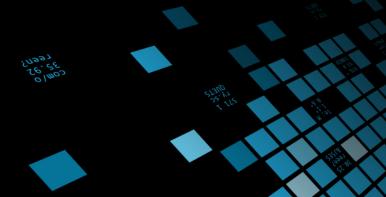




Michael Clayfield | Partner Consultant

03/09/2017 | 1.1



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.

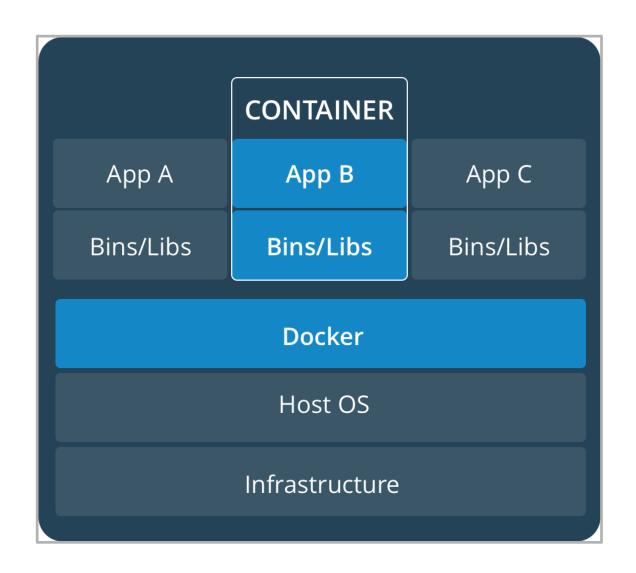
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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.



What is Docker?

- Docker is a container system
- Binaries and libraries are packaged in each container





Why use Splunk on Docker?

- Easily create Splunk clusters
 - Replicate production environment in a smaller footprint
 - Test cluster upgrades
 - Lab environments
- Reduced hardware resources and costs
- After initial setup, clusters can be created on-demand

▶ Not recommended for use in production environments



Getting Docker

- www.docker.com
- Community Edition
- www.docker.com/community-edition
- ► Installers available for:
 - Windows
 - Mac
 - Linux
 - AWS & Azure



Docker images

- A Docker image is a collection of binaries and settings to be used when starting a container
- Images are defined in a 'Dockerfile'

► There are official Splunk Docker images



hub.docker.com/r/splunk/splunk/



github.com/splunk/docker-splunk



Splunk Image from Docker Hub

- Splunk Enterprise:
 - "docker pull splunk/splunk"
- Splunk Universal Forwarder:
 - "docker pull splunk/universalforwarder"

- Tags can be used to download a specific version.
 - "docker pull splunk/splunk:6.5.3"
 - "docker pull splunk/universalforwarder:latest"



Splunk Image from Github

- "git clone https://github.com/splunk/docker-splunk"
- Splunk Enterprise
 - "docker build -t splunkenterprise ./enterprise/"
- Splunk Universal Forwarder
 - "docker build -t splunkuniversalforwarder ./universalforwarder/"
- Change branch for other versions of Splunk before building image
 - "git checkout 6.3"



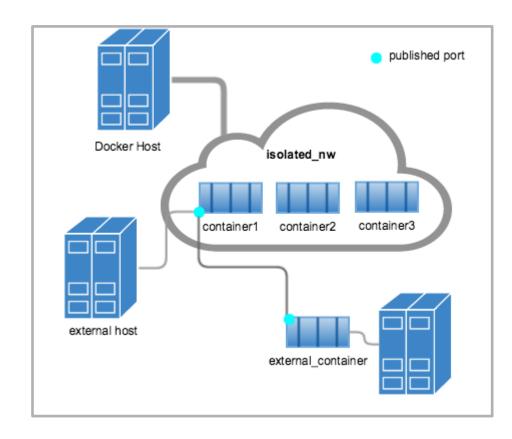
Running Splunk Images

- Creating a container
 - docker run –name splunk imagename
- Starting/stopping a container
 - docker stop splunk
 - docker start splunk
- Removing a container
 - docker rm splunk



Managing Ports

- Docker containers run in an isolated virtual network
 - -p hostip:hostport:destport
 - -p 0.0.0.0:8000:8000
 - -p 8000:8000
 - -p 8000
 - -p 443:8000
 - -p 1500-1600





Storage in Docker

- Changing ports or storage or upgrading the container version requires the container be removed and run again
 - docker stop splunk && docker rm splunk
 - docker run -p 8000 -name splunk splunk/splunk
- ► This destroys all data!
- Ways to have persistent data:
 - Volumes
 - Bind mounts



Bind mounts vs volumes

Bind mounts

- ► Files or folders on the host machine are mounted in the container
 - Easy to edit files
 - Dependant on host folder structure
 - Harder to share and migrate between hosts

Volumes

- Files or folders in a container that are managed by Docker
 - Everything is contained within Docker
 - Easier to back-up and migrate than bind mounts
 - Ability to use volume drivers

Both are used with the argument: --mount



Pulling it all together

```
docker run --name splunk \
    -p 80:8000 \
    -p 8089 \
    -p 9997 \
    --mount /data/splunk/etc:/opt/splunk/etc \
    --mount /data/splunk/var:/opt/splunk/var \
    -e SPLUNK_START_ARGS="--accept-license" \
    splunk/splunk:6.6.2
```



Docker Compose

- Used for defining and running multiple containers
- Written in YAML
- docs.docker.com/compose
- ► A sample Docker Compose file is in the Splunk Docker Github repo
- github.com/splunk/docker-splunk



Q&A

michael.clayfield@jds.net.au





Further Information

- Docker Documentation:
- ▶ docs.docker.com
- Docker Glossary
- docs.docker.com/glossary



Thank you

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

