

## Naredbe za koje (možda) niste znali 21: multital



Da logove na poslužitelju treba redovito pregledavati, zna svaki sistem-inženjer. Jednostavno, bez logova bi posao sistem-inženjera bio nemoguć. Iako imamo automatizirane programe (tipa logwatch, fail2ban ili OSSEC) koji nam pomažu u detekciji potencijalnih problema (poglavito sigurnosnih), neophodno je ponekad logove pogledati "uživo". Ovdje se možemo poslužiti programima tail i less, koji mogu pratiti logove onako kako se *pune*, ali imamo odličan alat za praćenje više logova odjednom - **multital**.

Kao i programčić "[nethogs](#) [1]", kojeg smo opisali u prethodnom članku u ovoj seriji, tako i multital slijedi jednostavnu logiku: raditi jednu stvar dobro, i ne zbunjivati korisnika bespotrebnim opcijama koje u većini slučajeva neće nikada rabiti. Pokretanje programa je standardno, samo treba nakon imena naredbe treba navesti logove koje želimo pratiti:

```
# multital /var/log/mail.log /var/log/daemon.log /var/log/apache2/access.log
```

Multital radi preko vrlo poznatog *ncurses* sučelja za tekstualne terminale, što znači da ima sustav prozora koji pokušava postići dio funkcionalnosti klasičnih grafičkih GUI-ja. Nakon pokretanja, bit će prikazana tri prozora kao na slici:

```
relay=local, delay=0.04, delays=0.01/0.01/0/0.02, dsn=2.0.0, status=sent (delivered to file: /tmp/.rewrite2.log)
Sep  1 13:40:24 postfix/qmgr[28813]: 685524B9BA: removed
Sep  1 13:40:25 dovecot: pop3-login: Login: user=< >, method=PLAIN, rip=161.53.12.111, lip=161.53.30.100
Sep  1 13:40:26 dovecot: POP3( ): Disconnected: Logged out top=0/0, retr=1/6477, del=0/841, size=28433625
00] /var/log/mail.log F1/<CTRL>+<h>: help 358KB - 2011/09/01 13:41:01
:1441(get_peer_addr_internal)
Sep  1 13:28:10 smbd[31177]: getpeername failed. Error was Transport endpoint is not connected
Sep  1 13:28:10 smbd[31177]: read_fd_with_timeout: client 0.0.0.0 read error = Connection reset by peer.
Sep  1 13:40:13 named[13268]: client 161.53.30.108#55203: update 'os.carnet.hr/IN' denied
01] /var/log/daemon.log F1/<CTRL>+<h>: help 361KB - 2011/09/01 13:41:01
6 "-" "Yeti/1.0 (NHN Corp.; http://help.naver.com/robots/)"
61.247.204.38 - - [01/Sep/2011:04:10:44 +0200] "GET / HTTP/1.1" 302 496 "-" "Yeti/1.0 (NHN Corp.; http://help.naver.com/robots/)"
208.91.113.20 - - [01/Sep/2011:07:58:21 +0200] "GET / HTTP/1.1" 302 496 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070227 Red Hat/1.5.0.10-0.1.el4 Firefox/1.5.0.10"
02] /var/log/apache2/access.log F1/<CTRL>+<h>: help 2KB - 2011/09/01 13:41:01
```

U svakom od tri prozora bit će prikazano nekoliko zadnjih redova odabranih log datoteka. Multital pokušava biti uslužan, pa može obojati određene dijelove logova drugom bojom, primjerice datum je označen plavom bojom, naizmjenično svjetlijom i tamnijom nijansom. U svakom trenutku možete dobiti pomoć ukoliko pritisnete kombinaciju tipki **<CTRL+h>**. U prozoru pomoći možete pregledati

sve dostupne naredbe sa standardnim **Page Up** i **Page Down** tipkama, a prozor gasite sa **<CTRL+g>**.

Ukoliko u nekom logu vidite nešto vrijedno pažnje, možete privremeno ugasiti sve prozore osim odabranog. Ovo možete napraviti pomoću tipke **"u"**, nakon čega odabirete željeni prozor:

```
p=161.53. . . 1, lip=161.53. . 1.
Sep 1 13:45:45 dovecot: POP3( ): Disconnected: Logged out top=0/0, re
tr=2/4434, del=0/843, size=28438025
Sep 1 13:46:31 postfix/smtpd[31395]: connect from unknown[218. .42.7]
Sep 1 13:46:31 po postfix/smtpd[31395]: warning: non-SMTP command from unknown[
218. .42.7]: GET http://www.sciencedirect.com/ HTTP/1.1
Sep 1 13:46:31 postfix/smtpd[31395]: disconnect from unknown[218. .42.7]
00] /var/log/mail.log 376KB - 2011/09/01 13:46:39
:1441(get_peer_addr_inte
Sep 1 13:28:10 smbd[ Select window to keep open rror was Transport endpoi
nt is not connected 00 /var/log/mail.log
Sep 1 13:28:10 smbd[ 01 /var/log/daemon.log client 0.0.0.0 read erro
r = Connection reset by 02 /var/log/apache2/access.
Sep 1 13:40:13 named[ Press ^G to abort 203: update ' .carnet.h
r/IN' denied
01] /var/log/daemon.log 361KB - 2011/09/01 13:46:39
6 "-" "Yeti/1.0 (NHN Corp.; http://help.naver.com/robots/)"
61.247.204.38 - - [01/Sep/2011:04:10:44 +0200] "GET / HTTP/1.1" 302 496 "-" "Yet
i/1.0 (NHN Corp.; http://help.naver.com/robots/)"
208.91.113.20 - - [01/Sep/2011:07:58:21 +0200] "GET / HTTP/1.1" 302 496 "-" "Moz
illa/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070227 Red Hat/1.5.0.1
0-0.1.el4 Firefox/1.5.0.10"
```

Nakon što završite, možete se vratiti u prethodni prikaz svih prozora s tipkom **"U"** (naravno, ovdje je riječ o kombinaciji **<Shift+u>**). Vizualni pregled očima nije uvijek i najbrži, zato multitail posjeduje funkciju traženja, koju možete pozvati s **"/"**. Slično ovoj, sa kombinacijom **<Shift+/,>**, možete dobiti **highlite** funkciju [1], kao na slici:

```
Sep 1 13:46:55 postfix/qmgr[28813]: A316F4B9BA: removed
Sep 1 13:49:06 postfix/anvil[31181]: statistics: max connection rate 2/60s f
or (smtp:161.53. .6) at Sep 1 13:40:22
Sep 1 13:49:06 postfix/anvil[31181]: statistics: max connection count 1 for
(smtp:161.53. .6) at Sep 1 13:40:20
Sep 1 13:49:06 postfix/anvil[31181]: statistics: max cache size 2 at Sep 1
13:42:49
00] /var/log/mail.log 381KB - 2011/09/01 13:49:30
:1441(get_peer_addr_internal)
Sep 1 13:28:10 s Transport endpoi
nt is not connecte Global highlight 0.0.0.0 read erro
r = Connection res error
Sep 1 13:40:13 [X] case insensitive (press TAB) pdate ' carnet.h
r/IN' denied
01] /var/log/daemon.log 361KB - 2011/09/01 13:49:30
6 "-" "Yeti/1.0 (NHN Corp.; http://help.naver.com/robots/)"
61.247.204.38 - - [01/Sep/2011:04:10:44 +0200] "GET / HTTP/1.1" 302 496 "-" "Yet
i/1.0 (NHN Corp.; http://help.naver.com/robots/)"
208.91.113.20 - - [01/Sep/2011:07:58:21 +0200] "GET / HTTP/1.1" 302 496 "-" "Moz
illa/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070227 Red Hat/1.5.0.1
0-0.1.el4 Firefox/1.5.0.10"
```

Mi smo potražili najzanimljiviju riječ koju možemo naći u logovima: **error**. Nakon što multitail

pronađe traženu riječ, označit će cijeli redak u kojemu je pronašao traženu riječ:

```
Sep  1 13:46:55 postfix/qmgr[28813]: A316F4B9BA: removed
Sep  1 13:49:06 postfix/anvil[31181]: statistics: max connection rate 2/60s f
or (smtp:161.53. .6) at Sep  1 13:40:22
Sep  1 13:49:06 postfix/anvil[31181]: statistics: max connection count 1 for
(smtp:161.53. .6) at Sep  1 13:40:20
Sep  1 13:49:06 postfix/anvil[31181]: statistics: max cache size 2 at Sep  1
13:42:49
00] /var/log/mail.log 381KB - 2011/09/01 13:49:34
:1441(get peer addr internal)
Sep  1 13:28:10 smbd[31177]: getpeername failed. Error was Transport endpoi
nt is not connected
Sep  1 13:28:10 smbd[31177]: read fd with timeout: client 0.0.0.0 read erro
r = Connection reset by peer.
Sep  1 13:40:13 named[13268]: client 161.53. .108#55203: update ' carn
et.h
r/IN' denied
01] /var/log/daemon.log 361KB - 2011/09/01 13:49:34
6 "-" "Yeti/1.0 (NHN Corp.; http://help.naver.com/robots/)"
61.247.204.38 - - [01/Sep/2011:04:10:44 +0200] "GET / HTTP/1.1" 302 496 "-" "Yet
i/1.0 (NHN Corp.; http://help.naver.com/robots/)"
208.91.113.20 - - [01/Sep/2011:07:58:21 +0200] "GET / HTTP/1.1" 302 496 "-" "Moz
illa/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070227 Red Hat/1.5.0.1
0-0.1.el4 Firefox/1.5.0.10"
```

Označavanje redaka ostaje i ako prijedemo u način rada s jednim prozorom.

Moramo priznati da smo vas malo prevarili, jer multital nema samo dvije-tri, nego preko dvadeset opcija. Tako, multital može pratiti izlaz naredbi (STDOUT), može izvršavati proizvoljne naredbe ukoliko se pojavi određeni string (točnije *regex*) unutar log datoteke ili u izlazu naredbe, a očekivano podržava prilagodbu boja i sučelja. Smatramo da su za ove naprednije stvari primjereniji već spominjani fail2ban, a pogotovo OSSEC, pa nećemo ulaziti dublje u ove mogućnosti multitaila.

[1] na tipkovnici s HR rasporedom tipaka znak / se dobija s kombinacijom **<Shift+7>**, dakle već rabimo Shift. Kako onda dobiti kombinaciju tipaka **<Shift+/>**? Postoje (barem) dva načina... odgovorite u komentarima.

- [Logirajte](#) [2] se za dodavanje komentara

pet, 2011-09-02 14:55 - Željko BorošKuharice: [Linux](#) [3]

**Kategorije:** [Software](#) [4]

**Vote:** 4.5

Vaša ocjena: Nema Average: 4.5 (2 votes)

**Source URL:** <https://sysportal.carnet.hr/node/877>

**Links**

- [1] <https://sysportal.carnet.hr/node/862>
- [2] <https://sysportal.carnet.hr/sysportallogin>
- [3] <https://sysportal.carnet.hr/taxonomy/term/17>
- [4] <https://sysportal.carnet.hr/taxonomy/term/25>