

Sandboxing with Splunk

...while you get settled...

► Latest Slides:

- <https://splunk.box.com/v/blueprints-docker-sandbox>

► Handout:

- <https://splunk.box.com/v/blueprints-docker-sandbox-ref>

► Collaborate: #docker-sandbox

- Sign Up @ <http://splk.it/slack>

► Load Feedback ----->

Best Practices and Better Prac...

Description	Notes
Administrator (150)	
Role	>
Architect (130)	
Skill Level	>
Beginner (23)	
SHOW 6 MORE ▼	

Feedback

How would you rate this session content: (Rate 1 to 5)

Low 1 2 3 4 5 High

How would you rate the session speaker(s): (Rate 1 to 5)

Low 1 2 3 4 5 High

General Feedback: (Open Text Area)

Submit Feedback

Sandboxing with Splunk

(with Docker)

Burch | Senior Best Practices Engineer

.conf2017 | 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.

Who are we?

Who are you?

This should make sense ----->

- ▶ Experience installing Splunk
- ▶ Familiar with Splunk's Ports
- ▶ Comfortable using Command Line

It's totally cool if you wanna bounce!

Gets a chance to onboard first log source




Meme credit to Angel Rios

Senior Best Practices Engineer

- # ~~Docker Expert~~



Follow up != Prerequisite



2016 Sessions

Sessions Filter Tracks ▾ Session Focus ▾ Skill Level ▾ Role ▾ Industries ▾ Products ▾ Other Topics ▾

1 Results sandbox 🌐



Splunk Snacks

Your Splunk Sandbox

Wednesday, September 28, 2016 | 11:00 AM-11:15 AM

INTERMEDIATE | **Products:** Splunk Enterprise | **Role:** Splunk Technical Champion, Architect, Developer, Administrator |

Track: Community Theater | **Session Focus:** Using Splunk | **Other Topics:** Best Practices, Getting Data In, Dev Tools

Speakers

Burch Simon, Senior Sales Engineer, Splunk

[Recording](#) | [Slides](#)



I sense much fear in you.

Install & Setup

Already done to your lab machines

Download Docker

<https://www.docker.com/>

What is Docker? Product Get Docker Docs Community Create Docker ID Sign In

New Release of Docker Enterprise Edition

Advancing CaaS leadership with a platform for modernizing diverse applications without disruption.

Free Hosted Trial Learn More

For Desktops
Mac
Windows
For Cloud Providers
AWS
Azure
For Servers
Windows Server
CentOS
Debian
Fedora
Oracle Linux
RHEL
SLES
Ubuntu

Join us in copenhagen!
dockercon17 october 16-18
register now

For Developers For IT Pros For The Enterprise

What is Docker? Product Get Docker Docs Community Create Docker ID Sign In

Docker for Mac


The fastest and easiest way to get started with Docker on Mac


Download from Docker Store


Overview Features Availability Resources

Join us in copenhagen!
dockercon17 october 16-18
register now

Hosted in Docker Store


docker store

[Explore](#)
[Publish](#)
[Feedback](#)

sloshburch



Docker Community Edition for Mac

By Docker

The fastest and easiest way to get started with Docker on Mac

Categories: [Docker Community Editions](#)

Get Docker Community Edition for Mac

Docker for Mac is available for free.

Requires Apple Mac OS Yosemite 10.10.3 or above.
Download [Docker Toolbox](#) for previous OS versions.

By downloading this, you agree to the terms of the [Docker Software End User License Agreement](#)

[Get Docker](#)
[Usage Instructions](#)

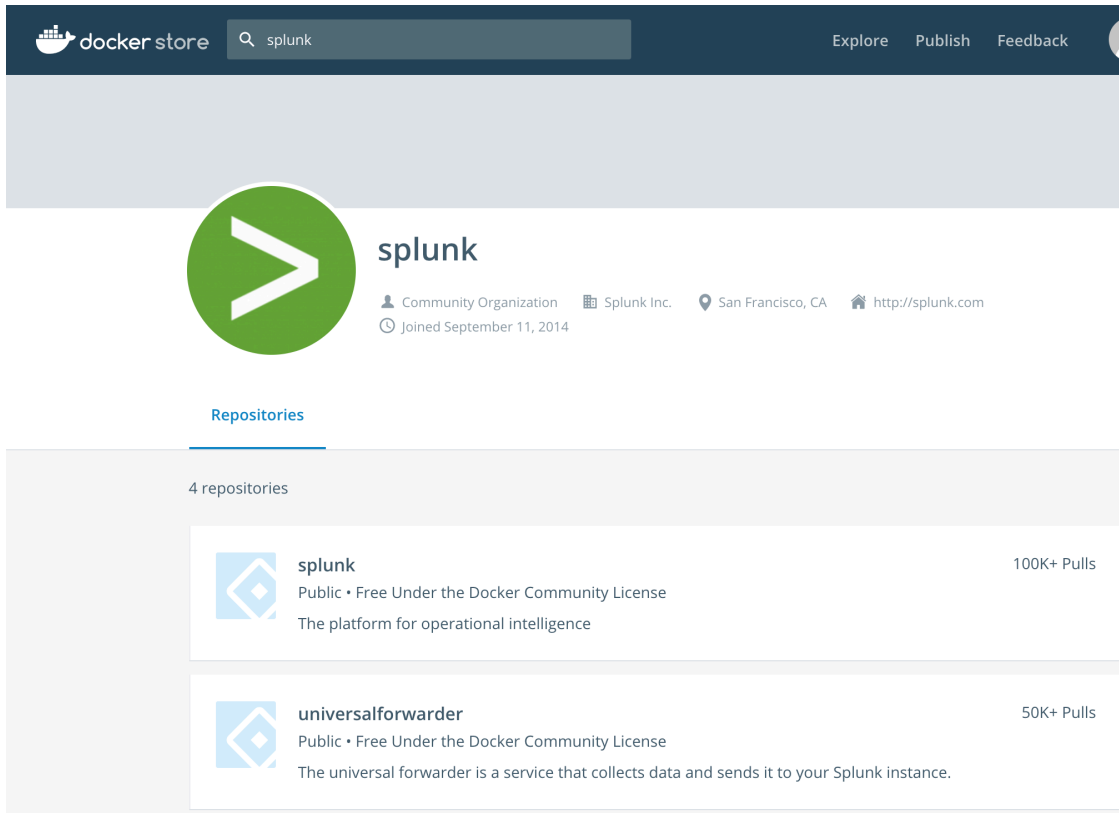
DESCRIPTION	REVIEWS	RESOURCES
<h3>Docker CE for Mac</h3> <p>Docker CE for Mac is an easy-to-install desktop app for building, debugging, and testing Dockerized apps on a Mac. Docker for Mac is a complete development environment deeply integrated with the Mac OS Hypervisor framework, networking, and filesystem. Docker for Mac is the fastest and most reliable way to run Docker on a Mac.</p>		

Features and Benefits

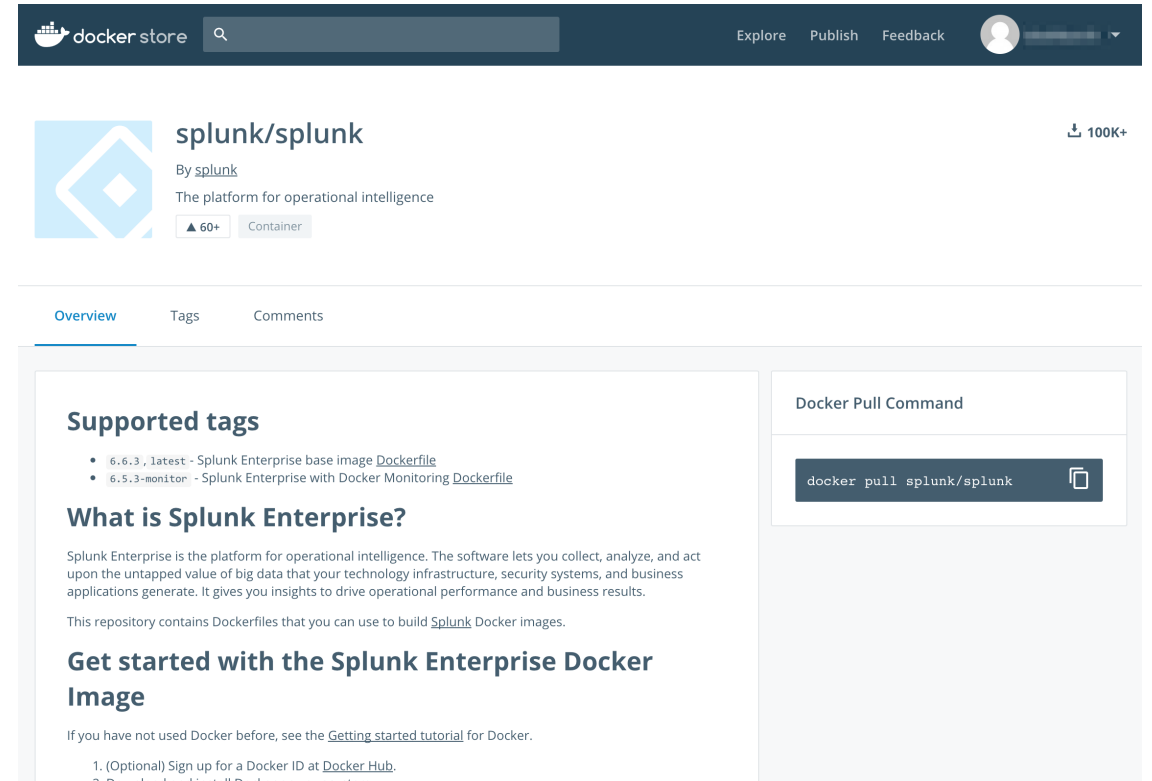
- Easy installation and setup of a complete Docker development environment for the Mac.
- Integrated Docker platform and tools [Docker command line](#), [Docker Compose](#), and [Docker Notary](#) command line.
- Automatic updates with channels for monthly Edge and quarterly Stable versions of Docker.
- Fast and reliable performance with native macOS virtualization running a custom minimal Linux distro.
- Seamless volume mounting for code and data, including file change notifications that unlock fast edit-test cycles.

Splunk Images

<https://store.docker.com/profiles/splunk>



The screenshot shows the Docker Store profile for 'splunk'. At the top, there's a search bar with 'splunk' entered and navigation links for 'Explore', 'Publish', and 'Feedback'. Below the header, the profile name 'splunk' is displayed next to a green circular logo with a white chevron. Underneath the name, it says 'Community Organization', 'Splunk Inc.', 'San Francisco, CA', and 'http://splunk.com'. It also notes 'Joined September 11, 2014'. A section titled 'Repositories' shows a list of 4 repositories. The first repository is 'splunk', which is public, free under the Docker Community License, and has 100K+ pulls. The second repository is 'universalforwarder', also public and free under the Docker Community License, with 50K+ pulls. The description for 'universalforwarder' states: 'The universal forwarder is a service that collects data and sends it to your Splunk instance.'



The screenshot shows the Docker Store page for the 'splunk/splunk' image. The header is similar to the previous screenshot. The main section features the 'splunk/splunk' image name, the creator 'By splunk', and the description 'The platform for operational intelligence'. It shows '60+' stars and 'Container' architecture. Below this, there are tabs for 'Overview', 'Tags', and 'Comments'. The 'Overview' tab is active, showing 'Supported tags' with two entries: '6.6.3, latest - Splunk Enterprise base image Dockerfile' and '6.5.3-monitor - Splunk Enterprise with Docker Monitoring Dockerfile'. A section titled 'What is Splunk Enterprise?' explains that it's the platform for operational intelligence. Below that, it says 'This repository contains Dockerfiles that you can use to build Splunk Docker images.' A section titled 'Get started with the Splunk Enterprise Docker Image' provides instructions: 1. (Optional) Sign up for a Docker ID at Docker Hub. 2. Download and install Docker on your system. On the right side, there's a 'Docker Pull Command' section with a button that says 'docker pull splunk/splunk' and a copy icon.

docker pull splunk/splunk

```
$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
splunk/splunk	latest	9cad3d52dc92	9 days ago	736MB

Command Crash Course

Put on your helmet

Instantiate & Start Splunk

► `docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk`

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"

Instantiate & Start Splunk

► `docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk`

- `run`

Run a command in a new container

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5015L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5035L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=50185L9FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5015L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5035L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=50185L9FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5015L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5035L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=50185L9FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:53.0) Gecko/20100101 Firefox/53.0"

Instantiate & Start Splunk

```
► docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk
```

- `run` Run a command in a new container
- `-P, --publish-all` Publish all exposed ports to random ports

Instantiate & Start Splunk

```
► docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk
```

- run

Run a command in a new container

- -P, --publish-all

Publish all exposed ports to random ports

- `-d, --detach`

Run container in background and print container ID

Instantiate & Start Splunk

```
▶ docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk
```

- run

Run a command in a new container

- `-P, --publish-all`

Publish all exposed ports to random ports

- `-d, --detach`

Run container in background and print container ID

- `-e, --env list`

Set environment variables

Instantiate & Start Splunk

► `docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk`

- `run` Run a command in a new container
- `-P, --publish-all` Publish all exposed ports to random ports
- `-d, --detach` Run container in background and print container ID
- `-e, --env list` Set environment variables
 - `SPLUNK_START_ARGS="--accept-license"`

Instantiate & Start Splunk

```
► docker run -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk
```

- `run` Run a command in a new container
- `-P, --publish-all` Publish all exposed ports to random ports
- `-d, --detach` Run container in background and print container ID
- `-e, --env list` Set environment variables
 - `SPLUNK_START_ARGS="--accept-license"`
- `splunk/splunk` Image name

Now what?

► \$ docker container list

- CONTAINER ID unique id
- IMAGE splunk/splunk
- COMMAND out of scope for us today
- CREATED relative time existing
- STATUS relative time running
- PORTS Port mappings. [See below](#)
- NAMES Random name (unless --name used)

► 0.0.0.0:32784->8000/tcp

- localhost:32784 traffic to container port 8000 (splunk web!)
- 32784 different each time (-P)

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.189] "GET /category.screen?category_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"
```

Look ma! Splunk!

The screenshot shows the Splunk Enterprise web interface in a browser. The address bar displays `localhost:32784/en-US/app/launcher/home`. The top navigation bar includes the Splunk logo, a user menu for 'Administrator', and links for 'Messages', 'Settings', and 'Activities'. A left sidebar contains 'Apps' and a large green button for 'Search & Reporting'. The main content area is titled 'Explore Splunk Enterprise' and features three green circular icons with corresponding text and descriptions:

- Product Tours**: New to Splunk? Take a tour to help you on your way.
- Add Data**: Add or forward data to Splunk Enterprise. Afterwards, you may [extract fields](#).
- Explore Data**: Explore data and define how Splunk parses that data.

At the bottom left, there is a faint, partially visible log snippet showing network traffic details.

Terminal Access

► But not much installed

- `docker exec -it <container name|id> bash`
 - `-i, --interactive` Keep STDIN open even if not attached
 - `-t, --tty` Allocate a pseudo-TTY
- But not much installed
- Not even vi
 - `apt-get FTW!`

Local Editing

- ▶ Or, mount a folder!
 - `-v, --volume list` Bind mount a volume
 - Example: `-v apps/local_app:/opt/splunk/etc/apps/remote_app`
 - `local_app` is a folder on the host; `remote_app` lives in the container
- ▶ Directly edit on your host (GUI editor)
- ▶ Direct link == edits reflected in container

Key Docker Commands

<https://splunk.box.com/v/blueprints-docker-sandbox-ref>

► Create and start a Splunk container

- `docker run --name foo -P -d -e SPLUNK_START_ARGS="--accept-license" splunk/splunk`
- Optional: `...license" -v ~/Desktop/myapp:/opt/splunk/etc/apps/conf2017_app splunk/s...`

► Navigate web browser to container

- `docker container list`

► Stop a container

- `docker stop foo`

► Start a container

- `docker start foo`

► Destroy a container

- `docker rm -fv foo`
 - `-f, --force` Force the removal of a running container (uses SIGKILL)
 - `-v, --volumes` Remove the volumes associated with the container

Create a Splunk Sandbox

This is where you come in...lazy bones ;)

should you choose to accept it...

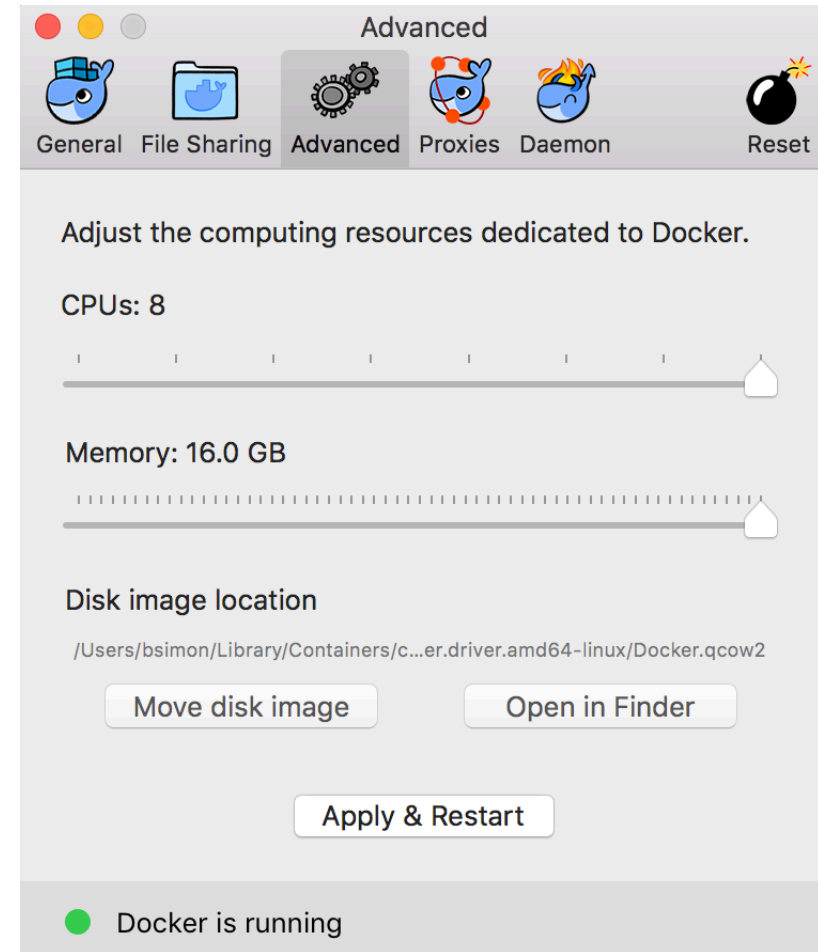
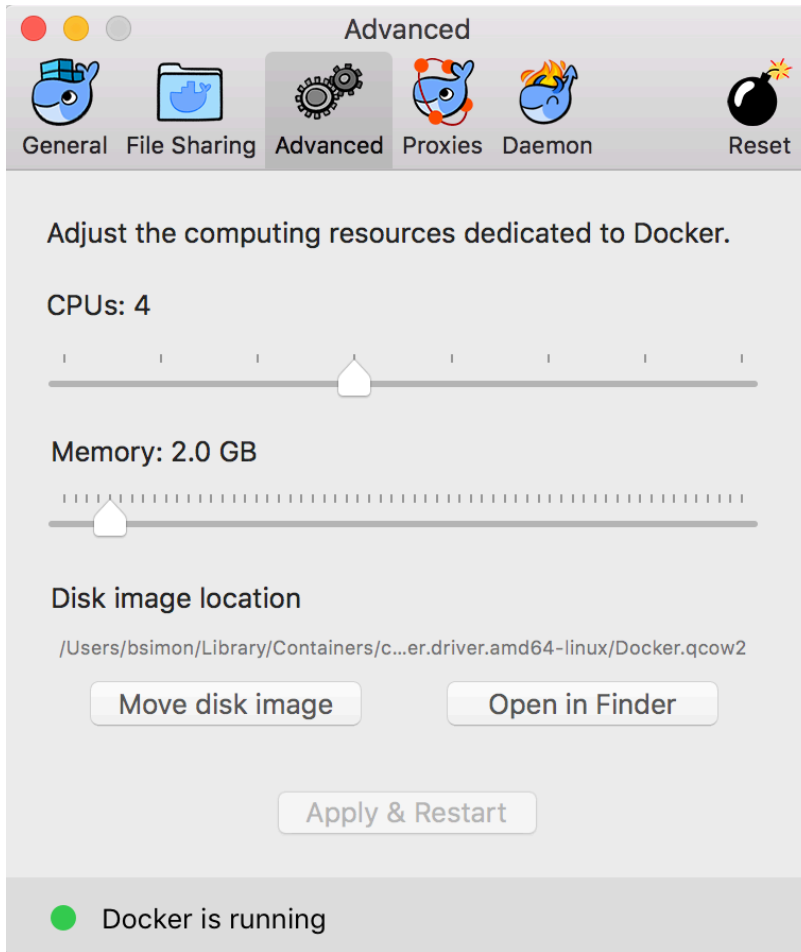
- ▶ Create and Connect many containers
- ▶ Change settings
 - Suggestion: http port and try UI restart ;)
- ▶ Destroy!
- ▶ Change environment variables, set hostname, etc...
 - <https://store.docker.com/community/images/splunk/splunk>
- ▶ Load Tutorial App & add web.conf settings
 - http://docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/CustomVizTutorial#Development_mode_settings

Next Steps!



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5015L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.20 (Win
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5055L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/4.0 (compatible; MSN
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.11 "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=50185L9FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/4.0 (compatible; MSN
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.11 "GET /category.screen?category_id=FLOWERS&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/4.0 (compatible; MSN
action=purchase&is.com/nl-02" 468 125.17 14.11 "GET /category.screen?category_id=FLOWERS&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/4.0 (compatible; MSN
buttercup-shopping.com/nl-02" 468 125.17 14.11 "GET /category.screen?category_id=FLOWERS&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/4.0 (compatible; MSN

Container Resources



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FI-SW-03"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=FI-SW-03"
http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=FI-SW-03"
http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=FI-SW-03"
http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=FI-SW-03"
http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D185L8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=FI-SW-03"
```


Do More!

<https://store.docker.com/community/images/splunk/splunk>

Ports

This Docker container exposes the following network ports:

- 8000/tcp - Splunk Web interface
- 8088/tcp - HTTP Event Collector
- 8088/tcp - Splunk Services
- 8191/tcp - Application Key Value Store
- 9997/tcp - Splunk receiving Port (not used by default) typically used by the Splunk Universal Forwarder
- 1514/tcp - Network Input (not used by default) typically used to collect syslog TCP data

This Docker image uses port 1514 instead of the standard port 514 for the syslog port because network ports below 1024 require root access. See [Run Splunk Enterprise as a different or non-root user](#).

Hostname

When you use this Docker image, set a `hostname` for it. If you recreate the instance later, the image retains the hostname.

Basic configuration with Environment Variables

You can use environment variables for basic configuration of the indexer and forwarder. For more advanced configuration, create configuration files within the container or use a Splunk deployment server to deliver configurations to the instance.

- `SPLUNK_ENABLE_DEPLOY_SERVER='true'` - Enables deployment server on Indexer.
- `SPLUNK_DEPLOYMENT_SERVER=<servername>:<port>` - [configure deployment client](#). Set deployment server url.
 - Example: `--env SPLUNK_DEPLOYMENT_SERVER='splunkdeploymentserver:8089'`.
- `SPLUNK_ENABLE_LISTEN=<port>` - enable [receiving](#).
 - Additional configuration is available using `SPLUNK_ENABLE_LISTEN_ARGS` environment variable.
- `SPLUNK_FORWARD_SERVER=<servername>:<port>` - [forward](#) data to indexer.
 - Additional configuration is available using `SPLUNK_FORWARD_SERVER_ARGS` environment variable.
 - Additional forwarders can be set up using `SPLUNK_FORWARD_SERVER<1..30>` and `SPLUNK_FORWARD_SERVER<1..30>_ARGS`.
 - Example: `--env SPLUNK_FORWARD_SERVER='splunkindexer:9997' --env SPLUNK_FORWARD_SERVER_ARGS='method clone' --env SPLUNK_FORWARD_SERVER_1='splunkindexer2:9997' --env SPLUNK_FORWARD_SERVER_1_ARGS='method clone'`.
- `SPLUNK_ADD='<monitor|add> <what_to_monitor|what_to_add>'` - execute add command, for example to [monitor files](#) or [listen](#) on specific ports.
 - Additional add commands can be executed (up to 30) using `SPLUNK_ADD<1..30>`.
 - Example `--env SPLUNK_ADD='udp 1514' --env SPLUNK_ADD_1='monitor /var/log/*'`.
- `SPLUNK_CMD='any splunk command'` - execute any splunk command.
 - Additional commands can be executed (up to 30) using `SPLUNK_CMD<1..30>`.
 - Example `--env SPLUNK_CMD='edit user admin -password random_password -role admin -auth`

> 60 day then doing it wrong



With the Splunk developer license, you can use our SDKs and other developer tools to build big data applications that plug into Splunk's map/reduce data-processing pipeline, storage technology, and management facilities. And, you can extend and enhance Splunk Web through our app framework. Just follow a few simple steps below and you'll be on your way.

- You want to build applications that work on top of Splunk platform, then you need a license to Splunk Enterprise software, which is our flagship core product. Splunk Enterprise is a snap to install and easy to configure. Download it [here](#).

- You'll need to [request your developer license](#).

- Learn how to [install your license](#).
- Get the SDKs from [Splunk GitHub](#).
- Check out the apps on [Splunkbase](#).
- Follow us on Twitter for latest updates [@splunkdev](#).
- Join our [Google Group](#).

Upgrade Splunk Image

docker pull splunk/splunk

```
$ docker pull splunk/splunk:latest
```

```
Using default tag: latest
```

```
latest: Pulling from splunk/splunk
```

```
ad74af05f5a2: Pull complete
```

```
6ed26c881126: Pull complete
```

```
0efc5eeb5075: Pull complete
```

```
123d19a3ee15: Pull complete
```

```
6fe48f1452ee: Pull complete
```

```
fc6bbc9992f6: Pull complete
```

```
8ebdf9134129: Pull complete
```

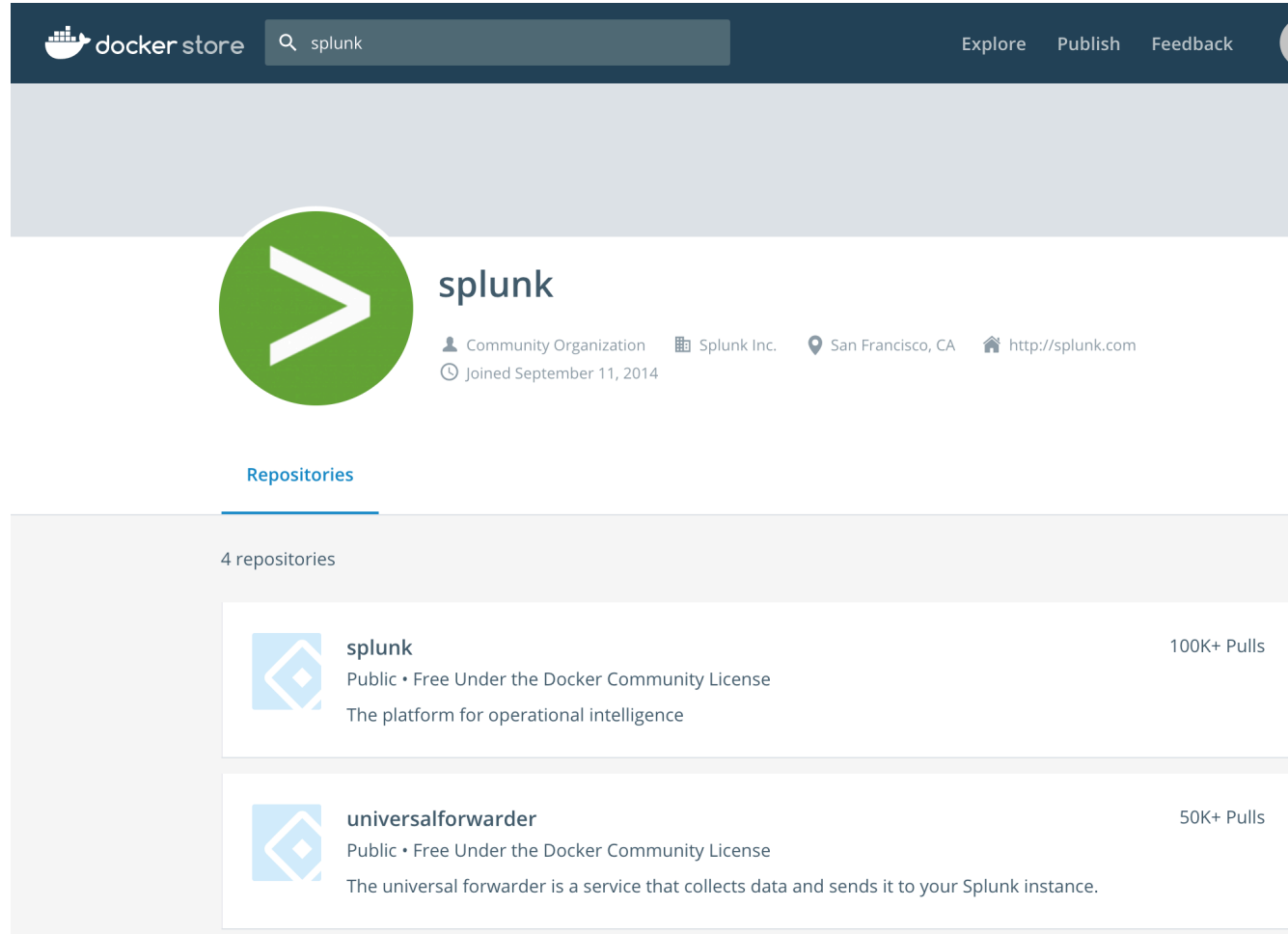
```
Digest: sha256:1be3208a6c1d96ca5ad320fc21cbfcf06428e3ea12f10773e2efc7d2dbb4b522
```

```
Status: Downloaded newer image for splunk/splunk:latest
```

```
$ docker images
```


REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
splunk/splunk	latest	9cad3d52dc92	9 days ago	736MB
splunk/splunk	6.6.2	1b6fa73035a6	5 weeks ago	736MB

Universal Forwarder



The screenshot shows the Docker Store interface for the 'splunk' organization. The header includes the Docker Store logo, a search bar with 'splunk' entered, and links for 'Explore', 'Publish', and 'Feedback'. The main content area features the 'splunk' organization profile, which includes a green circular logo with a white chevron, the organization name 'splunk', and details: 'Community Organization', 'Splunk Inc.', 'San Francisco, CA', 'http://splunk.com', and 'Joined September 11, 2014'. Below the profile, the 'Repositories' section is highlighted, showing a list of 4 repositories. Two repositories are visible: 'splunk' with 100K+ pulls and 'universalforwarder' with 50K+ pulls. Both are public and free under the Docker Community License. The 'universalforwarder' repository description states: 'The universal forwarder is a service that collects data and sends it to your Splunk instance.'


docker store Explore Publish Feedback


 **splunk**

Community Organization Splunk Inc. San Francisco, CA <http://splunk.com>
Joined September 11, 2014

Repositories

4 repositories

 **splunk** 100K+ Pulls
Public • Free Under the Docker Community License
The platform for operational intelligence

 **universalforwarder** 50K+ Pulls
Public • Free Under the Docker Community License
The universal forwarder is a service that collects data and sends it to your Splunk instance.

Splunk n' Box

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

Breakout Session

Splunk n' Box

Wednesday, September 27, 2017 | 3:30 PM-4:15 PM

INTERMEDIATE

Mo Hassan, Missouri, Splunk Inc.

I have written an extensive and feature-rich bash script (4000+ lines) that can be used by Splunk admins, regular users and Splunk employees to test multiple Splunk deployment scenarios using Docker (while shielding the user from learning Docker in the process). The script is widely used by Splunk customers, Splunk SEs and Splunk partners. The code base is the result of five months of development and testing.

Less

```
Splunk n' Box v4.2.2.9: MAIN MENU [Containers:0 Running:0 Paused:0 Stopped:0 I
=>DOCKER:[ver:17.03.1-ce cpu:8 mem:15GB] OS:[FreeMem:5.2GB Load:3.39] Image:[splunknb
```

MAIN - MENU

- 1) Manage All Containers & Images
 - 2) Manage Lunch & Learn Containers
 - 3) Manage Splunk Clusters
 - 4) Manage Splunk Demos [****internal use only****]
 - 5) Manage 3Rd Party Containers & Images [****under construction****]
 - 6) Manage System
 - 7) Change Log Level
 - ?) Help
 - Q) Quit
- Enter your choice [1-6] _

What Now?

Related breakout
sessions and
activities...



8DEC0D

1. Rate this! (be honest)
2. Collaborate: #docker-sandbox
 - Sign Up @ <http://splk.it/slack>
3. Customer Success Studio
4. More talks, search for
 - Blueprints
 - Burch
 - Champagne
 - Delaney
 - Optimization
 - Best Practices
 - Veuve

Questions & Discussion?

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

splunk> .conf2017