sysdig

Official Sysdig Cheatsheet

Basic usage

Capture and write every system event to standard output

```
$ sysdig
```

Capture events to a trace file for later analysis

```
$ sysdig -w myfile.scap
```

Read events from a trace file

```
$ sysdig -r myfile.scap
```

Filter events based on certain fields

```
$ sysdig proc.name=httpd and evt.type!=open
```

Customize output with text and fields

```
$ sysdig -p "user:%user.name dir:%evt.arg.path"
```

Run a chisel for advanced functionality

```
$ sysdig -c topprocs_cpu
```

List all available fields

```
$ sysdig -l
```

List all available chisels

```
$ sysdig -cl
```

Network

Show the network data exchanged with a host

```
$ sysdig -s2000 -A -c echo_fds fd.cip=192.168.0.1
```

List all the incoming connections that are not served by apache.

```
$ sysdig -p "%proc.name %fd.name" "evt.type=accept
and proc.name!=httpd"
```

File system

List the processes using the highest number of files

```
$ sysdig -c fdcount_by proc.name "fd.type=file"
```

Observe the I/O activity on all the files named 'passwd'

```
$ sysdig -A -c echo_fds "fd.filename=passwd"
```

Performance

See the files where apache spent the most time

```
$ sysdig -c topfiles_time proc.name=httpd
```

See the top processes in terms of I/O errors

```
$ sysdig -c topprocs_errors
```

Security

Show the directories that root visits

```
$ sysdig -p "%evt.arg.path" "evt.type=chdir and
user.name=root"
```

Observe ssh activity

```
$ sysdig -A -c echo_fds fd.name=/dev/ptmx and
proc.name=sshd
```

Logs

Display all syslog messages from python

```
$ sysdig -c spy_syslog proc.name=python
```

Super-tail all log files in the system

```
$ sysdig -c spy_logs
```

sysdig.org