Outils de Diagnostic de GNU/Linux

Guillaume Chazarain

<Guillaume.Chazarain@sophia.inria.fr>

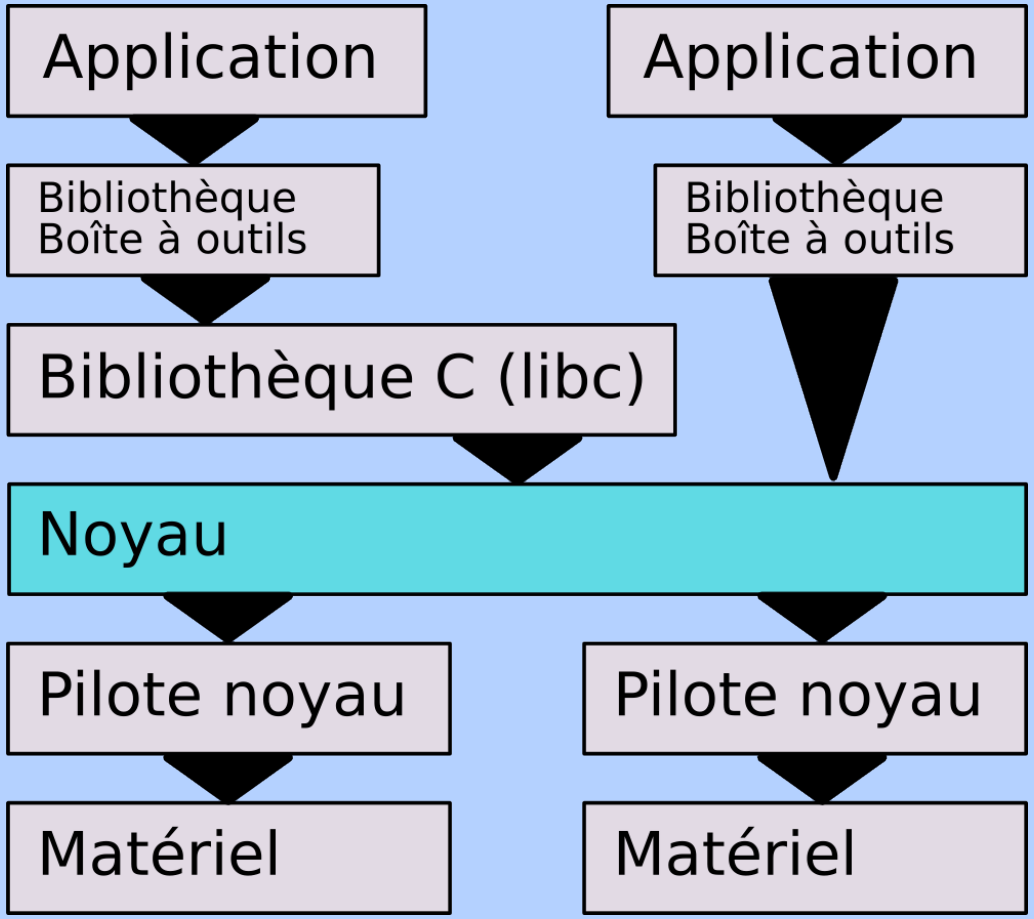
6 Mai 2006 - Journée Méditerranéenne des Logiciels Libres JM2L 2006

Plan

- Généralités
- Système de fichiers
- Mémoire
- Processeur(s)
- Noyau
- Réseau
- Divers

Généralités

- Le noyau est le seul point de passage obligé
- Contact avec l'environnement
- Il fournit donc des informations fiables
- La plupart des outils se basent donc sur ses possibilités



Généralités : `strace`

- Affiche les appels systèmes effectués par un programme
- Et leur résultat
- Ralentit l'exécution
- Surtout si l'affichage est dans un terminal
- Principales options

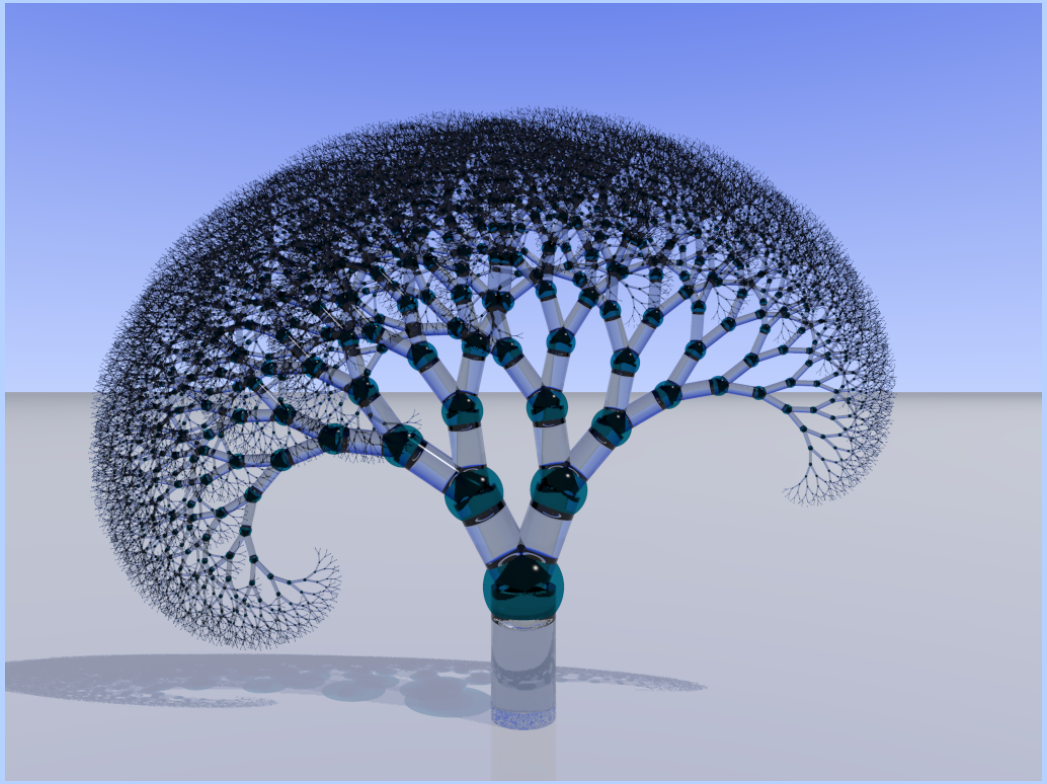
```
alarm(0)                                = 1
rt_sigaction(SIGALRM, {SIG_DFL}, NULL, 8) = 0
open("/etc/passwd", O_RDONLY)           = 6
fcntl64(6, F_GETFD)                     = 0
fcntl64(6, F_SETFD, FD_CLOEXEC)         = 0
fstat64(6, {st_mode=S_IFREG|0644, st_size=1842, ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1,
0) = 0xb7f92000
read(6, "root:x:0:0:root:/root:/bin/zsh\nb"..., 4096) = 1842
close(6)                                = 0
munmap(0xb7f92000, 4096)                = 0
stat64("/dev/pts/0", {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ..
.}) = 0
```

`-p PID` trace un processus existant

`-f` suit les threads/processus fils

Système de fichiers

- Fichiers manquants
- Problèmes de permissions
- Fichiers corrompus



Système de fichiers

- **`strace -e open` *`zsh`***
  - Permet de rapidement voir si un fichier manque

```
[g@localhost ~]$ zsh
compdef:88: failed to load module: zsh/complete
compdef:zle:88: can't load complete module
```

↳ **`open("/usr/lib/zsh/4.2.5/zsh/complete.so", O_RDONLY|O_LARGEFILE) = -1 ENOENT (No such file or directory)`**

Système de fichiers

- **`strace -e file` *`MonProgramme`***
  - Pour les autres manipulations de fichiers

```
...
read(5, "..."..., 4096) = 4096
...
--- SIGABRT (Aborted) @ 0 (0) ---
```

  - Fichier corrompu
    - Chercher avec **`strace`** le **`open(...)`** = *5*
    - **`gdb`** + **`ls -l /proc/PID/fd/5`**

```
[g@localhost ~]$ ls -l /proc/4225/fd/5
lrwx------ 1 g g 64 mai  2 22:53 /proc/4225/fd/5  -> /home/g/JM2L.odp
```

Mémoire

- Difficile à mesurer malgré la simplicité apparente
  - Partage de mémoire
  - Allocations paresseuses

- **`vmstat 1`**

```
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu------
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0    124  95432  24856 543504    0    0     0    72 1577 3753  4  0 96  0  0
 0  0    124  95432  24856 543504    0    0     0     0 1478 3616  2  0 97  0  0
 1  0    124  95432  24856 543504    0    0     0     0 1538 3728  2  1 97  0  0
 0  0    124  95432  24856 543504    0    0     0     0 1522 3691  2  0 97  0  0
 1  0    124  95712  24856 543504    0    0     0     0 1473 3674  4  0 96  0  0
```

- **`/proc/meminfo`**

Mémoire

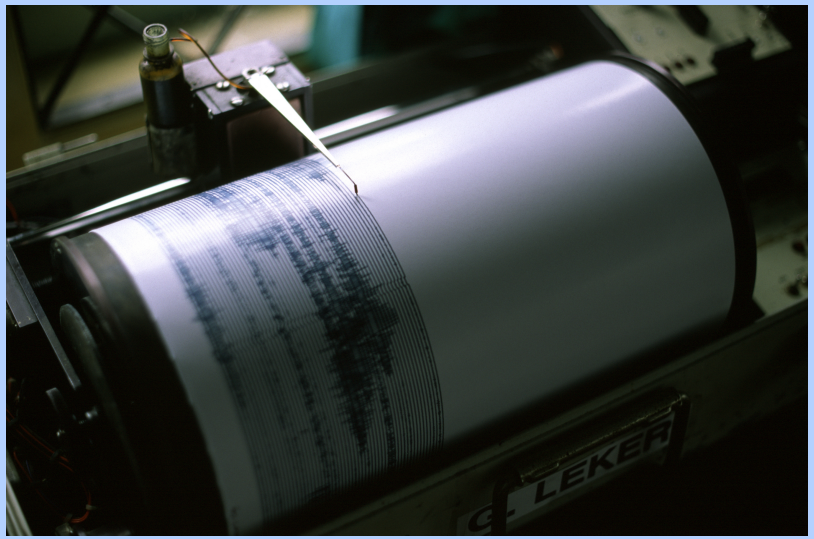
- **xrestop**
  - Mémoire utilisée par le serveur X
- **top/ps**
  - Attention à l'interprétation
- **pmap, /proc/PID/smaps**
  - Affichage détaillé
  - **http://guichaz.free.fr/mem.sh**
- **/proc/PID/status**

```
xrestop - Display: localhost:0
          Monitoring 29 clients. XErrors: 0
          Pixmaps:   20767K total, Other:      59K total, All:   20827K total

res-base Wins  GCs Fnts Pxms Misc    Pxm mem  Other   Total   PID Identifier
2e00000    46  106    1  649   79    16476K     6K  16482K     ?  JM2L.odp -
2600000    78   33    1    8   62      412K     5K    417K     ?  Terminal
2a00000    23   35    0    5   14      408K     1K    410K  4136 NetworkMana
0a00000    11   32    2    2  519      384K    15K    399K  4119 metacity
1200000    87   46    0    4   23      386K     3K    390K  4136 Bottom Pane
1400000    10   42    1    5   15      386K     2K    388K  4138 Bureau
2400000    28   44    0    2   13      384K     1K    385K  4136 mixer_apple
2200000    16   40    0    2   21      384K     1K    385K  4136 WindowNavig
0c00000    15   32    0    2   12      384K     1K    385K  4136 gnome-power
2800000     5   31    0    2   10      384K     1K    385K  4136 cpufreq-app
0600000     2    3    0    2    9      384K   336B    384K  4063 gnome-sessi
3400000     2    2    0    2    9      384K   312B    384K  4460 notify-daem
2000000     6   32    0    2    4        9K  1008B     10K  4136 multiload
3200000     2    1    0    0  364        0B     8K      8K  4239 gnome-scree
0800000     4    1    0    0   82        0B     2K      2K  4117 gnome-setti
1e00000     6   40    0    1    7       4B     1K      1K  4136 ClockApplet
```

```
VmPeak:     3636 kB
VmSize:     3636 kB
VmLck:         0 kB
VmHWM:       436 kB
VmRSS:       436 kB
VmData:      156 kB
VmStk:        84 kB
VmExe:        20 kB
VmLib:      1300 kB
VmPTE:        28 kB
```

Processeur(s)

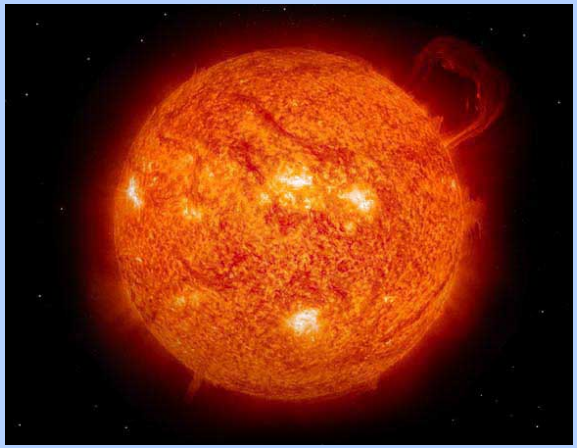
- **`top`, `htop`**
  - **`htop`** pour voir les threads
- **`ltrace`**
  - Appels aux bibliothèques
  - Souvent incomplet
  - **`http://guichaz.free.fr/getenv.sh`**
- **`gdb`, `gstack`**
  - **`thread apply all bt`**



```
[g@localhost ~]$ gstack 4225
Thread 6 (Thread 62401440 (LWP 4226)):
#0  0x002a8402 in __kernel_vsyscall ()
#1  0x00dd2216 in pthread_cond_wait@@GLIBC_2.3.2 () from /lib/libpthread.so.0
#2  0x068fa56c in osl_waitCondition ()
#3  0x06bc1a4d in vos::OCondition::wait ()
#4  0x06bc7319 in vos::OTimerManager::run ()
#5  0x06bc5781 in vos::_cpp_OThread_WorkerFunction ()
#6  0x06bc57af in _OThread_WorkerFunction ()
#7  0x068fd55f in osl_resumeThread ()
#8  0x00dcf3b6 in start_thread () from /lib/libpthread.so.0
#9  0x00bfe33e in clone () from /lib/libc.so.6
Thread 5 (Thread -1365861472 (LWP 4227)):
#0  0x002a8402 in __kernel_vsyscall ()
#1  0x00dd4d88 in accept () from /lib/libpthread.so.0
#2  0x069053ed in osl_acceptPipe ()
#3  0x06bc9eaf in vos::OPipe::accept ()
#4  0x07e882a7 in desktop::OfficeIPCThread::run ()
#5  0x06bc5781 in vos::_cpp_OThread_WorkerFunction ()
#6  0x06bc57af in _OThread_WorkerFunction ()
#7  0x068fd55f in osl_resumeThread ()
```

Noyau

- **`dmesg`**
  - Incontournable si le noyau a détecté une erreur
- **`(Alt)-SysRq-t`**
  - **`echo t > /proc/sysrq-trigger`**
  - Piles d'appel du noyau
- Systemtap/Kprobes
  - Instrumentation du noyau
  - Dernier recours ...



Linux-audit

- Pas encore facilement utilisable
- **auditctl -a exit,always -S open -F auid=500 -F success=0**
- **type=SYSCALL msg=audit(1146599881.325:34787): arch=40000003 syscall=5 success=no exit=-2 a0=8983070 a1=0 a2=1b6 a3=89827a8 items=1 pid=4119 auid=500 uid=500 gid=500 euid=500 suid=500 fsuid=500 egid=500 sgid=500 fsgid=500 comm="metacity" exe="/usr/bin/metacity"**
- **type=CWD msg=audit(1146599881.325:34787): cwd="/home/g"**
- **type=PATH msg=audit(1146599881.325:34787): item=0 name="/home/g/.icons/Bluecurve/index.theme" flags=101**

Réseau

```
$ netstat --tcp --extend --program
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       Utilisatr  Inode      PID/Program name
tcp        0      0 trinidad.inria.fr:35161     bise.inria.fr:ms-wbt-server ESTABLISHED gchazara   2066518    28140/rdesktop

# ethereal -f 'tcp && ((src host trinidad && src port 35161) || (dst host trinidad && dst port 35161))'
```

- Netstat
  - Qui est connecté à qui ?
  - **`netstat --tcp --extend --program`**
- Ethereal
  - Que se disent-ils ?
  - **`ethereal -f 'tcp && port imap'`**

Divers

- **`$SHELL -x` *`ScriptShell`***

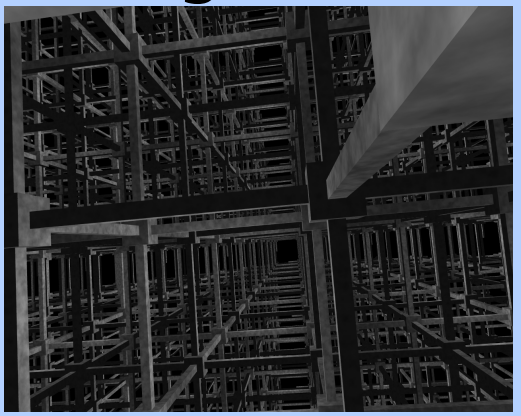
```
+ ALREADY_RUNNING=0
+ '[' 0 -eq 1 ']'
+ MOZARGS=
++ echo fr_FR.UTF-8
++ sed 's|_\([^.]*\).*|-\1|g'
+ MOZLOCALE=fr-FR
+ '[' -f /usr/lib/firefox-1.5.0.2/chrome/fr-FR.jar ']'
+ '[' -z '' ']'
+ exec /usr/lib/firefox-1.5.0.2/firefox

[g@localhost ~]$
```

- **`dbus-monitor`** (pour le futur)

```
signal sender=org.freedesktop.DBus -> dest=(null destination) interface=org.freedesktop.DBus; member=Nam
eOwnerChanged
 string "org.gnome.evince.ApplicationService"
string ""
string ":1.13"
method call sender=:1.13 -> dest=org.freedesktop.DBus interface=org.freedesktop.DBus; member=RequestName
 string "org.gnome.evince.ApplicationService"
uint32 4
signal sender=org.freedesktop.DBus -> dest=(null destination) interface=org.freedesktop.DBus; member=Nam
eOwnerChanged
```

Conclusion

- Nombreuses possibilités d'introspection
  - Du fonctionnement du noyau ...
  - Aux communications inter-application
- Utilisations aussi à but éducatif
  - Compréhension du fonctionnement
  - Pas de tentative de camouflage
- Bonne exploration !!



ethereal
$SHELL -x
dbus-monitor
xrestop
ltrace
strace
netstat
vmstat
top, htop, ps
gdb, gstack
/proc/meminfo
/proc/PID/smaps
/proc/PID/status
dmesg
sysrq
linux-audit
systemtap