If like me you didn’t understand cray logs, make a picture and become a real manager

Sébastien Tricaud

INL

Usenix, San Diego 2008

The Honeynet PROJECT

Approach

Since I started the contest after my talk, I focused on the biggest file: 0809181018.tar.gz

- 415M of logs!
- 4250838 lines!

Approach

Since I started the contest after my talk, I focused on the biggest file: 0809181018.tar.gz

- 415M of logs!
- 4250838 lines!
- Since I am a busy man, I'll make a picture to understand those

0809181018/eventlogs/eventlog

Stats

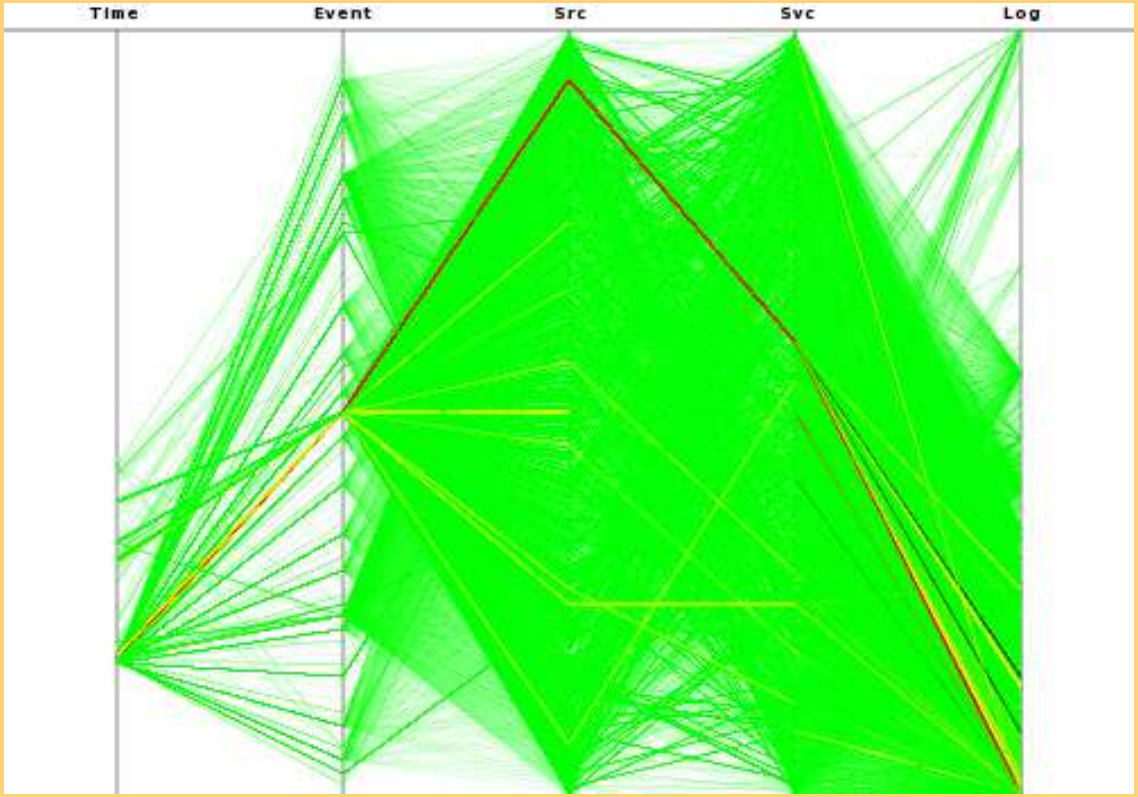
- 34054 lines

First three lines

2008-09-18 04:04:54|2008-09-18 04:04:54|ec_console_log|src:::c0-0c0s3n0|svc:::c0-0c0s3n0|
2008-09-18 04:04:54|2008-09-18 04:04:54|ec_console_log|src:::c0-0c0s3n0|svc:::c0-0c0s3n0|7[?25l[1A[80C[10D[1;32mdone[m8[?25h
2008-09-18 04:04:54|2008-09-18 04:04:54|ec_console_log|src:::c0-0c0s3n0|svc:::c0-0c0s3n0|cat: /sys/class/net/rsip333x1/type

0809181018/eventlogs/eventlog

Picture

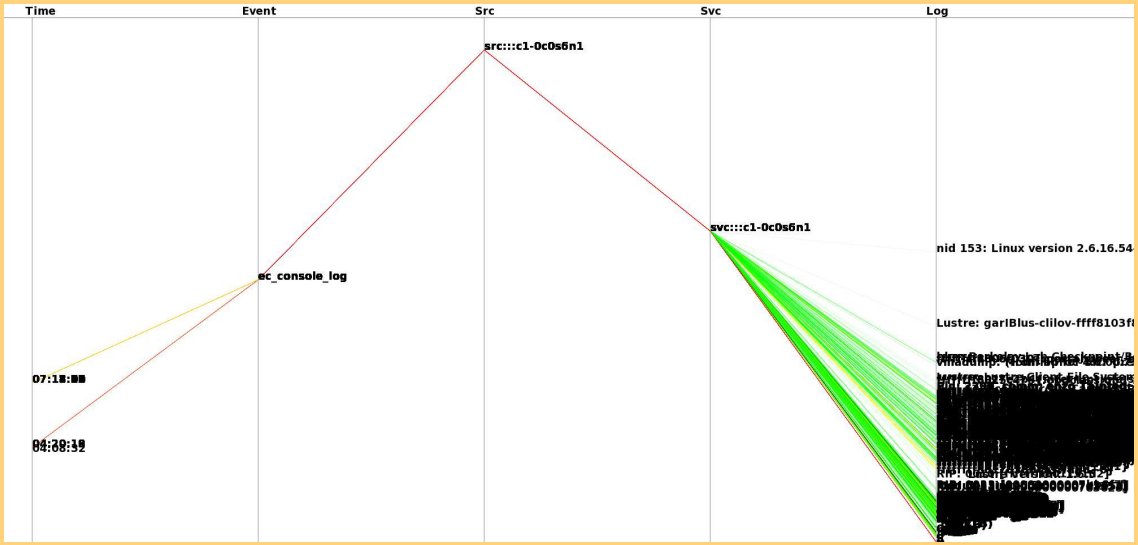


0809181018/eventlogs/eventlog

A **src** value is high frequency

pcv -Tpngcairo event.pcv -Rheatline 'show value = "src:::c1-0c0s6n1" on axis 3' -rra

Frequency filtering

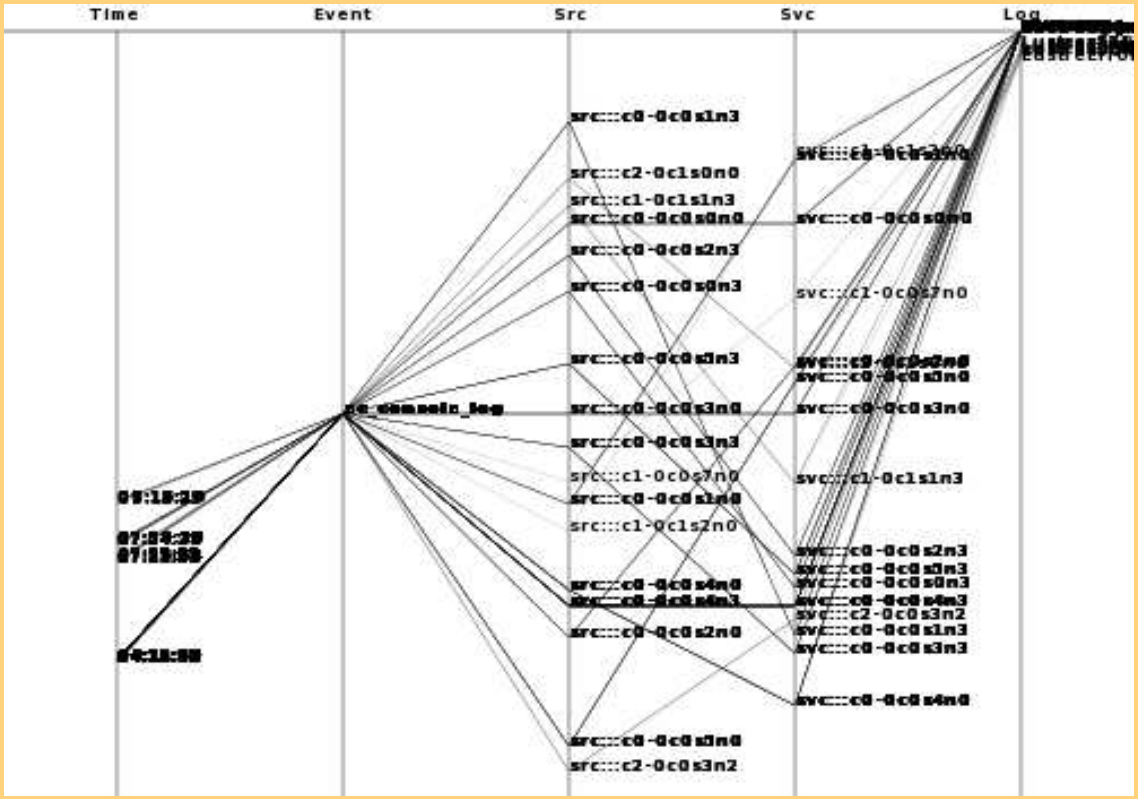


0809181018/eventlogs/eventlog

Look at those log plotted on top on the fifth axis

pcv -Tpngcairo event.pcv 'show plot > 90% on axis 5' -a

Picture



0809181018/eventlogs/eventlog

Data on this axis:

Log #1

Bootdata ok (command line is earlyprintk=rcal0 load_ramdisk=1 ramdisk_size=80000 console=ttyL0 bootnodeip=192.168.0.1 bootproto=ssip bootpath=/rr/current rootfs=nfs-shared root=/dev/sda1 pci=lastbus=3 oops=panic elevator=noop xtrel=2.1.33HD)

Log #2

Bootdata ok (command line is earlyprintk=rcal0 load_ramdisk=1 CMD LINE [earlyprintk=rcal0 load_ramdisk=1 ramdisk_size=80000 console=ttyL0 bootnodeip=192.168.0.1 bootproto=ssip bootpath=/rr/current rootfs=nfs-shared root=/dev/sda1 pci=lastbus=3 oops=panic elevator=noop xtrel=2.1.33HD]

0809181018/eventlogs/eventlog

Data on this axis:

Log #3

Bootdata ok (command line is earlyprintk=rcal0 load_ramdisk=1 Kernel command line: earlyprintk=rcal0 load_ramdisk=1 ramdisk_size=80000 console=ttyL0 bootnodeip=192.168.0.1 bootproto=ssip bootpath=/rr/current rootfs=nfs-shared root=/dev/sda1 pci=lastbus=3 oops=panic elevator=noop xtrel=2.1.33HD

Log #4

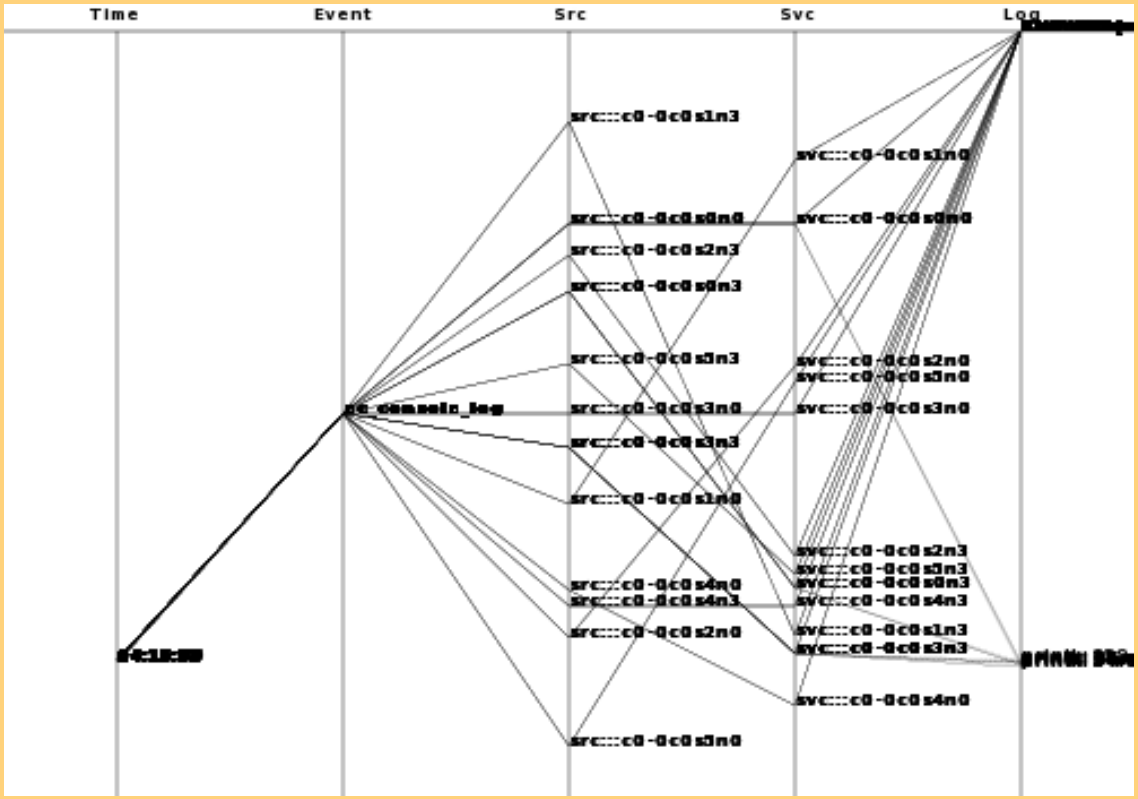
Lustre: garIBlus-OST0005-osc-ffff8103f3fab800: Connection to service garIBlus-OST0005 via nid 19@ptl was lost; in progress operations using this service will wait for recovery to complete.

0809181018/eventlogs/eventlog

I want the printk

pcv -Tpngcairo -Wpcre event.pcv 'show value = ".*printk.*" on axis 5 -a

Picture



0809181018/eventlogs/eventlog

What are those printk on half on the fifth axis?

Log #1

printk: 64 messages suppressed

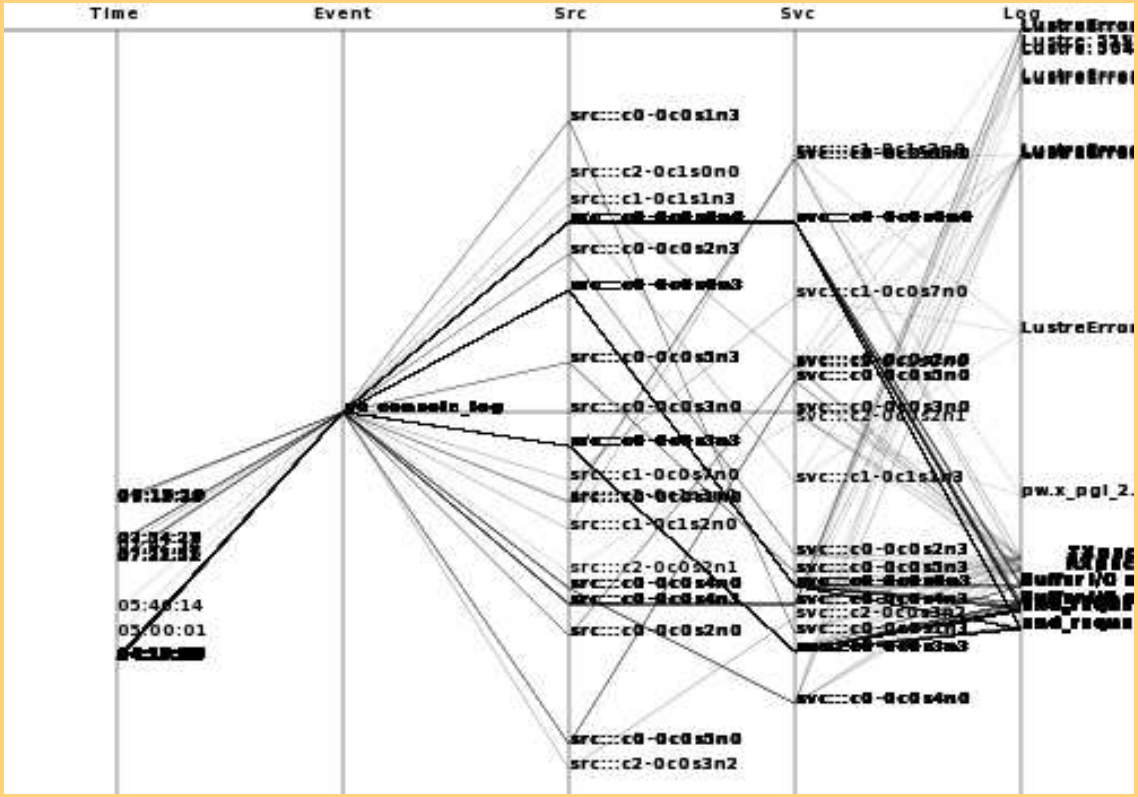
Log #2

printk: 336 messages suppressed

0809181018/eventlogs/eventlog

This are lines carrying *error* on the fifth axis

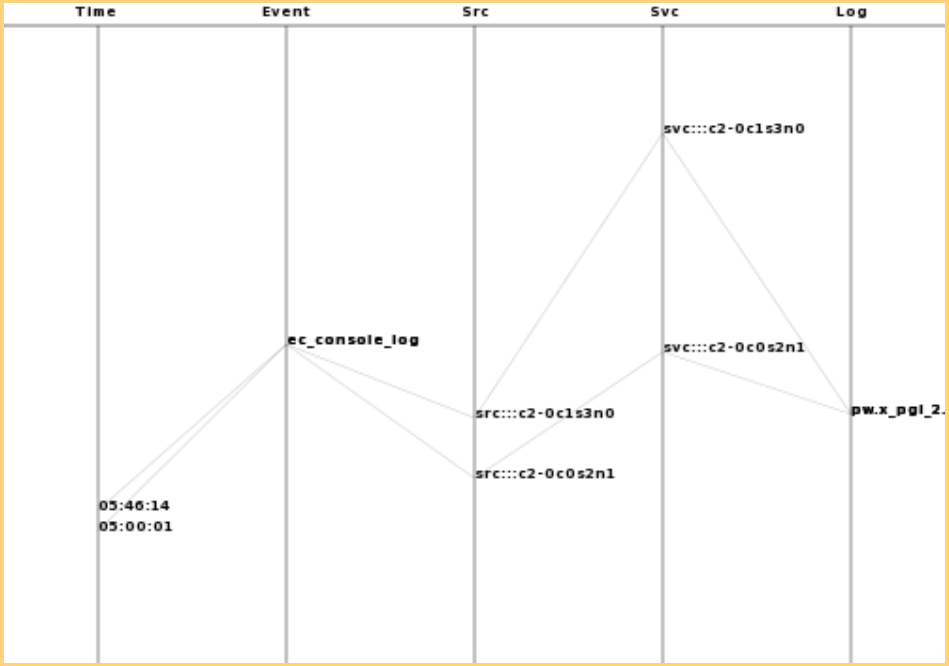
Picture



0809181018/eventlogs/eventlog

What are this value at about 40% on the axis 5 ?

Picture



Log

pw.x_pgi_2.8.0[2199] general protection rip:79ad77 rsp:7fffffffd28 error:0

0809181018/eventlogs/eventlog

What are those lower than 30% on the axis 5 ?

Log #1

Buffer I/O error on device sdj, logical block 0

Log #2

end_request: I/O error, dev sdj, sector 410588032

Conclusion

I just focused on the event log, However:

- We discovered stuff
  - Hard drive problems (ok I did not do that two days ahead ;)
  - software problems (remember the printk...)
  - we know the source device logging the most: src:::c1-0c0s6n1
- Am not not skilled enough with Cray systems to know the problems severity
- Greg, do we have time to do the analysis of an other file all together?