



链滴

# springboot 项目部署到 ubuntu18.04 的过程, http 跳转 https, 使用 acme.sh 安装证书

作者: [cmlanche](#)

原文链接: <https://ld246.com/article/1557834537899>

来源网站: 链滴

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

最近开发的友链联盟项目即将“竣工”，准备拿到公有云Ubuntu是测试下，想要达到的理想状态有如几点：

1. 端口保持9090，发布spring boot的jar包，后台运行
2. nginx部署，强制https访问应用
3. 使用 [acme.sh](#)来生成、安装ssl证书
4. 开启防火墙，打开80、443端口，关闭9090端口(避免直接访问9090打开应用)

目前已经完成上面的要求，可以尝试访问<http://sitefriendlinks.com>、<http://sitefriendlinks.com:900>，前者会强制跳转到<https://sitefriendlinks.com>，后者无法打开。

## 环境安装

### 1. nginx

```
apt install nginx
```

安装后自动就启动了，你可以用如下命令进行开启和关闭：

```
service nginx stop
service nginx start
service nginx restart # 重启
```

### 2. mysql

```
apt install mysql-server
```

详情请看：<https://www.jianshu.com/p/3821c2603b92>

需要注意修改root密码：

```
show databases;
```

```
use mysql;
```

```
update user set authentication_string=PASSWORD("yourpassword") where user='root';
```

```
update user set plugin="mysql_native_password";
```

```
flush privileges;
```

```
quit;
```

### 3. java 8

```
apt install openjdk-8-jre-headless
```

[参考链接](#)

## 部署nginx

```
server {
    listen    80;
    server_name sitefriendlinks.com;
```

```

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

server {
    listen    443;
    server_name sitefriendlinks.com;
    ssl      on;
    ssl_certificate /etc/nginx/ssl/fullchain.cer;
    ssl_certificate_key /etc/nginx/ssl/sitefriendlinks.com.key;
    ssl_session_timeout 5m;
    ssl_protocols TLSv1;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
    location / {
        proxy_pass          http://localhost:9090/;
        proxy_set_header    Host $host;
        proxy_set_header    X-Real-IP $remote_addr;
        proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header    X-Forwarded-Proto $scheme;
        proxy_set_header    X-Forwarded-Port $server_port;
    }
}

```

## 使用acem.sh安装证书

参考文档: <https://github.com/Neilpang/acme.sh/wiki/%E8%AF%B4%E6%98%8E>

关键步骤:

### 1. 创建别名

```
alias acme.sh=~/.acme.sh/acme.sh
```

### 2. 生成证书

```
acme.sh --issue -d mydomain.com --nginx
```

### 3. 安装证书

```
acme.sh --installcert -d <domain>.com \
    --key-file /etc/nginx/ssl/<domain>.key \
    --fullchain-file /etc/nginx/ssl/fullchain.cer \
    --reloadcmd "service nginx force-reload"
```

**注意, 你需要手动创建/etc/nginx/ssl目录, 不如上面的安装命令会报路径错误**

此时, 你已经能正常用https打开你的网站了

## 打开防火墙

Ubuntu的防火墙命令是ufw, 参考: <https://www.cnblogs.com/yuanlipu/p/7103740.html>

先查询下防火墙是否打开:

```
sudo ufw status
```

如果没打开，则开启防火墙

```
sudo ufw enable
```

默认情况下，防火墙是会把所有端口都关闭的，不允许外界访问，但是我们要做三件事：开启80、443端口，关闭9090端口

```
sudo ufw allow 80
sudo ufw allow 443
sudo ufw deny 9090
```

此时，咱们的服务器会变的非常安全，注意哦，因为没打开3306端口，所以你的数据库是无法远程访问的，如需要则打开3306端口即可。

## 后台运行spring boot工程

把打包好的jar包发到服务器（通常用scp命令即可），然后执行如下命令即可后台启动：

```
nohup java -jar sitefriendlinks.jar >> ./output.log 2>&1 &
```

---

ok, 部署完成!

by [cmlanche.com](http://cmlanche.com)