

## Statistika antivirusnog poslužitelja

### PAKET `amavis-stats` OD INAČICE `SQUEEZE` NIJE VIŠE DOSTUPAN NA DEBIANOVIM REPOZITORIJIMA!

Upotrebom različitih statističkih programa možemo dobiti korisne informacije o radu nekog servisa na poslužitelju. Obično takve informacije sadrže i grafički prikaz što povećava preglednost rezultata obrade.

U ovom tekstu prikazati ćemo program **`amavis-stats`** za analizu rada antivirusne programske podrške na poslužiteljima koji koriste paket **`amavis`**. Kao rezultat instalacije ovog programa dobiti ćemo web stranicu sa grafičkim prikazom e-mail prometa s posebnim naglaskom na zaustavljene poruke s virusima. Stranica se sastoji od četiri grafikona koji prikazuju dnevnu, tjednu, mjesečnu i godišnju statistiku rada antivirusnog poslužitelja.

Instalacija ovog paketa sastoji se od instalacije deban paketa `amavis-stats` i nekoliko manjih izmjena u konfiguraciji poslužitelja.

Paket ćemo instalirati korištenjem programa `apt-get`:

```
apt-get update
apt-get install amavis-stats
```

Uz `amavis-stats` instalirati će se još i paketi `wwwconfig-common` i `rrdtool` koji su nužni za njegovo normalno funkcioniranje. Instalacijski program će nam postaviti jedno pitanje:

```
Amavis-stats keeps its database files under /var/cache/amavis-stats.
Should this directory be removed completely on purge?
```

```
Remove RRD files on purge?
```

Upit se odnosi na eventualnu deinstalaciju ovog paketa i čuvanje podataka koji su obrađeni za vrijeme njegovog rada. Ako odgovorimo sa 'no' podaci će biti sačuvani.

Instalacijski program otvoriti će korisnika `amavis-stats` pod čijim će se vlasništvom pokretati program.

Da bi se statistika mogla uspješno napraviti, korisnik `amavis-stats` mora imati pristup logovima e-mail poslužitelja koji se nalaze u direktoriju `/var/log/mail`. Datoteka `mail.info` koju `amavis-stats` analizira ima ovakva prava pristupa:

```
-rw-r----- 1 root adm 1098452 Oct 26 13:40 mail.info
```

Dakle, korisnik `amavis-stats` mora biti član grupe `adm`, što upisujemo u datoteku `/etc/group`:

```
adm:x:4:logcheck,amavis-stats
```

Sljedeći korak je dozvola pristupa `amavis-stats` programu u sam direktorij `/var/log/mail` koji obično ima ovakva prava:

```
drwxr-s--- 2 root mail 4096 Oct 26 00:11 /var/log/mail/
```

Da bi korisnik `amavis-stats` mogao pristupiti datotekama unutar tog direktorija dovoljno je dodati pravo ulaska za sve:

```
chmod o+x /var/log/mail
```

nakon čega će stanje biti ovakvo:

```
drwxr-s--x 2 root mail 4096 Oct 26 00:11 /var/log/mail/
```

Da bi se statistika uspješno provodila potrebno je povremeno pokrenuti program `amavis-stats`, što se radi pomoću `cron-a`. Instalacijski paket postavlja datoteku `amavis-stats` u direktorij `/etc/cron.d` koja izgleda ovako:

```
#
# cron job for the amavis-stats package
#
*/5 * * * * amavis-stats [ -x /usr/sbin/amavis-stats ] && /usr/sbin/amavis-
stats /var/log/mail.info
```

Potrebno je ovo još prilagoditi konfiguraciji na našim poslužiteljima i popraviti direktorij gdje se nalazi log datoteka. Umjesto `/var/log/mail.info` napisati ćemo `/var/log/mail/mail.info` tako da imamo ovakav zapis u spomenutoj datoteci:

```
*/5 * * * * amavis-stats [ -x /usr/sbin/amavis-stats ] && /usr/sbin/amavis-
stats /var/log/mail/mail.info
```

Kada cron prvi put pokrene statistiku generirati će se rezultati koje možemo vidjeti preko web preglednika, upisom adrese našeg web poslužitelja i direktorija `amavis-stats`, npr. <http://www.domena.hr/amavis-stats/>

Kao primjer može se pogledati stranica <http://www.krs.hr/amavis-stats/>.

- [Logirajte](#) [1] se za dodavanje komentara

pon, 2007-10-29 12:21 - Damir Mrkonjić **Kuharice:** [Linux](#) [2]

**Vote:** 0

No votes yet

**Source URL:** <https://sysportal.carnet.hr/node/313>

### Links

[1] <https://sysportal.carnet.hr/sysportallogin>

[2] <https://sysportal.carnet.hr/taxonomy/term/17>

