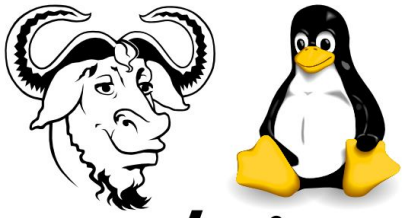
Linux Tracing

What Why and How?

Minto Joseph

whoami



GNU/Linux

Devops Engineer

Pythian

love your data

Over 17 years in IT industry

Why?

What?

How?

strace

system calls, signals

strace -p <pid>

strace <command>

strace -c <command>

- k Print the execution stack trace of the traced processes after each system call (experimental).

https://blog.pythian.com/using-strace-to-debug-application-errors-in-linux/

sysrq

/etc/sysctl.conf

kernel.sysrq = 1

echo 1 > /proc/sys/kernel/sysrq

echo m > /proc/sysrq-trigger

alt+sysrq+ <key>

https://blog.pythian.com/lessons-learned-from-debugging-application-performance-in-cloud/

Ftrace

/sys/kernel/debug/tracing

trace-cmd list -f

trace-cmd record -p function -l __do_page_fault
trace-cmd report

perf

perf_events

oprofile 0.9.8 onwards uses perf counters.

https://blog.pythian.com/debugging-high-cpu-usage-using-perf-tool-and-vmcore-analysis/

systemtap

Need to load kernel module.

```
stap -v -e 'probe vfs.read {printf("read performed\n"); exit()}'
```

ebpf

- bpftrace
- bcc-tools
  /usr/share/bcc/tools/*


ANY QUESTIONS?
imgflip.com