# BIND: promjene u Lennyju

Nakon svake nadogradnje poslužitelja neminovno je da poneki od servisa treba ponovno podesiti, odnosno iskonfigurirati. Razlog ovome je nepostojanje automatizirane procedure koja će postavke, primjerice, freeradiusa 1.x prebaciti u postavke za freeradius 2.x. O nekoliko čimbenika ovisi što je bolje, ostaviti staru konfiguraciju ili uzeti novu pa prebaciti relevantne dijelove iz stare. No, o tome sada nećemo pisati, nego ćemo se ograničiti na promjene u konfiguraciji BIND-a u Lenny distribuciji, koje su neke sistem-inženjere zatekle nespremne jer su odgovorili da žele zadržati staru konfiguraciju, a ponašanje DNS servisa se promijenilo.

Problem se manifestira tako da DNS poslužitelj iznenada počinje odbijati upite s nekih vaših mrežnih segmenata, ili IP adresa koje rabite. U logovima se mogu pronaći unosi poput ovog:

```
Jul 28 13:02:03 stroj named[27283]: client 193.198.XXX.3#7308: query (cache) 'server.
domena.hr/A/IN'
  denied
Jul 28 13:02:03 stroj named[27283]: client 161.53.XXX.YYY#32925: query (cache) 'domen
a.hr/A/IN'
  denied
Jul 28 13:02:07 stroj named[27283]: client 87.253.32.130#36614: query (cache) 'stroj.
domena.hr/AAAA/IN'
  denied
Jul 28 13:02:07 stroj named[27283]: client 91.124.47.34#23295: query (cache) 'domena.
hr/MX/IN' denied
```

Vidimo da se nekim klijentima odbija upit za autorativnim podacima (to su podaci o vašim zonama i svim zonama za koje ste sekundar), a isto se događa i kad upite šalje profesorov laptop koji se fizički nalazi na drugoj lokaciji u drugom mrežnom segmentu.

Što se promijenilo, pa kod nadogradnje nismo mijenjali konfiguraciju? Odgovor se nalazi u datoteci /usr/share/doc/bind9/NEWS.Debian.gz (ne možemo dovoljno naglasiti koliko je korisno pročitati datoteke u /usr/share/doc direktoriju, barem za najbitnije servise!).

Maintaineri kažu:

```
As of bind 9.4, allow-query-cache and allow-recursion default to the builtin
acls 'localnets' and 'localhost'. If you are setting up a  name server for a
network, you will almost certainly need to change this.
```

Komentar se odnosi na dvije-tri najbitnije zabrane u BIND-u: **allow-query**, **allow-query-cache** i **allow-recursion**. Do inačice BIND-a 9.4, sve tri su bile potpuno otvorene, dakle svi su klijenti mogli postavljati upite bilo kojeg tipa. Ovo je dovelo do ozbiljnih sigurnosih problema, pa je vaš DNS poslužitelj mogao biti upotrijebljen u DoS napadu, ili se preko njega moglo saznati koje stranice posjećuju vaši korisnici (uvjetno rečeno).

Iako to nigdje nije napisano u konfiguraciji, *default* u BIND-u iz Lennyja je:

```
    allow-query { any; };
```

```
    allow-recursion { localhost; localnets; };
    allow-query-cache { localhost; localnets; };
```

Dakle, rekurzivni upiti i upiti iz *cachea* su ograničeni samo na "localhost" i "localnets". Po imenu možemo zaključiti o čemu se radi, i ujedno gdje je problem: BIND ne može znati da imate još nekoliko mrežnih segmenata kojima želite omogućiti neometane upite. On može samo pronaći konfiguraciju na postojećim mrežnim sučeljima i po tome se ravnati.

Što trebamo učiniti: našim korisnicima trebamo omogućiti sve upite, a ograničiti upite za sve ostale. Kako danas situacija nije jednostavna (mrežno gledajući), najlakše je promjene napraviti preko pristupnih lista (ACL-ova). Obično je dovoljno u named.conf.local (ili named.conf.options) dodati:

```
 acl "trusted" {
  161.53.XXX.YYY/24;
  193.198.XXX.0/26;
  localhost;
  localnets;
};

options {
  ...
  allow-query { any; };
  allow-recursion { trusted; };
  allow-query-cache { trusted; };
   ...
};
```

Ovime smo kreirali ACL "**trusted**", gdje ćemo upisati sve mreže kojima vjerujemo, a to su naravno svi segmenti mreža nad kojima imamo nadzor, ili eventualno segmenti kakvog domaćeg ISP-a, ukoliko vaši korisnici to zahtijevaju i rabe vaš DNS umjesto DNS od tog providera. **Za izračun CIDR načina označavanja mrežnih segmenata (npr. 161.53.1.0/24) poslužite se alatom** ipcalc **[1]**.

Definicija pristupne liste mora biti izvan "**options {}**" bloka, dok **allow-*** direktive mogu biti navedene ovako, u globalnom kontekstu, ili za svaku zonu pojedinačno. Obično želimo imati samo jednu konfiguraciju, pa **allow-*** direktive samo dopišite unutar "**options {}**" bloka.

Nakon toga samo treba restartati DNS poslužitelj. Svi bi DNS upiti vaših korisnika sada trebali biti odgovoreni, a u logovima i dalje pisati da je drugim klijentima zabranjen pristup (barem nekim vrstama upita).

Ukoliko primjetite da se opetovano s neke IP adrese ili mreže ponavljaju upiti, probajte kontaktirati administratora tog poslužitelja ili mrežnog segmenta. Ukoliko nema odgovora ni tada, možda bi za vas bilo dobro da napravite fail2ban [2] pravilo koji će klijente koji naprave **daleko previše** upita unutar nekog vremena, jednostavno blokirati preko iptables pravila?

UPDATED: 2010-04-21

- Logirajte [3] se za dodavanje komentara

uto, 2009-08-04 12:27 - Željko Boroš**Kuharice:** Linux [4]
**Kategorije:** Servisi [5]
**Vote:** 4

Vaša ocjena: Nema Average: 4 (1 vote)

**Source URL:** https://sysportal.carnet.hr/node/616

**Links**
[1] https://sysportal.carnet.hr/node/330
[2] https://sysportal.carnet.hr/node/542
[3] https://sysportal.carnet.hr/sysportallogin
[4] https://sysportal.carnet.hr/taxonomy/term/17
[5] https://sysportal.carnet.hr/taxonomy/term/28