Greške u ClamAV-u

Posljednjih dana dobijamo upite što se događa s ClamAV-om, antivirusnim softverom koji se nalazi na svim našim poslužiteljima (osim ako niste kupili neki drugi). I prije se događalo da se antivirusne datoteke ne mogu skinuti, ali sve je to obično potrajalo koji sat ili eventualno dan-dva. Sada je ispad malo duži i traje tjednima. Zato smo krenuli istražiti što se događa.

Problem se manifestira u logovima na sljedeći način:

```
WARNING: getpatch: Can't download daily-24111.cdiff from database.clamav.net
ERROR: getpatch: Can't download daily-24111.cdiff from database.clamav.net
WARNING: Incremental update failed, trying to download daily.cvd
ERROR: Can't download daily.cvd from database.clamav.net
Giving up on database.clamav.net...
Update failed. Your network may be down or none of the mirrors listed in
 /etc/clamav/freshclam.conf is working. Check
 http://www.clamav.net/doc/mirrors-faq.html for possible reasons
```

ClamAV ima sustav zrcalnih poslužitelja koji opslužuje određene regije, a sve ide preko aliasa database.clamav.net i db.local.clamav.net. Preko njega svaka regija dobije najbliže polužitelje, kako bi se opterećenje distribuiralo na sve poslužitelje u mreži podjednako. Mi pripadamo (tko bi rekao) regiji jugoistočne Europe:

```
$ host db.local.clamav.net
db.local.clamav.net is an alias for db.southeu.clamav.net.
db.southeu.clamav.net has address 193.92.150.194
$ host 193.92.150.194
194.150.92.193.in-addr.arpa domain name pointer athftp02.forthnet.gr.
```

Dakle, za nas je odgovoran jedan poslužitelj u Grčkoj, koji ni nakon nekoliko tjedana očigledno nije proradio. Na stranicama blog.clamav.net [1] smo pronašli da se zaista dogodio ispad zrcalnih poslužitelja, ali da je sve riješeno još 15.11.2017. Kako to očigledno nije bio slučaj, odlučili smo sami potražiti rješenje.

Najlakše rješenje koje smo našli je dodati nove poslužitelje u /etc/clamav/freshclam.conf, a koje smo pronašli uz nešto malo guglanja i nešto malo logike: db.de.clamav.net, db.at.clamav.net, db.it.clamav.net. No, postoji i poslužitelj **db.eu.big.clamav.net**, koji bi trebao posluživati cijelu Europu (odnosno preusmjeravati na poslužitelje po cijeloj Europi, ne samo regionalno). Ovo pretpostavljamo nije rješenje koje bi se svidjelo pokretačima projekta ClamAV, pa ga shvatite kao privremeno rješenje. Problem će sigurno biti riješen u nekom trenutku, ali do tada sve što trebate napraviti je dodati redak u datoteku /etc/clamav.freshclam.conf, pa će popis zrcalnih poslužitelja biti:

```
DatabaseMirror db.eu.big.clamav.net
DatabaseMirror db.local.clamav.net
DatabaseMirror database.clamav.net
```

Još samo trebate restartati freshclam:

```
# systemctl restart clamav-freshclam
```

Nakon ovoga poruke o greškama se više ne bi trebale pojavljivati.

pon, 2017-12-11 16:14 - Željko Borš**Vijesti:** Linux [2]
Kategorije: Software [3]
Servisi [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

story_tag: clamav [5]

Source URL: https://sysportal.carnet.hr./node/1779

Links
[1] http://blog.clamav.net/2017/11/mirror-sync-outage-for-clamav-av-updates.html
[2] https://sysportal.carnet.hr./taxonomy/term/11
[3] https://sysportal.carnet.hr./taxonomy/term/25
[4] https://sysportal.carnet.hr./taxonomy/term/28
[5] https://sysportal.carnet.hr./taxonomy/term/187