Container Monitoring
In 5 Minutes

Mark Stemm,
Sysdig Engineer
Containers are Great...

• Simple
• Scalable
• Isolated
• Service-oriented
• Elastic
• Flexible
• Separation of concerns
But Some Things Are Becoming More Complex

Legacy Monolithic App

- Cache
- Webserver
- Database
But Some Things Are Becoming More Complex

Container-based App

Computing Node

Service1

Service2

Service3

Computing Node

Computing Node

Computing Node

Computing Node

Service1

Service2

Service3

Service1

Service2

Service3
But Some Things Are Becoming More Complex
But some things are becoming more complex.

Two problems.
Problem 1: How do we get data out of these guys?

- System
- Network
- Process
- JVM
- Response Time
- Requests
- Errors
Problem 2: How do we make sense of the data?

- System
- Network
- Process
- JVM
- Response Time
- Requests
- Errors
How Do I Get Data Out of These Things: VMs

VM1

VM2

VM3

Hypervisor
Monitoring VMs, Option 1

Hypervisor

Hypervisor-level instrumentation, Amazon CloudWatch

VM1  VM2  VM3
Monitoring VMs, Option 2
Monitoring Containers

- Container 1
- Container 2
- Container 3

OS
Monitoring Containers, Option 1
Monitoring Containers, Option 1

- Not scalable
- Not composable
- Adds dependencies/size
- Kills the concept of one process per container

Container1 • Container2 • Container3

Monitoring Agent
Monitoring Containers, Option 2

Container runtime – level monitoring
Kernel-level instrumentation
Monitoring Containers, Option 3

Diagram showing the relationship between OS, Container1, Container2, and the Monitoring Container.
Introducing Sysdig

• Capture system events, filter them, display them
• Filter expression language to control what and how events are displayed
• Open source
• Nice curses UI
Sysdig Data Collection

Kernel

Container 1
Docker

Container 2
Docker

Container 3
LXC

App

App
Sysdig Data Collection

Instrumentation through kernel module

Kernel
Sysdig Data Collection

Capture and analysis

Kernel

App

Container 1
Docker

Container 2
Docker

Container 3
LXC

sysdig
More than just system calls

- Sysdig also has native support for containers
  - Docker
  - LXC
  - Libvirt
  - Mesos
  - CoreOS
- And orchestration
  - Kubernetes
  - Mesos
  - Docker Swarm
Csysdig: Moving From This
### Cysdig: To This

```
2. mstemm@ubuntu: ~ (ssh)

<table>
<thead>
<tr>
<th>CPU</th>
<th>VIRT</th>
<th>RES</th>
<th>FILE</th>
<th>NET ID</th>
<th>NAME</th>
<th>NAMESPACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>360M</td>
<td>231M</td>
<td>563</td>
<td>1.76K</td>
<td>99f36021-8f34-11e6-a17c-08002719228f</td>
<td>wordpress-2182556466-16c-dev</td>
</tr>
<tr>
<td>0.5</td>
<td>2G</td>
<td>187M</td>
<td>41K</td>
<td>586.00</td>
<td>100d74ed-8f34-11e6-a17c-08002719228f</td>
<td>mongodb-886875792-c8pg3-dev</td>
</tr>
<tr>
<td>0.5</td>
<td>3G</td>
<td>280M</td>
<td>112</td>
<td>248.00</td>
<td>0dec9158-8f34-11e6-a17c-08002719228f</td>
<td>cassandra-1803904136-cz4-dev</td>
</tr>
<tr>
<td>0.5</td>
<td>1G</td>
<td>211M</td>
<td>128</td>
<td>49.32K</td>
<td>2bc05b01-8f34-11e6-a17c-08002719228f</td>
<td>mysql-1403861048-9neca-dev</td>
</tr>
<tr>
<td>0.0</td>
<td>378M</td>
<td>17M</td>
<td>65K</td>
<td>1.40K</td>
<td>56779179-8f34-11e6-a17c-08002719228f</td>
<td>jclient-2531512532-4ti3g-dev</td>
</tr>
<tr>
<td>0.0</td>
<td>200M</td>
<td>10M</td>
<td>742K</td>
<td>357.20K</td>
<td>44f6e59f-8f34-11e6-a17c-08002719228f</td>
<td>client-1400073070-hlx4n-dev</td>
</tr>
<tr>
<td>0.0</td>
<td>360M</td>
<td>8M</td>
<td>6K</td>
<td>70.00</td>
<td>1f6bb328-8f34-11e6-a17c-08002719228f</td>
<td>redis-3547843244-eakfn-dev</td>
</tr>
<tr>
<td>0.0</td>
<td>360M</td>
<td>217M</td>
<td>503</td>
<td>1.39K</td>
<td>99f2aabb-8f34-11e6-a17c-08002719228f</td>
<td>japp-2458569569-7lexq-dev</td>
</tr>
<tr>
<td>0.0</td>
<td>360M</td>
<td>230M</td>
<td>0</td>
<td>0.00</td>
<td>99f44db5-8f34-11e6-a17c-08002719228f</td>
<td>japp-2458569569-6wopd-dev</td>
</tr>
</tbody>
</table>
```

---

**sysdig**
What is Csysdig

- Ncurses-based frontend to Sysdig
- Leverages Sysdig event collection and processing
- Adds terminal-friendly user interface
- Ability to drill down from overview to individual items
- Customizable views and filters
- Like Sysdig, support for containers and orchestration
• Start with Sysdig’s monitoring capabilities
• Add cloud-based SAAS visualization
• Sysdig Monitor!
Sysdig Monitor Architecture

- Sysdig (open source) -> Sysdig Agent (free download)
- Agent sends to Sysdig Monitor SAAS
- View metrics, events, topology, etc. in browser
- On-premise variant also available.
Out of the box support

<table>
<thead>
<tr>
<th>MySQL</th>
<th>NGINX</th>
<th>Node.js</th>
<th>OpsGenie</th>
<th>PAGERDUTY</th>
<th>TokuteK</th>
<th>PGBOunser</th>
<th>PHP</th>
<th>POSTFIX</th>
<th>PostgreSQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Python</td>
<td>RabbitMQ</td>
<td>RedHat</td>
<td>Redis</td>
<td>Riak</td>
<td>rabbitMQ</td>
<td>Ruby</td>
<td>Slack</td>
<td>Solr</td>
<td>StatsD</td>
</tr>
<tr>
<td>ActiveMQ</td>
<td>Apache</td>
<td>AWS</td>
<td>Cassandra</td>
<td>CentOS</td>
<td>Consul</td>
<td>CoreOS</td>
<td>Couchbase</td>
<td>CouchDB</td>
<td>Debian</td>
</tr>
<tr>
<td>Docker</td>
<td>Elastic</td>
<td>EtcD</td>
<td>Fluentd</td>
<td>GCP</td>
<td>Gearman</td>
<td>Go</td>
<td>Gunicorn</td>
<td>Hadoop</td>
<td>HAProxy</td>
</tr>
<tr>
<td>HBase</td>
<td>Java</td>
<td>Kafka</td>
<td>Kubernetes</td>
<td>Kyoto Tycoon</td>
<td>LightTPD</td>
<td>Memcached</td>
<td>Mesos</td>
<td>Mesosphere</td>
<td>MongoDB</td>
</tr>
</tbody>
</table>
Demo
What we’re going to show you

- Monitoring with Sysdig
- Hosts
- Containers
- Orchestration (K8s)
- Monitoring with Csysdig
- Monitoring with Sysdig Monitor
Join The Community

• Website
  • https://www.sysdig.org/
• Public Slack
  • https://sysdig.slack.com/messages/open-source-sysdig/
• Blog
  • https://sysdig.com/blog/
• Sysdig Monitor
  • https://sysdig.com/product
Learn More

- Github
  - https://github.com/draios/sysdig
  - Pull Requests welcome!
- Wiki
  - https://github.com/draios/sysdig/wiki
- Docker Hub
  - https://hub.docker.com/r/sysdig
Thank You!