

Napredno korištenje operacijskog sustava Linux

4. Sistemski logovi i nadziranje

Leonard Volarić Horvat, Borna Skukan

Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

01.04.2017

1 Logging

2 Monitoring

Logging

Logovi

- Dnevničke datoteke
 - tekstualne
 - binarne (systemd dnevnički sustav: journald; journalctl)
- Zapisuju radnje vezane za praćeni proces
- Primjena: dijagnoza kvarova, praćenje stanja sustava, kronologija događaja, sigurnosni zapisi...

/var/log direktorij

- Direktorij s glavninom log datoteka na sustavu
- Primjeri:
 - boot.log - boot poruke
 - auth.log - poruke o autentikacijama korisnika
 - dpkg.log - poruke vezane uz dpkg (npr. `apt install paket`)
- S dolaskom systemd-a dio logova prelazi iz /var/log u journalctl

Syslog

- Sustav koji hvata sve poruke u Linux sustavu
- Vrlo složena arhitektura, ugrađena u sve distribucije
- rsyslog (Reliable Syslog) - moderna verzija sysloga
- Daemon proces, jednostavan za korištenje
- Konfiguracija u `/etc/[r]syslog.conf`

- Danas dijelom zasjenjen journald-om
- I dalje moguće paralelno koristiti oba

/etc/syslog.conf

- item.priority [; item.priority] /path/to/file

Vrsta:

- auth, authpriv (general and private auth)
- cron
- kern (kernel)
- mail
- news
- user (user process)
- uucp
- local0..

Prioritet:

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug
- none

/etc/syslog.conf

- item.priority [; item.priority] /path/to/file

```
# All info, none mail nor privat auth
*.info; mail.none; authpriv.none    /var/log/messages
```

```
# Everybody gets emergency messages
*.emerg                               *
*.emerg                               @10.1.1.254
```

```
# " = " will force ONLY specific priority
news.=crit                            /var/log/news/critical
```


Logger utility - API to syslog

- Korištenje iz drugih programa
- `logger [options] [message]`
- Ispisuje poruku u `/var/log/syslog`
- `Ožu 31 09:51:05 rincewind-N551JK rincewind[569]: This is the Central Scrutinizer`

Logrotate

- Održavanje logova
- `/etc/logrotate.conf` `/etc/logrotate.d/`

```
# rotate
weekly
# keep [weeks]
rotate 4
# create new after rotation
create
# compress
compress
# additional
include /etc/logrotate.d
```

Logrotate

- Specifična datoteka

```
# /etc/logrotate.d/nginx
/var/log/nginx/*.log {
    daily
    missingok
    rotate 52
    compress
    delaycompress
    notifempty
    create 640 nginx adm
    sharedscripts
    postrotate
        [ -f /var/run/nginx.pid ] &&
        kill -USR1 'cat /var/run/nginx.pid'
    endscript
}
```

Monitoring

ps

- "process status"
- Alat za prikaz trenutno aktivnih procesa
- Često koristen u kombinaciji s grep-om

ps aux

ps -ejH

top

- *Realtime* praćenje trenutnih procesa
- Mogućnost sortiranja i filtriranja
- Prikazuje i osnovne metrike o sustavu
- `htop` - intuitivniji i pregledniji

htop

```

1 [ 0.0%] 5 [ 0.0%]
2 [|| 1.9%] 6 [||||||||||||||||||||||||||||||||| 100.0%]
3 [ 0.0%] 7 [ 0.0%]
4 [||||||||||||||||||||||||||||||||| 100.0%] 8 [||| 1.4%]
Mem [||||||||||||||||||||| 11310/24155MB] Tasks: 87, 29 thr; 1 running
Swp [||||||||||||||||||||| 2024/2047MB] Load average: 1.71 1.39 1.37
Uptime: 64 days, 20:42:00

  PID USER      PRI  NI  VIRT   RES   SHR  S  CPU% MEM%   TIME+  Command
12865 leonard.v  20    0 14608   3028  2344  R   0.5  0.0   0:00.69 htop
18468 nginx      20    0 27132   7636  3880  S   0.5  0.0  28:38.76 nginx: worker process
    25 root       20    0 188M    125M  123M  S   0.5  0.5  26:38.80 /lib/systemd/systemd-journald
 5986 incanus   20    0 116M    6328  3832  S   0.0  0.0  12:00.33 irssi
 5040 capica    20    0 29096  11220  2208  S   0.0  0.0   0:25.85 squid -NsY
31076 vrabac   20    0 171M   18888  5472  S   0.0  0.1   2:34.11 weechat-curses
 8854 capica    20    0 23692   5160  1928  S   0.0  0.0   2:28.84 SCREEN
25389 shifty    20    0 188M   34572  6640  S   0.0  0.1  34:26.67 weechat-curses
 7100 robert    20    0 171M    7056  5104  S   0.0  0.0  16:37.37 weechat-curses
 4550 nidzo    20    0 171M   18932  5284  S   0.0  0.1  16:05.09 weechat-curses
   292 nagios    20    0 10736   1652  1524  S   0.0  0.0   3:47.28 /usr/sbin/nsca --daemon -c /etc
13872 cetko     20    0 116M    5832  4012  S   0.0  0.0   0:16.00 irssi
   199 root      20    0 254M    3404  2192  S   0.0  0.0   6:14.50 /usr/sbin/rsyslogd -n
   189 root      20    0 254M    3404  2192  S   0.0  0.0  12:21.35 /usr/sbin/rsyslogd -n
   281 nsld      20    0 422M    5952  3780  S   0.0  0.0  19:07.75 /usr/sbin/nsld
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit

```

Slika: htop

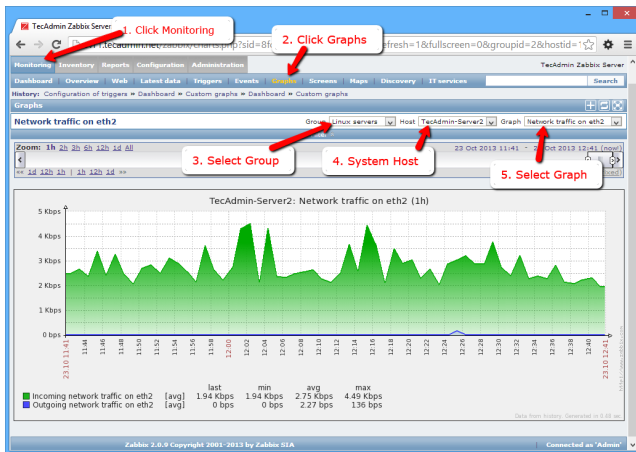
/proc

- Direktorij /proc - izvor većine podataka
 - uptime - /proc/uptime
 - loadavg - /proc/loadavg
 - proces s traženim PID-om - /proc/<PID>
- /proc koristi procfs pseudo-filesystem
- Dinamička struktura - stvara i briše pripadajuće datoteke zajedno s procesima

Nadzor procesa i sustava

- Zabbix - agent + server + vizualizacija
- Ossec - Nadzor logova + mail
- Sentry - Ossec + akumulacija
- Sentry - agent + server + plugins
- Kibana - vizualizacijski alat
- Sentry - Ossec + akumulacija

Zabbix



Slika: Zabbix

Literatura

http://www.srce.unizg.hr/fileadmin/Srce/proizvodi_usluge/obrazovanje/tecajevi/linux-akademija/L120.pdf

http://www.linuxcommand.org/man_pages/logrotate8.html

<http://man7.org/linux/man-pages/man3/syslog.3.html>

<http://www.zabbix.com>

<https://www.elastic.co/products/kibana>