Containers from Scratch

Bastian Hofmann

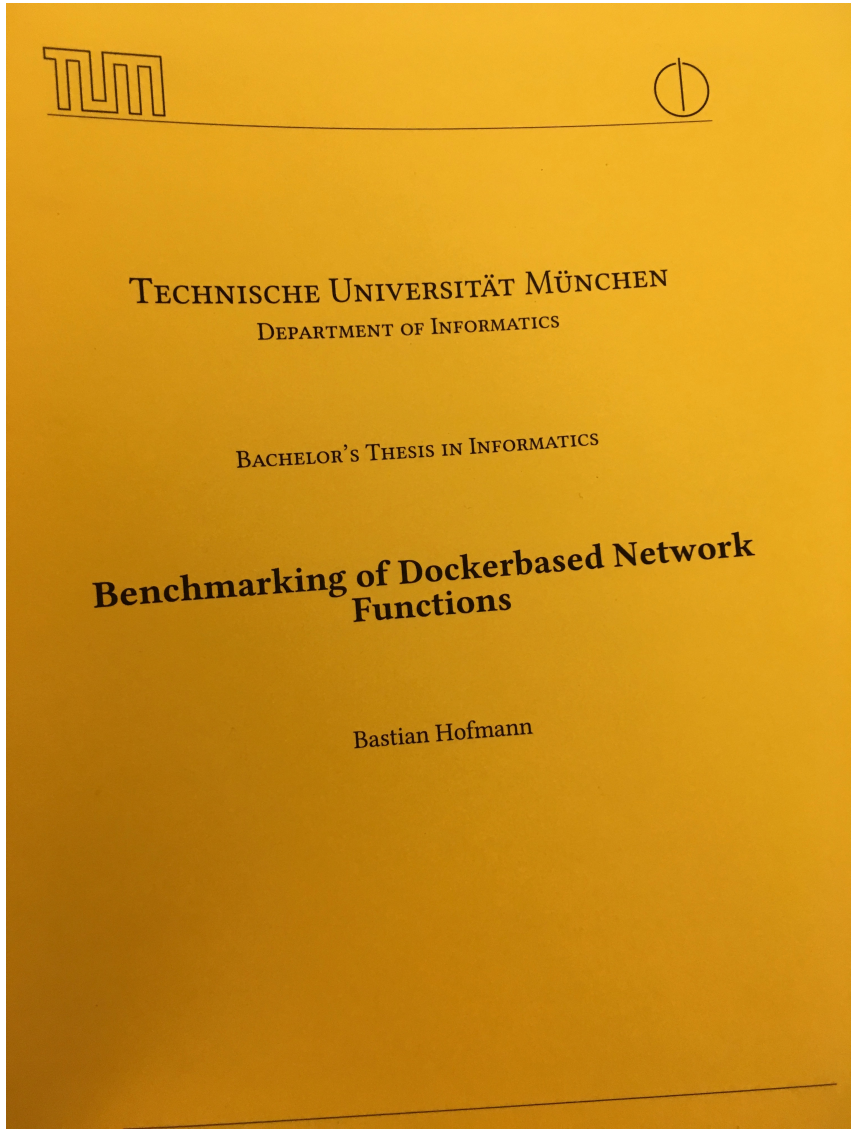
Docker Meetup Rosenheim

2019-04-11

About Me

- Ivoke GmbH
- Timecount GmbH
- **Joblocal GmbH**
- B. Sc. Informatik
  TU München
- **M. Sc. Informatik**
  TH Rosenheim

bastian.hofmann@joblocal.de



Joblocal GmbH

- Network of regional Jobportals in Germany.
- Microservice architecture (alongside monolith) powered by Docker hosted on AWS.
- We are hiring!
  - **Software Engineer (m/w/d)**
  - **DevOps (m/w/d)**

Goals of Virtualisation

- gather accurate resource usage statistics for groups of processes
- allocate part of the system's resources to a group of processes
- isolate system resources between groups of processes on one physical host
- separate instances of the operating system on one physical host
- $\Rightarrow$ make one physical host "feel" like multiple hosts

VM vs Container

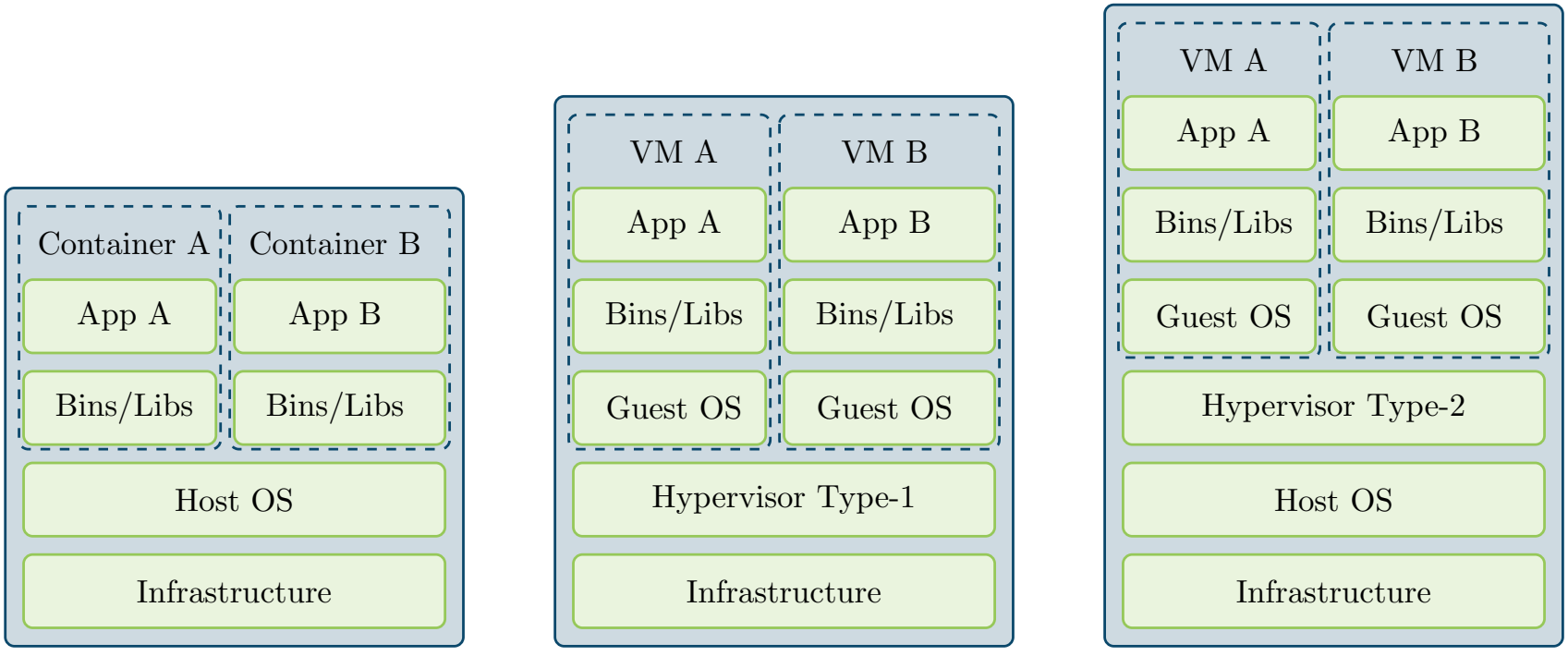


Figure: VM vs Container

VM vs Container

"I once heard that hypervisors are the living proof of operating system's incompetence" - Glauber Costa

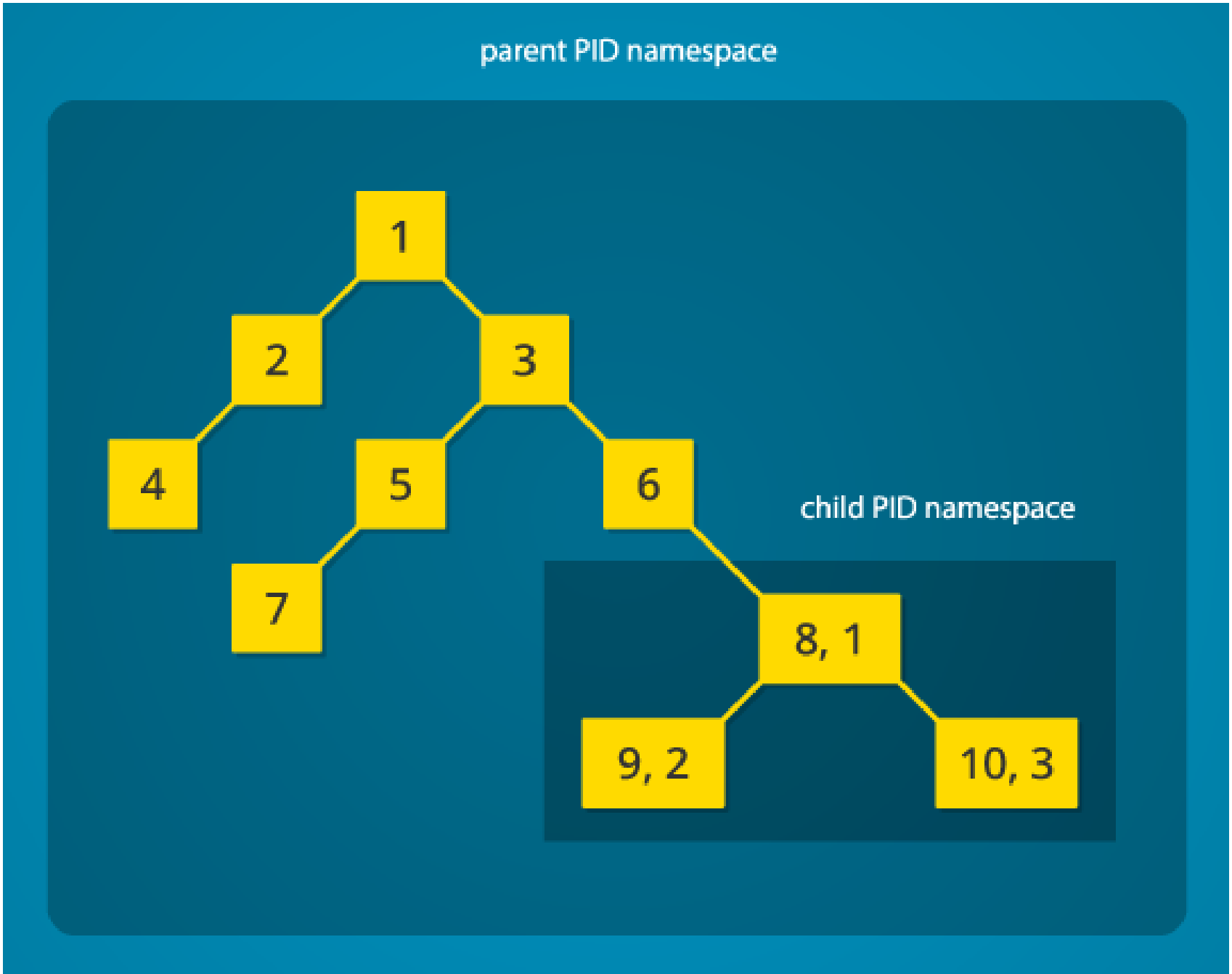
Namespaces

Mount namespace: 2002 in Linux kernel Linux 2.4.19 [1]

- Mount (mnt)
- Process ID (pid)
- Network (net)
- Interprocess Communication (ipc)
- UTS
- User ID (user)
- Control group (cgroup)

[1] https://lwn.net/Articles/689856/

Example - Process ID namespace



Demo

Chroot

- Changes the root directory of the calling process
- Only changes pathname resolution process
- Additional security measures required to achieve filesystem isolation

Cgroups

- Processes can be grouped in cgroups
- Resources can be limited per cgroup

Demo

Further Reading

- Security
  - Capabilities
  - AppArmor
  - Seccomp
- Images
  - WOC
  - Layered Filesystems

Open Container Initiative (OCI)

- Docker
- Red Hat
- IBM
- Microsoft
- Google
- SUSE
- Cruise Automation

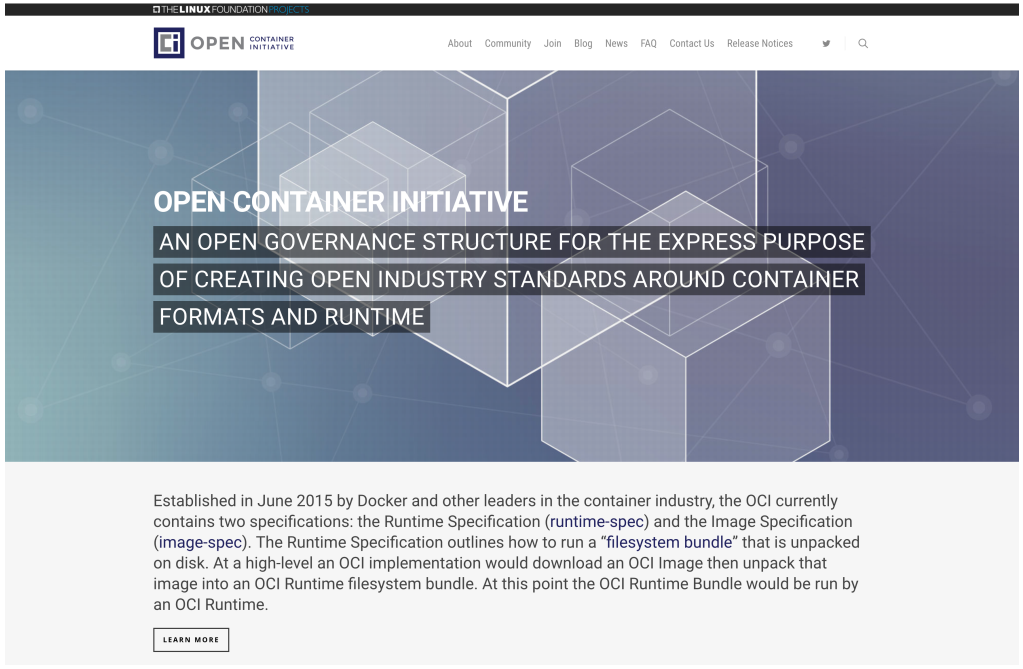


Figure: www.opencontainers.org

OCI Runtime Specification

"The goal of a Standard Container is to encapsulate a software component and all its dependencies in a format that is self-describing and portable, so that any compliant runtime can run it without extra dependencies, regardless of the underlying machine and the contents of the container."