

Commit to Excellence

Java in Containers

Markus Eisele

@myfear



What we'll discuss today

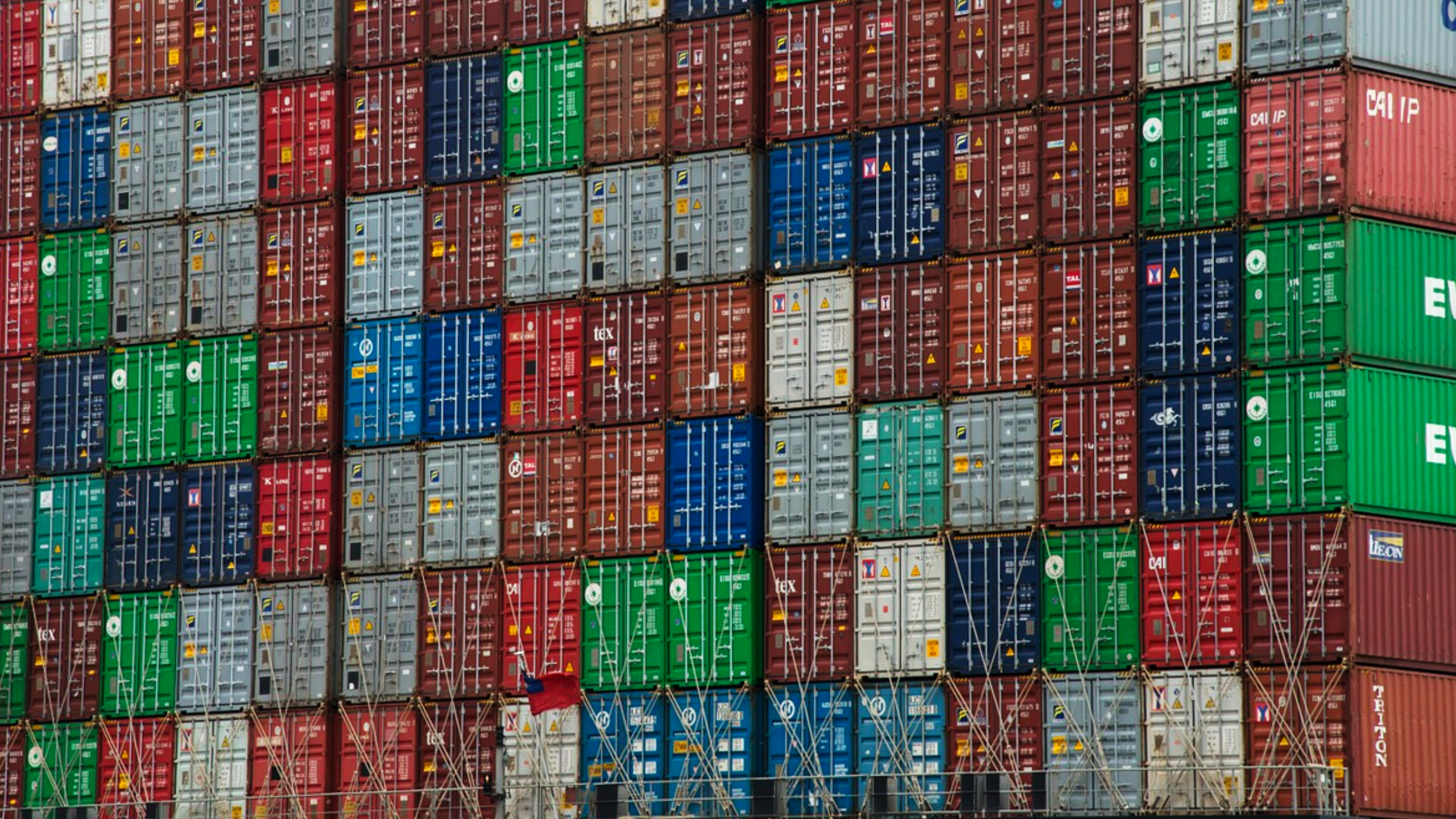
Java in containers ... a good idea ?

Creating effective Java images: smaller, faster, secure.

Some tools

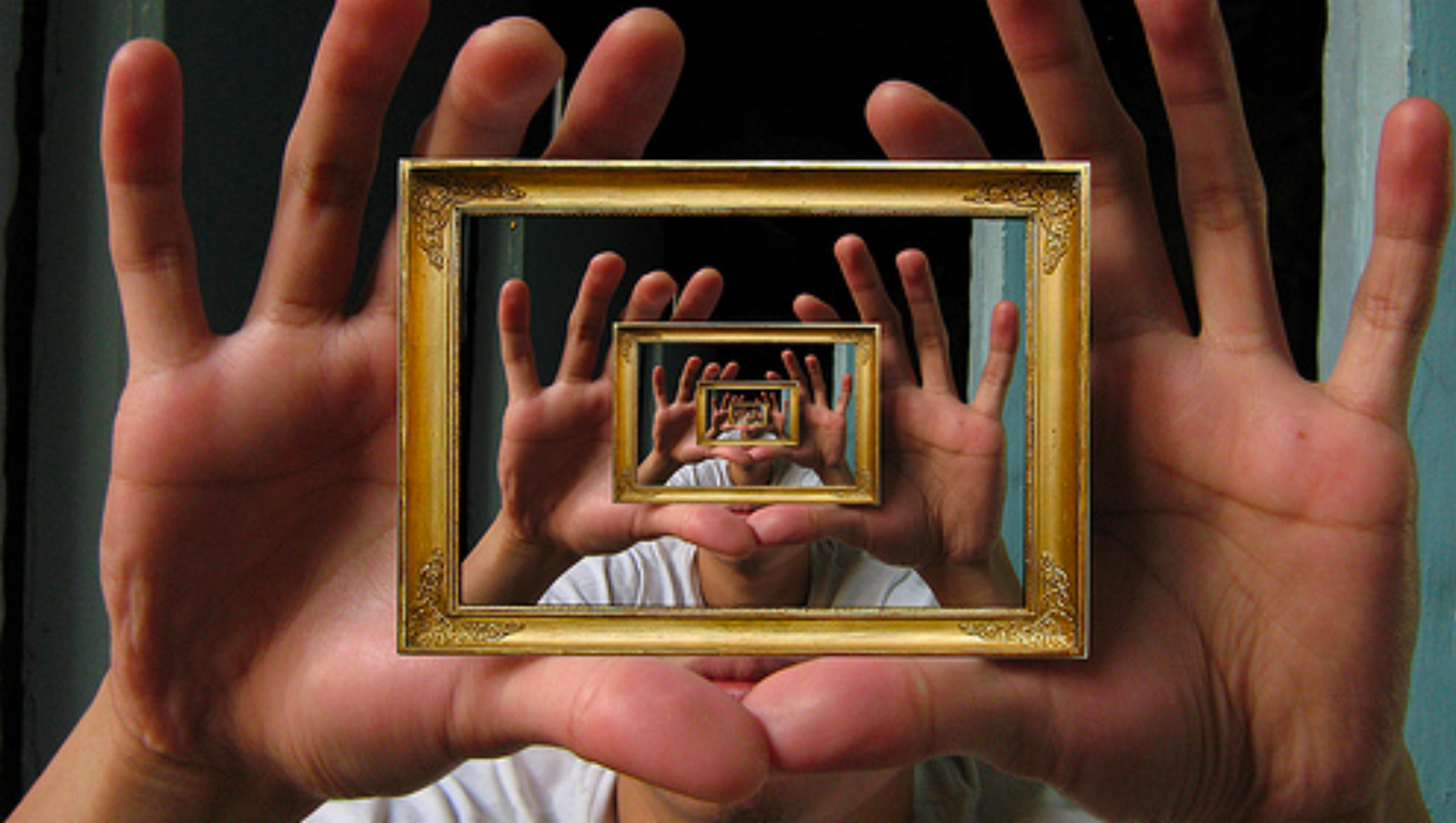
Some security

Some development



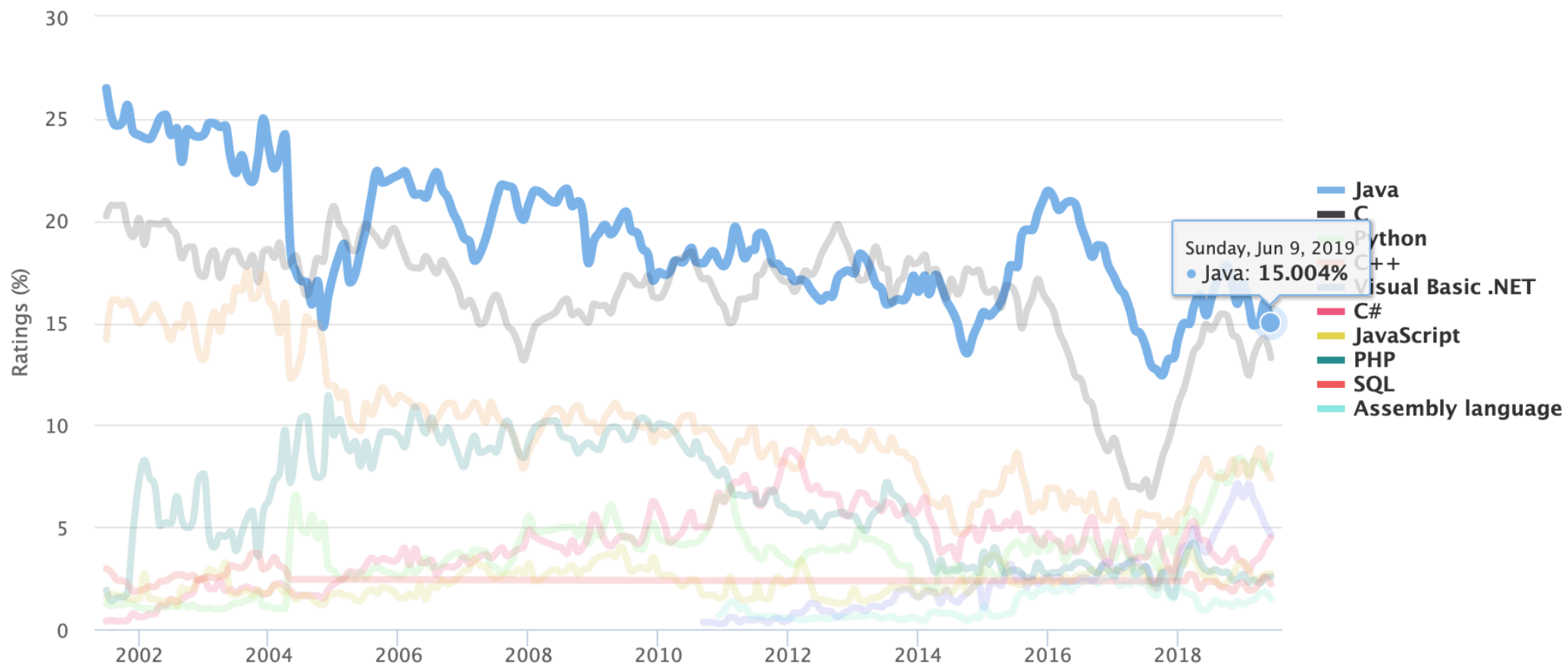
Why containers

- Easy deployment
- Easy Scaling
- Decoupled architecture and services
- Immutability & declarative configuration
- Efficient resource utilization
- Rich ecosystem
- ...



Container and Java





I'LL STOP CODING IN

JAVA

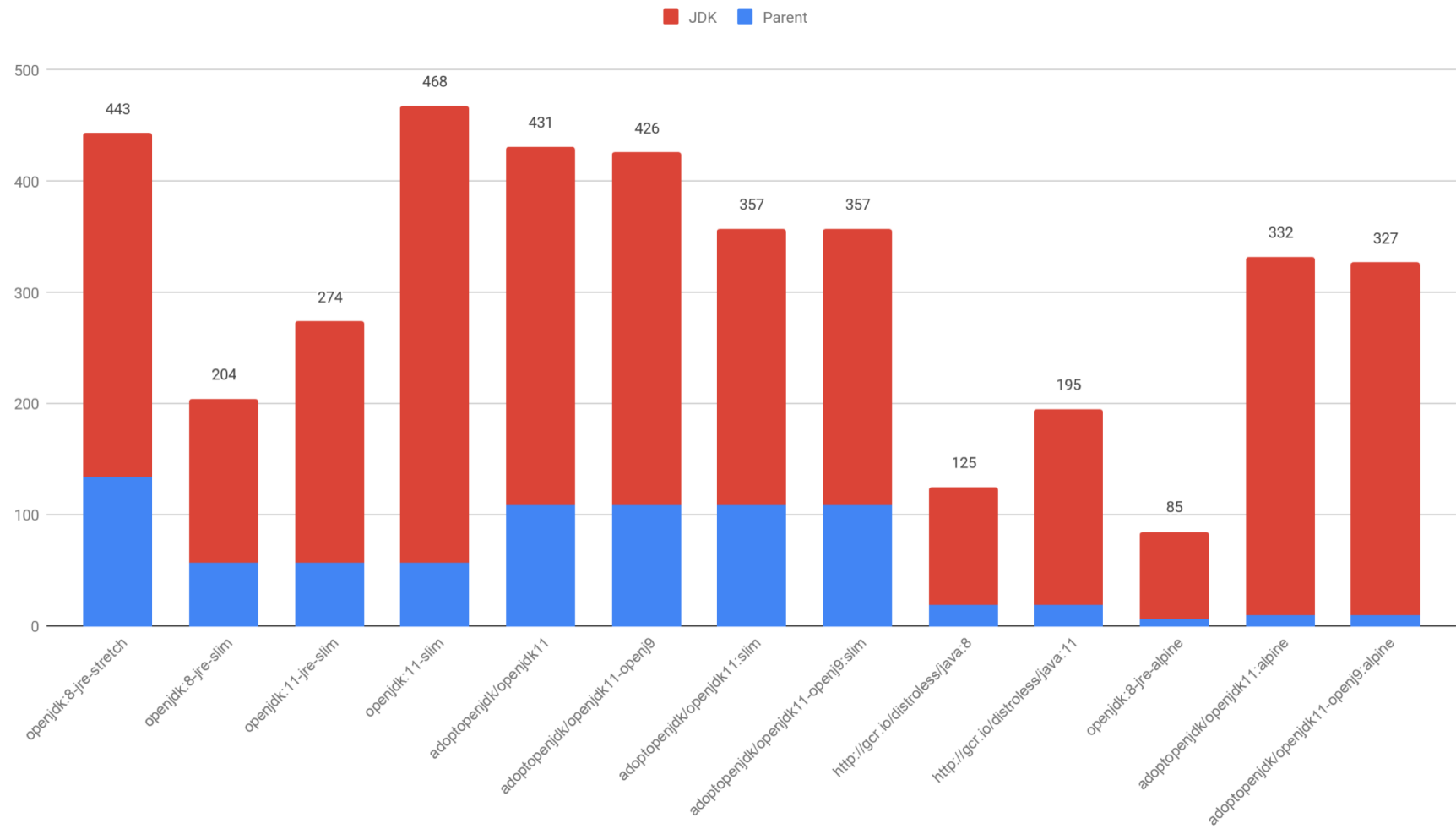
IF THEY MAKE A

BETTER

TECHNOLOGY



Java Docker Imagesizes





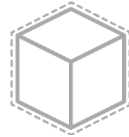
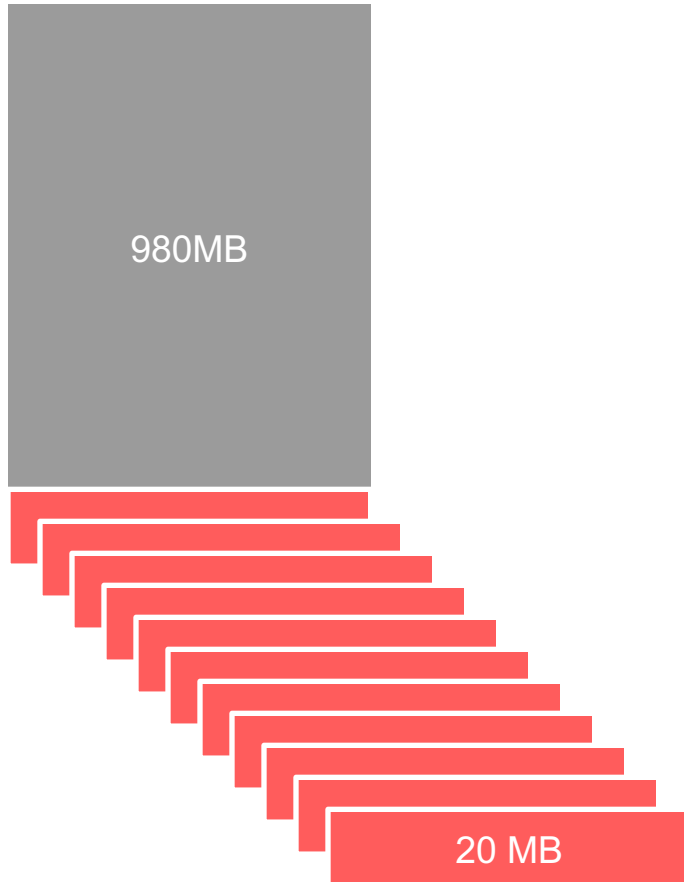
Distroless Container Images

"Distroless" images contain only your application and its runtime dependencies. They do not contain package managers, shells or any other programs you would expect to find in a standard Linux distribution."

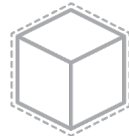
- Built using Google's bazel tool
- Provide stripped down base image
- Support for: Java, Golang, Dotnet, Node, Python, C



Does size really matter?



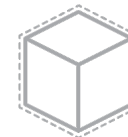
1 x 980 MB base image



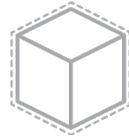
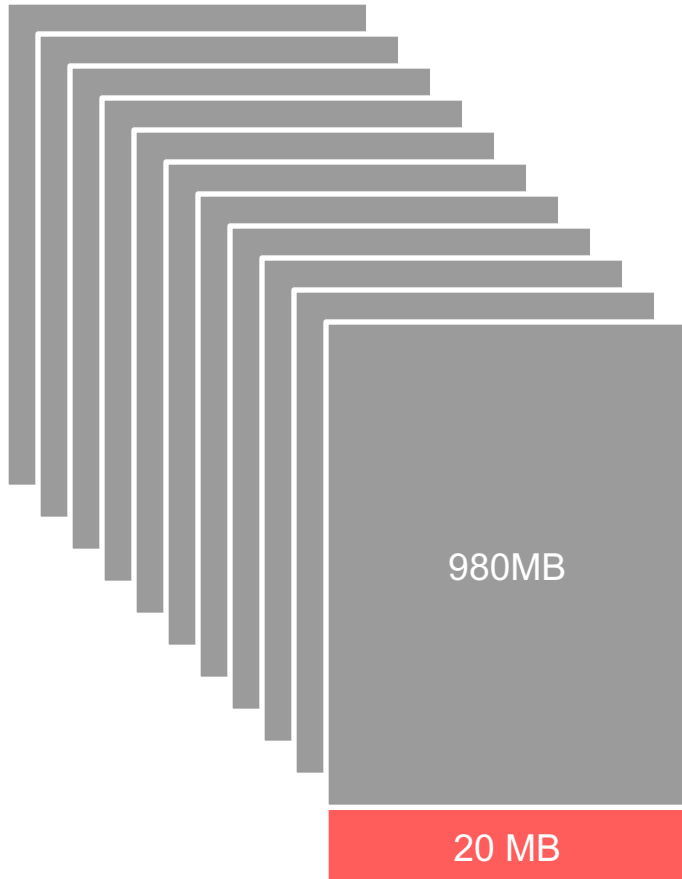
10 x 20 MB project specific image

$$980 + 10 * 20 = 980 + 200 = \mathbf{1180 \text{ MB}}$$

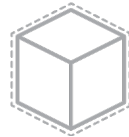
≈ **118 MB**



Does size really matter?



10 x 980 MB project specific image



1 x 20 MB base image

$$20 + 10 \times 980 = 20 + 9800 = \mathbf{9820 \text{ MB}}$$

\approx **982 MB**



Size does not matter!

- Total image size does not matter.
- Base image size does not matter. Thus, reducing base image size in an attempt to reduce total disk consumption is meaningless (except in some borderline cases when the disk is unrealistically small).
- What really matters when it comes to disk usage is the size of frequently changing layers.

What should I care about?

- **Effective tracking:** Improves the signal to noise of scanners (e.g. CVE)
- **Time and cost:** Faster updates, less network costs
- **Security:** Less components that can be exploited and smaller attack surface

Don't be afraid of UBI!

Standard

Image name: ubi

- Unified, OpenSSL crypto stack
 - Full YUM stack
- Includes useful basic OS tools (tar, gzip, vi, etc.)

Minimal

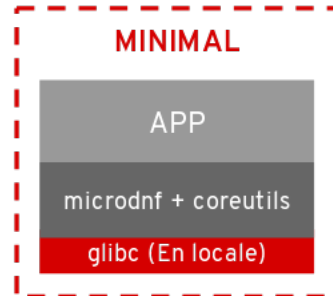
Image name: ubi-minimal

- Minimized pre-installed content set
 - No suid binaries
- Minimal package manager (install, update, and remove)

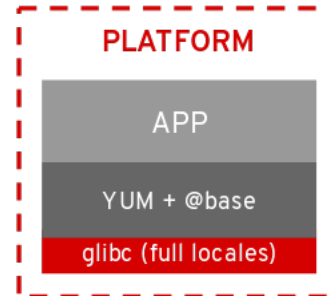
Multi-service

Image name: ubi-init

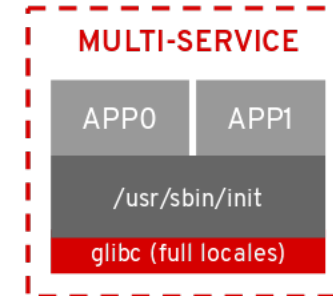
- run mysql and httpd side-by-side in the same container
- run systemd in a container on start
- Enables services at build time



ubi8/ubi-minimal



ubi8/ubi

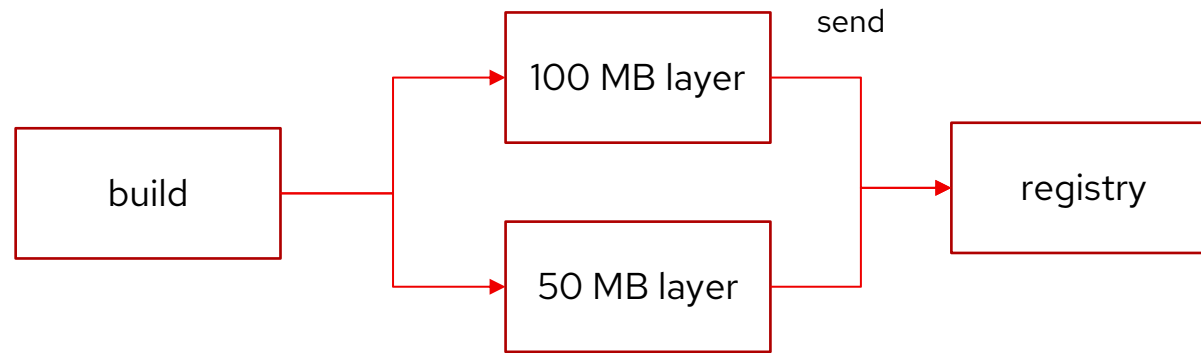


ubi8/ubi-init

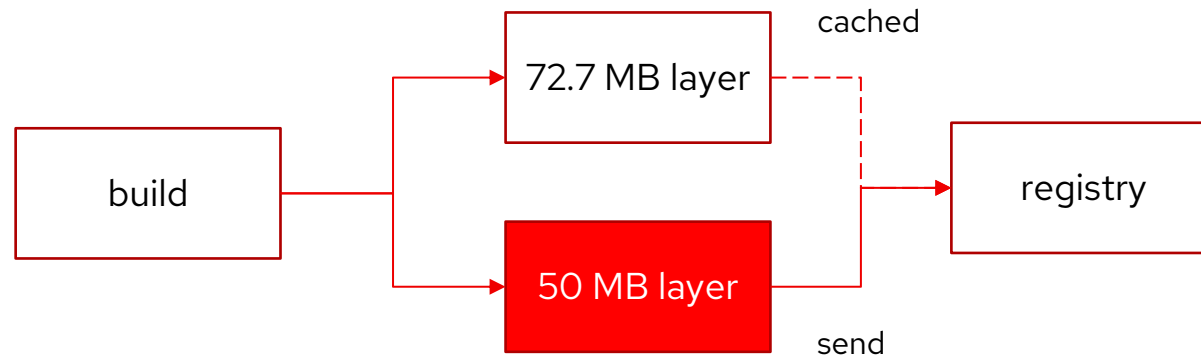


Quay [builds, analyzes, distributes] your container images

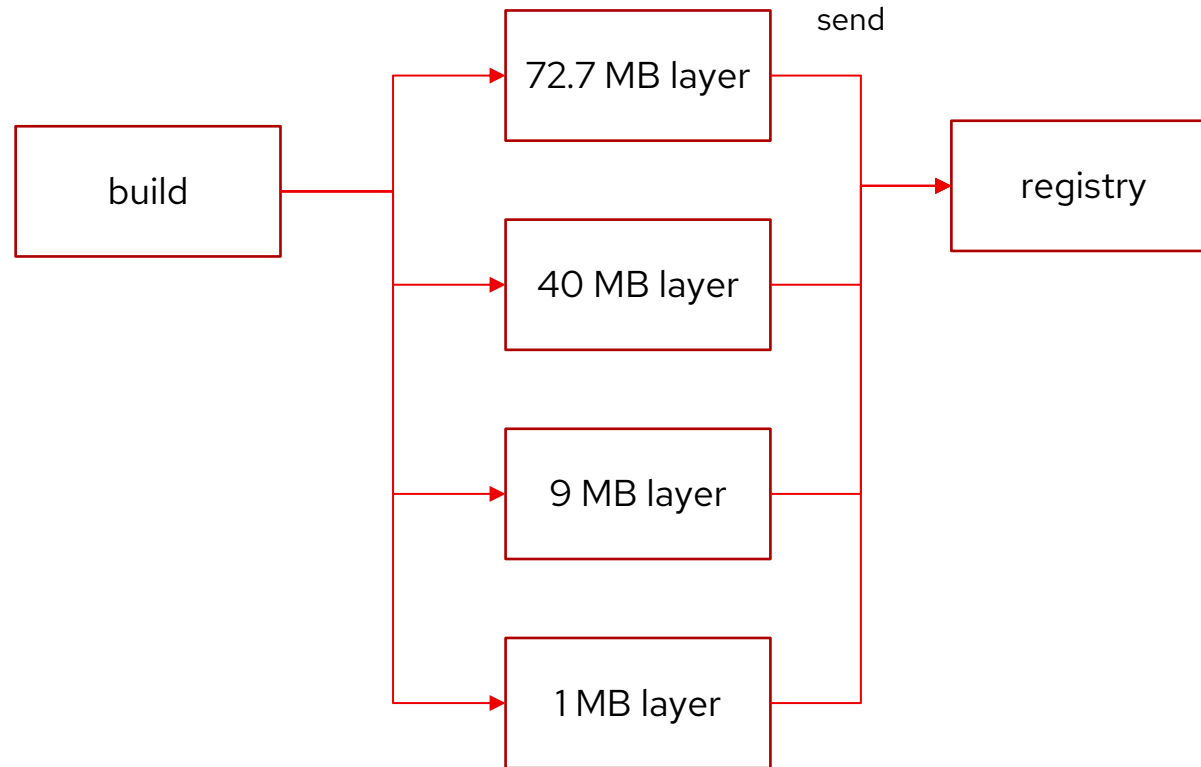
Construct application layers the right way



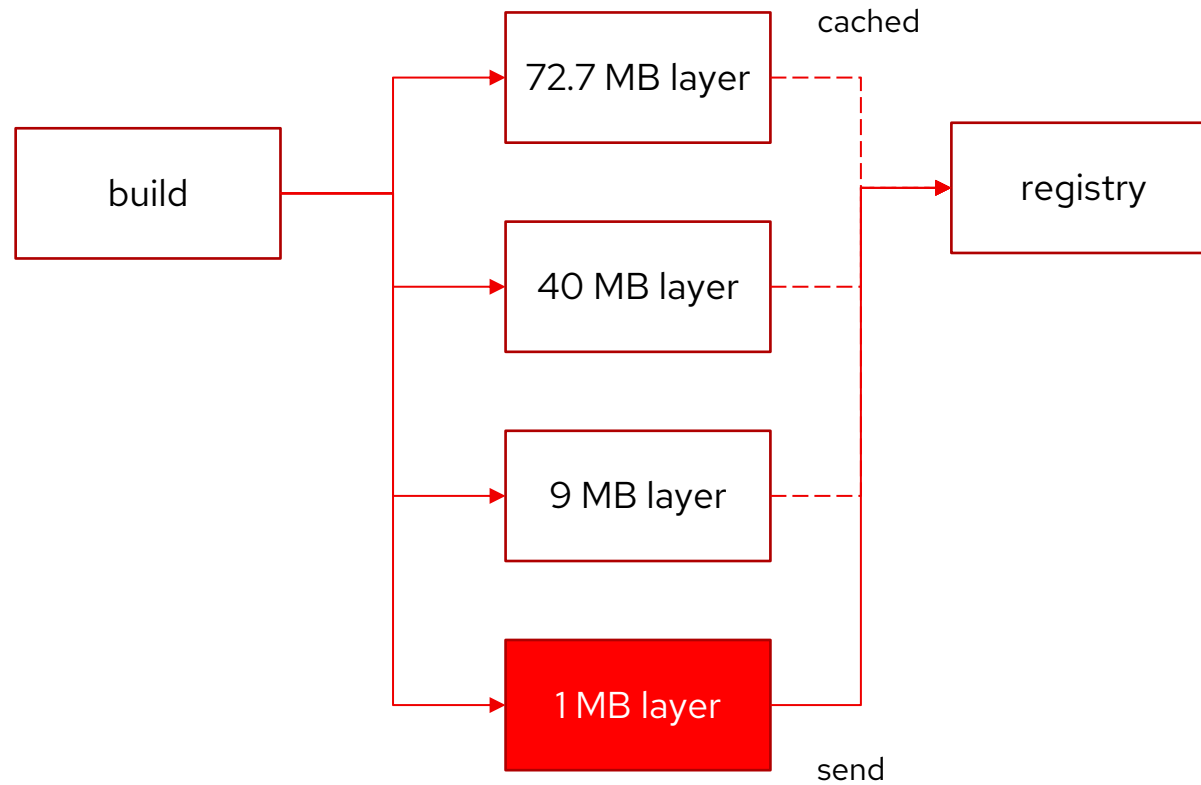
Construct application layers the right way



Construct application layers the right way



Construct application layers the right way



Construct application layers the right way

72.7 MB layer

FROM registry.redhat.io/ubi7/ubi

40 MB layer

COPY target/dependencies /app/dependencies

9 MB layer

COPY target/resources /app/ resources

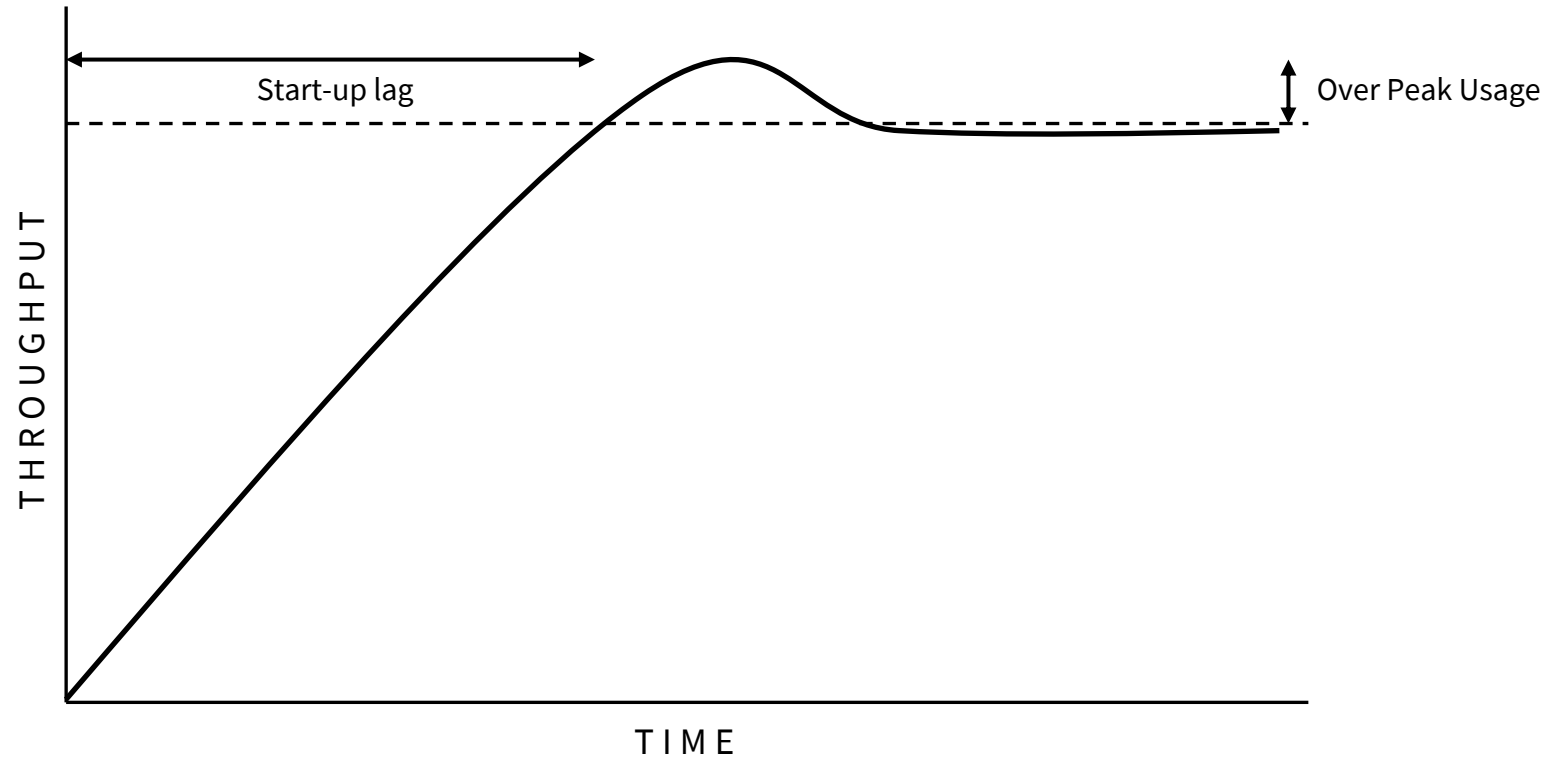
1 MB layer

COPY target/classes /app/ classes

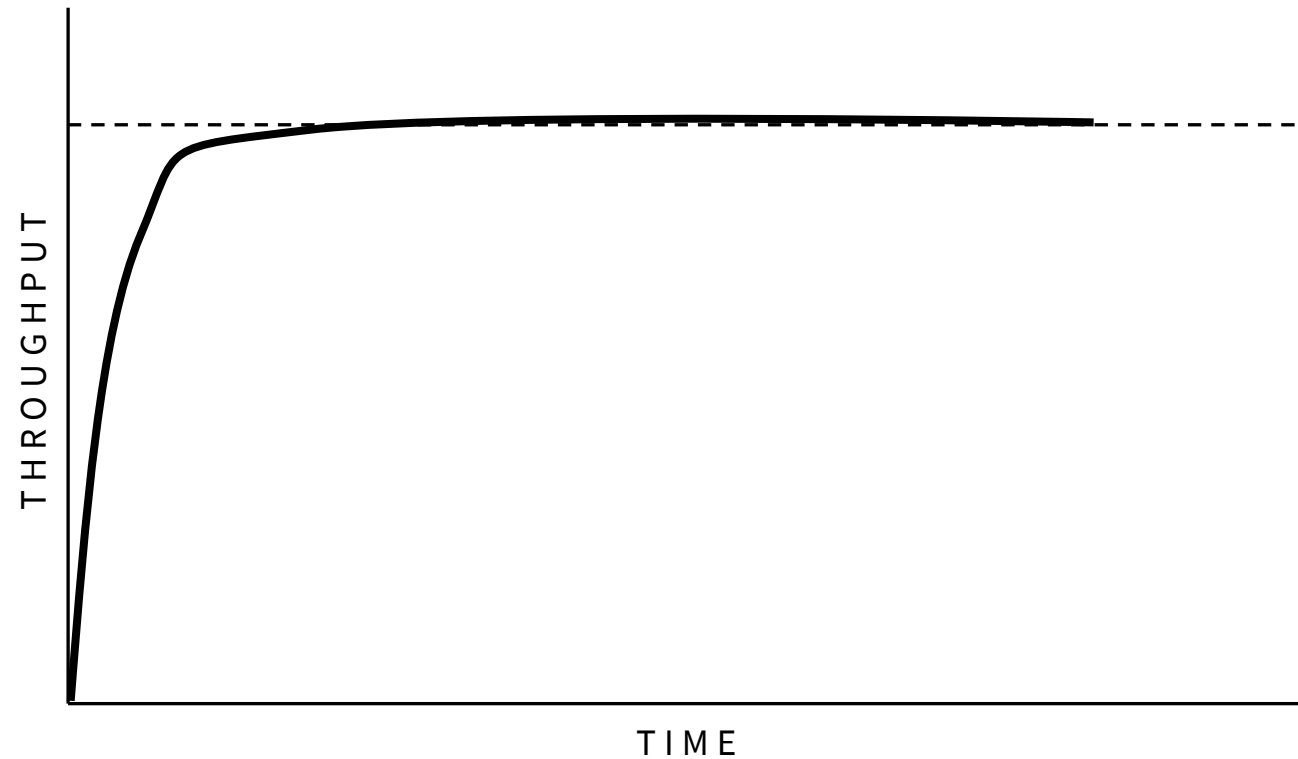
ENTRYPOINT java -cp /app/dependencies/*: /app/ resources: /app/ classes my.app.Main



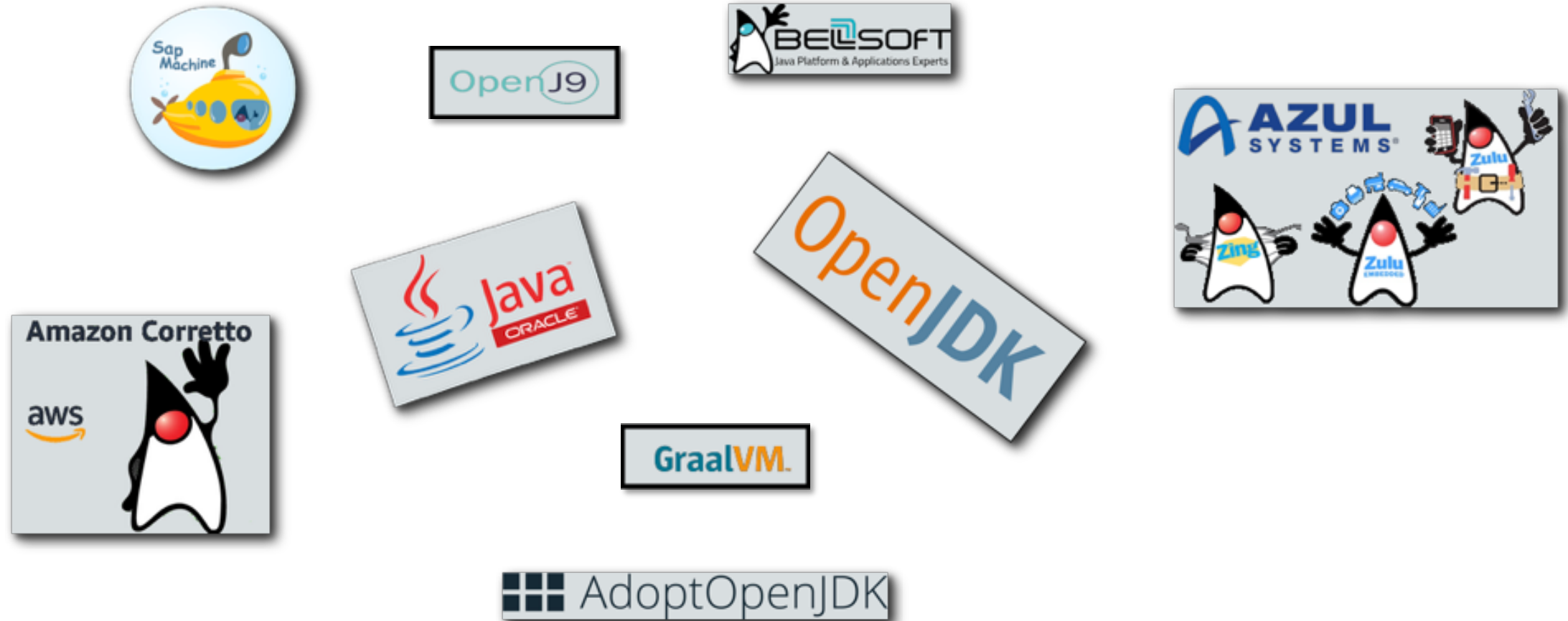
Typical Java Application Memory Usage



Ideal Memory Usage Profile to Save \$\$\$/€€€



Available Java Runtimes



Java 8u121??



Java 9, 8u131

- `-XX:ParallelGCThreads` and `-XX:CICompilerCount` are set based on Containers CPU limits (can be overridden)
 - calculated from `--cpuset-cpus`
- Memory Configuration
 - `-XX:+UnlockExperimentalVMOptions`
 - `-XX:+UseCGroupMemoryLimitForHeap`
 - set `-XX:MaxRAMFraction` to 2 (default is 4)

Java 10+ & 8u191 +

More container awareness...

- Improve heap memory allocations [JDK-8196595]:
 - `-XX:InitialRAMPercentage`, `-XX:MaxRAMPercentage`, and `-XX:MinRAMPercentage`
 - `-XX:InitialRAMFraction`, `-XX:MaxRAMFraction`, and `-XX:MinRAMFraction` are Deprecated
- The total number of CPUs available to the Java process is calculated from `--cpus`, `--cpu-shares`, `--cpu-quota` [JDK-8146115]
 - Use `-XX:-UseContainerSupport` to return to the old behavior
 - # processors that the JVM will use internally `-XX:ActiveProcessorCount`
- Attach in linux became be relative to `/proc/pid/root` and namespace aware (`jcmd`, `jstack`, etc)

Java 11

Even more container awareness...

- **Removes** `-XX:+UnlockExperimentalVMOptions`, `-XX:+UseCGroupMemoryLimitForHeap` [JDK-8194086]
- `jcmd -l` and `jps` commands do not list JVMs in Docker containers [JDK-8193710]
- Container Metrics (`-XshowSettings:system`) [JDK-8204107]
- Update CPU count algorithm when both cpu shares and quotas are used [JDK-8197867]
 - `-XX:+PreferContainerQuotaForCPUCount`

Java 12 & 13

Even more more container awareness...

- Adds container support to jhsdb command [JDK-8205992]
- Java Flight Recorder (JFR) improvements for containers [JDK-8203359]
- Improve container support when Join Controllers option is used [JDK-8217766]
- Improve systemd slice memory limit support [JDK-8217338]

Java and Container Future

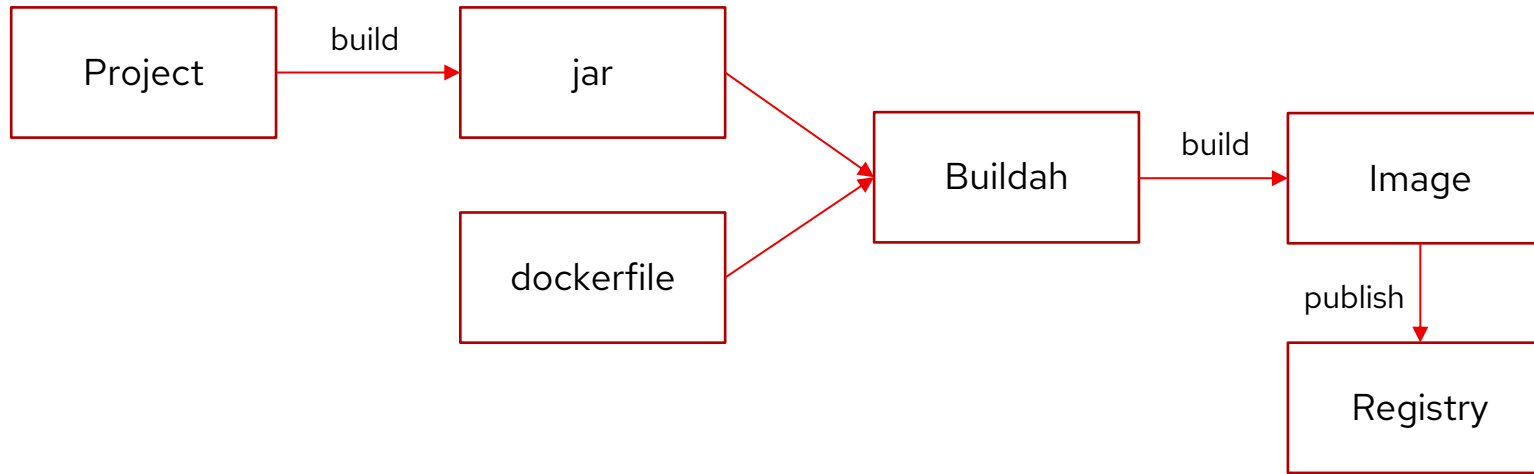
And maybe more to come...

- JFR `jdk.CPUInformation` event reports incorrect information when running in Docker container [JDK-8219999]
- Investigate adding NUMA container support to hotspot [JDK-8198715]
- Add Container MBean to JMX [JDK-8199944]

JVM Troubleshooting & Monitoring

- Built-in tools within the JDK:
 - jstat
 - jcmd
 - jmap (Not recommended)
 - jhat ...
- Expose JMX port
 - VisualVM
 - jConsole
- Micrometer
- Others: New Relic, Stackify, AppDynamics, Dynatrace...
- Docker commands
 - stats
 - inspect
 - top
- Container aware tools
 - ctop
 - dstat
- CAdvisor
- Prometheus
- Docker EE, Datadog, Sysdig, ...

How does the build process change?





“I am a **Java** developer, I don’t want to have to care about Dockerfiles, Images and stuff.”

Every Java Developer
Everywhere

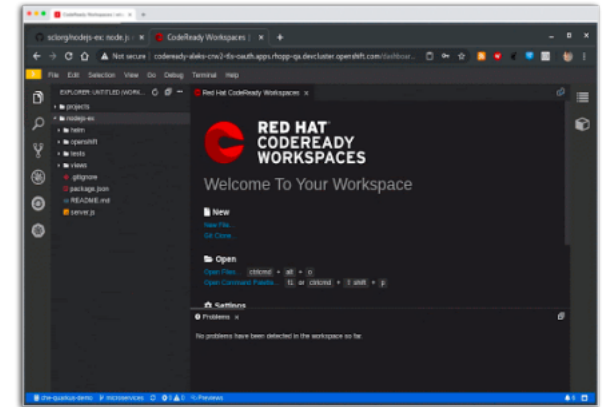
Your little build helper

Maven:

- fabric8-maven-plugin (Fabric8)
- dockerfile-maven-plugin (Spotify)
- Maven exec plugin (Not elegant!)
- jib-maven-plugin (Google)

Gradle

- Docker Gradle Plugin (Benjamin Muschko)
- Docker Gradle Plugin (palantir)
- Docker Gradle Plugin (Transmode)
- jib-gradle-plugin (Google)



Quarkus

The Kubernetes native application development framework

- A Kubernetes Native Java stack tailored for GraalVM & OpenJDK HotSpot, crafted from the best of breed Java libraries and standards.
- Go comparable footprint and speed makes Java ready for cloud architectures and operations!
- Available as Community Release 1.0.
- **Build Time Metadata Processing and Reduction in Reflection Usage** lead to less memory usage, and also faster startup time.
- **Native Image Pre Boot** for super fast startup times.
- First Class Support for **Graal/SubstrateVM**

Project Site

<https://quarkus.io/>

GitHub Repo

<https://github.com/quarkusio/quarkus>

OpenShift odo

Developer CLI

A developer-focused command-line tool for rapid development iterations on OpenShift (inner loop).

Simplifies building of microservices applications on OpenShift.

```
$ odo create java backend  
Component 'frontend' was created.  
To push source code to the component run 'odo push'
```

```
$ odo push  
Pushing changes to component: frontend
```

```
$ odo url create  
frontend - http://frontend-myapp.192.168.99.100.nip.io
```

```
$ odo watch  
Waiting for something to change in /dev/frontend
```


IDE Integrations

VS Code, IntelliJ, Eclipse, Azure DevOps



OpenShift Connector by Red Hat

Azure DevOps > Azure Pipelines > OpenShift Extension




OpenShift Extension

Red Hat | 281 installs | ★★★★★ (0) | Preview

OpenShift tasks for Azure DevOps

[Get it free](#)

Visual Studio Code > Other > OpenShift Connector



OpenShift Connector Preview

Red Hat | 7,589 installs | 22,799 downloads | ★★★★★ (2) | Free

Interacting with Red Hat OpenShift clusters and providing a streamlined developer experience using Visual Studio Code

[Install](#) [Trouble Installing?](#)



<https://developers.redhat.com>

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

 linkedin.com/company/red-hat

 youtube.com/user/RedHatVideos

 facebook.com/redhatinc

 twitter.com/RedHat