Monitoring and Troubleshooting Docker Across Cloud and On-prem Environments

Marc Chéné

IT Markets Product Manager, Splunk

Denis Gladkikh

Principal Dev Engineer (aka outcoldman), Splunk

.conf2016

splunk>

Who we are?

- Marc Chéné
  - Engineer, IT Markets Product Manager, APMer
  - Dad to 3, super-fan and coach
  - Lover of skiing, golfing, music and good drink
  - Resident groundskeeper/ gardener
  - Twitter: @marcchene
- Denis Gladkikh
  - System programming developer - building Enterprise applications, Mobile Apps, Dev Tools and scalable systems
  - Open source contributor (VS Code, Docker, cAdvisor, antigen, Mongo C Driver and more...).
  - Skydiver, Scuba diver, Downhill/nordic skier, hiker, GSD owner
  - Twitter: @outcoldman

Disclaimer

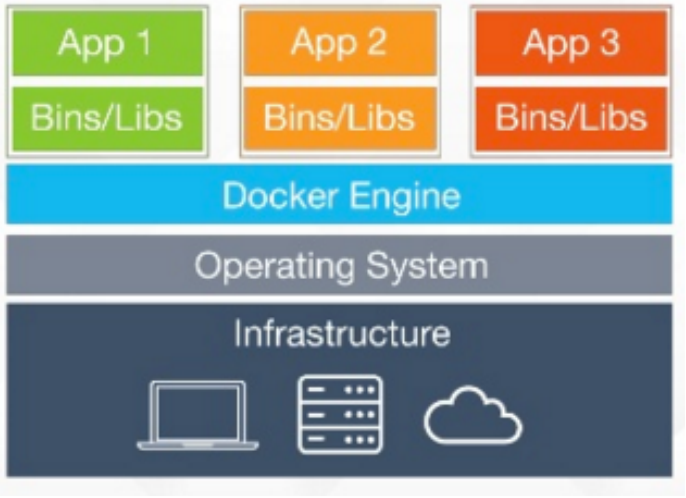
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- What is Docker?
- How to Monitor Containers?
- Splunk Analytics for Docker
- Monitoring your Cloud Containers


First, a bit about containers...

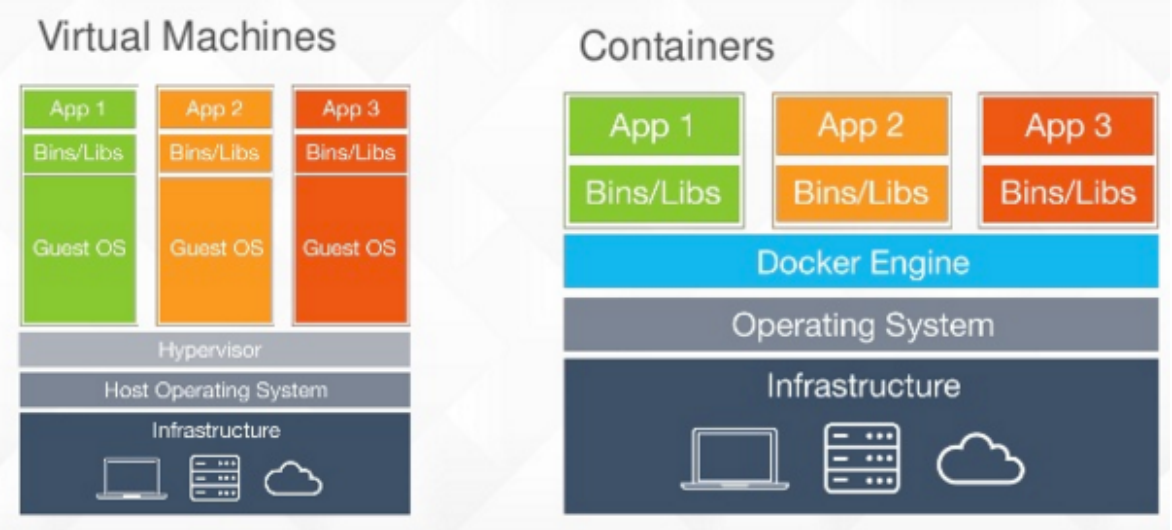
Docker, in one Slide



- Build - Ship - Run your applications
  - ”Infrastructure as code”
  - Enables microservices architectures
  - Portable – Enables Cloud Migration
- Open Source and Community Minded
  - Docker Engine is Open Source
  - Thousands of apps can be “pulled” in Docker Hub / Docker Store
  - Your developers

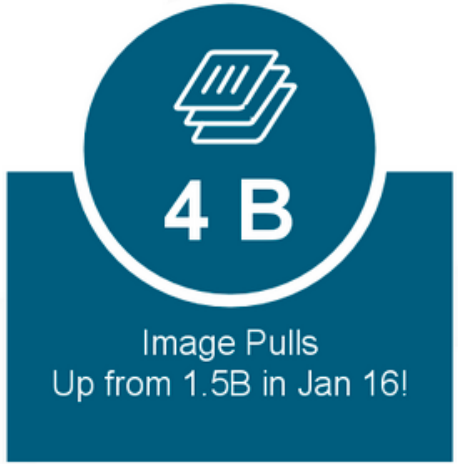
Docker – It's not Virtualization

- VMs – focus on OS
- Docker – focus on applications
- Docker – lightweight and FAST
- NOT mutually exclusive with VMs

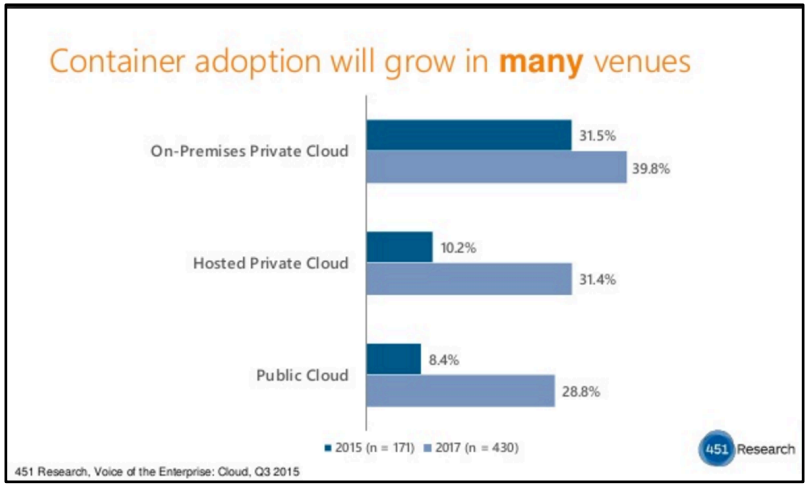


Docker – it's a big deal

Open Source driven ecosystem

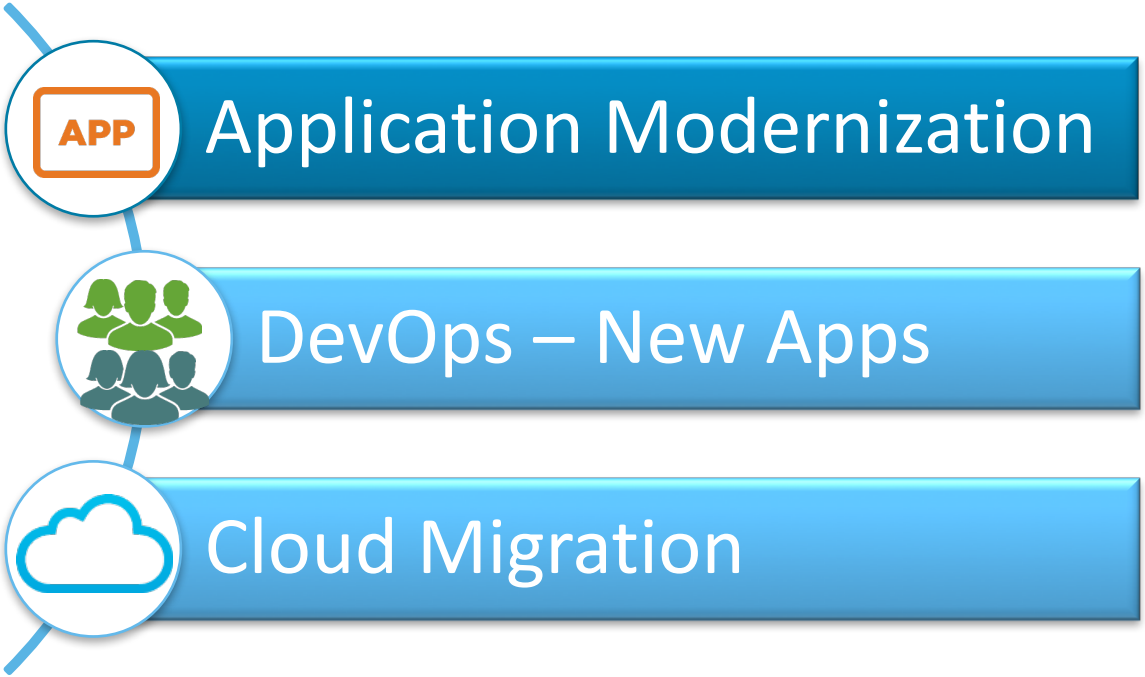


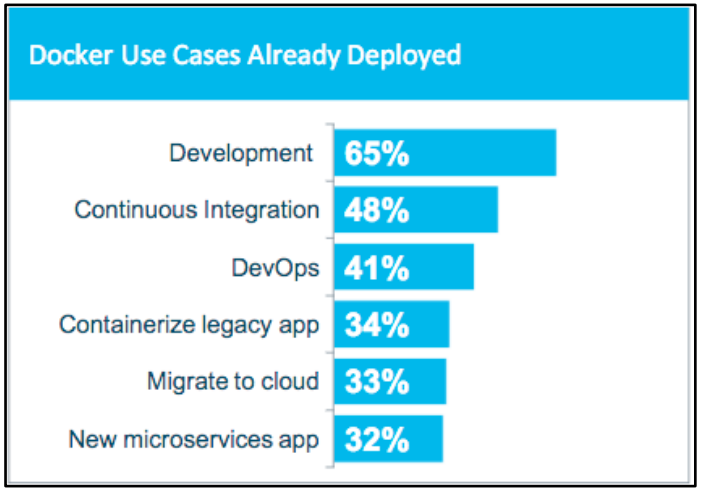
Massive increase in adoption…



…But the growth is just getting started

3 Primary Container Use Cases

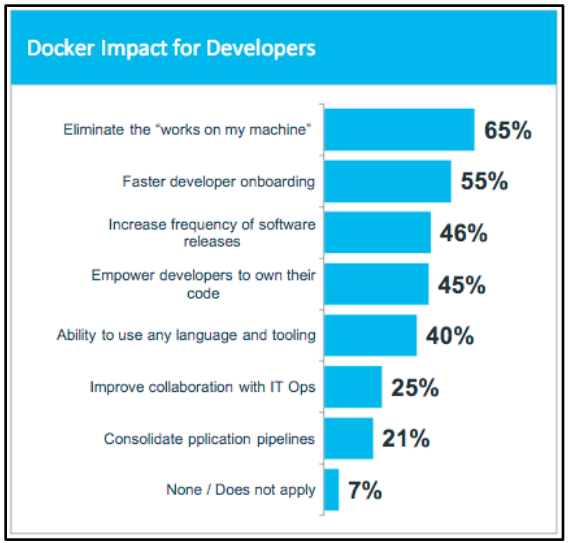





CONTAINERS
ARE GOING TO MAKE YOUR LIFE BETTER
imgflip.com

Docker Addresses Customer Pain Points

"But it worked in dev..."



- Standardization between dev and production environments
- Less effort to put into release management = faster development

Docker Creates New Monitoring Challenges

- New layers of abstraction
- Containers have Short lifespans
- You still have dependencies on other levels of the stack
- New consumers of monitoring data

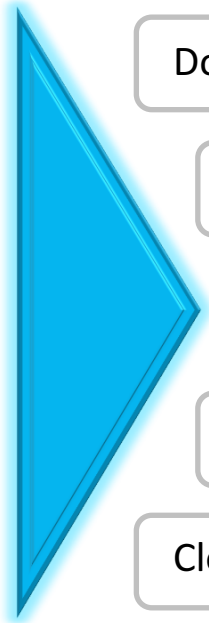
Container monitoring and troubleshooting needs to be easy, focused on analytics, and related with other parts of your infrastructure

How to Monitor Containers?
- Getting Data In (GDI)

.conf2016

splunk>

Splunk Log Streaming Options for Docker



- Docker Native Logging – **Splunk logging driver**, Syslog, AWS, JSON files, etc.
- Universal Forwarder – App Logs, Syslog forwarding, Performance, etc.
- Logging libraries in .NET, Java and node.js
- Custom (e.g., Kafka with HTTP Event Collector)
- Cloud – AWS, GCP, Azure

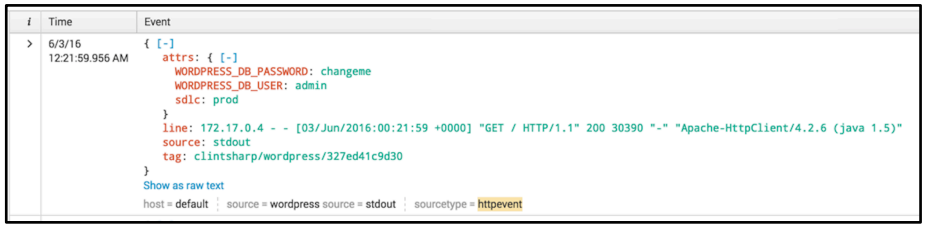
Use the option that is right for you!

Visibility to your Container Environments

Splunk Logging Driver for Docker

- Secure—supports TLS/SSL and tokens
- Simple – config-based setup and collect data
- Scale – Based on HTTP Data Collector Based on Splunk HTTP
- Configurable - Supports container labels, environment variables

```
docker run --log-driver=splunk \
    --log-opt splunk-token=176FCEBF-4CF5-4EDF-91BC-703796522D20 \
    --log-opt splunk-url=https://splunkhost:8088 \
    --log-opt splunk-capath=/path/to/cert/cacert.pem \
    --log-opt splunk-caname=SplunkServerDefaultCert
    --log-opt tag="{{.Name}}/{{.FullID}}"
    --log-opt labels=location
    --log-opt env=TEST
    --env "TEST=false"
    --label location=west
    your/application
```



Based on Splunk HTTP Event Collector + Driver built directly into Docker

Visibility into your Container Environments

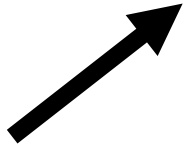
Splunk Logging Driver for Docker (*coming soon docker 1.13*)

- Skip verification for the valid splunk url
- Raw data collection from the native log driver
- Embedded json format support

```
--log-opt splunk-verifyconnection=true|false
```

```
MyImage/MyContainer env1=val1 label1=label1 my message
MyImage/MyContainer env1=val1 label1=label1 {"foo": "bar"}
```

```
{
    "attrs": {
        "env1": "val1",
        "label1": "label1"
    },
    "tag": "MyImage/MyContainer",
    "line": "my message"
}
{
    "attrs": {
        "env1": "val1",
        "label1": "label1"
    },
    "tag": "MyImage/MyContainer",
    "line": "{\"foo\": \"bar\"}"
}
```

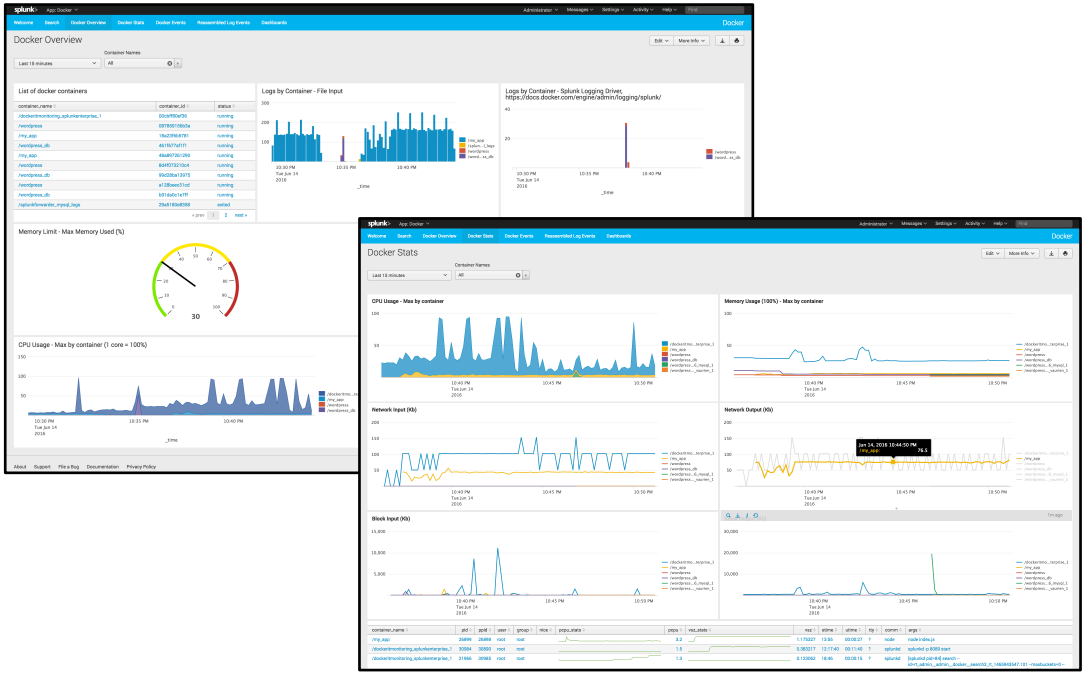


```
{
    "attrs": {
        "env1": "val1",
        "label1": "label1"
    },
    "tag": "MyImage/MyContainer",
    "line": "my message"
}
{
    "attrs": {
        "env1": "val1",
        "label1": "label1"
    },
    "tag": "MyImage/MyContainer",
    "line": {"foo": "bar"}
}
```

Visibility to your Container Environments

Adding Universal Forwarders to your Docker Environments

- Logs – Access to Applogs, syslog UDP forwarding, JournalD
- Stats – Data from Docker containers
- Search – Troubleshoot Docker related problems
- Dashboards and Alerts- Proactively monitor Docker environments



Many ways to get Docker-based machine data – choose what's best for you

Splunk Analytics

- Splunk Images
- It’s Time for Analytics

.conf2016

splunk>

Delivering Splunk as a Container Image

- Splunk container images
  - Splunk Enterprise 6.4.1
  - Splunk Universal Forwarder 6.4.1
- Includes configuration and Docker Add-On for container monitoring out-of-the-box
- Certified image
- Coming soon to the Docker Store (http://store.docker.com)


```
docker run splunk/enterprise:6.4.1-monitor
docker run splunk/universalforwarder:6.4.1-monitor
```

Demo Setup

- Use case: Container Log Analysis and Monitoring
- “full stack” application with 4 containers monitored with Splunk
  - MariaDB – our open source database layer
  - Wordpress -- a rather busy application
  - My_app – our made-up app
  - Splunk – yes, we’re running Splunk IN A CONTAINER!
- Key takeaways
  - Time-to-value – Splunk is pre-configured to discover and collect machine from all your containers running on a node
  - Insight across logs and metrics
  - Insight into containers, applications, compliance, and the data those applications generate
  - Docker – up and running

Demo Time!

- Getting Data In (GDI)
- Splunk Logging Driver
- Analytics

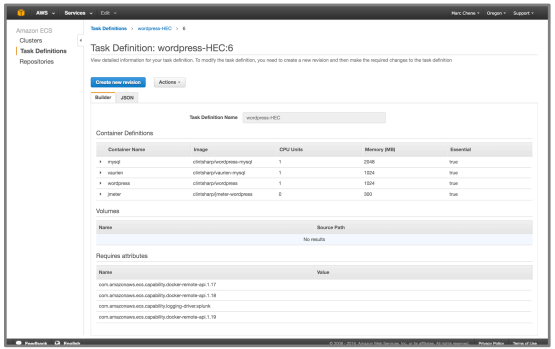
.conf2016

splunk>

Monitoring your Cloud Containers

Monitoring for Your Cloud Environments

- Amazon Web Service integration via CloudWatch and Elastic Container Service (ECS)
- Google Cloud Platform integration via Stackdriver Pub/Sub and cloud monitoring APIs



Sample Docker Cloud Data

splunk> App: Search & Reporting

Administrator | 1 Messages | Settings | Activity | Help | Find

Search | Pivot | Reports | Alerts | Dashboards | Search & Reporting

Google Cloud Platform (GCP) Log Dashboard

Edit | More Info

GCP Service Type: All

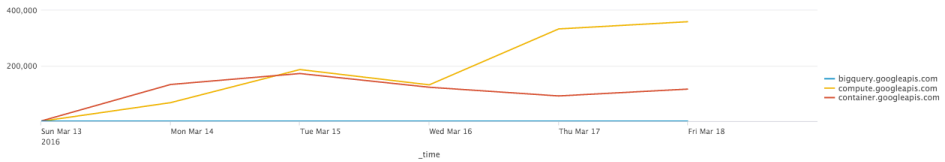
GCP Source Type: All

Week to date

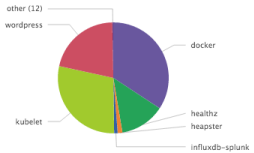
Could not create search.

# of GCP Log Events 1,714,289

Log count by Service Name



Log Count by Source



of Events by GCP Sources

_time	OTHER	docker	etcd	healthz	heapster	splunk	jmeter-wordpress	kubelet	vaurien-mysql	wordpress	wordpress-mysql
2016-03-13	0	0	0	783	74	76	0	0	0	1	0
2016-03-14	72	0	130	54956	5359	5268	0	67139	181	66653	89
2016-03-15	144	57187	137	55973	5468	5367	0	129443	160	104972	106
2016-03-16	241	0	145	59740	5762	5692	0	131427	192	50946	112
2016-03-17	173	237874	123	32282	3937	1268	1032	95386	98	52443	84
2016-03-18	63	292809	27	21305	3065	0	2115	67683	0	90082	0

Log Count by Source and Log Level

log	error	info
docker	795	586328
cloudaudit.googleapis.com/data_access	0	0
compute.googleapis.com/activity_log	0	0
etcd	0	0
fluent.warn	0	0
fluentd-cloud-logging	0	0
healthz	0	0
heapster	0	0
influxdb-splunk	0	0
jmeter-wordpress	0	0

« prev 1 2 next »

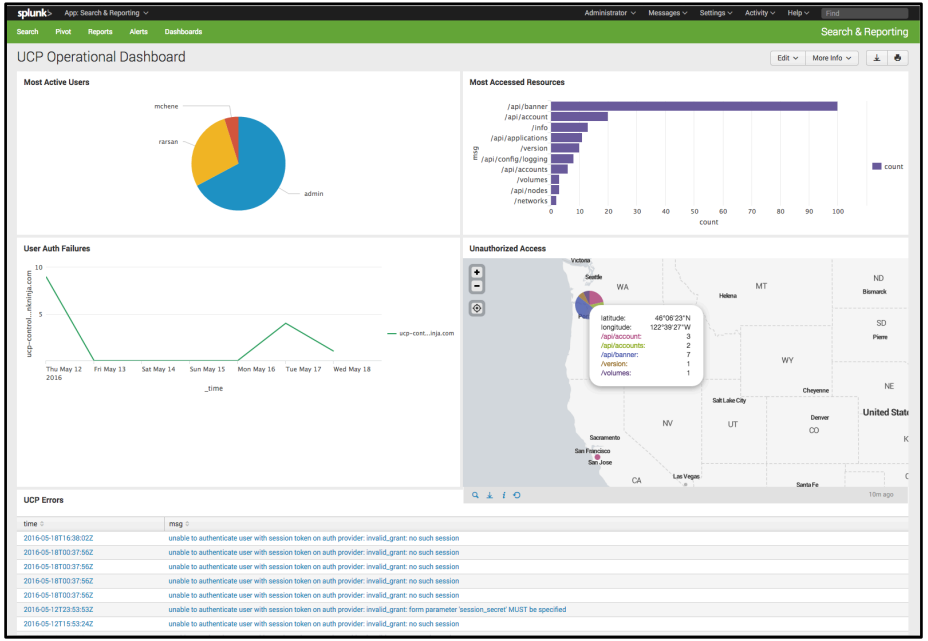
About | Support | File a Bug | Documentation | Privacy Policy

Visibility to your Container Environments

Splunk Add-On for Docker Universal Control Plane

- **Monitor Changes –** Identify changes in containers, updates to container deployments
- **Usage Insight –** Insight into containers, clusters, and nodes
- **Analyze and Correlate –** Changes, usage, errors and configuration

Improve Docker container compliance, availability and performance



Call to Action…

```
# 1. Come visit us at our booth
docker run splunk/visitourbooth
visitourbooth_1 | Booth IT Markets

# 2. Test out our Splunk logging driver
docker run --name wordpress --label web=wordpress \
--log-driver=splunk \
--log-opt splunk-token=00000000-0000-0000-0000-000000000000 \
--log-opt splunk-url=https://192.168.99.100:8088 \
--log-opt labels=web --log-opt tag="{{.Name}}" \
--publish 80:80 \
-d wordpress
```

Call to Action…

```
# 3. Try out our docker images in Docker Store
docker run splunk/enterprise:6.4.1-monitor
docker run splunk/universalforwarder:6.4.1-monitor

# 4. Demos will all be available on GitHub under Splunk!
git clone https://github.com/splunk/docker-gettingstarted-conf2016.git

# 5. Visit our site to learn more about containers
curl http://www.splunk.com/containers
```

What Now?

Related breakout sessions and activities…

- How to run Splunk as a Docker Image? Session ID: SF88089

THANK YOU

splunk>