13.11.2019
ContainerConf 2019 / Mannheim

Eine kurze Geschichte der Containerisierung

Christoph Iserlohn

INNOQ

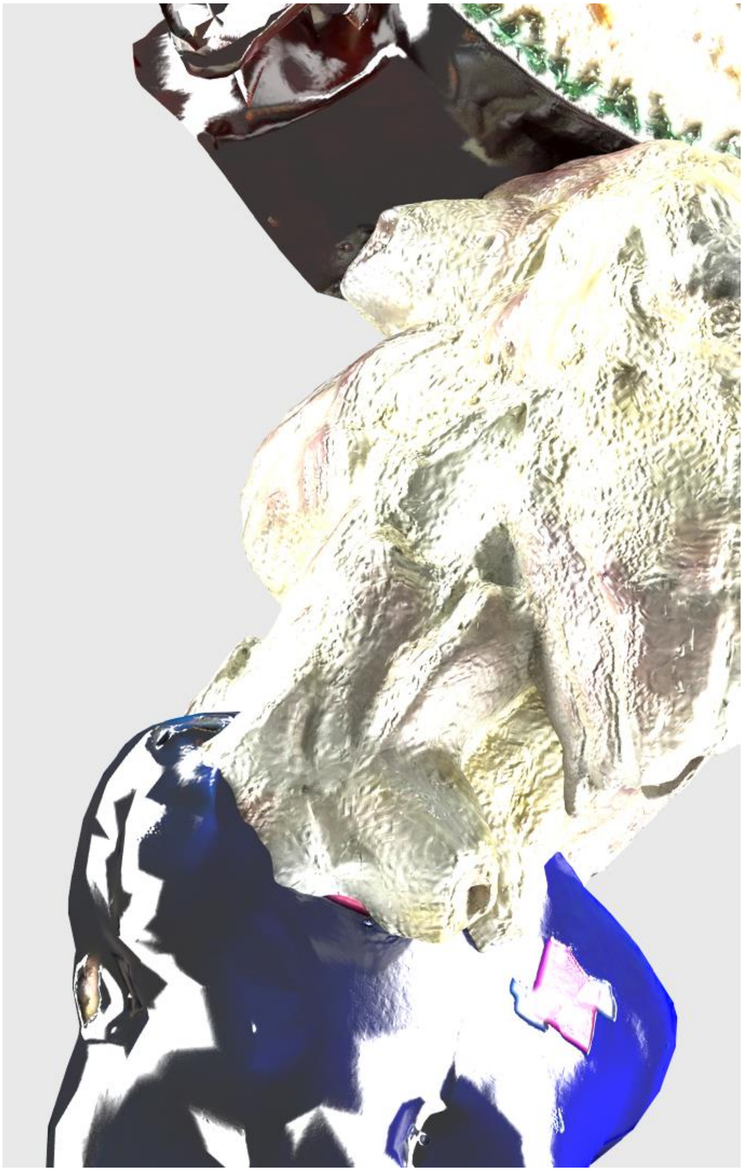
CHRISTOPH ISERLOHN

Senior Consultant @ INNOQ

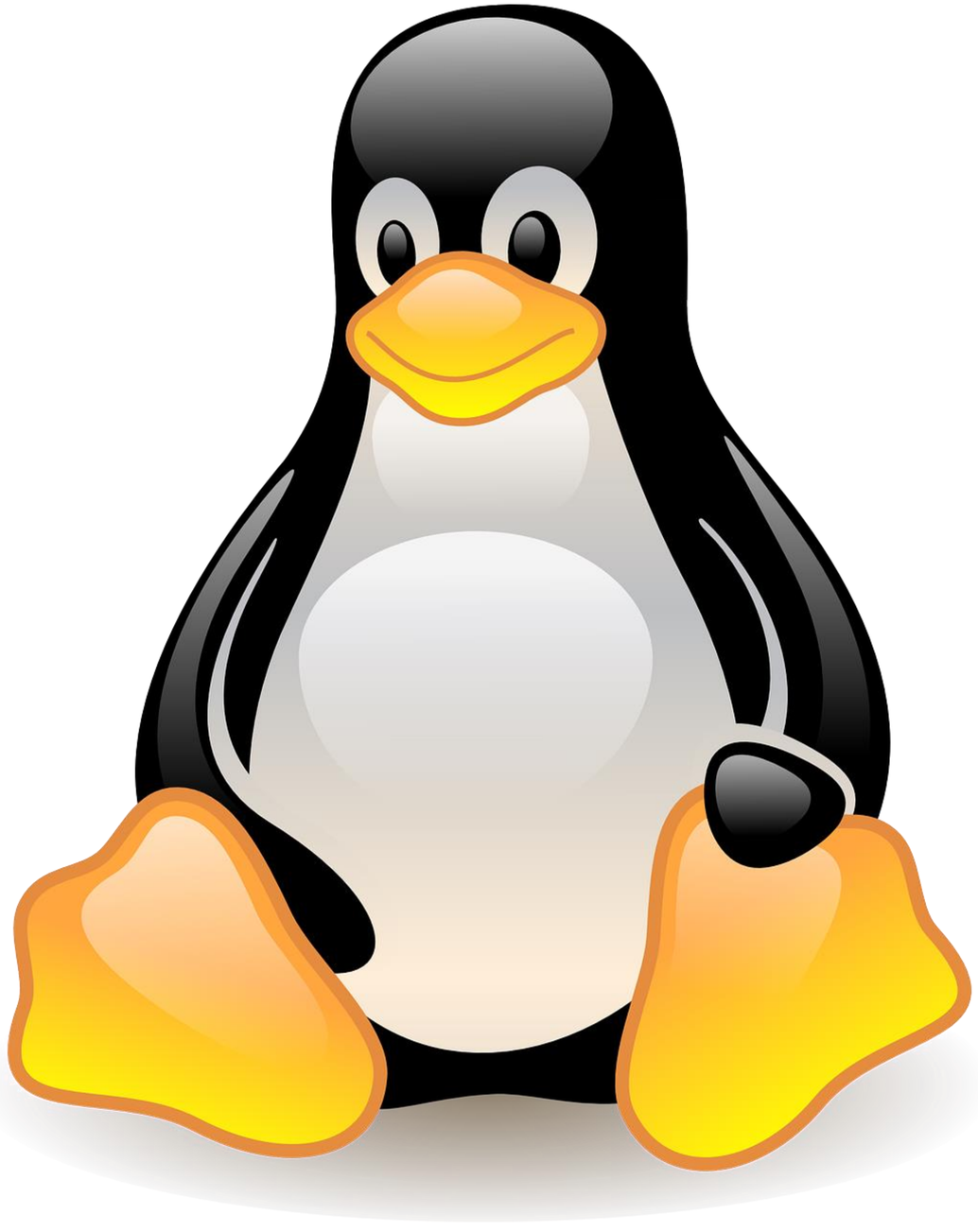
Container: Geheimnisse aus 40 Jahre Computergeschichte

Agenda

- 1979, 2000, 2001, 2004, 2005, 2006, 2008, 2013, 2017 und ein Blick in die Zukunft
- Chroot, FreeBSD Jails, Linux VServer, Solaris Zones, OpenVZ, LXC/LXD, Docker, J(2)EE, Kubernetes, Firecracker, gVisor
- Container selber machen mit chroot, namespaces und cgroups



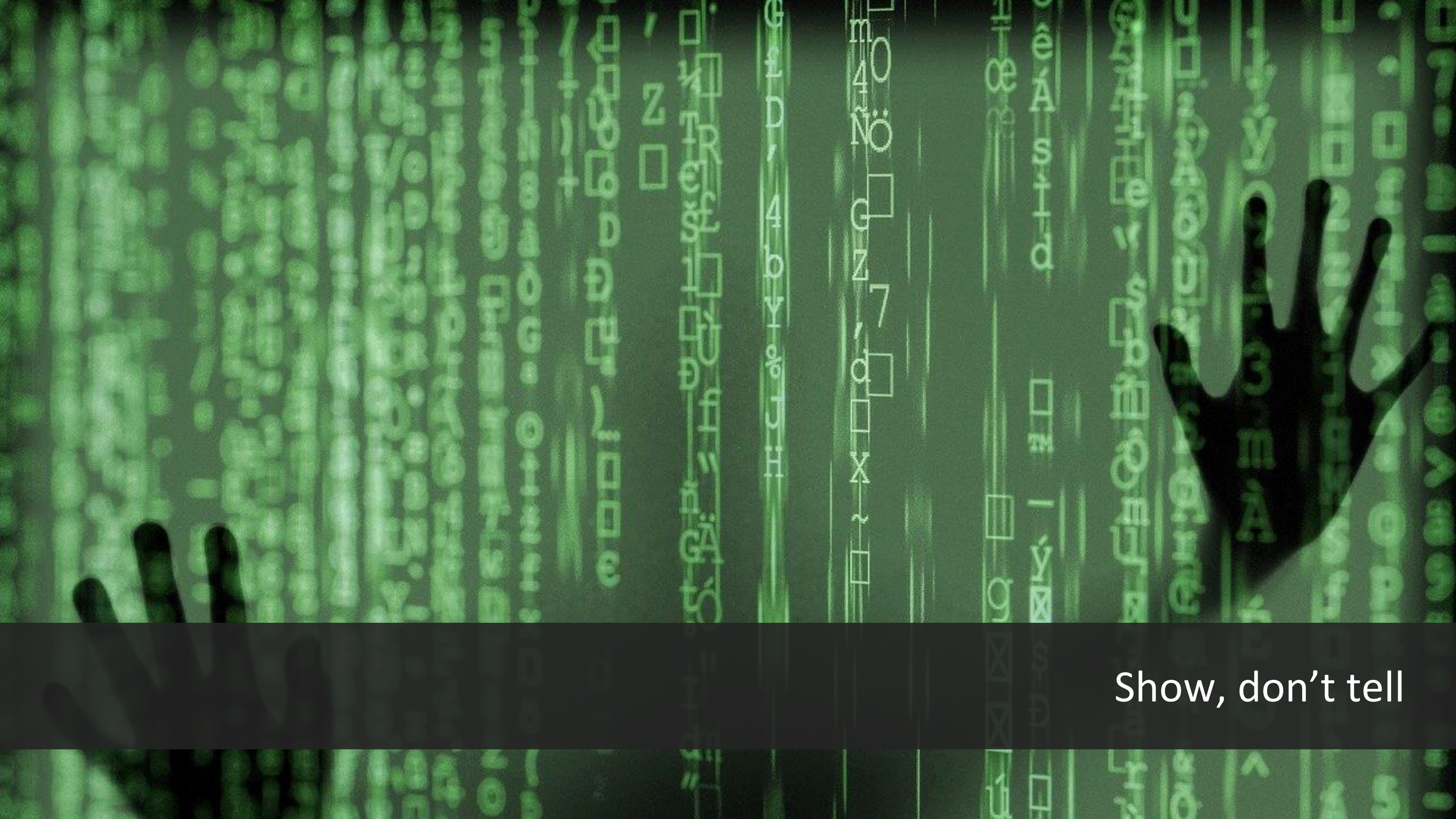

IBM
z



1979 - CHROOT

chroot

- `== change root`
- **Ändert das Wurzelverzeichnis (/) eines Prozesses sowie aller seiner Kindprozesse**
- **Einrichtung per CLI** `chroot(8)` **oder syscall** `chroot(2)`
- **Anwendungsgebiete: Testen, Isolation, Rechtetrennung, ABI-Kompatibilität mit alten Programmen**
- **Sicherheitsfeature? Abhängig von *NIX Variante**



Show, don’t tell

Unsere Container schleppen zu viel Ballast mit sich rum


L2 O1 V4 E

2000 - FreeBSD Jails

FreeBSD Jails

- **Explizit als Sicherheitsfeature ausgelegt**
- **Baut auf** `chroot` **auf**
- **Eigener Hostname**
- **Eigene IP-Adresse**
- **Eigene** `user` **und** `root` **Konten**
- **Kein Änderungen an Kernel/Netzwerk, kein** `mount, sysctls`
- **Einrichtung per CLI** `jail(8)` **oder syscall** `jail(2)`

Jailbreak

Linux™ Server

OpenVZ

2001 - Linux Vserver / OpenVZ

Linux VServer / OpenVZ

- **OpenVZ seit 2005 die Open-Source Variante von Virtuzzo (2001)**
- **Linux VServer/OpenVZ sind in der Funktionsweise sehr ähnlich**
- **Vergleichbare Funktionen wie `namespaces` und `cgroups`**
- **Einsatz primär bei Webhostern**
- **Pflege als Patchset außerhalb des Mainline-Kernels**
- **Nur noch wenig Verbreitung**

2004 - Solaris Zones

Solaris Zones

- **Bis Solaris 10 (2005) war `chroot` kein Sicherheitsfeature**
- **Danach *„chroot on steroids“***
- **Wie FreeBSD Jails plus dediziert zugewiesene Ressourcen**
- **Branded Zones – Zonen mit abweichendem Betriebssystem:**
  - **Solaris 8**
  - **Solaris 9**
  - **Red Hat Enterprise Linux 3**


Container

2002 - namespaces

namespaces

- **Isolation von globalen Kernel-Ressourcen für Prozesse:**
  - **PID**
  - **UID / GID**
  - **IPC**
  - **UTS**
  - **Network**
  - **Mount**
  - **cgroup**

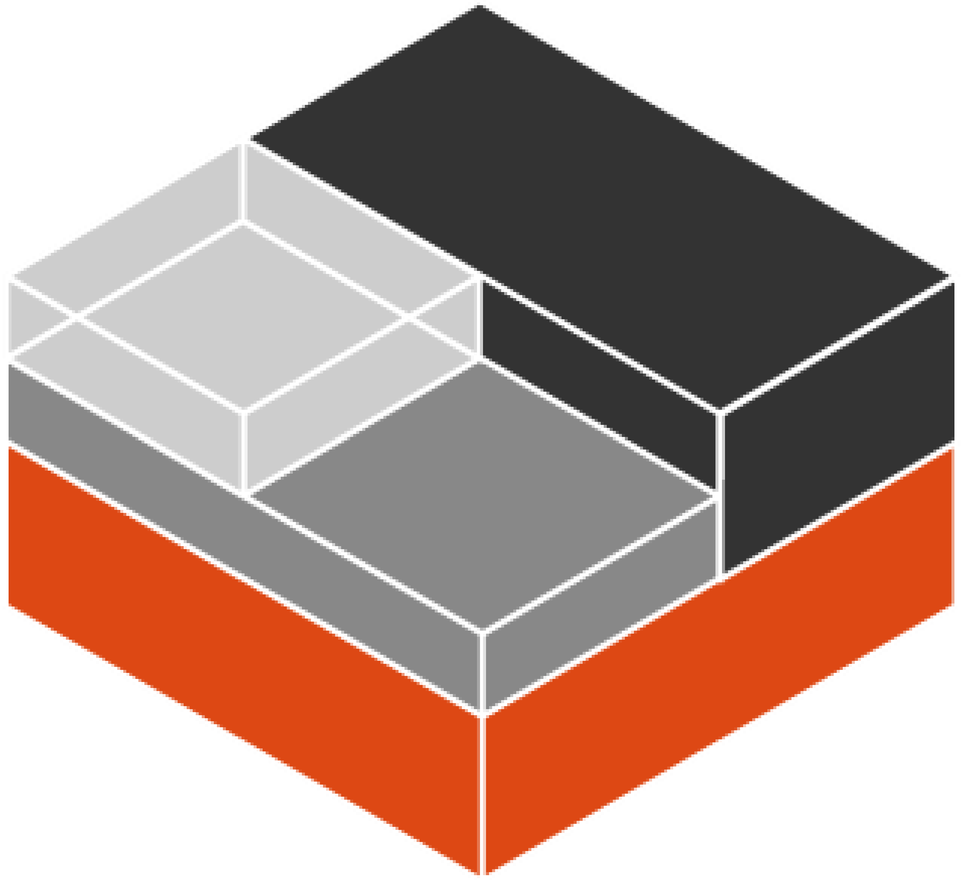
2006 - cgroups

cgroups

- **Ursprünglich** *process containers*
- **Ressourcen Beschränkung für Prozesse:**
  - **CPU**
  - **I/O**
  - **Memory**
  - **Network**


Container
selber bauen

https://github.com/innoq/container-conf-2019



2008 – LXC / LXD

LXC / LXD

- **LXC = Linux Containers**
- **LXD = Container Manager**
- **Wiederverwendung über Templates**
- **Ressourcenbeschränkung und Isolation über** `cgroups`, `namespaces` **und** `chroot`
- **Unterstützung von CRIU (Checkpoint/Restore in Userspace)**
- **Focus auf** *system containers*

2013 – Docker

Docker

- **CLI, Runtime, Container Manager**
- **Wiederverwendung über Images**
- **Ressourcenbeschränkung und Isolation über** `cgroups`, `namespaces` **und** `chroot`
- **Focus auf** *application containers*

Warum ist Docker so erfolgreich?

1. **Benutzerfreundlichkeit**
2. **Standardisierte Deployment-Unit**
3. **Ausrichtung auf Entwickler*Innen**

kubernetes

2014 - Kubernetes

Docker-Compose für verteilte Systeme / Rechenzentrum

Hatten wir das nicht alles schon einmal?

Docker / Kubernetes

==

J(2)EE done right!

WAT?

1. Standardisierte Deployment-Unit
2. Isolation von Anwendungen / Ressourcen
3. Lifecyclemanagement von Anwendungen


Ende der Geschichte?

1. Container sind nicht genügend isoliert
2. seccomp-bpf ist schwer zu konfigurieren
3. Für *aaS-Anbieter nicht praktikabel

gVisor

Die Zukunft

Danke. Fragen? Antworten!

Christoph Iserlohn
christoph.iserlohn@innoq.com

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim am Rhein
Germany
+49 2173 3366-0

Ohlauer Str. 43
10999 Berlin
Germany
+49 2173 3366-0

Ludwigstr. 180E
63067 Offenbach
Germany
+49 2173 3366-0

Kreuzstr. 16
80331 München
Germany
+49 2173 3366-0

Hermannstrasse 13
20095 Hamburg
Germany
+49 2173 3366-0

innoQ Schweiz GmbH

Gewerbestr. 11
CH-6330 Cham
Switzerland
+41 41 743 0116