OFFICIAL OPENSOURCE SYSDIG CHEAT SHEET

Basic usage

Capture & 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
```

Run a chisel for advanced functionality
```
$ sysdig -c topprocs_cpu
```

List all available fields
```
$ sysdig -l
```

List all available chisels
```
$ sysdig -cl
```

Containers

View the list of processes with container context
```
$ sysdig -pc
```

View the CPU usage of the processes running in wordpress1 container
```
$sysdig -pc -c topprocs_cpu container.name=wordpress1
```

View the top HTTP requests made to the Kubernetes-based mySQL service
```
$sysdig -k http://127.0.0.1:8080 -c httptop k8s.svc.name=mysql
```

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"
```

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
```

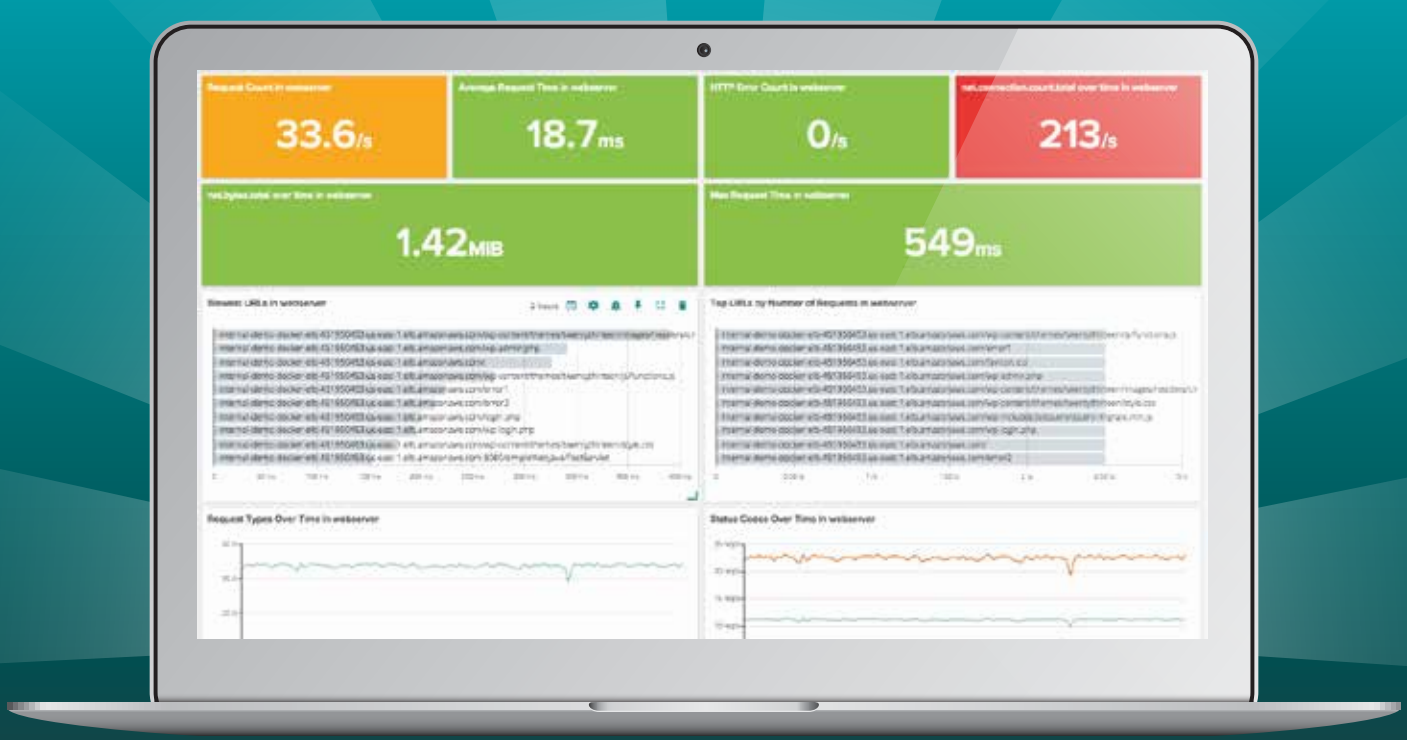
Super-tail all log files in the system
```
$ sysdig -c spy_logs
```

CSysdig

Run Csysdig, the curses based UI for Sysdig, with Mesos metadata
```
$ csysdig -m http://127.0.0.1:8080
```

sysdig

The most powerful container troubleshooting tool now monitors your entire distributed environment



Deep container monitoring

Service-oriented performance management

Trace-driven troubleshooting

Out-of-the-box integrations

docker

OPENSHIFT

kubernetes

DC/OS

Google Cloud Platform

amazon web services™

sysdig.com