Containerplattform

Lego für DevOps

Dr. Jonas Trüstedt

10. März 2018

SIMPLIFY YOUR DATACENTER

ATIX

orcharhino
RED HAT OPENSHIFT
docker

Configuration Management

puppet
SALTSTACK
ANSIBLE

Container

Datacenter Automation

Lifecycle Management

CONSULTING ENGINEERING SUPPORT

orcharhino

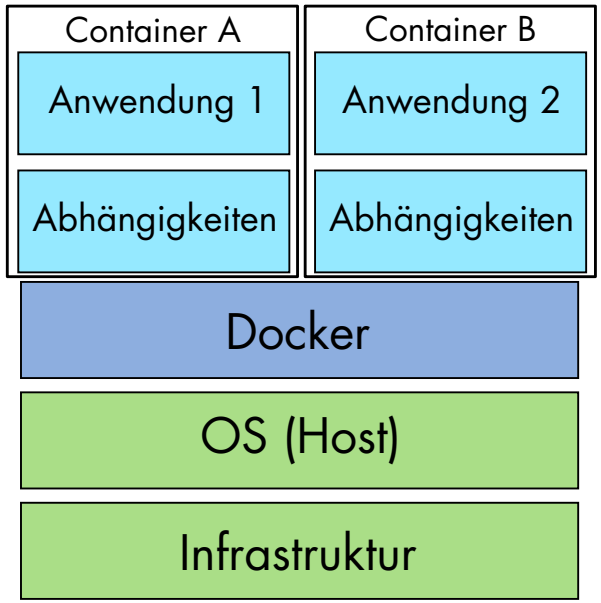
DEPLOY
RUN
CONTROL

Container

Virtualisierung in Containern:

- Minimalisierung der Abhängigkeiten
- Mit Host geteilter Kernel
- Wenig Overhead
- 1 Container pro Funktion/Prozess (Microservices)

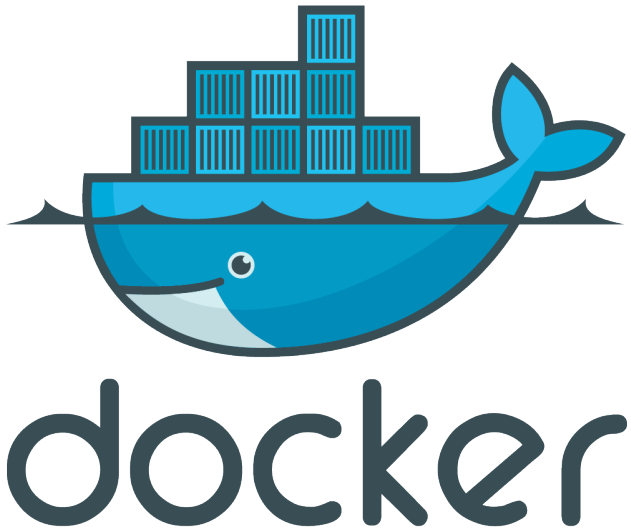
  → Anwendungen aus mehreren Containern



Container

Vorteile:

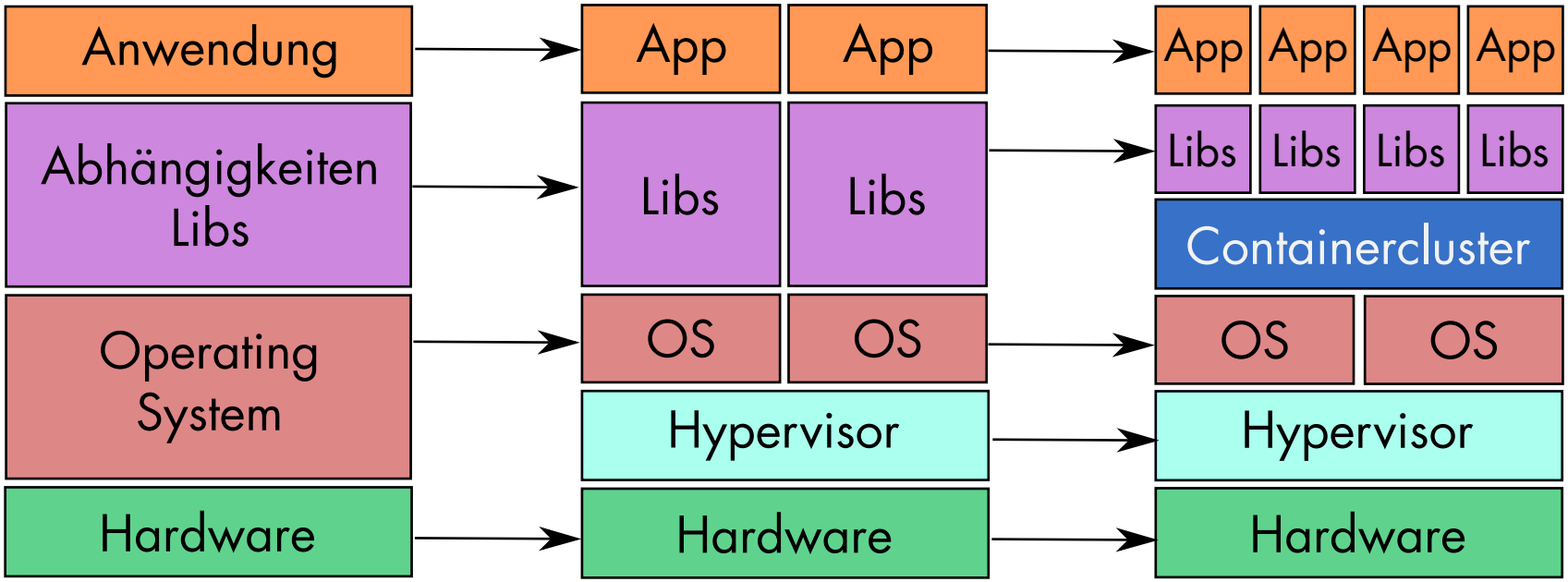
- Portabel
- Schnell
- Skalierbar
- Effiziente Hardwarenutzung



VMs vs Container
Pets vs Cattle

Container ≠ Docker
Alternative: z.B. rkt

Entwicklung der Server

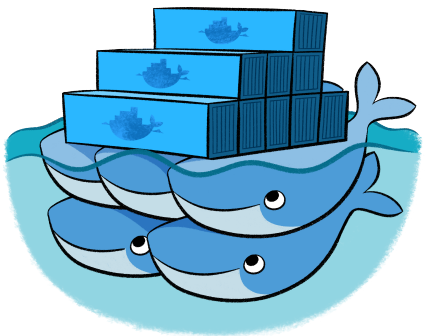


Ein Container kommt selten allein

Limits für einzelnen Docker-Host:

- Anzahl der Container
- Lastverteilung (Skalierung)
- Automatisierung

→ Erweiterung der Infrastruktur auf einen Cluster mithilfe von z.B.:



RANCHER

kubernetes

Containerorchestrierung

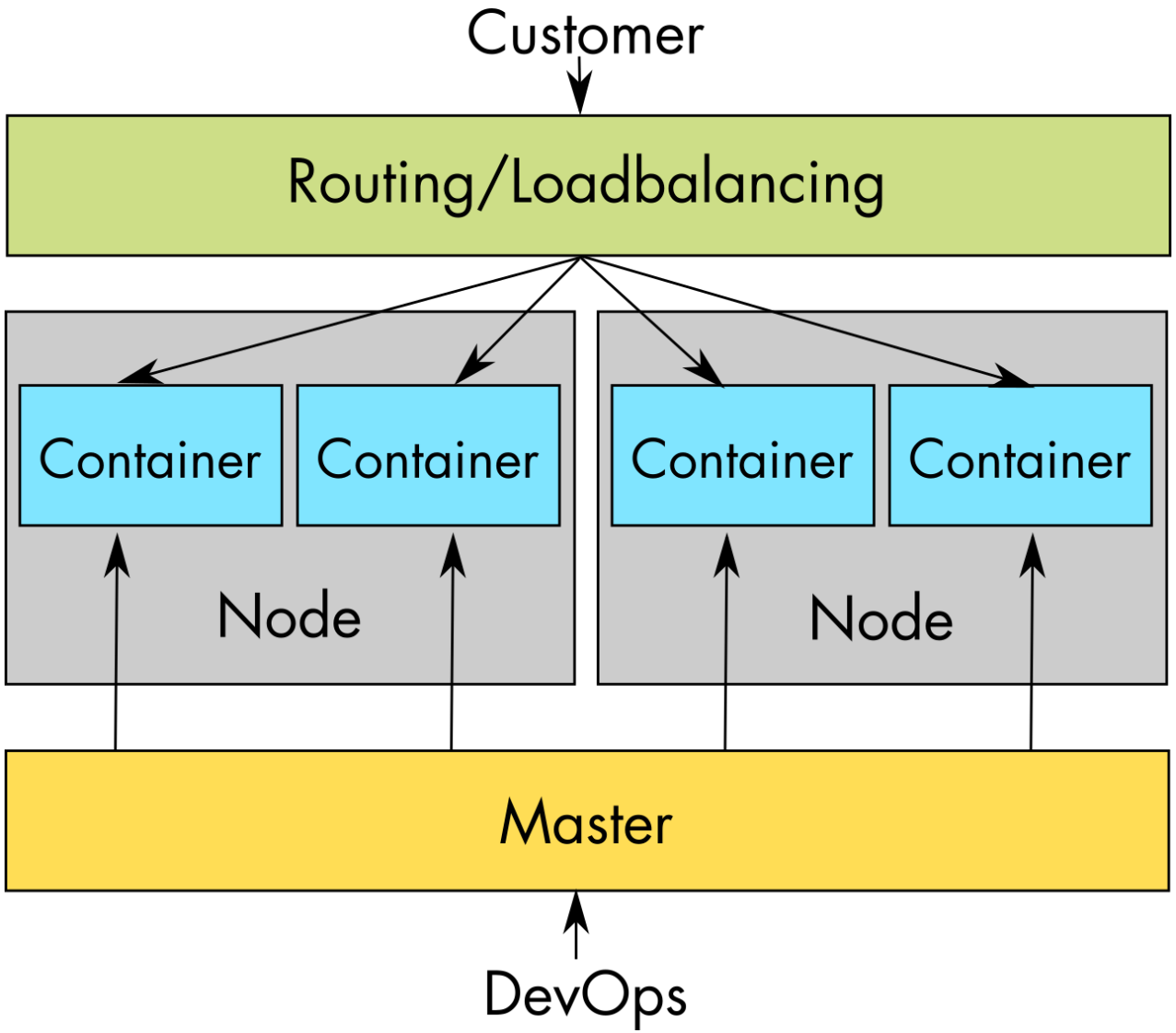
- Docker Swarm Mode:
  - Erweiterung auf mehrere Hosts von Docker selbst
- Rancher mit Cattle:
  - Unterstützung von Docker, Kubernetes, Mesos, Docker Swarm
  - Ab Version 2.0 nur mit Kubernetes
- Kubernetes:
  - Ursprünglich entwickelt von Google
  - Fokus auf hohe Skalierbarkeit

Kubernetes

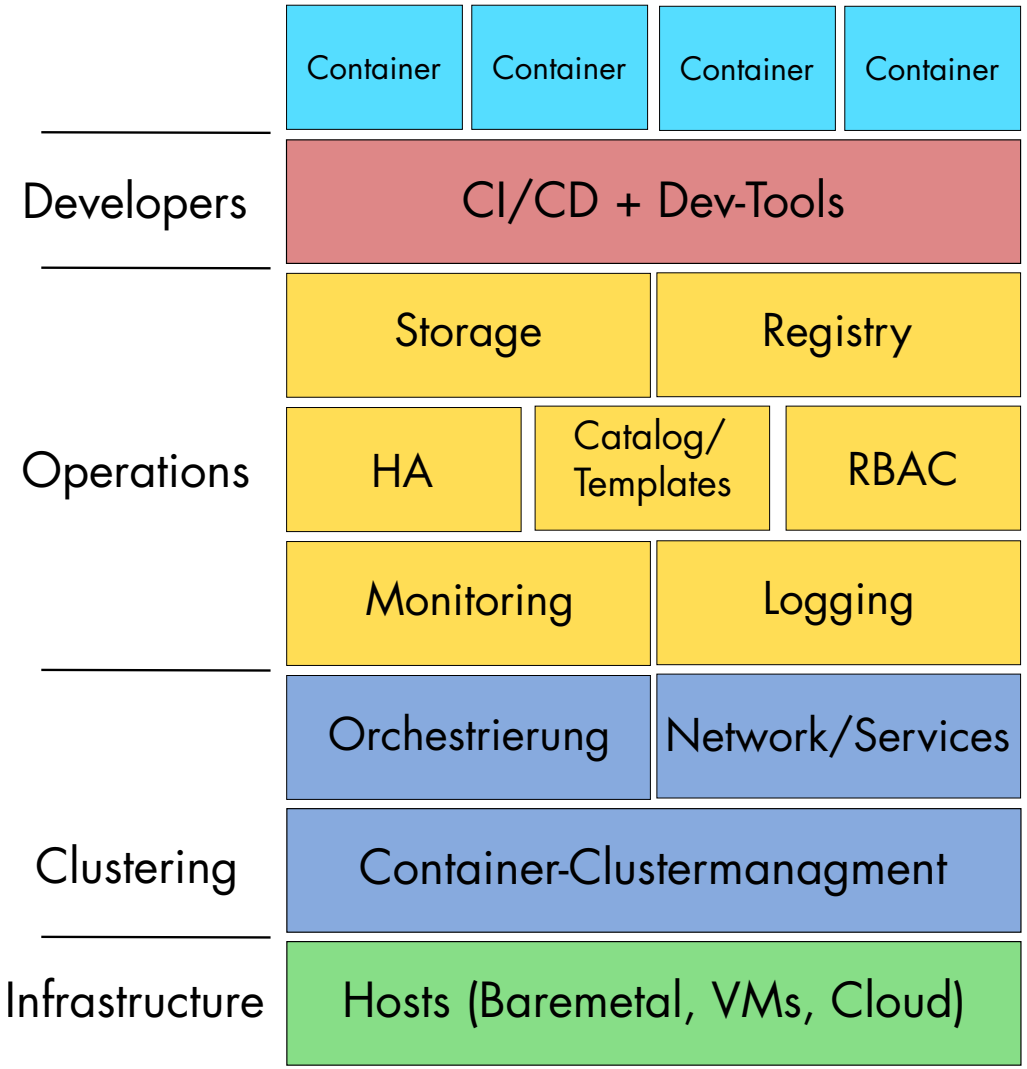
Kubernetes inzwischen Industriestandard:

- Rancher:
  Wechsel von Docker zu Kubernetes als Basiskomponente
- Red Hat:
  Openshift mit RHEL Atomic Host
- Canonical:
  Kubernetes mit Ubuntu Core
- SUSE:
  SUSE CaaS mit SLE MicroOS

Kubernetes - schematischer Aufbau



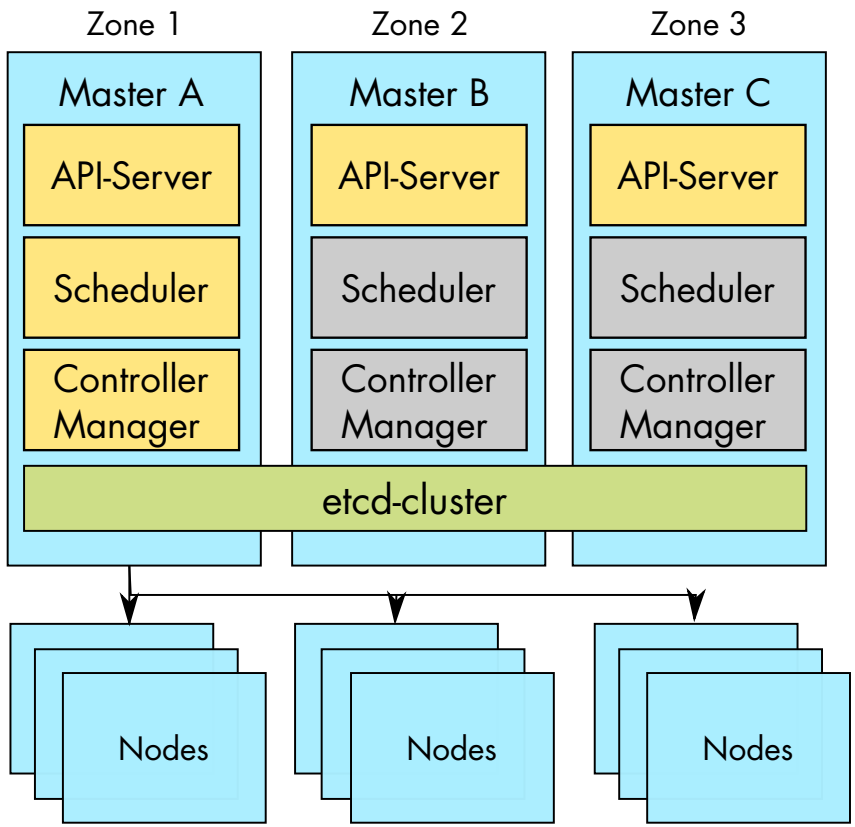
Containerplattform



Hochverfügbarkeit

HA-Umsetzung durch:

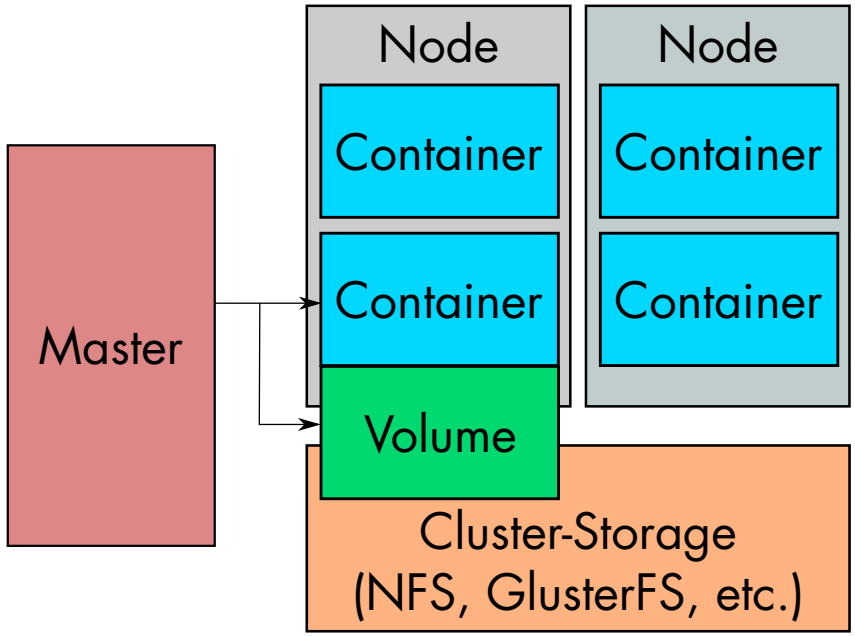
- 3 Master (oder mehr)
- Synchronisation der Konfiguration
- Node-Ausfälle automatisch abfangen
- Container-Ausfälle durch Healthchecks abfangen



Persistenter Speicher

Daten-Container:

- Cluster-Storage für alle Nodes erreichbar
- Bereitstellung von Volumes für Container
- Wahl des Storages bei Planung der Infrastruktur berücksichtigen!



Registry

Zentrale Sammelstelle für Containerimages
(z.B. Docker Registry, Quay, Docker Hub)

- Bereitstellung der Container-Images mit Versionskontrolle/Tags
- Intern gehostet oder öffentliche Varianten
- Docker Hub als zentrale öffentliche Registry

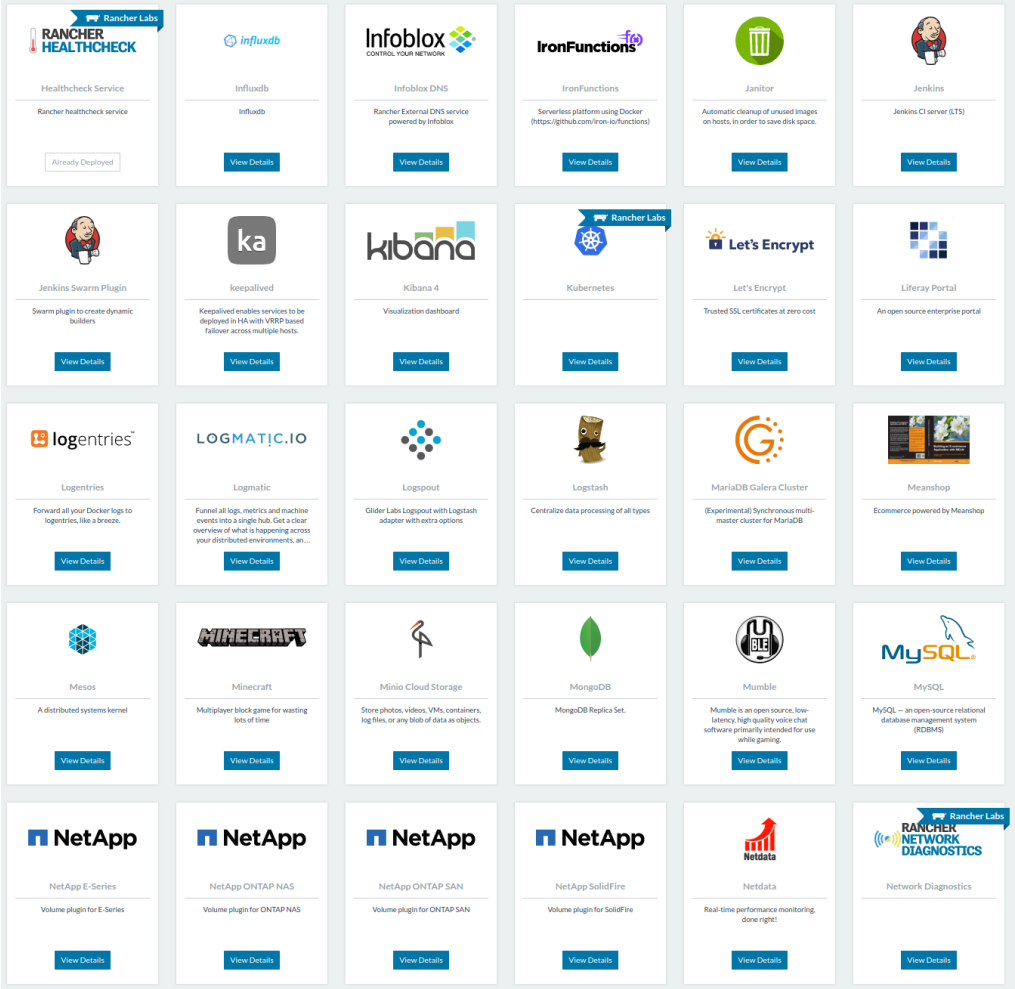
  → offizielle Images von Entwicklern

  → potentielles Sicherheitsrisiko
- Zertifizierte Registries wie z.B. Red Hat Container Catalog

Kataloge/Templates

Vorkonfigurierte Vorlagen:

- Häufig verwendete Setups schneller zu starten
- Verfügbarkeit für Nicht-Admins (Selbstbedienungsportal)

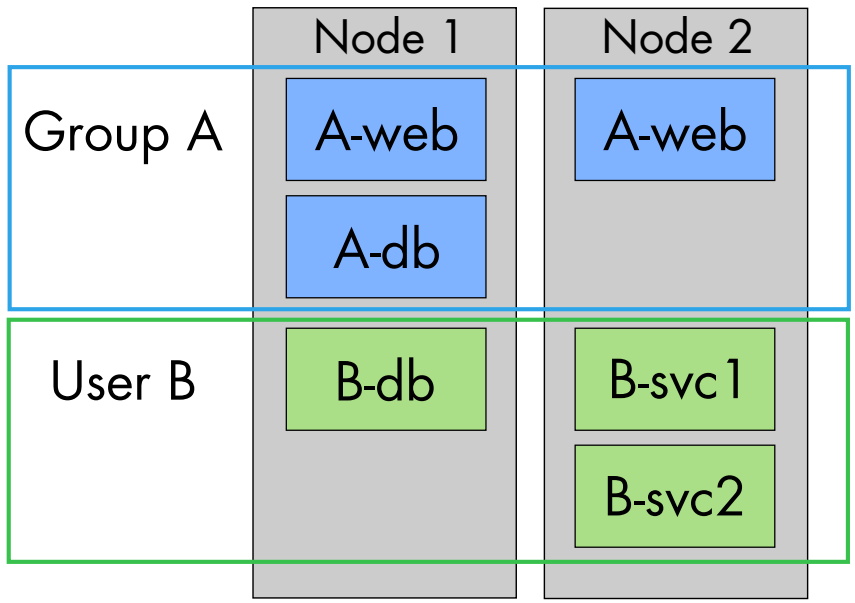


Ausschnitt des Rancher-Katalogs

RBAC

Rollenbasierte Zugriffsrechte:

- Rechteverwaltung für Benutzer, Gruppen, Umgebungen, Projekte
- Grafische Oberfläche (WebGUI)
- Zuweisung von Ressourcen an Projekte



Monitoring & Logging

Mögliche Monitoring Ansätze:

- Verfügbarkeit der Dienste (Health-Checks)
- Metrics = RAM-, CPU- und Netzwerkauslastung

  → Monitoring & Alerting-Tools z.B. mit Prometheus (+ Grafana) oder sysdig

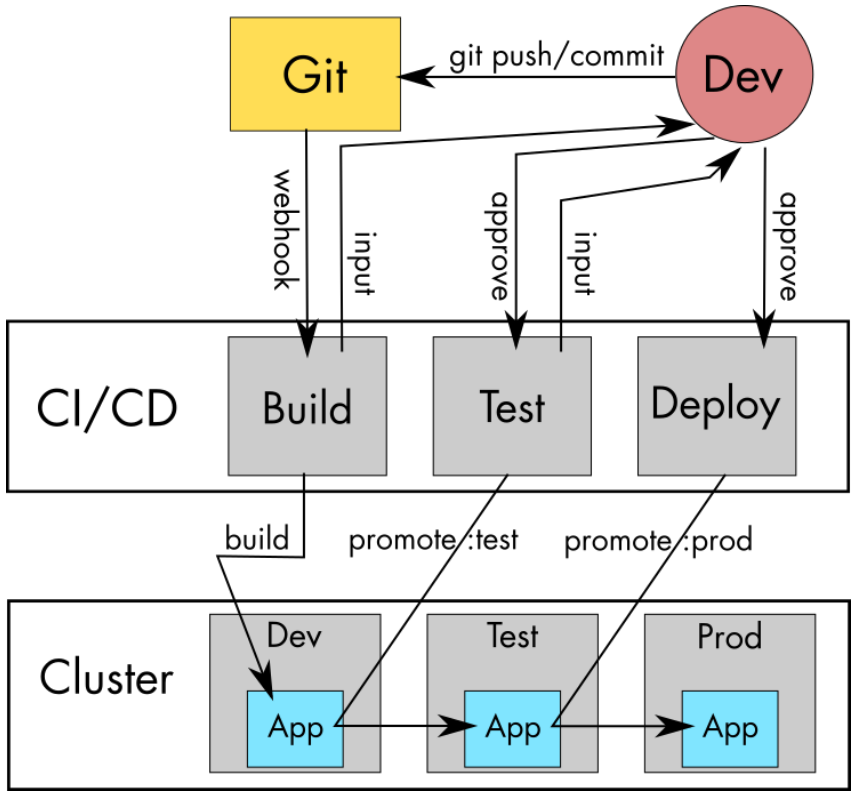
Logging:

- Fluentd als Logging-Agent
- Meistens mit Elasticsearch und Kibana (ELK/EFK-Stack)

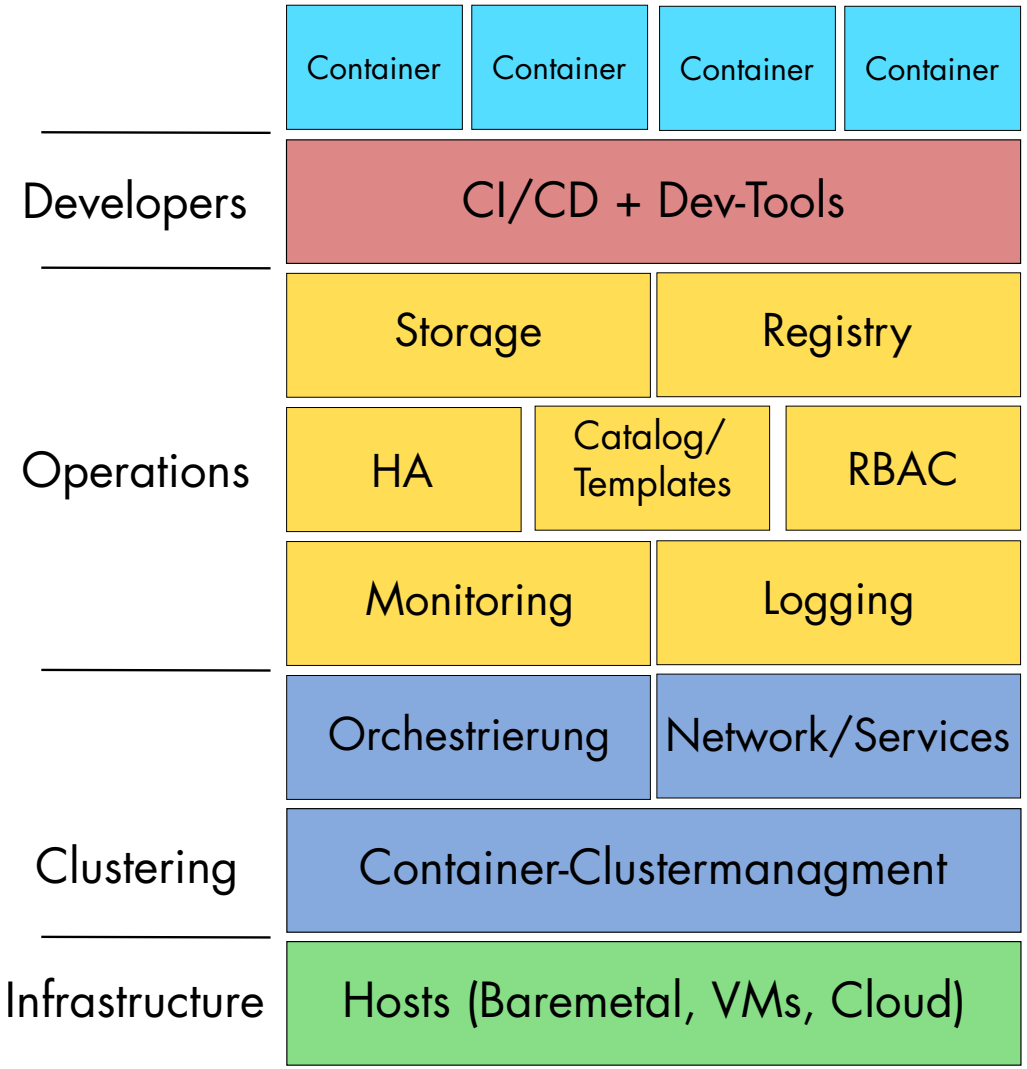
CI/CD

Automatisiertes Bauen, Testen und Ausrollen:

- Build über Webhooks
- Automatische Testläufe
- (Teil-)Automatisierung der Lifecycles
- Tools: z.B. Jenkins, Drone



Containerplattform

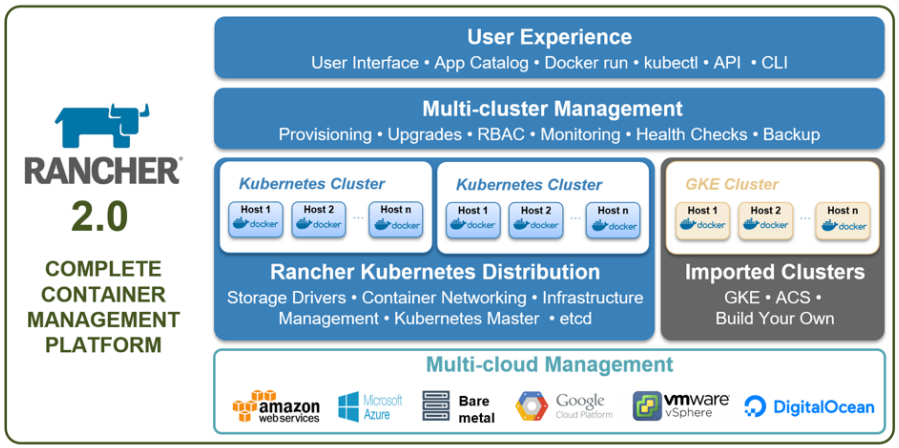


Rancher

RANCHER

Rancher 2.0 als Plattform:

- Großteil der Grundbausteine integriert
- Für 2.X geplant:
  - CI/CD mit Jenkins
  - integriertes Logging
  - Monitoring mit Prometheus
- Viele Features bereits in Rancher 1



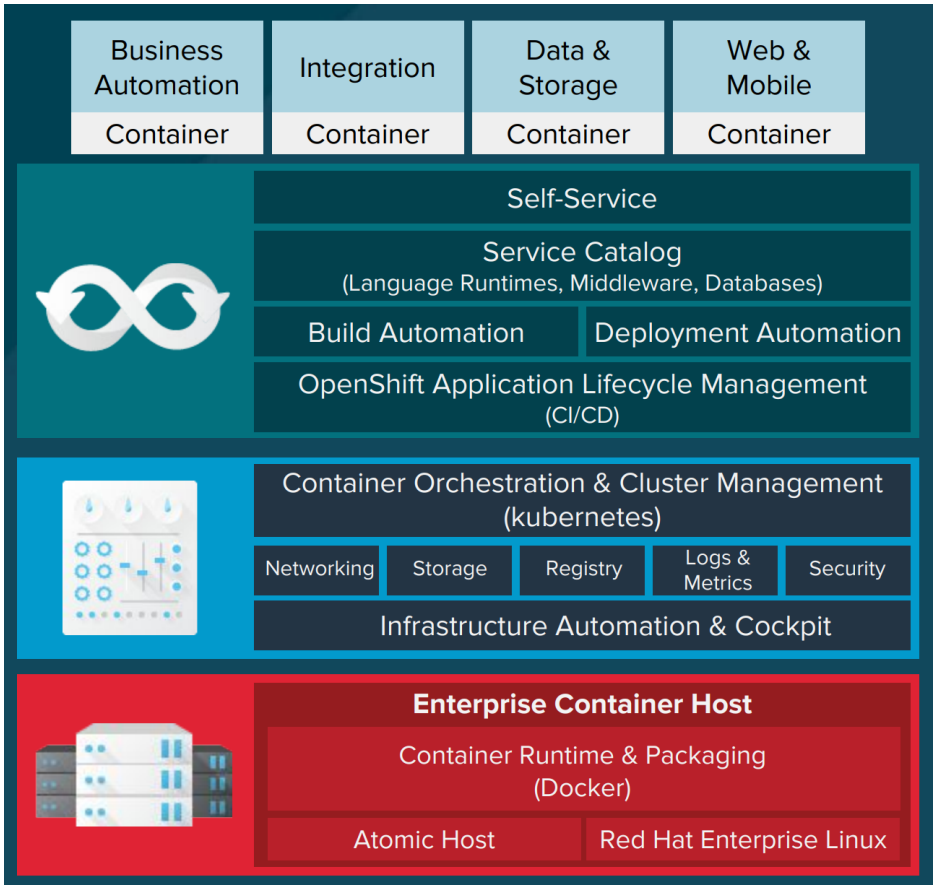
Quelle: Rancher

Openshift

OPENSHIFT

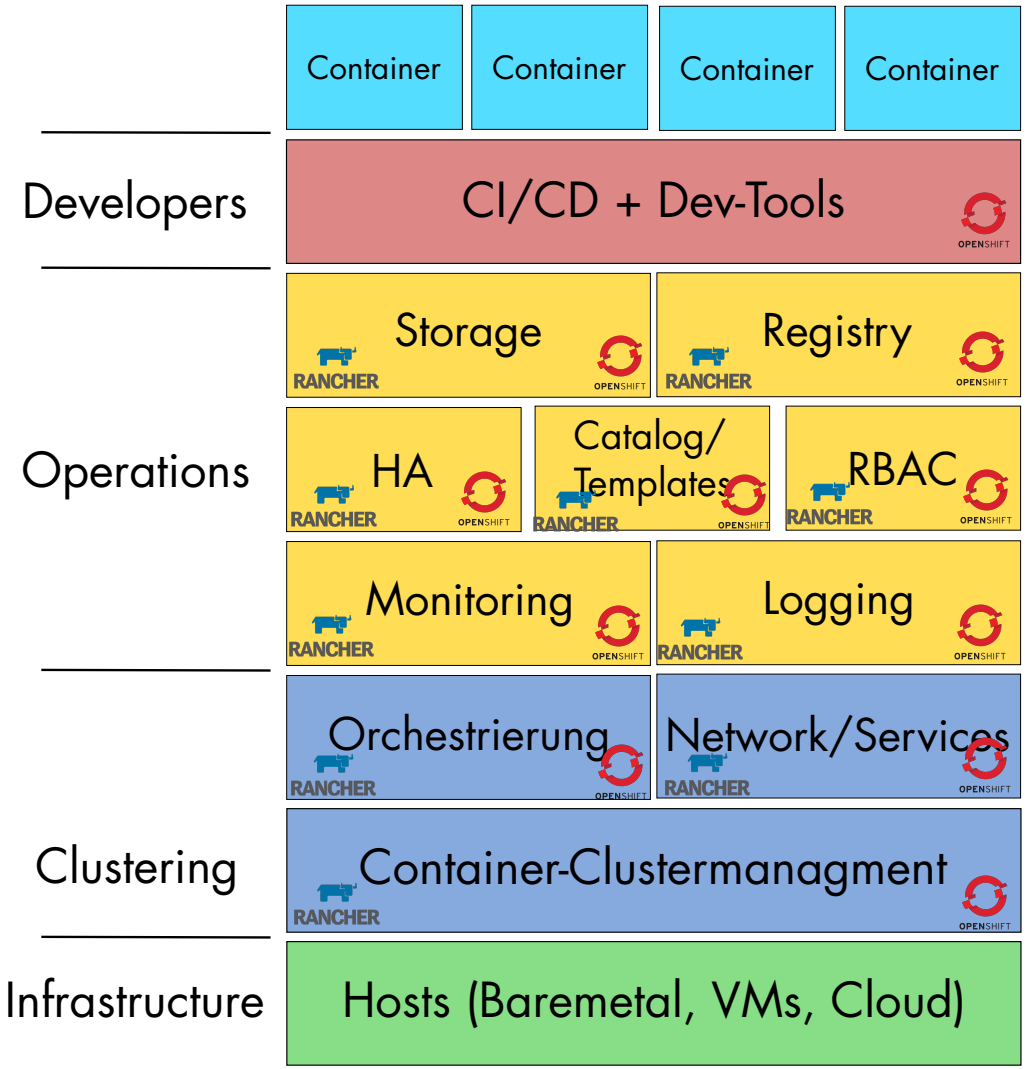
Red Hats Containerplattform:

- Alle Grundbausteine integriert
- Viele Entwicklertools, wie z.B.:
  - Source-to-Image Builds (S2I)
  - Integrierter Jenkins



Quelle: Red Hat

OpenShift 3.7 vs Rancher 2.0



Zusammenfassung

Aufbau einer Containerplattform:

- Bausteine in verschiedenen Varianten
- Einige Bausteine optional
- Planung um Anforderungen zu berücksichtigen

Viele Plattformen liefern schon viele Features mit:

- Rancher (2.0) - leicht aufzusetzen und zum ausprobieren
- OpenShift - sehr gute Developer-Tools integriert

⇒ Container-Plattformen sind erweiterbar und konfigurierbar

Kontakt

Dr. Jonas Trüstedt

XING: www.xing.com/profile/Jonas_Truestedt

LinkedIn: www.linkedin.com/in/jonas-truestedt

Mail: truestedt@atix.de