

# Napredno korištenje operacijskog sustava Linux

## 4. Sistemski logovi i nadziranje

Leonard Volarić Horvat, Marin Petričević

Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu  
Fakultet elektrotehnike i računarstva

29.03.2017

## 1 Logging

# 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

## 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 ONYL specific priority
news.=crit                          /var/log/news/critical
```



# Logger utility - API to syslog

- Koristenje iz drugih programa
- `logger [options] message`
- Ispisuje poruku u `/var/log/messages`
- `Apr 8 21:24:26 g550 ulicar: message`

# 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
}
```

# 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

# Literatura

[http://www.srce.unizg.hr/fileadmin/Srce/proizvodi\\_usluge/obrazovanje/tecajevi/linux-akademija/L120.pdf](http://www.srce.unizg.hr/fileadmin/Srce/proizvodi_usluge/obrazovanje/tecajevi/linux-akademija/L120.pdf)

[http://www.linuxcommand.org/man\\_pages/logrotate8.html](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>