# 用 Nginx 禁止国外 IP 访问网站

## **前言**

先来说说为啥要写这篇文章（一是面试被问了N次），还有就是之前小编看了下 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247512619&idx=1&sn=de1b25b04b8c3fc03d00f183dbe96967&chksm=e918d737de6f5e21c4482299be7708b265b5b8b33f05c7dfd72197fe23bb2a1a30d9ab6bc114&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank) 的访问日志，发现每天有好多国外的 IP 地址来访问我的网站，并且访问的内容基本上都是恶意的。因此我决定禁止国外 IP 来访问我的网站。

想要实现这个功能有很多方法，下面我就来介绍基于 **NGINX 的 ngx\_http\_geoip2 模块** 来禁止国外 IP 访问网站。

## **安装 geoip2 扩展依赖**

[root@fxkj ~]# yum install libmaxminddb-devel -y

## **下载 ngx\_http\_geoip2\_module 模块**

[root@fxkj tmp]#  git clone https://github.com/leev/ngx\_http\_geoip2\_module.git  
[ro tmp]#

## **解压模块到指定路径**

我这里解压到/usr/local 目录下

[root@fxkj tmp]# mv ngx\_http\_geoip2\_module/ /usr/local/  
[root@fxkj local]# ll ngx\_http\_geoip2\_module/  
total 60  
-rw-r--r-- 1 root root  1199 Aug 13 17:20 config  
-rw-r--r-- 1 root root  1311 Aug 13 17:20 LICENSE  
-rw-r--r-- 1 root root 23525 Aug 13 17:20 ngx\_http\_geoip2\_module.c  
-rw-r--r-- 1 root root 21029 Aug 13 17:20 ngx\_stream\_geoip2\_module.c  
-rw-r--r-- 1 root root  3640 Aug 13 17:20 README.md

## **安装 nginx 模块**

首先说明下环境，我的 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247509451&idx=1&sn=31082f7c17d04ff42002d988a30885e0&chksm=e918c0d7de6f49c107db26408a6199e7606e2ce746f5b949149b7f689eb2b086d318d99915b9&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank)版本是 1.16 , 在网上查了下安装 ngx\_http\_geoip2 模块至少需要 1.18 版本及以上，因此此次安装我是升级 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247509016&idx=1&sn=0e6d0e99b0902a39da7fb083cb885fb0&chksm=e918c104de6f481284122ebfb704aeef803df4391f8b395b0ef730fe0de4c60f48bf8db2d060&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank)1.18，添加 ngx\_http\_geoip2 模块。

下载 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247507251&idx=2&sn=82bbf6075d50f9b5172dc61d950af762&chksm=e918b82fde6f31393185eb26a5f8fd03ef5f4d9a4aeb894c79c52923ceafccc611cf927b8310&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank) 1.18 版本

[root@fxkj ~]# yum install libmaxminddb-devel -y

解压 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247502884&idx=1&sn=fd270a85e3e4613052eefb82144209ac&chksm=e918a938de6f202ee96a7b950bbcdcca6a66d0fd8229af8a72cdef2ddecb265816c930d3d31a&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank)1.18 软件包并升级为 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247501127&idx=3&sn=5125ca47866c778a5e07428fd0fd3951&chksm=e918a05bde6f294d8584ff031e05ed33dc568effa0f8dcaf2de36163cb1f8243e70a04c1f9c0&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank)1.18 ，添加 ngx\_http\_geoip2 模块

需要注意

1、升级 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247500849&idx=1&sn=0e34b19f81f1519ef4f0743a55b3c08f&chksm=e918a12dde6f283b218d4fd67a1e3523d4b0fe973907d2821226ad1890dde55ab5426eb03120&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank), 添加 nginx 模块只需要编译然后 make 不需要 make instll 不然线上的 nginx 会被新版本 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247497725&idx=1&sn=ab7a474821ac3c0ffd14749d47d64979&chksm=e91892e1de6f1bf74842e37ca868030bdc371ef4c5b6419151434d32ea6643efc80475de5637&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank) 完完整整的替换掉

2、编译前需要看下 [nginx](http://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247495416&idx=1&sn=bada1264baa5cc387cc2790fb87d5fc3&chksm=e9188be4de6f02f2a79586c60d1071132b8b70a83ab268808cb08139efc21b142790195383f5&scene=21" \l "wechat_redirect" \t "https://mp.weixin.qq.com/s/_blank)当前安装了哪些模块

[root@fxkj tmp]# /usr/local/nginx/sbin/nginx -V  
  
nginx version: nginx/1.16.0  
  
built by gcc 4.8.5 20150623 (Red Hat 4.8.5-39) (GCC)  
  
built with OpenSSL 1.0.2k-fips 26 Jan 2017  
  
TLS SNI support enabled  
  
configure arguments: –with-http\_stub\_status\_module –prefix=/usr/local/nginx –user=nginx –group=nginx –with-http\_ssl\_module –with-stream

编译安装

[root@fxkj tmp]# tar -xf nginx-1.18.0.tar.gz  
[root@fxkj tmp]# cd nginx-1.18.0/  
[root@fxkj nginx-1.18.0]# ./configure --with-http\_stub\_status\_module \  
 --prefix=/usr/local/nginx \  
 --user=nginx --group=nginx --with-http\_ssl\_module --with-stream \  
 --add-module=/usr/local/ngx\_http\_geoip2\_module  
[root@fxkj nginx-1.18.0]# make  
[root@fxkj nginx-1.18.0]# cp /usr/loca/nginx/sbin/nginx /usr/loca/nginx/sbin/nginx1.16    #备份  
[root@fxkj nginx-1.18.0]# cp objs/nginx /usr/local/nginx/sbin/    #

用新的去覆盖旧的

[root@fxkj nginx-1.18.0]# pkill nginx     #杀死nginx  
[root@fxkj nginx-1.18.0]# /usr/local/nginx/sbin/nginx    #再次启动Nginx

注意：不过生产环境不建议大家这样操作，平滑升级操作大家可以参考：[1分钟搞定 Nginx 版本的平滑升级与回滚](https://mp.weixin.qq.com/s?__biz=MzI0MDQ4MTM5NQ==&mid=2247488666&idx=1&sn=91c77bddd39679e395ba05ee4eed1d65&chksm=e91b7186de6cf8906151518fed5c9f01df850b4677fe0974a210869d71f75372e6c76ae4732a&token=440973402&lang=zh_CN&scene=21" \l "wechat_redirect) 这篇文章。

查看 nginx 版本以及安装的模块

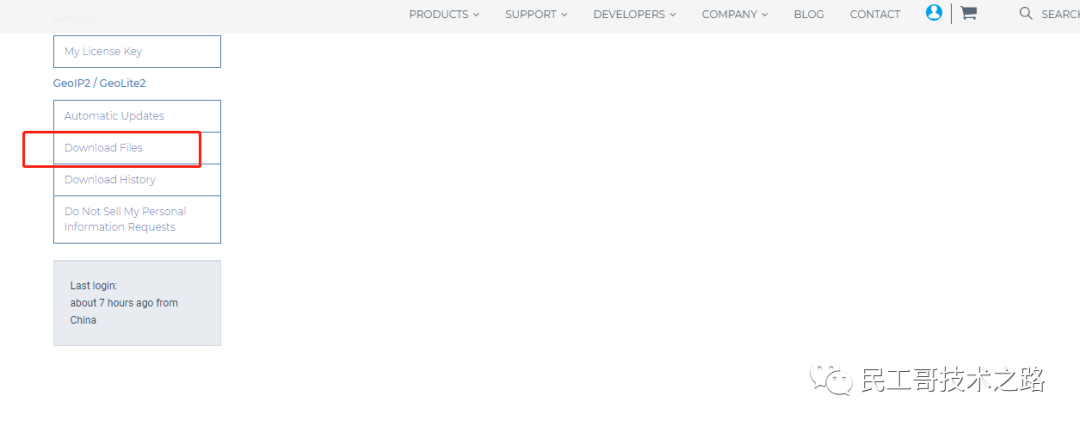
[root@fxkj nginx-1.18.0]# /usr/local/nginx/sbin/nginx -V  
  
nginx version: nginx/1.18.0  
  
built by gcc 4.8.5 20150623 (Red Hat 4.8.5-39) (GCC)  
  
built with OpenSSL 1.0.2k-fips 26 Jan 2017  
  
TLS SNI support enabled  
  
configure arguments: –with-http\_stub\_status\_module –prefix=/usr/local/nginx –user=nginx –group=nginx –with-http\_ssl\_module –with-stream –add-module=/usr/local/ngx\_http\_geoip2\_module

## **下载最新的 IP 地址数据库文件**

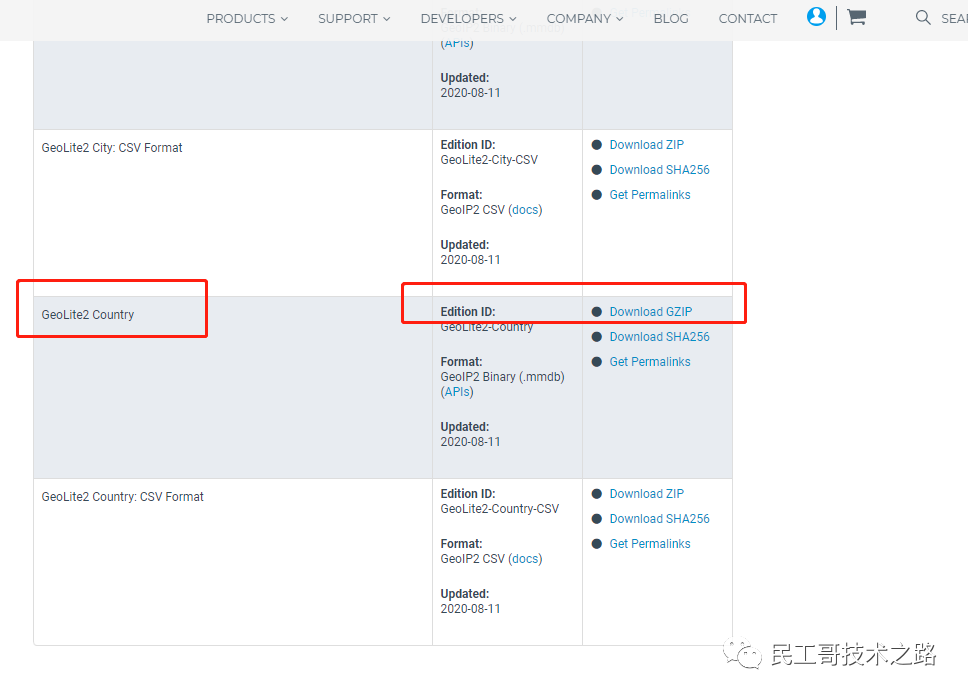
模块安装成功后，还要在 Nginx 里指定数据库，在安装运行库时默认安装了两个，位于 /usr/share/GeoIP/ 目录下，一个只有 IPv4，一个包含 IPv4 和 IPv6：

登录 www.maxmind.com 网址，创建账户下载最新的库文件（账户创建就不演示了）

点击左侧 ，Download Files



选择 GeoLite2 Country ，点击 Download GZIP 下载即可



上传到 /usr/share/GeoIP/ 下并解压

[root@fxkj local]# cd /usr/share/GeoIP/  
[root@fxkj GeoIP]# ll  
total 69612  
lrwxrwxrwx. 1 root root       17 Mar  7  2019 GeoIP.dat -> GeoIP-initial.dat  
-rw-r--r--. 1 root root  1242574 Oct 30  2018 GeoIP-initial.dat  
lrwxrwxrwx. 1 root root       19 Mar  7  2019 GeoIPv6.dat -> GeoIPv6-initial.dat  
-rw-r--r--. 1 root root  2322773 Oct 30  2018 GeoIPv6-initial.dat  
-rw-r--r--  1 root root  3981623 Aug 12 02:37 GeoLite2-Country.mmdb

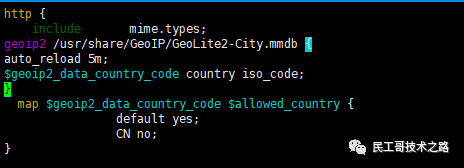
## **配置 nginx 配置文件**

修改前先备份配置文件

[root@fxkj ~]# cp /usr/local/nginx/conf/nginx.conf /usr/local/nginx/conf/nginx.conf-bak  
[root@fxkj ~]# vim /usr/local/nginx/conf/nginx.conf

在 http 中添加 几行，定义数据库文件位置

geoip2 /usr/share/GeoIP/GeoLite2-City.mmdb {  
auto\_reload 5m;  
$geoip2\_data\_country\_code country iso\_code;  
}  
  map $geoip2\_data\_country\_code $allowed\_country {  
                default yes;  
                CN no;  
}

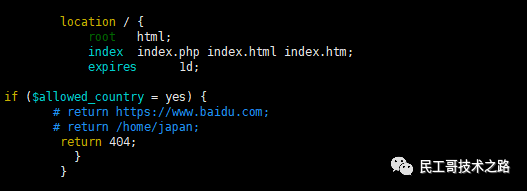


在 server 中的 location 下添加条件

如果满足 IP 是国外 IP 就执行下面的 return 动作，我这里定义了 3 种, 注释了其中两个。

当访问 IP 是国外 IP ，直接返回 404。

**if** ($allowed\_country = yes) {  
       # return https://www.baidu.com;  
       # return /home/japan;  
        return 404;  
 }



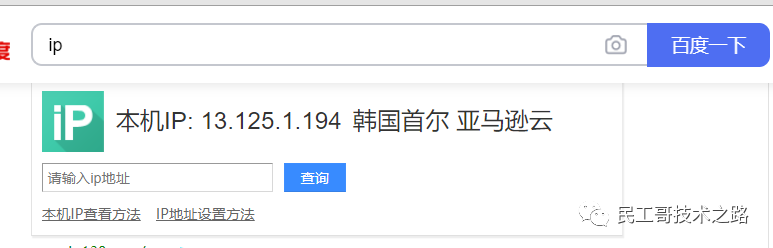
修改完毕后， 检测下配置文件，重新加载下 nginx

[root@fxkj ~]# /usr/local/nginx/sbin/nginx -t  
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok  
nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful  
[roo@fxkj ~]# /usr/local/nginx/sbin/nginx -s reload

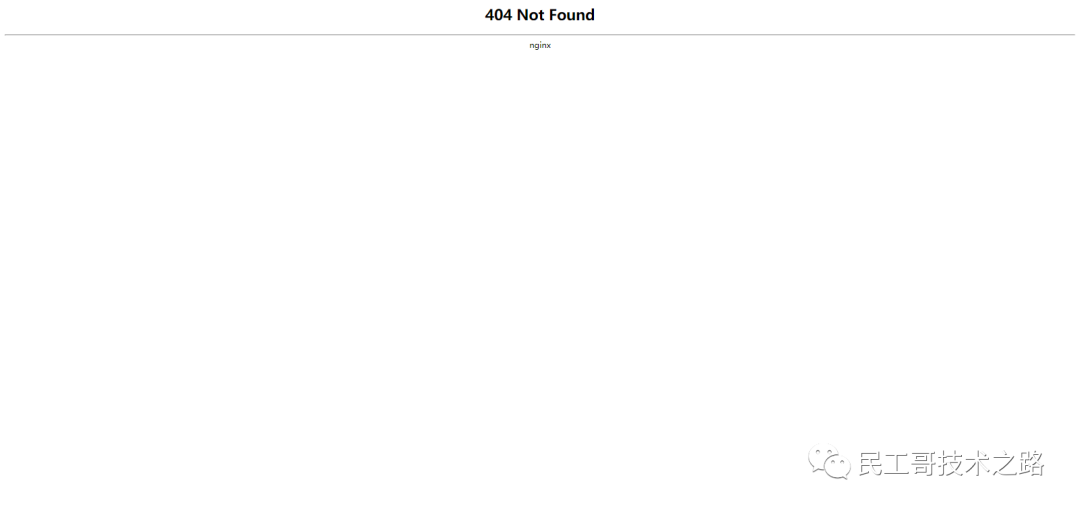
## **模拟测试验证**

使用海外节点的服务器去访问网站

这里我的 IP 是 来自于韩国



可以看到访问网站报错 404 Not Found



我们再来看下 nginx 的访问日志

“13.125.1.194 – – [14/Aug/2020:16:15:51 +0800] “GET /favicon.ico HTTP/1.1” 404 548 “https://www.fxkjnj.com/” “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36”

IMG_264

至此，我们通过 Nginx 来实现禁止国外 IP 访问网站 就结束了~