

4. Cloud Native Bern Meetup

Building Mission-Critical Applications on k8s

18.09.2019

Christian Bürgi, PostFinance AG
Acquiring System Lead Developer
Twitter: @buergich

PostFinance 



CHF



EUR

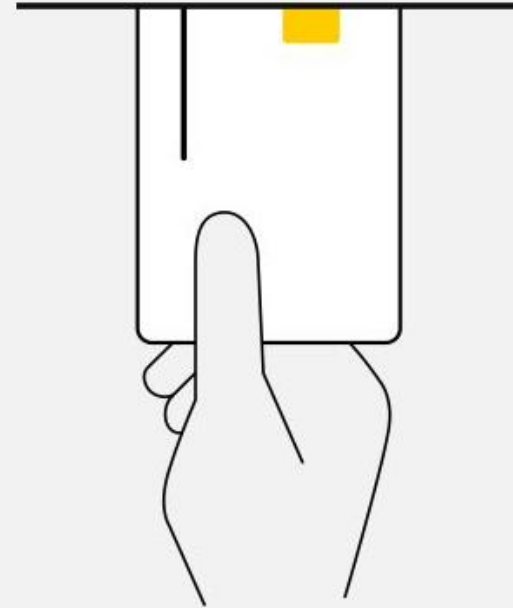


Bitte Karte einfügen.

Veuillez insérer la carte.

Inserisca la carta.

Please insert your card.



Agenda

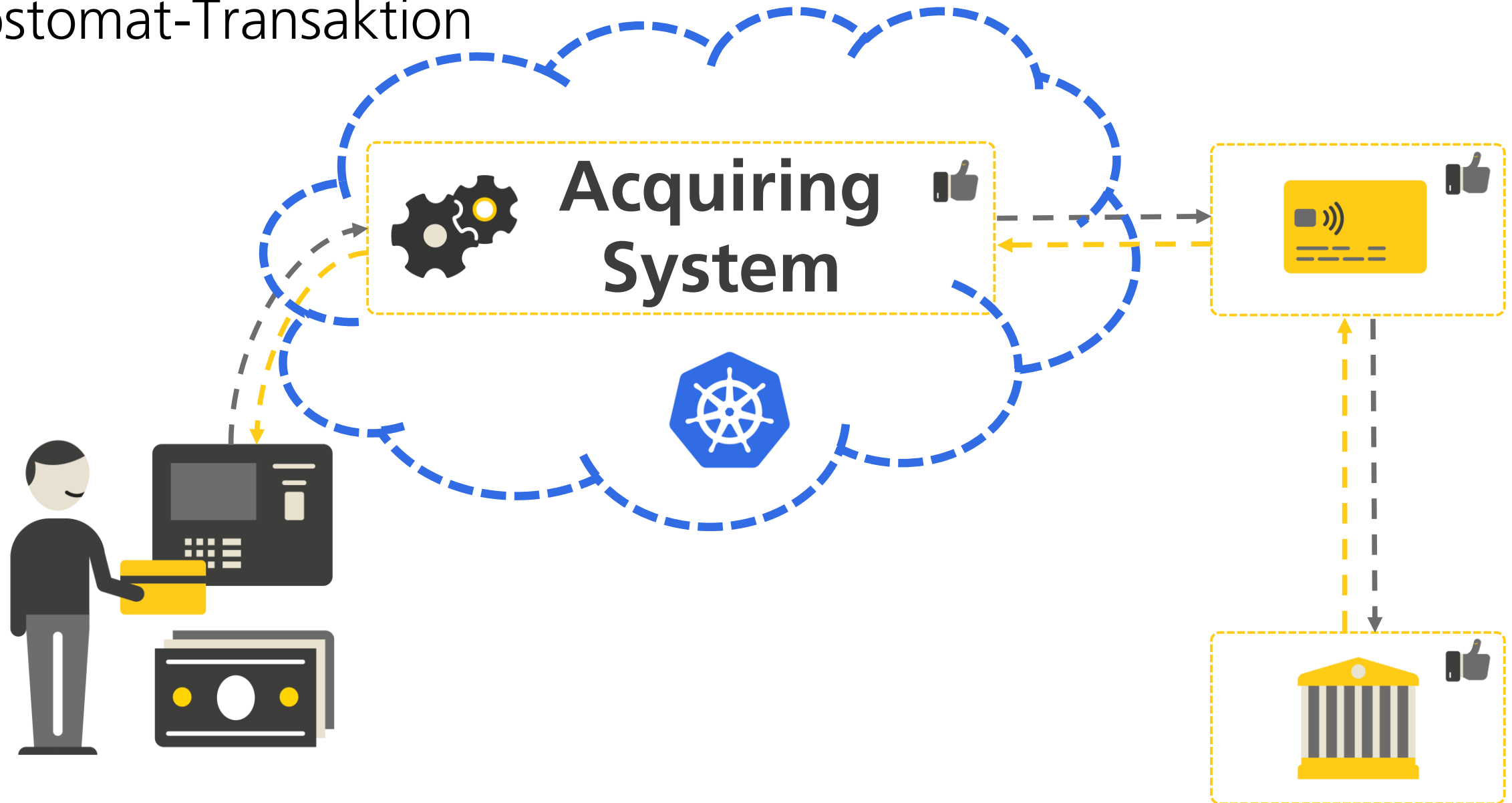
- **Einführung**
Use Case Postomaten-Backend
- **PostFinance k8s-Cloud als Anwender**
Namespace-Administration und System-Integration
- **Learnings**
Erfahrungen aus Build und Betrieb
- **Ausblick**



Einführung

Use Case: Postomaten-Backend

Postomat-Transaktion



Roadmap

- **Oktober 2017**

Entscheid: Neues Postomaten-Backend läuft auf Docker (Native oder Cluster)
Anschliessend erste PoCs auf bestehender Openshift-Plattform

- **April 2018**

Entscheid: Neue Plattform wird mit k8s gebaut

- **Ab Mai 2018**

Wöchentlicher k8s-Tag: Infrastruktur (Linux, Middleware), Applikation, Operations

- **September 2018**

Test-Cluster bereit

- **19. Mai 2019**

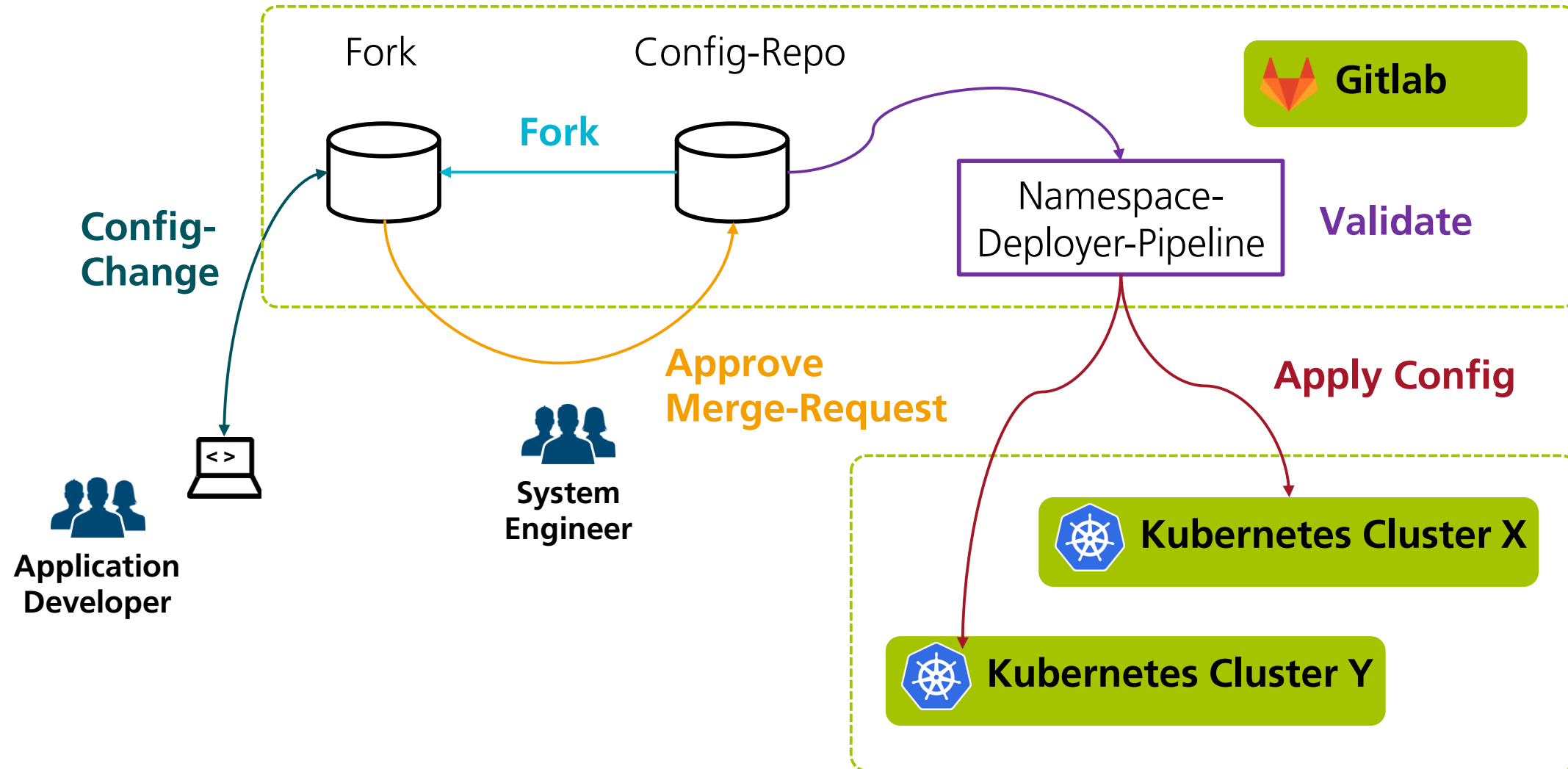
Live-Schaltung Prod-Cluster, anschliessend geräteweise Migration



PostFinance k8s-Cloud als Anwender

Namespace-Administration und System-Integration

Namespaces: Config-As-Code





René Moser

@resmo79



Redefining my job title: YAMLineer

♡ 6 11:52 AM - Sep 17, 2019



 [See René Moser's other Tweets](#)



Namespaces: Config-As-Code

📄 **appl-aqs-cncfdemo-e1.yaml** 219 Bytes 🔗

```
1  roles:
2  - appl_aqs
3  application:
4    sysappl: AQS
5    owners:
6    - christian.buergi@postfinance.ch
7    operations:
8    - christian.buergi@postfinance.ch
9  quota:
10   limits:
11     cpu: 15
12     memory: 30Gi
13  vault:
14   role: applam_team_aqs
```

Namespace-Name

Zugriffs-Rolle im zentralen Identity-Management

Owner: Architektur-Komponente

Mail-Kontakt für Owner/Operations

Namespace-Quotas

Vault-Rolle für Secret-Sync

Integration

Zertifikate, Truststores

- Zentrale Verwaltung in eigenem System
- Verteilung über Operator in berechnigte Cluster/Namespaces

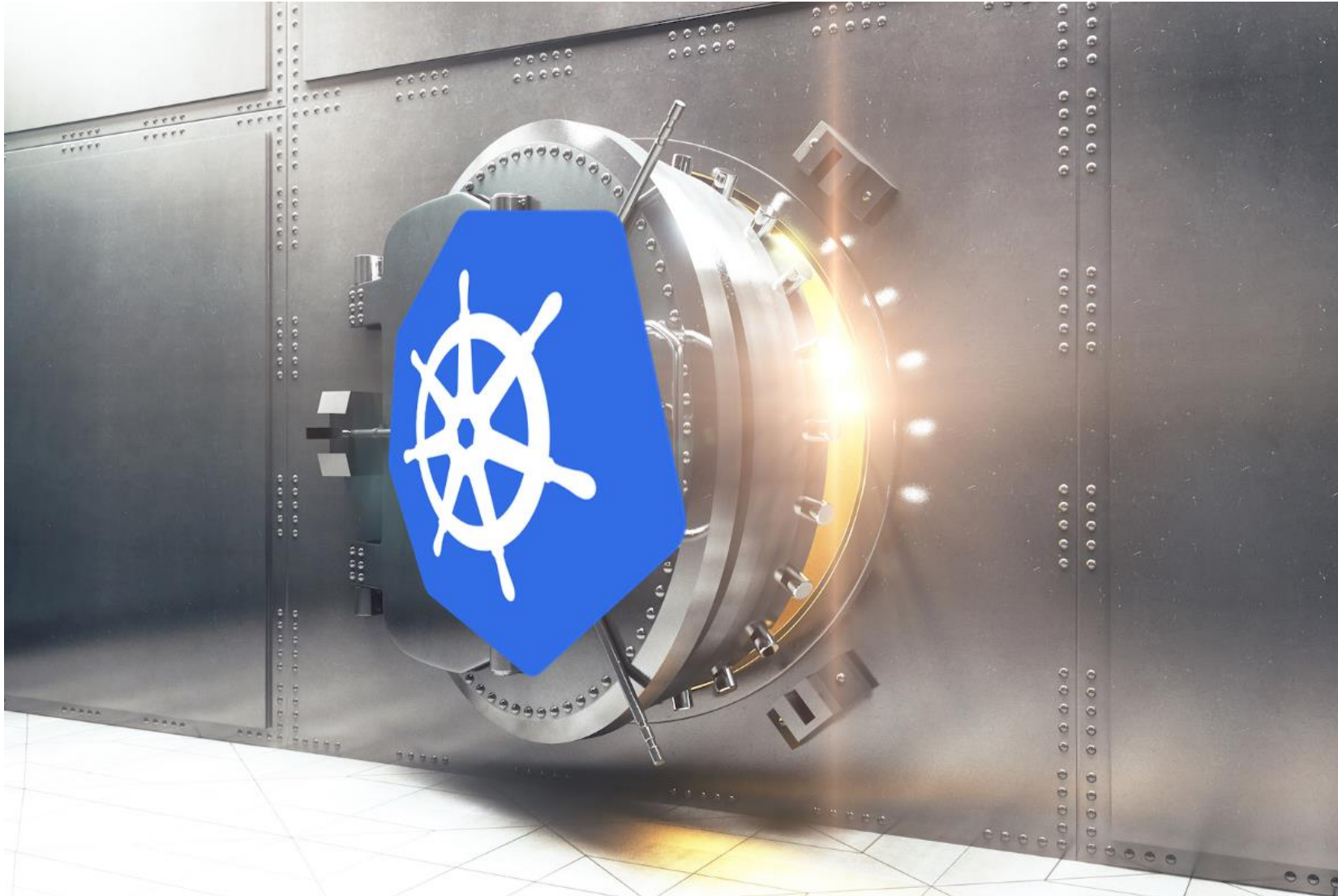
Integration

Observability

- Konfiguration über Annotationen («Pull-Prinzip»)
 - Logging: Splunk
 - Metrics: Prometheus
- Konfiguration über ENV («Push-Prinzip»: Agent auf Worker-Nodes)
 - Tracing: Jaeger
 - Alarming: In-House Library

Vault

Demo

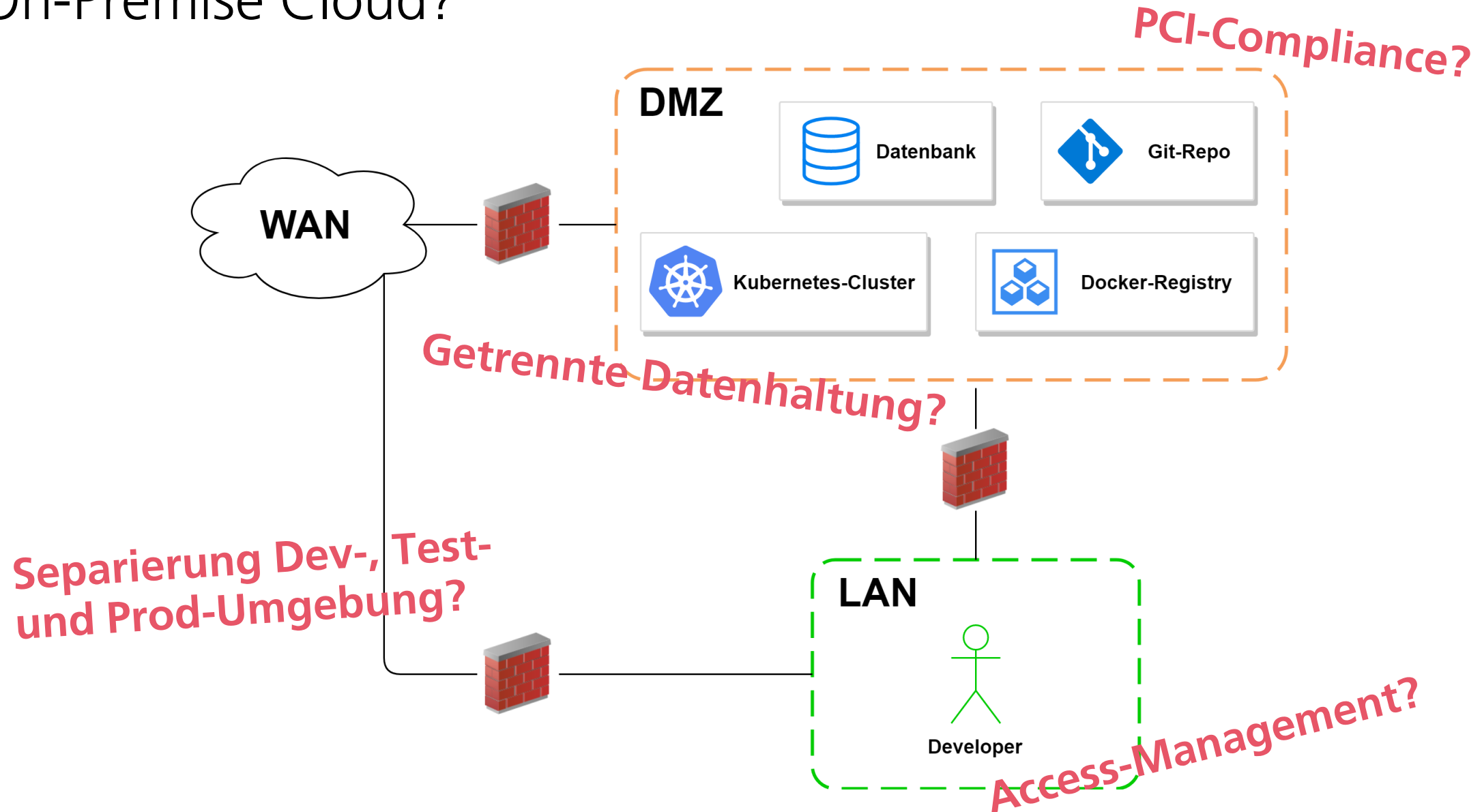




Learnings

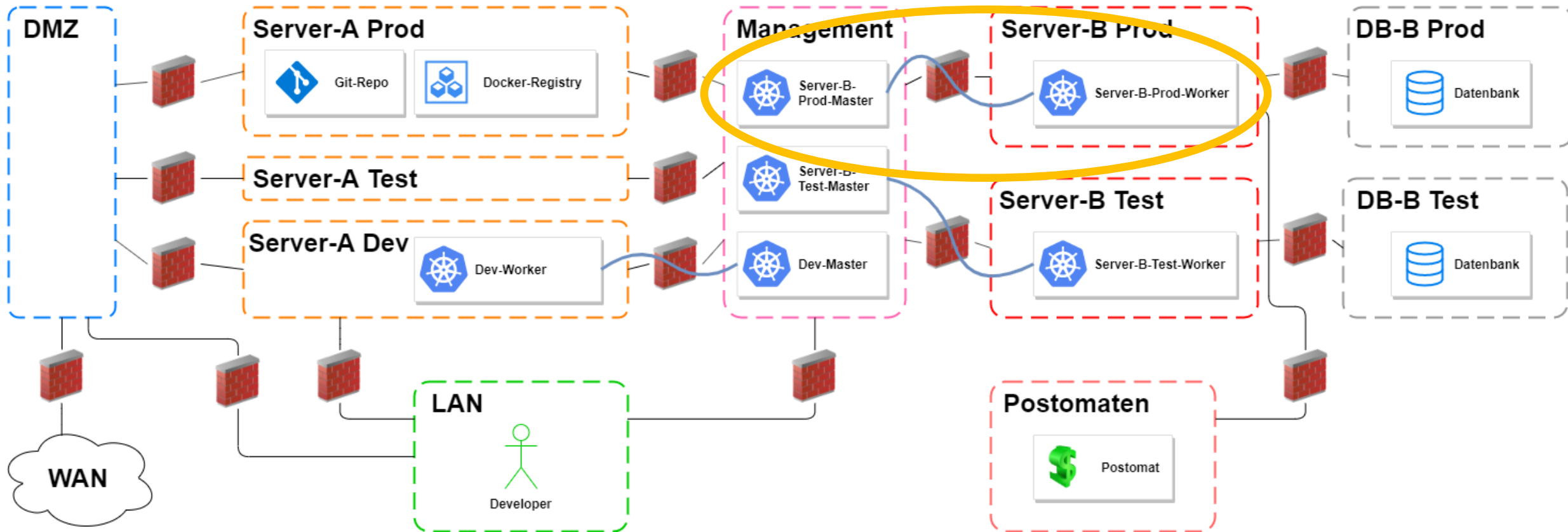
Erfahrungen aus Build und Betrieb

On-Premise Cloud?

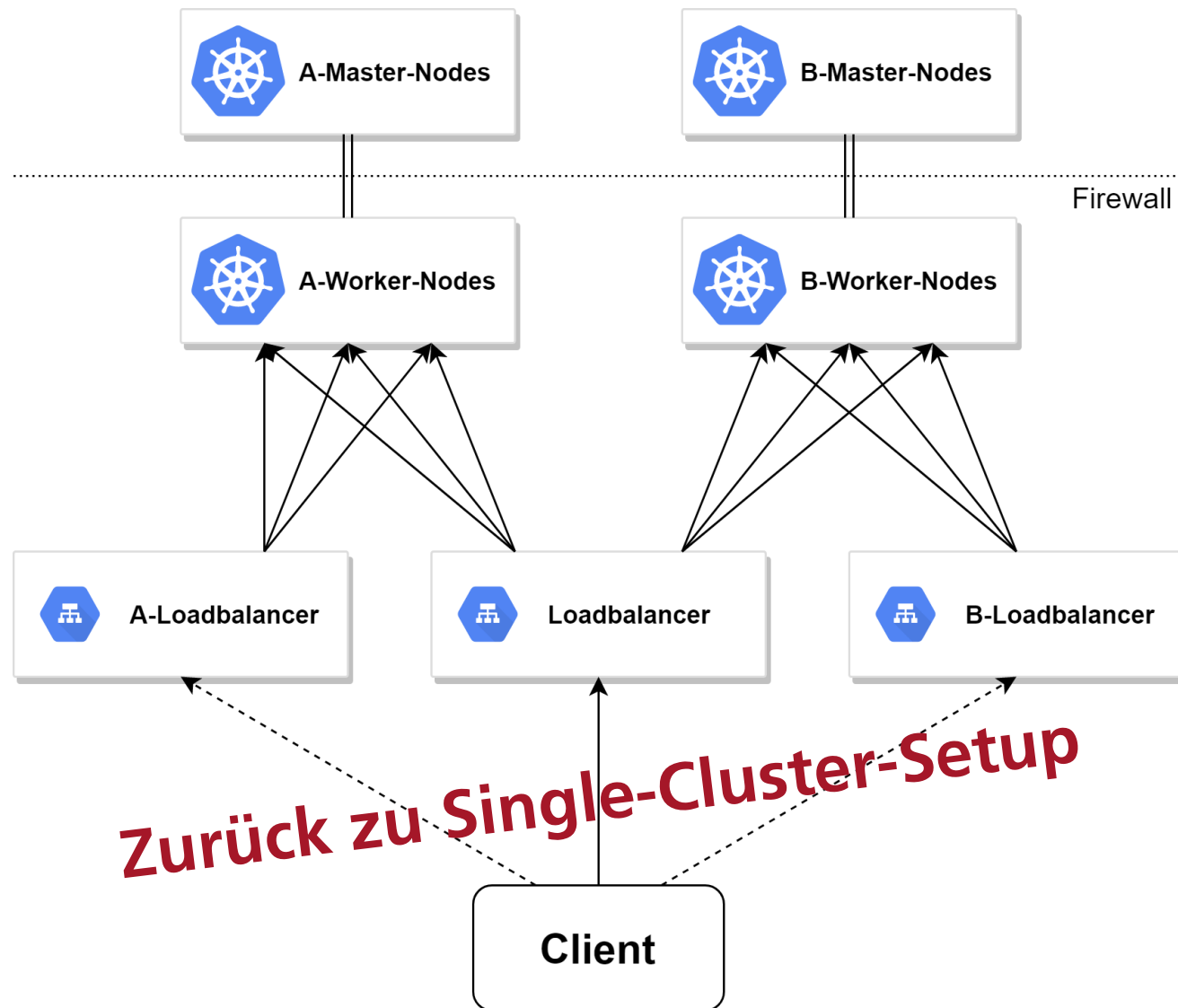


PostFinance-Setup

Network-Lag (e.g. DNS)



Multi-Cluster Setup

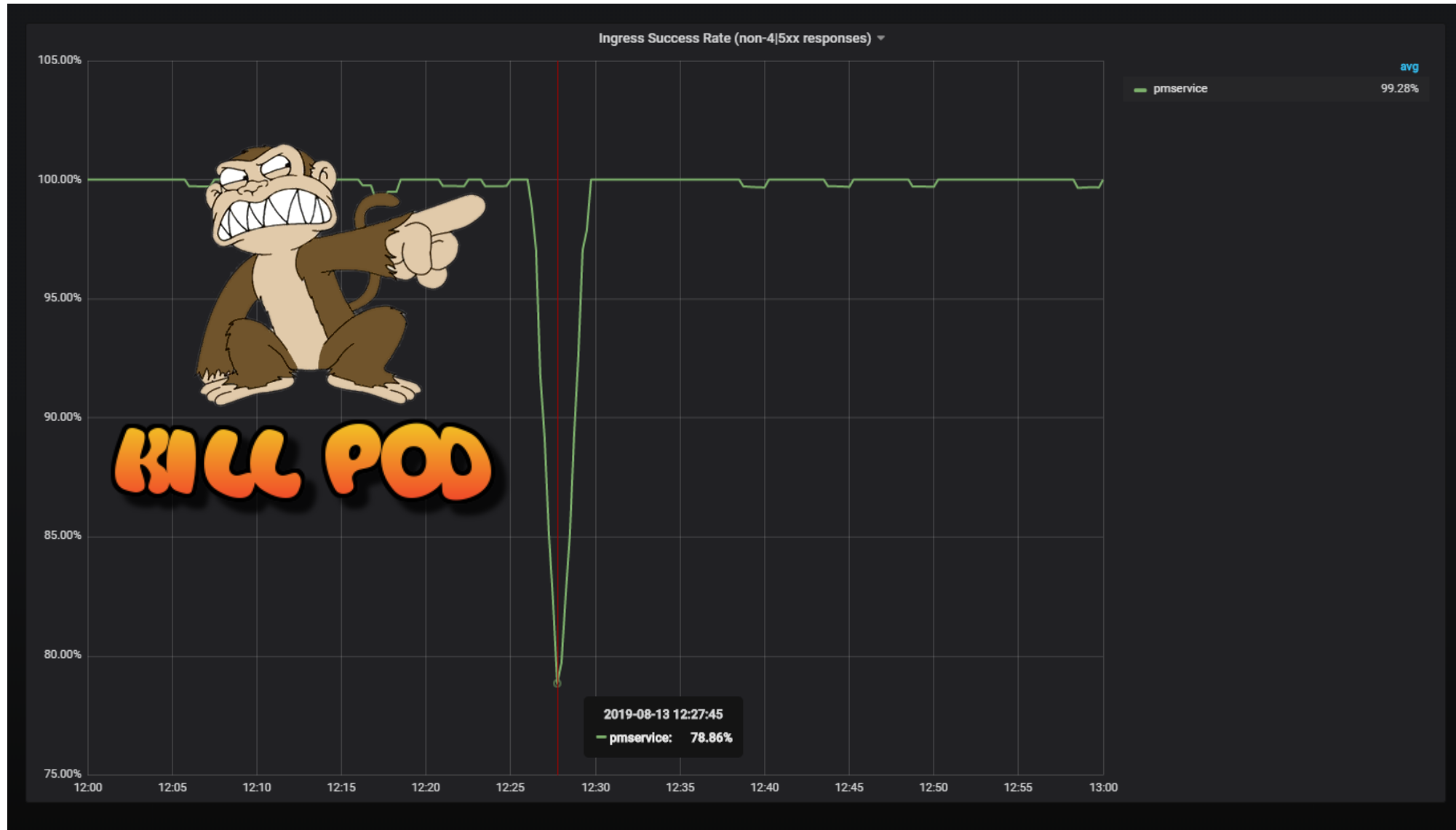


- Initiale Cluster wurden redundant aufgebaut
- Ingress-LB delegiert an Worker aus beiden Cluster
- Dedizierte A- und B-Cluster Loadbalancer

Problematik

- Single-Execution Workloads
- Disaster-Fall wirklich zweckmässig?

Chaos Monkey




Incident-Analyse

- Chaos-Monkey löste unter Last einen Pod-Restart aus
- Synchronisierungs-Fehler in der Applikations-Initialisierung führt zu undefiniertem Zustand im Pod
- Alarmierung über Prometheus Alert-Manager
- **System erholt sich von selber (Resilienz!)**
- **Operations kann selbständig Fehleranalyse und Behebung durchführen**
- **Bug wird ins Applikations-Backlog aufgenommen und gefixt**

Ausblick

Ausblick

- Oktober 2019
 - Migration Cluster 2.0
 - Weitere Services auf k8s Plattform
- 2020
 - Deployment: GitOps
 - Migration restliche Workloads auf k8s Plattform (Kartengeldsysteme)



«We choose to deploy our mission-critical workloads on k8s, not because they are easy, but because they are hard»

Präge mit uns den Fortschritt des Digitalen Bankings



2,9 Mio. Kundinnen und Kunden vertrauen für ihren täglichen Umgang mit Geld auf PostFinance.



Mission-Critical
Mit Leidenschaft und Teamgeist arbeiten wir tagtäglich an systemrelevanten Services.



Q & A

Geldbezug

Bitte Beleg und Geld entnehmen.

