科学上网 2【v2ray】

科学上网路线图

操作步骤	内容
1	参考网站：网络跳跃和 tlanyan【作者微信号 chiocs，有问题可联系】
2	购买服务器并登陆，vultr【linode 活着亚马逊 AWS】【其他的可参考上述网站中 vps 商家整理】
3	服务器端安装 v2ray 并配置
4	购买域名 Namesilo【或其他】
5	为域名申请证书，可以用免费的 Let's Encrypt 证书
6	v2Ray 流量伪装
7	客户端下载并配置

第三步 服务器端安装 v2ray

https://tlanyan.me/v2ray-tutorial/

第四步 Namesilo 购买域名详细教程

账户注册

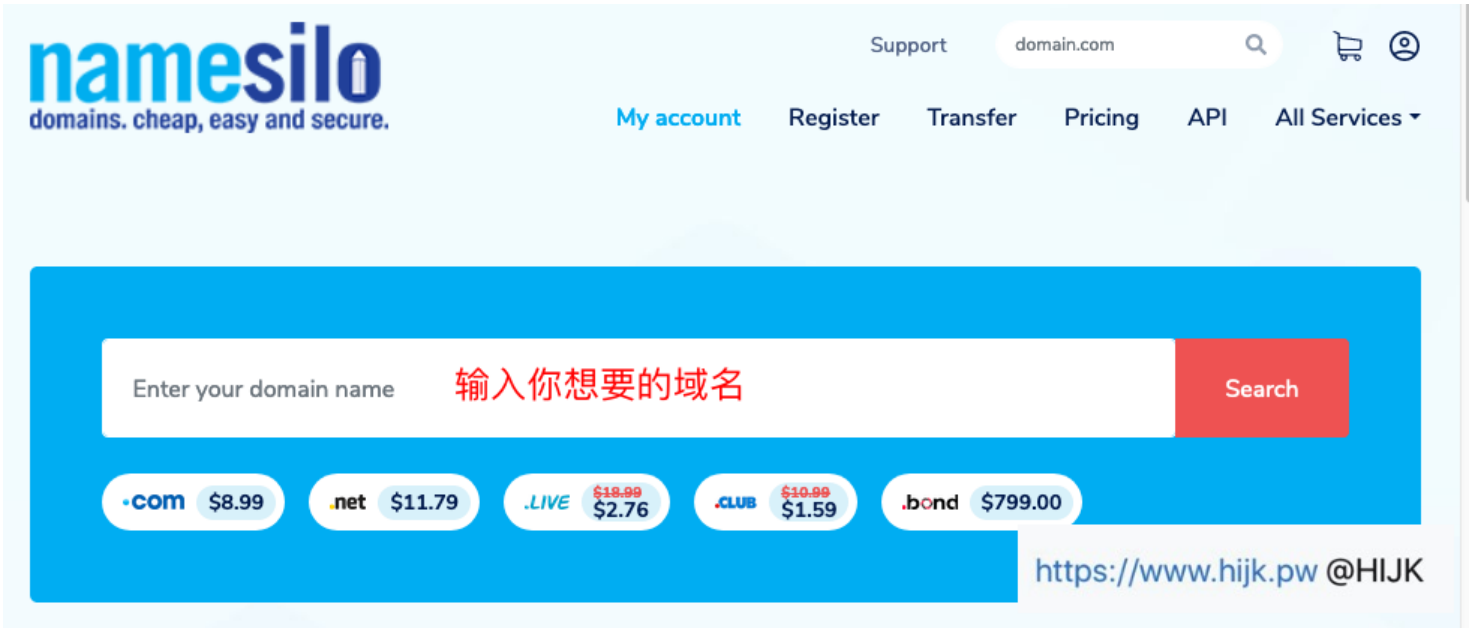
进入 Namesilo 官方 ， 点击右上角 **“Sign-up”** 进入账号注册页面：

在输入框设置账号的用户名、电子邮箱、密码和重复密码，输入验证码，勾选下方的两个框，点击“CREATE MY NEW ACCOUNT” 橙色按钮注册账户。

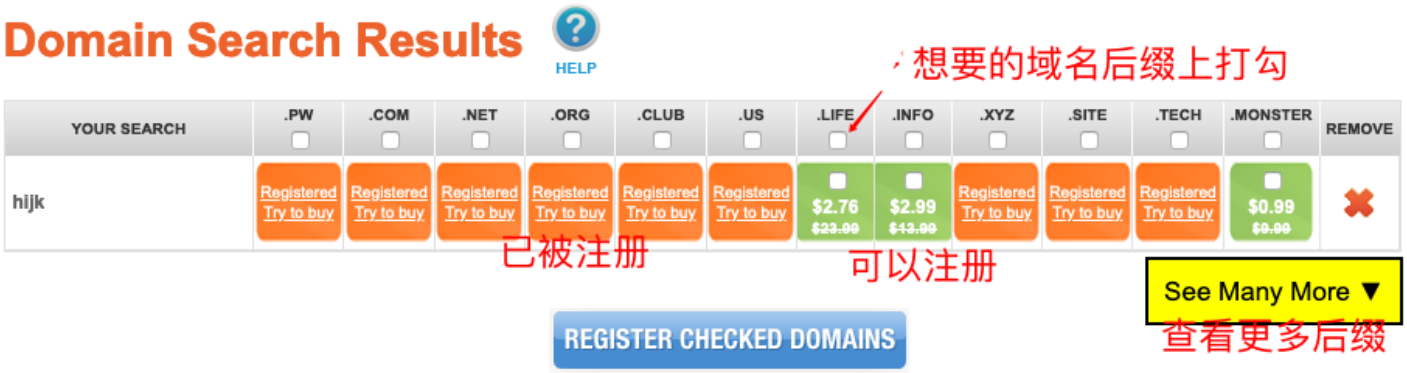
注册成功后界面跳转到账号主页，同时邮箱会收到两封邮件：一封账号创建成功通知邮件，一封邮件验证邮件，邮件标题是：Action required – WHOIS Verification，打开邮件，点击里面的验证链接，就完成了账户注册。

购买域名

1. 登陆（注册成功后默认是登录状态）后进入主页，在搜索框中输入想要注册的域名，例如 hijk.pw，然后点右边的 “search” 按钮：

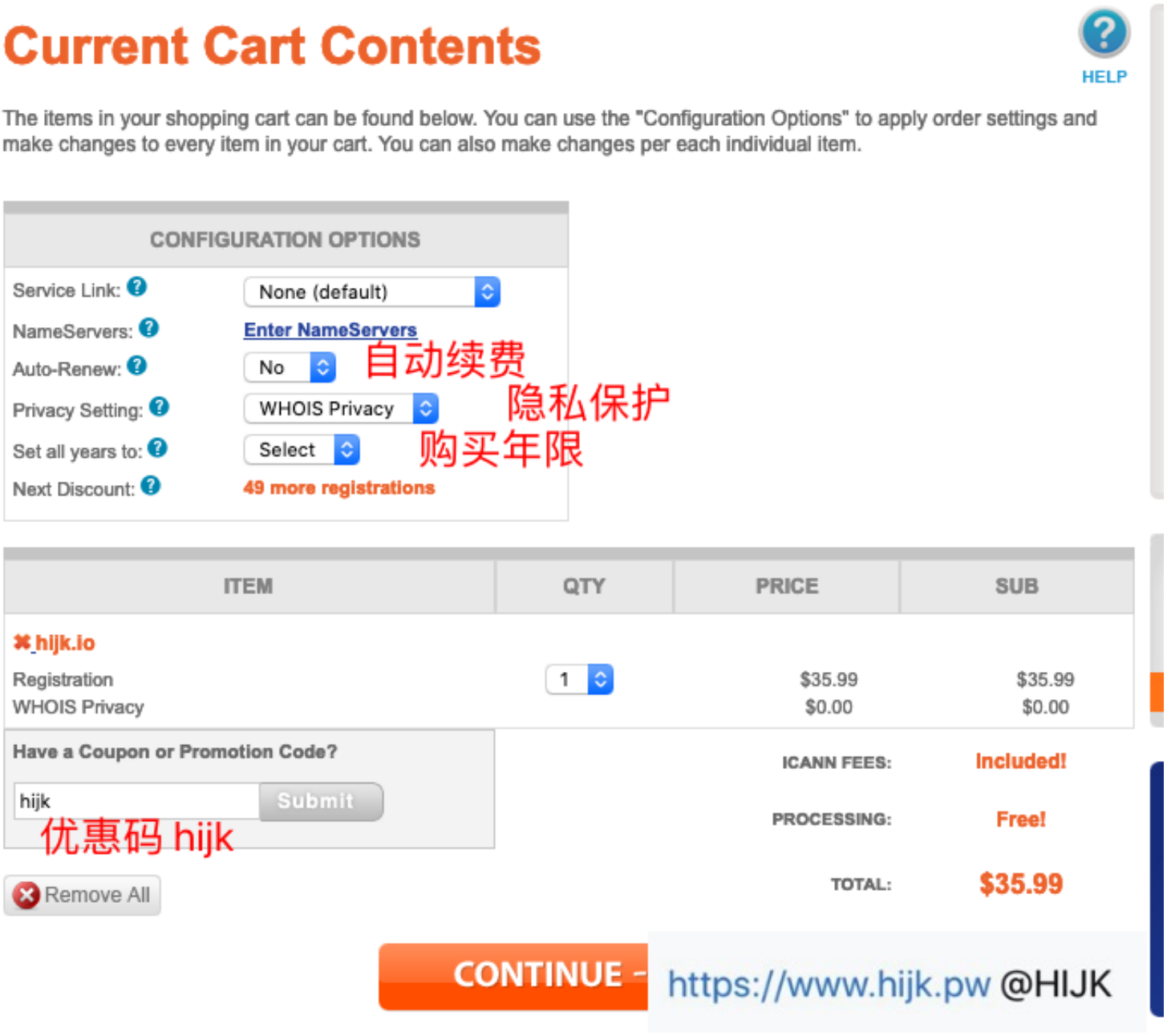


2. 接着界面会跳转到搜索结果页面，如果域名已被注册，会显示为橙色的 “Registered” 状态，绿色表示可注册。每个后缀都会显示价格，在想要的域名后缀上打勾，或者点 “see many more” 查看更多后缀：



3. 选择好后，点击蓝色的 “REGISTER CHECKED DOMAINS” 确认订单，系统接下来会问你是否需要高级 DNS 防护，选择 “No, I don’t want to protect my domain”：

4. 点“Continue to Cart”进入购物车界面，设置域名续费规则、注册时长等。在“Have a Coupon……”处输入优惠码 hijk ，点击“Submit”应用，优惠一美元（每个用户限用一次）：



其中：

- NameServers：域名解析服务器设置，未确定的可以等稍后在后台设置也一样；
- Auto-Renew：自动续费，如果决定长期使用，可以选择 Yes；
- Privacy Setting：隐私保护，选择 “WHOIS Privacy”；
- Set all years to：注册时长，如果是活动价格，则只能选择一年。

5. 点击 “CONTINUE” 按钮去付款，支持支付宝、Paypal 等。这里我们用支付宝付款，在右侧输入框填写支付宝绑定的邮箱，点击 **“GO”** 跳转扫码界面支付。

打开手机支付宝、扫码、付款就 OK 了！

域名解析

域名注册购买成功后，就可以把域名解析到服务器了。

点击右上角 “**Manage My Domains**” 进入域名管理页面，进入域名列表。然后点击右边的 **蓝色小球** 编辑 DNS。默认已经存在一些解析记录，点右边的删除按钮先全部删除，然后再添加想要的解析。例如添加 www.hijk.pw 的解析，操作流程如下：点击上方的 A，在 hostname 里填 www，ipv4 address 填你服务器的 ip，TTL 改成 3600。示例图如下：

A 记录指向*ipv4*地址， *AAAA* 记录指向*ipv6*地址，绝大部分时候用*A*记录就可以
如果你要添加其他的解析，例如test.hijk.pw，按照同样的操作步骤进行即可：hostname填test，ipv4 address填服务器的ip，TTL填3600。**一个域名可以添加无数个二级域名(主机名)**，所以你可以添加test1.hijk.pw, 1234.hijk.pw等任何有效主机名。

第五步 使用Let's Encrypt获取免费证书

https已经走向主流（那些烦人的运营商弹窗广告终于消停的差不多了），目前已经可以做到0成本获取SSL证书。国内的阿里云、腾讯云等云计算厂商提供了申请免费证书的服务，按照官方给出的步骤即可在一天之内拿到免费的证书。如果你需要便宜一点的泛域名证书，可以参考 这篇文章。
国内的企业都是忠诚于党的，申请证书就需要向这些企业提供私钥。所以有一天政府想要解密你的网站流量，那是so easy啊～鉴于这个考虑，本站从Let's Encrypt获取的免费证书。Let's Encrypt由互联网安全研究小组（ISRG）支持，是一个免费、非营利性的开放证书权威中心。任何域名持有人均可使用Let's Encrypt申请到免费的证书来加密网站流量，公司则建议用EV类的证书获取更权威的认证。

本文介绍如何从Let's Encrypt获取免费证书。前提是有一个域名（例如tlanyan.me）和一台vps，如果你的域名没备案且vps在国内，可能无法申请成功，解决办法请参考 这篇文章。本文教程机遇CentOS 7操作系统，如果你的环境与本博客的有差异，请参考官方指引。

安装certbot

首先安装certbot：yum install -y python36 && pip3 install certbot（注意：该安装方式不是官方推荐的，但一直都很好使）
安装完毕后，运行certbot --help可以查看该工具的命令详情。

解析域名

进入dns解析服务提供商的网站，将需要申请证书域名的A记录指向服务器IP。本人使用 DNSLA, 为www.tlanyan.me网站申请证书，在记录值出填写服务器ip，截图如下：

主机记录	记录类型	线路类型	记录值	MX优先级	TTL	管理
www	A	默认	[redacted]	--	600	
@	A	默认	[redacted]	--	600	

请在涂改部分填上你vps的IP。

获取证书

【这个时候需要等一下，网站需要时间去解析，并且要关闭防火墙】

运行命令 certbot certonly --standalone -d tlanyan.me -d www.tlanyan.me为域名tlanyan.me和www.tlanyan.me获取证书。如果你要获取多个站点，继续添加-d参数即可。certbot会检测80和443端口是否已经占用，如果已被占用需要先停止web服务器（例如停止Nginx：systemctl stop nginx）再运行命令。如果域名的A记录未指向该服务器，会报错提示域名解析问题。

大概半分钟就拿到了免费的证书，很爽有没有？运行 certbot certificates命令可查看获取到所有申请的证书及所在目录。

证书自动更新

通过certbot certificates命令可以看到证书的有效期是三个月，超过期限则需要续签。证书续期可以手动完成，例如：

systemctl stop nginx

certbot renew

systemctl restart nginx

也可以配置crontab任务自动续签，在/etc/crontab文件末添加一行：

0 0 0 */2 0 root systemctl stop nginx; /usr/bin/certbot renew; systemctl restart nginx

证书将每两个月自动续签一次。如果你的证书快到期了还没有续签，贴心的EFF（电子前哨基金会）会发邮件提醒，记得到期前续签就行。

第六步 V2Ray高级技巧：流量伪装

下文介绍流量伪装的配置步骤，演示域名为tlanyan.me，服务器为linux(centos)，web服务器软件用nginx，websocket+tls+web组合，最终效果为：http/https方式打开域名，显示正常的网页；V2Ray客户端请求特定的路径，例如https://tlanyan.me/awesomepath，能科学上网；浏览器直接请求https://tlanyan.me/awesomepath，返回”400 bad request”。即外部看起来完全是一个人畜无害的正规网站，特定手段请求特定网址才是科学上网的通道。

操作步骤

服务端涉及到了nginx和v2ray，分别介绍其配置。

1. 配置dns

先设置dns将域名解析到vps的ip，例如www.tlanyan.me解析到xxx.xxx.xx.xx。

如果你上了cdn，则dns要解析到cdn给的ip或者别名网址（cname）。使用cdn能隐藏真实vps的ip，

避免vps被墙或能拯救被封锁ip的vps。上cdn有好处，但国内cdn要求域名备案，国外cdn基本上会降低网速，而且配置起来稍显麻烦。建议新手先摸透https流量伪装，有特殊需求再考虑上cdn。

注意：如果你要用Let's Encrypt签发的证书，并且希望上cdn，那么应该先解析到vps的ip，获取到证书后再解析到cdn。

2. 配置nginx

如果你的域名并正确配置了ssl证书，可忽略这一步。

nginx是市面上占有率最高的网站服务器软件，centos 7系统安装nginx命令：yum install -y epel-release && yum install -y nginx。

linux系统上nginx默认站点配置文件是/etc/nginx/conf.d/目录下的default.conf，我们对伪装网站进行全站https配置，示例内容如下：

```
server {
    listen 80;
    server_name xxxxx;  # 改成你的域名
    rewrite ^(.*) https://$server_name$1 permanent;
}

server {
    listen       443 ssl http2;
    server_name xxxxx;
    charset utf-8;

    # ssl配置
    ssl_protocols TLSv1.2 TLSv1.3; # tls 1.3要求nginx 1.13.0及以上版本
    ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
    ssl_ecdh_curve secp384r1;
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout 10m;
    ssl_session_tickets off;
    ssl_certificate xxxxx; # 改成你的证书地址
    ssl_certificate_key xxxx; # 改成证书密钥文件地址

    access_log  /var/log/nginx/xxxx.access.log;
    error_log /var/log/nginx/xxx.error.log;

    root /usr/share/nginx/html;
    location / {
        index  index.html;
    }
```

```
}
```

配置好用 nginx -t 命令查看有无错误，没问题的话 systemctl restart nginx 启动 nginx。打开浏览器在地址栏输入域名，应该能看到 https 访问的 nginx 欢迎页。
新域名如何快速做一个像模像样的网站？最简单的办法是从网上下载网站模板，上传到 web 服务器的根目录（默认是 /usr/share/nginx/html）。对于伪装站来说，静态站足够。如果你的境外流量比较大，建议用爬虫或者其他手段做一个看起来受欢迎、流量大的站点，例如美食博客，图片站等。

配置 web 服务器使用证书。

各个 web 服务器的配置不一样，这里提供一个 nginx 的配置范例。例如本站的配置文件 /etc/nginx/conf.d/tlanyan.conf 文件，编辑其内容为：

```
server {
    listen 80;
    server_name www.tlanyan.me tlanyan.me;
    rewrite ^(.*) https://$server_name$1 permanent;
}

server {
    listen 443 ssl;
    server_name www.tlanyan.me tlanyan.me;
    charset utf-8;

    ssl_certificate /etc/letsencrypt/live/tlanyan.me/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/tlanyan.me/privkey.pem;
    ssl_protocols TLSv1.2 TLSv1.3; # TLSv1.3 需要 nginx 1.13.0 以上版本
    ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-GCM-SHA384:DHE
-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
    ssl_ecdh_curve secp384r1;
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout 10m;
    ssl_session_tickets off;
    keepalive_timeout 70;

    # 这里填写其他配置
}
```

配置分为两个 server 段，第一段是所有 http 请求都导向 https；第二段以 ssl 开头的配置都和证书相关：设置证书和私钥的位置、证书采用的协议、证书的加密算法等信息。
为了增强安全性，ssl_protocols、ssl_ciphers 和 ssl_perfer_server_ciphers 的配置建议采用以上配置。

配置好以后，运行 nginx -t 命令查看有无错误。如果没有可运行 systemctl restart nginx 重新开启 web 服务。

3. 安装配置 V2Ray

详细过程可参考上篇：V2Ray 教程

到此为止，nginx 和 V2ray 应该都能各自独立正常工作。如果有一个出现问题，应该先解决再继续下面的操作。

4. 服务端配置 websocket

接下来我们让 nginx 和 v2ray 结合，完成服务端的配置。

首先我们选择一个路径，建议为二级或者较长的一级路径，例如 /abc/def 或 /awesomepath。

配置 nginx 将这个路径的访问都转发到 v2ray。编辑 /etc/nginx/conf.d/default.conf 的第二个 server 段，增加以下转发配置：

```
location /abc/def { # 与 V2Ray 配置中的 path 保持一致
    proxy_redirect off;
    proxy_pass http://127.0.0.1:12345; # 假设 v2ray 的监听地址是 12345
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    proxy_set_header Host $host;
    # Show real IP in v2ray access.log
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

配置好后重启 nginx：systemctl restart nginx。

配置 v2ray 接受 nginx 传来的数据。编辑 /etc/v2ray/config.json 文件，在“inbounds”中新增“streamSetting”配置，设置传输协议为“websocket”。配置好后 config.json 文件看起来是：

```
{
  "log": {
    "loglevel": "warning",
    "access": "/var/log/v2ray/access.log",
    "error": "/var/log/v2ray/error.log"
   },
  "inbounds": [{
    "port": 12345,
    "protocol": "vmess",
    "settings": {
      "clients": [
        {
          "id": "xxxxx", # 可以使用 v2ctl uuid 生成
```

```
        "level": 1,
        "alterId": 64
      }
    ]
  },
  "streamSettings": {    # 载体配置段，设置为 websocket
    "network": "ws",
    "wsSettings": {
      "path": "/abc/def  # 与 nginx 中的路径保持一致
    }
  },
  "listen": "127.0.0.1" # 出于安全考虑，建议只接受本地链接
 }],
 "outbounds": [{
  "protocol": "freedom",
  "settings": {}
 },{
  "protocol": "blackhole",
  "settings": {},
  "tag": "blocked"
 }],
 "routing": {
  "rules": [
   {
    "type": "field",
    "ip": ["geoip:private"],
    "outboundTag": "blocked"
   }
  ]
 }
}
```

注意：json 文件不支持注释，上述配置中”#” 号及后续内容都要删掉。

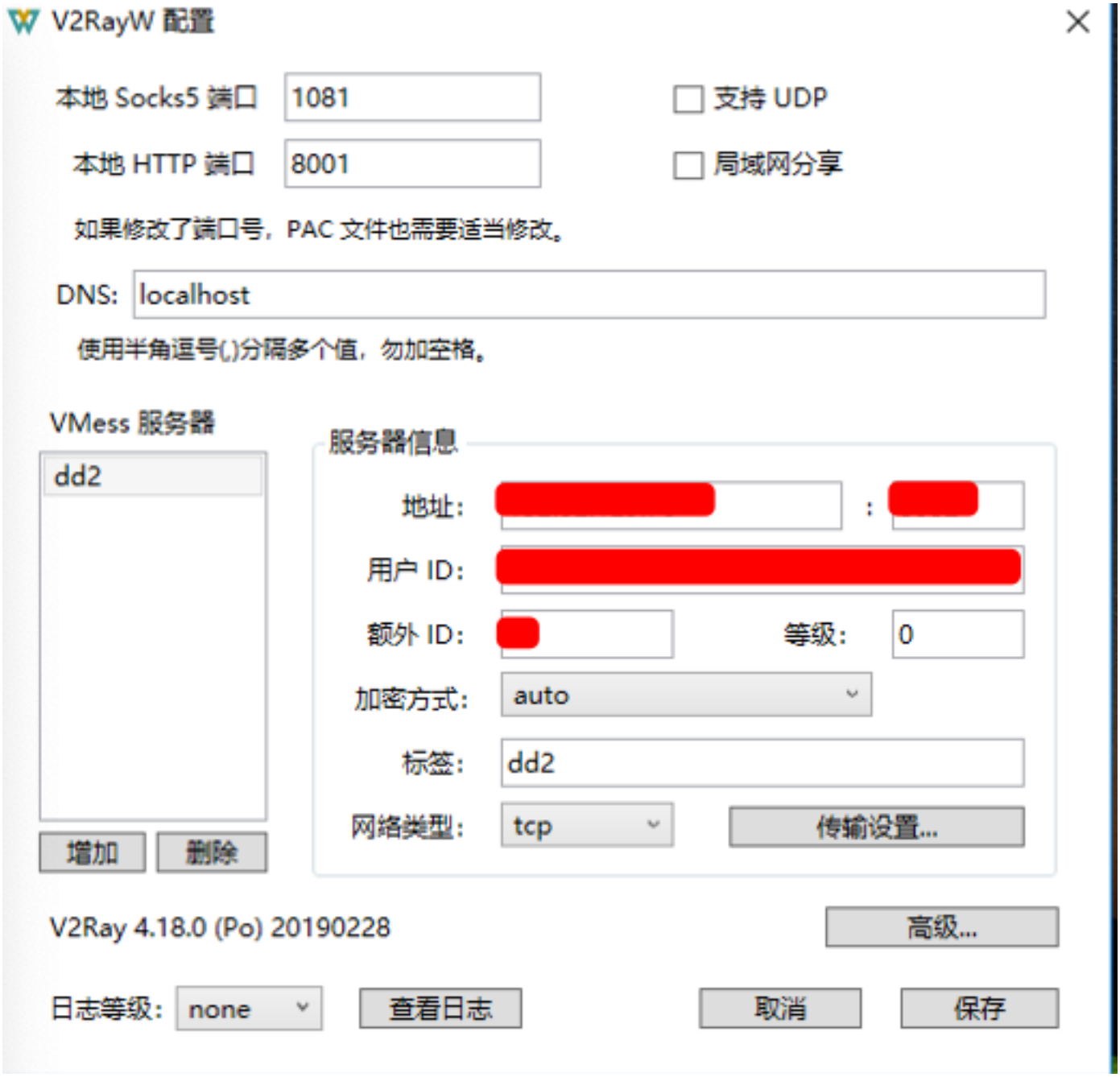
配置无误后，重启 v2ray 服务：systemctl restart v2ray。

如何测试 nginx 与 v2ray 结合没有问题？打开浏览器，输入域名及其他路径，应该显示正常网页或者页面不存在，说明 nginx 正常工作；输入域名加 v2ray 路径，例如 https://tlanyan.me/awesomepath，应该出现” Bad Request”，说明 nginx 将流量转发给了 v2ray，并且 v2ray 收到了请求。

第七步 客户端下载和使用

下面以Windows平台的V2RayW为例说明客户端的配置和使用方法：

1. 下载客户端，双击V2RayW.exe启动（注意：如果从V2RayW官网下载的客户端，需额外下载v2ray-core，本站提供的客户端无需额外下载）；
2. 右键系统托盘的V2RayW图标，点击“配置”；
3. 在配置窗口点击“增加”，然后在右侧“服务器信息”中填入服务器的ip、端口、用户id和额外id：



4.右键托盘图标，点击“加载v2ray”，同时勾选“自动模式（pac）”。
服务器信息配置无误的话，接下来就可以愉快的访问外网了。

打开V2RayW，右键托盘图标，点击“配置”。

在弹框中新建或修改已有的服务器，输入服务器ip，端口写443，把用户id、额外id信息填上，网络类型选择”ws”。接着点“传输设置”，找到“websocket”，路径一栏输入nginx和v2ray中的路径，例如“/awesomepath”；http头部输入：

```
{
"Host":"你的域名，例如www.tlanyan.me"
}
```

截图如下：

接着点击“tls”，勾选“启用传输层加密 tls”（同时建议勾选“允许不安全的加密方式”和“允许不安全连接”），在“服务器域名”的输入框中输入域名，截图如下：

【记住端口写 443】

信息填写正确后，点击“保存”。打开浏览器访问 google.com，youtube.com 等网站，配置无误的话应该都能正常打开。