Compliant Kubernetes

Power-Team: Elastisys & Exoscale

Referenten

Cristian Klein **Daniel Tremmel**

Wir beginnen in Kürze

elastisys

EXOSCALE

Informationen rund um dieses Webinar

Dieses Webinar wird aufgezeichnet

Als Teilnehmer sind Sie stummgeschaltet. Fragen können Sie aber jederzeit über das Chatfenster stellen. Wir bemühen uns Ihre Fragen im Laufe des Webinars zu beantworten.

Im Nachgang erhalten Sie zeitnah

Das PDF der Präsentation

Die Fragen inkl. der Antworten

elastisys

EXOSCALE

Compliant Kubernetes

Power-Team: Elastisys & Exoscale

Referenten

Cristian Klein

Daniel Tremmel

elastisys

EXOSCALE

Unsere heutigen Themen

- Was ist "Cloud-Nativ" und warum wenden sich die meisten Unternehmen Containern und cloud-nativen Technologien zu?
- Wie sieht in der Regel eine Cloud-Native-Transformation aus?
- Cloud-Native-Ökosystem: Verschiedene Projekte der CNCF mit Schwerpunkt auf Kubernetes.
- Was sind die Herausforderungen beim Betrieb eines Cloud Native Stacks in Europa?
- Wie können Exoscale, A1 Digital Security, Elastisys, konforme Kubernetes und umgebende verwaltete native Cloud-Dienste diese Probleme lösen?

elastisys

EXOSCALE

Ihre Referenten:

Cristian Klein

Cristian ist ein Cloud-Native-Architekt bei Elastisys, promoviert in Cloud Computing und lehrt an der Universität Umeå, Schweden. Cristian verfügt über mehr als 9 Jahre Erfahrung auf dem Gebiet des Cloud Computing als Anwender, Lehrer und Forscher. Er leitete Cloud-Computing-Kurse, war Chief-Cloud-Architect, Führungskraft in einem Start-up-Unternehmen und arbeitete praktisch mit Kunden zusammen, um ihnen beizubringen, wie sie die Vorteile der nativen Cloud-Technologien nutzen können.

Daniel Tremmel

Daniel Tremmel verantwortet im Security-Department den Aufbau Entwicklung der Enterprise Security Architecture Consulting Services und ist maßgeblich am Produkt- und Lösungsbau im Bereich Cloud Security in der A1 Digital beteiligt. Durch seine langjährige Tätigkeit bei DAX30-Unternehmen bringt er viel Erfahrung in den Bereichen Network Infrastructure, Datacenter, Cloud Security und Managed Security Services mit. Zuletzt war Tremmel als Senior Consultant im DACH-Raum für die Beratung und die Implementierung von Security-Produkten tätig.

elastisys

EXOSCALE

Eine neue IT-Landschaft

Warum brauchen wir Cloud Native Development?

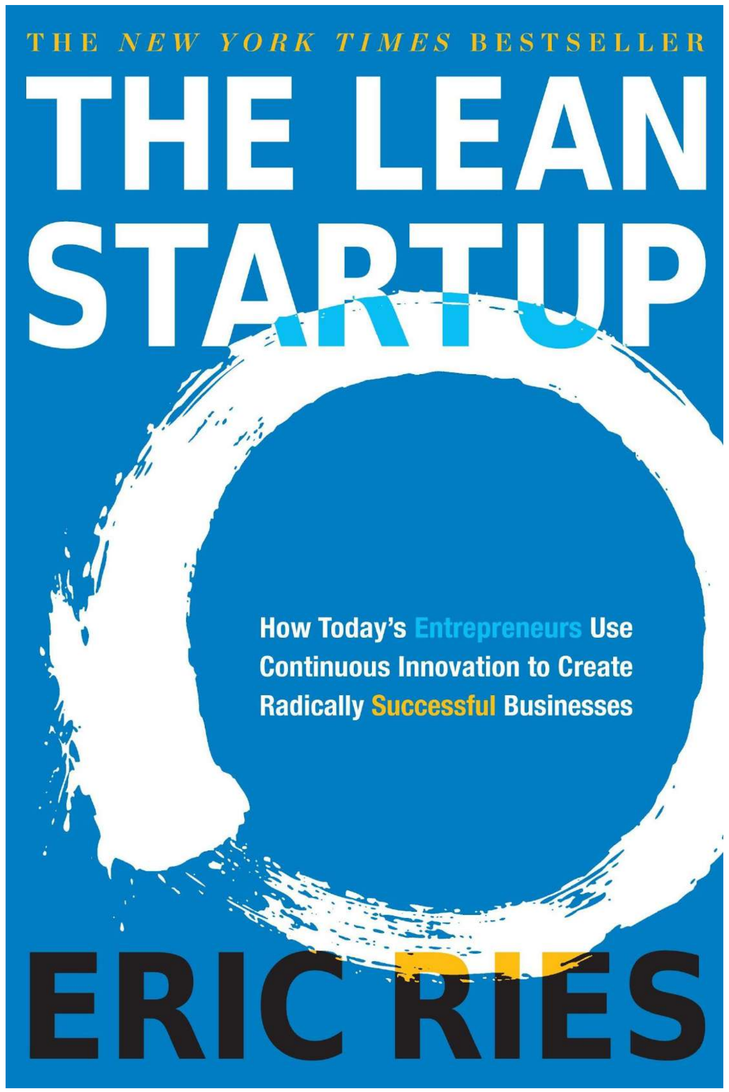
Quiz: Nehmen wir eine SaaS-Lösung

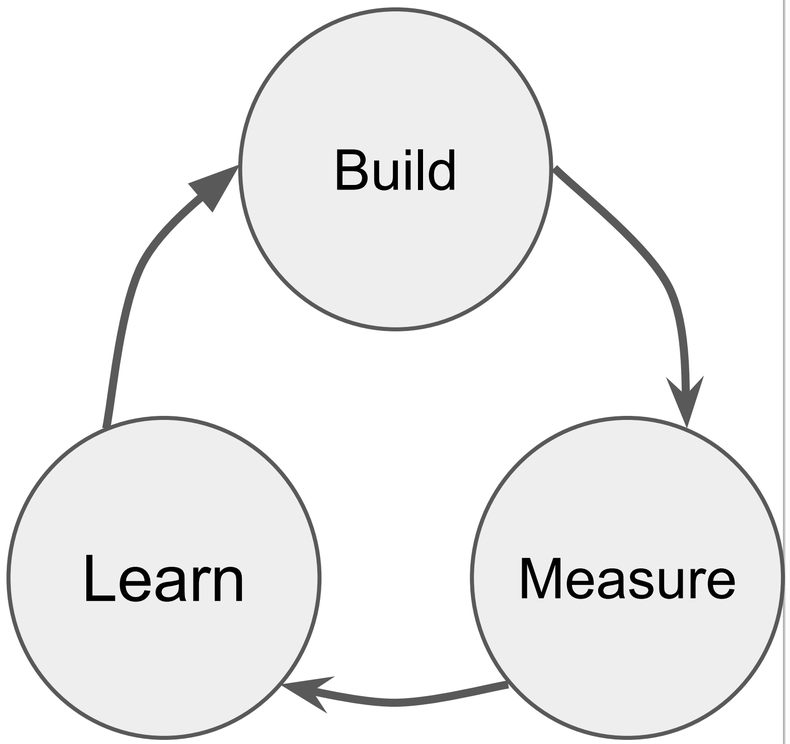
Q: Welche Version verwenden Sie?

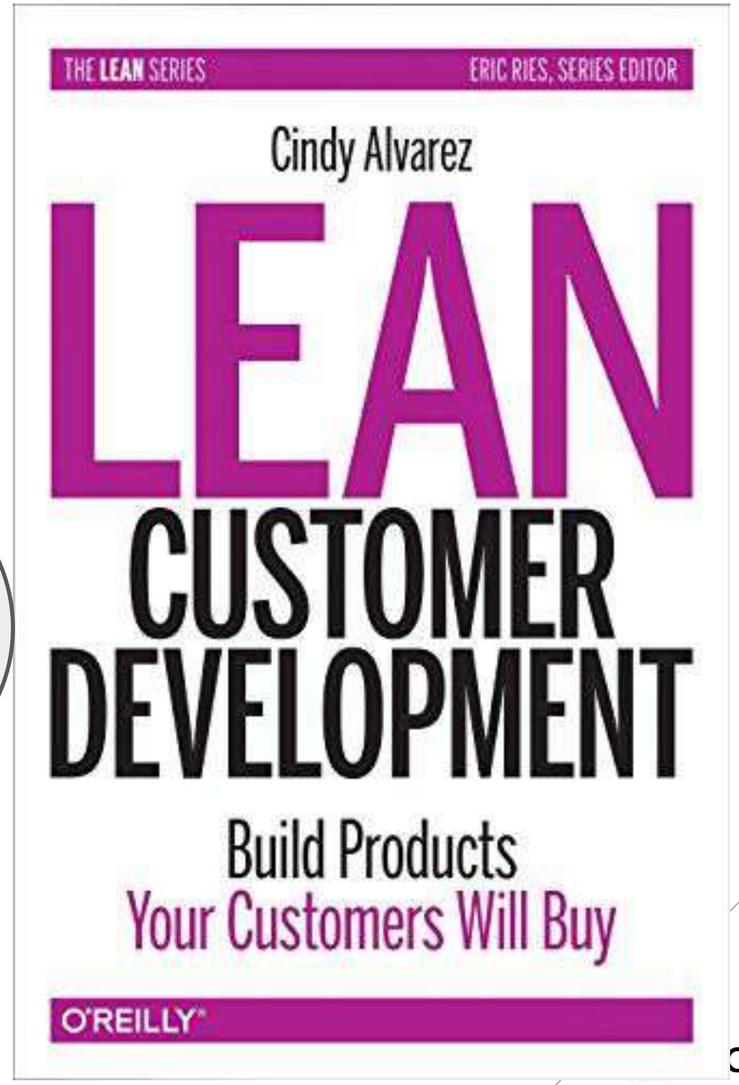
A: Ca.10 Mal täglich wird eine neue Office 365-Version veröffentlicht.

Mehrere Veröffentlichungen wöchentlich ist das “neue Normal”

Warum? **Lean** thinking



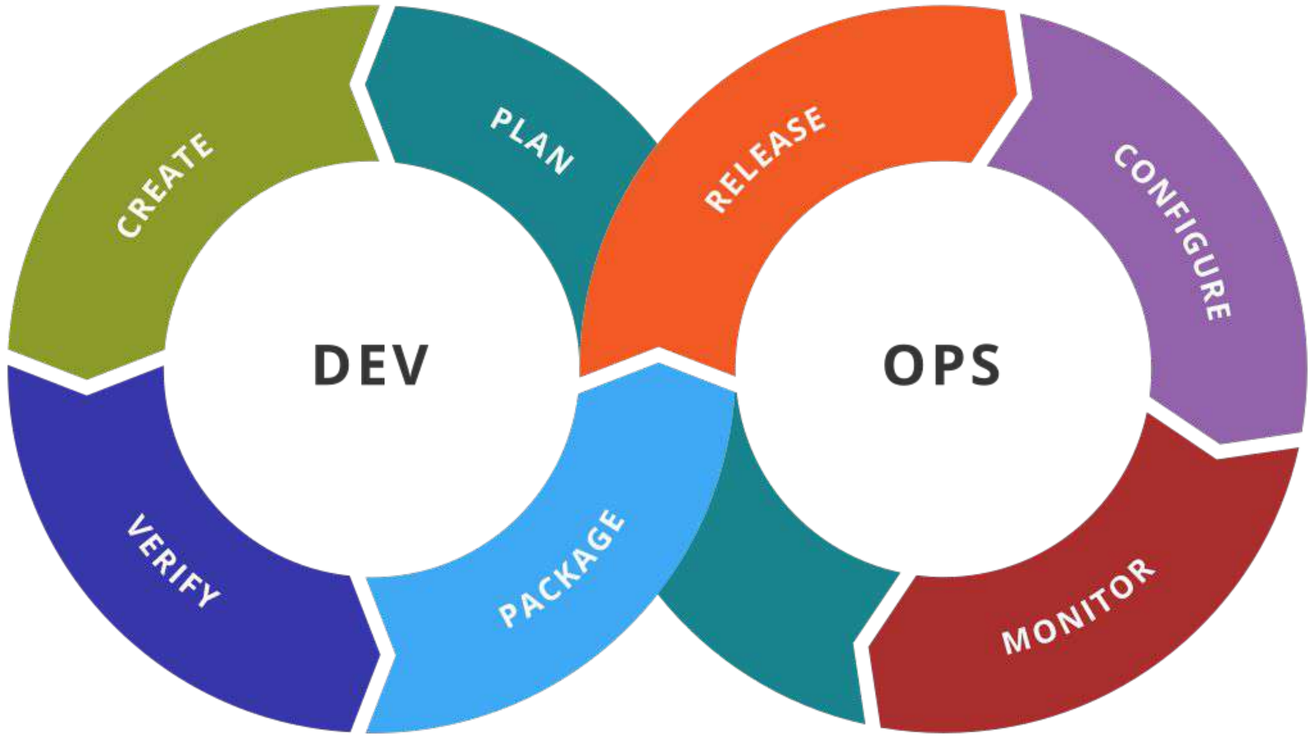




elastisys

OSCALE

Wie kommen Sie dorthin?
Ein kultureller Wandel



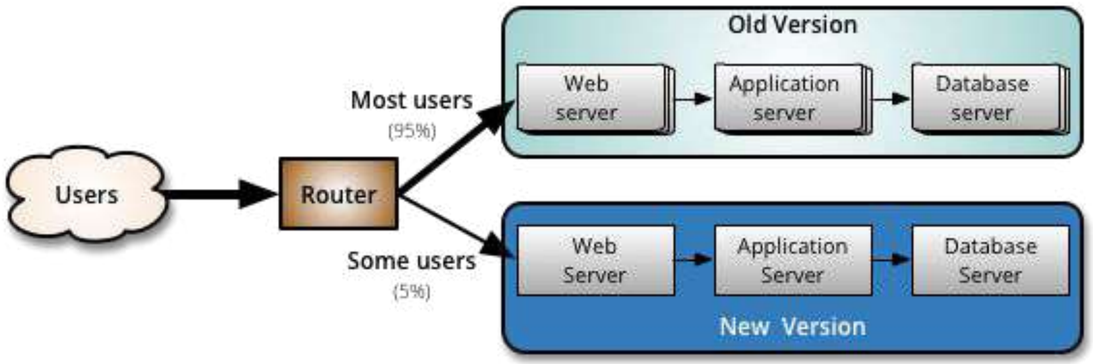
https://commons.wikimedia.org/wiki/File:Devops-toolchain.svg

elastisys

EXOSCALE

Softwarelieferung im 21. Jahrhundert

- Softwarelieferung = **ein konstanter Strom kleiner Änderungen**
- Marketing Release ≠ Software Release
  - Feature-Flags verwenden
- Lieferung **automatisieren** und so risikofrei wie möglich gestalten
  - Pre-Integration Testing
  - Canary Releases
  - Blue-green Deployments
- **Auswirkungen beobachten**
  - Im Zweifelsfall, **rollback**
- Single Version Software
  - Reduziert die Betriebskosten



elastisys

EXOSCALE

Anforderung von Cloud Applikationen

- **Schnell und einfach zu entwickeln**
  - Einsatz mehrmals täglich
- Hohe Betriebszeit (>99,95%)
  - Wann haben Sie eine "Website ist wegen Wartung außer Betrieb" gesehen?
- Skalierbar
  - Die Anwendung "wächst" mit der Last (z.B. Anzahl der Benutzer)
- Stabil und ausfallsicher
  - Server und Netzwerke können ausfallen, die Anwendungen darauf dürfen es nicht
- Sicher und konform **(Details in Webinar Teil 2)**

Cloud Native

Was ist Cloud Native?

Was ist die Cloud Native Computing Foundation?

What is Cloud Native?

Native Cloud-Technologien ermöglichen es Unternehmen, skalierbare Anwendungen in modernen, dynamischen Umgebungen wie **öffentlichen, privaten und hybriden** Clouds zu erstellen und auszuführen. [...] Diese Techniken ermöglichen lose gekoppelte Systeme, die belastbar, verwaltbar und beobachtbar sind. In Kombination mit einer robusten Automatisierung ermöglichen sie es den Technikern, **häufig** und **vorhersehbar kritische Änderungen** mit **minimalem Arbeitsaufwand** vorzunehmen.

CLOUD NATIVE
COMPUTING FOUNDATION

part of THE LINUX FOUNDATION

Aufbau eines nachhaltigen **Ökosystems** für Cloud Native Software

Die Cloud Native Computing Foundation (CNCF) beherbergt kritische Komponenten der globalen Technologieinfrastruktur. Die CNCF bringt die weltbesten **Entwickler, Endbenutzer und Anbieter** zusammen und veranstaltet die größten Open-Source-Entwicklerkonferenzen.

CNCF Members

Platin: 19

Gold: 21

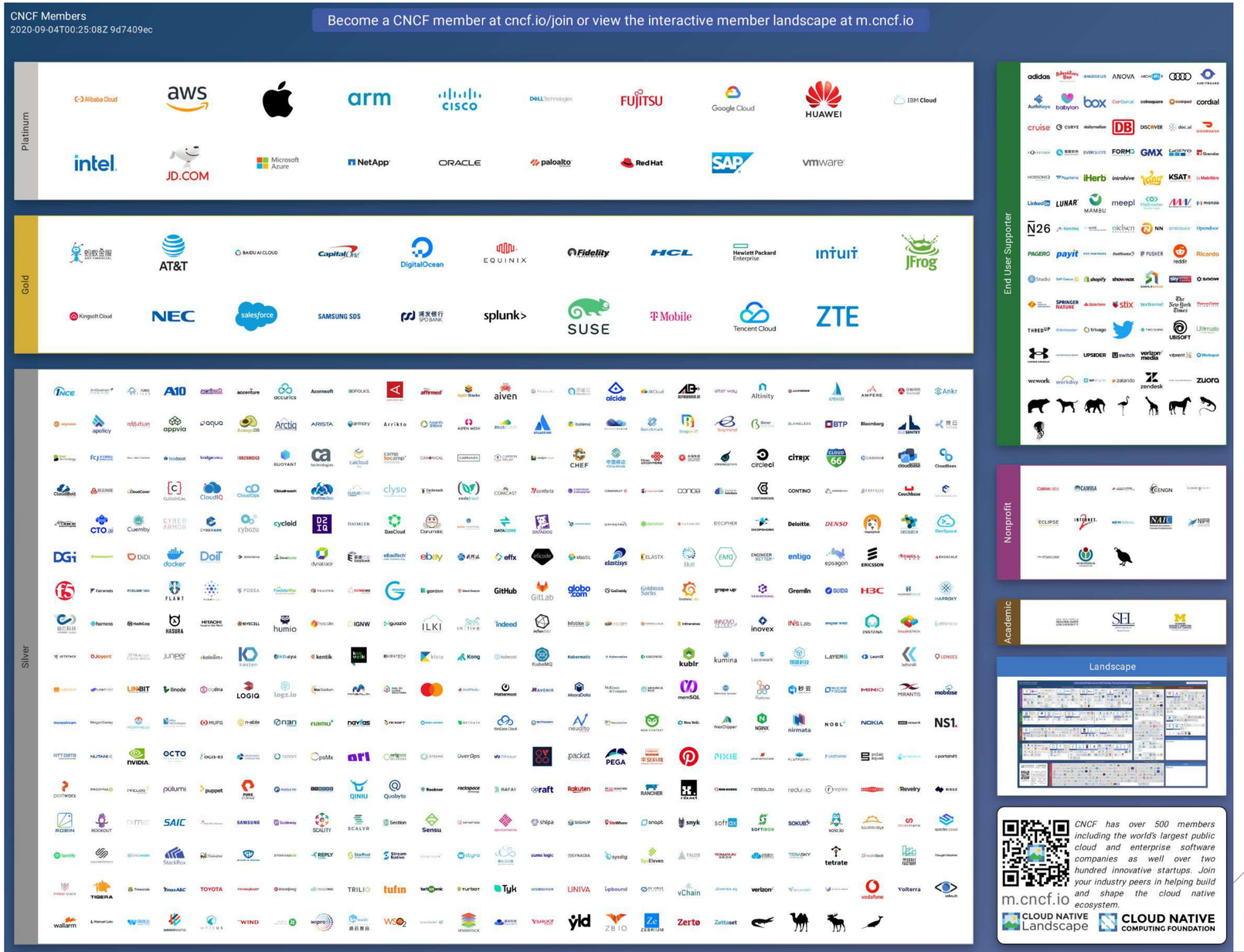
Silber: 423

Akademisch: 3

Gemeinnützig: 13

Endnutzer: 99

Summe: 578



elastisys

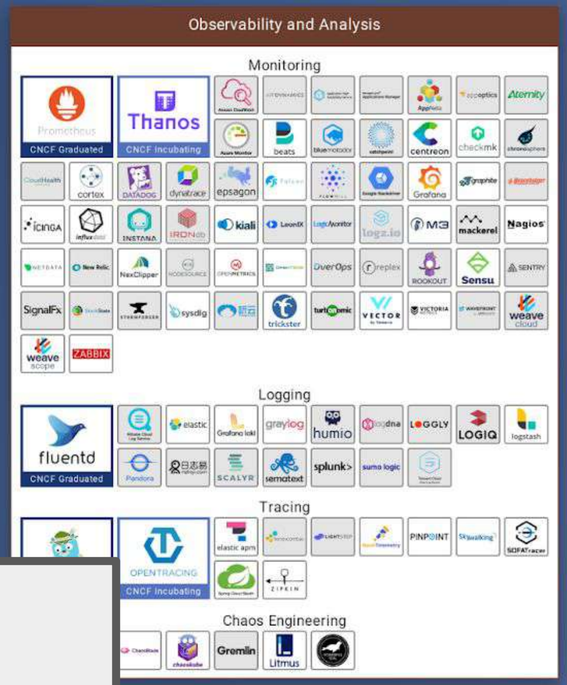
EXOSCALE

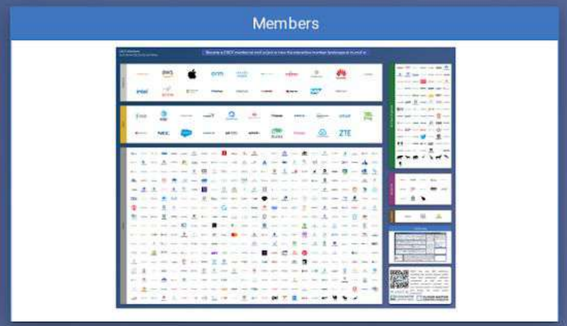
CNCF Cloud Native Landscape
2020-09-04T00:25:08Z 9d7409ec

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Greyed logos are not open source

1473 Projekte und mehr





CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint Amplify

l.cncf.io

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

CLOUD NATIVE
COMPUTING FOUNDATION

CLOUD NATIVE TRAIL MAP

The Cloud Native Landscape *l.cncf.io* has a large number of options. This Cloud Native Trail Map is a recommended process for leveraging open source, cloud native technologies. At each step, you can choose a vendor-supported offering or do it yourself, and everything after step #3 is optional based on your circumstances.

HELP ALONG THE WAY

A. Training and Certification

Consider training offerings from CNCF and then take the exam to become a Certified Kubernetes Administrator or a Certified Kubernetes Application Developer

cncf.io/training

B. Consulting Help

If you want assistance with Kubernetes and the surrounding ecosystem, consider leveraging a Kubernetes Certified Service Provider

cncf.io/kcsp

1. CONTAINERIZATION

- Commonly done with Docker containers
- Any size application and dependencies (even PDP-11 code running on an emulator) can be containerized
- Over time, you should aspire towards splitting suitable applications and writing future functionality as microservices

2. CI/CD

- Setup Continuous Integration/Continuous Delivery (CI/CD) so that changes to your source code automatically result in a new container being built, tested, and deployed to staging and eventually, perhaps, to production
- Setup automated rollouts, roll backs and testing
- Argo is a set of Kubernetes-native tools for deploying and running jobs, applications, workflows, and events using GitOps paradigms such as continuous and progressive delivery and MLops

argo
CNCF Incubating

3. ORCHESTRATION & APPLICATION DEFINITION

- Kubernetes is the market-leading orchestration solution
- You should select a Certified Kubernetes Distribution, Hosted Platform, or Installer: cncf.io/ck
- Helm Charts help you define, install, and upgrade even the most complex Kubernetes application

kubernetes
CNCF Graduated

HELM
CNCF Graduated

4. OBSERVABILITY & ANALYSIS

- Pick solutions for monitoring, logging and tracing
- Consider CNCF projects Prometheus for monitoring, Fluentd for logging and Jaeger for Tracing
- For tracing, look for an OpenTracing-compatible implementation like Jaeger

Prometheus
CNCF Graduated

fluentd
CNCF Graduated

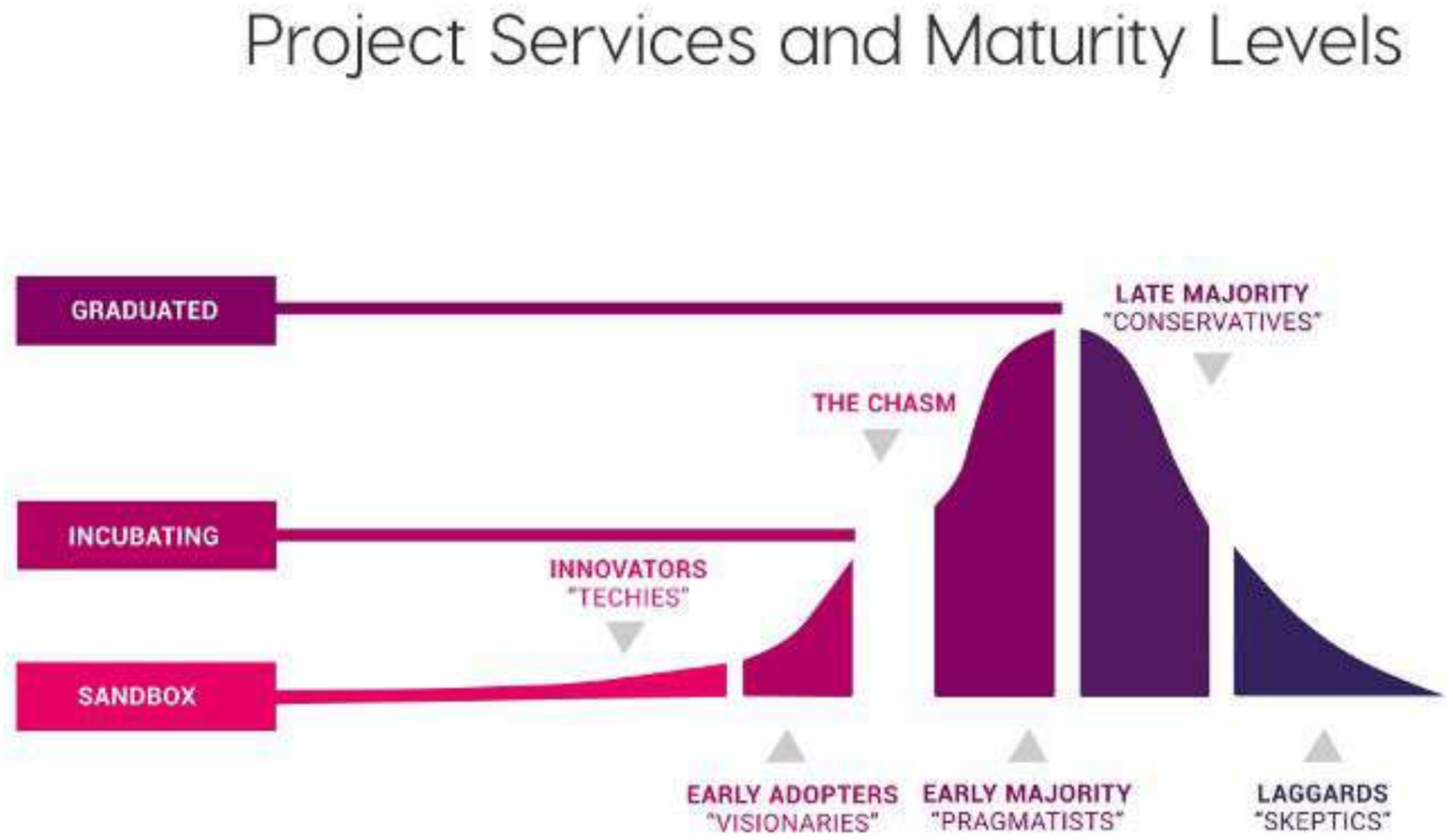
JAEGER
CNCF Graduated

OPENTRACING
CNCF Incubating

5. SERVICE PROXY, DISCOVERY, & MESH

- CoreDNS is a fast and flexible tool that is useful for service discovery
- Envoy and Linkerd each enable service mesh architectures
- They offer health checking, routing,

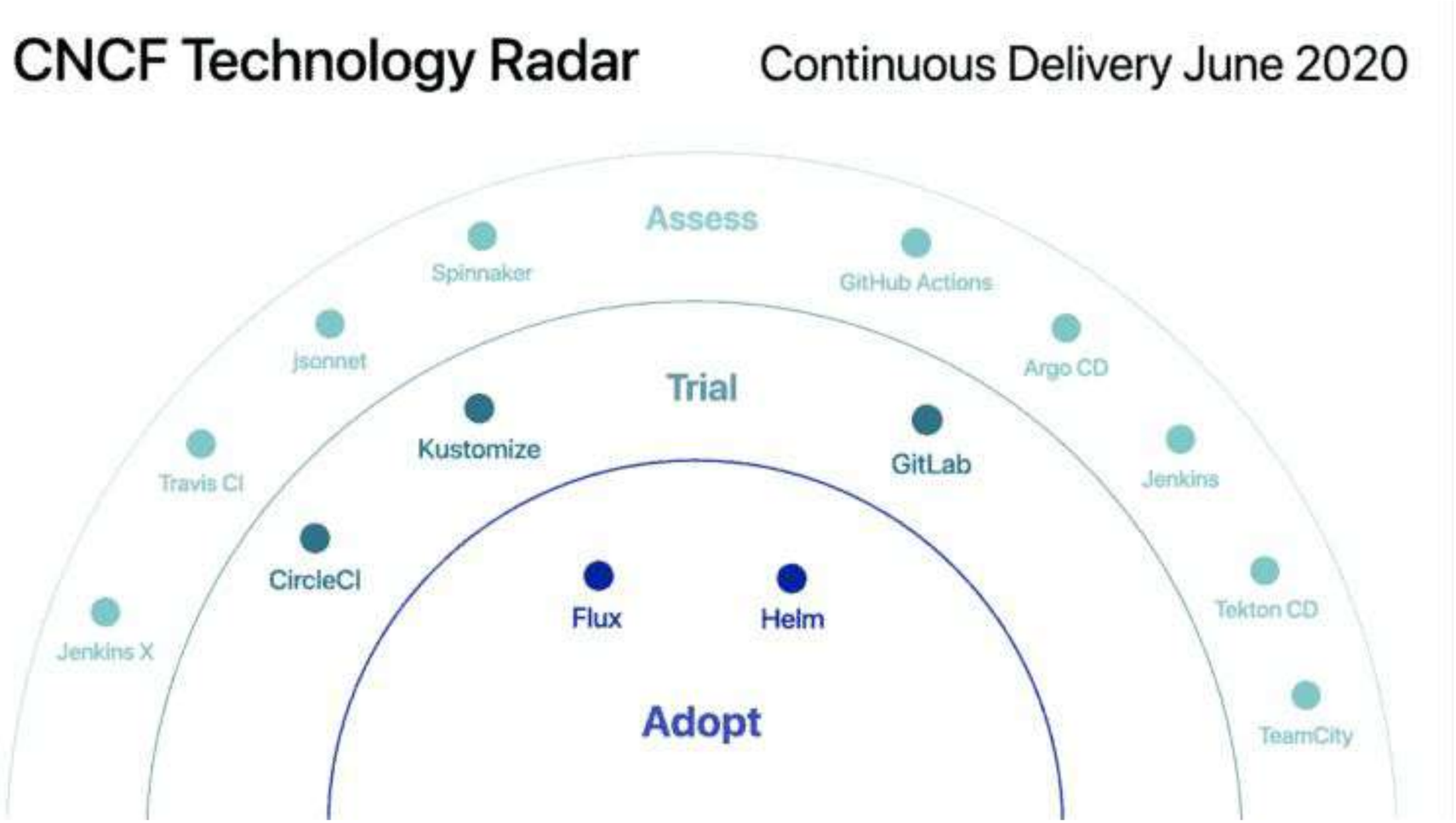
CNCF: Project Maturity Levels



elastisys

EXOSCALE

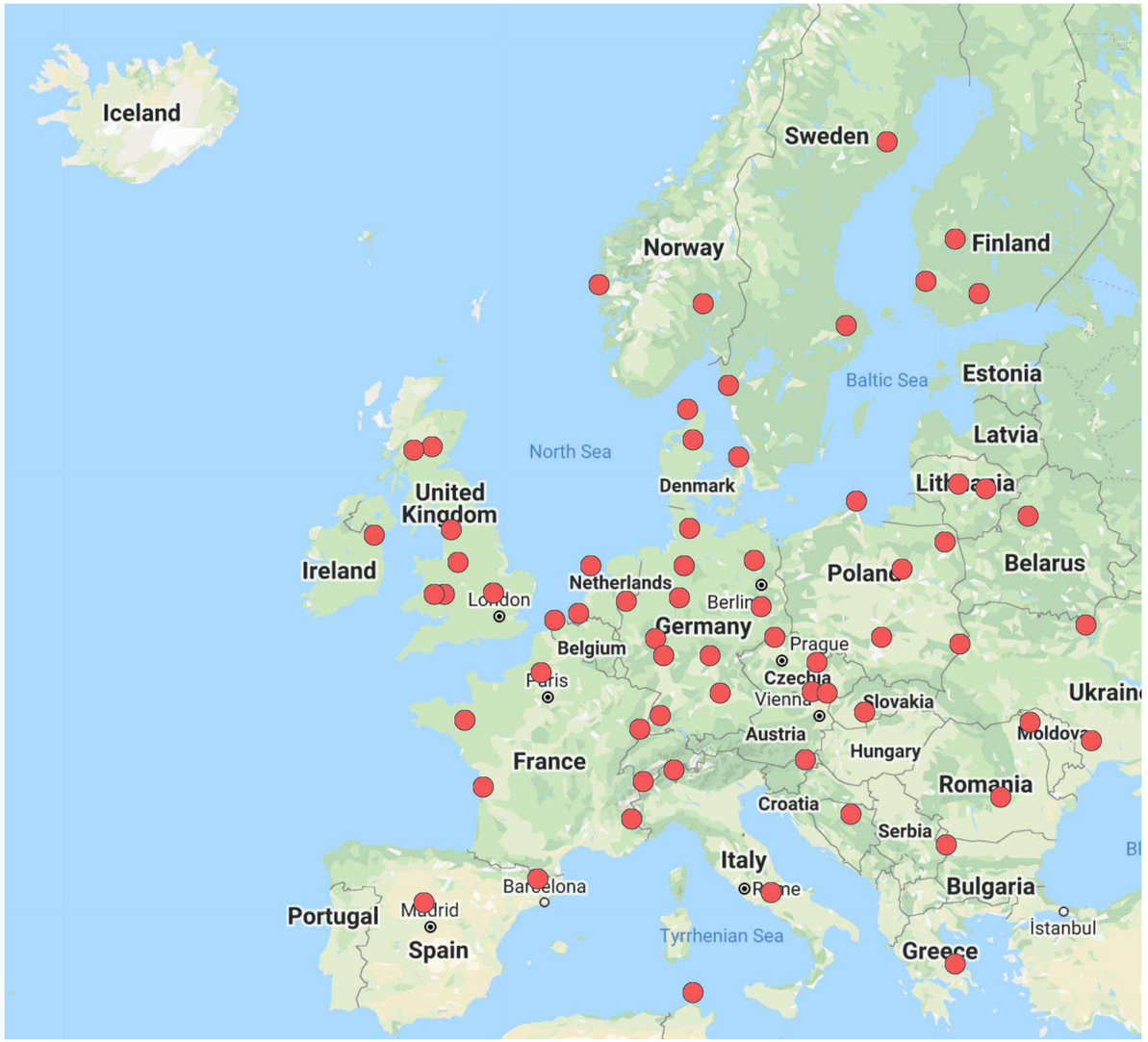
CNCF: End-user Perspective



elastisys

EXOSCALE

Cloud Native Meetups: Hilfe steht vor der Tür



https://www.meetup.com/pro/cncf/

elastisys

EXOSCALE

Zuverlässiger Bereitstellung

Wie stellt man eine zuverlässige Auslieferung sicher?

Wie stellt man eine zuverlässige Auslieferung sicher?

Software-Komponenten **reproduzierbar** bauen

Komponenten auf reproduzierbare Weise **zusammenbauen**

kubernetes

Infrastruktur auf reproduzierbare Weise bauen

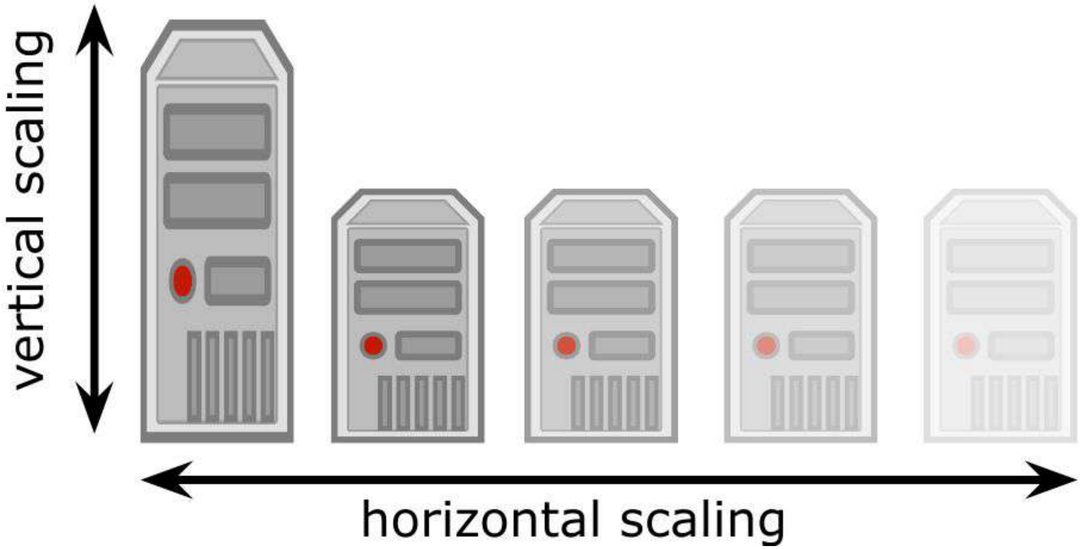
Die obigen Schritte **verbinden**

Container-Orchestrierung

Wie können Container auf mehreren Servern betrieben werden?

Warum mehrere Server?

- Horizontale Skalierbarkeit



- Verschiedene Node-Typen (z.B. High-Mem vs. SSD, GPUs usw.)
- Redundanz, sogar Multi-AZ-Redundanz

elastisys

EXOSCALE

Herausforderungen mit mehreren Servern

Absolutes Minimum:

- **Vernetzung:** Wie sollen Container einander erreichen?
- **Ressourcenplanung:** Auf welchem Server soll ich welche Container laufen lassen?
- **Service Discovery:** Wie kann ich das andere Container und das Backend erreichen?
- **Load-Balancing**: Was ist, wenn mehrere Container den Service X bereitstellen?
- **Ingress**: Wie gelangt der Traffic in den Cluster?
- Selbstheilend? Speicherplatz? Konfigurationsmanagement?

- Führen Sie Ihre eigene Lösung ein oder verwenden Sie eine bewährte und produktionsreife Lösung?

kubernetes

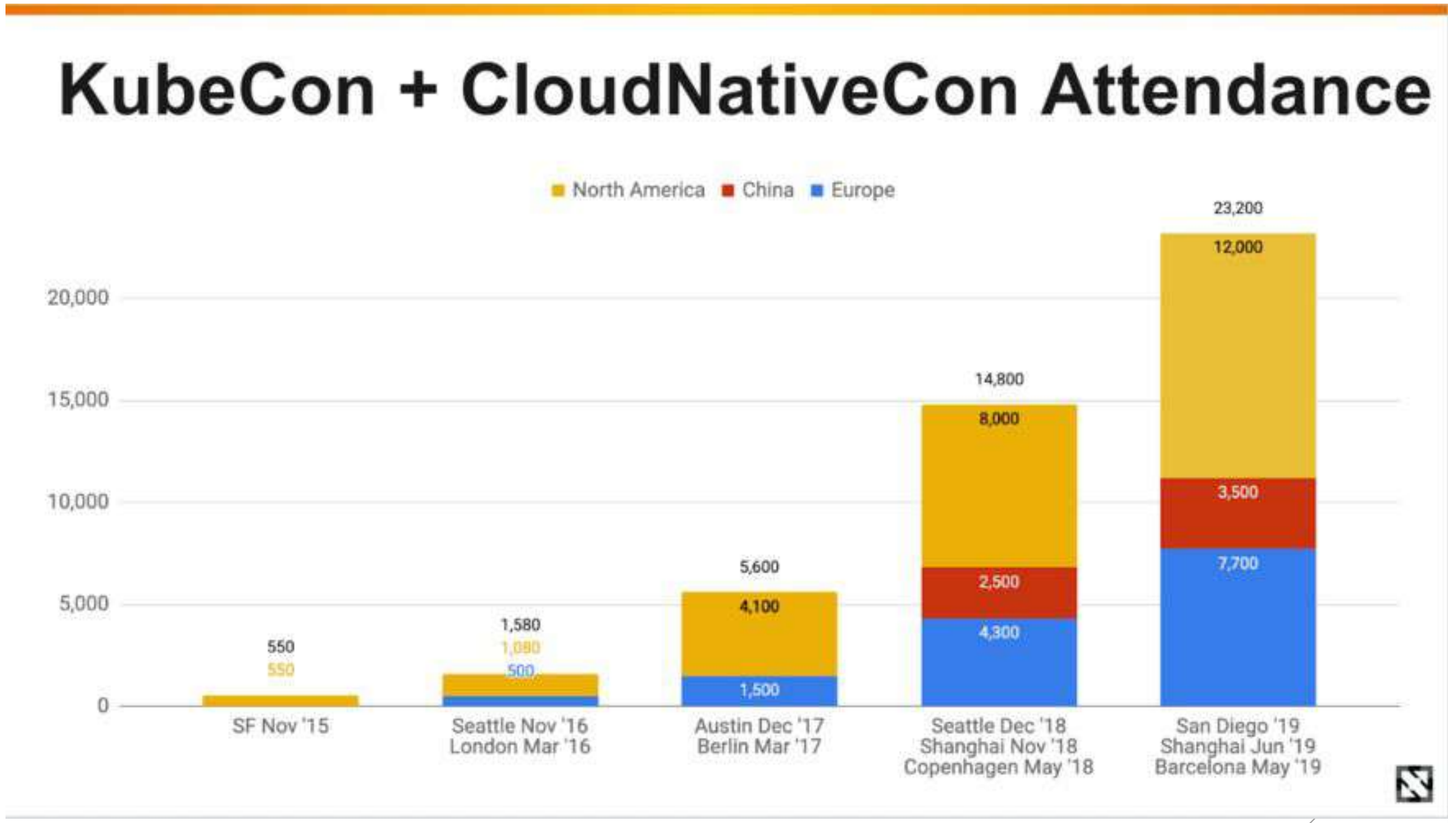
Kubernetes ist eine portable, erweiterbare Open-Source-Plattform zur Verwaltung **containerisierter Anwendungen und Dienste**, die sowohl die **deklarative Konfiguration** als auch die **Automatisierung** erleichtert. Sie verfügt über ein großes, schnell wachsendes **Ökosystem.** Kubernetes-Dienste, -Support und -Tools sind breitflächig verfügbar.

elastisys

EXOSCALE

Kubernetes: Geschichte, Adoption

- 2015: v1.0 Release
  - Basierend auf Erfahrungen mit der Verwaltung von Arbeitslasten bei Google (Borg)
  - gesetzt in der Cloud Native Computing Foundation (CNCF), Teil der Linux Foundation
- 2018: 9. Platz in der Anzahl der GitHub Code Updates (“commits”)



Source: CNCF

elastisys

EXOSCALE

Was macht Kubernetes?

- Service discovery and load balancing
- Storage orchestration
- Automated rollouts and rollbacks
- Automatic bin packing (i.e., scheduling)
- Self-healing
- Secret and configuration management

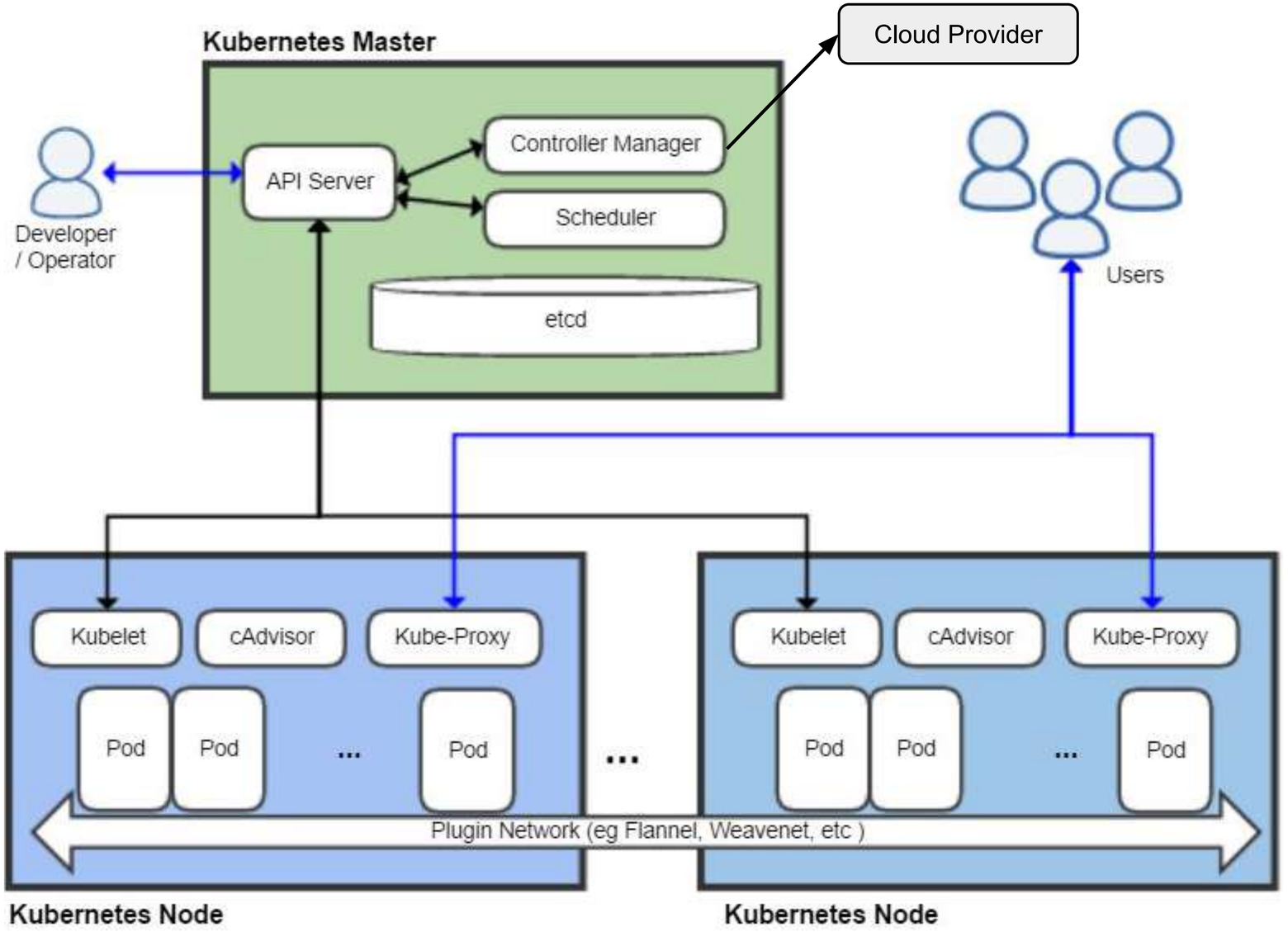
Interaktion mit Kubernetes

- Eine Reihe von **Controllern**
- Benutzer erstellt Ressourcen und legt **Spezifikationen** fest
- Controller gleicht Ressourcen ab und setzt **Status**
- **Deklarativ,** nicht imperativ

Ressourcen

- Ressourcen können sein: im **Namespace** oder Cluster-weit
- **Node**: Ein Server oder eine VM, auf dem/der Container laufen können
- **Pod**: Eine Gruppe von Containern, die **als Einheit agieren**
  - Pods teilen sich den **Lebenszyklus** und das **Netzwerk** und ggf. den **Speicherplatz**
- **Deployment:** Ein Satz homogener Pods
- **Service**: Eine Menge von Containern, die als Netzwerkdienst (z.B. DNS-Name) bereitgestellt werden
- **Ingress**: Eine Möglichkeit für den Netzwerkverkehr, in den Cluster zu gelangen

Kubernetes Architecture



Source: Wikipedia

elastisys

EXOSCALE

Wie betreibt man Kubernetes?

- Lokale Entwicklung: minikube, K3s, KIND
- DIY: kubeadm, kubespray, Rancher
- Hosted (USA): Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE)
- Hosted EU: Compliant Kubernetes auf Exoscale

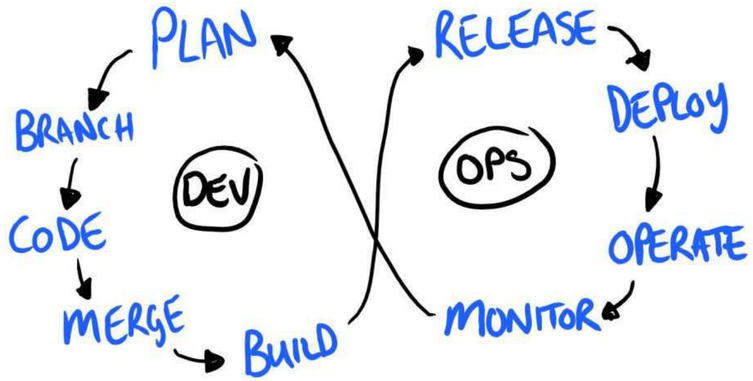
EXOSCALE

Beobachtungsmöglichkeit

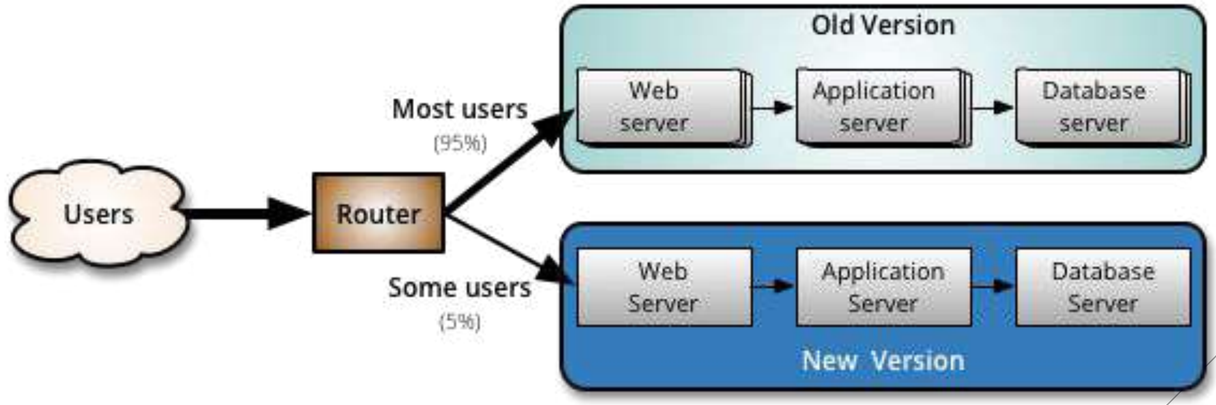
Wie geht es meiner Anwendung heute?

Warum Überwachung?

- Schließen der DevOps-Schleife
- Beobachten Sie die Auswirkungen einer Änderung



- Geht es der Infrastruktur gut?
- Geht es der Anwendung gut?
- Sind die Benutzer zufrieden?
  - z.B. Kreditkarten-Transaktionen
  - **Sehr geschäftsspezifisch**

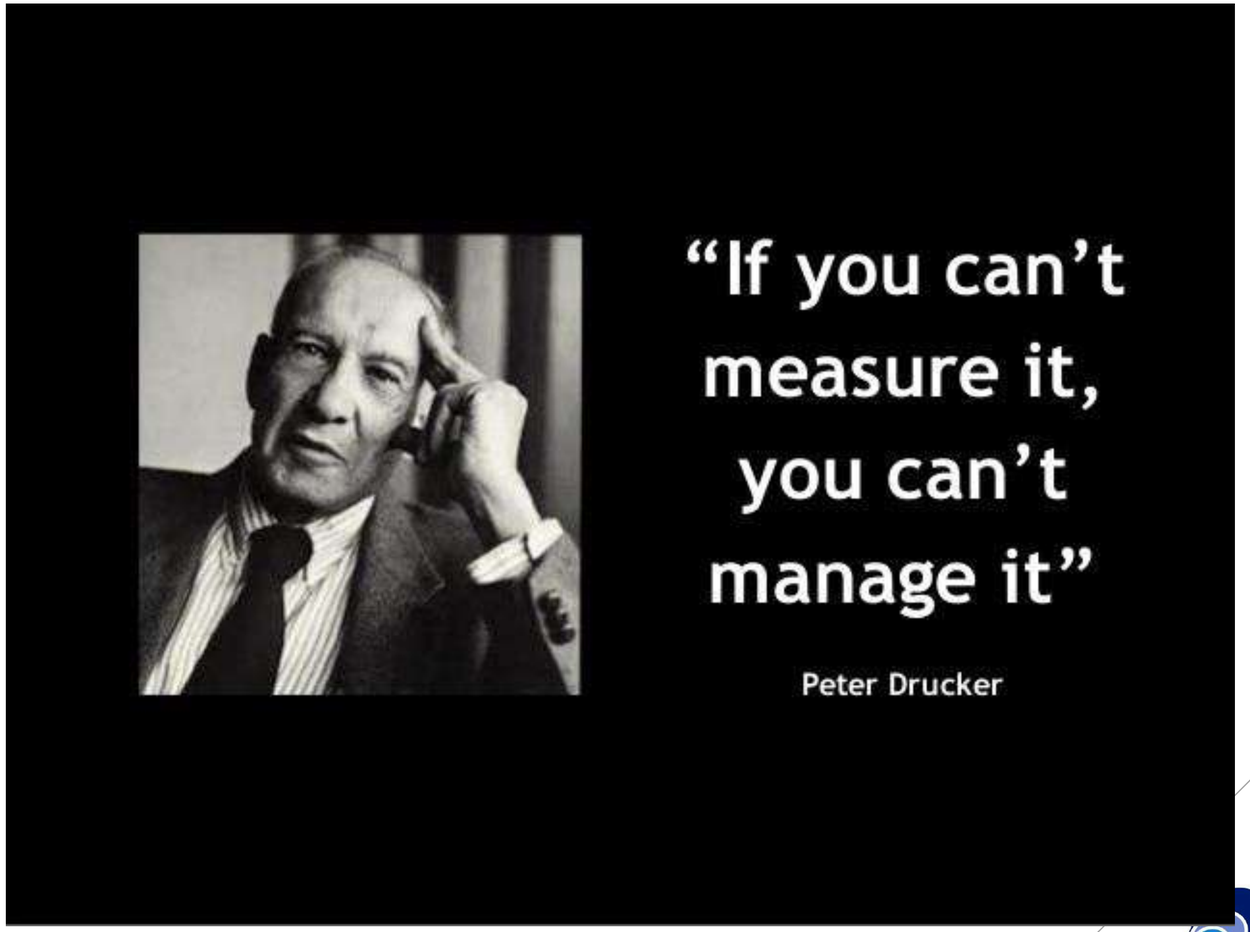


elastisys

EXOSCALE

Telemetry

Telemetrie ist die Sammlung von Messungen oder anderen Daten an entfernten oder unzugänglichen Punkten und ihre automatische Übertragung an Empfangsgeräte zur Überwachung.



Dutch government report says Microsoft Office telemetry collection breaks GDPR

Microsoft pledges to address issues; has already released a "zero exhaust" Office telemetry setting.

elastisys

EXOSCALE

Geschmacksrichtungen der Software-Telemetrie

(Traces)

Logs

Metriken

mehr Daten, aber wirklich mehr Information?

Alle Daten:

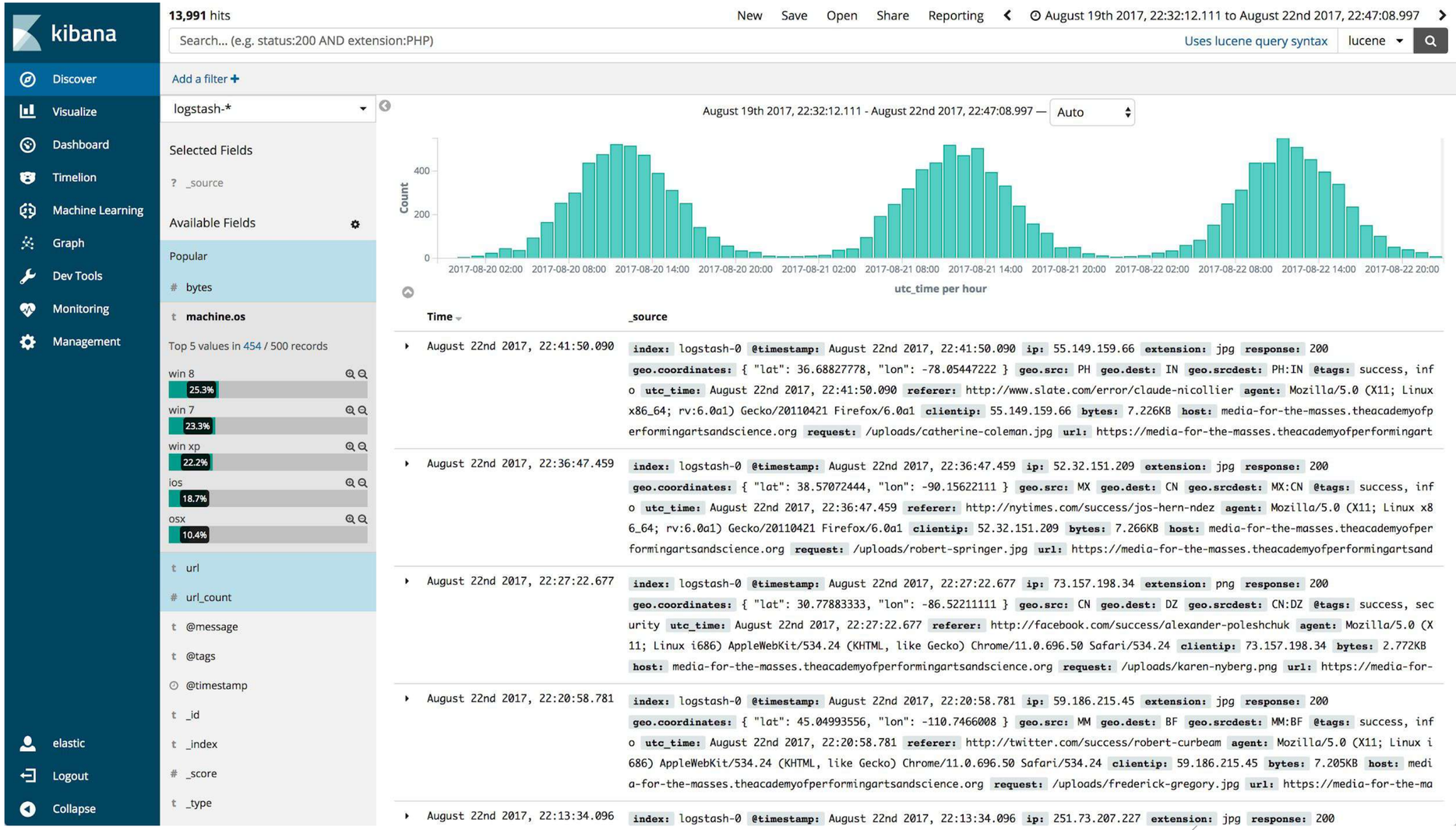
- nahezu in Echtzeit
- Aufbewahrungsfrist

Logs

Granularität?

Anwendungsbereich?

Kosten?



Metriken

- zeitbasiert
- explizit
- Günstig und aufschlussreich

Prometheus

Grafana

elastisys

EXOSCALE

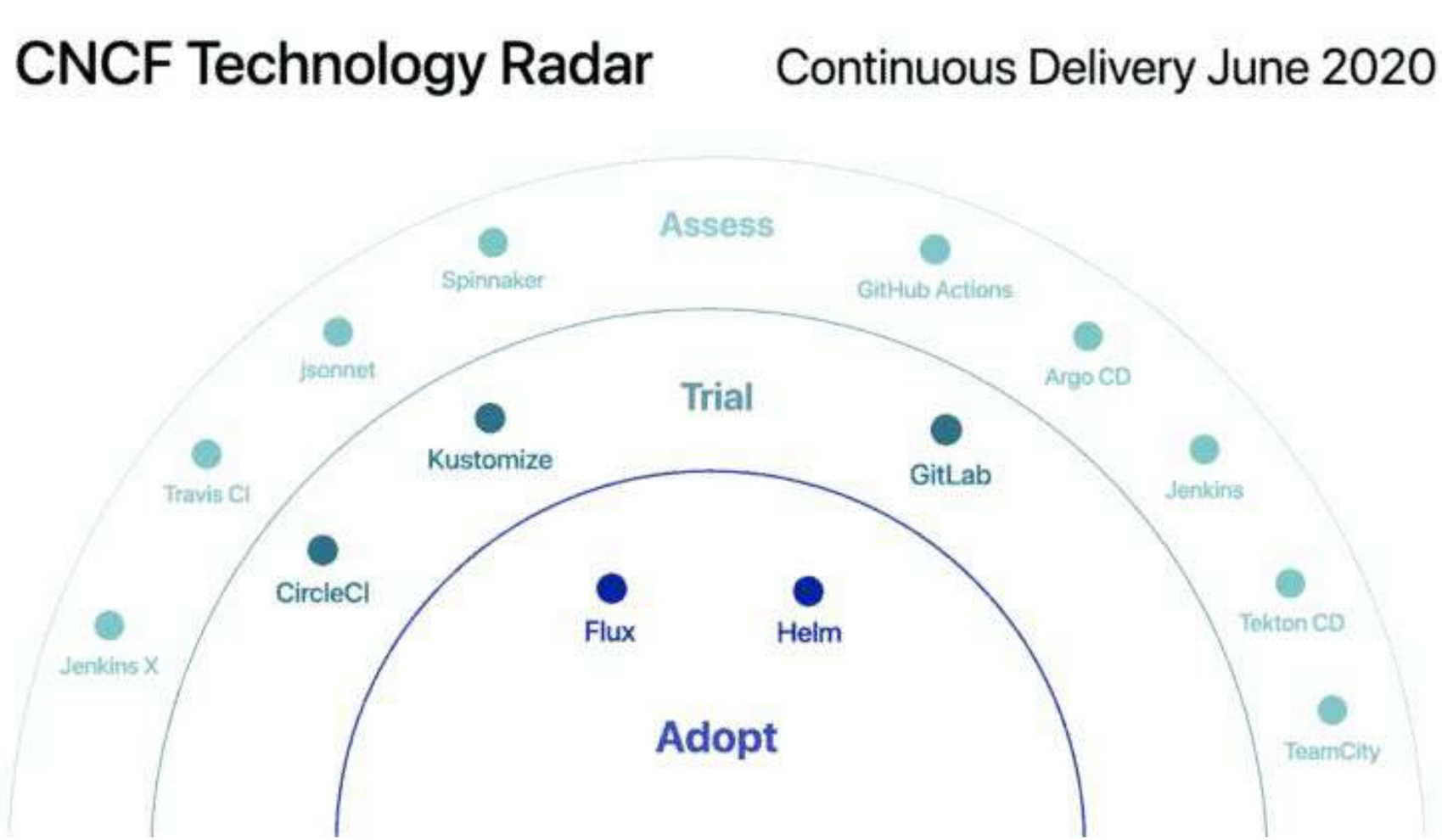
Was ist GitOps?

- Alle Systemänderungen über Git vornehmen

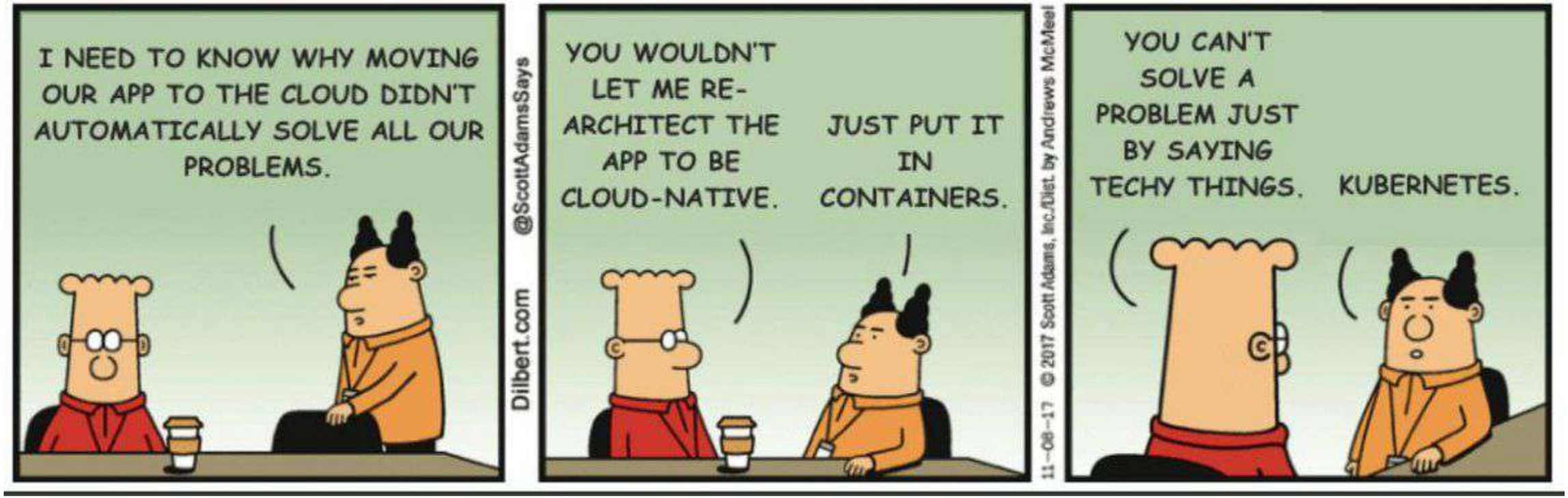
Warum?

- Klarer Prozess für das Änderungsmanagement
- Kostenloses Audit-Protokoll
- Änderungen können überprüft, genehmigt, abgelehnt, getestet usw. werden.
  - Neuer Trend: Wegwerf-Cluster
- Änderungen können vorsichtig ausgerollt werden

Flux und Helm



Fallstricke bei Kubernetes



elastisys

EXOSCALE

Zusammenfassung

- Anforderungen für Cloud-Anwendungen:
  - Schnell entwicklungsfähig, hohe Verfügbarkeit, skalierbar, belastbar
  - Sicher und konform
- Cloud native ecosystem
  - Ideen und Bausteine, um obige Anforderungen zu Erfüllen
  - Kubernetes als Zentrum der Transformation
- Überwachung nicht vergessen!

- Kubernetes: "Nicht standardmäßig sicher, auch nicht von sich aus"
  - Compliant Kubernetes: ISO-27001, GDPR, PCI-DSS, PDL
  - **Unsere eigenen Erfahrungen bei Kubernetes in stark regulierte Branchen!**
  - **Inkl. Demo!**

elastisys

EXOSCALE

Compliant Kubernetes

Power-Team: Elastisys & Exoscale

Q&A - Fragerunde

elastisys

EXOSCALE

Compliant Kubernetes

Power-Team: Elastisys & Exoscale

Vielen Dank für Ihre Aufmerksamkeit!

elastisys

EXOSCALE