< Linux

Linux diagnosztika

- **Szerző:** Sallai András

- Web: http://szit.hu

DNS

host

A host tartományok és zónák adatait kérdezi le névkiszolgálóktól.

A következő parancs egy tartományhoz tartozó MX rekordot kérdezi le:

```
host -t MX szit.hu
```

Az eredmény valami ilyesmi:

```
szit.hu mail is handled by 5 mail.szit.hu.
```

Ezzel megtudtuk, ha valaki egy szit.hu tartományra küld leveleket, akkor azokat a mail.szit.hu szerver fogja kezelni, azaz fogadni.

A tartományhoz elérhető zónainformációk lekérdezése:

```
host -t any szit.hu
```

Lehetséges eredmény:

```
szit.hu mail is handled by 5 mail.szit.hu.
szit.hu has SOA record ns.tdns1.net. hostmaster.cpserver.net. 2011102801
10800 3600 3600000 3600
szit.hu name server ns.tdns1.net.
szit.hu name server ns.tdns2.net.
szit.hu has address 84.21.31.224
```

dig

DNS szerver diagnosztizálása

A '@' karakter után adjuk meg szóközök nélkül a lekérdezett DNS szervert:

```
dig @szervercim amelydomaintszeretnem
```

```
dig szit.hu any +noall +answer
```

```
; <<>> DiG 9.7.3 <<>> szit.hu any +noall +answer
;; global options: +cmd
szit.hu.                3600        IN        MX        5 mail.szit.hu.
szit.hu.                3600        IN        SOA        ns.tdns1.net.
hostmaster.cpserver.net. 2011102801 10800 3600 3600000 3600
szit.hu.                3600        IN        NS        ns.tdns2.net.
szit.hu.                3600        IN        NS        ns.tdns1.net.
szit.hu.                3600        IN        A        84.21.31.224
```

nslookup

```
nslookup -ty=any szit.hu
```

```
Server:         84.2.44.1
Address:        84.2.44.1#53

Non-authoritative answer:
szit.hu
        origin = ns.tdns1.net
        mail addr = hostmaster.cpserver.net
        serial = 2011102801
        refresh = 10800
        retry = 3600
        expire = 3600000
        minimum = 3600
szit.hu nameserver = ns.tdns2.net.
szit.hu nameserver = ns.tdns1.net.
Name:   szit.hu
Address: 84.21.31.224
szit.hu mail exchanger = 5 mail.szit.hu.

Authoritative answers can be found from:
mail.szit.hu    internet address = 84.21.31.224
```

Az nslookup paraméter nélkül indítva egy interaktív program, amely parancsokat vár az indítása után.

Hálózat

socat

Leírás

Több célú kétirányú adatforgalom kezelő. A man socat elég hosszan taglalja a lehetőségeket.

Telepítése

```
apt-get install socat
```

Vagy a legújabb:

- http://www.dest-unreach.org/socat/download/

Használat

Például tesztelhetjük a levelezőszerverünket:

```
socat - TCP4:localhost:25
```

```
220 evelin ESMTP Postfix (Debian/GNU)
ehlo vagyok
250-evelin
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
```

Portot irányíthatunk át:

```
socat TCP4-LISTEN:8000 TCP4:debian.org:www
```

Persze ez a második kérést már nem szolgálja ki.

Ez utóbbi például a mi gépünk 8000-es portjára érkező minden kérést átirányít a debian.org IP címéhez tartozó webszerver főoldalára.

```
socat TCP4-LISTEN:8000,fork TCP4:debian.org:www
```

Így több kérést is fogad, sőt, minden egyes kérésre újabb socat szállat indít.

Egy démon rögtönzése:

```
socat - TCP-LISTEN:5555,crlf
```

Csak szerveroldalon szakítható meg.

Ha csak olvasni akarom a foglalatot:

```
socat readline TCP-LISTEN:5555,crlf
```

mtr

Leírás

Az mtr egy teljesképernyős ncurses és X11 alapú tracroute program. Ping paranccsal megvalósított nyomkövetést tesz lehetővé (traceroute).

(A traceroute képes csomagok nyomkövetésére. Kideríthetjük milyen routereken ment keresztül a csomagunk)

Telepítés

```
apt-get install mtr
```

Használat

Az mtr X felülete indul el, ha érzékeli a grafikus felületet. Ellenkező esetben ncurses módban fut. Akármelyik felületen vagyunk elég beírni mtr:

```
mtr
```

A program interaktív, kilépni a „Q” billentyű lenyomásával lehet.

Azonban grafikus felületen is rávehetjük az ncurses módra:

```
mtr -t
```

vagy

```
mtr --curses
```

Egyéb paraméter nélkül a localhostra küld folyamatosan pinget. Ha megadunk számára egy tartománynevet, akkor az adott címre fog echo request parancsokat küldeni, miközben mutatja az eredményt.

A használatához a célgépnek válaszolni kell a ping parancsra.

arp

Leírás

Az ARP tábla lekérdezése, manipulálása.

Telepítés

Az arp parancs a net-tools csomagban van. Telepítés:

```
apt-get install net-tools
```

Használat

A -n kapcsoló lebeszéli a programot a host, port és felhasználói nevek feloldásáról. Az arp -n és arp parancs egyazon kimenetet adja, de a -n gyorsabb. Ha nincs más kapcsoló, akkor érdemes a -n kapcsolót használni:

```
arp -n
```

Lehetséges válasz:

```
Address                  HWtype  HWaddress           Flags Mask
Iface
192.168.5.100            ether   08:00:27:98:43:27   C
eth0
192.168.5.1              ether   00:14:78:ef:fe:88   C
eth0
```

Más paraméter nélkül lekérdezzük az arp táblánkat.

arping

Telepítés

Az arping parancs a vele azonos nevű csomagban van. A telepítés:

```
apt-get install arping
```

Használat

```
arping 00:14:78:ef:fe:88
```

Eredmény:

```
ARPING 00:14:78:ef:fe:88
60 bytes from 111.111.111.111 (00:14:78:ef:fe:88): icmp_seq=0 time=1.649
msec
60 bytes from 111.111.111.111 (00:14:78:ef:fe:88): icmp_seq=1 time=1.234
msec
60 bytes from 111.111.111.111 (00:14:78:ef:fe:88): icmp_seq=2 time=1.231
msec
60 bytes from 111.111.111.111 (00:14:78:ef:fe:88): icmp_seq=3 time=1.209
msec
60 bytes from 111.111.111.111 (00:14:78:ef:fe:88): icmp_seq=4 time=1.234
msec
^C
--- 00:14:78:ef:fe:88 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
^C
```

jnettop

Leírás

Hálózati forgalom figyelése. A jnettop egy interaktív felületen biztosítja a forgalom valósidejű figyelését.

Telepítés

```
apt-get install jnettop
```

Használat

```
jnettop
```

Kilépés: Q

Beállíthatunk konkrét hálózati kártyát. Például:

```
jnettop -i eth1
```

Alkalmas szippantó tevékenységre (promiscuous mód) is.

```
jnettop -p
```

vagy

```
jnettop --promiscuous
```

A -x vagy –filter kapcsolókkal szűrési szabályokat adhatunk meg. A szűrési szabályok szintaxisa megegyezik a tcpdump szintaktikájú. Használatához lásd a tcpdump(1) kézikönyvet.

iptraf

Leírás

Az iptraf egy menüs csomag és kapcsolatmonitorozó eszköz, ncurses alapokon.

Telepítés

```
apt-get install iptraf
```

Indítás

```
iptraf
```

traceroute

Leírás

Csomagok nyomonkövetése a hálózaton.

Futtatás

Szeretnénk megnézni a szit.hu domainig, hány csomóponton megy át a csomagunk.

```
traceroute -I szit.hu
```

Eredmény:

```
traceroute to szit.hu (195.21.31.224), 30 hops max, 60 byte packetes
1  * * *
2  * * *
3  * * *
4  * * *
5  * * *
6  * * *
7  * * *
8  * * *
9  zold.and (195.21.31.224)  30.308 ms 32.644 ms  35.827 ms
```

- A -I ICMP csomagokat küld.
- A -T syn jelzős TCP csomagokat küld.

netstat

Hálózati kapcsolatok, routing tábla, hálózati eszközök, maszkolt kapcsolatok, csoportos átvitel megjelenítése.

```
netstat -nt
```

A fenti példában, például nem szeretném feloldani a számokat nevekké (-n kapcsoló), és csak TCP kapcsolatokat szeretném látni (-t kapcsoló).

A MySQL milyen porton hallgatózik:

```
netstat -tap | grep mysql
```

Az eredmény ilyen lehet:

```
tcp                        0              0          localhost:mysql
*:*              LISTEN
1026/mysqld
```

iptstate

Leírás

A iptstate egy top szerű program az iptables kapcsolatkövető táblájának (state tábla) megtekintéséhez.

Telepítés

```
apt-get install iptstate
```

Használat

```
iptstate
```

Honlap

- http://www.phildev.net/iptstate/

tcpdump

A hálózati forgalom figyelése

A echo request kéréseket szeretnénk:

```
tcpdump 'icmp[icmptype] == icmp-echo'
```

Minden olyan csomagot szeretnék, amely nem visszhang kérés és nem visszhang válasz:

```
tcpdump 'icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply'
```

A helyi géről a 192.168.5.1-es gépekre haladó csomagok:

```
tcpdump net 192.168.5.1
```

A webes forgalom figyelése:

```
tcpdump -A -s 0 port 80
```

netcat

Írás és olvasás a hálózati forgalomba.

Például kapcsolódjunk egy SMTP szerverhez:

```
nc localhost 25
```

lnstat

A hálózatról ad információkat.

A /proc/net/stat/ állományait lehet vele listázni fájl és kulcsok alapján.

A fájloké és kulcsok listáját adja:

```
lnstat -d
```

Fájlok és kulcsok megadásával szűrhetünk:

```
lnstat -k arp_cache:entries, rt_cache:in_hit,arp_cache:destroys
```

nstat

Hálózati statisztika.

Az nstat futtatása önmagában ehhez hasonló eredményeket produkál:

```
IpInReceives                    65816              0.0
IpInAddrErrors                  2                  0.0
IpInDelivers                    65794              0.0
IpOutRequests                   54342              0.0
...
```

routel

A routing kiíratása szebb formában. Legalábbis szándék szerint.

ss

A socketek vizsgálata.

Az összes socket megtekintése:

```
ss -a
```

Hallgatózó socketek:

```
ss -l
```

A hallgatózó socketeket milyen folyamat tartja fent:

```
ss -l -p
```

route

A routingtábla kiíratása és változtatása.

Paraméter nélkül kiírja a routing táblát:

```
route
```

Lehetséges eredmény:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.5.0     *               255.255.255.0   U     1      0        0 eth0
default         192.168.5.1     0.0.0.0         UG    0      0        0 eth0
```

Az eredményből látjuk, hogy az alapértelmezett átjáró a 192.168.5.1, vagyis ezen keresztül érjük az internetet.

ip

A routing tábla kezelése.

Az ip parancsnak meg kell adni egy objektumot. Lehetséges objektumok:

- link

- addr
- addrlabel
- route
- rule
- neigh
- tunnel
- maddr mroute
- monitor

```
ip route show
```

Lehetséges eredmény:

```
192.168.5.0/24 dev eth0  proto kernel  scope link  src 192.168.5.4  metric 1
default via 192.168.5.1 dev eth0  proto static
```

Az eth0 linkjének megtekintése:

```
ip link show eth0
```

Lehetséges eredmény:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 1000
    link/ether 00:50:8d:7c:ab:04 brd ff:ff:ff:ff:ff:ff
```

nmap

Nyitott portok keresése.

```
apt-get install nmap
```

Grafikus felülettel:

```
apt-get install zenmap
```

Rootként futtatható zenmap paranccsal.

Használat:

```
nmap localhost
```

Nézzük meg, hogy a 192.168.16.0 hálózatban van-e 445-ös part nyitva.

```
nmap -sT 192.168.16.1-254 -p 445
```

openvas

```
apt-get openvas-client openvas-server
```

Nem biztonságos portok keresése.

iftop

Leírás

A hálózati eszköz forgalmának figyelése.

Telepítés

```
apt-get install iftop
```

Használat

```
iftop
```

Kilépés: q

A „h” billentyűvel újabb használható billentyűket tekinthetünk meg. Kisbetű és nagybetű különböző!

A „P” (nagy P billentyű) megállítja a képernyőt. Ez hasznos lehet, mivel a program valós időben mutatja a történéseket.

A „p” (kis p billentyű) a port megjelenítést kapcsolja ki vagy be.

tsharp

Hálózati analizátor

Igaz nem grafikus program, de igen jó hasznát vehetjük. A hálózati forgalmat tudjuk analizálni. Rootként kell futtatni.

```
tshark 'port ftp or ftp-data'
```

wireshark

A hálózati forgalmat tudjuk analizálni. Rootként kell futtatni.

```
apt-get install wireshark
```

Filter:

```
pop and ip.src==192.168.5.4
```

A fenti filterben csak a 110 portot célzó és 192.168.5.4-es IP címről érkező csomagokat szeretnénk látni.

De ugyanezt leírhatjuk így is:

```
tcp.port eq 110 and ip.src==192.168.5.4
```

Egy http forgalomban keresünk valamit:

```
http contains tartalom
```

Filterbeállításokról:

- http://wiki.wireshark.org/DisplayFilters

etherape

Leírás

A hálózati forgalmat tudjuk vele figyelni. Rootként kell indítani. A program grafikus felületű!

Telepítés

```
apt-get install etherape
```

Weblap:

- http://etherape.sourceforge.net

ngrep

Hálózati csomaganalizátor.

Az eth0 eszközön bejövő forgalmat elkapjuk és a következők szerint megjelenítünk:

- csak TCP alapú
- csak HTTP forgalmat 80 porton
- Csak azokat ahol egy sor elején szerepel a GET vagy a POST külcsszó

```
ngrep -l -q -d eth0 "^GET |^POST " tcp and port 80
```

Telepítés:

```
apt-get install ngrep
```

nast

Leírás

Hálózat analizáló

Telepítés

```
apt-get isntall nast
```

Használat

```
nast
```

Promiscuous módban indul. Ennél több nem szükséges.

A -i kapcsolóval megadható hálózati eszköz is.

```
nast -i eth1
```

A -f vagy --filter kapcsolóval pedig szűrést állíthatunk be.

A szűrő szintaktika a man nast kézikönyv „FILTER SYNTAX” része tartalmazza.

Ncurses felület

Van ncurses alapú felülete. Ez a -G kapcsolóval használhatjuk.

```
nast -G
```

vagy:

```
nast --ncurses
```

Kilépés:

F1 után a menüpontok aktívak lesznek. De az egyes menüpontok külön is elérhetők.

```
(S)niffer   (A)nalyzer   (O)ptions  (F1)
```

Az Options menüben van kilépés menüpont, de a Ctrl+C is segít.

tcpick

Leírás

TCP kapcsolat analizáló.

Telepítés

```
apt-get install tcpick
```

használat

```
tcpick
```

```
man tcpick
```

netsniff-ng

Hálózat analizálás:

```
apt-get install netsniff-ng
```

dsniff

Hálózati sniffer

```
apt-get install dsniff
```

hunt

Hálózatbiztonsági analizátor.

```
apt-get install hunt
```

darkstat

Hálózati forgalom gyűjtése.

```
apt-get install darkstat
```

snort

Hálózatfigyelő

```
apt-get install snort
```

lsof

Az lsof a nyitott fájlok listázására való, de megmondja, azt is melyik portot mi tartja nyitva -i kapcsolóval:

```
lsof -i
```

fuser

Folyamatok azonosítására találták ki.

Mely folyamatok használják a 80-as portot?

```
fuser www/tcp
```

```
www/tcp:              1474 10284 22123 22124 22125 22126 22127
```

nbtscan

Az nbtscan csommaggal telepszik:

```
apt-get install nbtscan
```

NetBIOS nevek keresése. NetBIOS státusz kérést küld minden címre a megadott hálózatban, majd a kapott információt olvasható formában közli. Kapunk egy IP címet, egy NetBIOS számítógépnevet, a bejelentkezett felhasználó nevét és a MAC címet.

Például:

```
nbtscan -r 192.168.16.0/24
```

Eredmény:

```
Doing NBT name scan for addresses from 192.168.16.0/24

IP address        NetBIOS Name         Server           User
MAC address
------------------------------------------------------------------------------
-----------------------
192.168.16.0     Sendto failed: Permission denied
192.168.16.21    <unknown>                             <unknown>
192.168.16.20    C16-20                                <unknown>
00:19:66:ef:58:cc
192.168.16.255   Sendto failed: Permission denied
192.168.16.252   FILESERVER           <server>         FILESERVER
00:00:00:00:00:00
192.168.16.253   SERVER               <server>         SERVER
00:00:00:00:00:00
```

hping3

Tetszőleges TCP/IP csomagok küldése a hálózat gépeinek.

A hping3 parancs a vele azonos nevű csomagban van. A telepítése tehát a következő:

```
apt-get install hping3
```

sntop

Curses alapú hálózati top program.

```
(sntop) simple network top
HOST                STATUS          COMMENT
Gator               DOWN            local linux/alpha server
Yahoo               UP              something on the outside
localhost           UP              does loopback even work?

3 hosts polled: 2 up, 1 down
```

netdiscover

Hálózati címkereső, amely arp kérésekkel kérdezi le a hálózatokat.

```
apt-get install netdiscover
```

honeyd

Egy virtuális hostot hoz létre.

```
apt-get install honeyd
```

Weblap:

- http://www.honeyd.org/

A telepítés után a honeyd paranccsal indítható, de ne tegyük meg a dokumentáció olvasása nélkül!

xprobe

Távoli rendszer operációs rendszerének lekérdezése.

Telepítés:

```
apt-get install xprobe
```

Használat:

```
xprobe2
```

resolvconf

A DNS szerverekről az információkat karbantartja.

```
apt-get install resolvconf
```

httest

Webszerver és kliens tesztelő, teljesítménymérő.

```
apt-get install httest
```

sendemail

SMTP email kliens

```
apt-get install sendemail
```

Nem tévesztendő össze a levelezőszerverrel (sendmail) !

mz

```
apt-get install mz
```

Csomag és hálózati forgalom generátor. Mindenféle érvényes és érvénytelen csomag generálható vele. VoIP és multicast hálózatok tesztelésére kiváló.

Folyamatok

strace

Rendszerhívások nyomonkövetése.

ptrace

Folyamatok nyomonkövetése.

atop

A rendszer és a folyamatok statisztikája.

```
apt-get install atop
```

Kernel

lsmod

Az elérhető kernelmodulok listázása

dmesg

Rendszerüzenetek

Egyéb

```
cat /proc/version
```

Hardver

htop

Rendszer figyelő

```
  CPU[|||||                    15.9%]     Tasks: 337 total, 1 running
  Mem[||||||||||||||||||||832/1518MB]     Load average: 0.26 0.21 0.12
  Swp[|                       8/486MB]     Uptime: 02:22:03

  PID USER     PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 4006 andras    20   0  284M  169M  132M S  5.0 11.1  1:09.86
/usr/lib/virtualbo
 2596 andras    20   0  284M   99M 26824 S  3.0  6.6  4:46.19
/opt/google/chrome
 1258 root      20   0 69100 22692  9156 S  3.0  1.5  3:01.92 /usr/bin/Xorg
```

```
:0 -
 4142 andras    20   0  2624  1348   984 R  1.0  0.1  0:01.03 htop
 3999 andras    20   0  284M  169M  132M S  1.0 11.1  0:14.51
/usr/lib/virtualbo
 2449 andras    20   0  172M 32636 17612 S  1.0  2.1  0:09.43
/opt/google/chrome
 2823 andras    20   0 91492 12552  9708 S  0.0  0.8  0:04.27 gnome-terminal
 2617 andras    20   0  172M 32532 17736 S  0.0  2.1  0:04.57
/opt/google/chrome
 2419 andras    20   0  452M  105M 35560 S  0.0  6.9  3:04.59
/opt/google/chrome
 3948 andras    20   0  174M 31700 17836 S  0.0  2.0  0:02.65
/opt/google/chrome
 2492 andras    20   0  185M 37100 21920 S  0.0  2.4  0:05.73
/opt/google/chrome
    1 root      20   0  2032   644   608 S  0.0  0.0  0:00.95 init [2]
  414 root      16  -4  2532   636   424 S  0.0  0.0  0:00.08 udevd --daemon
  988 daemon    20   0  1808   404   400 S  0.0  0.0  0:00.00 /sbin/portmap
 1000 statd     20   0  1936   644   640 S  0.0  0.0  0:00.02
/sbin/rpc.statd
 1162 root      20   0 27448  1276  1044 S  0.0  0.1  0:00.00
/usr/sbin/rsyslogd
 1172 root      20   0 27448  1276  1044 S  0.0  0.1  0:00.00
/usr/sbin/rsyslogd
F1Help  F2Setup F3SearchF4InvertF5Tree  F6SortByF7Nice -F8Nice +F9Kill
F10Quit
```

free

```
free -m
```

df

```
df -h
```

du

Lemezfoglaltság összegzése.

Célszerű egy konkrét könyvtárra alkalmazni, mert teleírja a képernyőt.

vnstat

Virtuális memória statisztika.

```
apt-get install vnstat
```

lspci

A PCI kártyák listázása.

```
00:00.0 Host bridge: nVidia Corporation nForce3 250Gb Host Bridge (rev a1)
00:01.0 ISA bridge: nVidia Corporation nForce3 250Gb LPC Bridge (rev a2)
00:01.1 SMBus: nVidia Corporation nForce 250Gb PCI System Management (rev a1)
00:02.0 USB Controller: nVidia Corporation CK8S USB Controller (rev a1)
00:02.1 USB Controller: nVidia Corporation CK8S USB Controller (rev a1)
00:02.2 USB Controller: nVidia Corporation nForce3 EHCI USB 2.0 Controller
(rev a2)
```

lsusb

Az USB eszközök listázása.

```
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 001 Device 002: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

lshw

Jelenlévő hardverek listázása.

Előtt telepítés szükséges:

```
apt-get install lshw
```

dmidecode

Információk a hardverről.

powertop

Laptop akumlátorfigyelő.

iostat

Processzor statisztika.

Telepítés:

```
apt-get install sysstat
```

De innen jönnek még a következő parancsok:

- mpstat
- pidstat
- sadf
- sar.sysstat

Egyéb

```
cat /proc/cpuinfo
```

Merevlemez

bonnie++

Merevlemez diagnózis.

blkid

Blokk eszköz tulajdonságainak kiíratása.

Persze ez is segíthet:

```
ls -l /dev/disk/by-uuid/
```

udevadm

udev kezelés.

hdparm

A háttértárak kezelése.

fdisk

Partíciónáló.

Leggyakrabban használt kapcsoló a -l:

```
fdisk -l
```

Az elérhető partíciókat és tulajdonságaikat listázza.

sfdisk

Partíciónáló.

cfdisk

Menüs partícionáló.

smartctl

Infók a merevlemezről:

```
smartctl -a /dev/sda
```

Health teszt:

```
smartctl -H /dev/sda
```

Bőbeszédű info:

```
smartctrl -x /dev/sda
```

Egyéb

Az elérhető háttértárak:

```
cat /proc/partitions
```

Képernyő

xvinfo

X-Video kiterjesztések

xrandr

A RandR kiterjesztéshez parancssoros kezelőfelület.

```
xrandr
```

```
xrandr --verbose
```

xdpyinfo

Képernyőinformációk

Programozás

```
apt-get install systemtap-sdt-dev
```

```
dtrace
```

Malware

rkhunter

rootkint, backdoor és rootkit kereső.

```
apt-get install rkhunter
```

Egyéb

nmon

Általános bencsmárk program, ncurses alapokon.

```
apt-get install nmon
```

uptime

Mennyi ideje fut a rendszer.

```
21:11:11 up 15 min,  2 users,  load average: 0.06, 0.10, 0.17
```

Fájlrendszer

tripwire

Fájlrendszer integritás ellenőrző.

```
apt-get install tripwire
```

Telepítéskor két jelszót fog kérni.

iwatch

```
apt-get install iwatch
```

systraq

```
apt-get install systraq
```

integrit

Fájlintegritás ellenőrző program. Figyelmeztetést kapunk, ha a fájlrendszerben változások történtek az általunk maghatározott helyeken.

Telepítés:

```
apt-get install integrit
```

Weblap:

- http://integrit.sourceforge.net

Rendszer

Curses alapú élő rendszerstatisztika.

```
Hostname  : evelin         Uptime : 00:40:59          Date : 2012-09-29
19:08:02

Load 1    :   0.00   CPU Idle  :  97.76%  Running   :     1   Zombie    :
0
Load 5    :   0.03   CPU System:   0.50%  Sleeping  :   182   Total     :
183
Load 15   :   0.24   CPU User  :   1.74%  Stopped   :     0   No. Users :
5

Mem Total :   1518M  Swap Total:    486M  Mem Used  : 93.52%  Paging in :
0
Mem Used  :   1419M  Swap Used :  15956K  Swap Used :  3.20%  Paging out:
0
Mem Free  : 100756K  Swap Free :    470M  Total Used: 71.61%

Disk Name      Read         Write         Network Interface        rx
tx
sda              0B           0B         lo                       0B
0B
```

```
sdc                0B                0B         eth0                          0B
0B
sdb                0B                0B         pan0                          0B
0B
                                                vboxnet0                      0B
0B
Total              0B                0B
                                                Mount Point                 Free
Used
                                                /mnt/tartaly              33480M
88.36%
```

Link

- http://sectools.org