

Współczesne systemy komputerowe

Monitorowanie systemu

1. Informacje o systemie komputerowym.

- Informacje o starcie systemu i komunikaty jądra;

```
suse:~ # cat /var/log/boot.msg | less

klogd 1.4.1, log source = ksyslog started.
<6>[ 0.000000] Initializing cgroup subsys cpuset
<6>[ 0.000000] Initializing cgroup subsys cpu
<5>[ 0.000000] Linux version 3.0.13-0.27-default (geeko@buildhost) (gcc version
4.3.4 [gcc-4_3
-branch revision 152973] (SUSE Linux) ) #1 SMP Wed Feb 15 13:33:49 UTC 2012 (d73692b)
<6>[ 0.000000] BIOS-provided physical RAM map:
<6>[ 0.000000] BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
<6>[ 0.000000] BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
<6>[ 0.000000] BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
<6>[ 0.000000] BIOS-e820: 0000000000100000 - 000000003fff0000 (usable)
<6>[ 0.000000] BIOS-e820: 000000003fff0000 - 0000000040000000 (ACPI data)
<6>[ 0.000000] BIOS-e820: 00000000ffffc000 - 0000000100000000 (reserved)
<5>[ 0.000000] Notice: NX (Execute Disable) protection missing in CPU!
<6>[ 0.000000] DMI 2.5 present.
...
```

```
suse:~ # dmesg | less

[ 0.000000] Initializing cgroup subsys cpuset
[ 0.000000] Initializing cgroup subsys cpu
[ 0.000000] Linux version 3.0.13-0.27-default (geeko@buildhost) (gcc version 4.3.4
[gcc-4_3-br
anch revision 152973] (SUSE Linux) ) #1 SMP Wed Feb 15 13:33:49 UTC 2012 (d73692b)
[ 0.000000] BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
[ 0.000000] BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
[ 0.000000] BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
[ 0.000000] BIOS-e820: 0000000000100000 - 000000003fff0000 (usable)
[ 0.000000] BIOS-e820: 000000003fff0000 - 0000000040000000 (ACPI data)
[ 0.000000] BIOS-e820: 00000000ffffc000 - 0000000100000000 (reserved)
[ 0.000000] Notice: NX (Execute Disable) protection missing in CPU!
[ 0.000000] DMI 2.5 present.
```

- Wersja jądra;

```
suse:~ # uname -r
3.0.13-0.27-default
```

- Architektura komputera;

```
suse:~ # uname -m
i686
```

- Procesor;

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

- Wszystkie informacje;

```
suse:~ # uname -a
Linux suse 3.0.13-0.27-default #1 SMP Wed Feb 15 13:33:49 UTC 2012 (d73692b) i686
athlon i386 GNU/Linux
```

- Czas pracy komputera;

```
suse:~ # uptime
14:47pm up 14:58, 3 users, load average: 0.15, 0.17, 0.10
```

- Wersja SUSE;

```
suse:~ # cat /etc/SuSE-release
SUSE Linux Enterprise Server 11 (i586)
VERSION = 11
PATCHLEVEL = 2
```

2. Logi.

- Log (dziennik, plik dziennika, rejestr zdarzeń) to chronologiczny zapis zawierający informacje o zdarzeniach i działaniach dotyczących systemu komputerowego czy komputera, i jest tworzony automatycznie przez program komputerowy;
- Pliki logów znajdują się w katalogu `/var/log`;

```
suse:~ # ls -l --group-directories-first /var/log/
total 5304
drwxr-xr-x 2 root root 4096 Mar 12 13:38 ConsoleKit
drwx----- 2 root root 4096 Apr 7 11:56 YaST2
drwx----- 2 root root 4096 Mar 12 14:30 audit
drwxr-xr-x 2 lp lp 4096 Mar 12 14:17 cups
drwxrwx--T 2 root gdm 4096 Apr 7 15:37 gdm
drwx----- 2 root root 4096 Dec 29 2011 krb5
drwxr-x--- 2 news news 4096 Mar 12 16:50 news
drwxr-x--- 2 puppet puppet 4096 Feb 1 2012 puppet
drwxr-x--- 2 root root 4096 Feb 3 2012 samba
drwxr-xr-x 2 root root 4096 Feb 4 2012 zypp
-rw-r----- 1 root root 0 Mar 12 16:50 NetworkManager
-rwxr-xr-x 1 root root 1353 Mar 31 18:07 PackageKit
-rw-r--r-- 1 root root 4087 Mar 12 14:17 SaX.log
-rw-r--r-- 1 root root 431 Mar 14 17:47 VBoxGuestAdditions-uninstall.log
-rw-r--r-- 1 root root 98 Mar 18 15:04 VBoxGuestAdditions.log
-rw-r--r-- 1 root root 25317 Apr 9 23:30 Xorg.0.log
-rw-r--r-- 1 root root 19900 Apr 7 15:28 Xorg.0.log.old
-rw-r--r-- 1 root root 6876 Mar 12 14:17 Xorg.99.log
-rw-r----- 1 root root 3395 Apr 7 15:42 acpid
-rw-r--r-- 1 root root 30943 Apr 7 15:37 boot.msg
-rw-r--r-- 1 root root 47832 Apr 6 00:57 boot.omsg
lrwxrwxrwx 1 root root 10 Mar 12 17:00 dump -> /var/crash
-rw----- 1 root root 24048 Mar 25 23:14 faillog
-rw-r----- 1 root root 125707 Apr 7 15:50 firewall
```

```

-rw-r--r-- 1 root  tty    292584 Apr  7 15:43 lastlog
-rw-r----- 1 root  root   33346 Apr  8 23:59 localmessages
-rw-r----- 1 root  root    4023 Apr  6 00:57 mail
-rw-r----- 1 root  root     98 Mar 12 13:50 mail.err
-rw-r----- 1 root  root    3826 Apr  6 00:57 mail.info
-rw-r----- 1 root  root     99 Mar 14 15:12 mail.warn
-rw-r----- 1 root  root  356517 Apr  9 23:32 messages
-rw-r--r-- 1 root  root     0 Mar 12 16:43 ntp
-rw-r----- 1 root  root 2689172 Apr  9 17:44 pk_backend_zypp
-rw-r--r-- 1 root  root    1680 Mar 29 20:35 scpm
-rw-r--r-- 1 root  root     73 Mar 18 15:04 vboxadd-install-x11.log
-rw-r--r-- 1 root  root   166873 Mar 14 18:01 vboxadd-install.log
-rw-r----- 1 root  root    67637 Apr  7 15:44 warn
-rw-rw-r-- 1 root  tty   197760 Apr  8 17:46 wtmp
-rw-r----- 1 root  root  1486720 Apr  8 16:50 zypper.log

```

- Najważniejsze logi systemowe;
 - **boot.msg** - komunikaty ze startu systemu;
 - **cron** - komunikaty demona cron;
 - **firewall** - komunikaty firewalla;
 - **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**;
 - **dmesg** - **polecenie** wyświetlające komunikaty jądra;
- Logi niektórych usług i programów;
 - **httpd/access_log**, **httpd/error_log** - serwer Apache;
 - **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;

```

suse:~ # lastlog
Username          Port      Latest
at                **Never logged in**
bin               **Never logged in**
daemon           **Never logged in**
ftp              **Never logged in**
games            **Never logged in**
gdm              **Never logged in**
haldaemon        **Never logged in**
lp               **Never logged in**
mail             **Never logged in**
man              **Never logged in**
messagebus       **Never logged in**
news            **Never logged in**
ntp              **Never logged in**
polkituser       **Never logged in**
postfix          **Never logged in**
pulse            **Never logged in**
puppet           **Never logged in**

```

```

root      tty1      Sun Apr  7 15:35:39 +0200 2013
sshd      **Never logged in**
suse-ncc  **Never logged in**
uucp      **Never logged in**
uuuid     **Never logged in**
wwwrun    **Never logged in**
user      :0          Sun Apr  7 15:43:35 +0200 2013
vboxadd   **Never logged in**
dummy     **Never logged in**
suse:~ # last
user pts/0      :0.0      Mon Apr  8 17:46   still logged in
user pts/0      :0.0      Mon Apr  8 17:15 - 17:43   (00:27)
user pts/3      :0.0      Mon Apr  8 16:57 - 17:15   (00:18)
user pts/0      :0.0      Mon Apr  8 14:42 - 17:12   (02:30)
user pts/0      :0.0      Mon Apr  8 14:27 - 14:41   (00:14)
user pts/1      :0.0      Sun Apr  7 15:44   still logged in
user pts/0      :0.0      Sun Apr  7 15:44 - 14:26   (22:42)
user :0          Sun Apr  7 15:43   still logged in
user tty7       :0        Sun Apr  7 15:43   still logged in
root tty1      Sun Apr  7 15:35 - 15:38   (00:03)
user pts/1      :0.0      Sat Apr  6 00:59 - 15:28   (1+14:28)
user pts/0      :0.0      Sat Apr  6 00:59 - 15:28   (1+14:28)
user :0          Sat Apr  6 00:58 - 15:43   (1+14:44)
user tty7       :0        Sat Apr  6 00:58 - 15:28   (1+14:29)
reboot system boot 3.0.13-0.27-defa Fri Apr  5 22:53   (4+01:32)
reboot system boot 3.0.13-0.27-defa Fri Apr  5 22:43   (02:06)
...

```

- Wyświetlił błędy serwera Xorg w otoczeniu trzech linii;

```

suse:~ # grep -n3 \(EE\) /var/log/Xorg.0.log
10-      to make sure that you have the latest version.
11-Markers: (-- ) probed, (**) from config file, (==) default setting,
12-      (++) from command line, (!!) notice, (II) informational,
13-      (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
14-(==) Log file: "/var/log/Xorg.0.log", Time: Sun Apr  7 15:37:06 2013
15-(==) Using config file: "/etc/X11/xorg.conf"
16-(==) ServerLayout "Layout[all]"
--
129-(II) LoadModule: "freetype"
130-(WW) Warning, couldn't open module freetype
131-(II) UnloadModule: "freetype"
132:(EE) Failed to load module "freetype" (module does not exist, 0)
133-(II) LoadModule: "extmod"
134-(II) Loading /usr/lib/xorg/modules/extensions/libextmod.so
135-(II) Module extmod: vendor="X.Org Foundation"
--
315-(II) Next line is added to allow vboxvideo_drv.so to appear as whitelisted driver
316-(II) The file referenced, is *NOT* loaded
317-(II) Loading /usr/lib/xorg/modules/drivers//ati_drv.so
318:(EE) AIGLX error: vboxvideo does not export required DRI extension
319:(EE) AIGLX: reverting to software rendering
320-(II) AIGLX: Loaded and initialized /usr/lib/dri/swrast_dri.so
321-(II) GLX: Initialized DRISWRAST GL provider for screen 0
322-(II) VBoxVideo(0): Setting screen physical size to 211 x 158
--
365-(**) Mouse[2]: (accel) set acceleration profile 0
366-(II) Mouse[2]: On.
367-(II) config/hal: Adding input device ImExPS/2 Generic Explorer Mouse
368:(EE) config/hal: NewInputDeviceRequest failed (8)
369-(II) config/hal: Adding input device VirtualBox USB Tablet

```

```

370:(EE) config/hal: NewInputDeviceRequest failed (8)
371-(II) config/hal: Adding input device VirtualBox mouse integration
372:(EE) config/hal: NewInputDeviceRequest failed (8)
373-(II) config/hal: Adding input device AT Translated Set 2 keyboard
374:(EE) config/hal: NewInputDeviceRequest failed (8)
375-(II) VBoxVideo(0): EDID vendor "VBX", prod id 0
376-(II) VBoxVideo(0): DDCModeFromDetailedTiming: 800x600 Warning: We only handle
        separate sync.
377-(II) VBoxVideo(0): Using hsync ranges from config file

```

- Za zbieranie logów odpowiada demon **syslog** (aktualny program nazywa się **syslog-ng**, w starszych wersjach używany był program **syslogd**);

```

suse:~ # rcsyslog status
Checking for service syslog: running

```

- Pliki konfiguracyjne;
 - `/etc/sysconfig/syslog` - podstawowa konfiguracja akceptowana przez **syslog-ng** i **syslogd**;
 - `/etc/syslog-ng/syslog-ng.conf` - plik konfiguracyjny;
- Wyświetli i przejrzyj plik `/etc/sysconfig/syslog`;

```

suse:~ # cat /etc/sysconfig/syslog
## Path:                System/Logging
## Description:         System logging
## Type:                list(0,1,2,3,4,5,6,7)
## Default:             1
## Config:              ""
## ServiceRestart:    syslog
#
# Default loglevel for klogd
#
KERNEL_LOGLEVEL=1

## Type:                string
## Default:             ""
## Config:              ""
## ServiceRestart:    syslog
#
# if not empty: parameters for syslogd
# for example SYSLOGD_PARAMS="-r -s my.dom.ain"
#
SYSLOGD_PARAMS=""

## Type:                string
## Default:             -x
## Config:              ""
## ServiceRestart:    syslog
#
# if not empty: parameters for klogd
# for example KLOGD_PARAMS="-x" to avoid (duplicate) symbol resolution
#
KLOGD_PARAMS="-x"

## Type:                list(syslogd,syslog-ng, "")
## Default:             ""
## Config:              ""
## ServiceRestart:    syslog
#

```

```
# The name of the syslog daemon to use as syslog service:
# "syslogd", "syslog-ng" or "" for autodetect.
#
SYSLOG_DAEMON="syslog-ng"

## Type:          string
## Default:      ""
## Config:       ""
## ServiceRestart: syslog
#
# Parameters for Syslog New-Generation - see syslog-ng(8)
#
SYSLOG_NG_PARAMS=""
```

- Wyświetl plik konfiguracyjny `/etc/syslog-ng/syslog-ng.conf` bez komentarzy;

```
suse:~ # egrep -v ^[[[:blank:]]*\# /etc/syslog-ng/syslog-ng.conf | sed -e '/^$/d'
options { long_hostnames(off); sync(0); perm(0640); stats(3600); };
source src {
    internal();
    unix-dgram("/dev/log");
};
filter f_iptables { facility(kern) and match("IN=") and match("OUT="); };
filter f_console { level(warn) and facility(kern) and not filter(f_iptables)
    or level(err) and not facility(authpriv); };
filter f_newsnotice { level(notice) and facility(news); };
filter f_newscrit { level(crit) and facility(news); };
filter f_newserr { level(err) and facility(news); };
filter f_news { facility(news); };
filter f_mailinfo { level(info) and facility(mail); };
filter f_mailwarn { level(warn) and facility(mail); };
filter f_mailerr { level(err, crit) and facility(mail); };
filter f_mail { facility(mail); };
filter f_cron { facility(cron); };
filter f_local { facility(local0, local1, local2, local3,
    local4, local5, local6, local7); };
filter f_acpid_full { match('^acpid:'); };
filter f_acpid { level(emerg..notice) and match('^acpid:'); };
filter f_acpid_old { match('^\[acpid\]:'); };
filter f_netmgm { match('^NetworkManager:'); };
filter f_messages { not facility(news, mail) and not filter(f_iptables); };
filter f_warn { level(warn, err, crit) and not filter(f_iptables); };
filter f_alert { level(alert); };
destination console { pipe("/dev/tty10" owner(-1) group(-1) perm(-1)); };
log { source(src); filter(f_console); destination(console); };
destination xconsole { pipe("/dev/xconsole" owner(-1) group(-1) perm(-1)); };
log { source(src); filter(f_console); destination(xconsole); };
destination newscrit { file("/var/log/news/news.crit"
    owner(news) group(news)); };
log { source(src); filter(f_newscrit); destination(newscrit); };
destination newserr { file("/var/log/news/news.err"
    owner(news) group(news)); };
log { source(src); filter(f_newserr); destination(newserr); };
destination newsnotice { file("/var/log/news/news.notice"
    owner(news) group(news)); };
log { source(src); filter(f_newsnotice); destination(newsnotice); };
destination mailinfo { file("/var/log/mail.info"); };
log { source(src); filter(f_mailinfo); destination(mailinfo); };
destination mailwarn { file("/var/log/mail.warn"); };
log { source(src); filter(f_mailwarn); destination(mailwarn); };
destination mailerr { file("/var/log/mail.err" fsync(yes)); };
```

```

log { source(src); filter(f_mailerr); destination(mailerr); };
destination mail { file("/var/log/mail"); };
log { source(src); filter(f_mail); destination(mail); };

destination acpid { file("/var/log/acpid"); };
destination null { };
log { source(src); filter(f_acpid); destination(acpid); flags(final); };
log { source(src); filter(f_acpid_full); destination(null); flags(final); };
log { source(src); filter(f_acpid_old); destination(acpid); flags(final); };
destination netmngm { file("/var/log/NetworkManager"); };
log { source(src); filter(f_netmngm); destination(netmngm); flags(final); };
destination localmessages { file("/var/log/localmessages"); };
log { source(src); filter(f_local); destination(localmessages); };
destination messages { file("/var/log/messages"); };
log { source(src); filter(f_messages); destination(messages); };
destination firewall { file("/var/log/firewall"); };
log { source(src); filter(f iptables); destination(firewall); };
destination warn { file("/var/log/warn" fsync(yes)); };
log { source(src); filter(f_warn); destination(warn); };

```

- W pliku konfiguracyjnym są zdefiniowane tzw.;

- Facilities - grupy programów;

authpriv	używany przez programy które używają bibliotek PAM lub muszą autentykować się w systemie
cron	komunikaty demonów cron i at
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 – local7	dowolnie konfigurowane przez użytkownika

- Priorities - priorytet komunikatu;

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

- Sources - definicja sposobu grupowania komunikatów;
- Filters - definicja filtrów;

- Destinations – docelowe miejsce komunikatów (plik, kolejka FIFO, inny komputer);
- Log Paths - definiuje jakie komunikaty gdzie są zapamiętywane, w jaki sposób filtrowane i grupowane;
- Do pliku konfiguracyjnego loggera dodaj filtry;

```
filter f_localdebug {level(debug) and facility(local0)};
filter f_localinfo  {level(info)  and facility(local0)};
filter f_local      {                facility(local0)};
```

- Następnie miejsca docelowe i ścieżki logowania;

```
destination d_localdebug {file("/var/log/local.debug");};
destination d_localinfo  {file("/var/log/local.info");};
destination d_local      {file("/var/log/local.log");};

log {source(src); filter(f_localdebug); destination(d_localdebug)};
log {source(src); filter(f_localinfo);  destination(d_localinfo)};
log {source(src); filter(f_local);      destination(d_local)};
```

- Zrestartuj loggera;

```
suse:~ # rcsyslog restart
Shutting down syslog services                               done
Starting syslog services                                   done
```

- Sprawdź działanie;

```
suse:~ # logger -p local0.info "log: info-1"
suse:~ # logger -p local0.info "log: info-2"
suse:~ # logger -p local0.debug "log: debug-1"
suse:~ # logger -p local0.debug "log: debug-2"
suse:~ # logger -p local0.err "log: err-1"
suse:~ # logger -p local0.err "log: err-2"
suse:~ # cat /var/log/local.debug
Apr 10 23:41:44 suse user: log: debug-1
Apr 10 23:41:49 suse user: log: debug-2
suse:~ # cat /var/log/local.info
Apr 10 23:40:36 suse user: log: info-1
Apr 10 23:40:44 suse user: log: info-2
suse:~ # cat /var/log/local.log
Apr 10 23:40:36 suse user: log: info-1
Apr 10 23:40:44 suse user: log: info-2
Apr 10 23:41:44 suse user: log: debug-1
Apr 10 23:41:49 suse user: log: debug-2
Apr 10 23:42:56 suse user: log: err-1
Apr 10 23:43:00 suse user: log: err-2
```

- Otwórz drugi terminal, wyślij komunikaty do loggera i jednocześnie w drugim terminalu obserwuj log poleceniem **tail -f**;

3. Archiwizacja logów.

- Kolejnym zadaniem administratora jest dbanie o to, aby pliki logów nie rozrosły się do wielkich rozmiarów oraz archiwizacja logów (wymagana min. przez prawo)

- Archiwizacja logów często nazywa się rotowaniem logów, do rotowania służy program o nazwie **logrotate**;
- Program logrotate jest uruchamiany codziennie przez demona **cron**;

```
suse:~ # ls -l /etc/cron.daily/logrotate
-rwxr-xr-x 1 root root 587 May 19 2011 /etc/cron.daily/logrotate
```

- Program sprawdza wszystkie zdefiniowane pliki logów i podejmuje zdefiniowane w pliku konfiguracyjnym akcje np. kompresowanie logów, kasowanie logów, liczba zarchiwizowanych plików dziennika;
- Sprawdź plik konfiguracyjny **logrotate**;

```
suse:~ # egrep ^[^\#] /etc/logrotate.conf
weekly
rotate 4
create
dateext
compresscmd /usr/bin/bzip2
uncompresscmd /usr/bin/bunzip2
include /etc/logrotate.d
```

- Powyższy plik mówi, że:
 - pliki logów są tworzone lub zamieniane w tygodniowych odstępach;
 - przetrzymywane są cztery ostatnie pliki logów;
 - stare pliki są zapamiętywane pod zmienioną nazwą i tworzone nowe puste pliki logów;
 - kopie logów są kompresowane (bzip2);
 - pobierane są pliki konfiguracyjne z katalogu **/etc/logrotate.d**;
- Przejrzyj plik konfiguracyjny **/etc/logrotate.d/syslog**;
- Dodaj konfigurację dla logowania grupy local0;
- Utwórz plik **/etc/logrotate.d/local0** i zapisz w nim konfigurację;

```
/var/log/local.debug /var/log/local.info /var/log/local.log
{
    compress
    dateext
    maxage 1
    rotate 5
    size 20
    postrotate
        date >> /var/log/local.info
    endscrip
}
```

- Ręcznie uruchom **logrotate**;

```
suse:~ # logrotate /etc/logrotate.conf
```

- Sprawdź katalog **/var/log**;

```
suse:~ # ls -l /var/log/local*
```

```
-rw-r----- 1 root root    0 Apr 11 10:05 /var/log/local.debug
-rw-r----- 1 root root   90 Apr 11 10:05 /var/log/local.debug-20130411.bz2
-rw-r----- 1 root root   60 Apr 11 10:05 /var/log/local.info
-rw-r----- 1 root root  114 Apr 11 10:05 /var/log/local.info-20130411.bz2
-rw-r----- 1 root root    0 Apr 11 10:05 /var/log/local.log
-rw-r----- 1 root root  136 Apr 11 10:05 /var/log/local.log-20130411.bz2
```

- Sprawdź zawartość zarchiwizowanego pliku;

```
suse:~ # bzcata /var/log/local.info-20130411.bz2
Apr 10 23:40:36 suse user: log: info-1
Apr 10 23:40:44 suse user: log: info-2
Thu Apr 11 10:05:47 CEST 2013
```

- Przejrzyj manual do polecenia **logger**;
- Przejrzyj manuale do poleceń **zcat** i **bzcata**;