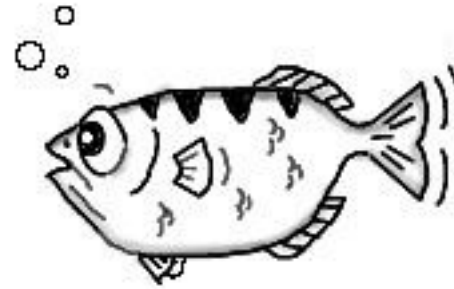
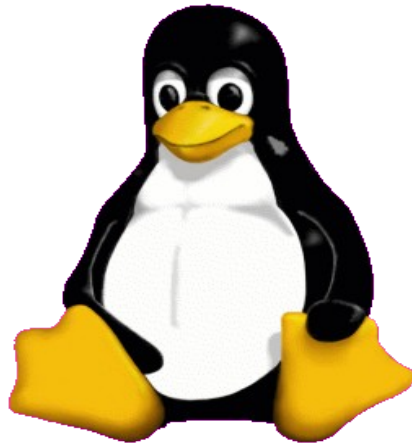


Linux Kernel GDB tracepoint module(KGTP)



HelloGcc Workshop

2010-11-06

Hui Zhu

teawater@gmail.com

GDB Tracepoint

- What is GDB tracepoint?
- Why GDB tracepoint?

The file of KGTP

- gtp.c
- Makefile
- gtp.patch
- getgtprsp.pl

How to config

- `KERNELDIR :=`
`/home/teawater/kernel/bamd64`
- `CROSS_COMPILE :=x86_64-glibc_std-`
- `ARCH := x86_64`

How to build, install and run

- `make`
- `make D=1`
- `sudo make install`
- `sudo insmod gtp.ko`
- `sudo modprobe gtp.ko`

How to use

- trace vfs_readdir
- commands
- collect \$reg
- collect file->f_path.dentry->d_iname
- collect jiffies_64
- collect *(unsigned char *)\$rsp@512
- end

Trace a interrupt

- trace /home/teawater/kernel/linux-2.6/drivers/char/keyboard.c:kbd_event
- commands
- collect *(unsigned char *)\$rsp@1024
- end

Trace a interrupt

- tvariable \$c
- trace handle_irq
- condition \$bpnum (irq==47)
- commands
- teval \$c=\$c+1
- end

Trace a special task with \$current_task

- trace vfs_write
- condition \$bpnum ((* (struct task_struct *) \$current_task)->pid == 5298)
- commands
- collect file->f_op
- collect file->f_path.dentry->d_iname
- collect *buf@10
- end

- Set the trace buffer into a circular buffer
- set circular-trace-buffer on
- Do not stop tracepoint when the GDB disconnect
- set disconnected-tracing on

Offline debug

- `target remote | perl ./getgtprsp.pl`
- Simple trace command
- `cat gtpstart > /proc/gtp`
- `cat gtpstop > /proc/gtp`
- `(gdb) target tfile ./gtpframe`

How to get KGTP

- <https://code.google.com/p/kgtp/>
- svn checkout
<http://kgtp.googlecode.com/svn/> kgtp-read-only

Thanks!