BIND: ignoriranje pojedinih logova u Lennyju

Kako smo već pisali [1], inačica BIND DNS poslužitelja donosi neke novosti. Neke od njih mogu izazvati velik broj lažnih upozorenja od raznih sustava za nadzor logova (logcheck [2], OSSEC). Kako je ovo samo odraz činjenice da su uvedena neka ograničenja, ova se upozorenja mogu ignorirati. Na prvom mjestu, radi se o upozorenju o tome da je "EDNS ugašen", te da je nekom klijentu izvan vaše mreže uskraćen rekurzivni upit.

EDNS je proširenje DNS-a, u smislu proširenja postojećeg polja OPT kako bi se zadovoljile nove, poželjnije funkcije. Kako EDNS nije tema članka, za više informacija pogledajte Wikipediju na linku http://en.wikipedia.org/wiki/EDNS [3]. Također, ukoliko želite provjeriti dolazi li do ovih poruka zbog nekog vašeg vatrozida, pogledajte poruku na Usenetu: http://groups.google.com/group/comp.protocols.dns.bind/browse_thread/thread/cfa8c63ec6bd08d6 [4].

U većini slučajeva, pojavljivanje ovih poruka će biti dovoljno samo spriječiti putem direktive u named.conf.local (jer drugo i nećete moći učiniti). Dovoljno je upiati u *logging* blok:

```
logging {
        category edns-disabled { null; };
};
```

Nakon restarta procesa "named", poruke se više ne bi trebale pojavljivati.

Drugi problem koji se pojavio je pojavljivanje mnogobrojnih poruka "denied", u obliku:

```
client 161.53.XXX.YYY#50184: query (cache) 'domena.com/A/IN' denied
```

Zbog novosti uvedenih u novom BIND-u, ove poruke će se pojavljivati za svakog klijenta izvan "trusted" deklaracije. Nije baš razborito ukloniti u potpunosti ove poruke: bolje je da ih logcheck ignorira. Ovo ćemo postići tako da u /etc/logcheck/ignore.d.server/local upišete:

```
.*named.*client \[161\.53\.[0-9]+\.[0-9]+\].*query.*denied
```

Za OSSEC, taj redak upišite u ovom obliku u datoteku /var/ossec/rules/local_rules.xml:

```
<rule id="100131" level="0">
  <if_sid>1002</if_sid>
  <program_name>^named</program_name>
  <match>denied</match>
  <description>BIND denied upozorenja</description>
</rule>
```

SID je broj koji vam se prikaže kod izvješća, pa ga prilagodite po potrebi. Stvar je jednostavnija za rule_id, samo odaberite prvi slobodni broj veći od 100000, što je rezervirano za korisnička pravila.

Kako smo već spomenuli, nije razborito ove poruke potpuno izbrisati iz logova. No, i to se može:

```
logging {
        category security { null; };
};
```

U ovom slučaju nemate nikakve indikacije o odbijanju upita, iako je ta informacija izuzetno korisna kod prvotnog postavljanja DNS sustava na računalo. Rješenje je ili odgoditi postavljanje ove direktive dok ne postavite sustav DNS-a, ili filtrirati ove unose u vašem omiljenom *log checkeru*.

- Logirajte [5] se za dodavanje komentara

pon, 2009-08-31 01:07 - Željko Boroš**Kuharice:** Linux [6]
Kategorije: Servisi [7]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/625

Links
[1] https://sysportal.carnet.hr/node/616
[2] https://sysportal.carnet.hr/node/604
[3] http://en.wikipedia.org/wiki/EDNS
[4] http://groups.google.com/group/comp.protocols.dns.bind/browse_thread/thread/cfa8c63ec6bd08d6
[5] https://sysportal.carnet.hr/sysportallogin
[6] https://sysportal.carnet.hr/taxonomy/term/17
[7] https://sysportal.carnet.hr/taxonomy/term/28