

# Współczesne systemy komputerowe

## Monitorowanie systemu

### Informacje o systemie

- Wersja jądra

```
root@debian:~# uname -r
4.9.0-6-686
```

- Model programowy (często nazywany architekturą)

```
root@debian:~# uname -m
i686
```

- Procesor

```
suse:~ # uname -p
phenom
```

- Wszystkie informacje

```
root@debian:~# uname -a
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686 GNU/Linux
```

- Czas pracy komputera

```
root@debian:~# uptime
05:51:11 up 2:00, 1 user, load average: 0.22, 0.14, 0.06
```

- Wersja Debian GNU/Linux

```
root@debian:~# cat /etc/debian_version
4.9
```

### 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**)

## journalctl

- Wyświetl ostatnie log od momentu startu systemu (bez filtrowania)

```
root@debian:~# journalctl
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 03:50:44 debian kernel: Linux version 4.9.0-6-686 (debian-kernel@lists.de
Mar 16 03:50:44 debian kernel: x86/fpu: Legacy x87 FPU detected.
...
Mar 16 03:50:44 debian kernel: x86/PAT: MTRRs disabled, skipping PAT initializat
Mar 16 03:50:44 debian kernel: CPU MTRRs all blank - virtualized system.
Mar 16 03:50:44 debian kernel: x86/PAT: Configuration [0-7]: WB WT UC- UC WB
```

- Wyświetl log z dzisiaj

```
root@debian:~# journalctl --since today
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 03:50:44 debian kernel: Linux version 4.9.0-6-686 (debian-kernel@lists.de
Mar 16 03:50:44 debian kernel: x86/fpu: Legacy x87 FPU detected.
...
Mar 16 03:50:44 debian kernel: x86/PAT: MTRRs disabled, skipping PAT initializat
Mar 16 03:50:44 debian kernel: CPU MTRRs all blank - virtualized system.
Mar 16 03:50:44 debian kernel: x86/PAT: Configuration [0-7]: WB WT UC- UC WB
```

- Wyświetl ostatnie 10 linii

```
root@debian:~# journalctl -n 10
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 08:17:01 debian CRON[2866]: pam_unix(cron:session): session opened for us
Mar 16 08:17:01 debian CRON[2867]: (root) CMD ( cd / && run-parts --report /et
Mar 16 08:17:01 debian CRON[2866]: pam_unix(cron:session): session closed for us
Mar 16 08:20:39 debian su[2847]: pam_unix(su:session): session closed for user r
Mar 16 08:21:30 debian tracker-extract[846]: unable to create file '/run/user/10
Mar 16 08:21:34 debian tracker-extract[846]: unable to create file '/run/user/10
Mar 16 08:46:54 debian dbus[333]: [system] Activating via systemd: service name=
Mar 16 08:46:54 debian systemd[1]: Starting Time & Date Service...
Mar 16 08:46:54 debian dbus[333]: [system] Successfully activated service 'org.f
Mar 16 08:46:54 debian systemd[1]: Started Time & Date Service.
```

- Wyświetl komunikaty z ostatniego startu systemu

```
root@debian:~# journalctl -b
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 05:17:01 EDT
Mar 16 03:50:44 debian kernel: Linux version 4.9.0-6-686 (debian-kernel@lists.de
Mar 16 03:50:44 debian kernel: x86/fpu: Legacy x87 FPU detected.
```

```
...
Mar 16 03:50:44 debian kernel: x86/PAT: MTRRs disabled, skipping PAT initializat
Mar 16 03:50:44 debian kernel: CPU MTRRs all blank - virtualized system.
Mar 16 03:50:44 debian kernel: x86/PAT: Configuration [0-7]: WB WT UC- UC WB
```

- Wyświetl komunikaty jądra

```
root@debian:~# journalctl -k
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 05:48:38 EDT
Mar 16 03:50:44 debian kernel: Linux version 4.9.0-6-686 (debian-kernel@lists.de
...
Mar 16 03:50:44 debian kernel: x86/PAT: MTRRs disabled, skipping PAT initializat
Mar 16 03:50:44 debian kernel: CPU MTRRs all blank - virtualized system.
Mar 16 03:50:44 debian kernel: x86/PAT: Configuration [0-7]: WB WT UC- UC WB
```

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

```
root@debian:~# journalctl -u cron
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 03:50:50 debian systemd[1]: Started Regular background program processing
Mar 16 03:50:50 debian cron[330]: (CRON) INFO (pidfile fd = 3)
Mar 16 03:50:50 debian cron[330]: (CRON) INFO (Running @reboot jobs)
Mar 16 04:17:01 debian CRON[1475]: pam_unix(cron:session): session opened for us
Mar 16 04:17:01 debian CRON[1476]: (root) CMD ( cd / && run-parts --report /et
Mar 16 05:17:01 debian CRON[1835]: pam_unix(cron:session): session opened for us
Mar 16 05:17:01 debian CRON[1836]: (root) CMD ( cd / && run-parts --report /et
Mar 16 06:17:01 debian CRON[2095]: pam_unix(cron:session): session opened for us
Mar 16 06:17:01 debian CRON[2096]: (root) CMD ( cd / && run-parts --report /et
Mar 16 06:25:01 debian CRON[2113]: pam_unix(cron:session): session opened for us
Mar 16 06:25:01 debian CRON[2114]: (root) CMD (test -x /usr/sbin/anacron || ( cd
Mar 16 07:17:02 debian CRON[2745]: pam_unix(cron:session): session opened for us
Mar 16 07:17:02 debian CRON[2746]: (root) CMD ( cd / && run-parts --report /et
Mar 16 07:30:01 debian CRON[2751]: pam_unix(cron:session): session opened for us
Mar 16 07:30:01 debian CRON[2752]: (root) CMD ([ -x /etc/init.d/anacron ] && if
Mar 16 08:17:01 debian CRON[2866]: pam_unix(cron:session): session opened for us
Mar 16 08:17:01 debian CRON[2867]: (root) CMD ( cd / && run-parts --report /et
```

- Logi **crona** od wczoraj

```
root@debian:~# journalctl -u cron --since yesterday
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 03:50:50 debian systemd[1]: Started Regular background program processing
Mar 16 03:50:50 debian cron[330]: (CRON) INFO (pidfile fd = 3)
Mar 16 03:50:50 debian cron[330]: (CRON) INFO (Running @reboot jobs)
Mar 16 04:17:01 debian CRON[1475]: pam_unix(cron:session): session opened for us
Mar 16 04:17:01 debian CRON[1476]: (root) CMD ( cd / && run-parts --report /et
Mar 16 05:17:01 debian CRON[1835]: pam_unix(cron:session): session opened for us
Mar 16 05:17:01 debian CRON[1836]: (root) CMD ( cd / && run-parts --report /et
Mar 16 06:17:01 debian CRON[2095]: pam_unix(cron:session): session opened for us
Mar 16 06:17:01 debian CRON[2096]: (root) CMD ( cd / && run-parts --report /et
Mar 16 06:25:01 debian CRON[2113]: pam_unix(cron:session): session opened for us
Mar 16 06:25:01 debian CRON[2114]: (root) CMD (test -x /usr/sbin/anacron || ( cd
Mar 16 07:17:02 debian CRON[2745]: pam_unix(cron:session): session opened for us
Mar 16 07:17:02 debian CRON[2746]: (root) CMD ( cd / && run-parts --report /et
Mar 16 07:30:01 debian CRON[2751]: pam_unix(cron:session): session opened for us
Mar 16 07:30:01 debian CRON[2752]: (root) CMD ([ -x /etc/init.d/anacron ] && if
```

```
Mar 16 08:17:01 debian CRON[2866]: pam_unix(cron:session): session opened for us
Mar 16 08:17:01 debian CRON[2867]: (root) CMD ( cd / && run-parts --report /et
```

- 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
-- Logs begin at Fri 2018-03-16 03:50:44 EDT, end at Fri 2018-03-16 08:46:54 EDT
Mar 16 03:50:44 debian kernel: piix4_smbus 0000:00:07.0: SMBus base address unin
Mar 16 03:50:53 debian avahi-daemon[385]: chroot.c: open() failed: No such file
Mar 16 03:55:53 debian pulseaudio[750]: [pulseaudio] bluez5-util.c: GetManagedOb
Mar 16 03:58:27 debian pulseaudio[750]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA
Mar 16 03:58:27 debian pulseaudio[750]: [alsa-sink-Intel ICH] alsa-sink.c: Most
Mar 16 03:58:27 debian pulseaudio[750]: [alsa-sink-Intel ICH] alsa-sink.c: We we
```

- Wyświetl informacje o wielkości plików logów

```
root@debian:~# journalctl --disk-usage
Archived and active journals take up 5.0M in the file system.
```

- Skasuj pliki archiwalnych logów, pozostawiając dwa ostatnie

```
root@debian:~# journalctl --vacuum-files=2
Deleted archived journal
/run/log/journal/68a85263197041b5a662f7880c14cde8/system@0a7489b34a1a4723b8f3c2
9231c23ace-0000000000000001-00056782dd9b1ee0.journal (1.2M).
Deleted archived journal
/run/log/journal/68a85263197041b5a662f7880c14cde8/system@0a7489b34a1a4723b8f3c2
9231c23ace-0000000000000277-00056782de3a2b3e.journal (1.2M).
Vacuuming done, freed 2.5M of archived journals from
/run/log/journal/68a85263197041b5a662f7880c14cde8.
```

## syslog

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

```
root@debian:~# ls -l --group-directories-first /var/log
total 16756
drwxr-xr-x 2 root      root      4096 Mar 16 04:06 apt
drwxr-xr-x 2 root      root      4096 Mar 16 03:56 cups
drwx--x--x 2 root      Debian-gdm 4096 Jun  6 2017 gdm3
drwxr-xr-x 3 root      root      4096 Aug 18 2017 hp
drwxr-xr-x 3 root      root      4096 Aug 18 2017 installer
drwx----- 2 speech-dispatcher root      4096 Mar  5 2017 speech-dispatcher
drwxr-x--- 2 root      adm       4096 Mar  5 03:53 unattended-upgrades
-rw-r--r-- 1 root      root      348 Mar 12 10:02 alternatives.log
-rw-r--r-- 1 root      root      5776 Feb 28 12:16 alternatives.log.1
-rw-r--r-- 1 root      root      5730 Dec 19 06:15 alternatives.log.2.gz
-rw-r----- 1 root      adm       47897 Mar 16 05:48 auth.log
-rw-r----- 1 root      adm       28688 Mar 12 10:07 auth.log.1
-rw-r----- 1 root      adm       1222 Mar  5 03:53 auth.log.2.gz
-rw-r----- 1 root      adm       2300 Feb 28 07:02 auth.log.3.gz
-rw-r----- 1 root      adm       1933 Dec 19 03:05 auth.log.4.gz
-rw----- 1 root      utmp      0 Mar  5 03:53 utmp
-rw----- 1 root      utmp      0 Feb 28 07:06 bttmp.1
-rw-r----- 1 root      adm       557891 Mar 16 05:03 daemon.log
-rw-r----- 1 root      adm       197556 Mar 12 10:07 daemon.log.1
-rw-r----- 1 root      adm        8810 Mar  5 03:53 daemon.log.2.gz
```

-rw-r-----	1	root	adm	15312	Feb	28	07:06	daemon.log.3.gz
-rw-r-----	1	root	adm	48606	Dec	19	03:09	daemon.log.4.gz
-rw-r-----	1	root	adm	121900	Mar	16	03:55	debug
-rw-r-----	1	root	adm	43272	Mar	12	10:01	debug.1
-rw-r-----	1	root	adm	1760	Mar	5	03:49	debug.2.gz
-rw-r-----	1	root	adm	2674	Feb	28	07:02	debug.3.gz
-rw-r-----	1	root	adm	16779	Dec	19	03:04	debug.4.gz
-rw-r--r--	1	root	root	16830	Mar	16	04:06	dpkg.log
-rw-r--r--	1	root	root	5588	Mar	5	03:49	dpkg.log.1
-rw-r--r--	1	root	root	109516	Feb	28	07:06	dpkg.log.2.gz
-rw-r--r--	1	root	root	24072	Mar	5	06:25	faillog
-rw-r--r--	1	root	root	2956	Feb	28	07:06	fontconfig.log
-rw-r-----	1	root	adm	535857	Mar	16	03:55	kern.log
-rw-r-----	1	root	adm	191362	Mar	12	10:01	kern.log.1
-rw-r-----	1	root	adm	10124	Mar	5	03:49	kern.log.2.gz
-rw-r-----	1	root	adm	19964	Feb	28	07:05	kern.log.3.gz
-rw-r-----	1	root	adm	44949	Dec	19	03:04	kern.log.4.gz
-rw-rw-r--	1	root	utmp	292876	Mar	15	07:33	lastlog
-rw-r-----	1	root	adm	4397827	Mar	16	05:04	messages
-rw-r-----	1	root	adm	1341588	Mar	12	10:07	messages.1
-rw-r-----	1	root	adm	33998	Mar	5	03:53	messages.2.gz
-rw-r-----	1	root	adm	67350	Feb	28	07:06	messages.3.gz
-rw-r-----	1	root	adm	112397	Dec	19	03:09	messages.4.gz
-rw-r-----	1	root	adm	4057	Mar	16	05:17	syslog
-rw-r-----	1	root	adm	2779972	Mar	16	03:56	syslog.1
-rw-r-----	1	root	adm	186975	Mar	15	06:27	syslog.2.gz
-rw-r-----	1	root	adm	32295	Mar	13	04:13	syslog.3.gz
-rw-r-----	1	root	adm	24299	Mar	12	10:07	syslog.4.gz
-rw-r-----	1	root	adm	95124	Mar	8	07:02	syslog.5.gz
-rw-r-----	1	root	adm	35269	Mar	6	04:58	syslog.6.gz
-rw-r-----	1	root	adm	47084	Mar	5	03:53	syslog.7.gz
-rw-r-----	1	root	adm	3967132	Mar	16	05:04	user.log
-rw-r-----	1	root	adm	1186957	Mar	12	10:02	user.log.1
-rw-r-----	1	root	adm	24773	Mar	5	03:49	user.log.2.gz
-rw-r-----	1	root	adm	50873	Feb	28	07:06	user.log.3.gz
-rw-r-----	1	root	adm	73280	Dec	19	03:04	user.log.4.gz
-rw-r--r--	1	root	root	50230	Dec	19	06:24	vboxadd-install.log
-rw-r--r--	1	root	root	73	Dec	19	06:24	vboxadd-install-x11.log
-rw-r--r--	1	root	root	161	Dec	19	06:24	VBoxGuestAdditions.log
-rw-rw-r--	1	root	utmp	45312	Mar	16	03:55	wtmp
-rw-rw-r--	1	root	utmp	1152	Mar	5	03:49	wtmp.1
-rw-r--r--	1	root	root	55834	Mar	16	03:55	Xorg.0.log
-rw-r--r--	1	root	root	55834	Mar	15	09:04	Xorg.0.log.old
-rw-r--r--	1	root	root	55548	Mar	16	03:55	Xorg.1.log
-rw-r--r--	1	root	root	56517	Mar	15	09:11	Xorg.1.log.old
-rw-r--r--	1	root	root	56676	Mar	13	08:05	Xorg.2.log
-rw-r--r--	1	root	root	56678	Dec	19	03:39	Xorg.2.log.old

- Pliki z liczbami większymi od 0 w nazwie, są logami archiwalnymi
- Najważniejsze logi systemowe
  - **boot.msg** - komunikaty ze startu systemu (nie ma domyślnie)
  - **messages** - plik zdarzeń ogólnego przeznaczenia
  - **lastlog** - log w formacie binarnym, zapamiętuje czasy ostatnich logowań użytkowników, można go przeglądać poleceniem **lastlog**
  - **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 **Apache** (http)
- **mail, mail.err, mail.info, mail.warn** - serwer poczty **postfix**
- **mysqld.log** - serwer **MySQL**
- **Xorg.0.log** - serwer **Xorg** (interfejs graficzny)
- **samba/log.smbd** - serwer **Samba**
- **squid/access.log** - serwer **Squid** (proxy)
- Sprawdź ostatnie logowania użytkowników i historię logowań

```
root@debian:~# lastlog
Username      Port      From      Latest
root          tty2                Thu Mar 15 07:33:13 -0400 2018
daemon
bin           **Never logged in**
...
foo          **Never logged in**
vboxadd     **Never logged in**
dummy
```

```
root@debian:~# last
foo      tty2      :1      Fri Mar 16 03:55  still logged in
reboot  system boot 4.9.0-6-686  Fri Mar 16 03:50  still running
foo      tty2      :1      Thu Mar 15 09:04 - 09:11  (00:06)
...
reboot  system boot 4.9.0-6-686  Wed Mar 7 08:53 - 08:56  (00:03)
foo      tty2      :1      Tue Mar 6 04:52 - 09:05  (04:13)
reboot  system boot 4.9.0-6-686  Tue Mar 6 04:51 - 09:07  (04:15)

wtmp begins Mon Mar 5 06:30:54 2018
```

- Wyświetl błędy serwera **Xorg** w otoczeniu trzech linii

```
root@debian:~# cat /var/log/Xorg.0.log | grep -n3 EE
13-   to make sure that you have the latest version.
14-[ 15.732] Markers: (--) probed, (**) from config file, (==) default setting,
15-   (++) from command line, (!!) notice, (II) informational,
16-   (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
17-[ 15.732] (==) Log file: "/var/log/Xorg.0.log", Time: Fri Mar 16 03:50:56 2018
18-[ 15.761] (==) Using system config directory "/usr/share/X11/xorg.conf.d"
19-[ 15.792] (==) No Layout section.  Using the first Screen section.
--
85-[ 16.033] (II) modesetting: Driver for Modesetting Kernel Drivers: kms
86-[ 16.033] (II) FBDEV: driver for framebuffer: fbdev
87-[ 16.033] (II) VESA: driver for VESA chipsets: vesa
88-[ 16.033] (EE) open /dev/dri/card0: No such file or directory
89-[ 16.033] (WW) Falling back to old probe method for modesetting
90-[ 16.033] (EE) open /dev/dri/card0: No such file or directory
91-[ 16.033] (II) Loading sub module "fbdevhw"
92-[ 16.033] (II) LoadModule: "fbdevhw"
93-[ 16.033] (II) Loading /usr/lib/xorg/modules/libfbdevhw.so
94-[ 16.045] (II) Module fbdevhw: vendor="X.Org Foundation"
95-[ 16.045] compiled for 1.19.2, module version = 0.0.2
96-[ 16.045] ABI class: X.Org Video Driver, version 23.0
```

```

97:[    16.045] (EE) open /dev/fb0: No such file or directory
98-[    16.045] (WW) Falling back to old probe method for fbdev
99-[    16.045] (II) Loading sub module "fbdevhw"
100-[   16.045] (II) LoadModule: "fbdevhw"
--
102-[   16.045] (II) Module fbdevhw: vendor="X.Org Foundation"
103-[   16.045] compiled for 1.19.2, module version = 0.0.2
104-[   16.045] ABI class: X.Org Video Driver, version 23.0
105:[    16.045] (EE) open /dev/fb0: No such file or directory
106:[    16.045] (EE) Screen 0 deleted because of no matching config section.
107-[    16.045] (II) UnloadModule: "modesetting"
108:[    16.045] (EE) Screen 0 deleted because of no matching config section.
109-[    16.045] (II) UnloadModule: "fbdev"
110-[    16.045] (II) UnloadSubModule: "fbdevhw"
111-[    16.045] (II) Loading sub module "vbe"
--
1293-[   16.478] (==) RandR enabled
1294-[   16.482] (II) SELinux: Disabled on system
1295-[   16.483] (II) AIGLX: Screen 0 is not DRI2 capable
1296:[    16.484] (EE) AIGLX: reverting to software rendering
1297-[   17.390] (II) IGLX: enabled GLX_MESA_copy_sub_buffer
1298-[   17.393] (II) IGLX: Loaded and initialized swrast
1299-[   17.394] (II) GLX: Initialized DRISWRAST GL provider for screen 0

```

- Za zbieranie logów odpowiada demon **syslog** (aktualny program nazywa się **rsyslog**)

```

root@debian:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset:
   Active: active (running) since Fri 2018-03-16 03:50:51 EDT; 5h 7min ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 331 (rsyslogd)
     Tasks: 4 (limit: 4915)
    CGroup: /system.slice/rsyslog.service
            └─331 /usr/sbin/rsyslogd -n

Mar 16 03:56:39 debian liblogging-stdlog[331]: [origin software="rsyslogd" swVe
Warning: Journal has been rotated since unit was started. Log output is incomple

```

- 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
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$WorkDirectory /var/spool/rsyslog
$IncludeConfig /etc/rsyslog.d/*.conf
auth,authpriv.*      /var/log/auth.log
*.*;auth,authpriv.none  -/var/log/syslog
daemon.*             -/var/log/daemon.log
kern.*               -/var/log/kern.log
lpr.*                 -/var/log/lpr.log
mail.*                -/var/log/mail.log

```

```

user.*                -/var/log/user.log
mail.info             -/var/log/mail.info
mail.warn             -/var/log/mail.warn
mail.err              /var/log/mail.err
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none     -/var/log/messages
*.emerg              :omusrmsg:*

```

- W pliku konfiguracyjnym są zdefiniowane min. grupy programów

authpriv	używany przez programy które używają bibliotek <b>PAM</b> lub muszą autentykować się w systemie
cron	komunikaty demonów <b>cron i at</b>
daemon	używane przez różne demony systemowe
kern	komunikaty jądra
lpr	komunikaty systemu drukowania
mail	komunikaty związane z systemem poczty
news	komunikaty związane z systemem grup dyskusyjnych
syslog	komunikaty loggera
user	różne komunikaty poziomu użytkownika
uucp	komunikaty systemu uucp
local0 - local17	dowolnie konfigurowane przez użytkownika

- A także priorytety komunikatów

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
emerg	poważne błędy, często nieprawidłowo działającego systemu

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

### Wysyłanie komunikatów do sysloga

- 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 wysyłania komunikatów (najczęściej takiej techniki używa się w połączeniu ze skryptami powłoki) i obserwuj log

```
root@debian:~# logger -p syslog.info "info-1"
```



```
root@debian:~# logger -p syslog.info "info-2"
```

```
root@debian:~# logger -p syslog.debug "debug-1"
```

```
root@debian:~# logger -p syslog.debug "debug-2"
```

- Sprawdź zawartość logów **sysloga**

```
root@debian:~# tail -n 5 /var/log/messages
Mar 16 09:00:38 debian NetworkManager[345]: <info> [1521205238.4572] manager:
    NetworkManager state is now CONNECTED_GLOBAL
Mar 16 09:00:38 debian NetworkManager[345]: <info> [1521205238.4573] policy: set
    'Wired connection 1' (enp0s3) as default for IPv4 routing and DNS
Mar 16 09:00:38 debian NetworkManager[345]: <info> [1521205238.4575] device (enp0s3):
    Activation: successful, device activated.
Mar 16 09:10:51 debian foo: info-1
Mar 16 09:10:53 debian foo: info-2
```

```
root@debian:~# tail -n 5 /var/log/debug
Mar 16 03:55:28 debian rtkit-daemon[353]: Supervising 2 threads of 1 processes of 1
    users.
Mar 16 03:55:28 debian rtkit-daemon[353]: Supervising 3 threads of 1 processes of 1
    users.
Mar 16 06:56:42 debian PackageKit: new update-packages transaction /1346_dbeeeeab
    scheduled from uid 1001
Mar 16 09:10:57 debian foo: debug-1
Mar 16 09:10:59 debian foo: debug-2
```