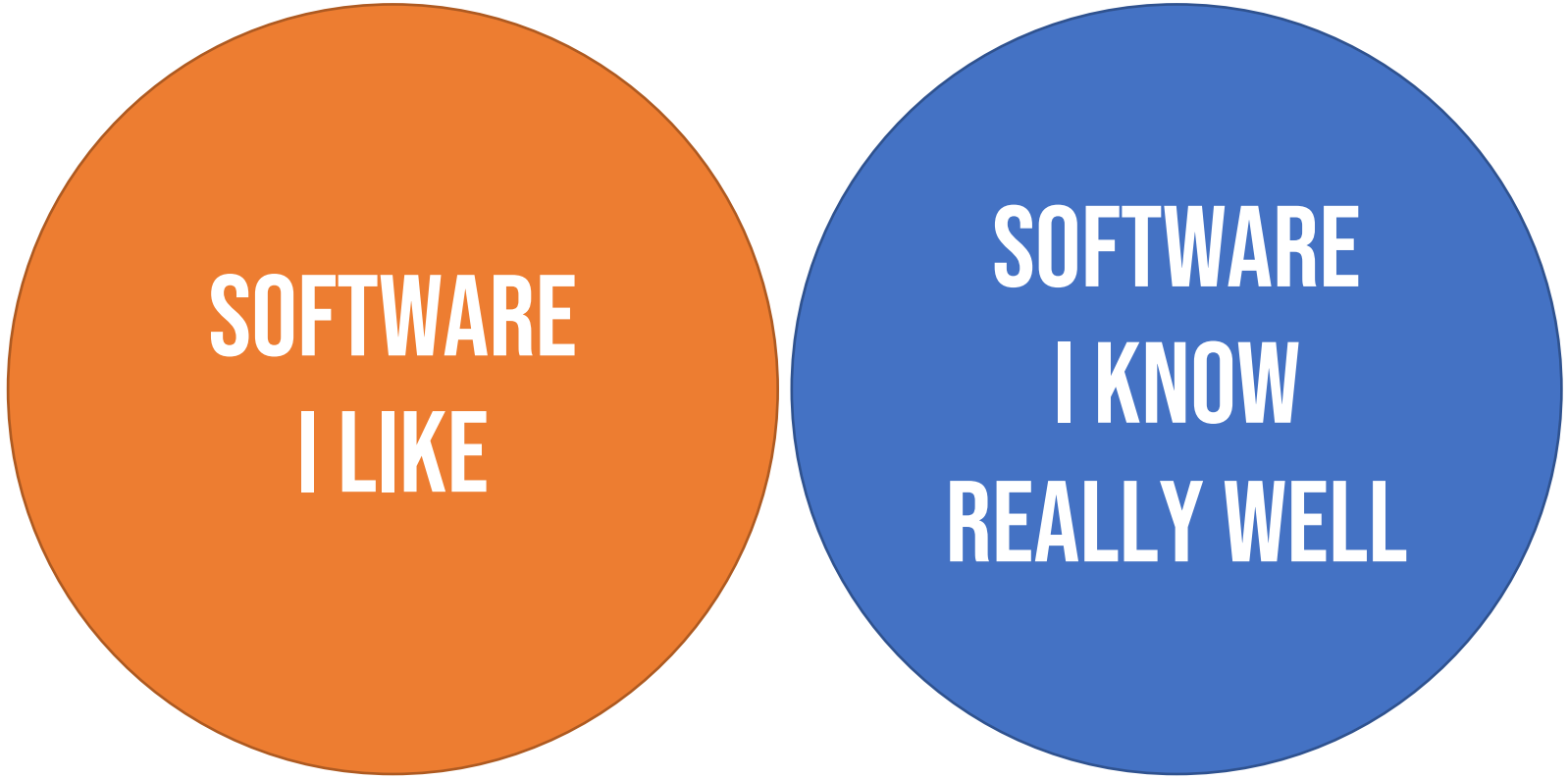
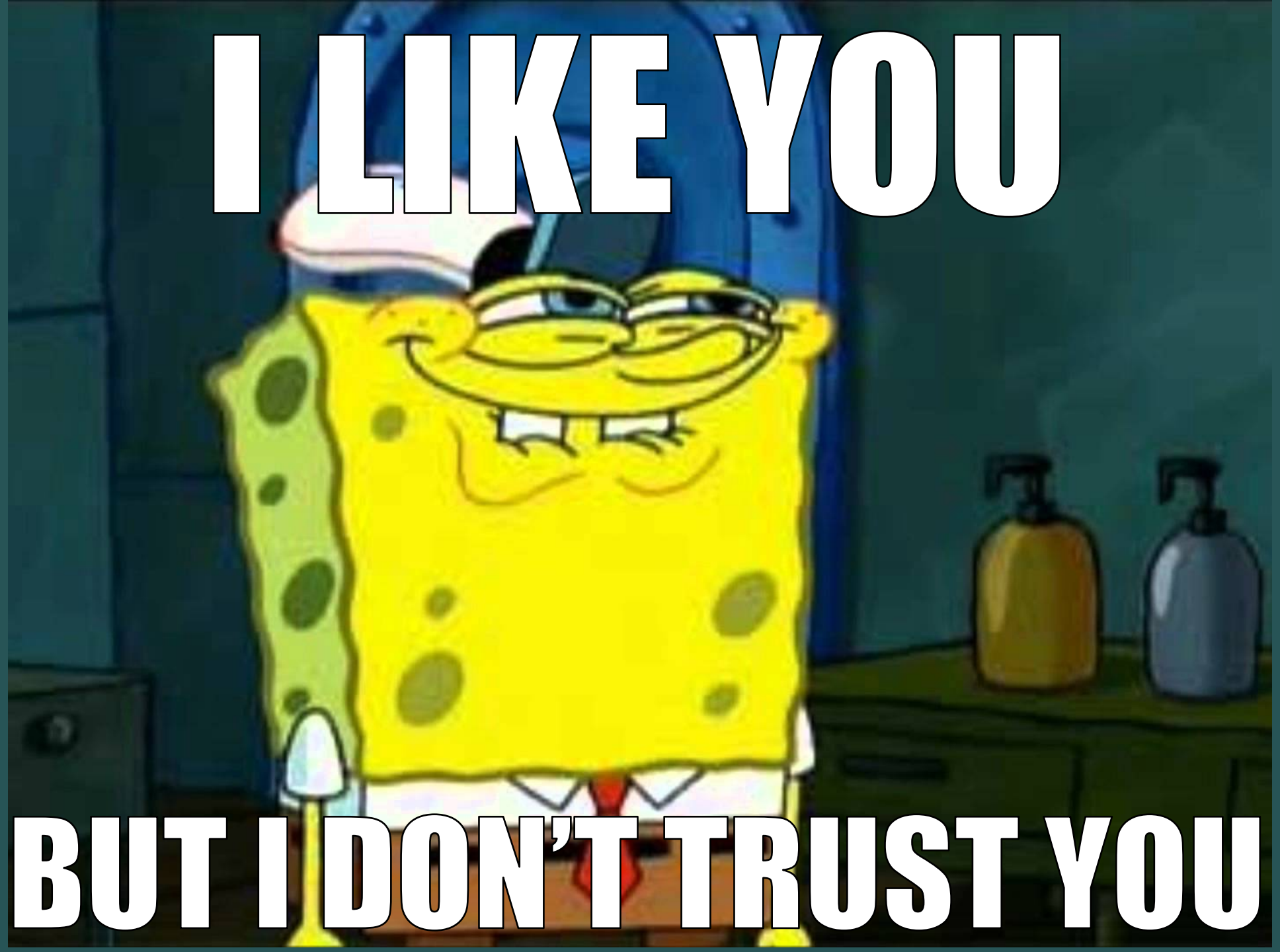
BEST PRACTICES IN IMPLEMENTING CONTAINER IMAGE PROMOTION PIPELINES


CONTAINERS


SOFTWARE
I LIKE
SOFTWARE
I KNOW
REALLY WELL


I LIKE YOU
BUT I DON'T TRUST YOU

BARUCH SADOGURSKY

CHIEF STICKER OFFICER

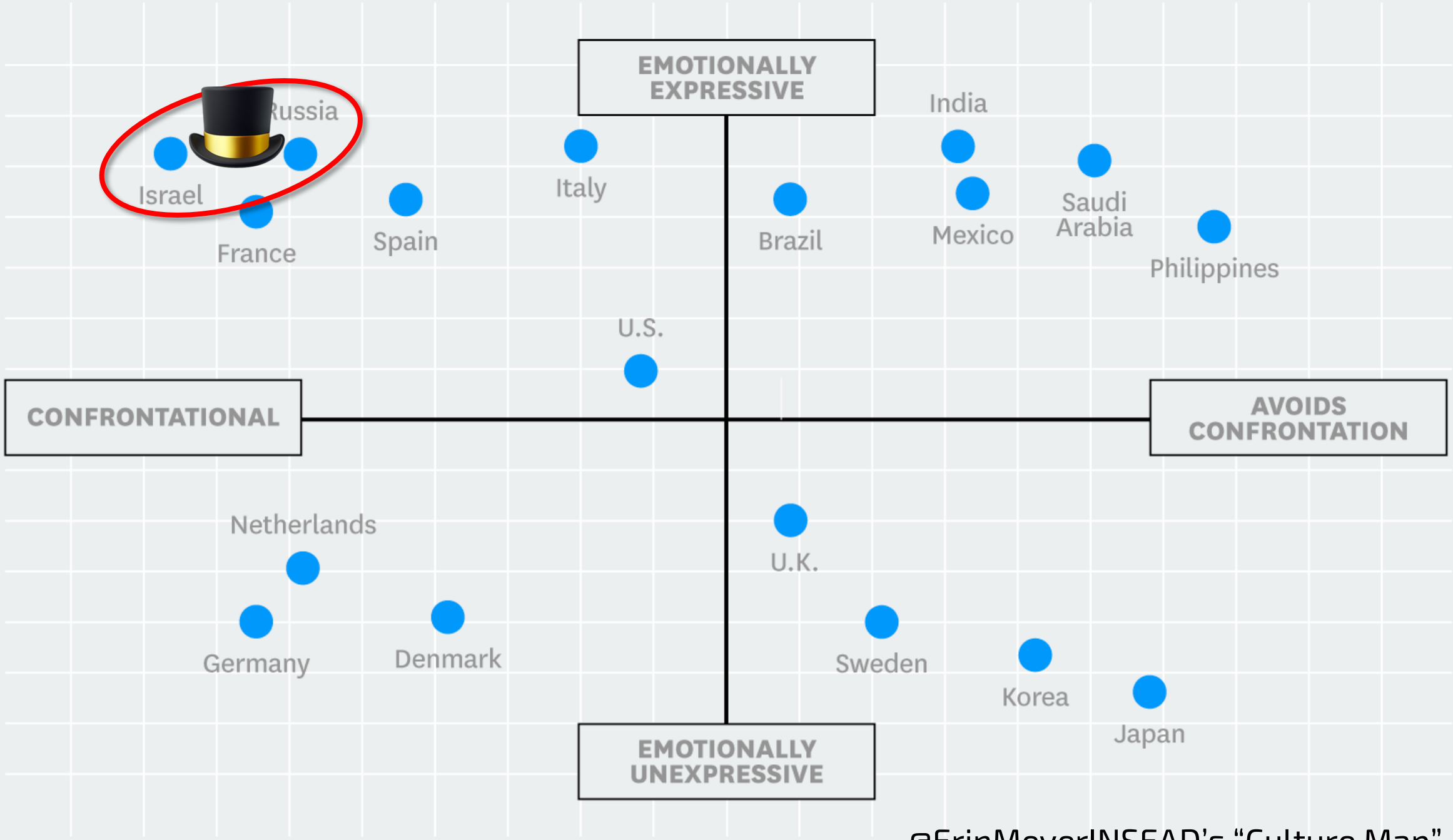
(ALSO 🎩 OF DEVELOPER ADVOCACY)

✉ JBARUCH@JFROG.COM

🐦 @JBARUCH

🎩 +1(408)890-9281

JFrog

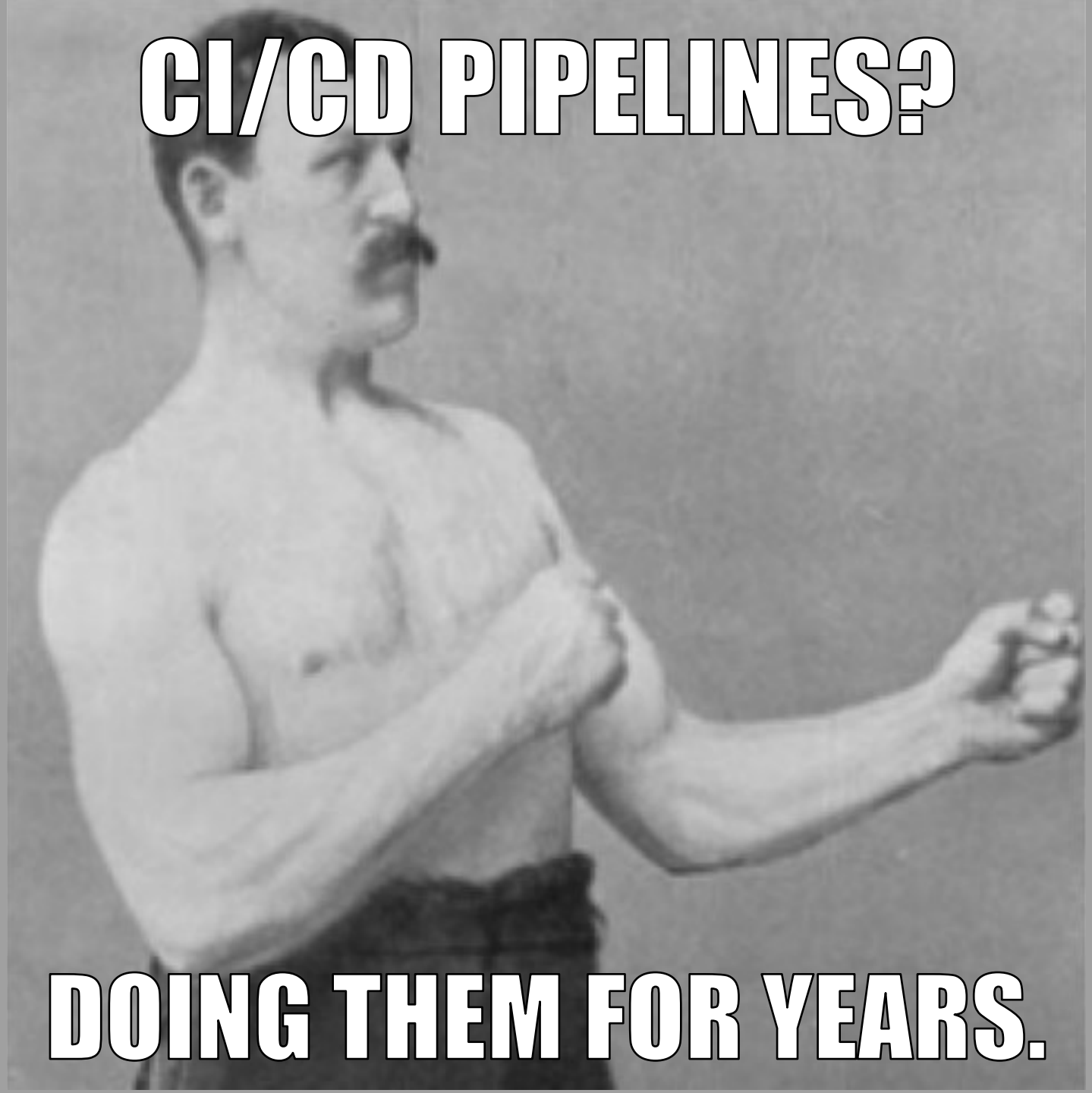


@ErinMeyerINSEAD's "Culture Map"

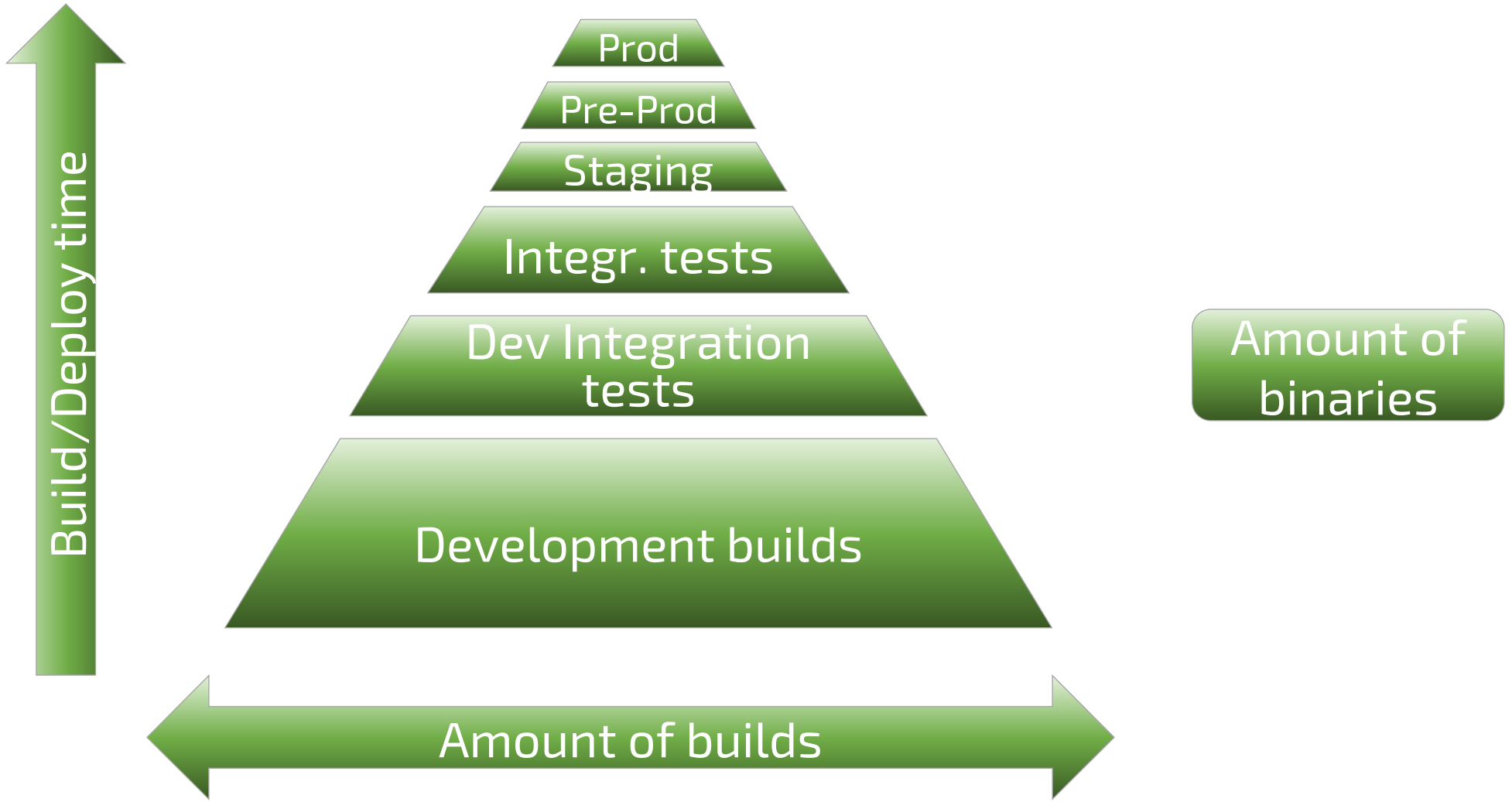
SHOWNOTES

- http://jfrog.com/shownotes
  - Slides
  - Video
  - Links
  - Comments, Ratings
  - Raffle

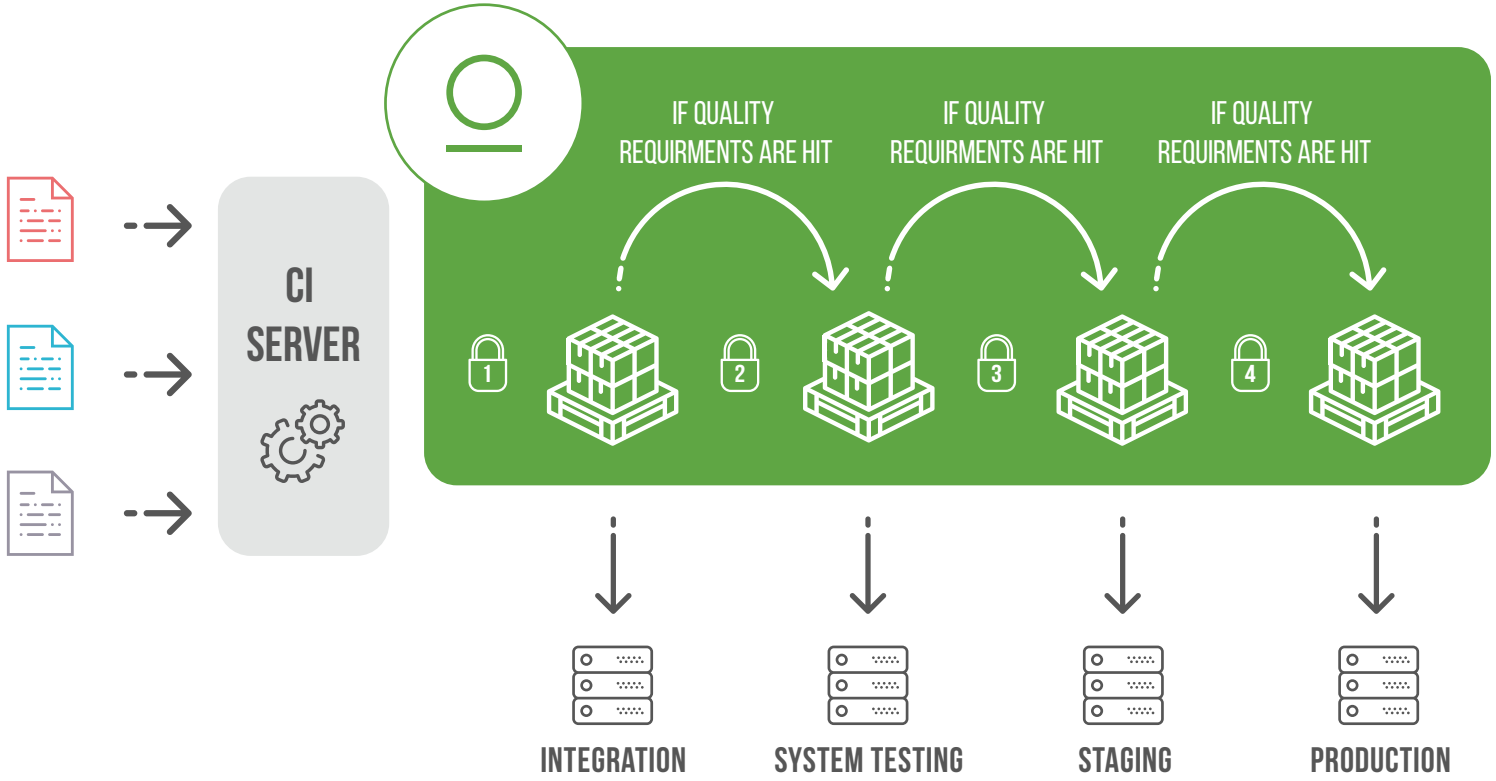

DO WE HAVE AN EXISTING PATTERN?
DO WE NEED TO ADAPT IT?


CI/CD PIPELINES?
DOING THEM FOR YEARS.

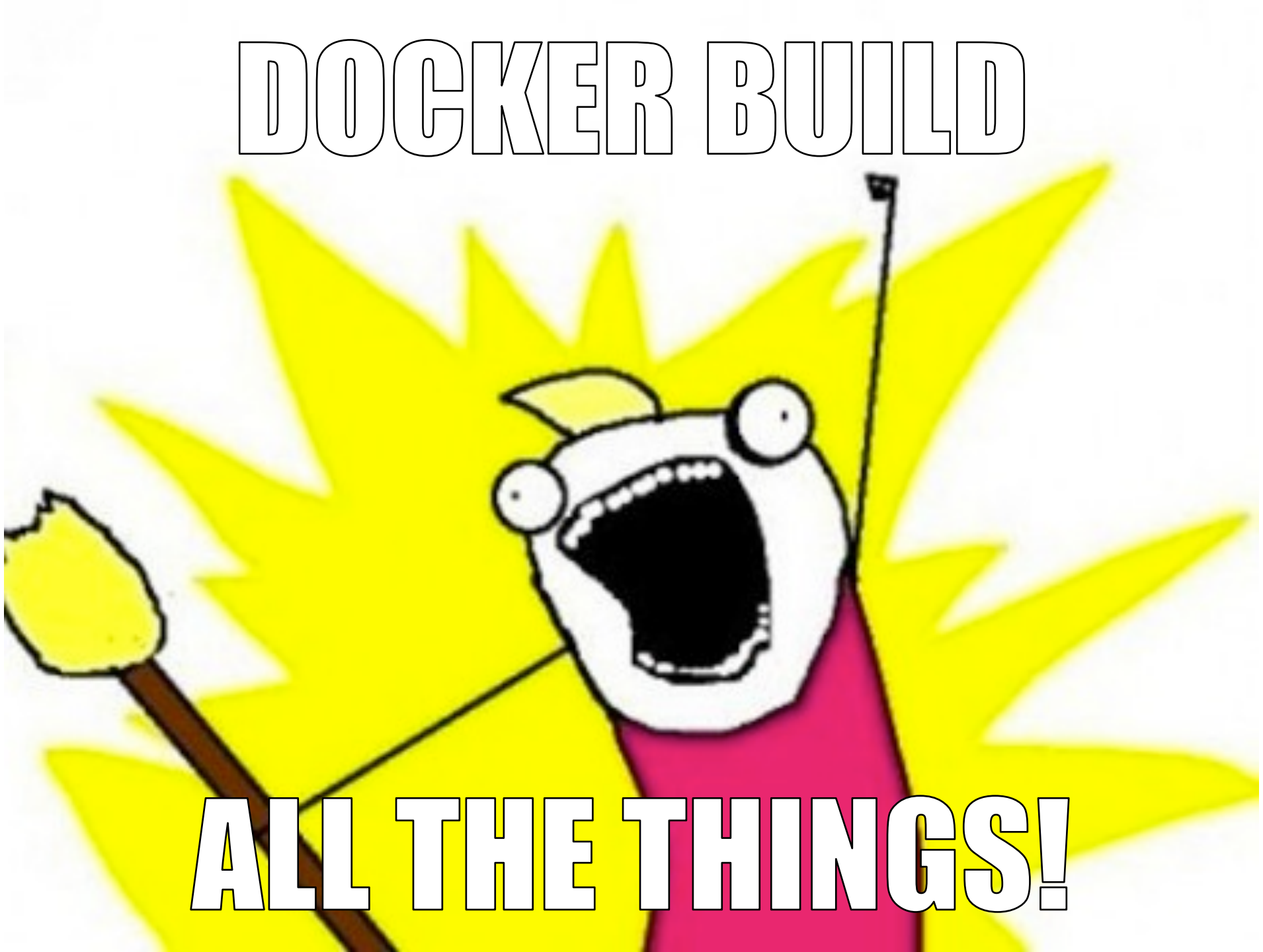
THE PROMOTION PYRAMID



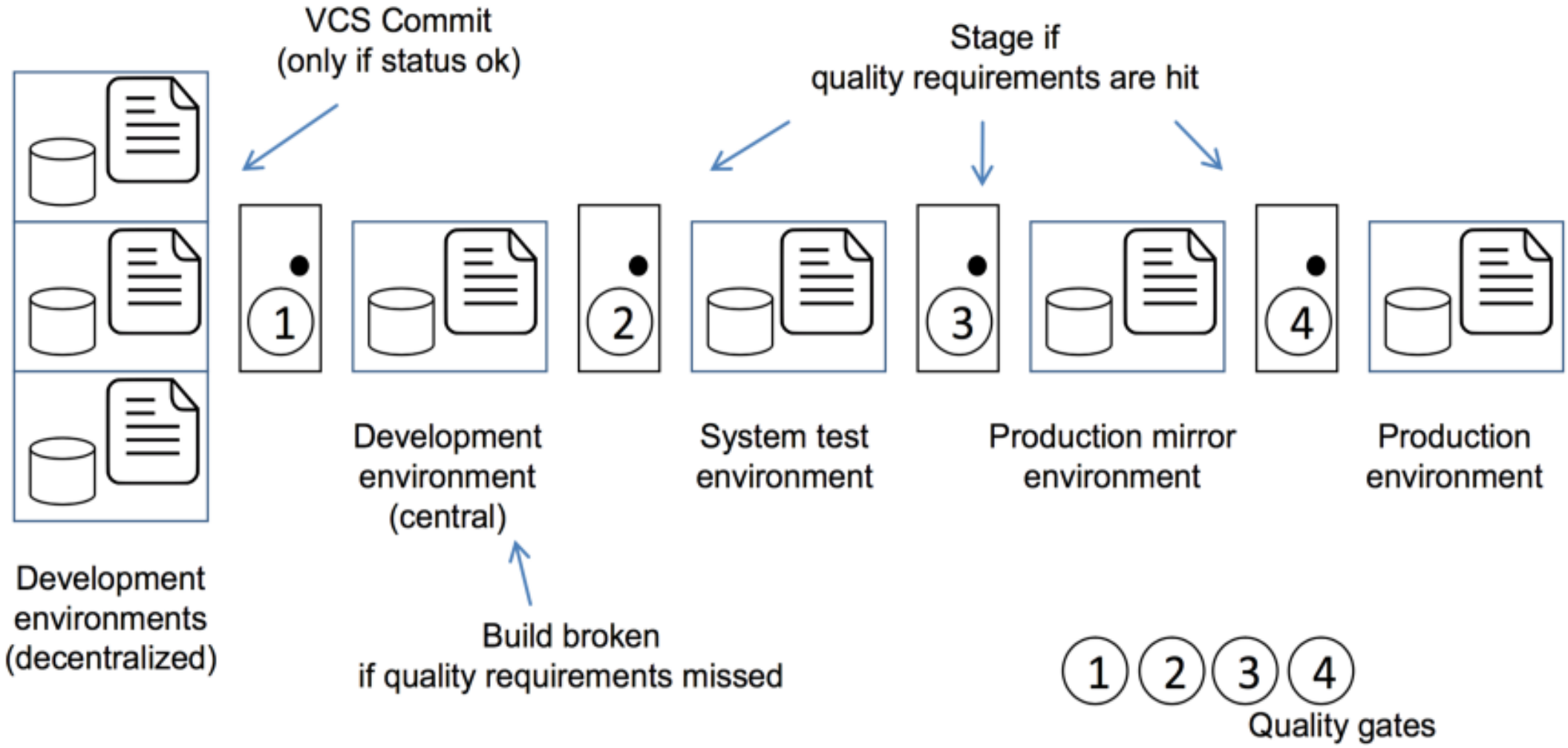
PIPELINE: QUALITY GATES AND VISIBILITY



$docker build


DOCKER BUILD
ALL THE THINGS!

LET'S `docker build` IN EVERY ENV!




FAST AND CHEAP BUILDS
NOT ALWAYS THE WAY TO GO

THAT'S WHY.

```
FROM ubuntu

RUN apt-get install -y software-properties-common python
RUN apt-get install -y nodejs
RUN mkdir /var/www

ADD app.js /var/www/app.js

CMD ["/usr/bin/node", "/var/www/app.js"]
```

Latest version

Latest version

Latest version

Latest version

THAT'S WHY.

```
FROM ubuntu:19.04
```

Better now?

```
RUN apt-get install -y software-properties-common python
RUN apt-get install -y nodejs
RUN mkdir /var/www

ADD app.js /var/www/app.js

CMD ["/usr/bin/node", "/var/www/app.js"]
```

THAT'S WHY.

```
FROM ubuntu:4033353383af19ec179c01dda7f355a246c6adcafaf93c8f98

RUN apt-get install -y software-properties-common python
RUN apt-get install -y nodejs
RUN mkdir /var/www

ADD app.js /var/www/app.js

CMD ["/usr/bin/node", "/var/www/app.js"]
```

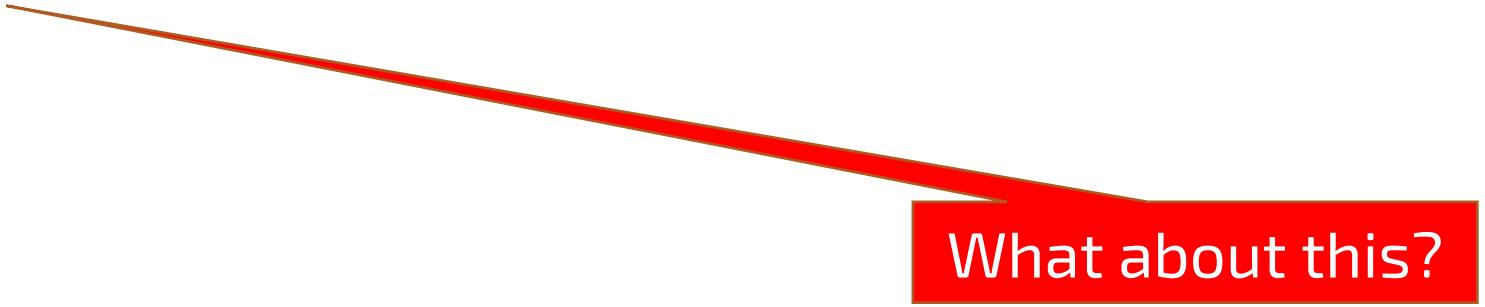
And now?

THAT'S WHY.

```
FROM ubuntu:4033353383af19ec179c01dda7f355a246c6adcafaf93c8f98


RUN apt-get install -y software-properties-common python
RUN apt-get install -y nodejs
RUN mkdir /var/www


ADD app.js /var/www/app.js


CMD ["/usr/bin/node", "/var/www/app.js"]
```

THAT'S WHY.

```
FROM ubuntu:4033353383af19ec179c01dda7f355a246c6adcafaf93c8f98

RUN mvn clean install

CMD ”java –jar Main.class"
```

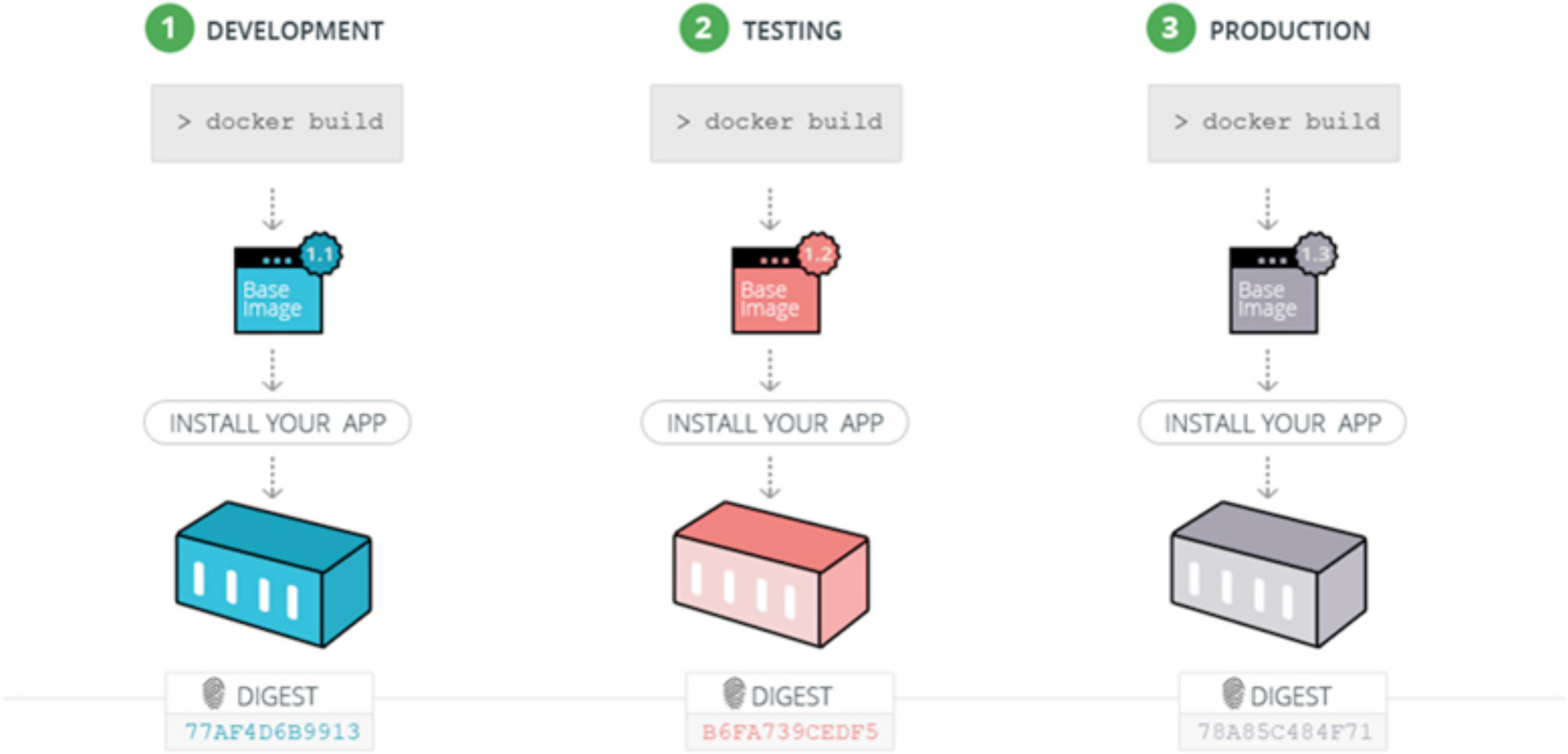


THAT'S WHY.

```
FROM ubuntu:4033353383af19ec179c01dda7f355a246c6adcafaf93c8f98

RUN download_random_sh*t_from_the_internet.sh

CMD ["/usr/bin/node", "/var/www/app.js"]
```

And how about this?

THAT'S WHY YOU DON'T TRUST DOCKER




I DON'T ALWAYS BUILD PROMOTION PIPELINES
BUT WHEN I DO, IT'S WITH
IMMUTABLE AND STABLE BINARIES

1 DEVELOPMENT

2 TESTING

3 PRODUCTION

```
> docker build
```

INSTALL YOUR APP

```
> build once

> automatically promote the same image
through the pipeline to production
```

PROMOTE

PROMOTE

DIGEST
77AF4D6B9913

DIGEST
77AF4D6B9913

DIGEST
77AF4D6B9913

WHAT'S UP WITH THE GATES?!

- QA SHOULDN'T TEST DEV IMAGES
- NON-TESTED IMAGES SHOULDN'T BE STAGED
- NON-STAGED, NON-TESTED OR DEV IMAGES SHOULDN'T END UP IN PRODUCTION!!!

LET’S BUILD ROCK-SOLID PIPELINE!

HOW DO I SEPARATE DEV FROM PROD?!

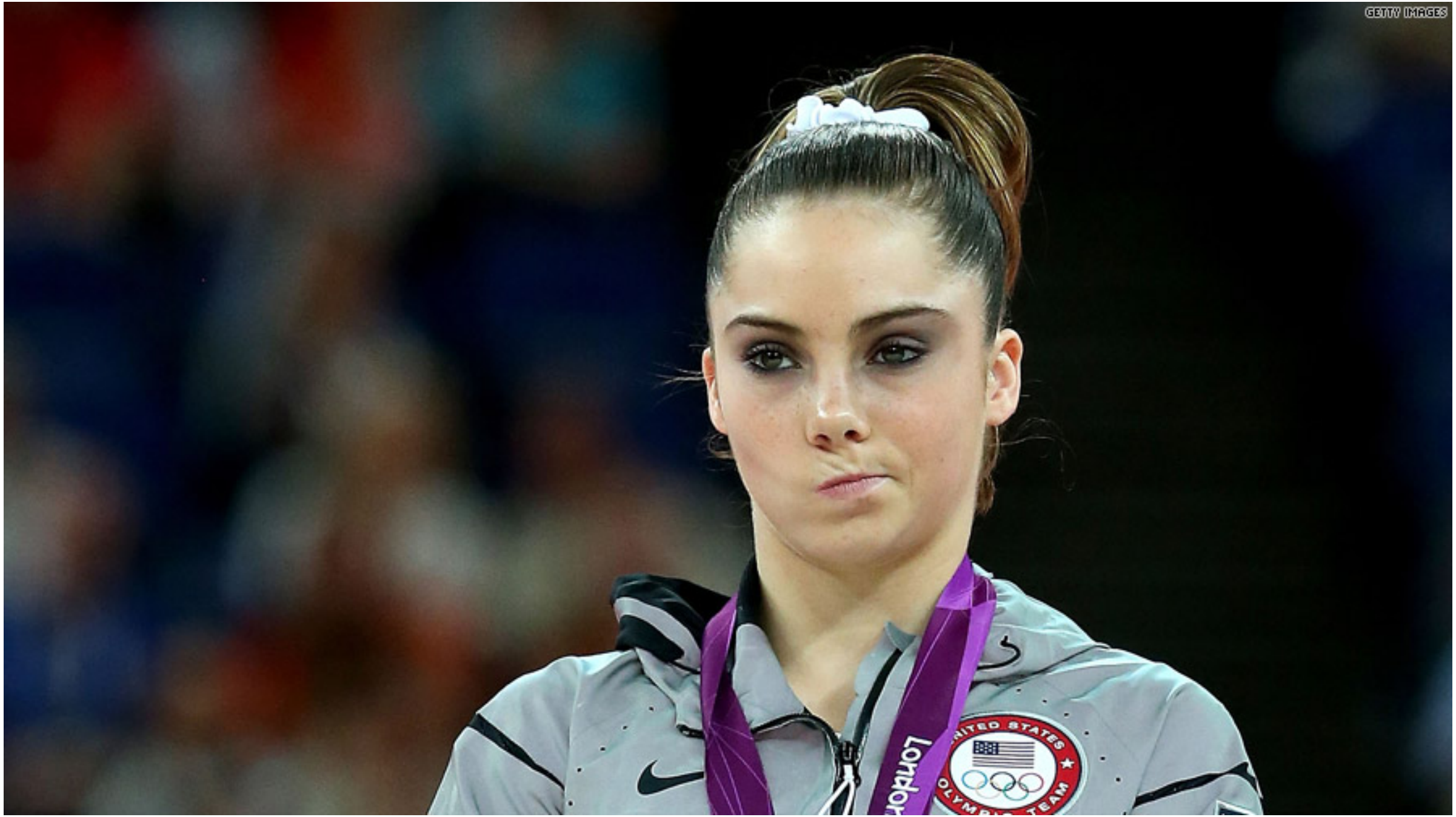
OPTION 1: METADATA TAGS

LABEL

```
LABEL <key>=<value> <key>=<value> <key>=<value> ...
```

The `LABEL` instruction adds metadata to an image. A `LABEL` is a key-value pair. To include spaces within a `LABEL` value, use quotes and backslashes as you would in command-line parsing. A few usage examples:

```
LABEL "com.example.vendor"="ACME Incorporated"
LABEL com.example.label-with-value="foo"
LABEL version="1.0"
LABEL description="This text illustrates \
that label-values can span multiple lines."
```


GETTY IMAGES

OPTION 2: DOCKER REPOSITORIES

Repositories

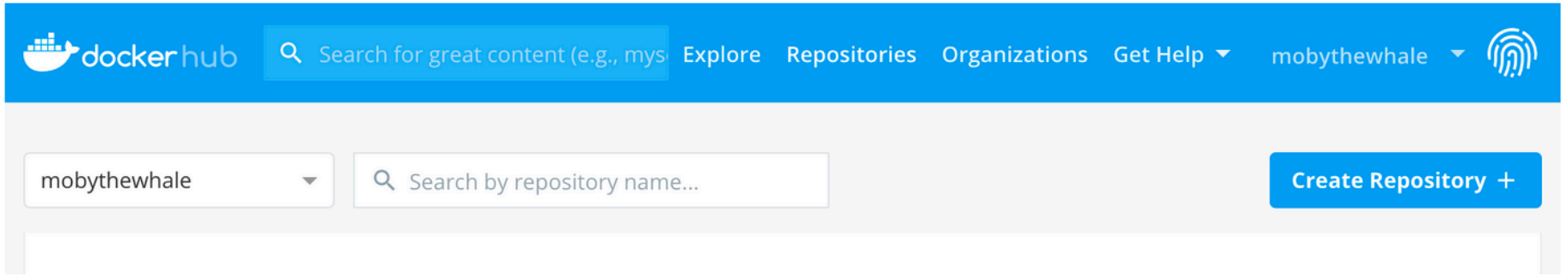
Estimated reading time: 5 minutes

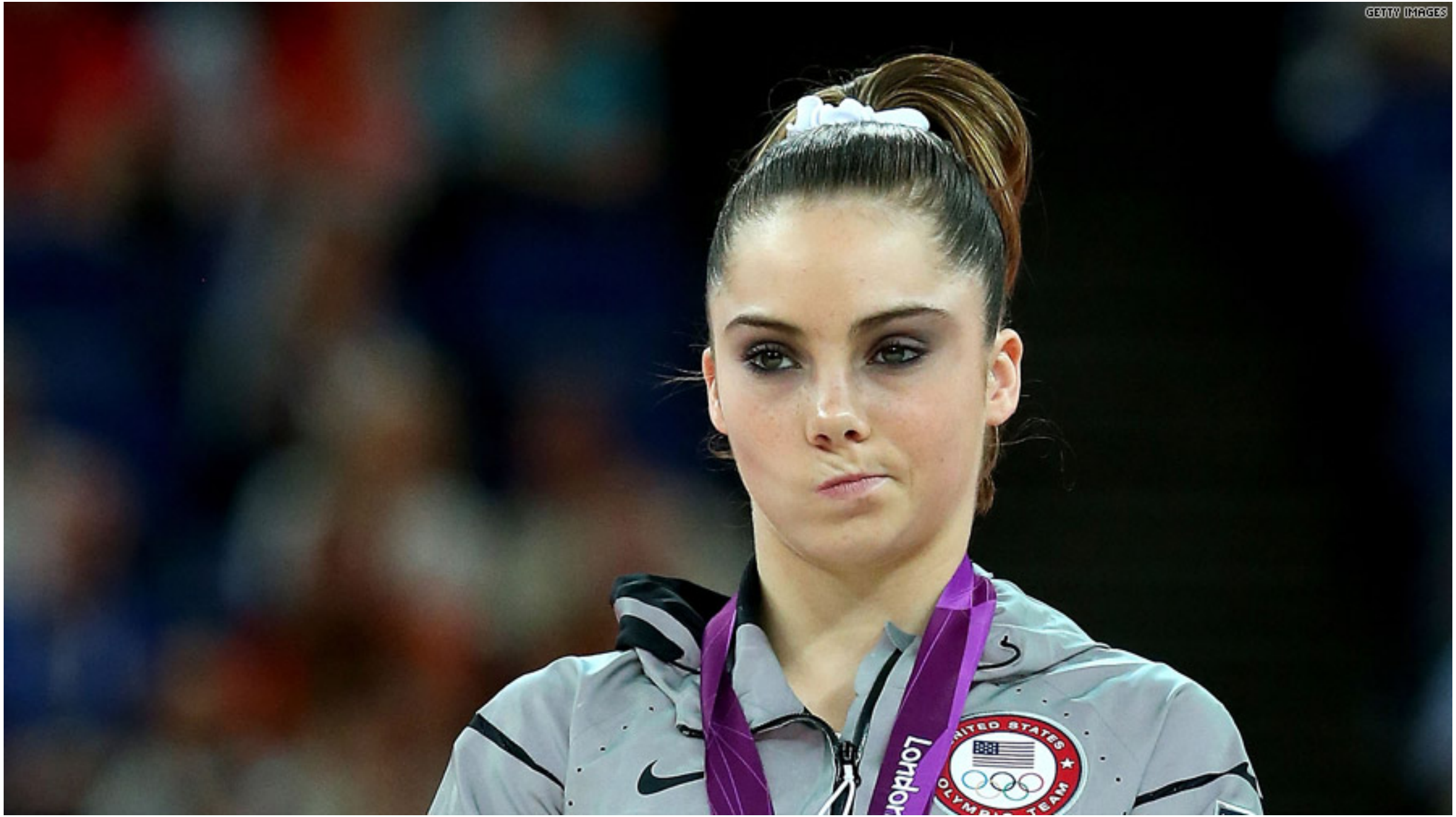
Docker Hub repositories allow you share container images with your team, customers, or the Docker community at large.

Docker images are pushed to Docker Hub through the `docker push` command. A single Docker Hub repository can hold many Docker images (stored as **tags**).

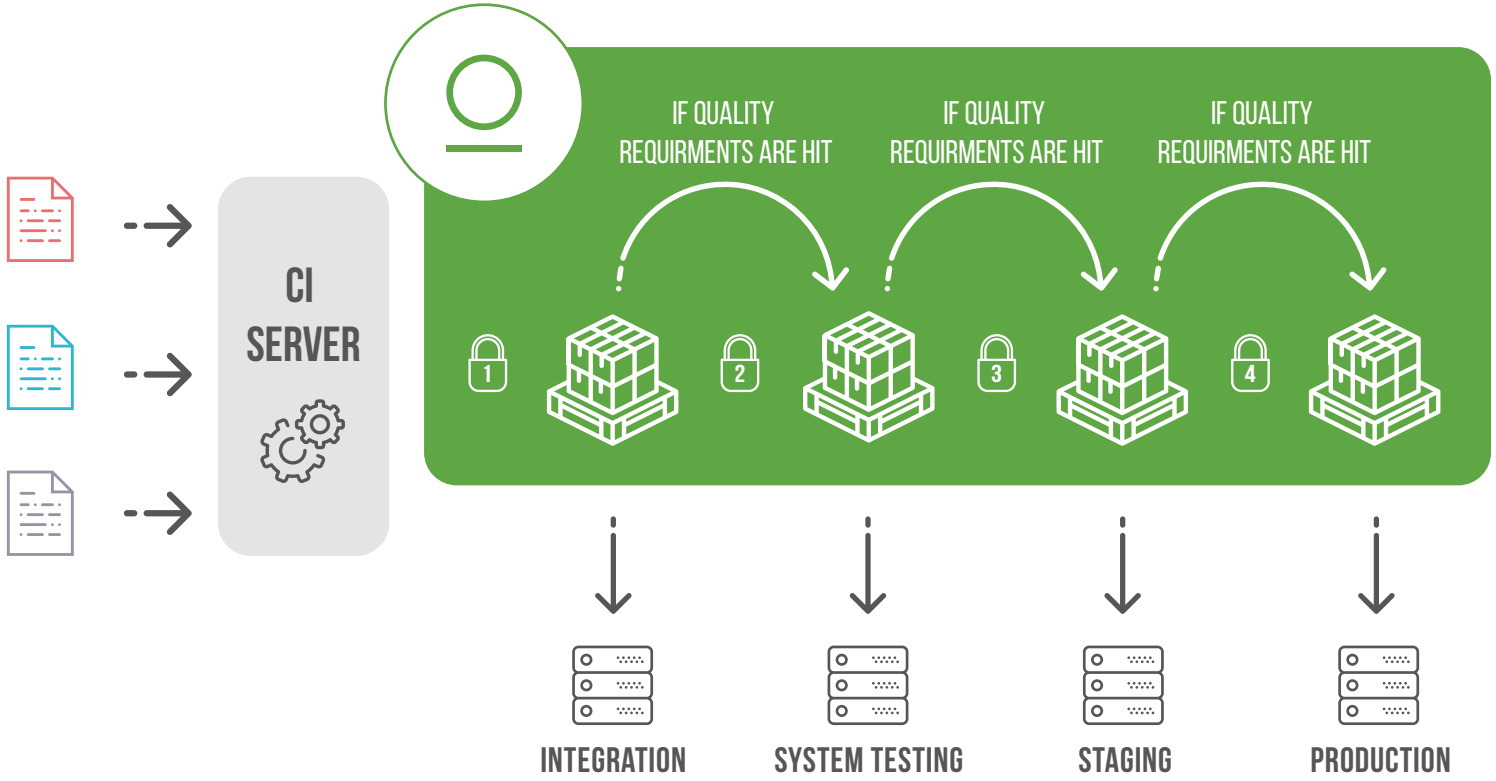
Creating repositories

To create a repository, sign into Docker Hub, click on **Repositories** then **Create Repository**:

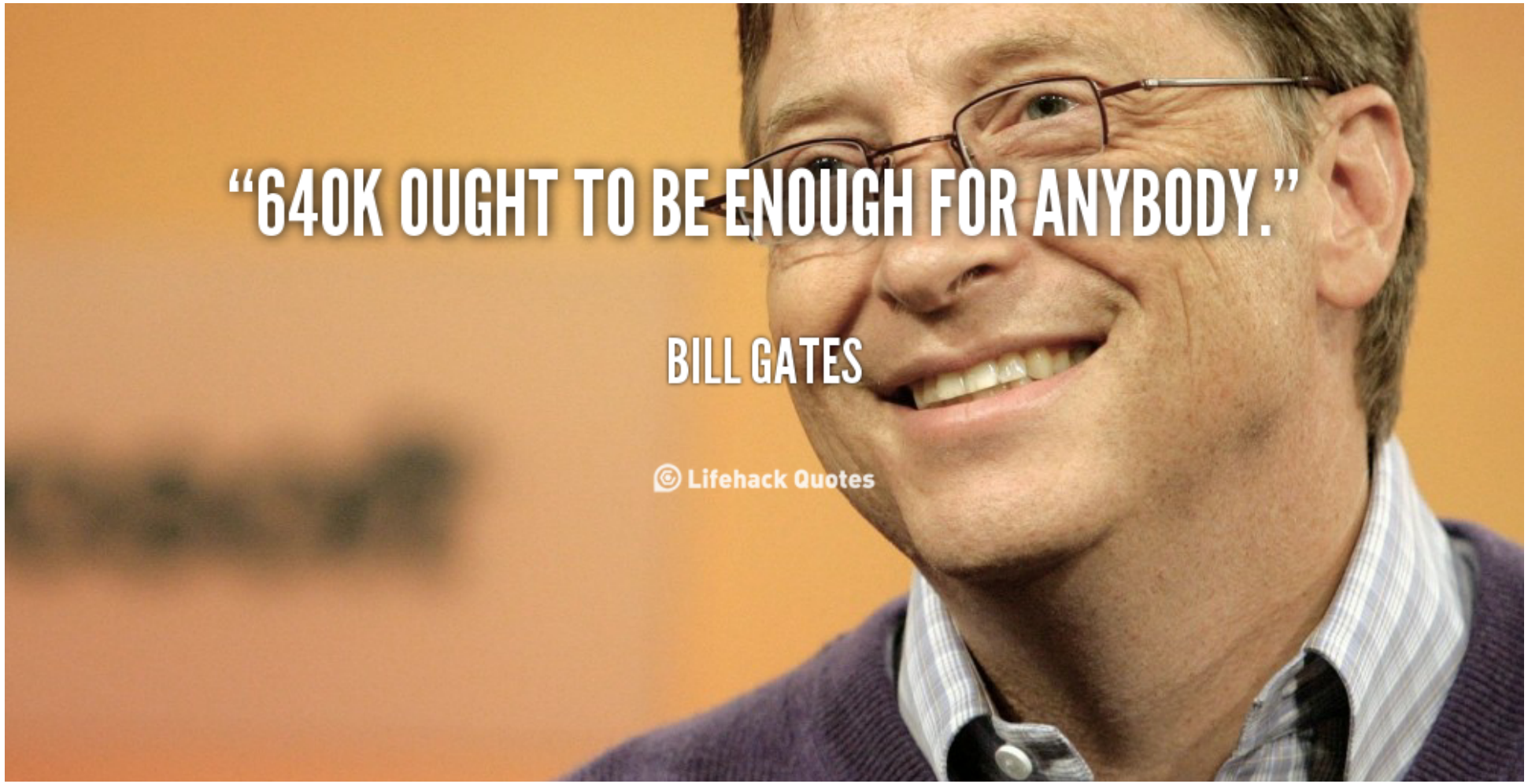



GETTY IMAGES

SEPARATE REGISTRIES PER ENVIRONMENT



TRUMPED-UP LIMITATIONS



THE ANATOMY OF DOCKER TAG

Tag an image for a private repository

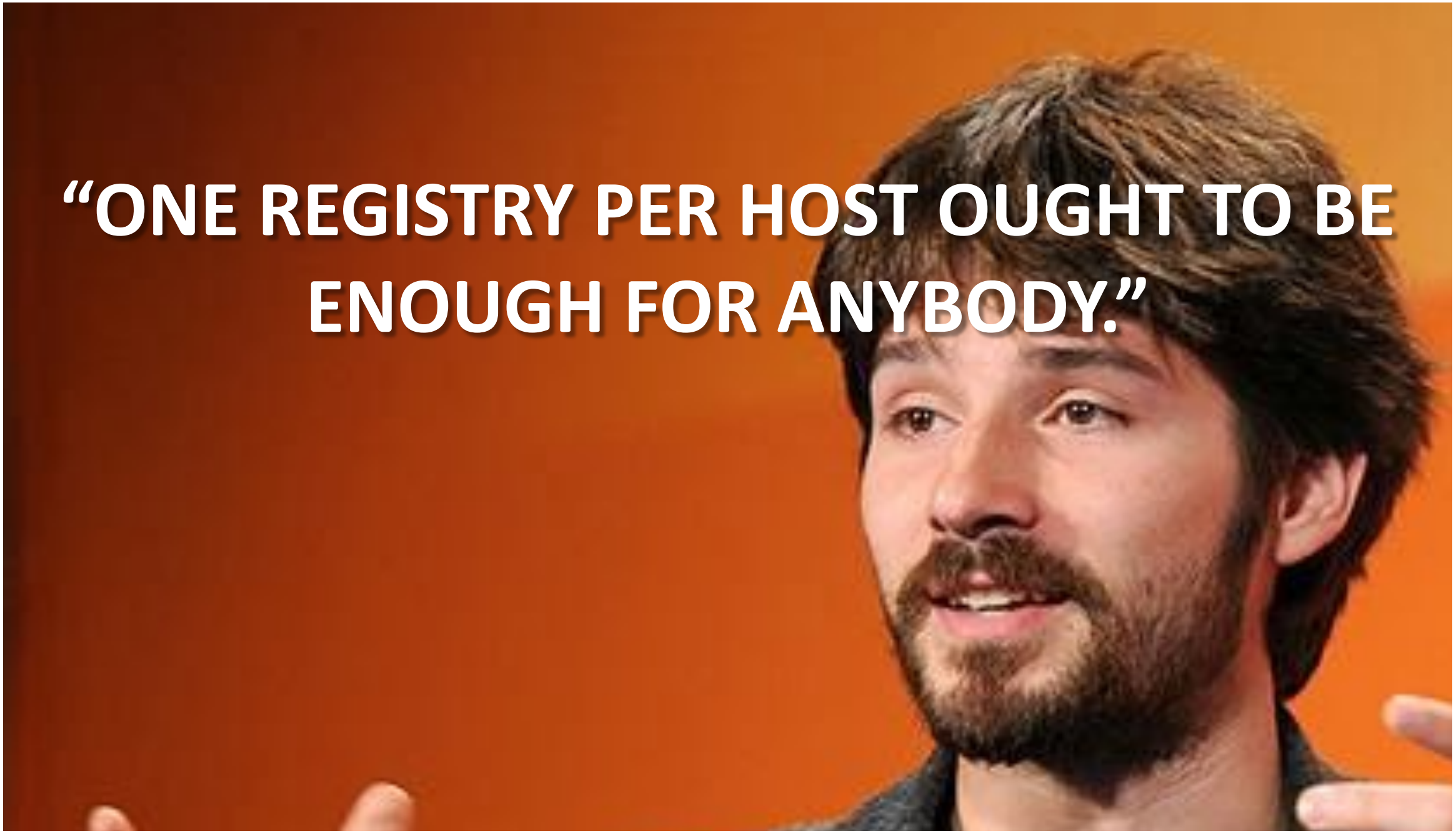
To push an image to a private registry and not the central Docker registry you must tag it with the registry hostname and port (if needed).

```
$ docker tag 0e5574283393 myregistryhost:5000/fedora/httpd:version1.0
```

Wait a second, how can I have more than one registry per host now?!

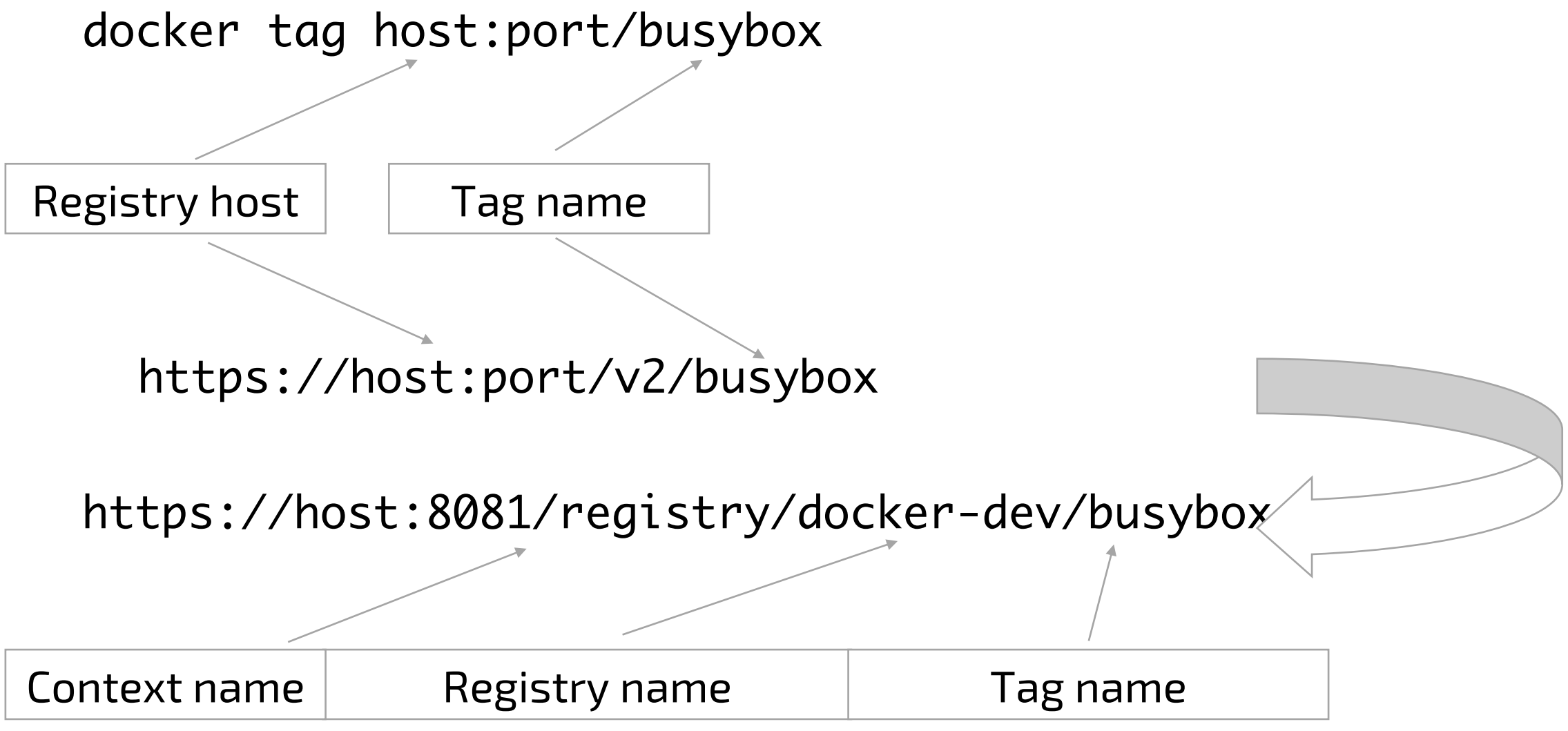
HOW CAN WE SUPPORT THIS?

```
https://host:8081/registry/docker-dev/busybox

https://host:8081/registry/docker-qa/busybox

https://host:8081/registry/docker-staging/busybox

https://host:8081/registry/docker-prod/busybox
```

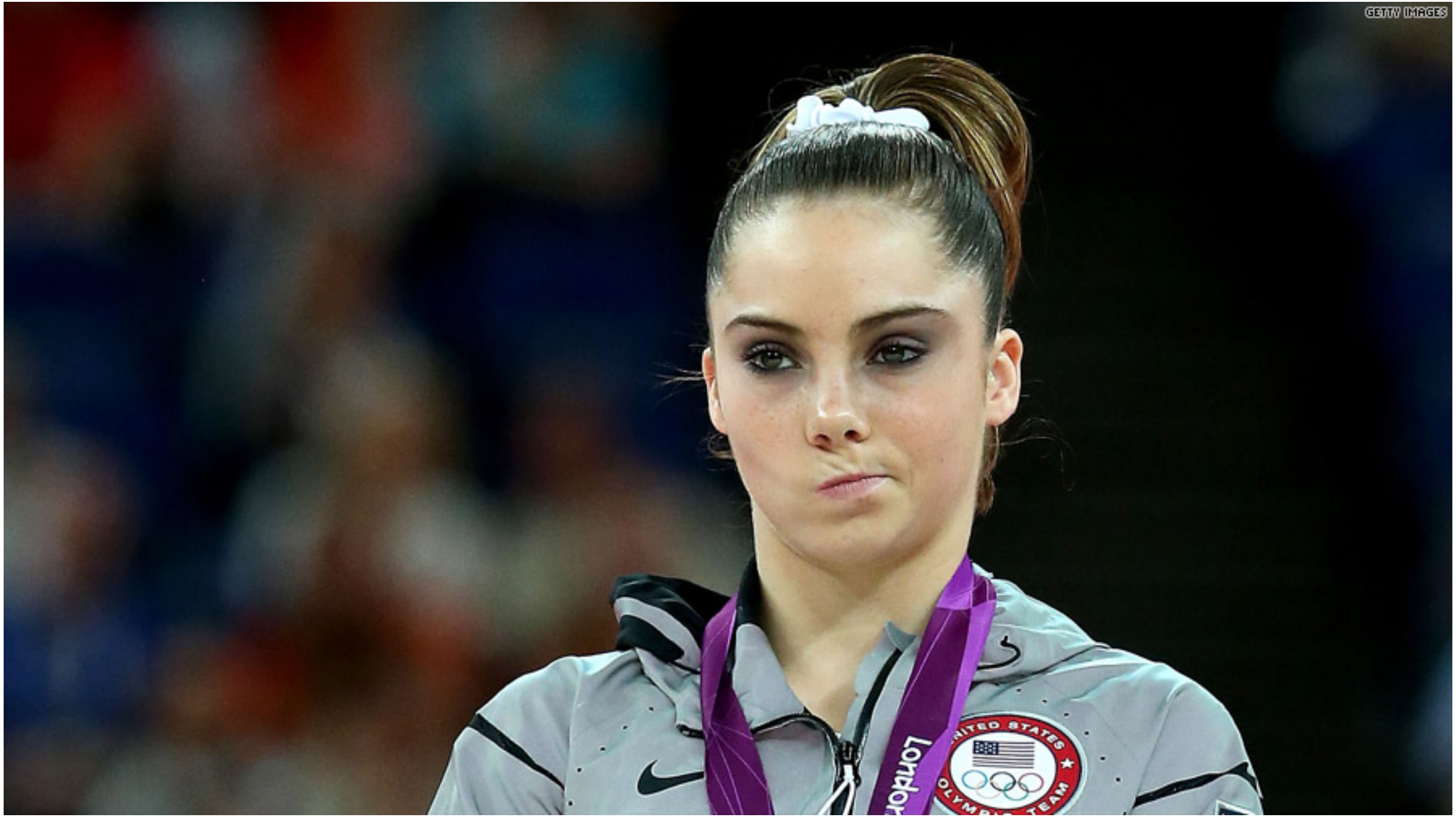

“ONE REGISTRY PER HOST OUGHT TO BE ENOUGH FOR ANYBODY.”

PANIC!

VIRTUAL HOSTS/PORTS TO THE RESCUE



```
server {
    listen 5001;


    server_name 192.168.99.100;
    if ($http_x_forwarded_proto = '') {
        set $http_x_forwarded_proto  $scheme;
    }
    rewrite ^/(v1|v2)/(.*) /artifactory/api/docker/docker-dev/$1/$2;
    …
    }
}
```


GETTY IMAGES

LET'S ABUSE THINGS!

Tag an image for a private repository

To push an image to a private registry and not the central Docker registry you must tag it with the registry hostname and port (if needed).

no-one uses this anyway

```
$ docker tag 0e5574283393 myregistryhost:5000/fedora/httpd:version1.0
```

LET'S ABUSE THINGS!

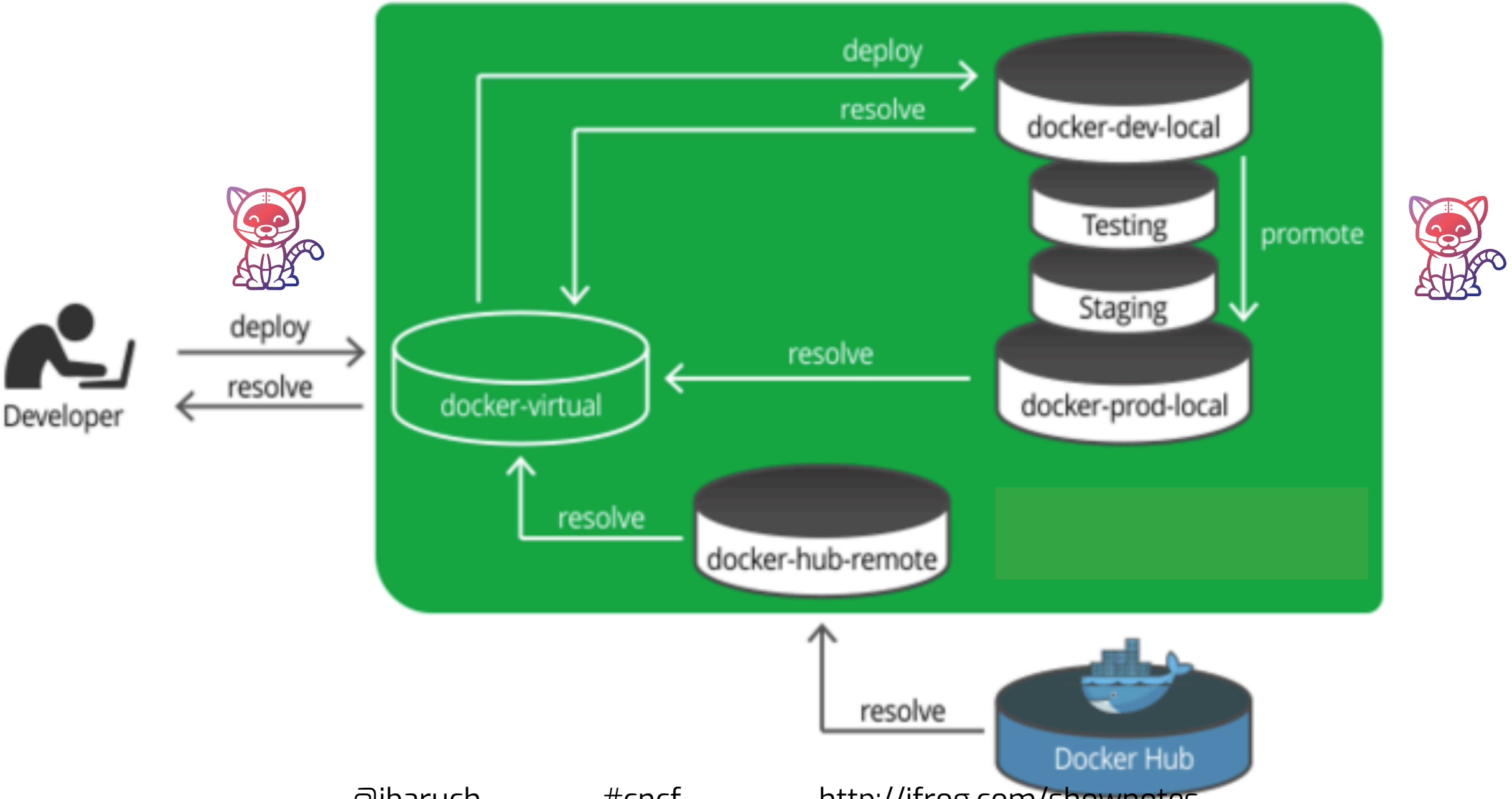
Tag an image for a private repository

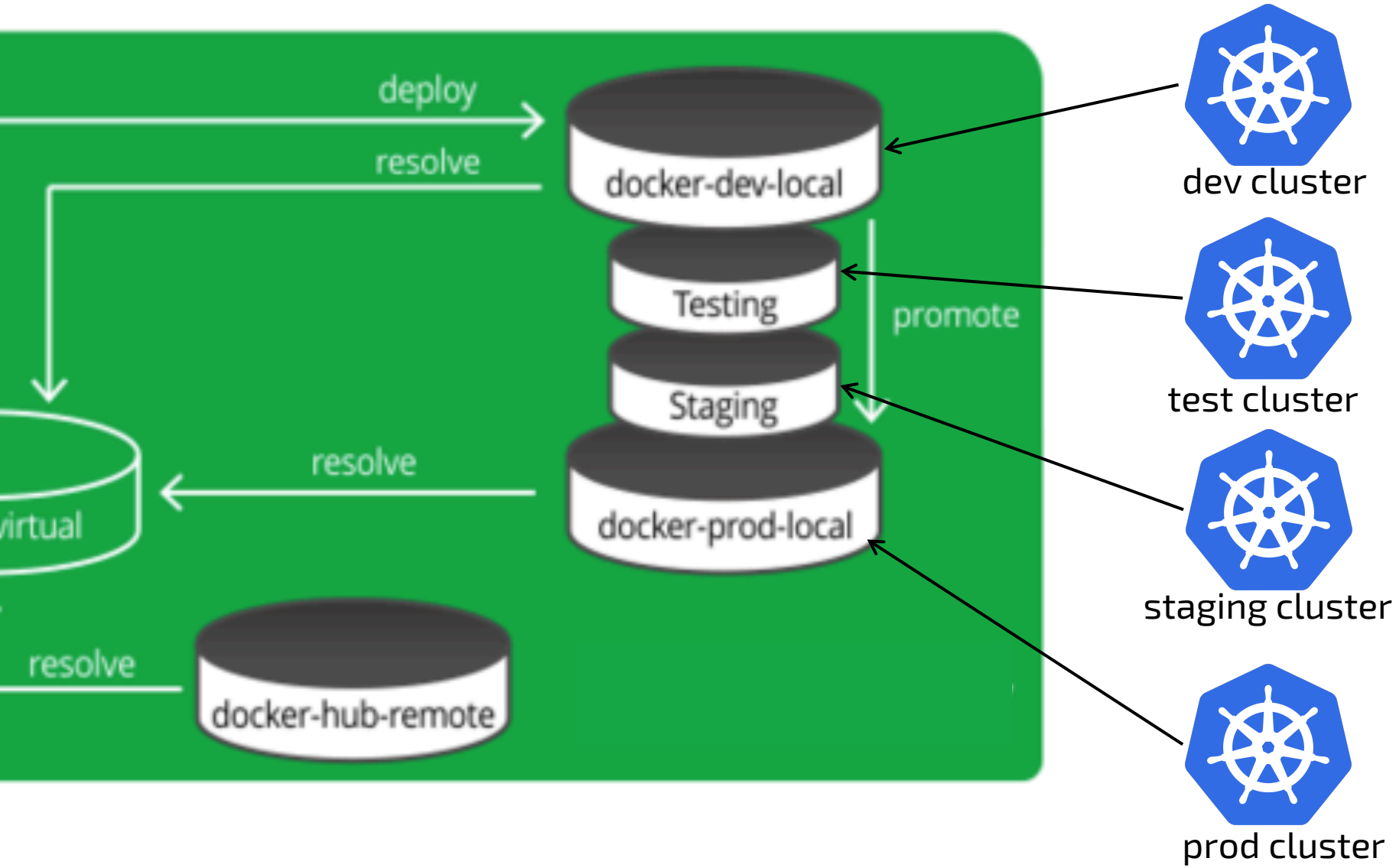
To push an image to a private registry and not the central Docker registry you must tag it with the registry hostname and port (if needed).

```
$ docker tag 0e5574283393 myregistryhost:5000/staging/httpd:version1.0
```

BUT THEN YOU REALIZE...

Wait a second, now I need to pull, retag and push for every step?!


deploy
resolve
docker-dev-local
Testing
promote
Staging
deploy
resolve
Developer
docker-virtual
resolve
docker-prod-local
resolve
docker-hub-remote
resolve
Docker Hub



dev cluster

test cluster

staging cluster

prod cluster

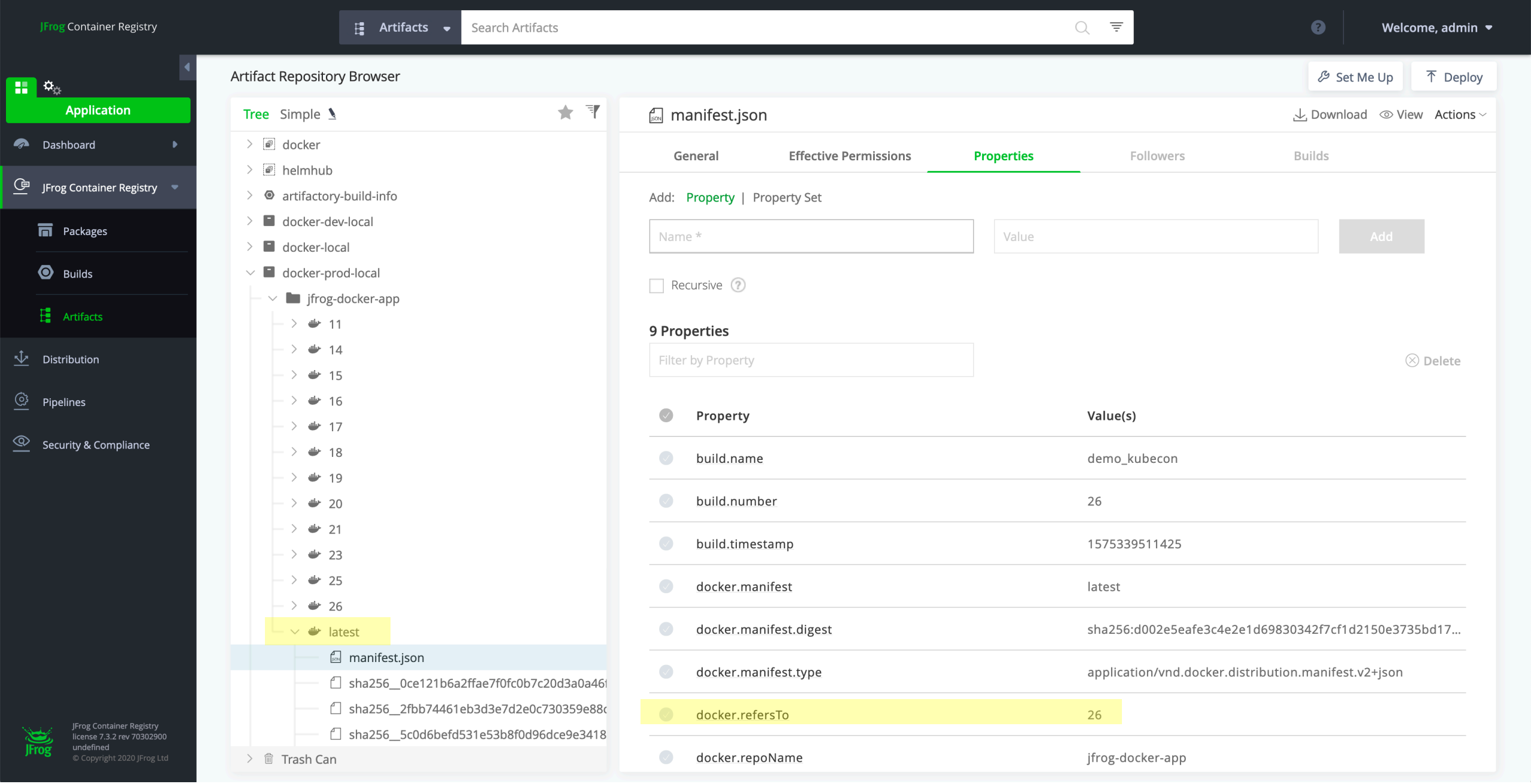
REPOSITORY (DOCKER): Top level directory in a registry

REPOSITORY (THE REST OF THE WORLD): A registry

WIN-WIN-WIN

- SINGLE POINT OF ACCESS TO MULTIPLE REGISTRIES WHEN NEEDED
- COMPLETELY ISOLATED ENVIRONMENTS
- IMMEDIATE AND FREE PROMOTIONS

KIM REINICK/SHUTTERSTOCK

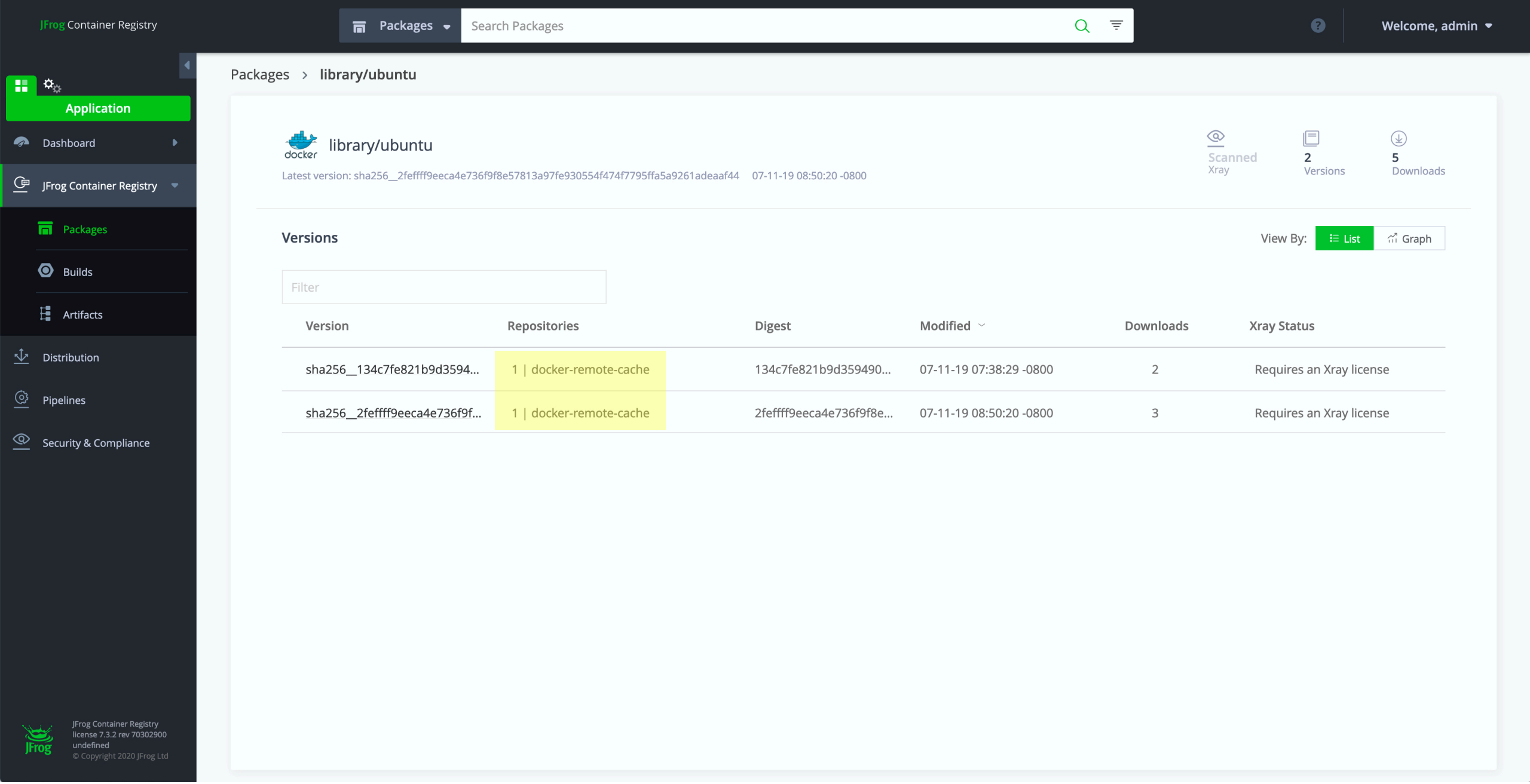


@jbaruch #cncf http://jfrog.com/shownotes

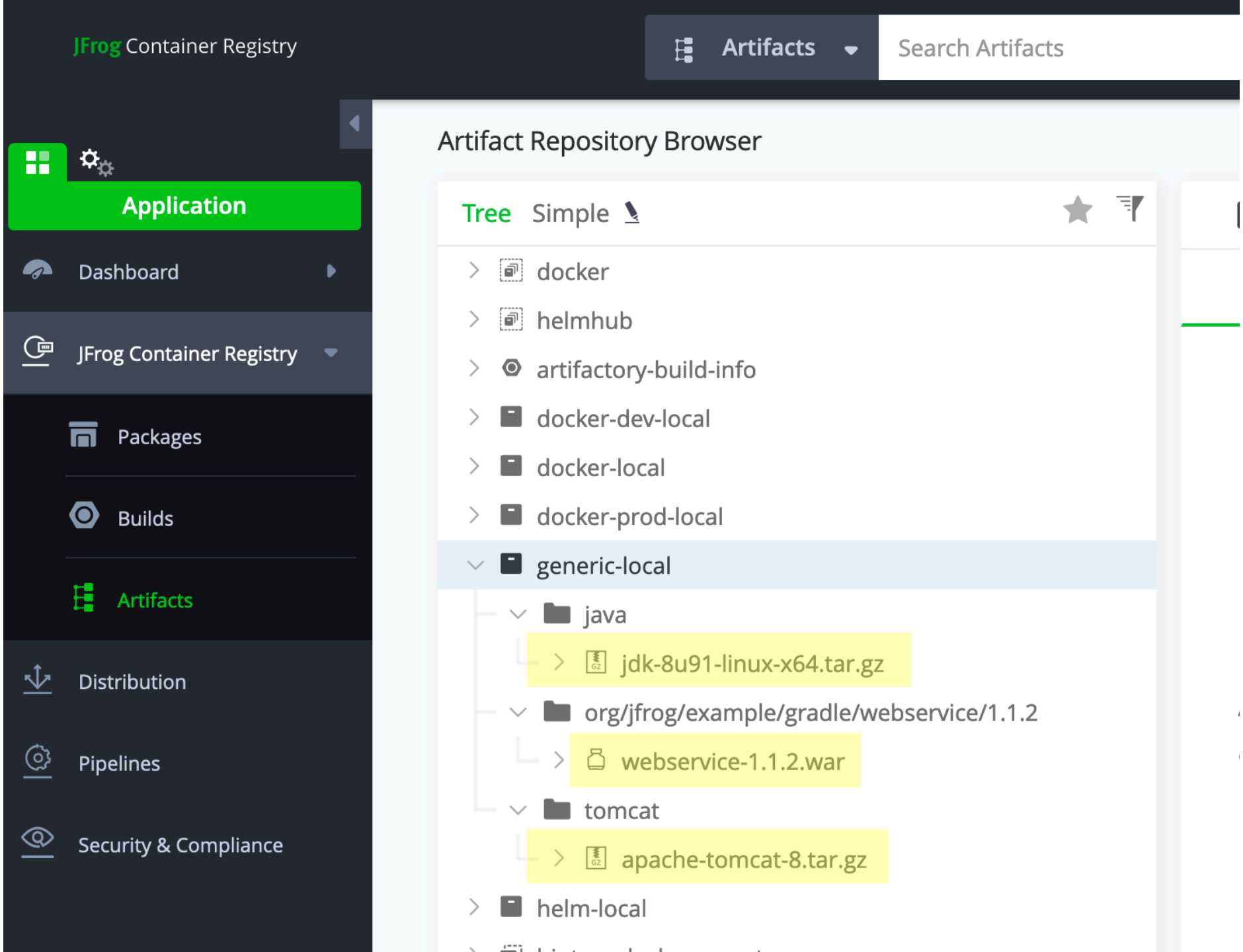
WIN-WIN

- SIMPLICITY OF LATEST
- ALWAYS KNOW WHAT IT REALLY MEANS
- AS LONG AS YOU PROMOTED IMMUTABLE ARTIFACT


@LateNightSeth
But what about the rest of the dependencies?



@jbaruch #cncf http://jfrog.com/shownotes


JFrog Container Registry
Artifacts
Search Artifacts
Application
Dashboard
JFrog Container Registry
Packages
Builds
Artifacts
Distribution
Pipelines
Security & Compliance
Artifact Repository Browser
Tree
Simple
docker
helmhub
artifactory-build-info
docker-dev-local
docker-local
docker-prod-local
generic-local
java
jdk-8u91-linux-x64.tar.gz
org/jfrog/example/gradle/webservice/1.1.2
webservice-1.1.2.war
tomcat
apache-tomcat-8.tar.gz
helm-local

OWN YOUR DEPENDENCIES

- YOUR BASE IMAGE
- YOUR INFRA
- YOUR APPLICATION FILES

CONCLUSIONS

- BUILD ONLY ONCE
- SEPARATE ENVIRONMENTS
- PROMOTE WHAT YOU'VE BUILT
- OWN YOUR DEPENDENCIES

Q&A AND LINKS

- @jbaruch
- #CNCF
- http://jfrog.com/shownotes