Sysdig

Tony Espinoza

am.espinoza@utexas.edu

What is sysdig?

Sysdig is a tool that combines:

- `top`, `htop`
  - Display running processes.
- `strace`
  - System call tracer.
- `tcpdump`
  - Dump traffic on the network.
- `iotop`
  - I/O monitor that looks like top.
- `lsof`
  - List open files.

Sysdig

- csysdig
  - Interactive UI similar to top
- sysdig
  - Can record to a file
  - sysdig -w test.scap
  - sysdig -G 3600 -W 24 -w dumpfile.scap
- sysdig-inspect
  - Interactive, browser based sysdig file inspector.

Installation steps: sysdig

https://github.com/draios/sysdig/wiki/How-to-Install-Sysdig-for-Linux

- `sudo apt install sysdig`
- Run sysdig as sudo

Reading a sysdig recording.

- `docker run -it -v $(pwd):/captures -p8085:3000 sysdig/sysdig-inspect:latest`
  - Make life easy by running sysdig from the folder you have the capture sysdig file.
  - At the start screen use the path `captures/FILENAME.scap`
- Allows filters.
  - `proc.name=nginx`
- Notice the filter at the top of the screen.