/nginx/cert/214ssl.pem; // 申请的证书
```

```
ssl_certificate_key /etc/nginx/cert/214ssl.key; // 申请的证书
```

```
ssl on; //开启SSL协议支持， 否则无法访问
```

```
ssl_session_timeout 5m;
```

```
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!AH:!RC4;
```

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

```
ssl_prefer_server_ciphers on;
```

2) 重定向所有HTTP请求到HTTPS

```
server {
```

```
listen :80;
```

```
server_name yufuer.com www.yufuer.com;
```

```
rewrite ^(.) https://host$1 permanent;
```

```
}
```

3、保存nginx配置文件，重启nginx服务。

说明：

a、对于ngin+Tomcat的服务器配置，只需要在nginx中修改即可。

b、目前SSL证书有好多网站可以申请免费版本，不用自己只做SSL证书(阿里云、七牛)。

c、对于http自动跳转至https，网络多要求修改nginx.conf文件，其本质是各个网站的conf文件，即conf.d 下的各个配置文件。

今天踩到的坑似乎就这么多，后续有想到了再补充。