Logwatch - logovi na jednom mjestu

 U vrijeme godišnjih odmora većina sistemaca nema pretjeranu želju svakodnevno pregledavati desetke i stotine linija logova. Tu uskače **logwatch**, alat koji za vas analizira sve logove i jednom dnevno pošalje e-mail na vašu adresu.

U tom e-mailu se nalazi sumirani izvještaj tj. bitne stvari iz svih log datoteka na sustavu. Logwatch je modularan, pa je moguće dodavati i izbacivati log datoteke koje će analizirati, odrediti period i dubinu analize, format izvještaja te, primjerice, da li će alat pretraživati i arhivirane logove. Sama instalacija je klasična:

```
apt-get update
apt-get install logwatch
```

"Out of the box" konfiguracija je dovoljna za početnu upotrebu i izvještaj će, između ostalog, sadržavati greške pri prijavljivanju na e-mail, greške ssh pristupa i stanje diskovnog prostora. Primjerice, sumirani dio izvještaja o pokušajima ssh pristupa (iz datoteke *auth.log*) izgleda ovako:

```
################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Mon Jul 30 06:25:03 2012
        Date Range Processed: yesterday
                                        ( 2012-Jul-29 )
                                        Period is day.
        Detail Level of Output: 0
        Type of Output/Format: mail / text
        Logfiles for Host: hostname
##################################################################

--------------------- SSHD Begin ------------------------
Failed logins from:
    60.250.214.155 (60-250-214-155.HINET-IP.hinet.net): 30 times
    61.235.147.19: 37 times
    87.106.150.224 (s15410618.onlinehome-server.info): 10 times
    94.23.72.122 (94-23-72-122.ovh.net): 3 times
    202.130.104.235 (mail.toppanforms.com): 26 times
---------------------- SSHD End ------------------------
```

Konfiguracijska datoteka *logwatch.conf* se nalazi na neuobičajenom mjestu, unutar direktorija */ush/share/logwatch/default.conf/*, a na istom se mjestu, u poddirektoriju *logfiles*, nalaze i konfiguracijske datoteke za svaku log datoteku. Između ostalih, tu se nalaze *clam-update.conf*, *fail2ban.conf*, *iptables.conf*, *samba.conf* i *xferlog.conf*. Sadašnja verzija logwatcha donijela je veliko poboljšanje u odnosu na verziju koja je radila na Debianu 5, gdje se velika većina ovih konfiguracijskih datoteka morala ručno kreirati i uključivati u izvještaje. Ukoliko nedostaje neki log koji bi željeli uključiti u izvještaj, jednostavno ćete kreirati njenu kofiguracijsku datoteku u kojoj je potrebno navesti lokaciju log datoteke.

Za slanje dnevnog izvještaja instalacija je kreirala zadatak *00logwatch* smješten u */etc/cron.daily/* u kojem je kao *output* parametar naveden mail definiran u kofiguracijskoj datoteci. Naravno, izvještaj se može i ručno kreirati u bilo kojem trenutku te poslati na određenu mail adresu pomoću naredbe:

```
/usr/sbin/logwatch --mailto adresa@domena
```

Iako možda ne može u potpunosti zamijeniti praćenje "pravih" logova, logwatch može pomoći u svakodnevnom radu svojim brzim stvaranjem ukupne slike događanja na poslužitelju, što je uvijek dobrodošlo.

pet, 2012-08-10 09:26 - Mirko Lovričević**Vijesti:** Linux [1]
Kuharice: Za sistemce [2]
Kategorije: Operacijski sustavi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1077

Links
[1] https://sysportal.carnet.hr/taxonomy/term/11
[2] https://sysportal.carnet.hr/taxonomy/term/22
[3] https://sysportal.carnet.hr/taxonomy/term/26