BIND: kako podesiti razinu logiranja?

U prethodnim člancima [1] smo se dotaknuli teme o načinima *logginga* u BIND-u, odnosno kako napraviti da se određene kategorije log zapisa uopće ne pojavljuju u logovima. Naravno da tu nije kraj, te da BIND može puno više. Vratimo se malo u povijest... BIND inačice 4 je imao samo rudimentarne mogućnosti logiranja, odnosno samo uobičajeni način povećanja ili smanjivanja razine zapisa (*verbosity*), kao što to ima većina drugih servisa.

Novije inačice BIND-a uvode pojam kanala (*channela*), preko kojih možete definirati što će se (koje informacije iz BIND-a) i gdje logirati (zapisivati u posebnu datoteku ili slati u syslog). Pri tome je u kanalu moguće kombinirati obje opcije, i tako definirati način logiranja kako vam u određenim situacijama najviše odgovara.

Neki su kanali već ugrađeni, ali njih ne možete mijenjati, nego možete samo dopisivati nove kanale. To znači da ako određeni kanal zapisuje i u syslog i u posebnu datoteku, nećete moći promijeniti to ponašanje. Ali, vrlo je jednostavno kreirati drugi kanal koji će raditi po vašim potrebama.

Iako ovaj sustav logiranja nudi veliku fleksibilnost, i nije tako jednostavan za definirati, pa ćemo se ograničiti samo na praktičnu primjenu. Za više informacija pogledajte odličnu O'Reillyevu knjigu "BIND & DNS", ili dokumentaciju na Internetu (npr. http://www.bind9.net/).

Primjer 1: kako spriječiti pojavljivanje "*lame server*" poruka u logovima?

Ova se poruka pojavljuje zbog loše podešenosti drugih DNS poslužitelja, ne vašeg, stoga je razumljiva ideja da se te poruke ne bilježe u vašem syslogu. Te poruke se ponekad mogu pretjerano pojavljivati i oduzimati vam mrežne i procesorske resurse.

U named.conf.local ukucajte sljedeće retke:

```
logging {
        category lame-servers { null; };
};
```

Ovime smo kateogoriju "lame-servers" presumjerili na ugrađeni kanal "null", što, jasno, znači da se poruke o *lame* poslužiteljima jednostavno neće bilježiti. Ipak, u slučaju da imate problema s konfiguracijom DNS poslužitelja, zakomentirajte ove linije kako biste mogli vidjeti sve poruke koje će vam možda pomoći u rješavanju problema.

Naravno, morat ćete BIND-u reći da se konfiguracija promjenila:

```
# rndc reload
```

Pažljiviji će čitatelji primjetiti da ove retke donosi paket bind9-cn, pa ih ne treba posebno unositi.

Primjer 2: kako vidjeti koje upite naš poslužitelj prima?

U named.conf.local ukucajte slijedeće:

```
logging {
        channel moja_datoteka {
        file "log.queries";
        severity dynamic;
        };

        category queries { moja_datoteka; };
};
```

Ovdje smo kreirali novi kanal, i nazvali ga "moja_datoteka", da nas podsjeća da na to zapisi idu samo u jednu datoteku, /var/cache/bind/log.queries. Direktiva "severity" može biti jedna od:

```
critical | error | warning | notice | info | debug [ level ] | dynamic
```

Slično kao i kod sysloga, ova direktiva određuje da će se zapisivati samo ta razina informacija i viša. Pretpostavljena vrijednost je **info**. "Dynamic" znači da razinu određujemo preko naredbenolinijskog parametra "-d" ili preko naredbe "rndc trace".

U ovom primjeru, potrebno je pokrenuti **debug** način rada putem naredbe:

```
# rndc trace
```

Kao što smo prije spomenuli, ovaj sustav logiranja je kompleksan, te će se uključivanjem debug načina rada odjednom pojaviti i datoteka named.run u istom direktoriju. U njoj se nalaze dodatni debug podaci, koji nas u ovoj
konfiguraciji ne zanimaju, pa ćemo ih isključiti. Cijela konfiguracija tada izgleda ovako:

```
logging {
        channel moja_datoteka {
        file "log.queries";
        severity dynamic;
        };

        category lame-servers { null; };
        category default { default_syslog; };
        category queries { moja_datoteka; }
;};
```

I opet:

```
# rndc reload
```

Sa cijelom ovom konfiguracijom isključili smo logiranje poruka o "*lame* serverima", preusmjerili standardne poruke u syslog i ugasili dodatne debug podatke, te na kraju logiranje upita preusmjerili u datoteku po želji.

Logovi znaju jako brzo narasti, pa ih je upitno staviti u neki logrotate sustav, ukoliko na dulje vrijeme želite pratiti rad DNS sustava.

- Logirajte [2] se za dodavanje komentara

pon, 2009-08-31 23:16 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Servisi [4]

Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/626

Links
[1] https://sysportal.carnet.hr/node/625
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28