Systemd.journald i njegovi binarni logovi

 Unixoidi su dosad logove (dnevničke zapise) zapisivali kao običan tekst, a iskusni sistemci naučili su ih "grepati" kako bi iz njih filtrirali informacije koje ih zanimaju. No Lennart Poettering odlučio je to promijeniti, pa tako systemd zapisuje binarne logove. To je naravno izazvalo rasprave, čak je Linus Thorvalds bio protivan. Znamo da njega nije teško naljutiti. :) No Lennar bez uvijanja objašnjava što ga je navelo da promijeni uhodanu praksu.

Evo njegovih prigovora dosadašnjem načinu zapisivanja dnevnika.

- Poruke koje se zapisuju u logove u čovjeku razumljivom obliku nemaju propisan standard i programeri mogu u novim verzijama softvera unositi izmjene. Programi za analizu logova koriste pravilne izraze koje treba stalno prilagođavati. Lennart to naziva "regex horror".
- Iako je na prvi pogled lako čitati logove, ipak je teško uspostavljati korelaciju među različitim zapisima.
- Syslog ne zapisuje informacije o zbivanjima u ranoj fazi podizanja niti pri kraju spuštanja OS-a.

Tu su i brojni sigurnosni problemi:

- Bilo koji proces može tvrditi da ja Apache server i syslog će zapisivati njegove poruke bez provjere
- Napadač može s lakoćom mijenjati sadržaj logova i prikrivati tragove
- Kontrola pristupa je po principu sve ili ništa, znači da korisnik ili ne vidi logove ili ima sva prava nad njima
- Vremenski zapis ne uključuje podatak o vremenskim zonama
- Syslogov mrežni protokol je vrlo elementaran i ograničen, šalje pakete bez provjere da li su uredno spremljeni na ciljnom računalu
- Rotacija i kompresija starih logova postoje, ali bez provjere zauzeća diska, tako da DoS napad može izazvati zapunjavanje particije.
- Ne postoji "rate limiting", odbacivanje zapisa u slučaju preopterećenja sustava

Mora se priznati, sve su to valjani argumenti. Sistemci starog kova doduše rado koriste posebnu particiju za logove, kako u slučaju napada zapunjavanje te particije ne bi ugrozilo root particiju i rad OS-a. Pogledajmo kako je te probleme riješio Lennart, odnosno njegov systemd.

Proces koji je po novom zadužen za logiranje zove se **systemd.journald**. Admin može u

konfiguraciji odlučiti da li će logove čuvati trajno, ili privremeno u radnoj memoriji, a može i posve isključiti logiranje. Ako želi logove u RAM-u, dateteka će biti smještena u /run/log/journal direktoriju. Trajni zapis smješta se u /var/log/journal. Razlika je u tome što je /var na tvrdom disku, a /run u ramdisku. U /run particiju, koja je tipa privremenog datotečnog sustava (tmpfs) smještaju se podaci trenutno potrebni za rad sustava, ali ih ne treba čuvati da bi bili dostupni nakon restarta.

Sa system daemonom više nema potrebe za dodatnim procesom koji se bavi rotiranjem logova, jer journald cijelo vrijeme vodi računa o zauzeću diska i čisti stare zapise.

Konfiguracija journal daemona nalazi se u datoteci j**ournald.conf**, a njena lokacija varira. Ubuntu je smješta u /etc/systemd/journald.conf, ali može biti u /run/systemd/ ili /usr/lib/systemd. Osim toga, neki paketi mogu instalirati svoje konfiguracije u poddirektorije, na primjer u /etc/systemd/journald.conf.d/.

U isporučenom journald.conf konfiguracijske varijable su redom zakomentirane, što bi značilo da su aktivne defaultne vrijednosti. Na nama je da unesemo promjene ako nam se nešto ne sviđa.

Na početku piše ovo:

```
[Journal]
#Storage=auto
```

Storage može imati četiri vrijednosti:

- “none” isključuje logiranje
- “volatile” sprema log u memoriju gdje je dostupan do gašenja računala
- “persistent” šalje log na tvrdi disk u /var/log/journal
- "auto" je načelno kao persistent, ali samo ako postoji direktorij /var/log/journal; u protivnom zapis ide u RAM, odnosno /run/systemd.

Na prvi je pogled zadnja vrijednost, "auto", posve nepotrebna jer ne donosi ništa što bi prethodne propustile. Zapisivanje na tvrdi disk ovisi o tome da li je kreiran direktorij /var/log/journal, što lako promakne pažnji, pa se može dogoditi da admin i ne zna gdje mu idu logovi, sve dok ih ne krene tražiti.

Naredna varijabla određuje da li komprimirati starije zapise. Podrazumijeva se da je kompresija uključena.

```
#Compress=yes
```

Tu su i dvije grupe varijabli koje služe ograničavanju veličine zapisa, da se ne bi zagušila particija. Prva grupa se bavi ograničenjem prostora, a podijelili smo ih u stupce zavisno od toga da li se odnose na zapis u RAM-u (volatile) i na tvrdom disku (persistent).

Volatile	**Persistent**	
RuntimeKeepFree	SystemKeepFree	Određuje koliko prostora log mora ostaviti drugim aplikacijam, default 15%
RuntimeMaxUse	SystemMaxuse	Maksimalna veličina žurnala,

		default 10%
RuntimeMaxFileSize	SystemMaxFileSize	Najveća veličina datoteke, default je 1/8 od MaxUse.

Ime varijable je slično u oba slučaja, razlika je u prefiksu. Ako počinje s Runtime, odnosi se na zapis u RAM-u, a System označava trajni zapis na disku.

Druga grupa bavi se ograničenjem vremena čuvanja zapisa.

MaxRetentionSec	Maksimalno vrijeme čuvanja zapisa. Podrazumijevana vrijednost je 0.
MaxFileSec	Dok se prethodna varijabla odnosi na žurnale u cjelini, ova se bavi pojedinačnin datotekama

Journald može slati poruke na razne strane, na primjer syslogu, što je zgodno ako na primjer imate jedan server koji prikuplja logove svih drugih servera. Nazivi postavki govore dovoljno, ne treba im objašnjenje:

ForwardToSyslog

ForwardToWall

ForwardToKMsg

ForwardToConsole

Naredne postavke određuju koja će se vrsta zapisa bilježiti, da li samo kritične greške ili sve odreda, ili nešto između.

MaxLevelStore	0 ili “emerg” 1 ili “alert” 2 ili “crit” 3 ili “err” 4 ili “warning” 5 ili “notice” 6 ili “info” 7 ili “debug”

Kako se poruke mogu usmjeravati na razne strane, predviđene su postavke za svako odredište zasebno:

MaxLevelSyslog

MaxLevelKMsg

MaxLevelConsole

MaxLevelWall

Na primjer, na konzoli vjerojatno želite gledati samo kritične greške.

Toliko o zadavanju postavki i konfiguriranju journal daemona. U narednom nastavku naučit ćemo kako pretraživati binarne logove.

uto, 2017-10-31 12:02 - Aco Dmitrović**Vote:** 0

No votes yet

story_tag: Linux [1]
systemd [2]
journald [3]

Source URL: https://sysportal.carnet.hr/node/1770

Links
[1] https://sysportal.carnet.hr/taxonomy/term/119
[2] https://sysportal.carnet.hr/taxonomy/term/120
[3] https://sysportal.carnet.hr/taxonomy/term/158