

**Jacek WOŁOSZYN**

Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego  
w Radomiu, Polska

## **Monitorowanie logów systemowych z wykorzystaniem programu Logcheck**

### **Wstęp**

Klasyczny użytkownik systemów komputerowych zaczyna się interesować logami systemowymi przeważnie w sytuacji, kiedy pojawiają się błędy systemowe lub niestabilność pracy systemu czy usługi [Chirillo 2002b]. Inaczej wygląda sprawa w przypadku administratorów systemów. Zazwyczaj powinni oni na bieżąco śledzić pracę systemu [Rash 2008] i reagować na zachodzące sytuacje. Jednak codzienna duża ilość obowiązków i spraw, szczególnie tych niezaplanowanych i przypadkowych, nie pozwalają na rzetelne śledzenie wpisów w logach i monitorowanie systemu [Chirillo 2002a]. A właśnie nieustanne, rutynowe śledzenie i reagowanie na pojawiające się sytuacje pozwoli na uniknięcie wielu nieoczekiwanych sytuacji. Na maszynie serwerowej przeglądanie logów powinno następować bez przerwy. Korzystanie ze standardowych przeglądarek jest bardzo nużące i mało skuteczne. W wielkiej ilości wpisów łatwo jest przeoczyć ważne informacje.

Dlatego warto skorzystać z oprogramowania Logcheck, które odpowiednio skonfigurowane samo kontroluje i analizuje wpisy otrzymane z demona `rsyslog` w `/var/log/messages` i przesyła użytkownikowi root list z informacją o podejrzanym wpisach celem ich wyjaśnienia.

### **1. Instalacja i konfiguracja Logcheck**

Zakładając, że zostało już wcześniej skonfigurowane repozytorium z paczkami debiana, bo akurat na tym systemie przeprowadzana jest instalacja, należy wydać polecenie `apt-get install logcheck`.

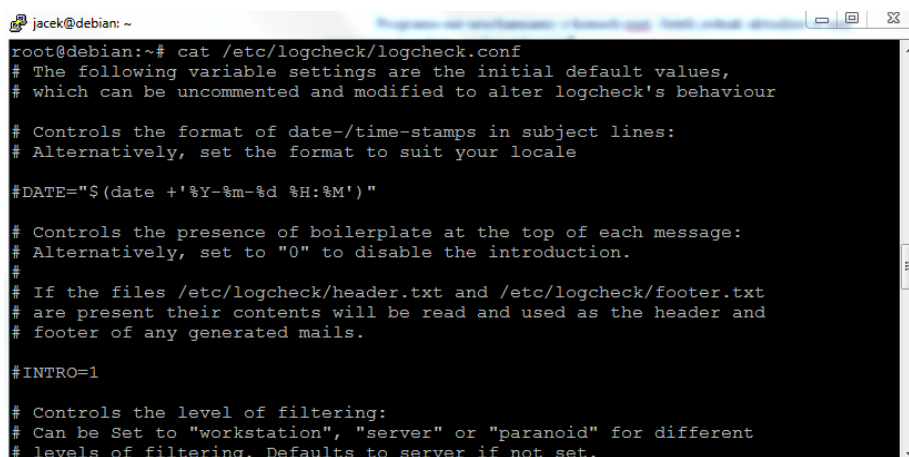
Programu nie należy uruchamiać z konsoli roota, jeśli jednak aktualnie w niej odbywa się praca, to należy wydać polecenie:

```
su -s /bin/bash -c '/usr/sbin/logcheck' logcheck  
lub  
sudo-u logcheck logcheck.
```

Aby zdefiniować, które pliki mają podlegać monitoringowi w pliku konfiguracyjnym `/etc/logcheck/logcheck.logfiles`, należy wypisać ich nazwy.

Domyślnie znajdują się tam tylko `syslog` i `auth.log`, warto dodać logi kluczowych usług, jeśli nie piszą do `syslog`a, a do własnych logów. Np. aby monitorować także logi `nginx`, należy dopisać `/var/log/nginx/error.log`. Podobnie można dopisać logi bazy danych czy jakiegos serwera aplikacji.

Logcheck obsługuje wyłącznie wierszowe logi (tj. takie, w których każda informacja jest zapisana w pojedynczym wierszu).



```
jacek@debian: ~  
root@debian:~# cat /etc/logcheck/logcheck.conf  
# The following variable settings are the initial default values,  
# which can be uncommented and modified to alter logcheck's behaviour  
  
# Controls the format of date-/time-stamps in subject lines:  
# Alternatively, set the format to suit your locale  
  
#DATE="$ (date +%Y-%m-%d %H:%M) "  
  
# Controls the presence of boilerplate at the top of each message:  
# Alternatively, set to "0" to disable the introduction.  
#  
# If the files /etc/logcheck/header.txt and /etc/logcheck/footer.txt  
# are present their contents will be read and used as the header and  
# footer of any generated mails.  
  
#INTRO=1  
  
# Controls the level of filtering:  
# Can be Set to "workstation", "server" or "paranoid" for different  
# levels of filtering. Defaults to server if not set.
```

**Rys. 1. Fragment pliku konfiguracyjnego `logcheck.conf`**

*Źródło:* opracowanie własne.

Logchecka można skonfigurować do pracy w jednym z trzech trybów: `paranoid`, `server` i `workstation`. W zależności od użytej konfiguracji program będzie się wykazywał dużą lub umiarkowaną „gadatliwością”.

„Paranoid” „duża gadatliwość” oznacza, że zastosowany został tylko minimalny zestaw filtrów w `ignore.d.paranoid`. Należy je stosować w urządzeniach o wysokim poziomie bezpieczeństwa, takich jak zapory ogniowe.

„Server” oznacza, że ustawiony został środkowy zestaw filtrów, czyli taki który w większości przypadków reaguje na standardowe usługi. Logcheck wykorzystuje zestaw filtrów `ignore.d.server`, jak nazwa wskazuje, jest to przeznaczone do wycięcia rutynowych wpisów.

„Workstation” – w tym najmniej restrykcyjnym filtrze ignorowane są zarówno reguły `paranoid`, jak i `server`.

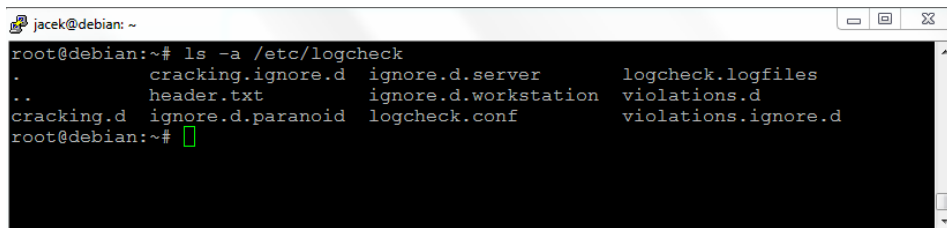
Poziom filtrowania wybiera jeden z zestawów reguł – odpowiednio: `/etc/logcheck/ignore.d.paranoid`,  
`/etc/logcheck/ignore.d.server`, albo  
`/etc/logcheck/ignore.d.workstation`. Są one po kolei łączone na poziomie `server`. Obowiązują zarówno reguły z katalogu `ignore.d.server`, jak

i z `ignore.d.paranoid`, a na poziomie `workstation` z wszystkich trzech katalogów.

`Ignore.d.server/postfix` zawiera wyrażenia regularne opisujące wpisy z logów postfixa, które nie wymagają alarmowania administratora, a `ignore.d.server/maradns` analogicznie traktuje wpisy MaraDNS. Przy czym i ten podział to tylko konwencja, `logcheck` zbiera reguły z wszystkich plików z odpowiedniego katalogu i analizuje pod ich względem każdy znaleziony wpis.

`Logcheck` uwzględnia pliki o nazwach złożonych z liter, cyfr, podkreśleń i myślników.

Szczególnie alarmowe wpisy definiują zaś reguły z katalogów `cracking.d` (maile Security Alert, sygnalizujące próby włamań) i `violations.d` (maile Security Event, sygnalizujące poważne zagrożenia).



```
jacek@debian: ~  
root@debian:~# ls -la /etc/logcheck  
.  
..  
cracking.d  
header.txt  
ignore.d  
logcheck.conf  
logcheck.logfiles  
ignore.d.server  
ignore.d.workstation  
violations.d  
violations.ignore.d  
root@debian:~#
```

**Rys. 2. Zawartość katalogu `/etc/logcheck`**

*Źródło: opracowanie własne.*

## Strojenie reguł

Konfigurując program, należy wyliczyć komunikaty, na które nie powinien reagować alarmem.

Po niedługiej działalności `logchecka`, można łatwo zauważyć, które wpisy można zignorować umieszczając je w plikach. Należy jednak w tym względzie zastosować złoty środek i dokładnie przemyśleć konfigurację. Albowiem jeżeli program zostanie skonfigurowany mało restrykcyjnie, to będzie zalewał administratora olbrzymią ilością informacji, w morzu której łatwo jest przeoczyć tę akurat ważną dla pracy systemu. Z kolei duże restrykcje mogą spowodować, że ważne informacje mogą do administratora nie dotrzeć.

Domyślne filtry są raczej ostrożne i wyłączają tylko najbardziej ewidentnie nieistotne wpisy, do tego czasem nie nadążają za zmianami w programach. Jeśli monitorowany log nietypowej aplikacji nie posiada reguł, wówczas rozwiązaniem jest uzupełnić reguły tak, by daną informację pomijały. Gdy list od `logchecka` zawiera zbędne wpisy, należy utworzyć nowy plik w `/etc/logcheck/ignore.d.server` i dodać w nim odpowiednie wyrażenie lub wyrażenia.

Nawet gdy reguła dotyczy programu, który już swoje reguły ma, lepiej jest założyć nowy plik, a nieuwzględnione standardowo ostrzeżenia postfixa dotyczące weryfikacji certyfikatów dopisać w `ignore.d.server/postfix-my`

(nazwa pliku jest oczywiście przykładowa i użytkownik może ją sobie dowolnie zmieniać). Powód jest prosty: przy aktualizacjach dystrybucji standardowe pliki reguł bardzo często głęboko się zmieniają, prościej mieć swoje konfiguracje zapisane oddzielnie i zaakceptować upgrade, niż dokonywać każdorazowo zmiany.

Przykład: nginx wpisuje do logów informację o buforowaniu żądania i odpowiedzi. Nie jest to nic alarmującego, dlatego należy utworzyć sobie plik `ignore.d.server/nginx` o treści:

```
^[0-9]{4}/[0-9]{2}/[0-9]{2} [0-9:]{8} \[warn\] [0-9\#]+:
[0-9\*]+ an upstream response is buffered
^[0-9]{4}/[0-9]{2}/[0-9]{2} [0-9:]{8} \[warn\] [0-9\#]+:
[0-9\*]+ a client request body is buffered
```

W wyrażeniach obowiązuje syntaks egrep. Warto zwrócić uwagę na wiodący `^`. Podobnie ewentualny końcowy `$` nakazuje dopasować cały napis.

Ważne jest, że tworzony wpis zostanie uwzględniony przy pełnej analizie wszystkiego. Dlatego trzeba pisać dosyć rozbudowane, restrykcyjne wyrażenia, by przypadkowo nie wymaskować istotnych informacji innych programów.

Tą samą metodą można rozszerzyć listę alarmów, dodając nowe elementy w `cracking.d` lub `violations.d`.

### Testowanie reguł

Rzadko zdarza się napisać regexpa bez żadnej pomyłki, dlatego dopisaną regułę warto od razu przetestować.

Prosta metoda testowania:

```
$ sudo -u logcheck logcheck -tdo -l
/sciezka/testowanego/logu
```

Znaczenie podanych flag:

- t powoduje wyłączenie aktualizowania znacznika dokąd przejrano,
- o wypisanie wyników na standardowe wyjście zamiast wysyłania ich mail-em,
- d wyświetlenie informacji debugingowych.

## 2. Używanie Logcheck

Program można uruchomić wydając polecenie:

```
sudo-u logcheck logcheck -o-t
```

Opcje:

- C CFG Unieważnić domyślny plik konfiguracyjny.
- D Trybie debugowania.
- H Pokaż informacje o użytkowaniu.
- H Użyj tego hosta ciąg w przedmiocie Logcheck mail.

- L LOG Uruchom plik dziennika przez Logcheck.
- L CFG Unieważnić domyślny logów listę.
- M Raport mail odbiorcy.
- O Tryb STDOUT nie, wysyłanie poczty.
- P Ustawianie poziomu raportu do „paranoikiem”.
- DIR-r Unieważnić domyślne reguły katalogu.
- R Dodaje „Reboot:” w temacie wiadomości e-mail.
- S Ustawianie poziomu raportu do „serwer”.
- S DIR Unieważnić katalog domyślny stan.
- T Tryb testowania nie aktualizuje offset.
- T Nie wyjmuj tmpdir.
- U Włącz syslog-podsumowanie.
- V Wydrukuj bieżącą wersję.
- W Ustawianie poziomu raportu do „stacji roboczej”.

```

jacek@debian: ~
Message 1:
From logcheck@debian Mon May 20 11:54:06 2013
Envelope-to: logcheck@debian
Delivery-date: Mon, 20 May 2013 11:54:06 +0200
To: logcheck@debian
Subject: debian 2013-05-20 11:54 +0200 System Events
Auto-Submitted: auto-generated
MIME-Version: 1.0 (mime-construct 1.11)
From: logcheck system account <logcheck@debian>
Date: Mon, 20 May 2013 11:54:06 +0200

This email is sent by logcheck. If you no longer wish to receive
such mail, you can either deinstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

System Events
-----
May 19 09:38:43 debian gnome-screensaver-dialog: gkr-pam: unlocked login keyring
May 19 10:06:39 debian gnome-screensaver-dialog: gkr-pam: unlocked login keyring
May 19 10:15:58 debian polkitd(authority=local): Operator of unix-session:/org/freedesktop/ConsoleKit/Session2 successfully authenticated as unix-user:root to gain TEMPORARY authorization for action org.freedesktop.consolekit.system.stop-multiple-users for system-bus-name::1.31 [x-session-manager] (owned by unix-user:j
:

```

**Rys. 3. Mail od logcheck**

*Źródło: opracowanie własne.*

Po uruchomieniu systemu logcheck przegląda dzienniki i w przypadku gdy nie znajdzie w nich żadnych podejrzanych informacji, kończy działanie bez podejmowania żadnej akcji. Jeśli stwierdzi wpisy, które nie są ujęte w logcheck.ignore, wyśle do administratora list zatytułowany „system check” zawierający wylistowane zdarzenia. Gdyby zaś w dzienniku były odnotowane zdarzenia ujęte w kategoriach zebranych w logcheck.hacking lub logcheck.violations, tytuł listu do administratora użytkownika będzie miał tytuł „Active system attack”. Logcheck wykorzystuje logtail do odnotowania

informacji o sprawdzonych przez siebie partiach dziennika. Dzięki temu nie są wyświetlane wielokrotnie te same fragmenty logów systemowych.

Automatyzacji procesu dopełni wpis, który umieszczony w crontabie co cztery godziny będzie uruchamiał logchecka:

```
0 */4 * * * sudo-u logcheck logcheck
```

## Podsumowanie

Każde narzędzie [Fry, Nystrom 2010; Kennedy, O'Gorman, Kearns, Aharoni 2013] wspomagające pracę administratora jest cenne. Tym bardziej narzędzia, które wykonują uciążliwą i żmudną pracę, jaką jest ciągła analiza logów [Camou, Gorzen, Couvenberghe 2001], dlatego warto spróbować i wdrożyć do swojej pracy takie rozwiązanie, jakim jest Logcheck. Jednak należy tu wspomnieć o przemyślanej konfiguracji, aby to narzędzie nie stało się przyczyną kłopotów w przypadku błędów w konfiguracji, a tym samym nieotrzymania ważnej informacji.

## Literatura

- Camou M., Gorzen J., Couvenberghe A. (2001), *Debian Linux. Księga eksperta*, Gliwice.
- Chirillo J. (2002a), *Hack Wars. Na tropie hakerów*, Gliwice.
- Chirillo J. (2002b), *Hack Wars. Administrator kontratakuję*, Gliwice.
- Fry Ch., Nystrom M. (2010), *Monitoring i bezpieczeństwo sieci*, Gliwice.
- Kennedy D., O'Gorman J., Kearns D., Aharoni M. (2013). *Metasploit. Przewodnik po testach penetracyjnych*, Gliwice.
- Rash M. (2008), *Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort*, Gliwice.

## Streszczenie

Artykuł ten opisuje sposób działania, zastosowanie oraz elementy konfiguracji programu Logcheck, który będzie pomocny administratorowi sieci w bieżącym monitorowaniu logów systemowych.

**Słowa kluczowe:** Logcheck, logi systemowe, bezpieczeństwo systemu.

## Monitoring system logs using the Logcheck

### Abstract

This article describes a program Logcheck. Briefly presented the use, installation and the configuration elements. It is a helpful tool for network administrators to assist in the monitoring system logs.

**Key words:** Logcheck, system logs, security system.