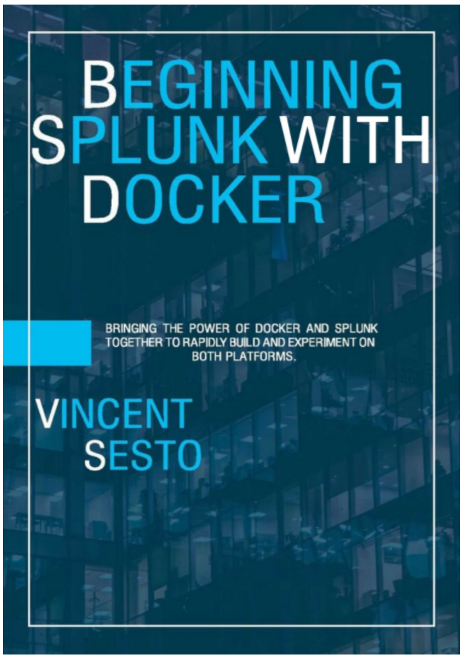
DOCKER & SPLUNK COMMAND REFERENCE CHEAT SHEET

THIS REFERENCE GUIDE HAS BEEN TAKEN FROM THE BOOK "BEGINNING SPLUNK WITH DOCKER" BY VINCENT SESTO

FIRST STEPS

Display the Version of Docker running on your system. If you need to instal Docker go to https://www.docker.com/get-docker	docker --version
Run the basic hello-world Docker service.	docker run hello-world
Search for a Docker image or type that you need from Docker Hub. Replace <image> with the image you are looking for. Eg; splunk	docker search <image>
Pull the latest stable version of your required image.	docker pull <image>:latest
Display all running Docker containers.	docker ps
Display all running and stopped Docker containers.	docker ps -a
View all Docker images available on your system.	docker images



BEGINNING SPLUNK WITH DOCKER

BRINGING THE POWER OF DOCKER AND SPLUNK TOGETHER TO RAPIDLY BUILD AND EXPERIMENT ON BOTH PLATFORMS.

VINCENT SESTO

Beginning Splunk With Docker

This book gets you started working with Splunk and Docker together. It book takes you through the command line with Docker Fundamentals, expands your knowledge and image functionality by using Dockerfiles and then provides you with the power of working with Docker Compose.

GET YOUR SPLUNK IMAGE RUNNING WITH DOCKER

Running Splunk as a Docker container with variables to accept license and set the user as root. Port 8000 is mapped to the host and we are using the Splunk image. Open a browser to http://localhost:8000 when complete.

```
docker run -d -e "SPLUNK_START_ARGS=--accept-license" -e
"SPLUNK_USER=root" -p 8000:8000 splunk/splunk
```

Once your container has started up. Go to http://localhost:8000 in your browser and start up your new Splunk environment.

Show all relevant information for a Docker container.

```
docker inspect <cont_id>
```

Access the shell of a running container.

```
docker attach <cont_id>
```

Perform the touch command on a running container using exec.

```
docker exec -d <cont_id>
touch /tmp/test.txt
```

Access the bash shell of a running container.

```
docker exec -it <
cont_id> /bin/bash
```

CREATING DOCKERFILES

To help streamline the process of creating and running our Docker containers, we can use a Dockerfile to specify all the details for the container we are wanting to run. Below is an example Dockerfile.

```
FROM splunk/splunk:latest
MAINTAINER vince.sesto@gmail.com

# Set up environment variables
ENV SPLUNK_START_ARGS --accept-license
ENV SPLUNK_USER root

# Run touch .ui_login in the same directory as your Dockerfile
# Copy ui_login to stop the first time login screen
COPY .ui_login /opt/splunk/etc/.ui_login

# If you have a Splunk App ready to be installed
COPY mood_radiator/ /opt/splunk/etc/apps/mood_radiator/

# In case we need to install anything extra
RUN apt-get update && apt-get install -y vim
```

Build your image from a Dockerfile and give it a name.

```
docker build -t <name> .
```

Run a Docker container in detached mode exposing port 8000.

```
docker run -d -p
8000:8000 <name>
```

The command below will allow you to clean up your environment. It will kill all running containers, then remove all stopped containers, finally it will the delete any docker images.

```
docker kill $(docker ps -q); docker rm -f $(docker ps -a -q)
docker rmi -f $(docker images -q)
```

MOVING TO DOCKER COMPOSE

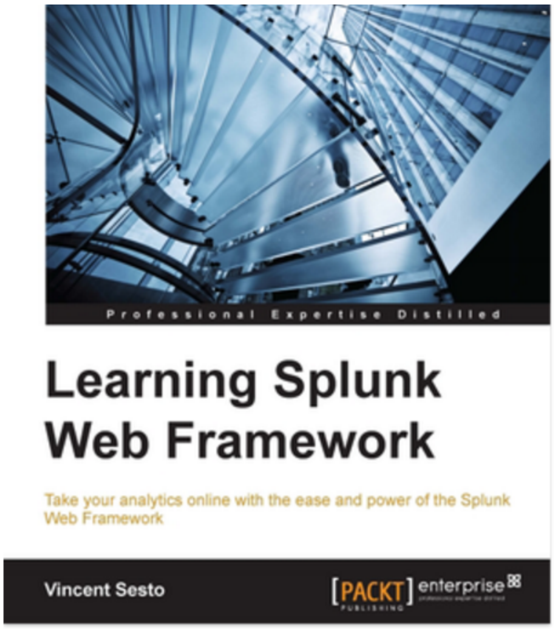
With Docker Compose, you can use a simple compose file to create numerous networked containers and images. The code below is a simple Splunk server and can be created by opening your text editor and saving the file as “docker-compose.yml”.

```
version: '3'
services:

  splunkserver:
    image: splunk/splunk
    hostname: splunkserver
    environment:
      SPLUNK_START_ARGS: --accept-license --answer-yes
      SPLUNK_ENABLE_LISTEN: 9997
      SPLUNK_USER: root
    ports:
      - "8000:8000"
      - "9997:9997"
      - "8088:8088"
```

Use Docker Compose to build and run your compose file in detached mode.

```
docker-compose up -d
```


Professional Expertise Distilled
Learning Splunk Web Framework
Take your analytics online with the ease and power of the Splunk Web Framework
Vincent Sesto
[PACKT] enterprise
PUBLISHING

Learning Splunk Web Framework

Take your analytics online with the ease and power of the Splunk Web Framework About This Book Want to build rich applications on the Web using Splunk? This book will be your ultimate guide! Learn to use web framework components with the help of this highly practical, example-rich guide Perform excellent Splunk analytics on the Web and bring that knowledge to your own projects.