metal-stack & SAP Gardener

Kubernetes im eigenen Rechenzentrum

Christian Brunner, Abteilung Cloud-Native, 6.10.2021

Wer ist FI-TS

| Anbieter für standardisierte, flexibel gestaltbare Serviceleistungen mit spezifischem Prozess-Know-how für Banken und Versicherungen

| Auf Erfolgskurs seit 1994

| Fünf Mitarbeiter-Standorte, zwei Rechenzentrums-Standorte mit jeweils zwei Rechenzentren

| Über 1.000 Mitarbeiterinnen und Mitarbeiter

400 Mio.
Umsatz

finanz **informatik**
technologie service

FI-TS betreut 6 der 13 von BaFin und EBA als systemrelevant eingestuften Institute* in Deutschland. Mit unserer Expertise sind wir einzigartig.

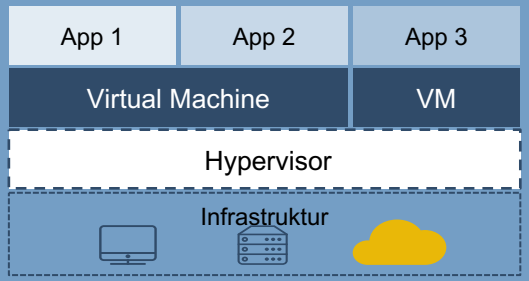
*BaFin 2020

finanz informatik technologie service

FI-TS Cloud Strategie

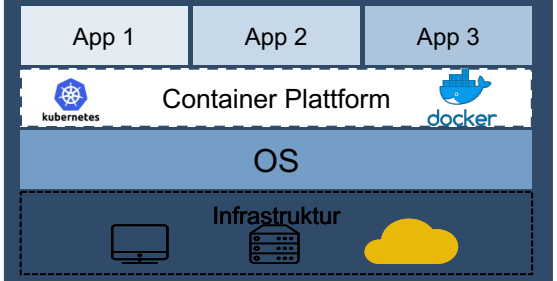
Bestandssysteme

- On-premise Bereitstellung aus FI-TS Rechenzentren in Deutschland
- Statische Konfiguration von Anwendungen auf einzelnen Servern



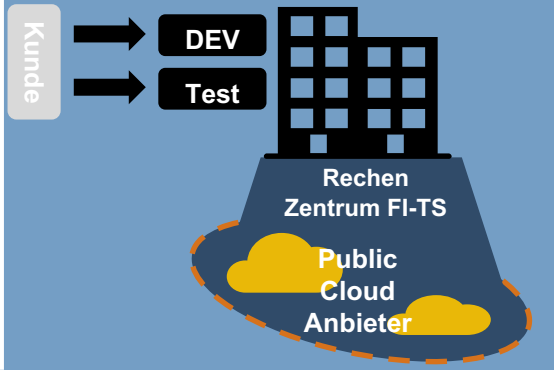
Finance Cloud Native

- Basis: Vollautomatisiertes Management von Kubernetes-Clustern auf physischen Servern.
- Bereitstellung in den FI-TS Rechenzentren in Deutschland



Managed Public Cloud

- Kombination von **Public Hyperscaler-** mit FI-TS Services.
- FI-TS = ServiceProvider für den Kunden
- Integration der Services von Public Cloud Providern



FI-TS Finance Cloud Native - Produkte

Dynamisch bereitgestellte Services in eigenen Rechenzentren mit Abrechnung auf Stundenbasis.

Mindestabnahme für die Cluster-Laufzeit
64 CPU; 128GB RAM; 512GB Storage

Kubernetes CPU
(1 CPU = 1 Hyperthread)

Kubernetes RAM

Abrechnung anhand der im Kubernetes-Deployment vorgenommenen Ressourcen-Reservierungen (spec.containers[].resources.requests.cpu, bzw. .memory)*.

Automatische Skalierung des Kubernetes-Clusters anhand der vorgenommenen Reservierungen.

Kubernetes Volumes

Bereitstellung von „Local Persistent Volumes“ auf NVMe-Disks im jeweiligen Kubernetes Worker-Node. Verrechnung anhand der angeforderten Größe (GB).

Kubernetes Block-Storage

Volumes auf hoch performatem, zentraler Storage zur Node-unabhängigen Bereitstellung von Speicherplatz für Container.

Kubernetes Traffic

Erfassung des ein- und ausgehenden Datenverkehrs Richtung Internet oder MPLS-Backbone.

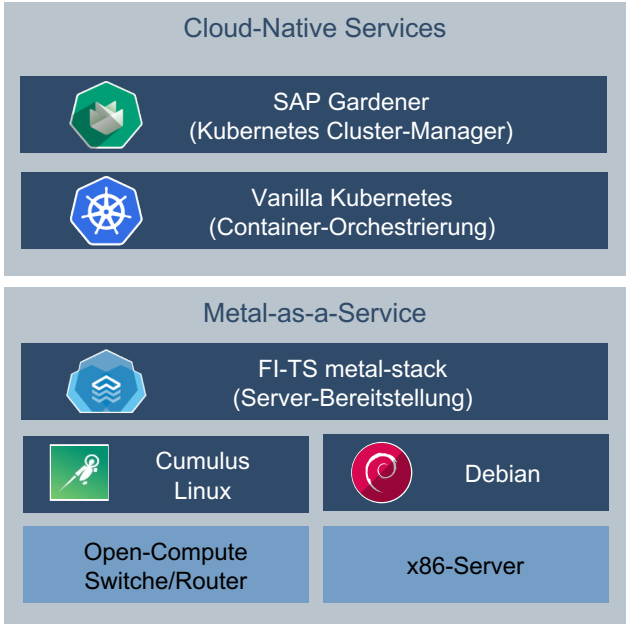
S3-Object-Storage

Der S3-Object-Storage wird in jeder Lokation zentral zur Verfügung gestellt. Die durchschnittlich belegte Menge je S3-Object-Storage wird verrechnet.

* siehe auch https://kubernetes.io/docs/concepts/configuration/manage-compute-resources-container/

FI-TS Finance Cloud Native - Architektur

Bare-Metal Kubernetes-Service aus dem eigenen Rechenzentrum.



FI-TS setzt bei der technischen Architektur der Cloud-Native Plattform auf Open-Source und standardisierte Schnittstellen.

- Gardener: Vollautomatisiertes Kubernetes-Management mit Unterstützung für Google, Azure, AWS, Metal-Stack, …
- Kubernetes: Nutzung der Open-Source Variante von Kubernetes gewährleistet Austauschbarkeit der Anbieter und schnelle Weiterentwicklung.
- Metal-Stack: Open-Source Orchestrierungslösung für die Infrastruktur zur Bereitstellung von physischen Servern in separierten Netzsegmenten (https://metal-stack.io).
- Linux: Einheitliches Betriebssystem für alle Komponenten der Plattform, bietet weitgehende Hardware-Unabhängigkeit. Automatisierte Installation und Management durch Metal-Stack.

FI-TS Finance Cloud Native – Bare-Metal Hardware

Zentrale Netz-Komponente: Spine/Leaf Router

- Linux basierender Router/Switch
- Cumulus Linux
- OpenCompute Networking-Design
- 32x 100 GBit/s oder 128x 25 GBit/s
- Software-Defined Networking mit dynamischem Routing

Worker-Nodes & Firewall

- 4 Server in 2HE
- 2x Xeon Silver 4116, bzw. 4214 Prozessoren (24 Cores)
- 96GB RAM
- Lokale NVMe-Disks (vsl. 2x 1,6 TB)
- Anbindung mit 2x 25 GBit/s

Netz

- CLOS-Topologie mit redundanter Anbindung aller Komponenten
- Routing-to-the-Host für maximale Flexibilität, Performance, Ausfallsicherheit und Lastverteilung
- Eigene Layer-3 Netzsegmente je Kubernetes-Cluster

Server & Storage

- „Versiegeltes“ Open-Source Linux
- Image basiertes Installationsverfahren
- Keine administrative Anmeldung auf den Servern
- Lokaler Storage (643.000 / 199.000 IOPS)
- Keine Widerherstellung

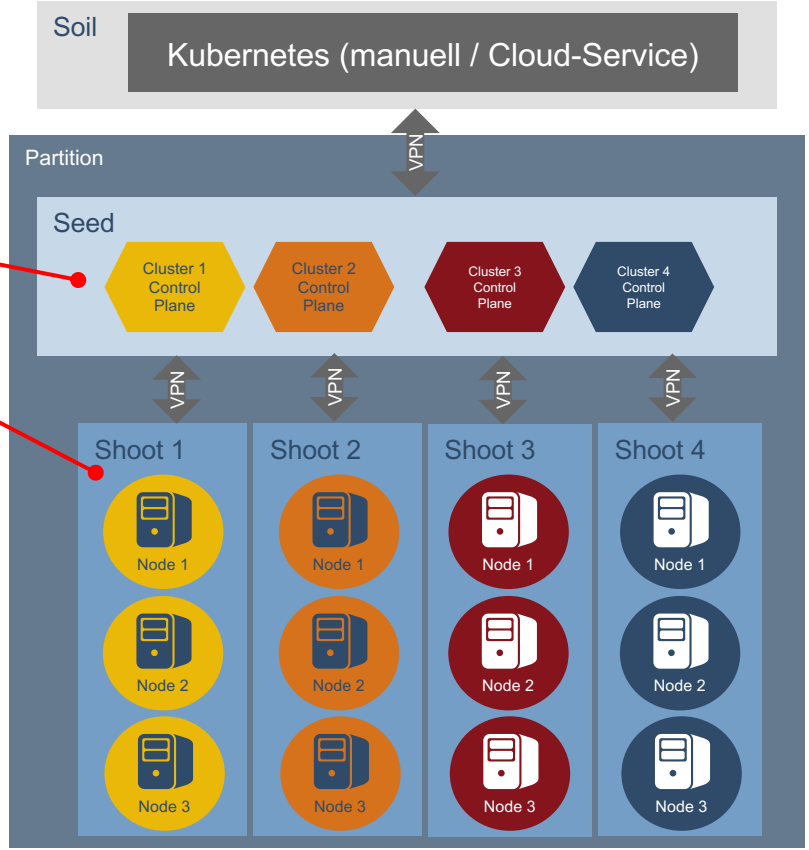
SAP Gardener

Automatisiertes Management von vielen Kubernetes-Clustern

Zentrale Control-Plane der FI-TS

Mandanten-getrennte Umgebungen

- Installation und Management von Kubernetes-Clustern
- Hierarchisches Management von verschiedenen Umgebungen (Soil->Seed->Shoot)
- Extension-Provider für verschiedene Cloud-Anbieter (AWS, Azure, Google, VMware, Metal-stack, …)



metal-stack.io

Metal-stack besteht aus mehreren Komponenten und steuert die Infrastruktur-Bereitstellung im Zusammenspiel mit SAP-Gardener und Kubernetes

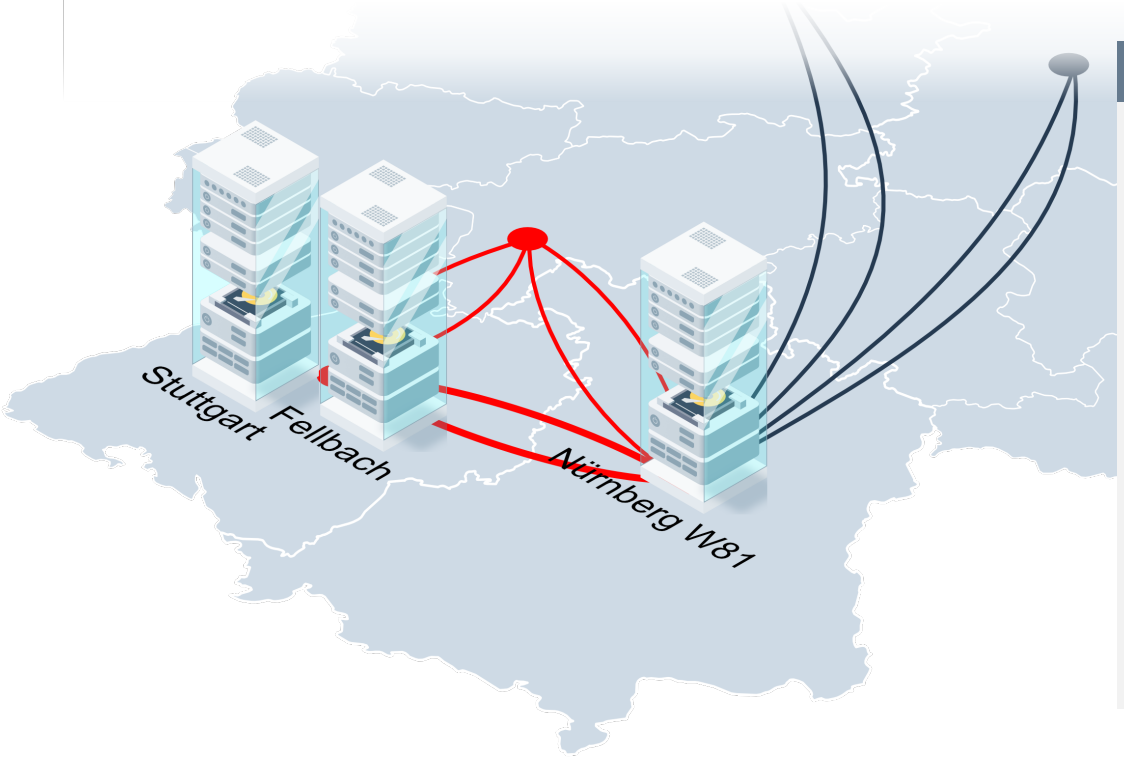
- Zentrale Konfigurations-Datenbank und –APIs (metal-api)
- Management-Komponente auf den Switches (metal-core)
  - PXE-Proxy (zur metal-api)
  - Steuerung von Netzwerk-Interfaces und dynamischen Routing
- Automatische Installation von Systemen
  - Discovery und Steuerung der Systeme über IPMI (bmc-catcher)
  - Image-basiertes Installationsverfahren & Network-Discovery (metal-hammer)
- API-Schnittstellen für Kubernetes- und Gardener-Plugins
  - Plugin für SAP-Gardener (gardener-extension-provider-metal)
  - Cloud Controler Manager für Kubernetes (metal-ccm)
- Vagrant basierte lokale Testumgebung (mini-lab)

metal-stack.io

Allgemein nutzbare Tools- und Kubernetes-Plugins

- CSI-Provider für Local-Persistant-Volumes (csi-lvm)
- Kubernetes-Controller zum Deployment von Lightbits-Storage (CSI-Provider, Authentication)
- Firewall-Controller zur Kubernetes-basierten Verwaltung einer vorgeschalteten Firewall
  - Ingress: Exponieren von im Cluster definierten Loadbalancer-Services
  - Egress: Auswerten einer speziellen Custom-Ressource-Definition (ClusterWideNetwortkPolicy)
  - Generiert nftables-Regeln
  - Optional: Konfiguration von Suricata auf der Firewall

FI-TS Finance Cloud Native – Rechenzentren



Standorte

Aktuell sind 3 Rechenzentren mit Cloud-Native Partitionen ausgestattet.

Jedes Rechenzentrum verfügt über einen Server-Pool von ca. 150 physischen Servern.

In Summe verfügt FI-TS damit für die Cloud-Native Produkte über ca.

- 10.000 Cores
- 40 TB RAM
- 5 PB NVMe Storage
- 3 PB S3-Storage