Nguồn: <https://echorand.me/posts/nginx-geoip2-mmdblookup/> (hướng dẫn áp dụng)

Và <https://github.com/leev/ngx_http_geoip2_module> (code chính)

Và <https://medium.com/@karljohnson/geoip-discontinuation-upgrade-to-geoip2-with-nginxon-centos-c2a3dbcf8fd> (block country)

Contents

[Cài đặt 1](#_Toc45660742)

[Compile nginx với thư viện geoip2 1](#_Toc45660743)

[Để lưu log ta thêm dạng log như sau: 2](#_Toc45660744)

[Để chặn IP ngoài Vietnam ta sử dụng như sau: 3](#_Toc45660745)

## Cài đặt thư viện cần thiết

# yum -y install epel-release

# yum install pcre pcre-devel zlib zlib-devel openssl openssl-devel gcc

# yum -y install libmaxminddb-devel

Chuẩn bị sẵn 2 file download ở maxmind GeoLite2-Country.mmdb và GeoLite2-City.mmdb

## Compile nginx với thư viện geoip2

wget http://nginx.org/download/nginx-VERSION.tar.gz

tar zxvf nginx-VERSION.tar.gz

cd nginx-VERSION

Tải thêm module geoip2 ở link sau <https://github.com/leev/ngx_http_geoip2_module>

mkdir -p /opt/nginx/modules\_extend/ ; cd /opt/nginx/modules\_extend/

git clone <https://github.com/leev/ngx_http_geoip2_module>

Hoặc sử dụng file.zip đã tải.

(Mẫu compile của tuanda)

# ./configure --sbin-path=/usr/bin/nginx --prefix=/opt/nginx --conf-path=/opt/nginx/nginx.conf --error-log-path=/opt/nginx/logs/error.log --http-log-path=/opt/nginx/logs/access.log --with-pcre --pid-path=/var/run/nginx.pid --with-http\_ssl\_module --with-http\_realip\_module --with-http\_stub\_status\_module --add-module=/opt/nginx/modules\_extend/ngx\_http\_geoip2\_module

# make

# make install

Kiểm tra bằng lệnh

$ mmdblookup --file /vị\_trí\_lưu\_file/GeoLite2-City.mmdb --ip 49.255.14.118

Thêm config

Ta để ý:

$geoip2\_data\_country\_name source=$http\_x\_forwarded\_for country names en;

GeoIP source có thể thay đổi bằng remote\_addr hoặc bất kỳ trường nào. Không cần phải theo XforwardFor

Thêm config này ở nginx.conf

geoip2 /etc/GeoLite2-Country.mmdb {

auto\_reload 5m;

$geoip2\_metadata\_country\_build metadata build\_epoch;

$geoip2\_data\_country\_code default=US source=$http\_x\_forwarded\_for country iso\_code;

$geoip2\_data\_country\_name source=$http\_x\_forwarded\_for country names en;

}

geoip2 /etc/GeoLite2-City.mmdb {

$geoip2\_data\_city\_name source=$http\_x\_forwarded\_for city names en;

$geoip2\_data\_time\_zone source=$http\_x\_forwarded\_for location time\_zone;

}

## Để lưu log ta thêm dạng log như sau:

log\_format **json\_combined** escape=json

'{'

'"time\_local":"$time\_local",'

'"remote\_addr":"$remote\_addr",'

'"remote\_user":"$remote\_user",'

'"request\_method":"$request\_method",'

'"request":"$request",'

'"response\_status": "$status",'

'"body\_bytes\_sent":"$body\_bytes\_sent",'

'"request\_time":"$request\_time",'

'"http\_referrer":"$http\_referer",'

'"http\_user\_agent":"$http\_user\_agent",'

'"real\_ip": "$http\_x\_forwarded\_for",'

'"geoip\_country\_code": "$geoip2\_data\_country\_code",'

'"geoip\_country\_name": "$geoip2\_data\_country\_name",'

'"geoip\_city": "$geoip2\_data\_city\_name",'

'"geoip\_timezone": "$geoip2\_data\_time\_zone"'

'}';

Log sẽ hiển thị mẫu như sau:

{

"time\_local":"14/Jul/2020:21:23:29 +0700",

"remote\_addr":"149.248.33.188",

"remote\_user":"",

"request\_method":"POST",

"request":"POST /mapi/services/authen\_msisdn HTTP/1.1",

"response\_status":"200",

"body\_bytes\_sent":"180",

"request\_time":"0.486",

"http\_referrer":"",

"http\_user\_agent":"okhttp/3.9.1",

"real\_ip":"149.248.33.188",

"geoip\_country\_code":"US",

"geoip\_country\_name":"United States",

"geoip\_city":"Seattle",

"geoip\_timezone":"America/Los\_Angeles"

}

Log thêm Location vào log:

# Mod log city country

log\_format modlog\_country '$remote\_addr - "$geoip2\_data\_country\_name" - $remote\_user [$time\_local] '

'"$request" $status $body\_bytes\_sent ${request\_time}ms '

'"$http\_referer" "$http\_user\_agent"';

## Để chặn IP ngoài Vietnam ta sử dụng như sau:

Đặt ở ngoài config nginx.conf

map $geoip2\_data\_country\_code $allowed\_country {

default no;

VN yes;

}

Đặt ở trong location /xxx

if ($allowed\_country = no) {

access\_log /opt/nginx/logs/myvnpt\_api.banned\_location.log modlog;

return 444;

}

## MultiIP khi đứng sau nhiều Proxy

map $http\_x\_forwarded\_for $realip {

~^(\d+\.\d+\.\d+\.\d+) $1;

default $remote\_addr;

}

Sau đó ta đẩy vào GeoIP2

geoip2 /etc/GeoLite2-Country.mmdb {

$geoip2\_data\_country\_code default=US source=$realip country iso\_code;

$geoip2\_data\_country\_name source=$realip country names en;

}

Bài gốc: <https://echorand.me/posts/nginx-geoip2-mmdblookup/>

# Nginx and geoip lookup with geoip2 module

#### First posted on: 2019/05/24

#### Last modified: 2019/07/11,[55f5a1c](https://github.com/amitsaha/echorand.me/commit/55f5a1c70cd06fb4d65501ddb167c74089ed921d)

Categories: [infrastructure](https://echorand.me/categories/infrastructure)

I wanted to setup Nginx logging so that it would perform GeoIP lookup on the IPv4 address in the X-Forwarded-For header. Here’s how I went about doing it on CentOS 7.

This [nginx module](https://github.com/leev/ngx_http_geoip2_module) integrates Maxmind GeoIP2 database with the RPMs being available by [getpagespeed.com](https://www.getpagespeed.com/server-setup/nginx/upgrade-to-geoip2-with-nginx-on-cens-rhel-7).

Once I had installed the module, the hard part for me was how to get the data I wanted - city, timezone information and others from nginx and the geoip2 module integration. This is where [mmdblookup](https://maxmind.github.io/libmaxminddb/mmdblookup.html) helped tremendously.

# mmdblookup

mmdblookup can be used to read a MaxMind DB file for an IP address and query various information. To install:

# yum -y install libmaxminddb-devel

We need to give it a path to the DB file and the IP address and it spits out all that it finds out. For example:

$ mmdblookup --file /usr/share/GeoIP/GeoLite2-City.mmdb --ip 49.255.14.118

Now, let’s say we only wanted the name of the city in english, we would do something like this:

$ mmdblookup --file /usr/share/GeoIP/GeoLite2-City.mmdb --ip 49.255.14.118 city names en

"Sydney" <utf8\_string>

If you look at the first “object” in the output above, you will see that the above three arguments, city names en is almost like accessing a nested key inside a dictionary. I say almost, becomes it’s not a JSON format. Anyway, this was the key thing I needed to learn to be able to write the right things in my nginx configuration.

# Logging the GeoIP decoded data

This is how the relevant nginx configuration for GeoIP2 lookup looked like:

...

http {

geoip2 /etc/GeoLite2-Country.mmdb {

auto\_reload 5m;

$geoip2\_metadata\_country\_build metadata build\_epoch;

$geoip2\_data\_country\_code default=US source=$http\_x\_forwarded\_for country iso\_code;

$geoip2\_data\_country\_name source=$http\_x\_forwarded\_for country names en;

}

geoip2 /etc/GeoLite2-City.mmdb {

$geoip2\_data\_city\_name source=$http\_x\_forwarded\_for city names en;

$geoip2\_data\_time\_zone source=$http\_x\_forwarded\_for location time\_zone;

}

..

If you look at the two geoip2 sections, you can see how I am feeding the value in the http\_x\_forwarded\_for variable as the source for the IP lookup. This is how I understand how the above is working with inline comments:

*# this is similar to specfying --file /etc/GeoLite2-City.mmdb*

geoip2 /etc/GeoLite2-City.mmdb {

*# This is assigning a variable $geoip2\_data\_city\_name to the value of:*

*# mmdblookup --file /etc/GeoLite2-City.mmdb --ip $http\_x\_forwarded\_for city names en*

$geoip2\_data\_city\_name source=$http\_x\_forwarded\_for city names en;

*# This is assigning a variable $geoip2\_data\_time\_zone to the value of:*

*# mmdblookup --file /etc/GeoLite2-City.mmdb --ip $http\_x\_forwarded\_for location time\_zone*

$geoip2\_data\_time\_zone source=$http\_x\_forwarded\_for location time\_zone;

}

The explanations for the GeoLite2-Country DB is similar. Then later on in the nginx configuration, we log the value of this variables in JSON format. A complete nginx.conf is [here](https://gist.github.com/amitsaha/f43e9397e5f84903e5d1bffaf8b4b9d9#file-nginx-conf).

# Multiple IP addresses in X-Forwarded-For

What happens when your X-Forwarded-For has a chain of IP addresses: <UserIP>, <LB>, <API gateway>? We need to extract the user ip from this list and then perform GeoIP lookup on it. We will make use nginx’s map module (thanks to this [answer](https://stackoverflow.com/a/53630597):

map $http\_x\_forwarded\_for $realip {

~^(\d+\.\d+\.\d+\.\d+) $1;

default $remote\_addr;

}

We default to $remote\_addr if we don’t have any IP address in $http\_x\_forwarded\_for and then update our GeoIP lookup as follows:

geoip2 /etc/GeoLite2-Country.mmdb {

$geoip2\_data\_country\_code default=US source=$realip country iso\_code;

$geoip2\_data\_country\_name source=$realip country names en;

}

An updated complete nginx.conf is [here](https://gist.github.com/amitsaha/f43e9397e5f84903e5d1bffaf8b4b9d9#file-nginx-conf-multiple_x_forwarded_for).

# Other links you may find useful

* <https://blog.jayway.com/2014/03/28/how-to-get-the-client-ip-when-using-cloudfront-and-nginx/>