

splunk>

.conf2017

© 2017 SPLUNK INC.

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.

Agenda

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



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF1ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.purchase&itemId=EST-20&product_id=K9-CU-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD95L4FF1ADFF7 HTTP 1.1"
...

```

Who we are?

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

Booz | Allen | Hamilton

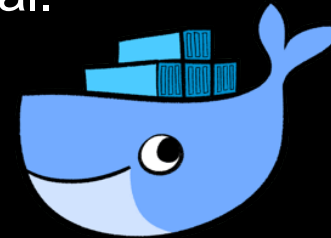
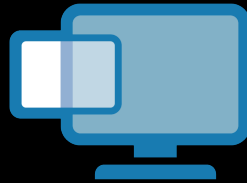
What is Docker?




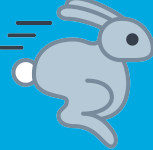


Why do I want to use Docker with Splunk?

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.

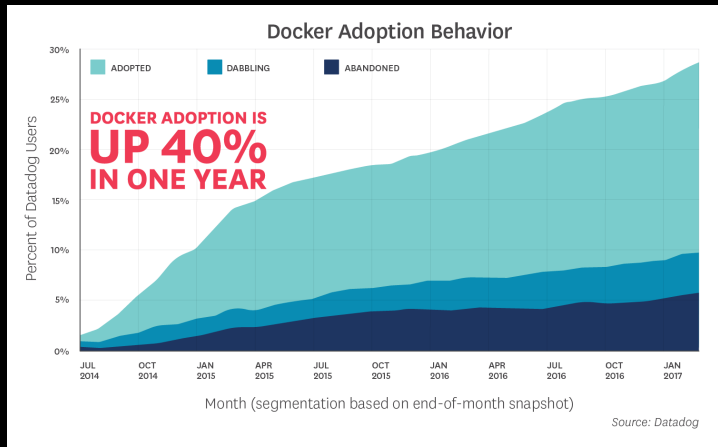


| | | |
|-------------|---|---|
| Size |  |  |
| Startup |  |  |
| Integration |  |  |

Docker Adoption Rate

Interesting data points

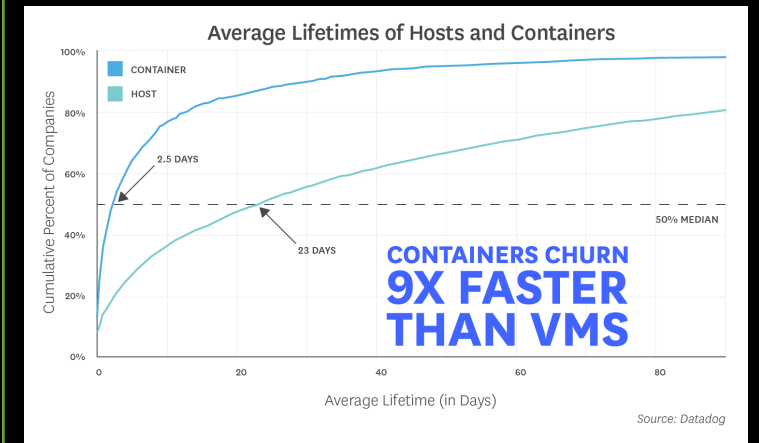
“Docker Adoption is up 40% in One Year”



“Docker Hosts Often Run Seven Containers at a Time”



“Containers Churn 9x Faster Than VMs”



Source: Datadog

Inspiration

.conf2016 Docker

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

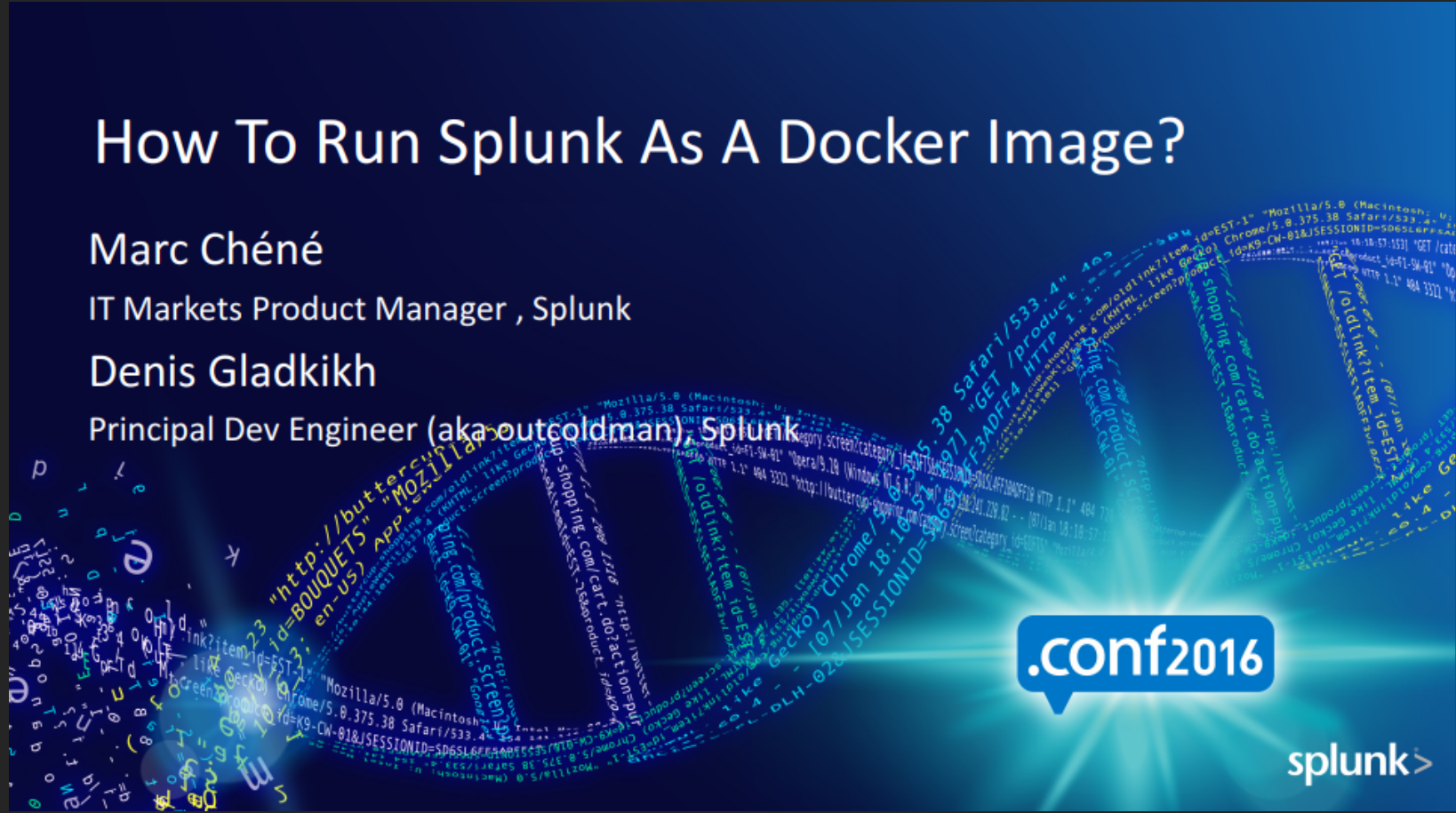
How To Run Splunk As A Docker Image?

Marc Chéné

IT Markets Product Manager , Splunk

Denis Gladkikh

Principal Dev Engineer (aka outcoldman), Splunk



.conf2016

splunk>

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/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01"
10.0.0.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L1E12ADFF9 HTTP 1.1"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD105L1E12ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01"

```

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>



Mo Hassan
Sales Engineer

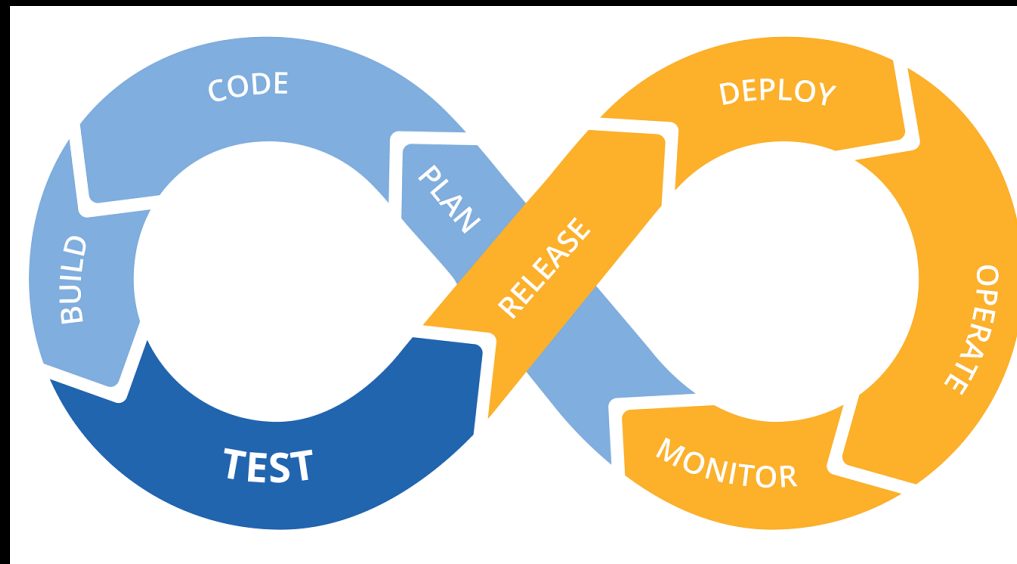
What is DevOps?

Back to Fundamentals

DevOps

Definition and Lifecycle

- ▶ “DevOps (**development and operations**) 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: Wikipedia

Splunk Developer Woes

Damnit, not again...

```
130.60.4 - - [07/Jan 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&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:53.0) Gecko/20100827 Firefox/53.0"
317.27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 189 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.2013.10 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=LI-02" "Opera/9.80.2013.10 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) "
```


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

Reference Material

All our links

► Our Code

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

► Splunk 'n Box

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

► Docker Adoption Data

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

► .conf2016 How to Run Splunk as a Docker Image?

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

```
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L7FF6ADFF9 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.14 [oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1] 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&item_id=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L1W74" "Opera/9.80.20
/buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
shopping.com/cart.do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
http://shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
http://shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
http://shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
http://shopping.com/category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
do?action=purchase&item_id=EST-26&JSESSIONID=SD5L9FF1A0FF3 HTTP 1.1" 200 3865 "http://shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=Mozill/27.0" "Opera/9.80.20
```

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