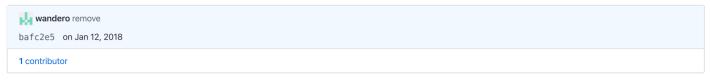
Branch: master ▼

Find file Copy path

#### blog / 17 / 171202 VPS 启用 HTTPS 记录.md





# VPS 启用 HTTPS 记录

(发现现在的 certbot 做的相当无脑好用了,但过程中还是有一些坑,记录如下)

# 环境

系统组件 Nginx @ Ubuntu 16.04

证书服务 Certbot @ Let's Encrypt

# 步骤

### 允许 https 通过防火墙

```
sudo ufw allow 'Nginx Full'
sudo ufw delete allow 'Nginx HTTP'
```

未设置会在签发证书阶段报错(The server could not connect to the client to verify the domain),网上有说法是 Dnspod 不支持 ssl 查询导致,实测 Dnspod 是支持的

#### 添加 Package Repository

sudo add-apt-repository ppa:certbot/certbot

# 安装 Certbot 的 Nginx Package

```
sudo apt-get update
sudo apt-get install python-certbot-nginx
```

## 签发证书

sudo certbot --nginx -d cloudlet.info #注意修改域名

执行后选择2 Redirect http 跳转 https 实际可能选择后未生效,可手动修改相应站点 nginx 配置,反注释 # Redirect non-https traffic to https 部分代码(新手提示,不要反注释掉 # Redirect non-https traffic to https 这里的 # 了……),建议修改 nginx 配置前备份(或者全部操作前镜像 VPS)

(只需要提供域名,certbot 就会自动侦测站点 nginx 配置文件并自动修改,不需要手动选择处理,官方指南上域名都不用提供,未测试)

#### 开启 http/2

继续编辑站点 nginx 配置, 将 listen 443 ssl; 修改为 listen 443 ssl http2;

(注意,某些杀毒软件如 ESET NOD32 Antivirus 启用 https 检查后会使用自己的证书替换站点证书,并导致相关页面 http 协议变为 1.1。Chrome 可在 Developer Tools - Security - View certificate 中查看当前页面使用证书)

# 重启 nginx 使修改生效

sudo service nginx restart

## 测试自动更新

Certbot 已自带定期更新,可使用 sudo certbot renew --dry-run 测试任务计划是否生效

# 其他

## SSL 检测评分

sslabs

# http/2 启用检测

「chrome developer tools」 - network - 文件列表面板标题列右键添加 Protocol 可查看资源协议

## 关于 HSTS

在指定期限强制浏览器使用 https 方式访问,会使域名 https 状态几乎无法撤销,新手建议暂缓使用