The Dark Art of Container Monitoring

Gianluca Borello
Gianluca Borello
- Software Engineer at Sysdig
- Core developer of sysdig

gianlucaborello
Seeing Inside Containers Is Not Easy!

Containers are:

- Isolated
- Self-Contained
- Simple
- Lightweight
Seeing Inside Containers Is Not Easy!

Containers are:
- Isolated
- Self-Contained
- Simple
- Lightweight

Can monitoring and troubleshooting play nice with these properties?
In This Talk

• Live overview of monitoring/troubleshooting options
  • command line
  • advanced namespaces tricks
  • sysdig
Demo environment

• Distributed Docker web application
…a troubleshooting nightmare
Some Things We Want to Monitor

- Resource usage (CPU/Memory/Disk)
- Network activity
- File I/O activity
- Errors/faults
- Application activity
Troubleshooting like a pro
sysdig

- Capture system events, filter them, run useful scripts
- `strace + tcpdump + lsof + htop + Lua`
- Open Source
- Nice curses UI

**Native support for containers!**
sysdig Architecture

Kernel

App

Container1
Docker

Container2
Docker

Container3
LXC
sysdig Architecture

Instrumentation through kernel module
sysdig Architecture

Capture and analysis
Great, but…

Multi-Node?!