Kako utvrditi geografsku lokaciju poslužitelja po IP adresi?

Ponekad nam je bitno pronaći geografsku lokaciju (odnosno, obično samo državu) poslužitelja ili klijentskog računala. Razlozi mogu biti različiti, bilo da želimo blokirati promet iz te zemlje ili regije (zbog nekakvog organiziranog napada), bilo da želimo isporučiti različite verzije web stranica za različite zemlje. Istina je da se velik dio ovih zahtjeva može ostvariti pregledom Top Level Domene, odnosno dijelom iza zadnje točke u nazivu računala. No, nisu sva računala unešena u DNS, niti nam nastavak ".com" mnogo govori o zemlji odakle računalo dolazi. Upravo zato ćemo pretraživati po IP adresi, što je pouzdanije. Naravno, sve ovo ćemo raditi iz komandne linije.

Prva opcija se nameće samo po sebi: **whois**. Whois je servis koji omogućava pregled općenitih podataka o domenama, odnosno IP adresama. Nas od svih informacija zanima uglavnom samo zemlja, pa možemo odmah upotrijebiti naredbu grep:

```
server$ whois 161.53.160.25  | grep country
country:        HR
```

Vidimo da se adresa 161.53.160.25 nalazi u Hrvatskoj (inače, to je adresa za www.carnet.hr).

I to je to, whois nam je pomogao, ali možemo li saznati nešto više? Iako whois nudi puno više informacija (podaci o abuse službi za taj range, registraru i slično), to nije ono što nas zanima.

Ono što može upotrijebiti je servis **ipinfo.io**, web stranica koja nam može reći konretnije stvari. Iako se radi o web stranici, do podataka je izrazito lako doći iz naredbene linije pomoću naredbi **wget** ili **curl**:

```
server$ wget -q -O - http://ipinfo.io/161.53.160.25
{
  "ip": "161.53.160.25",
  "hostname": "No Hostname",
  "city": null,
  "region": null,
  "country": "HR",
  "loc": "45.1667,15.5000",
  "org": "AS2108 Croatian Academic and Research Network"
}
```

Uz podatke o zemlji, dobit ćete i podatke o vlasniku mrežnog raspona gdje se nalazi traženi server ili klijent, kao i geografske koordinate (ovo je vjerojatno samo pozicija središte vlasnika, ne i realna pozicija servera).

Ukoliko na sustavu imate program curl, možda će vam jednostavnije biti koristiti oblik:

```
server$ curl http://ipinfo.io/161.53.160.25
```

Na kraju, ne možemo a da ne spomenemo GeoIP tvrtke MaxMind. GeoIP je najomiljeniji alat upravo webmastera i oglašivača, koji ovakvu funkcionalnost koriste kako bi posluživali prilagođene web

stranice, i što je bitnije, prilagođene reklame. No, mi ćemo koristiti besplatnu verziju, GeoLite (koga to zanima, ova baza se distribuira pod licencom "*Creative Commons Attribution-ShareAlike 3.0 Unported License*").

Ukoliko želite koristi GeoLite u komandnoj liniji, morate instalirati paket **geoip-bin**:

```
# apt-get install geoip-bin
...
The following NEW packages will be installed:
  geoip-bin
```

U paketu se nalazi alat **geoiplookup**, kojega koristimo vrlo jednostavno:

```
# geoiplookup 161.53.160.25
GeoIP Country Edition: HR, Croatia
```

Dakle, uporaba je vrlo jednostavna, a rezultat precizan. MaxMind svoje podatke obnavlja jednom mjesečno, tako da su prilično ažurni. No, nude i preciznije podatke, poput broja autonomnog sustava i grada. Za Hrvatsku su
ovi podaci, naravno, nepotpuni (no, ipak, dobit ćemo koordinate):

```
# geoiplookup -f /usr/share/GeoIP/GeoLiteCity.dat 161.53.160.25
GeoIP City Edition, Rev 1: HR, N/A, N/A, N/A, 45.166698, 15.500000, 0, 0
```

Datoteke GeoLiteCity.dat (i GeoIPASNum.dat) ne dolaze u paketu, pa ih je potrebno ručno skinuti (što se ipak može automatizirati jednim cron jobom):

```
# wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz
# wget http://download.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz
# wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
```

Sve se ove datoteke nalaze u direktoriju /usr/share/GeoIP, te ih je potrebno raspakirati i prebaciti tamo:

```
#!/bin/sh

cd /usr/share/GeoIP
wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz
wget http://download.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz
wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz

mv -f GeoIP.dat GeoIP.old
mv -f GeoIPASNum.dat GeoIPASNum.old
mv -f GeoLiteCity.dat GeoLiteCity.old

gzip -d GeoIP.dat.gz GeoIPASNum.dat.gz GeoLiteCity.dat.gz
```

Ovu skriptu ubacite u cron i pokrećite jednom mjesečno (podaci se osvježavaju svakom prvog utorka u mjesecu), i uvijek ćete imati svježe podatke:

```
MAILTO=vas_email@domena.hr
0 12 * * 3 /usr/bin/skripta
```

Postoji i naredba geoipupdate, ali ona se odnosi na pretplatni servis, te neće raditi ukoliko ne posjedujete odgovarajući ključ kojeg ćete upisati u /etc/GeoIP.conf

Zdravko Rašić

uto, 2014-04-01 00:00 - Zdravko Rašić**Kuharice:** Linux [1]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1375?page=0

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17