# Księgowanie procesów w systemie GNU/Linux

Grzegorz Jacek Nalepa

20.03.2001, Kraków, *Revision* : 1.2

**Streszczenie**

Artykuł opisuje mechanizm księgowania procesów (ang. *process accounting*) dostępny w systemie GNU/Linux. Przedstawiona jest współpraca jądra systemu z programami działającymi w przestrzenie użytkownika. Pokazane jest wykorzystanie narzędzi z pakietu *GNU Accounting utilities* do monitorowania pracy użytkowników systemu. Poruszone są również problemy zarządzania plikami rejestrowymi związanymi z księgowaniem procesów.

## Spis treści



[1]Tekst ukazał się w: *Magazynie TeleNetforum*, nr 4/2001, wydawanym przez Lupus.

[2]Kontakt z autorem: mail:gjn@agh.edu.pl

[3]Tytuł angielski: *Process Acounting in GNU/Linux system*

[4]Tekst jest rozpowszechniany na zasadach licencji *GNU Free Documentation License*, której pełny tekst można znaleźć pod adresem: http://www.gnu.org/copyleft/fdl.html

# 1. Wstęp

Księgowanie procesów i sesji użytkowników jest jednym z podstawowych mechanizmów w systemie GNU/Linux, umożliwiającym szczegółowe monitorowanie pracy systemu i wykorzystania udostępnianych zasobów.

W systemie GNU/Linux administrator ma wiele możliwości monitorowania jego pracy. Jednym z najczęściej wykorzystywanych jest system Syslog pozwalający na śledzenie pracy programów, szczególnie procesów systemowych. Syslog pozwala na gromadzenie informacji wysyłanych przez programy z wykorzystaniem mechanizmów dostarczanych przez bibliotekę standardową. Nie jest jednak w stanie gromadzić informacji, które nie są wysyłane przez pracujące procesy, takich jak informacje o samym tworzeniu czy usuwaniu procesu, a także wykorzystaniu przez niego zasobów. Zbieranie tego typu informacji umożliwia księgowanie procesów.

Oprócz informacji na temat procesów użytkowników system gromadzi szczegółowe informacje dotyczące ich pracy w systemie dzięki mechanizmowi księgowania sesji pracy.

# 2. Czym jest księgowanie procesów

Księgowanie procesów (ang. *process accounting*) jest systemowym mechanizmem pozwalających na gromadzenie informacji na temat procesów pracujących w systemie. Mechanizm księgowania procesów wywodzi się z BSD Unixa.

Księgowanie procesów jest realizowane na poziomie jądra systemu. Jądro systemu Linux gromadzi informacje między innymi o:

- nazwie procesu
- właścicielu i grupie procesu
- czasie jego stworzenia i usunięcia
- zużytym czasie systemowym w przestrzeni użytkownika i jądra
- zużyciu pamięci przez proces
- ilości przetransferowanych danych wejściowych i wyjściowych

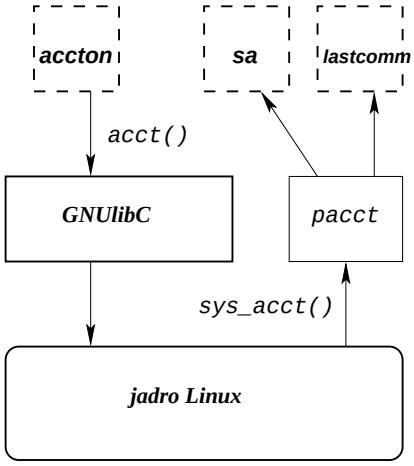
Dane gromadzone przez jądro są wysyłane do określonego pliku. Nazwa tego pliku jest przekazywana do jądra w trakcie inicjalizacji księgowania. Zgromadzone dane mogą być następnie przetwarzane przez dodatkowe programy.

# 3. Realizacja księgowania procesów

Na Rysunku 1 jest pokazana realizacja księgowania procesów w systemie GNU/Linux.

Inicjalizacja księgowania jest realizowana przez program `accton`, wywołujący funkcję systemową *acct() (2)* z biblioteki standardowej. Program przekazuje funkcji nazwę pliku w którym jądro ma gromadzić dane o procesach. W systemie GNU/Linux jest to najczęściej `/var/account/pacct`, lub `/var/log/acct`. Deklaracja funkcji *acct() (2)* znajduje się w systemowym pliku nagłówkowym `<unistd.h>`.

Na poziomie jądra systemu Linux obsługą księgowania procesów zajmuje się funkcja *sys_acct()*, której kod znajduje się w pliku `/usr/src/linux/kernel/acct.c`. Wykorzystuje ona strukturę danych opisującą rekord księgowania, zadeklarowaną w pliku `<linux/acct.h>`.




Rysunek 1: Realizacja księgowania procesów

Dane na temat procesów są gromadzone przez jądro systemu w postaci binarnej. Ich dalsza obróbka, w szczególności sporządzanie statystyk jest realizowane przez oddzielne narzędzia uruchamiane przez administratora systemu.

# 4. Czym jest księgowanie sesji pracy

Księgowanie sesji pracy (ang. *login accounting*) jest mechanizmem uzupełniającym księgowanie procesów. Jest realizowane głównie w przestrzeni użytkownika, przez procesy systemowe takie jak *init* czy *login* a także inne związane z zarządzaniem sesjami pracy.

Mechanizm księgowania sesji pozwala między innymi na gromadzenie informacji o:

- nazwie użytkownika
- czasie zamknięcia i otwarcia sesji
- typie sesji
- nazwie i adresie maszyny z której była otwarta sesja

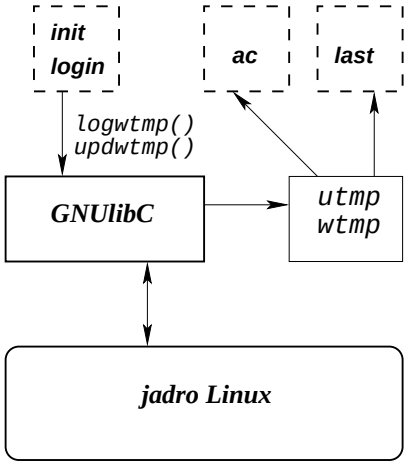
Dane o sesjach użytkownikach są gromadzone w dwóch plikach. Pierwszy z nich `utmp` zawiera informacje o aktualnie otwartych sesjach. Drugi, `wtmp` przechowuje informacje o sesjach, które zostały już zamknięte. Plik `utmp` znajduje się najczęściej w katalogu `/var/run`, a plik `wtmp` w `/var/log`.

# 5. Realizacja księgowania sesji

Realizacja mechanizmu księgowania sesji pracy w systemie GNU/Linux jest podobna jak w innych systemach uniksowych i opiera się głównie na funkcjach z biblioteki systemowej. Jest ona pokazana na Rysunku 2.

Księgowanie sesji jest realizowane poprzez kilka funkcji z biblioteki systemowej, takich jak *logwtmp() (2)* czy *updwtmp() (2)*, zadeklarowanych w pliku `<utmp.h>`. Funkcje używają struktury `utmp` opisującej rekord w bazie księgowanych sesji.

Obydwie funkcje są wywoływane przez wszystkie procesy związane z zarządzaniem sesją pracy użytkowników. Należą do nich przede wszystkim *init* i *login*.




Rysunek 2: Realizacja księgowania sesji

Informacje o księgowanych sesjach są przechowywane w plikach `utmp` i `wtmp` w postaci binarnej. Te pliki są poddawane dalszej obróbce przez dodatkowe programy uruchamiane przez administratora lub użytkowników systemu.

# 6. GNU Accounting Utilities

Programy wspomagające inicjalizację księgowania procesów i obróbkę danych gromadzonych przez system znajdują się w pakiecie *GNU Accounting Utilities*. Pakiet składa się z 7 programów, realizujących:

**ac** wyświetlanie statystyk na temat sesji użytkowników

**accton** inicjalizację księgowania procesów

**last** pokazywanie listy ostatnich sesji pracy użytkowników

**lastcomm** pokazywanie listy ostatnio uruchamianych procesów

**sa** generowanie statystyk dotyczących zużycia zasobów systemu przez polecenia uruchamiane przez konkretnych użytkowników

**dump-acct** bezpośrednie wyświetlanie zawartości pliku `acct` w postaci tekstowej

**dump-utmp** bezpośrednie wyświetlanie zawartości pliku `utmp` w postaci tekstowej

W celu uruchomienia księgowania procesów w systemie należy założyć plik `acct`, na przykład przy pomocy polecenia:

```
# touch /var/account/pacct
```

Podczas startu systemu powinno być uruchamianie polecenie *accton*:

```
if [ -x /sbin/accton ]
then
   /sbin/accton /var/log/pacct
   echo "Process accounting turned on."
fi
```

Informacje na temat procesów można wyświetlać przy pomocy programu `lastcomm`:

```
# lastcomm
lastcomm         X root     stderr     0.68 secs Mon Mar 19 23:47
mesg          S     root     stderr     0.01 secs Mon Mar 19 23:47
bash           F    root     stderr     0.01 secs Mon Mar 19 23:47
receive             root     stderr     0.01 secs Mon Mar 19 23:47
sh                  gjn      ??         0.02 secs Mon Mar 19 23:30
gzip                gjn      ??         0.01 secs Mon Mar 19 23:30
man                 gjn      ??         0.02 secs Mon Mar 19 23:23
pager               gjn      ??         0.07 secs Mon Mar 19 23:23
```

Widoczne powyżej flagi oznaczają kolejno: F – proces uruchomiony w wyniku funkcji *fork()*, S – proces uruchomiony przez administratora, X – proces zakończony sygnałem SIGTERM, D – proces zakończył się stworzeniem pliku `core`.

Możliwe jest również wyświetlanie poleceń wykonywanych przez podanego użytkownika, a także zadawanie wzorców wybierających z listy odpowiednie procesy.

Polecenie `sa` pozwala na sporządzenie sumarycznych raportów na temat uruchamianych procesów. Wywołane bez parametrów wyświetla posortowaną listę procesów i ilość wykorzystanych przez nie zasobów:

```
# sa
   81     792.12re    2.53cp      0avio   1564k   latex
   57   14837.17re    1.72cp      0avio   1329k   gs
    2  127061.33re    0.87cp      0avio    671k   mc
   12  300253.58re    0.54cp      0avio    787k   xterm
    9      98.55re    0.50cp      0avio   2176k   pdflatex
    4   74865.12re    0.29cp      0avio    600k   mutt
```

Możliwe jest również wyświetlanie stopnia zużycia zasobów przez konkretnych użytkowników:

```
# sa -m
8828 2428609.07re      31.87cp         0avio       460k gjn
1976 1495168.85re      19.26cp         0avio       530k root
6851  933440.15re      12.61cp         0avio       440k rwhod
```

Polecenie `ac` pozwala na wygenerowanie statystyk dotyczących czasu pracy poszczególnych użytkowników w systemie, na przykład forma:

```
# ac -dp
Mar 15  total   0.27
        gjn            23.89
        root            0.02
```

spowoduje wyświetlenie codziennego, sumarycznego czasu pracy użytkowników w systemie

Natomiast polecenie `last` umożliwia wyświetlenie listy ostatnio otwartych sesji użytkowników. Podane bez argumentów pokazuje informacje na temat sesji wszystkich użytkowników, uruchomione z nazwą konkretnego użytkownika podaje informacje, które dotyczą tylko niego.

```
gjn      :0           console          Tue Mar 20 20:51   still logged in
reboot   system boot  2.4.1            Tue Mar 20 20:50          (01:15)
gjn      pts/2        :0.0             Mon Mar 19 20:44 - 00:35  (03:51)
```

Jak widać zaznaczane są również czasy uruchomienia systemu.

Z mechanizmu księgowania sesji użytkowników korzystają również standardowe polecenia wyświetlające informacje na temat pracujących użytkowników, takie jak `w`, `who` czy `finger`.

# 7. Archiwizacja plików rejestrowych

Księgowanie procesów ma dość istotny skutek uboczny, a mianowicie tworzenie plików rejestrowych o bardzo dużej objętości. Nawet w systemie w którym pracuje kilku użytkowników pliki rejestrowe mogą osiągnąć wielkości rzędu megabajtów.

W związku z tym niezwykle istotne staje się kontrolowanie ich wielkości. Najlepiej nadają się do tego systemowe mechanizmy rotacji plików rejestrowych, takie jak demon *logrotate* i system *Cron*.

Aby zapobiec przepełnieniu systemu plików przez pliki rejestrowe związane z księgowaniem procesów mechanizm księgowania w jądrze systemu Linux może sprawdzać ilość wolnego miejsca w systemie plików. Ta procedura może być konfigurowana przez system `/proc`.

```
$ cat /proc/sys/kernel/acct
4       2       30
```

Środkowa liczba oznacza procent wolnego miejsca w systemie plików, poniżej którego księgowanie zostanie wstrzymane. Jeżeli ilość wolnego miejsca wzrośnie powyżej ilości określonej pierwszą liczbą księgowanie jest wznawiane. Ostatnia liczba oznacza częstość sprawdzania wolnego miejsca mierzoną w sekundach. Domyślne wartości to `4 2 30`, co oznacza, że jeżeli ilość wolnego miejsca spadnie poniżej 2 procent księgowanie zostanie zatrzymane, jeżeli wróci do poziomu 5 procent zostanie wznowione, a ilość wolnego miejsca będzie sprawdzana co 30 sekund.

# 8. Podsumowanie

Księgowanie procesów i sesji jest ważnym mechanizmem pozwalającym monitorować pracę użytkowników w systemie GNU/Linux. Jest łatwo konfigurowalne, a dostarczane narzędzia pozwalają na obróbkę zbieranych przez nie informacji. Mechanizm księgowania połączony z możliwościami systemu PAM (szczególnie modułu *limits*) umożliwia precyzyjne mierzenie i ograniczanie zasobów zużywanych przez użytkowników i ich procesy. Jakkolwiek nie jest to mechanizm przydatny dla wszystkich serwerów, to administratorzy pragnący dokładnie znać wykorzystanie zasobów ich systemów uznają go za bardzo przydatny.

# Literatura

[1] Noel Cragg, *GNU Accounting Utilities*, Version 6.3.5, 26 May 1998.

[2] Albert M.C. Tam, *Process Accounting HOWTO*, LDP, 2001-02-09.

[3] Rik van Riel, *Documentation for /proc/sys/kernel*, 1998, 1999.