

# MikroFAQ o Solarisie/x86 ( admin mode only is now on ).

Autor: Jakub Wartak <[vnull@pcnet.com.pl](mailto:vnull@pcnet.com.pl)>

## ChangeLog:

- ~10–29.08.2006: okres intensywnej Solaryzacji... i powstalo FAQ
- 31.08.2006: sotruss i info o Papillonie

## Spis tresci

Administracja codzienna.....	2
Jak prawidlowo zamykac/restartowac system – slyszalem ze komenda reboot na Solarisie jest “niebezpieczna” ?.....	2
Zapomnialem hasla root-a – ratunku...!!.....	3
Jak wyjsc z sesji zlogin ?.....	3
Jestem zalogowany do zone w trybie konsoli ( -C ), po wybraniu typu terminala nie dziala mi klawisz F2 , co zrobic ?.....	3
Gdzie jest xauth i jako go uzyc aby nie majac uruchomionego serwera X-ow na Solarisie moc zainstalowac np. Oracle / Java Enterprise System ( instalatory graficzne ) ?.....	3
Jak przeczytac mana, ktory jest powiedzmy w /usr/dt/man/man1/dtcostam.1 ?.....	4
Do czego sluzycy plik np. /etc/hba.conf ?.....	4
Uslugi i aplikacje.....	4
Gdzie jest kompilator GCC, MySQL, PgSQL itd ( opensource ) ?.....	4
Jak wylaczyc start serwera X11 ?.....	4
Jak odpalic Apache2 ?.....	5
Chce zmienic parametry startowe np. BINDa. Jak to zrobic ?.....	5
Jak ustawic date z serwera NTP ?.....	5
Chcialbym cos skompiowac statycznie ( dla wydajnosci, bezpieczenstwa etc. ) - jak to zrobic ?.....	6
Jak sledzic wykonywane przez aplikacje odwołania do bibliotek wspoldzielonych ( *.so ) ? .....	6
Bezpieczenstwo.....	6
Chcialbym zastosowac mocniejsze szyfrowanie hasla niz to obecne w /etc/shadow. Jak to osiagnac ?.....	6
Jak ograniczyc dostep do SSH tylko dla wybranych hostow ?.....	7
Jak zmylic remote OS detection ( nmap/queso ) ?.....	7
Czy sa jakies moduly kernela zwiakszajace bezpieczenstwo Solarisa ( zakaz ladowania modulow itd. ) ?..	8
Hardware.....	8
Jak sprawdzic czy system dziala w 32-bitach ?.....	8
Jak montowac CD-ROM ktory widziany jest jako IDE Secondary Master ( gdy VOLD nie dziala ) ?.....	8
Jak zmusic VOLDa do podmontowania nowych urzadzen ( CD, floppy ) ?.....	8
Jak wlaczyc DMA dla CD-ROMu ?.....	8
Jak wyswietlic konfiguracje PCI ?.....	9
Jak wyswietlic informacje o procesorze(-ach) ?.....	9
Mam (Open)Solarisa zainstalowanego pod VMware i czasami przestaje mi dzialac wirtualna karta pcn0 ( chipset AMD ).....	9
Co oznacza “CPU has 0 MCU Banks: expected 5: disabling MCA on this CPU” podczas startu systemu? .....	9
Co oznacza “MPO disabled because memory is interleaved” podczas bootowania ?.....	10
Optymalizacja i nadzor nad systemem.....	10
Jak przestawic system w tryb 32-bitowy z 64-bitowego (bardzo x86/GRUB specyficzne) ?.....	10
Czy da sie jakos zablokowac mozliwosc wyswietlania uzytkownikom wyswietlania wszystkich procesow	

w systemie ?.....	11
Klienci korzystajacy z mojego serwera dostaja bledy "connection refused". Co moze zrobic zeby podniesc wydajnos i wyeliminowac te bledy ?.....	11
Jak sprawdzic ilosc wolnej oraz calkowitej pamieci fizycznej ?.....	12
Jak sprawdzic uzywane tablice partycji oraz wykorzystanie swapa ?.....	12
Jakich bibliotek uzywa pid X ?.....	12
Jakie pliki ma otwarte PID x ?.....	12
Jakie pliki ma podmapowane do wlasnej przestrzeni adresowej ( mmap(2) ) ?.....	13
Mam program ktory alokuje pamiec, a nastepnie wykonuje funkcje free() - jednakze nie widac zeby proces zmniejszyl swoj rozmiar ( nie oddaje zwolnionej pamieci do VM Solarisa), czy to jest BUG ??...14	14
Pamiec wspoldzielona/kolejki komunikatow/semafory ( IPC ):.....	14
Jakie pliki otwiera np. program id ?.....	14
Jak wylaczyc logowanie na konsole ?.....	15
Jak cos wyswietlic na konsoli ( bezposrednio a nie przez syslog(3) ) ?.....	15
Jak sprawdzic wersje systemu ?.....	15
Jak zwiekszyz wielkosc pamieci wirtualnej ( swap ) przy uzyciu pliku ?.....	15
Jak zatrzymac przewijanie sie komunikatow przy startowaniu kernela ?.....	16
Nie odpowiada mi brak katalogu domowego roota. Jak go zalozyc ?.....	16
Storage (ten rozdzial potrzebuje znacznie wiecej q&a ).....	16
Dodalem nowy dysk IDE ( primary slave ). System go jednak nie widzi ?.....	16
Jak sprawdzic ilosc bledow na IDE/SCSI ?.....	17
Jaki system plikow jest na urzadzeniu /dev/dsk/XXXXXX ?.....	17
Jak uzywac cfgadm i devfsadm ?.....	18
Networking.....	18
Jak zmienic adres IP i brame domyslne ? .....	18
Dodalem nowa karte sieciowa – jak dodac ja do systemu ?.....	18
Jak wyswietlic tablice routingu ?.....	19
Czy jest cos podobnego do mii-tool, tj. czy mozna sprawdzic czy sieciowka ma link ?.....	19
Jak moze podejrzec co jest wysylane na porcie TCP <X> ?.....	19
Co oznacza: Aug 20 23:10:01 krogoth ip: [ID 903730 kern.warning] WARNING: IP: Hardware address '00:50:fc:f3:c1:31' trying to be our address 010.099.001.020! ?.....	20
Jak uruchomic firewalla ( ipfilter ) ?.....	20
Jak sprawdzic flow-control i tym podobne na sieciowce ?.....	21
Mam dwie karty sieciowe w jednej podsieci IP, np bge0=1.1.1.10/24 i bge1=1.1.1.20/24, niestety jak wypne jedna karte sieciowa to nie dziala druga.....	22
Pomimo ustawienia DNSow w /etc/resolv.conf hosty dalej sie nie resolwuja, co jest nie tak ?.....	22
Rozne dziwne.....	22
EXPERIMENTAL: Czy w Solarisie mozna zmienic czestotliwosc zegara ( dla zwiekszenia interaktywnosci w Xach, dla sterowania procesami produkcyjnymi ) ?.....	23
Chcialbym zbudowac OpenSolarisa i tam jest do wyboru cos takiego jak BFU – co to znaczy ?.....	23

## Administracja codzienna

### ***Jak prawidlowo zamykac/restartowac system – slyszalem ze komenda reboot na Solarisie jest "niebezpieczna" ?***

Tak to prawda, /sbin/reboot nie uruchamia procedur konczacych dzialanie programow w /etc/init.d/\* i SMF, lecz natychmiastowo zabija ( przez SIGTERM a potem SIGKILL ) procesy. W celu

unikniecia problemow najlepiej stosowac :

*bash-3.00# shutdown -y -i0 -g0 system bedzie wylaczony*

W celu zrebootowania serwera zamiast -g0 nalezy dac -g6.

### **Zapomnialem hasla root-a – ratunku...!!**

W GRUBie wybieramy “Solaris failsafe”.

Zostanie zadane pytanie o to czy podmontowac znalezione systemy jako /a: Wybieramy 'y'.

Dostajemy shella...:

```
# chroot /a /bin/sh
# <-- z tym ze teraz jestesmy juz w naszym systemie
# passwd
# exit
# <-- teraz jestesmy znow w “rescue mode”
# cd /
# umount /a
# reboot
```

### **Jak wyjsc z sesji zlogin ?**

Wpisac szybko: ~. ( tylda kropka )

### **Jestem zalogowany do zone w trybie konsoli ( -C ), po wybraniu typu terminala nie dziala mi klawisz F2 , co zrobic ?**

Zamiast F2 wcisnij ESC+2 ( jednoczesnie – jezeli to nie pomoze, mozesz sprobowac przez tworzenie pliku sysidcfg w /zone/nazwa/root/etc, ew. wybrac inny typ terminala ).

### **Gdzie jest xauth i jako go uzyc aby nie majac uruchomionego serwera X-ow na Solarisie moc zainstalowac np. Oracle / Java Enterprise System ( instalatory graficzne ) ?**

Xauth jest w: */usr/openwin/bin/xauth*

Na hoscie z Xami: *xauth list*

*10.99.1.1:0 MIT-MAGIC-COOKIE-1 cf2af89171ba6c26221e5168056407ea*

```
xeno/unix:0 MIT-MAGIC-COOKIE-1 cf2af89171ba6c26221e5168056407ea
```

```
oracle@db:/ora-install/Disk1$ /usr/openwin/bin/xauth add 10.99.1.1:0 MIT-MAGIC-COOKIE-1  
cf2af89171ba6c26221e5168056407ea
```

```
/usr/openwin/bin/xauth: creating new authority file /export/home/oracle/.Xauthority
```

```
oracle@db:/ora-install/Disk1$ export DISPLAY=10.99.1.1:0
```

```
oracle@db:/ora-install/Disk1$ /usr/openwin/bin/xterm
```

(powinno sie otworzyc okienko xterma na .1 )

albo najlepiej zastosowac X11 Forwarding ( ssh -X )

### **Jak przeczytac mana, ktory jest powiedzmy w /usr/dt/man/man1/dtcostam.1 ?**

```
bash-3.00# cd /usr/dt; man -M . dtconfig
```

### **Do czego sluzyc plik np. /etc/hba.conf ?**

```
bash-3.00# man -f /etc/hba.conf
```

Jezeli nie dziala bo twierdzi ze nie moze znalezc pliku /usr/share/man/windex nalezy zbudowac ten plik:

```
bash-3.00# nice catman &
```

( to potrwa dlugo )

## **Uslugi i aplikacje**

### **Gdzie jest kompilator GCC, MySQL, PostgreSQL itd ( opensource ) ?**

W /usr/sfw/, zwlaszcza w podkatalogu bin/ i sbin/. Linker i pozostale developerskie sa takze w /usr/css/bin/\*

### **Jak wylaczyc start serwera X11 ?**

```
bash-3.00# /usr/dt/bin/dtconfig -d  
done
```

desktop auto-start disabled.

## Jak odpalic Apache2 ?

```
bash-3.00# cd /etc/apache2
bash-3.00# cp httpd.conf-example httpd.conf
bash-3.00# vi httpd.conf
[ ... zmienamy co nas interesuje ... ]

bash-3.00# /usr/apache2/bin/apachectl configtest
Syntax OK
bash-3.00# svcadm enable network/http
```

(Logi sa w /var/apache2/logs/\*)

## Chce zmienic parametry startowe np. BINDa. Jak to zrobic ?

Tutaj dodajemy np. parametr “-d 3” do wywolania nameda.

```
# svccfg -s dns/server:default setprop start/exec = \"/usr/sbin/named -d 3\"
# svcadm restart dns/server
# pgrep -fl named
10211 /usr/sbin/named -d 3
```

## Jak ustawic date z serwera NTP ?

Jednorazowo mozna tak:

```
root@solek:/etc# ntpdate -v ntp.task.gda.pl
17 Aug 11:17:26 ntpdate[616]: ntpdate 3-5.93e+sun 03/06/05 23:16:45 (1.4)
17 Aug 11:17:29 ntpdate[616]: adjust time server 153.19.250.123 offset 0.117171sec
```

Lepiej jednak postawic daemona xntpd ( bedzie regularnie odpytywal serwer czasu ):

```
root@solek:/etc/inet# ln -s ntp.client ntp.conf
root@solek:/etc/inet# svcadm enable network/ntp
root@solek:/etc/inet# ps -ef | grep -i ntp
root 673 671 0 11:24:38 ?        0:00 /usr/sbin/ntpdate -s -m 224.0.1.1
root 671 7 0 11:24:38 ?        0:00 /sbin/sh /lib/svc/method/xnt
```

Tutaj widac ze dziala defaultowa konfiguracja – daemon jedynie czeka na pakiety NTP po multicascie – zeby np. uzywac jakiegos serwera/ow nalezy przeedytowac plik /etc/inet/ntp.conf i zostawic jedyna linijke odkomentowana w stylu:  
*server pl.pool.ntp.org.*

(Liste serwerow dostepnych pod tym aliasem mozna sprawdzic przez: *host -t any pl.pool.ntp.org* )

Nastepnie dajemy:

```
root@solek:/etc# svcadm restart network/ntp
```

## **Chcialbym cos skompiowac statycznie ( dla wydajnosci, bezpieczenstwa etc. ) - jak to zrobic ?**

Podobno Solaris nie wspiera standardowo statycznego linkowania, bo nie ma standardowo bibliotek statycznych ( tych z rozszerzeniem “.a” ).

```
root@solek:~# !gcc
gcc a.c -Wall -static
ld: fatal: library -lc: not found
ld: fatal: File processing errors. No output written to a.out
collect2: ld returned 1 exit status
```

Wiecej info tutaj:

[http://blogs.sun.com/roller/page/rie?entry=static\\_linking\\_where\\_did\\_it](http://blogs.sun.com/roller/page/rie?entry=static_linking_where_did_it)  
<http://www.deer-run.com/~hal/sol-static.txt>

## **Jak sledzic wykonywane przez aplikacje odwolania do bibliotek wspoldzielonych ( \*.so ) ?**

```
bash-3.00# man sotruss
```

## **Bezpieczenstwo**

### **Chcialbym zastosowac mocniejsze szyfrowanie hasla niz to obecne w /etc/shadow. Jak to osiagnac ?**

```
bash-3.00# cd /etc/security
```

```
bash-3.00# vi policy.conf
```

Znajdz linie `CRYPT_DEFAULT=__unix__` , zahashuj ja i dodaj pod nia:

```
CRYPT_DEFAULT=2a
```

“2a” oznacza ze do szyfrowania ma zostac uzyty szyfr Blowfish ( patrz plik: crypt.conf )

Nalezy jeszcze wszystkim uzytkownikom zmienic hasla, tak aby zostaly one zaszyfrowane nowym algorytmem ( do tego czasu beda dalej w starej formie w /etc/shadow ).

A dlaczego akurat uzywam Blowfisha ?

```
vnull@xeno:~$ /usr/sbin/John -test
```

[..]

*Benchmarking: FreeBSD MD5 [32/32]... DONE*

*Raw: 5066 c/s real, 5311 c/s virtual*

*Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE*

*Raw: 307 c/s real, 321 c/s virtual*

[..]

Liczba "c/s" świadczy o ilości szyfrowan na sekundę jaka może osiągnąć tutaj John The Ripper. Oczywiście im mniej tym lepiej.

### **Jak ograniczyć dostęp do SSH tylko dla wybranych hostów ?**

```
bash-3.00# mv -f /etc/hosts.allow /etc/hosts.allow.old
```

```
bash-3.00# cat > /etc/hosts.allow
```

```
sshd: 10.97.1.0/255.255.255.0 : allow
```

```
sshd: 127.0.0.1: allow
```

```
sshd: ALL: deny
```

```
CTRL+D
```

( a najlepiej dać ALL: ALL: deny ale wtedy może zostać zabroniony dostęp do innych usług )

```
bash-3.00# chmod 644 /etc/hosts.allow
```

### **Jak zmylić remote OS detection ( nmap/queso ) ?**

Głównie używając nmap można wpłynąć na różnorakie parametry stosu TCP/IP. Np:

```
nmap -set /dev/tcp tcp_ipv4_ttl 128
```

```
# nmap pokazuje: Sun Solaris 9 with TCP_STRONG_ISS set to 2
```

```
nmap -set /dev/tcp tcp_strong_iss 2
```

Ja jednak wykorzystałem IpFilter - dokładnie ta konfiguracja z tego dokumentu daje coś podobnego do:

*Device type: general purpose|webcam*

*Running (JUST GUESSING) : Microsoft Windows NT/2K/XP|95/98/ME (92%), AXIS embedded (86%)*

*Aggressive OS guesses: Microsoft Windows XP Pro SP1 (92%), Microsoft Windows XP Pro SP1 or Windows 2000 SP3 (92%), Microsoft Windows Millennium Edition (Me) (88%), Microsoft Windows 2000 Pro SP4 (88%), Axis 200+ Web Camera running OS v1.42(86%), Microsoft Windows NT 4.0 Terminal Server Edition (85%)*

*No exact OS matches for host (test conditions non-ideal).*

## **Czy sa jakies moduly kernela zwikszajace bezpieczenstwo Solarisa ( zakaz ladowania modulow itd. ) ?**

Jest Papillon ( <http://www.roqe.org/papillon/> ). Ochrona stosu jest zaimplementowana w Solarisie ale tylko dla procesorow to wspierajacych ( x86-64 i SPARCi ).

## **Hardware**

### **Jak sprawdzic czy system dziala w 32-bitach ?**

```
bash-3.00# isainfo -k -v  
64-bit amd64 kernel modules
```

### **Jak montowac CD-ROM ktory widziany jest jako IDE Secondary Master ( gdy VOLD nie dziala ) ?**

```
bash-3.00# mkdir -p /mnt/cdrom  
bash-3.00# mount -o ro -F hsfs /dev/dsk/c1t0d0p0 /mnt/cdrom
```

Mozemy tez zrobic sobie symlink, zeby nie uzywac dlugiej nazwy urzadzenia tylko intuicyjnie /dev/cdrom:

```
bash-3.00# ln -s /dev/dsk/c1t0d0p0 /dev/cdrom
```

### **Jak zmusic VOLDa do podmontowania nowych urzadzen ( CD, floppy ) ?**

```
bash-3.00# volcheck
```

### **Jak wlaczyc DMA dla CD-ROMu ?**

```
bash-3.00# eeprom atapi-cd-dma-enabled=1
```

## **Jak wyświetlić konfigurację PCI ?**

```
bash-3.00# /usr/X11/bin/scanpci  
( wymaga zainstalowanego środowiska X11R6 )
```

## **Jak wyświetlić informacje o procesorze(-ach) ?**

```
bash-3.00# psrinfo -v
```

## **Mam (Open)Solarisa zainstalowanego pod VMware i czasami przestaje mi działać wirtualna karta pcn0 ( chipset AMD )...**

To jest (znany) problem pomiędzy VMware/kernel Solarisa:

1. Wylacz całe VMware ( aplikacje GUI, nie tylko sesje systemu ).
2. Znajdz plik o rozszerzeniu .vmx w katalogu gdzie trzymasz obraz systemu ( na systemie hoscie ).
3. Dodaj ( na koncu ):  
ethernet0.virtualDev = "e1000"  
To zmieni typ emulowanej karty sieciowej na Intel PRO/1000 GigabitEthernet.
4. Wystartuj na nowo system, sieciowka przestanie być widoczna jako pcn0 a zacznie jako e1000g0 dlatego musisz przekonfigurować sieć, nowa karta sieciowa powinna być widoczna:  
bash-3.00# dmesg | grep e1000

Najłatwiej przekonfigurować przez: `mv /etc/hostname.pcn0 /etc/hostname.e1000g0 && reboot`

## **Co oznacza "CPU has 0 MCU Banks: expected 5: disabling MCA on this CPU" podczas startu systemu?**

MCU to skrót od Machine Check Architecture, Linux też to ma - monitoruje CPU czy wszystko jest OK ( przegrzanie, etc).

Komunikat informuje że mimo że linia procesorów powinna mieć takie rozszerzenie to go nie ma – więc wylacza cały monitoring.

## Co oznacza "MPO disabled because memory is interleaved" podczas bootowania ?

MPO to Multiprocessor Opteron. Ma to cos wspolnego z NUMA. Pojawialo mi sie w VMware ale zadnych problemow nie sprawia taki komunikat.

## Optymalizacja i nadzor nad systemem

### Jak przestawic system w tryb 32-bitowy z 64-bitowego (bardzo x86/GRUB specyficzne) ?

```
bash-3.00# cd /boot/grub
bash-3.00# cp menu.lst menu.lst.old
```

kopiujemy te pierwsze linie i zmienamy, u mnie bylo tak ( dodane/zmiany na czerwono ):

```
#----- ADDED BY BOOTADM - DO NOT EDIT -----
title Solaris 10 6/06 s10x_u2wos_09a X86 32bit mode
root (hd0,0,a)
kernel /platform/i86pc/multiboot kernel/unix
module /platform/i86pc/boot_archive
#-----END BOOTADM-----
```

Powyzszy fragment musi sie znalezc przed tym co skopiowalismy ( jako pierwszy ).

Sprawdzamy czy GRUB widzi zmiany:

```
bash-3.00# bootadm list-menu
The location for the active GRUB menu is: /boot/grub/menu.lst
default 0
timeout 10
0 Solaris 10 6/06 s10x_u2wos_09a X86 32bit mode
1 Solaris 10 6/06 s10x_u2wos_09a X86
2 Solaris failsafe
```

Zapisujemy:

```
bash-3.00# bootadm update-archive
```

uwaga: nie jestem pewien czy po prostu nie wystarczy zrobic jakiegos wpisu przez eeprom(1) ,  
chyba boot-file=kernel/unix

```
bash-3.00# reboot
```

Po reboocie powinno byc widac zmiane:

```
bash-3.00# isainfo -k -v
32-bit i386 kernel modules
```

## **Czy da sie jakos zablokowac mozliwosc wyswietlania uzytkownikom wyswietlania wszystkich procesow w systemie ?**

Do /etc/security/profile.conf nalezy dopisac na koncu:

```
PRIV_DEFAULT=basic
```

```
PRIV_LIMIT=all,!proc_info
```

a nastepnie sie przelogowac i sprawdzic czy zmiany odniosly skutek:

```
-bash-3.00$ ps -ef
```

```
  UID  PID  PPID  C  STIME TTY      TIME CMD
vnull 100968 100965  0 11:49:33 pts/1    0:00 -bash
vnull 100965 100946  0 11:49:33 ?        0:01 /usr/lib/ssh/sshd
vnull 101720 101717  0 12:07:01 ?        0:00 /usr/lib/ssh/sshd
vnull 101722 101720  0 12:07:01 pts/2    0:00 -bash
vnull 101726 101722  0 12:07:05 pts/2    0:00 ps -ef
```

```
-bash-3.00$ /usr/ucb/ps uaxww
```

```
USER      PID %CPU %MEM  SZ  RSS TT   S  START TIME COMMAND
vnull    101722  0.2  0.2 2624 1984 pts/2  S 12:07:00 0:00 -bash
vnull    101720  0.2  0.3 7912 2256 ?     S 12:07:00 0:00 /usr/lib/ssh/sshd
vnull    101727  0.2  0.2 2140 1964 pts/2  O 12:07:09 0:00 /usr/ucb/ps -uaxww
vnull    100965  0.0  0.3 7912 2248 ?     S 11:49:33 0:00 /usr/lib/ssh/sshd
vnull    100968  0.0  0.2 2624 1924 pts/1  S 11:49:33 0:00 -bash
-bash-3.00$
```

## **Klienci korzystajacy z mojego serwera dostaja bledy "connection refused". Co moge zrobic zeby podniesc wydajnosc i wyeliminowac te bledy ?**

Zwiekszamy ilosc polaczen nawiazanych ( zakonczony three-way-handshake ) ktore moga wisiec w accept-queue, tj. odebranych przez kernel, ale ktorych aplikacja jeszcze nie "odebrala" -- wiecej info: `man 2 accept`

```
bash-3.00# ndd -set /dev/tcp tcp_conn_req_max_q 2048
```

Zwiekszamy ilosc obslugiwanych polaczen ktore jeszcze nie zakonczyly three-way-handshake ( SYN, SYN-ACK, ACK ) :

```
bash-3.00# ndd -set /dev/tcp tcp_conn_req_max_q 2048
```

Nalezy jeszcze podniesc ilosc dostepnych deskryptorow dla kazdego procesu.

## **Jak sprawdzic ilosc wolnej oraz calkowitej pamieci fizycznej ?**

```
bash-3.00# vmstat 1
kthr  memory      page      disk      faults  cpu
r b w  swap free re  mf pi po fr de sr cd f0 s1 -- in sy cs us sy id
0 0 0 840028 369148 23 50 30 0 1 0 44 4 0 0 0 315 316 163 1 4 95
0 0 0 835244 356756 0 42 11 0 0 0 0 0 0 0 0 308 97 67 3 2 95
0 0 0 835244 356756 0 0 0 0 0 0 0 0 0 0 0 308 57 60 1 1 98
^C
```

Interesujace kolumny to 4-ta i 5-ta.

```
bash-3.00# prtconf | grep ^Mem
Memory size: 512 Megabytes
```

## **Jak sprawdzic uzywane tablice partycji oraz wykorzystanie swapa ?**

```
bash-3.00# swap -l
swapfile      dev swaplo blocks free
/dev/dsk/c0d0s1 102,1      8 1048568 1048568
```

```
bash-3.00# swap -s
total: 46212k bytes allocated + 19560k reserved = 65772k used, 835380k available
```

## **Jakich bibliotek uzywa pid X ?**

```
bash-3.00# pldd 624
624: bash
/lib/libcurses.so.1
/lib/libsocket.so.1
/lib/libnsl.so.1
/lib/libdl.so.1
/lib/libc.so.1
```

## **Jakie pliki ma otwarte PID x ?**

```
bash-3.00# pfiles 624
624: bash
Current rlimit: 256 file descriptors
0: S_IFCHR mode:0620 dev:270,0 ino:12582918 uid:100 gid:7 rdev:24,1
O_RDWR|O_NOCTTY|O_LARGEFILE
/devices/pseudo/pts@0:1
```

```

1: S_IFCHR mode:0620 dev:270,0 ino:12582918 uid:100 gid:7 rdev:24,1
  O_RDWR|O_NOCTTY|O_LARGEFILE
  /devices/pseudo/pts@0:1
2: S_IFCHR mode:0620 dev:270,0 ino:12582918 uid:100 gid:7 rdev:24,1
  O_RDWR|O_NOCTTY|O_LARGEFILE
  /devices/pseudo/pts@0:1
3: S_IFDOOR mode:0444 dev:279,0 ino:63 uid:0 gid:0 size:0
  O_RDONLY|O_LARGEFILE FD_CLOEXEC door to nscd[97]
  /var/run/name_service_door
255: S_IFCHR mode:0620 dev:270,0 ino:12582918 uid:100 gid:7 rdev:24,1
  O_RDWR|O_NOCTTY|O_LARGEFILE FD_CLOEXEC
  /devices/pseudo/pts@0:1

```

### **Jakie pliki ma podmapowane do własnej przestrzeni adresowej ( mmap(2) ) ?**

```

bash-3.00# pmap 624
624:  bash
08045000   12K rw---  [ stack ]
08050000   528K r-x--  /usr/bin/bash
080E3000   76K rwx--  /usr/bin/bash
080F6000   96K rwx--  [ heap ]
FEDB1000    4K rwxs-  [ anon ]
FEDC0000    4K rwx--  [ anon ]
FEDD0000  736K r-x--  /lib/libc.so.1
FEE98000   24K rw---  /lib/libc.so.1
FEE9E000    8K rw---  /lib/libc.so.1
FEEB0000   24K rwx--  [ anon ]
FEEC0000  512K r-x--  /lib/libnsl.so.1
FEF40000   20K rw---  /lib/libnsl.so.1
FEF45000   32K rw---  /lib/libnsl.so.1
FEF50000   44K r-x--  /lib/libsocket.so.1
FEF6B000    4K rw---  /lib/libsocket.so.1
FEF70000    4K rwx--  [ anon ]
FEF80000  136K r-x--  /lib/libcurses.so.1
FEFB2000   28K rw---  /lib/libcurses.so.1
FEFB9000    8K rw---  /lib/libcurses.so.1
FEFC0000    4K r-x--  /lib/libdl.so.1
FEFC9000  132K r-x--  /lib/ld.so.1
FEFFA000    4K rwx--  /lib/ld.so.1
FEFFB000    8K rwx--  /lib/ld.so.1
total    2448K

```

Jak widac to jest ta sama wartosc zwracana co przez ps ( 2448Kilobajtow ):

```
bash-3.00# /usr/ucb/ps uax | grep ' 624 '
```

```
root    624  0.2  0.4 2448 1632 pts/1  R 20:37:50  0:00 bash
```

**Mam program który alokuje pamięć, a następnie wykonuje funkcję free() - jednakże nie widac zeby proces zmniejszył swój rozmiar ( nie oddaje zwolnionej pamięci do VM Solarisa), czy to jest BUG ??**

Nie to nie jest BUG, większość UNIXów tak robi. Jeżeli chcesz żeby pamięć jednak była zwracana do systemu skompiluj program z dodatkowym parametrem/biblioteka -lmapmalloc, czyli zamiast:

```
$ gcc testmem.c -o testmem
```

należy dać

```
$ gcc testmem.c -o testmem -lmapmalloc
```

Przyczyna takiej implementacji jest założenie że aplikacja nawet jeśli zwolni pamięci to i tak jej będzie potrzebować. Nawet jeżeli pamięć będzie zaalokowana, ale nieużywana, to system ją i tak zeswajuje.

### **Pamięć współdzielona/kolejki komunikatów/semafony ( IPC ):**

```
bash-3.00# ipcs
```

```
IPC status from <running system> as of Thu Aug 10 20:44:35 CEST 2006
```

```
T    ID  KEY      MODE      OWNER  GROUP
```

```
Message Queues:
```

```
Shared Memory:
```

```
Semaphores:
```

(Jak widac powyzej nie ma zadnych mechanizmow IPC uzywanych na tym systemie – przykladowa aplikacja ktora z tego korzysta jest Oracle :) )

Do usuwania IPC sluzzy polecenie: *ipcrm*

### **Jakie pliki otwiera np. program id ?**

```
bash-3.00# truss -t open /usr/bin/id
```

```
open("/var/ld/ld.config", O_RDONLY)      Err#2 ENOENT
```

```
open("/usr/lib/libproject.so.1", O_RDONLY) = 3
```

```
open("/lib/libc.so.1", O_RDONLY)        = 3
```

```
open("/lib/libsecdb.so.1", O_RDONLY)    = 3
```

```
open("/lib/libproc.so.1", O_RDONLY)     = 3
```

```
open("/lib/libnsl.so.1", O_RDONLY)      = 3
```

```
open("/lib/libcmd.so.1", O_RDONLY)      = 3
```

```
open("/lib/librtld_db.so.1", O_RDONLY)  = 3
```

```
open("/lib/libelf.so.1", O_RDONLY)      = 3
```

```
open("/lib/libctf.so.1", O_RDONLY)      = 3
```

```
open64("/var/run/name_service_door", O_RDONLY) = 3
uid=0(root) gid=0(root)
```

## **Jak wyliczyc logowanie na konsole ?**

Zakomentowac w /etc/syslog.conf nastepujace wpisy:

```
*.err;kern.notice;auth.notice          /dev/sysmsg
*.alert;kern.err;daemon.err            operator
*.alert                                  root
*.emerg                                  *
```

A nastepnie:

```
bash-3.00# svcadm refresh system-log
```

## **Jak cos wyswietlic na konsoli ( bezposrednio a nie przez syslog(3) ) ?**

```
bash-3.00# echo "cos" > /dev/sysmsg
```

## **Jak sprawdzic wersje systemu ?**

```
bash-3.00# cat /etc/release
Solaris 10 6/06 s10x_u2wos_09a X86
Copyright 2006 Sun Microsystems, Inc. All Rights Reserved.
Use is subject to license terms.
Assembled 09 June 2006
```

```
bash-3.00# uname -a
SunOS solek 5.10 Generic_118855-14 i86pc i386 i86pc
```

Jeszcze nalezy pamietac o *showrev*

## **Jak zwiekszyc wielkosc pamieci wirtualnej ( swap ) przy uzyciu pliku ?**

```
root@solek:~# mkfile 128m /swapfile1
root@solek:~# swap -l
swapfile          dev swaplo blocks free
/dev/dsk/c0d0s1   102,1      8 1048568 1048568
```

Mozna tez VI-em :)

```
root@solek:~# grep ^/dev/dsk/c0d0s1 /etc/vfstab | sed 's/^\dev\dsk\c0d0s1\//swapfile1/g' > /tmp/aa.$$
```

```
root@solek:~# cat /tmp/aa.$$ >> /etc/vfstab
root@solek:~# rm /tmp/aa.$$
```

Sprawdzenie #1:

```
root@solek:~# grep swap /etc/vfstab
/dev/dsk/c0d0s1 - - swap - no -
/swapfile1 - - swap - no -
swap - /tmp tmpfs - yes -
```

Dodanie bez reboota:

```
root@solek:~# swap -a /swapfile1
```

Sprawdzenie ostateczne:

```
root@solek:~# swap -l
swapfile      dev  swaplo  blocks  free
/dev/dsk/c0d0s1  102,1  8 1048568 1048568
/swapfile1     -      8 204792 204792
```

### **Jak zatrzymać przewijanie się komunikatów przy startowaniu kernela ?**

Ponizsze kombinacje przydają się na konsoli w czasie startowania kernela w trybie verbose lub debug:

**CTRL+S** zatrzymuje bootowanie ( pauza )

**CTRL+Q** wznowia bootowanie

### **Nie odpowiada mi brak katalogu domowego roota. Jak go założyć ?**

```
bash-3.00# mkdir -m 700 /root
bash-3.00# chmod -d /root root
bash-3.00# mv ./[a-zA-Z0-9]* /root/
```

**JASS** automatycznie tworzy katalog /root.

### **Storage (ten rozdział potrzebuje znacznie więcej q&a )**

#### **Dodałem nowy dysk IDE ( primary slave ). System go jednak nie widzi ?**

```
root@solek:/etc# touch /reconfigure && reboot
```

Teraz dysk powinien już być widoczny jako /dev/dsk/c0d1\*

`root@solek:/etc# format`

Wybieramy że chcemy używać całego dysku dla Solarisa.

`root@solek:/etc# fdisk /dev/rdisk/c0d1p0`

`root@solek:/etc# prtvtoc /dev/rdisk/c0d1p0`

`* /dev/rdisk/c0d1p0 partition map`

`*`

`* Dimensions:`

`* 512 bytes/sector`

`[..]`

`* Flags:`

`* 1: unmountable`

`* 10: read-only`

`[..]`

`*`

`First Sector Last`

`* Partition Tag Flags Sector Count Sector Mount Directory`

`2 5 01 0 202752 202751`

`8 1 01 0 2048 2047`

`9 9 00 2048 4096 6143`

`root@solek:/etc# newfs /dev/rdisk/c0d1s2`

`newfs: construct a new file system /dev/rdisk/c0d1s2: (y/n)? y`

`/dev/rdisk/c0d1s2: 202752 sectors in 99 cylinders of 64 tracks, 32 sectors`

`99.0MB in 7 cyl groups (16 c/g, 16.00MB/g, 7680 i/g)`

`super-block backups (for fsck -F ufs -o b=#) at:`

`32, 32832, 65632, 98432, 131232, 164032, 196832,`

## **Jak sprawdzić ilość błędów na IDE/SCSI ?**

`root@solek:~# iostat -iE`

`sd16 Soft Errors: 7 Hard Errors: 0 Transport Errors: 0`

`Vendor: NECVMWar Product: VMware IDE CDR10 Revision: 1.00 Device Id:`

`Size: 3.02GB <3024814080 bytes>`

`Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0`

`Illegal Request: 7 Predictive Failure Analysis: 0`

## **Jaki system plików jest na urządzeniu /dev/dsk/XXXXXX ?**

`bash-3.00# fstyp /dev/dsk/c0d0s0`

`ufs`

## **Jak uzywac cfgadm i devfsadm ?**

```
cfgadm -c unconfigure cX
cfgadm -c configure cX
devfsadm -Cv
```

Gdzie cX to numer kontrolera do reinicjalizacji.  
( notka z grupy: pl.comp.os.unix )

## **Networking**

### **Jak zmienic adres IP i brame domyslne ?**

Nalezy przeedytowac nastepujace pliki:

```
/etc/defaultrouter
/etc/hosts
/etc/inet/*
/etc/netmasks
```

Po czym wykonac reboot.

### **Dodalem nowa karte sieciowa – jak dodac ja do systemu ?**

Na poczatek musimy ustalic jak sie nazywa, najlepiej komenda *dmesg*, a nastepnie:

```
bash-3.00# ifconfig pcn0 plumb
```

Teraz sprawdzamy czy jest widoczna:

```
bash-3.00# ifconfig pcn0
pcn0: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 0.0.0.0 netmask 0
    ether 0:c:29:bd:cf:6f
bash-3.00# echo 10.97.1.3 > /etc/hostname.pcn0
bash-3.00# echo 10.97.1.1 > /etc/defaultrouter
bash-3.00# echo -e "10.97.1.0 255.255.255.0" >> /etc/netmasks
```

A na koniec recznie podnosimy zebyśmy nie musieli restartowac serwera:

```
bash-3.00# ifconfig pcn0 10.97.1.3/24 up
bash-3.00# ping -s 10.97.1.3 1000 1
PING 10.97.1.3: 1000 data bytes
```

1008 bytes from 10.97.1.3: icmp\_seq=0. time=1.04 ms

----10.97.1.3 PING Statistics----

1 packets transmitted, 1 packets received, 0% packet loss  
round-trip (ms) min/avg/max/stddev = 1.04/1.04/1.04/-NaN

## Jak wyświetlić tablice routingu ?

```
bash-3.00# netstat -r -n
```

Routing Table: IPv4

Destination	Gateway	Flags	Ref	Use	Interface
10.97.1.0	10.97.1.3	U	1	0	pcn0
224.0.0.0	127.0.0.1	U	1	0	lo0
127.0.0.1	127.0.0.1	UH	8	135	lo0

## Czy jest coś podobnego do mii-tool, tj. czy można sprawdzić czy sieć ma link ?

```
bash-3.00# dladm show-dev
```

```
e1000g0 link: up speed: 1000 Mbps duplex: full
```

Poza tym jest też kilka ciekawych rzeczy ( polecam: `man dladm` ).

## Jak mogę podejrzeć co jest wysyłane na porcie TCP <X> ?

```
bash-3.00# snoop -P port 22
```

```
Using device /dev/pcn0 (non promiscuous)
```

```
10.97.1.1 -> 10.97.1.3 TCP D=22 S=36567 Push Ack=486060690 Seq=309854475 Len=48  
Win=10568 Options=<nop,nop,tstamp 3969889 406549>
```

```
10.97.1.1 -> 10.97.1.3 TCP D=22 S=36567 Ack=486060738 Seq=309854523 Len=0  
Win=10568 Options=<nop,nop,tstamp 3969891 406595>
```

```
10.97.1.1 -> 10.97.1.3 TCP D=22 S=36567 Push Ack=486060738 Seq=309854523 Len=48  
Win=10568 Options=<nop,nop,tstamp 3970350 406595>
```

```
10.97.1.1 -> 10.97.1.3 TCP D=22 S=36567 Ack=486060786 Seq=309854571 Len=0  
Win=10568 Options=<nop,nop,tstamp 3970351 406641>
```

( prawie jak tcpdump ;) )

**Co oznacza: Aug 20 23:10:01 krogoth ip: [ID 903730 kern.warning] WARNING: IP: Hardware address '00:50:fc:f3:c1:31' trying to be our address 010.099.001.020! ?**

Taki własnie komunikat mozna dostac w dmesgu w przypadku konfliktu adresow IP.

## **Jak uruchomic firewalla ( ipfilter ) ?**

```
bash-3.00# cd /etc/ipf
```

Odkomentujemy drivery sieciowek na ktorych chcemy miec IPF

```
bash-3.00# vi pfil.ap
```

```
bash-3.00# cat > ipf.conf << EOF
```

```
# by vnull 2006
```

```
#
```

```
# ruch na loopbacku
```

```
#
```

```
pass in quick on lo0 all
```

```
pass out quick on lo0 all
```

```
#
```

```
# fw -> ALL, polityka: przepuszczamy wszystko
```

```
#
```

```
pass out quick on e1000g0 all keep state
```

```
#
```

```
# ALL -> fw, polityka: blokowac wszystko na co nie pozwalamy
```

```
#
```

```
block in log on e1000g0 all # bez quick
```

```
# tniemy wszystko co za krotkie
```

```
block in quick on e1000g0 proto tcp all with short
```

```
# pakiety z source routingem
```

```
# oczywiscie... (nie) szanujemy ich ;]
```

```
block in quick on e1000g0 all with opt ssrr
```

```
block in quick on e1000g0 all with opt lsrr
```

```
# xmas/os detection(nmap)
```

```
block return-rst in log quick on e1000g0 proto tcp from any to any flags FUP
```

```
# syn-fin scan
```

```
block return-rst in log quick on e1000g0 proto tcp from any to any flags SF/SFRA
```

```
# null scan
```

```
block return-rst in log quick on e1000g0 proto tcp from any to any flags /SFRA
```

```
# blokujemy wszelkie nadmiarowe opcje IP – moze cos wyciac za bardzo
```

block in quick on e1000g0 all with ipopts

```
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type echo keep frags
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type echorep keep frags
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type squench keep frags
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type paramprob keep frags
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type timex keep frags
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 icmp-type unreachable keep frags
```

```
# TODO/FIXME packet-too-big ??
# jeszcze mozna byloby sobie wpuscic UDP ~32000 (traceroute udp)
```

```
pass in quick on e1000g0 proto icmp from any to 10.97.1.3 keep state
pass in quick on e1000g0 proto udp from any to 10.97.1.3 port = 53 keep state # named
pass in quick on e1000g0 proto tcp from any to 10.97.1.3 port = 22 flags S keep state
block return-rst in quick on e1000g0 proto tcp from any to 10.97.1.3 port = 111 flags S/SA keep state
```

EOF

```
bash-3.00# svcadm restart network/pfil
bash-3.00# svcadm enable network/ipfilter
```

Mozna tez inaczej, ale idziemy po najmniejszej linii oporu...

```
bash-3.00# reboot
```

Najlepiej teraz sprawdzic Nmap-em jakie porty sa dostepne z innego komputera. A lokalnie mozemy sprawdzic statystyke IpFiltera nastepujaco:

```
bash-3.00# ipfstat | grep packets
bad packets:      in 0 out 0
IPv6 packets:     in 0 out 0
input packets:    blocked 1 passed 619 nomatch 0 counted 0 short 0
output packets:   blocked 0 passed 419 nomatch 0 counted 0 short 0
input packets logged: blocked 1 passed 0
output packets logged: blocked 0 passed 0
packets logged:   input 0 output 0
```

## **Jak sprawdzic flow-control i tym podobne na sieciowce ?**

```
# ndd -get /dev/bge0 link_status
# ndd -get /dev/bge0 link_speed
# ndd -get /dev/bge0 link_duplex
```

Flow-control == 802.3x ( wiecej na stronie Cisco ):

```
# ndd -get /dev/bge0 link_rx_pause # odbior ( jak 1 to wspiera )
# ndd -get /dev/bge0 link_tx_pause # a tutaj pause frames dla wysylu ( jak 1 to wspiera )
```

**Mam dwie karty sieciowe w jednej podsieci IP, np bge0=1.1.1.10/24 i bge1=1.1.1.20/24, niestety jak wypne jedna karte sieciowa to nie dziala druga.**

Dwie ( i wiecej ) kart sieciowych podpietych do jednej podsieci nie sa wspierane bez specjalnych zabiegów.

Rozwiazaniem moze byc stworzenie urzadzenia agregujacego – tzw. bonding z linuxa, LACP ( man dladm ) i przypisaniu mu dwóch adresów IP lub tez wykorzystanie IP MultiPath ( IPMP ) - wiecej na stronach SUNa.

**Pomimo ustawienia DNSow w /etc/resolv.conf hosty dalej sie nie resolwuja, co jest nie tak ?**

Zapewne libc nie jest skonfigurowane aby korzystac z DNSow ( lecz jedynie z pliku /etc/hosts ):

```
root@solek:/etc# cp nsswitch.dns nsswitch.conf
```

Sprawdzamy:

```
root@solek:/etc# host -v www.wp.pl
```

```
Trying "www.wp.pl"
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 730
```

```
:: flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
:: QUESTION SECTION:
```

```
;www.wp.pl. IN A
```

```
:: ANSWER SECTION:
```

```
www.wp.pl. 1939 IN A 212.77.100.101
```

```
Received 43 bytes from 10.99.1.4#53 in 29 ms
```

10.99.1.4 to w tym wypadku nasz nameserver z /etc/resolv.conf

**Rozne dziwne...**

***EXPERIMENTAL: Czy w Solarisie mozna zmienic czestotliwosc zegara ( dla zwiekszenia interaktywnosci w Xach, dla sterowania procesami produkcyjnymi ) ?***

Standardowo Solaris uzywa 1000 taktow zegara na sekunde. Mozna to zmienic przez wpisy do /etc/system:

```
set hires_tick=1  
set hires_hz=10000
```

Dodatkowa informacja: z dokumentacji jadra Linuxa wynika ze czestotliwosc pracy rowna:

- a) 100HZ – jest najlepsza dla serwerow, batch computing itd
- b) 250HZ – jest dobra dla serwerow, ale zachowuje rozsadni poziom interaktywnosci
- c) 1000HZ – jest najlepsza dla desktopow, rola komputera jako systemu czasu prawie rzeczywistego

***Chcialbym zbudowac OpenSolarisa i tam jest do wyboru cos takiego jak BFU – co to znaczy ?***

BFU = Blasting Fast Upgrade czyli upgade bez kompilacji w skrocie ( bardzo szybki, ale tez czasami niebezpieczny ).