



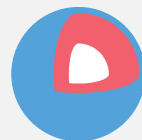
# Core OS

## **Building minimal containers**

by

Brian "redbeard" Harrington

**Principal Architect, CoreOS**





# Core OS

## Getting Weird with Containers

by

Brian "redbeard" Harrington

**Principal Architect, CoreOS**



# Brian “Redbeard” Harrington

Principal Architect

**CoreOS**

[redbeard@coreos.com](mailto:redbeard@coreos.com)

[github.com/brianredbeard](https://github.com/brianredbeard)

[twitter.com/brianredbeard](https://twitter.com/brianredbeard)

[brianredbeard.com](http://brianredbeard.com)



# Brian “Redbeard” Harrington

Principal Architect

**CoreOS**

[redbeard@coreos.com](mailto:redbeard@coreos.com)

[github.com/brianredbeard](https://github.com/brianredbeard)

[twitter.com/brianredbeard](https://twitter.com/brianredbeard)

[brianredbeard.com](http://brianredbeard.com)



WHO GETS EXCITED ABOUT

**TARBALLS**





# CONTAINER ATLAS

HANDBUCH DER  
CONTAINER ARCHITEKTUR

SLAWIK, BERGMANN, BUCHMEIER, TINNEY (Hrsg.)



gestalten



BREAK OUT  
THE ~~COOKIES~~  
BEER  
IT'S

**STORY  
TIME**



THERE ONCE WAS A LITTLE CONTAINER WHO WANTED TO GET



**TO  
PRODUCTION**





# BUT...



*MUCH LIKE*  
*REDBEARD*



**THE CONTAINER WAS  
GETTING A LITTLE  
TOO BIG**



AND ALL THE  
**PRODUCTION OPS**  
FOLKS SAID:



IF YOUR CONTAINERS ARE GETTING DEPLOYED  
ON **MY** INFRASTRUCTURE YOU BETTER  
COME CORRECT ON  
HOW **BIG**  
THEY ARE





TO WHICH THE  
**DEVELOPERS**  
REPLY:



BUT DISK SPACE IS  
**SO CHEAP**



AND SSD WRITE CYCLES ARE  
**EXPENSIVE**



# BIG CONTAINERS ARE A PROBLEM



# BIG CONTAINERS:

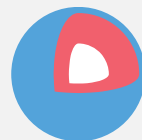
SLOW DOWN YOUR DEPLOYMENTS  
(NETWORK)





# BIG CONTAINERS:

CONSUME MORE SPACE  
(STORAGE)



# BIG CONTAINERS:

INCREASE COST OF OBJECT STORAGE  
(BUDGET)



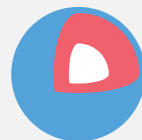
# BIG CONTAINERS:

DECREASE I/O PERFORMANCE  
(STORAGE)



# BIG CONTAINERS:

ARE HARDER TO AUDIT  
(SECURITY)



# **BIG CONTAINERS:**

NEED TO BE PUT ON A DIET







**LETS LOOK AT AN  
EXAMPLE:**



# The self-hosted web IRC client

Always connected.

```
npm -g install shout
```

version 0.51.0

Or try the **demo**.



### Step 3:

Verify that the image has been created:

```
$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	VIRTUAL
shout-img	latest	95da6797223b	9 minutes ago	833.1 M







# The source?

HTTP/1.1 200 OK

Content-Length: 592371

Access-Control-Allow-Origin: https://render.githubusercontent.com

Content-Security-Policy: default-src 'none'

X-XSS-Protection: 1; mode=block

X-Frame-Options: deny

X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=31536000

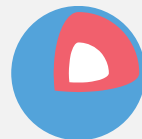
Vary: Authorization,Accept-Encoding

ETag: "7138ca6bda5430d1fdb9cf6e530d9cfd11247bd1"

Content-Type: application/zip

Content-Disposition: attachment; filename=shout-0.51.0.zip

Date: Wed, 29 Jul 2015 23:27:30 GMT



# The source?

HTTP/1.1 200 OK

Content-Length: 592371

Access-Control-Allow-Origin: https://render.githubusercontent.com

Content-Security-Policy: default-src 'none'

X-XSS-Protection: 1; mode=block

X-Frame-Options: deny

X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=31536000

Vary: Authorization,Accept-Encoding

ETag: "7138ca6bda5430d1fdb9f6e530d9cfd11247bd1"

Content-Type: application/zip

Content-Disposition: attachment; filename=shout-0.51.0.zip

Date: Wed, 29 Jul 2015 23:27:30 GMT



take note:  
**592KB**

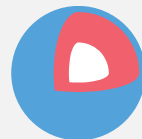


**FROM node**

**RUN npm -g install shout**

**EXPOSE 9000**

**CMD ["shout", "start"]**



**FROM ubuntu**

**RUN apt-get update && apt-get upgrade && \  
apt-get -y install nodejs**

**RUN npm -g install shout**

**EXPOSE 9000**

**CMD ["shout", "start"]**



**FROM ubuntu**

**ENV DEBIAN\_FRONTEND noninteractive**

**RUN apt-get update && apt-get upgrade && \  
apt-get -y install nodejs**

**RUN npm -g install shout**

**EXPOSE 9000**

**CMD ["shout", "start"]**



**FROM ubuntu**

**ENV DEBIAN\_FRONTEND noninteractive**

**RUN apt-key adv -keyserver keyserver.ubuntu.com -recv C0A52C50**

**RUN apt-get update && apt-get upgrade && \  
apt-get -y install nodejs**

**RUN npm -g install shout**

**EXPOSE 9000**

**CMD ["shout", "start"]**



**FROM buildpack-deps:jessie**

**# verify gpg and sha256: <http://nodejs.org/dist/v0.10.31/SHASUMS256.txt.asc>**

**# gpg: aka "Timothy J Fontaine (Work) <tj.fontaine@joyent.com>"**

**# gpg: aka "Julien Gilli <jgilli@fastmail.fm>"**

**RUN gpg --keyserver pool.sks-keyservers.net --recv-keys \**

**7937DFD2AB06298B2293C3187D33FF9D0246406D 114F43EE0176B71C7BC219DD50A3051F888C628D**

**ENV NODE\_VERSION 0.10.38**

**ENV NPM\_VERSION 2.7.3**

**RUN curl -SLO "http://nodejs.org/dist/v\$NODE\_VERSION/node-v\$NODE\_VERSION-linux-x64.tar.gz" \**

**&& curl -SLO "http://nodejs.org/dist/v\$NODE\_VERSION/SHASUMS256.txt.asc" \**

**&& gpg --verify SHASUMS256.txt.asc \**

**&& grep " node-v\$NODE\_VERSION-linux-x64.tar.gz\" SHASUMS256.txt.asc | sha256sum -c - \**

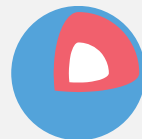
**&& tar -xzf "node-v\$NODE\_VERSION-linux-x64.tar.gz" -C /usr/local --strip-components=1 \**

**&& rm "node-v\$NODE\_VERSION-linux-x64.tar.gz" SHASUMS256.txt.asc \**

**&& npm install -g npm@"\$NPM\_VERSION" \**

**&& npm cache clear**

**CMD [ "node" ]**





```
$ docker images node
```

REPOSITORY	TAG	IMAGE ID	CREATED	VIRTUAL SIZE
node	latest	c03077d1e6a0	2 weeks ago	639.7 MB



what do we do?



# what **DO** we do?

- demystify how a container is built
- enumerate other ways to do it
- demonstrate how it's done



# LET'S STEP INTO THE KITCHEN



JULIA CHILD (PUBLIC DOMAIN)



WHO GETS EXCITED ABOUT

**TARBALLS**



REPEAT  
**AFTER REDBEARD**



A CONTAINER FILESYSTEM  
IS JUST A  
**TARBALL**

A CONTAINER FILESYSTEM ISN'T  
MAGIC...

IT'S JUST A **TARBALL**



anything that can  
make a tarball  
**CAN MAKE A CONTAINER**





```
$ mktemp -d  
/tmp/tmp.d3NqCJe2yJ
```



# grab gpg key:

```
$ curl -s -o /tmp/fedora.asc https://getfedora.org/static/8E1431D5.txt
```

# trust gpg key:

```
$ sudo rpm --import --root=/tmp/tmp.d3NqCJe2yJ/ /tmp/fedora.asc
```

# install packages signed with gpg key:

```
$ dnf --installroot=/tmp/tmp.d3NqCJe2yJ --releasever=22 \  
install httpd
```



```
$ cd /tmp/tmp.d3NqCJe2yJ  
$ tar zcvf ../fedora.tar ./
```



what do i do with this  
**hunk of junk?**



```
$ cat /tmp/fedora.tar | docker import - fedora *
```

(\* This has been fixed since the presentation. This is the correct syntax)



is it really  
**that simple?**



**YES**





really?



**YES**

**IT IS REALLY**

**THAT SIMPLE**



<demo>



</demo>



Don't I need a  
**Dockerfile?**



**NO**

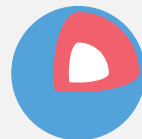


But I'll humor you....





```
$ cat Dockerfile  
FROM fedora  
  
CMD ["/bin/bash"]
```



<demo>



</demo>



And there are a **LOT** of  
tools to do similar  
processes...



- yum
- dnf
- debootstrap
- buildroot
- alpine
- gentoo



time for a PSA...



The More You Know!



**Are you.....**

**Utilizing framebuffers?**

***running a window  
manager?***

**Administering users?**

**Logging in?**

**Editing files?**





**these are the purview of  
general purpose  
computing**



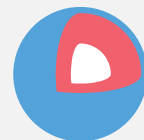


<http://buildroot.org>



BUILDROOT IS AN SDK FOR BUILDING

# **MINIMAL LINUX DISTROS**



<demo>



</demo>



# Agnostic

- Works with Docker, rkt, and others.
- The idea is to be able to build this through a continuous integration system like Buildbot, Jenkins, etc



# Signing

- Possible through `gpg` today with mechanisms for confirmed signing.
- Able to be automated by using `gpg-agent` to handle safe caching of credentials.



# QUESTIONS?

