Logovi

 Logovi su nezamjenljivi dio gotovo svakog operativnog sustava. U njima se mogu pronaći sve relevantne informacije o prošlom i, bitnije, trenutnom stanju sustava, te je njihova kontrola jedna od stvari koju svaki sistem-inženjer mora svakodnevno obavljati. U tome nam mogu pomoći alati poput OSSEC-a ili logchecka, ali ručni pregled se ne može ničim zamijeniti.

Na Linux sustavima log zapisi se nalaze u direktoriju /var/log (uz možda poneki izuzetak, no to nam u ovom trenutku nije važno). U slučaju da naiđete na bilo kakve probleme u radu sustava ili njegovih servisa, prvo mjesto gdje trebate pogledati je upravo tamo, i to u datoteci /var/log/syslog i /var/log/messages.

Iako su logovi obične tekstualne datoteke koje se mogu otvoriti u editoru ili naredbom less, vrlo često se one pregledavaju naredbom tail:

```
debian# tail /var/log/syslog
```

Naredba tail će prikazati zadnjih 10 redaka u datoteci. Ukoliko želite vidjeti manje ili više redaka (primjerice, pet), upotrijebite naredbu tail na ovaj način:

```
debian# tail -5 /var/log/syslog
```

No, logovi su datoteke koje se konstantno "pune" s novim unosima. Tako ćete pregledavanjem logova uvijek biti u malom zaostatku za aktualnim zbivanjima na sustavu. U ovom slučaju može vam pomoći opcija "-f". Uporabom ove opcije tail će konstantno nadzirati datoteku, i ispisati svaki novi redak koji se upiše u datoteku dok je pregledavate:

```
debian# tail -f /var/log/messages
Mar 19 08:50:43 server clamd[10182]: Reading databases from /var/lib/clamav
Mar 19 08:50:52 server clamd[10182]: Database correctly reloaded (953322
signatures)
```

Sličan rezultat možete postići i preko naredbe less, ukoliko pritisnete "<SHIFT> + f" dok pregledavate datoteku:

```
debian# less /var/log/dmesg
[   50.948259] e100: eth0: e100_watchdog: link up, 100Mbps, full-duplex
[   50.949378] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Waiting for data... (interrupt to abort)
```

Izdvojit ćemo najbitnije log datoteke iz /var/log direktorija, te što se u njih upisuje:

1. **auth.log** - poruke vezane uz autentikaciju korisnika
2. **daemon.log** - poruke vezane uz daemon procese na sustavu
3. **debug** - poruke razine debug (vidi dolje)

4. **syslog** - većina drugih poruka se zapisuje i ovdje
5. **kern.log** - poruke vezane uz jezgru sustava

Ove datoteke su konstantno otvorene za pisanje, a u njih zapisuje daemon syslogd. Ponašanje ovog daemona možete kontrolirati preko njegove konfiguracijske datoteke, /etc/syslog.conf. Konfiguracija je malo specifična, jer uvodi pojam klase i razine.

Svaka moguća poruka koja ide prema syslogu mora imati svoju klasu ("facility") i razinu ("severity"). Klase na Linuxu su redom: **auth**, **authpriv**, **cron**, **daemon**, **ftp**, **kern**, **lpr**, **mail**, **mark**, **news**, **security** (isto što i auth), **syslog**, **user**, **uucp** i **local0** do **local7**.

Moguće razine su: **debug**, **info**, **notice**, **warn**, **err**, **crit**, **alert**, **emerg** i **panic**. Neke nećete nikada rabiti, a uporaba klasa mark i security, te razina warn, err i panic se više ni ne preporuča (ili su za internu uporabu, kao primjerice mark).

U /etc/syslog.conf se podešava u koje datoteke se poruke određene klasifikacije i razine upisuju, odnosno hoće li se i gdje zapisivati, jednostavno ignorirati, slati na druge syslog poslužitelje i slično. Primjerice, standardne postavke za Debian su:

```
mail.*                          -/var/log/mail/mail.log
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
user.*                          -/var/log/user.log
uucp.*                          /var/log/uucp.log
local4.*                        /var/log/local4.log
```

Možemo vidjeti da je oblik retka u konfiguracijskoj datoteci:

```
klasifikacija.razina     /var/log/datoteka
```

Umjesto klasifikacije ili razine možete staviti zvjezdicu. Zvjezdica obuhvaća sve moguće klasifikacije za određenu razinu, i obrnuto.

Preko primjera je najlakše objasniti kako to sve funkcionira:

```
mail.*                          -/var/log/mail/mail.log
```

Ovim konfiguracijskim retkom smo odredili da se sve poruke klase "mail" upisuju u datoteku /var/log/mail/mail.log, bez synca. Ukoliko imate prometan mail poslužitelj, možete razbiti ovaj log na više manjih:

```
mail.info                       -/var/log/mail/mail.info
mail.warn                       -/var/log/mail/mail.warn
mail.err                        /var/log/mail/mail.err
```

Na ovaj način možete brže doći do željenih informacija, ali u uobičajenom radu CARNetovih poslužitelja najčešće nije potrebno ovo raditi.

Razine u syslogu su hijerarhijske, dakle na najnižoj razini je "debug", a na najvišoj "emerg". Dakle redak

```
mail.err                        /var/log/mail/mail.err
```

zapravo znači "upiši sve razine od err i više: err, crit, alert i emerg"

Postoje još neke dodatne oznake. Crtica na početku imena datoteke se rabi kad ne želimo raditi sinkronizaciju datoteke sa stanjem na disku svakim upisom u nju (ne želimo raditi "sync", više informacija o ovome možete dobiti sa man syslog.conf).

```
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages
```

Oznaka "=" označava da želimo filtrirati baš tu razinu, dakle ne i razine iznad navedene, dakle "=info" će zapisati samo poruke na toj razini. Ovdje se može dodati još i negacijski modifikator "!". Vjerojatno pogađate što će se dogoditi: bit će upisane sve razine osim navedene.

Dakle, "mail.!=warn" će upisati sve razine osim razine "mail.warn".

Ukoliko niste sigurni u koju datoteku neki servis zapisuje logove, pogledajte sljedeći redak:

```
*.*;auth,authpriv.none          -/var/log/syslog
```

Oznaka "*.*" znači da se sve klase i razine zapisuju i u datoteku /var/log/syslog, pa prvo pogledajte tamo. Ako ipak želite posebnu datoteku, nađite u manualu vašeg servisa (npr. tcpd/tcp_wrappers) koju klasu rabi, te upišite u /etc/syslog:

```
klasa.*         -/var/log/tcpd.log
```

Još bolje, tcpd podržava promjenu klase i razine, pa možete rabiti "local0" do "local7" klase kako se logovi ne bi miješali (default je klasa "auth", pa će biti upisivani i drugi događaji u toj klasi). Primjerice, ako u /etc/hosts.allow imate:

```
sshd: .hr .si .ba .at .it .de: severity local7.notice: ALLOW
```

a u /etc/syslog.conf:

```
local7.notice         -/var/log/tcpd.log
```

onda će sve iz klase "local7.notice" biti zapisano u datoteku tcpd.log.

Ne zaboravite restartati syslog kako bi promjene bile pročitane.

Kako poslužitelji rade 24 sata dnevno, log datoteke mogu postati jako velike. Kako administrator ne bi morao ručno brisati, odnosno skraćivati log datoteke, obično se rabi alat logrotate.

Logrotate se može konfigurirati tako da rotira, odnosno sažima stare i kreira nove, prazne log datoteke. Također se može konfigurirati tako da čuva stare logove samo određeno vrijeme, rotira logove samo određene veličine i slično. Na taj način disk na poslužitelju nikada neće biti zapunjen starim logovima.

Logrotate smo detaljnije opisali u članku: Logrotate - zaboravljeni junak [1]

Syslog može još dosta toga, no o tome drugi put.

- Logirajte [2] se za dodavanje komentara

pet, 2010-07-02 15:24 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/759

Links
[1] https://sysportal.carnet.hr/node/638
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28