

Współczesne systemy komputerowe

Monitorowanie systemu

Informacje o systemie

- Wersja jądra.

```
root@debian:~# uname -r
6.12.57+deb13-amd64
```

- Model programowy (często błędnie nazywany architekturą).

```
root@debian:~# uname -m
x86_64
```

- Procesor (w zależności od wersji jądra może odpowiedzieć *unknown*).

```
root@debian:~# uname -p
ryzen
```

- Wszystkie informacje.

```
root@debian:~# uname -a
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05)
x86_64 GNU/Linux
```

- Czas pracy komputera.

```
root@debian:~# uptime
14:30:19 up 1:23, 2 users, load average: 0.22, 0.14, 0.06
```

- Wersja Debian GNU/Linux.

```
root@debian:~# cat /etc/debian_version
13.2
```

Logi

- **Log** (dziennik, plik dziennika, rejestr zdarzeń) to chronologiczny zapis zawierający informacje o zdarzeniach i działaniach dotyczących systemu komputerowego czy komputera; jest tworzony automatycznie przez program komputerowy.
- Istnieją dwa narzędzia do rejestrowania logów:
 - **journald** (część menadżer startu systemu **systemd**) – głównie służy do rejestrowania logów uruchamianych usług przez **systemd**, posiada niektóre funkcjonalności **sysloga**, logi są zapisywane w plikach binarnych (szybkie przeszukiwanie, kosztem kłopotów z odczytem szczególnie po awarii systemu),
 - klasyczny **syslog (rsyslog)** – zaawansowany demon do rejestrowania zdarzeń w systemie przez bibliotekę systemową, pochodzących z jądra systemu lub z użyciem gniazd; może rejestrować zdarzenia przez sieć od innych maszyn, logi są zapisywane w plikach tekstowych.

- Oba programy mogą ze sobą współpracować, często **syslog** w maszynach produkcyjnych pobiera logi od **journald**, natomiast w komputerach osobistych częściej rezygnuje się z **sysloga** lub utrzymuje w minimalnej konfiguracji ze względów na kompatybilność ze starszym oprogramowaniem.
- **journald** domyślnie używa narzędzia do stronicowania (**less**).

journald

- Wyświetl ostatni log od momentu startu systemu (bez filtrowania).

```
root@debian:~# journalctl
Nov 27 05:15:04 debian kernel: Linux version 6.12.57+deb13-amd64 (debian-kernel>
Nov 27 05:15:04 debian kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.12.57+d>
Nov 27 05:15:04 debian kernel: BIOS-provided physical RAM map:
Dec 27 05:15:04 debian kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Dec 27 05:15:04 debian kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000000>
...
```

- Wyświetl log z dzisiaj.

```
root@debian:~# journalctl --since today
Dec 13 08:24:24 debian kernel: Linux version 6.12.57+deb13-amd64 (debian-kernel>
Dec 13 08:24:24 debian kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.12.57+d>
Dec 13 08:24:24 debian kernel: BIOS-provided physical RAM map:
Dec 13 08:24:24 debian kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Dec 13 08:24:24 debian kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000000>
...
```

- Wyświetl ostatnie 10 linii.

```
root@debian:~# journalctl -n 10
Dec 13 08:24:48 debian rtkit-daemon[985]: Supervising 13 threads of 7 processes>
Dec 13 08:24:48 debian rtkit-daemon[985]: Supervising 13 threads of 7 processes>
Dec 13 08:24:48 debian spice-vdagent[1852]: vdagent-audio: (capture-left) 65535>
Dec 13 08:24:48 debian spice-vdagent[1852]: vdagent-audio: (capture-right) 6553>
Dec 13 08:24:48 debian dbus-daemon[1602]: [session uid=1000 pid=1602 pidfd=5] S>
Dec 13 08:24:48 debian dbus-daemon[1602]: [session uid=1000 pid=1602 pidfd=5] A>
Dec 13 08:24:48 debian systemd[1580]: Starting xdg-document-portal.service - fl>
Dec 13 08:24:48 debian systemd[1580]: Started localsearch-3.service - Tracker f>
Dec 13 08:24:48 debian dbus-daemon[1602]: [session uid=1000 pid=1602 pidfd=5] S>
Dec 13 08:24:48 debian systemd[1580]: Started xdg-document-portal.service - fla>
...
```

- Wyświetl komunikaty z ostatniego startu systemu.

```
root@debian:~# journalctl -b
Dec 13 10:36:08 debian kernel: Linux version 6.12.57+deb13-amd64 (debian-kernel>
Dec 13 10:36:08 debian kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.12.57+d>
Dec 13 10:36:08 debian kernel: BIOS-provided physical RAM map:
Dec 13 10:36:08 debian kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Dec 13 10:36:08 debian kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000000>
...
```

- Wyświetl komunikaty jądra.

```
root@debian:~# journalctl -k
Dec 13 10:36:08 debian kernel: Linux version 6.12.57+deb13-amd64 (debian-kernel>
Dec 13 10:36:08 debian kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.12.57+d>
Dec 13 10:36:08 debian kernel: BIOS-provided physical RAM map:
...
Dec 13 10:36:08 debian kernel: iommu: DMA domain TLB invalidation policy: lazy >
Dec 13 10:36:08 debian kernel: pps_core: LinuxPPS API ver. 1 registered
Dec 13 10:36:08 debian kernel: PTP clock support registered
...
Dec 13 10:36:17 debian kernel: rfkill: input handler enabled
Dec 13 10:36:19 debian kernel: rfkill: input handler disabled
Dec 13 10:36:20 debian kernel: input: spice vdagent tablet as /devices/virtual/>
```

- Wyświetl logi usługi **cron** (można wyświetlić logi dla każdego unita).

```
root@debian:~# journalctl -u cron
Nov 27 05:15:13 debian systemd[1]: Started cron.service - Regular background pr>
Nov 27 05:15:13 debian cron[727]: (CRON) INFO (pidfile fd = 3)
Nov 27 05:15:13 debian cron[727]: (CRON) INFO (Running @reboot jobs)
...
```

- Logi **crona** od wczoraj.

```
root@debian:~# journalctl -u cron --since today
Dec 13 08:24:26 debian systemd[1]: Started cron.service - Regular background pr>
Dec 13 08:24:26 debian cron[785]: (CRON) INFO (pidfile fd = 3)
Dec 13 08:24:26 debian cron[785]: (CRON) INFO (Running @reboot jobs)
...
```

- Wyświetl logi informujące o błędach (inne możliwe typy: **0: emerg**, **1: alert**, **2: crit**, **3: err**, **4: warning**, **5: notice**, **6: info**, **7: debug**).

```
root@debian:~# journalctl -p err
Nov 27 05:15:05 debian systemd-udevd[370]: /usr/lib/udev/rules.d/90-alsa-restor>
Nov 27 05:15:05 debian systemd-udevd[370]: /usr/lib/udev/rules.d/90-alsa-restor>
Nov 27 05:15:38 debian kernel: watchdog: watchdog0: watchdog did not stop!
...
```

- Wyświetl informacje o wielkości plików logów.

```
root@debian:~# journalctl --disk-usage
Archived and active journals take up 181.2M in the file system.
```

- Skasuj pliki archiwalnych logów, pozostawiając dwa ostatnie.

```
root@debian:~# journalctl --vacuum-files=2
Vacuuming done, freed 0B of archived journals from /run/log/journal.
```

```
Deleted archived journal
/var/log/journal/918f6c2680a74c5c9c2f35e014f4cfd3/system@563b17c9d7c5443ebc13b337f003
eb60-000000000000000001-00064490c9639a64.journal (61.2M).
Deleted archived journal
/var/log/journal/918f6c2680a74c5c9c2f35e014f4cfd3/system@000645a8b7ef4690-
ce6f1d2c14165999.journal~ (56M).
Vacuuming done, freed 117.2M of archived journals from
/var/log/journal/918f6c2680a74c5c9c2f35e014f4cfd3.
Vacuuming done, freed 0B of archived journals from /var/log/journal.
```

syslog

- Pliki logów znajdują się w katalogu **/var/log**.

```
root@debian:~# ls -l --group-directories-first /var/log
total 1672
drwxr-xr-x  2 root          root          4096 Dec 11 11:58 apt
drwxr-xr-x  2 root          root          4096 Dec 13 09:10 cups
drwx--x--x  2 root          Debian-gdm   4096 Nov 27 05:15 gdm3
drwxr-xr-x  3 root          root          4096 Nov 27 05:14 installer
drwxr-sr-x+ 3 root          systemd-journal 4096 Nov 27 05:15 journal
drwx----- 2 root          root          4096 Nov 27 04:56 private
drwxr-x---  2 root          adm          4096 Oct 16 12:19 samba
drwx----- 2 speech-dispatcher root        4096 Jul  1 19:34 speech-dispatcher
-rw-r--r--  1 root          root          464 Dec 11 11:49 alternatives.log
-rw-r--r--  1 root          root        60582 Nov 29 17:51 alternatives.log.1
-rw-----  1 root          root          7317 Dec 13 10:36 boot.log
-rw-----  1 root          root          7885 Dec 13 09:10 boot.log.1
-rw-----  1 root          root        67597 Dec 12 14:59 boot.log.2
-rw-----  1 root          root        52506 Dec 11 02:03 boot.log.3
-rw-----  1 root          root          7771 Dec 10 05:31 boot.log.4
-rw-----  1 root          root        47323 Dec  9 17:02 boot.log.5
-rw-----  1 root          root        14973 Dec  1 13:29 boot.log.6
-rw-----  1 root          root        22118 Nov 30 10:42 boot.log.7
-rw-rw----  1 root          utmp          384 Dec 10 04:57 btmp
-rw-rw----  1 root          utmp              0 Nov 27 04:56 btmp.1
-rw-r--r--  1 root          root        22743 Dec 11 11:58 dpkg.log
-rw-r--r--  1 root          root       1271357 Nov 29 17:51 dpkg.log.1
-rw-r--r--  1 root          root          5818 Nov 27 05:13 fontconfig.log
-rw-rw-r--  1 root          utmp              0 Nov 27 04:56 lastlog
lrwxrwxrwx  1 root          root              39 Nov 27 04:56 README ->
./../usr/share/doc/systemd/README.logs
-rw-r--r--  1 sddm          sddm              0 Nov 27 05:12 sddm.log
-rw-rw-r--  1 root          utmp       33408 Dec 13 10:36 wtmp
-rw-r--r--  1 root          root      20480 Dec 13 10:36 wtmp.db
```

- Pliki z liczbami większymi od **0** w nazwie, są logami archiwalnymi.
- Najważniejsze logi systemowe:
 - **boot.msg** - komunikaty ze startu systemu (domyślnie w systemach z **systemd** nie występuje),
 - **messages** - plik zdarzeń ogólnego przeznaczenia,
 - **lastlog** - log w formacie binarnym, zapamiętuje czasy ostatnich logowań użytkowników, można go przeglądać poleceniem **lastlog**, w nowszych systemach operacyjnych może być nieobecny (z powodu zmiany sposobu zapisu logowań użytkowników) i zastąpiony narzędziem **lastlog2**,

- **wtmp** - log w formacie binarnym, zapamiętuje historię logowań użytkowników, można go przeglądać poleceniem **last**,
- **kern.log** - komunikaty jądra, można je wyświetlić poleceniem **dmesg**.
- Logi niektórych usług i programów:
 - **cron** - komunikaty demona cron,
 - **httpd/access_log**, **httpd/error_log** - serwer http (Apache),
 - **mail**, **mail.err**, **mail.info**, **mail.warn** - serwer poczty (postfix),
 - **mysqld.log** - serwer MySQL,
 - **samba/log.smbd** - serwer Samba,
 - **squid/access.log** - serwer proxy (Squid).
- Sprawdź historię logowań.

```
root@debian:~# last
root      pts/0                Sun Dec 14 02:44 - still logged in
foo       tty2                    Sun Dec 14 02:44 - still logged in
Debian-g  tty1                    Sun Dec 14 02:43 - 02:44 (00:00)
reboot    system boot  6.12.57+deb13-am Sun Dec 14 02:43 - still running
root      pts/0                Sun Dec 14 02:22 - 02:43 (00:21)
...
```

- Aby sprawdzić ostatnie logowania użytkowników, należy zainstalować pakiet **lastlog2** i zrestartować maszynę.

```
root@debian:~# apt update
```

```
root@debian:~# apt install lastlog2
```

```
root@debian:~# reboot
```

- Po uruchomieniu.

```
root@debian:~# lastlog2
Username      Port      From                Latest
Debian-gdm    tty1      Sun Dec 14 02:43:56 -0500 2025
foo           tty2      Sun Dec 14 02:44:05 -0500 2025
root          pts/0     Sun Dec 14 02:44:28 -0500 2025
```

- Za zbieranie logów odpowiada demon **syslog** (aktualny program nazywa się **rsyslog**).
- Nie jest domyślnie instalowany, zainstaluj i uruchom demona **rsyslog**.

```
root@debian:~# apt update
```

```
root@debian:~# apt install rsyslog
```

```
root@debian:~# systemctl enable rsyslog
```

```
root@debian:~# systemctl start rsyslog
```

```
root@debian:~# systemctl status rsyslog
```

```
● rsyslog.service - System Logging Service
```

```

Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: >
Active: active (running) since Sun 2025-12-14 03:02:47 EST; 49s ago
Invocation: a534f54858b34c138410794ac68f43b9
TriggeredBy: ● syslog.socket
Docs: man:rsyslogd(8)
      man:rsyslog.conf(5)
      https://www.rsyslog.com/doc/
Main PID: 2911 (rsyslogd)
Tasks: 4 (limit: 2296)
Memory: 1.9M (peak: 2.4M)
CPU: 40ms
CGroup: /system.slice/rsyslog.service
        └─2911 /usr/sbin/rsyslogd -n -iNONE

Dec 14 03:02:47 debian systemd[1]: Starting rsyslog.service - System Logging Se>
Dec 14 03:02:47 debian rsyslogd[2911]: imuxsock: Acquired UNIX socket '/run/sys>
Dec 14 03:02:47 debian rsyslogd[2911]: [origin software="rsyslogd" swVersion="8>
Dec 14 03:02:47 debian systemd[1]: Started rsyslog.service - System Logging Ser>

```

- Wyświetl plik konfiguracyjny **/etc/rsyslog.conf** (podstawowa konfiguracja, ustawienia użytkownika należy umieszczać w katalogu **/etc/rsyslog.d**).

```

root@debian:~# egrep ^\[^\#] /etc/rsyslog.conf
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$WorkDirectory /var/spool/rsyslog
$IncludeConfig /etc/rsyslog.d/*.conf
*. *;auth,authpriv.none      -/var/log/syslog
auth,authpriv.*             /var/log/auth.log
cron.*                      -/var/log/cron.log
kern.*                      -/var/log/kern.log
mail.*                      -/var/log/mail.log
user.*                      -/var/log/user.log
*.emerg                     :omusrmsg:*

```

- W pliku konfiguracyjnym są zdefiniowane grupy programów, domyślnie znajdują się: **authpriv**, **cron**, **kern**, **mail** i **user**.

authpriv	używany przez programy które używają bibliotek PAM lub muszą autoryzować się w systemie
cron	komunikaty demonów cron i at
kern	komunikaty jądra
mail	komunikaty związane z systemem poczty
user	różne komunikaty poziomu użytkownika
daemon	używane przez różne demony systemowe
lpr	komunikaty systemu drukowania
news	komunikaty związane z systemem grup dyskusyjnych

syslog	komunikaty loggera
uucp	komunikaty systemu uucp

- W domyślnej instalacji występuje tylko jeden priorytet komunikatów: **emerg** - poważne błędy, często nieprawidłowo działającego systemu.

emerg	poważne błędy, często nieprawidłowo działającego systemu
debug	komunikaty związane z debugowaniem programów
info	komunikaty informacyjne
notice	różne komunikaty opisujące normalny stan pracy systemu
warning	komunikaty ostrzeżeń
err	komunikaty błędów
crit	komunikaty błędów krytycznych
alert	komunikaty alarmów, na które należy bezzwłocznie zareagować

- Przejrzyj manual do polecenia **logrotate** (rotowanie i archiwizacja logów).

Wysyłanie komunikatów

- Otwórz dodatkowy terminal, ułóż okna tak, aby były oba widoczne, w jednym oknie uruchom śledzenie logów.

```
| root@debian:~# journalctl -f
```

- W drugim oknie wydaj polecenia wysłania komunikatów (najczęściej takiej techniki używa się w połączeniu ze skryptami powłoki) i obserwuj log.

```
| root@debian:~$ logger "ała ma psa"
```

```
| root@debian:~$ logger -p info "info"
```

```
| root@debian:~$ logger -p debug "debug"
```

```
| root@debian:~$ logger -p emerg "dramat i rozpacz"
```