

Napredno korištenje operacijskog sustava Linux

4. Sistemske logove i nadziranje

Leonard Volarić Horvat, Marin Petričević, Borna Skukan

Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

31.03.2017

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 korišten u kombinaciji sa grep-om

`ps aux`

`ps -ejH`

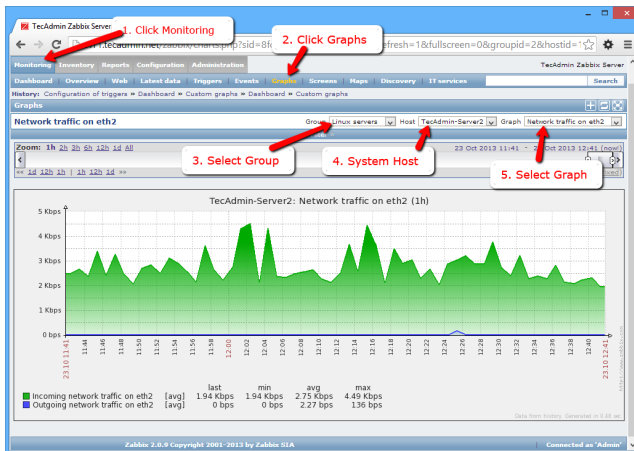
top

- Pracenje trenutnih procesa u real-timeu
- Mogucnost sortiranja i filtriranja
- Prikazuje i osnovne metrike o sustavu
- `htop` - intuitivniji i pregledniji

Nadzor procesa i sustava

- Ossec - Nadzor logova + mail
- Sentry - Ossec + akumulacija
- Zabbix - agent + server + vizualizacija
- 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>