Naredba fuser


Naredbom *fuser* izlistamo procese koji drže neku datoteku ili uređaj otvorenim, što može spriječiti odmontiranje uređaja (diska, na primjer) ili reboot servera. Naredba *fuser* će nam pokazati koji proces drži datoteku otvorenom, pa možemo ugasiti proces i nastaviti s planiranom akcijom. *fuser* je vrlo sličan naredbi *lsof*, no o njoj se već dosta pisalo na Portalu pa ćemo se pozabaviti samo naredbom *fuser*.

Ne moramo provjeravati da li su log datoteke u /var/log otvorene, jer su sasvim sigurno otvorene za pisanje (ukoliko nisu, imamo problem i fuser nam je već na taj način pomogao), no primjera radi:

```
server# fuser /var/log/*
/var/log/auth.log:   12278
/var/log/daemon.log:  9397 12278
/var/log/debug:      12278
/var/log/fail2ban.log:  1447
/var/log/kern.log:   12278
/var/log/mail.log:   12278
/var/log/messages:   12278
/var/log/syslog:      9396 12278
```

Vidimo koje su sve datoteke otvorene i brojeve procesa koji iz drže otvorenima. Pogledajmo koji se procesi skrivaju pod ovim brojevima:

```
server# ps -p 12278 9396 9397 1447 23097
  PID TTY      STAT   TIME COMMAND
 1447 ?        Sl   25557:28 /usr/bin/f2b-
server -b -s /v/r/f2b/f2b.sock -p /v/r/f2b/f2b.pid
 9396 pts/3    S      0:00 tail --follow=name -n 100 /var/log/syslog
 9397 pts/3    S      0:00 tail --follow=name -n 50 /var/log/daemon.log
12278 ?        Ssl   10:55 /usr/sbin/rsyslogd -n
```

Iznenađenja nema, jer *rsyslogd* drži gotovo sve log datoteke otvorenima. *Fail2ban* drži svoju log datoteku otvorenom, a ostali procesi su ručno otvorene log datoteke kako bi se na oku držale sumnjive aktivnosti.

```
server# fuser /home/*
/home/korisnik:        32744c
```

Ukoliko želimo saznati koji je to točno proces, ne moramo koristiti naredbu "ps", brže će biti:

```
server# fuser -v /home/*
                     USER          PID ACCESS COMMAND
/home/korisnik:      korisnik    32744 ..c.. sh
```

Ukoliko ste primjetili slovo "c" koje se pojavljuje pod "ACCESS" i na kraju kratke verzije naredbe, u

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

manualu je pojašnjeno da se radi o trenutnom radnom direktoriju procesa fuser. Postoje još neke oznake:

c current directory.
e executable being run.
f open file. f is omitted in default display mode.
F open file for writing. F is omitted in default display mode.
r root directory.
m mmap'ed file or shared library.

Oznaka "r" označava da se radi o root direktoriju, dakle svi će "sistemski" procesi (apache, postfix itd) imati ovu oznaku. nama ova činjenica i ne znači nešto, barem ne u uobičajenoj upotrebi.

Objasnit ćemo ostale oznake primjerom....

Naredbom *fuser* možete ubiti procese "koji smetaju". Ovu funkcionalnost *lsof* nema, pa iako *fuser* nema mogućnosti *lsofa*, ovako nešto može biti presudno kod odluke koju ćete naredbu koristiti.

```
server# fuser -v -k -i /home/korisnik/datoteka.txt
                     USER           PID ACCESS COMMAND
/home/korisnik/datoteka.txt:
                     korisnik    17340 f.... less
Kill process 17340 ? (y/N) y
```

Ova naredba gore može se jednostavno prevesti "pronađi koji proces drži datoteku otvorenom i ubij ga (uz upit)". Kod pokretanja smo stavili opciju "-i", koja znači isto kao i kod naredbe "rm" i sličnih: "interactive", dakle uz potvrdu korisnika.

Možda ste primjetili da je sada "ACCESS" postavljen na "f", što označava datoteku otvorenu za čitanje. Pogledajmo kako to izgleda kada je datoteka otvorena za pisanje:

```
                     USER           PID ACCESS COMMAND
/home/korisnik/datoteka.txt:
                     korisnik    17394 F.... cat
```

Sada je oznaka postala "F", što označava datoteku otvorenu za pisanje.

Inače, u drugom prozoru smo u datoteku pisali jednostavnom naredom "cat":

```
server$ cat > datoteka.txt
Neki tekst
Killed
```

Poruka "Killed" pojavila se u drugom prozoru kada smo potvrdili ubiijanje procesa u originalnom prozoru, odnosno shellu.

Fuser može detektirati "mrežne" procese, odnosno procese koji drže otvoren neki mrežni *socket*. Moramo koristiti opciju "-n", a sintaksa je sljedeća:

```
server# fuser -v -n tcp 20000
                     USER           PID ACCESS COMMAND
20000/tcp:           korisnik     17718 F.... nc
```

Na portu 20000 smo pokrenuli testni daemon i fuser ga je pronašao. Na isti način ubijamo i taj proces:

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

```
server# fuser -v -k -n tcp 20000
                     USER           PID ACCESS COMMAND
20000/tcp:           korisnik     17718 F.... nc
```

Potvrde da je proces zaustavljen nema, osim ovog ponovljenog ispisa, ali se u drugom prozoru pojavljuje "Killed", baš kao i u prethodnom slučaju. Naravno, sada više ništa ne sluša na portu 20000, što je defitivna potvrda ako nemate pristup drugom shellu gdje bi mogli imati vizualnu potvrdu.

Što se tiče mrežnog dijela naredbe *fuser*, ukoliko želite koristiti UDP protokol, morate to navesti s "-n udp". Opcija "-n" se može izraziti i ovako:

```
server# fuser -v -k 20000/tcp
```

Ovaj potonji način se čini praktičnijim, a ime porta možete napisati slovima, ako je naveden u datoteci /etc/services (fuser -k http/tcp, ftp/tcp i slično).

Zadnja opcija koja će nam zatrebati je "-m". Ona uključuje prikaz svih procesa koji drže neku datoteku otvorenu na cijelom montiranom filesystemu, dakle ne samo jednu određenu datoteku:

```
server# fuser -v -m /home
                     USER        PID ACCESS COMMAND
/home:
                     root        kernel mount /home
                     korisnik       470 ..c.. bash
                     korisnik      4343 ..c.. screen
                     root          4455 ..c.. bash
                     root          4462 ..c.. sudo
                     korisnik      5447 ..c.. ssh
                     korisnik      7168 ..c.. bash
                     root          9395 ..c.. multitail
                     root          9396 ..c.. tail
                     root          9397 ..c.. tail
                     korisnik     16458 ..c.. ssh
                     korisnik     17231 ..c.. bash
                     korisnik     28939 ..c.. screen
                     korisnik     32728 ..c.. ssh
```

Ova je opcija najkorisnija kada na brzinu želite odmontirati uređaj i ne zanima vas previše ili jednostavno nemate vremena za analizu može li se proces ubiti ili ne.

Kad smo već kod toga, *fuser* procesima šalje signal -9 (SIGKILL), koji odmah ubija proces, ne dajući mu šansu da se sam ugasi i zatvori otvorene datoteke i buffere. No, *fuser* može poslati i drugi signal:

```
server# fuser -v -k -15 20000/tcp
server# fuser -v -k -TERM 20000/tcp
```

Ovaj način šalje "blaži" signal SIGTERM, a tako se može poslati bilo koji signal. Popis svih podržanim sigbnala možete dobit s opcijom -l:

```
server# fuser -l
HUP INT QUIT ILL TRAP ABRT IOT BUS FPE KILL USR1 SEGV USR2 PIPE ALRM TERM
STKFLT CHLD CONT STOP TSTP TTIN TTOU URG XCPU XFSZ VTALRM PROF WINCH IO PWR
SYS UNUSED
```


Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Koji ćete odabrati od ovih ovisi o aplikaciji, ali vjerojatno će dostajati SIGTERM (inače ovaj signal šalje naredba kill po defaultu), a ako ne pomogne SIGKILL (čuvena devetka).

Kao zaključak, možemo navesti da *fuser* obavlja svoj posao kako treba, brži je za ubijanje nepoželjnih procesa od *lsof*a, ali ima manje mogućnosti. Rekli bismo, ima ih taman dovoljno da bude u svačijem arsenalu administratorskih alata.

pet, 2016-12-30 01:41 - Zdravko Rašić**Vijesti:** Linux [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1717

Links
[1] https://sysportal.carnet.hr/taxonomy/term/11

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr