Container technologies (Docker and Singularity)

Johann Gillhoff

Inhalt

- Warum Container technologies?
- What is a Container?
- Container vs VMs
- Technische Umsetzung
- Vor und Nachteile von von Containern
- Verwendung (Docker)
- Docker-Hub
- Singularity

Warum “Container technologies”?

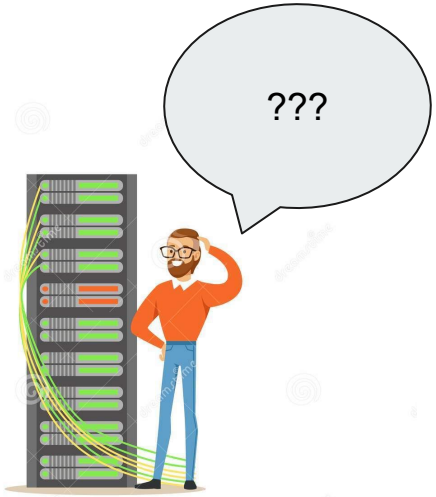
Warum “Container technologies”?

Java

php

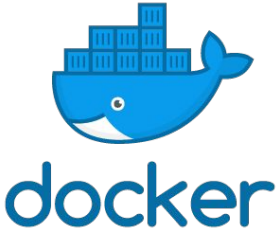
DLL

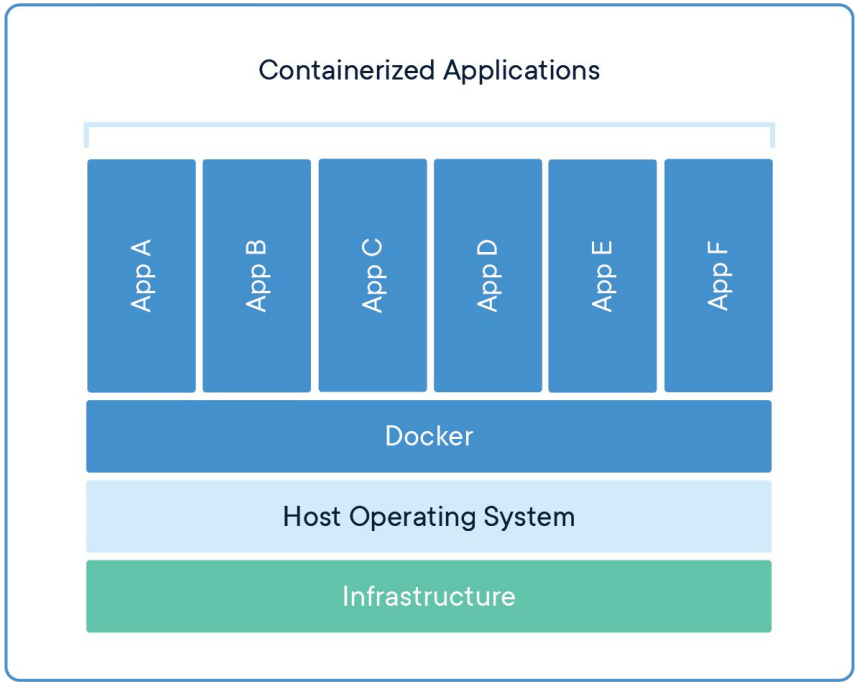
ubuntu

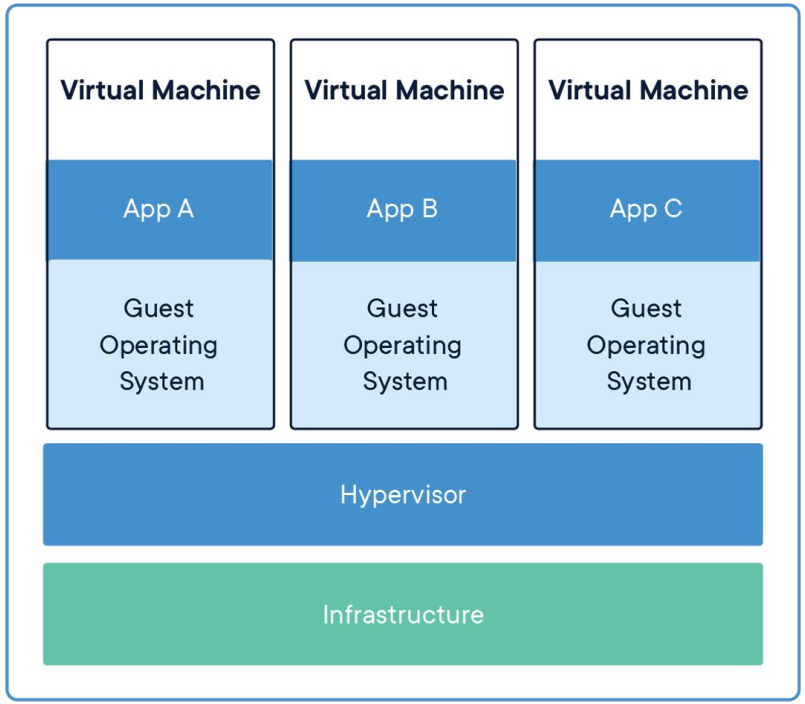


What is a Container?

A standardized unit of software

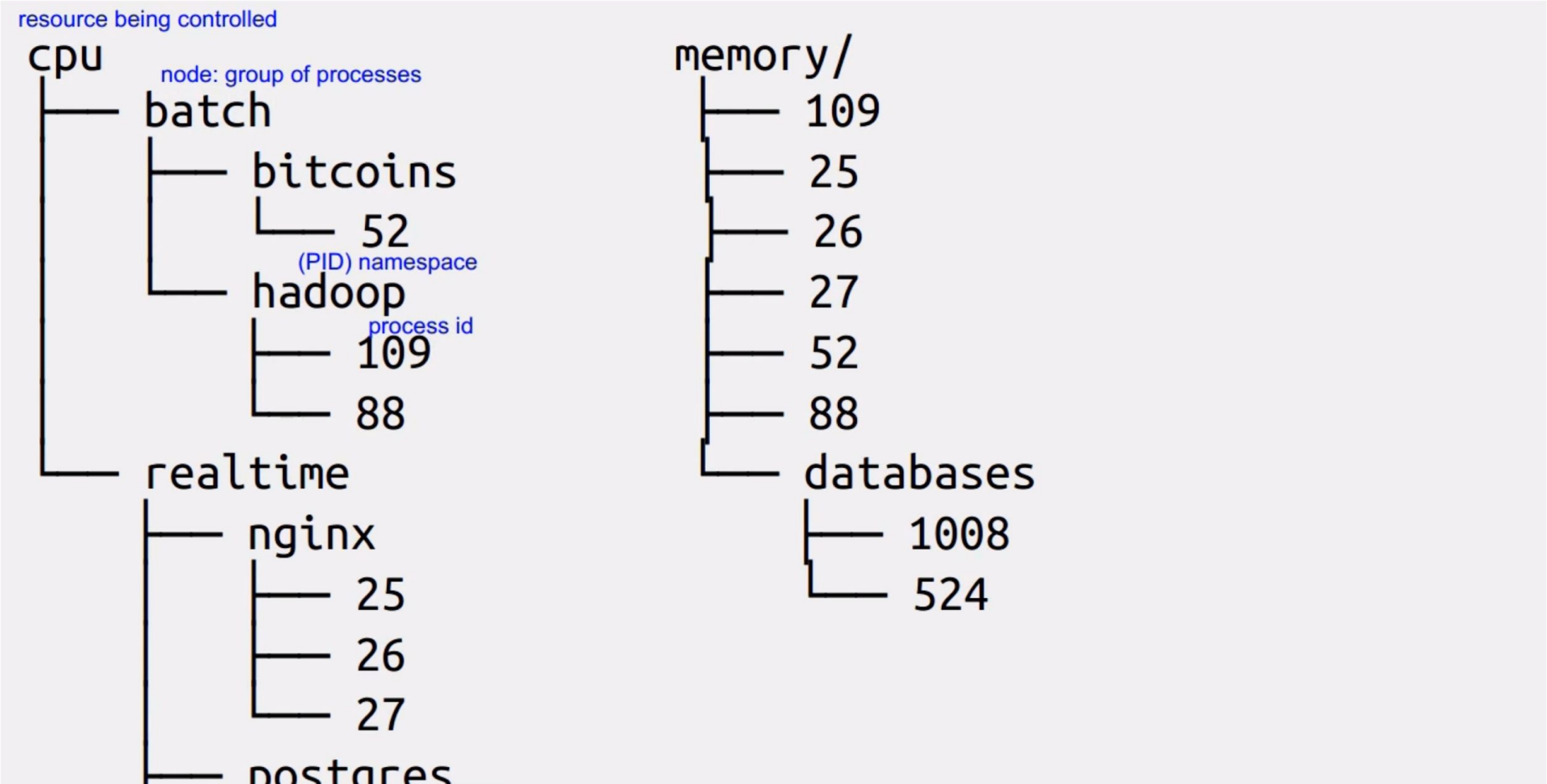



Containerized Applications
App A
App B
App C
App D
App E
App F
Docker
Host Operating System
Infrastructure


Virtual Machine
Virtual Machine
Virtual Machine
App A
App B
App C
Guest Operating System
Guest Operating System
Guest Operating System
Hypervisor
Infrastructure

Technische Umsetzung

- **cgroup**: limitiert ressourcen
  - memory
  - CPU
  - block I/O
  - network
- **namespaces:** gibt jedem Prozess eine eigene Sicht des Systems
  - pid
  - net
  - mnt
  - ...
- namespaces ist ein relativ neues Feature (July 2008)
- filterung von syscalls mit z.B. Seccomp


resource being controlled
cpu
node: group of processes
batch
bitcoins
52
(PID) namespace
hadoop
process id
109
88
realtime
nginx
25
26
27
memory/
109
25
26
27
52
88
databases
1008
524

Einschränkung von syscalls

Syscall	Description
`reboot`	Don't let containers reboot the host. Also gated by `CAP_SYS_BOOT` .
`request_key`	Prevent containers from using the kernel keyring, which is not namespaced.
`set_mempolicy`	Syscall that modifies kernel memory and NUMA settings. Already gated by `CAP_SYS_NICE` .
	Deny associating a thread with a namespace. Also gated by

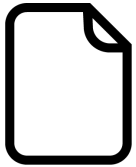
Vorteile von Containern

- Eliminierung des “Funktioniert doch auf meiner Maschine” Problems
- Container sind klein im Vergleich zu VMs
- Container verbrauchen weniger Ressourcen
- Ressourcen können geteilt werden
- Schnellere startzeiten als VMs

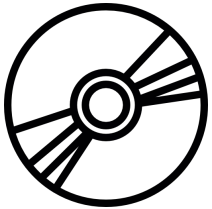
Nachteile von Containern

- **Isolation**: Container benutzen den gleichen Kernel
  - geringere Sicherheit als VMs
- GUI-Anwendungen funktionieren schlecht
- erhöhte (versteckte) Komplexität
- auf nicht-Linux Systemen muss trotzdem eine VM benutzt werden

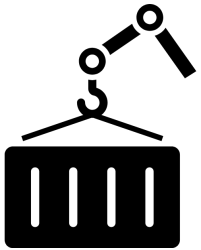
Verwendung (Docker)



Docker-File

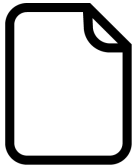


Docker-Image



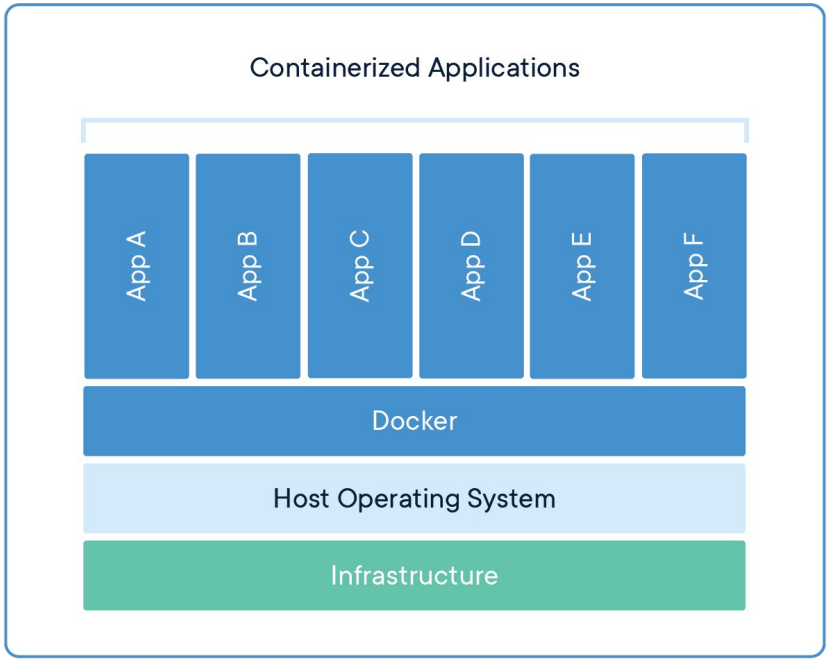
Docker-Container

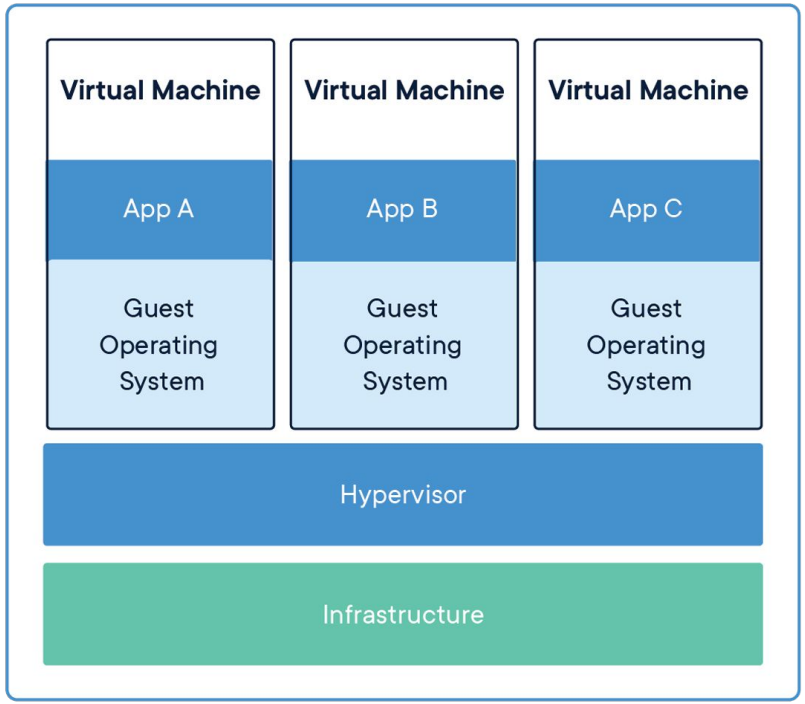
Verwendung (Docker)

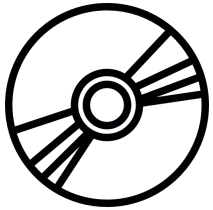


Docker-File

```
FROM ubuntu:18.04
COPY . /app
RUN make /app
CMD python /app/app.py
```

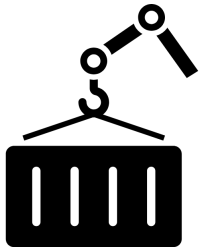

Containerized Applications
App A
App B
App C
App D
App E
App F
Docker
Host Operating System
Infrastructure


Virtual Machine
Virtual Machine
Virtual Machine
App A
App B
App C
Guest Operating System
Guest Operating System
Guest Operating System
Hypervisor
Infrastructure



Docker-Image

```
> docker build -t my-docker-image .
```



Docker-Container

```
> docker run my-docker-image -d -p 80:80
```

Docker-Hub

OFFICIAL IMAGE

redis

Updated an hour ago

10M+ Downloads 7.2K Stars

Redis is an open source key-value store that functions as a data structure server.

Container | Linux | Windows | IBM Z | PowerPC 64 LE | 386 | ARM 64 | ARM | x86-64 | Databases

OFFICIAL IMAGE

mongo

Updated an hour ago

10M+ Downloads 6.1K Stars

MongoDB document databases provide high availability and easy scalability.

Container | Linux | Windows | IBM Z | ARM 64 | x86-64 | Databases

OFFICIAL IMAGE

busybox

Updated an hour ago

10M+ Downloads 1.6K Stars

Busybox base image.

Singularity

- Für HPC
- HPC Systeme sind meist multi-user systeme
  - kein admin/root Zugriff für Benutzer gewünscht
  - direkter Zugriff auf docker Befehl erlaubt root-level access
  - schwierig mit Docker umzusetzen

Vielen Dank!

Quellen

- https://www.docker.com/resources/what-container#/package_software
- https://fr.slideshare.net/jpetazzo/anatomy-of-a-container-namespaces-cgroups-some-filesystem-magic-linuxcon
- https://www.youtube.com/watch?v=_dfLOzuIg2o
- https://www.quora.com/If-a-Docker-exists-why-would-anyone-use-singularity
- https://koukia.ca/why-docker-pros-and-cons-949d104478c5
- https://news.ycombinator.com/item?id=16892670
- https://www.youtube.com/watch?v=el7768BNUPw
- https://youtu.be/DA87Ba2dpNM?t=645
- https://security.stackexchange.com/questions/169642/what-makes-docker-more-secure-than-vms-or-bare-metal
- https://www.reddit.com/r/docker/comments/7y2yp2/why_is_singularity_used_as_opposed_to_docker_in/
- https://docs.docker.com/engine/security/seccomp/

Bildquellen

- https://jobsaround.tv/entwickler/res/img/programmierer-am-schreibtisch.png
- https://www.golem.de/1310/sp_102355-67112-i_rc.jpg
- https://image.flaticon.com/icons/png/512/55/55636.png
- https://www.docker.com/sites/default/files/d8/2018-11/container-vm-whatcontainer_2.png
- https://singularity.lbl.gov/images/logo/logo.svg
- https://www.docker.com/sites/default/files/social/docker_facebook_share.png