

Docker and Splunk Development

Empowering Splunk Development with Docker

Ron Cooper & David Kraemer | Booz Allen Hamilton

26 September 2017 | Washington, DC

Forward-Looking Statements

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 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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Demonstrating Docker for Splunk DevOps

- ▶ Provide a brief overview of Docker and Splunk benefits
- ▶ Why we chose Docker for DevOps
- ▶ Describe and demonstrate the Booz Allen use cases for Docker development



Who we are?

Ron Cooper & David Kraemer | Booz Allen Hamilton
Commercial and Cyber Security

Booz | Allen | Hamilton

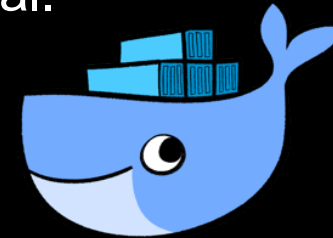
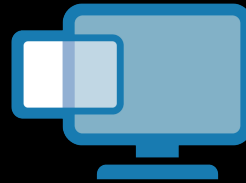
What is Docker?

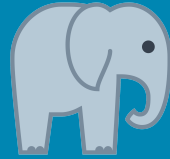
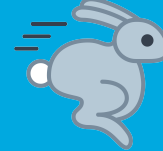
Why do I want to use Docker with Splunk?

What is Docker?

Docker is not VM

- ▶ Docker is an Open Source container based technology
 - Docker Separates Applications from Infrastructure using Container Technology, similar to how Virtual Machines separate the Operating System from Bare Metal.



Size		
Startup		
Integration		

Virtual Machine vs. Docker Container

How do they compare?

Virtual Machine

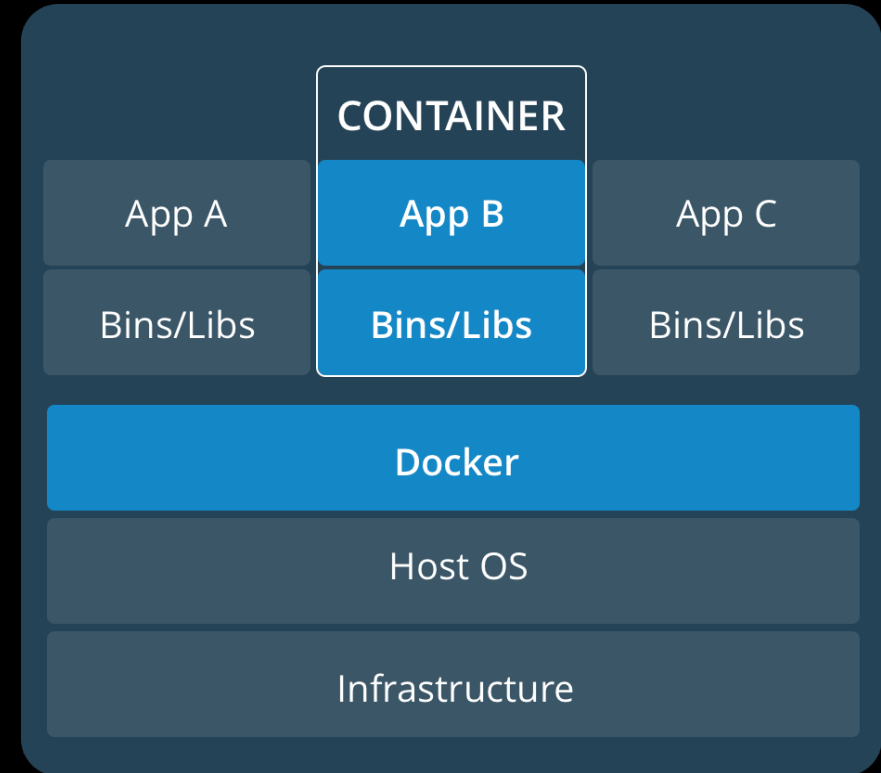
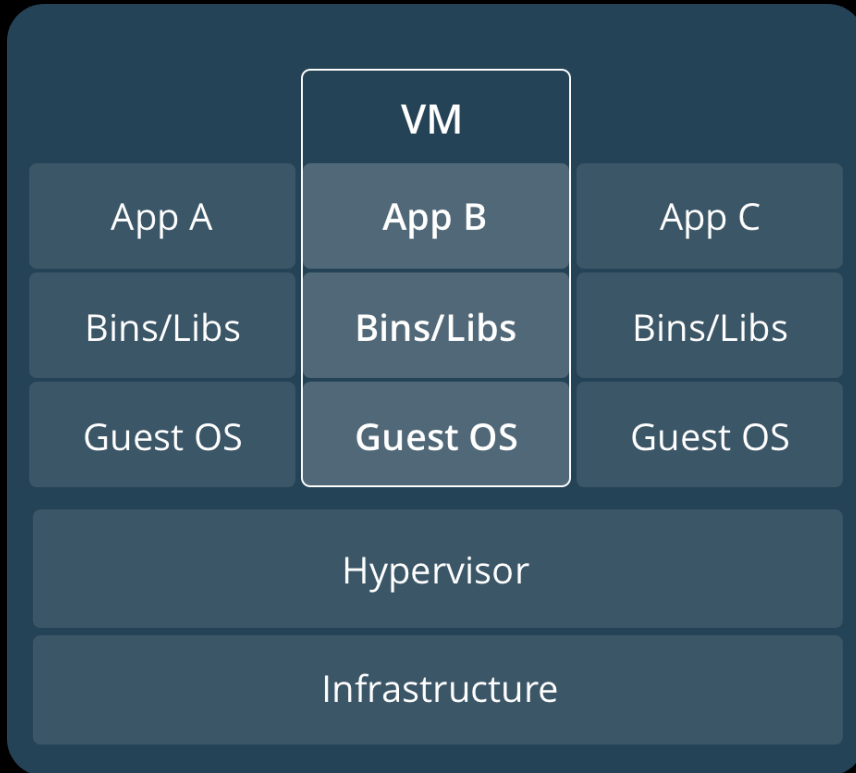
- Includes not only the virtualized application, dependent files and an entire guest OS
- Potential to weigh 10's of GB
- Isolated resources and allocations per VM limitations
- Requires a Hypervisor layer

Docker Container

- Contains just the application and its dependencies
- Isolated resources and allocation, with much more portability and efficiency
- Runs as an isolated process in userspace on the host operating system sharing the kernel with other containers

What is Docker?

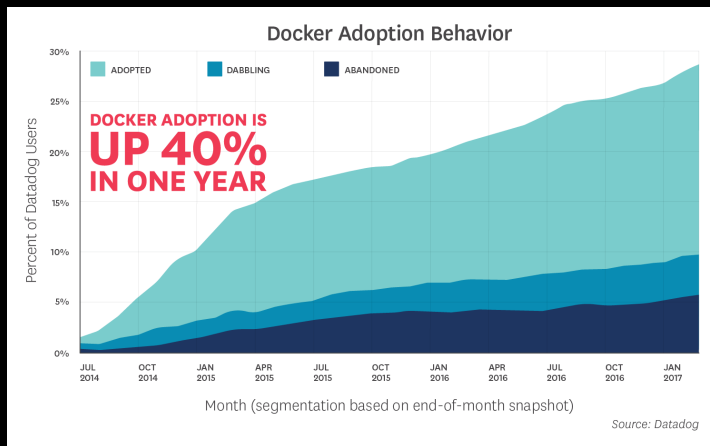
VM vs. Container



Docker Adoption Rate

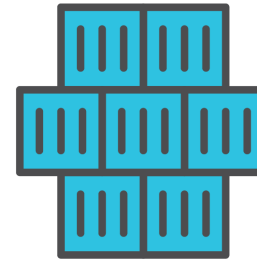
Interesting data points

“Docker Adoption is up 40% in One Year”



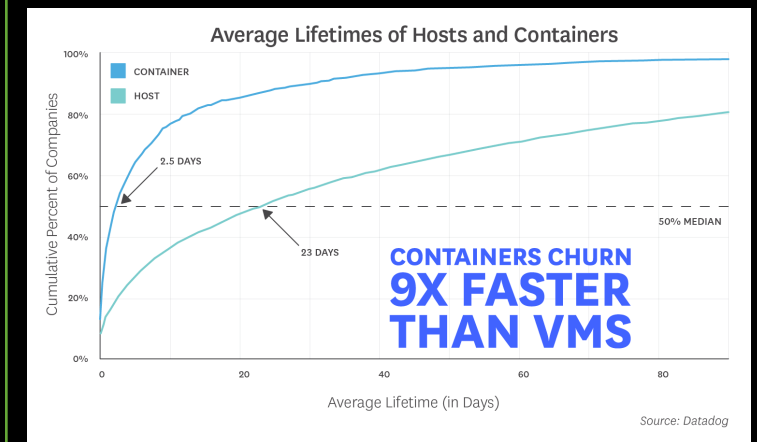
“Docker Hosts Often Run Seven Containers at a Time”

HOSTS RUN
SEVEN
CONTAINERS
AT A TIME



Source: Datadog

“Containers Churn 9x Faster Than VMs”



Source: Datadog

Inspiration

.conf2016 Docker

Be sure to check out for
more fundamental
Splunk/Docker
fundamentals

How To Run Splunk As A Docker Image?

Marc Chéné

IT Markets Product Manager , Splunk

Denis Gladkikh

Principal Dev Engineer (aka outcoldman), Splunk

.conf2016

splunk>

splunk> .conf2017

Why We Choose Docker For DevOps

Getting stuff done

- ▶ Easy to deploy purpose built Splunk Environments
 - Quick deployment
 - OS Independent
 - Roll back to standard configurations
 - Easy to contribute and support
- ▶ Have a portable testing environment
- ▶ Improve code quality and sharing



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
317.27.160.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=KIL-W-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:31.0) like Gecko"
```

Proof of concept

Spin up the
environment you need
Splunk 'n box

SH0 1	SH02	SH03
IDX0 1	IDX02	IDX03
CM0 1	LM0 1	DEP01

Splunk n' Box

Splunk multi-site clusters in 20 minutes or less!

<https://github.com/mhassan2/splunk-n-box>



presenter

Mo Hassan
Sales Engineer

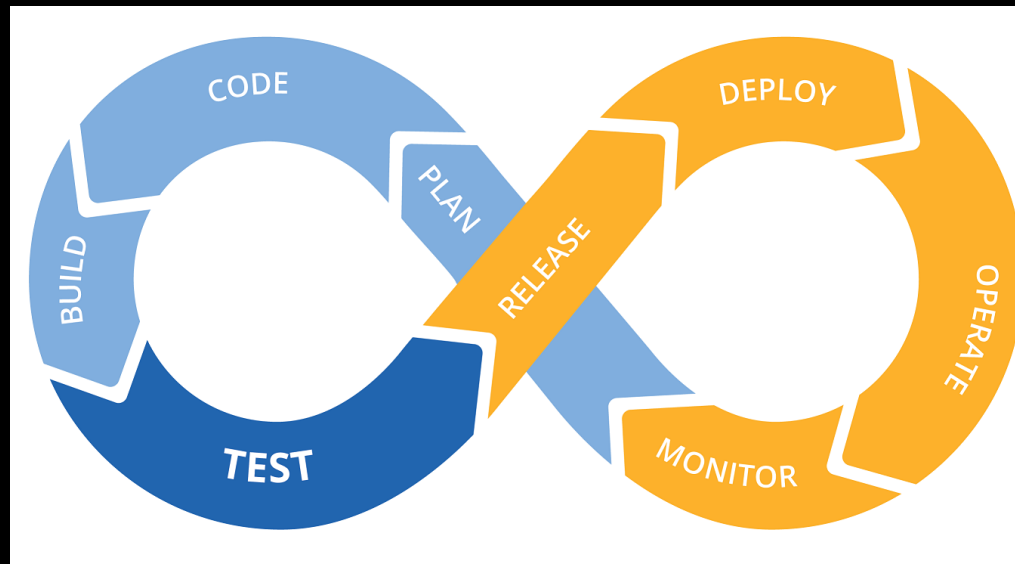
What is DevOps?

Back to Fundamentals

DevOps

Definition and Lifecycle

- ▶ “DevOps (**d**evelopment and **o**perations) is an enterprise software development phrase used to mean a type of agile relationship between development and IT operations. The goal of DevOps is to change and improve the relationship by advocating better communication and collaboration between these two business units.”



Source: Webopedia

What does yours look like?

- ▶ No development environment?
- ▶ Single server?
- ▶ Mirror-of-production development environment?
- ▶ **Some combination of the above?**

Damnit, not again...

Splunk Development Kit w/ Docker

Splunk Docker
deployment designed
for ease of
development



Key Takeaways

Sparking creativity

1. Demonstrate how we can quickly test, develop and share code for Splunk DevOps utilizing Docker
2. Think of new ways to quickly deploy purpose built Splunk environments
3. Continue to recognize new, unique ways Docker can provide benefit to Splunk Architects and Developers alike

All our links

- <https://github.com/TetchyTech/splunk.conf2017>

- <https://github.com/TetchyTech/splunk.conf2017>

- <https://github.com/mhassan2/splunk-n-box>

- <https://github.com/mhassan2/splunk-n-box>

- <https://www.datadoghq.com/docker-adoption/>

- <https://www.datadoghq.com/docker-adoption/>

- <http://conf.splunk.com/files/2016/slides/how-to-run-splunk-as-a-docker-image.pdf>

- <http://conf.splunk.com/files/2016/slides/how-to-run-splunk-as-a-docker-image.pdf>

Q&A

Ron Cooper | Cyber Security Architect
David Kraemer | Cyber Security Architect

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017