06.11.2019
W-JAX / München

Service Mesh

- das Missing Piece der Microservices-Architektur

INNOQ

Hanna Prinz

Warum Microservices?

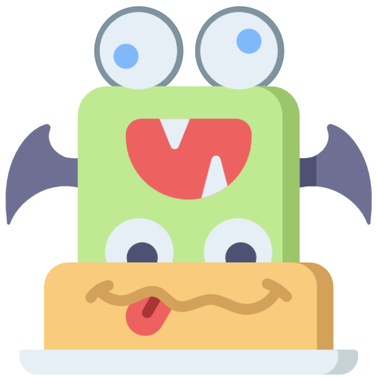
Microservices

+

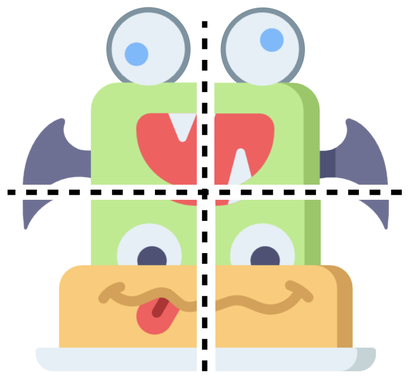
Kürzere Time-to-Market

Skalierbarkeit

Technologiefreiheit

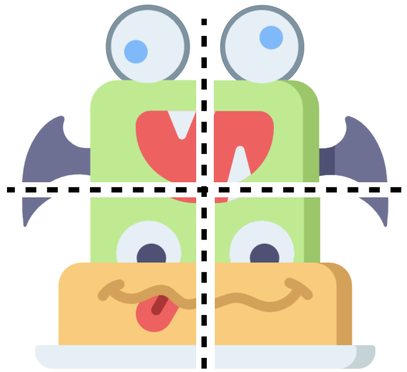


Monolith

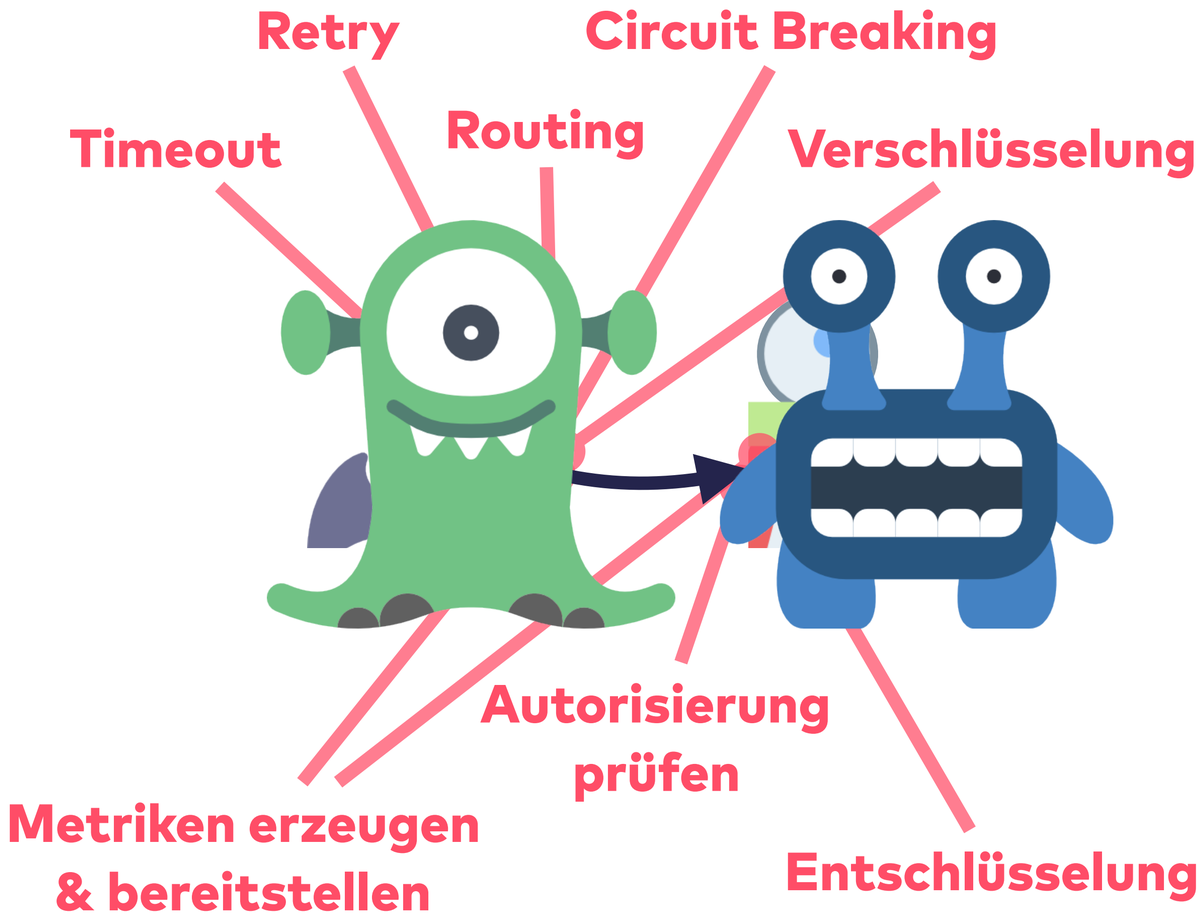


Microservices

Warum Service Meshes?

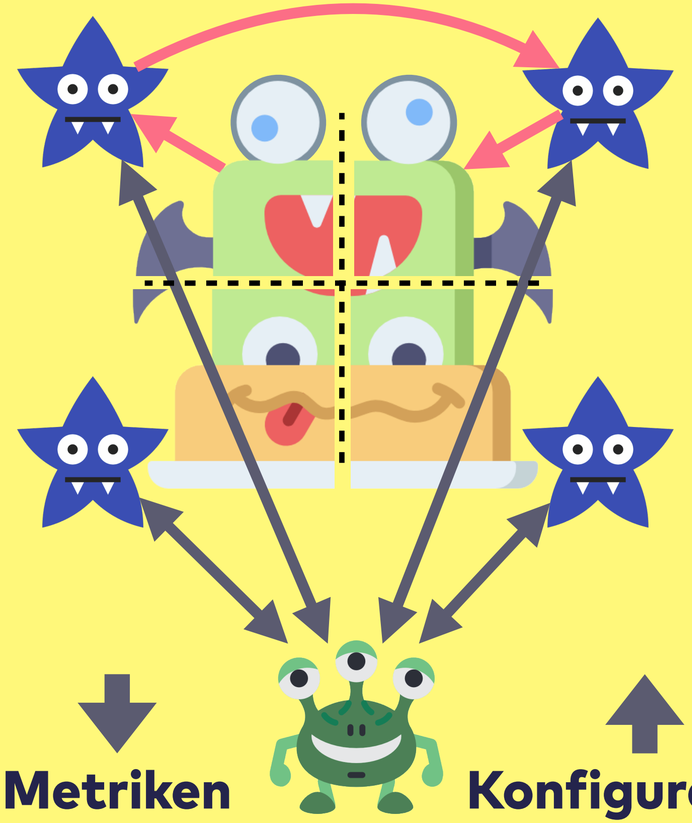


Microservices


Retry
Circuit Breaking
Timeout
Routing
Verschlüsselung
Autorisierung
prüfen
Metriken erzeugen
& bereitstellen
Entschlüsselung

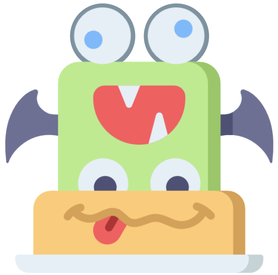
Service Mesh

Retry
Timeout
Circuit Breaker
Routing
Verschlüsseln
Entschlüsseln
Autorisierung
Metriken
...

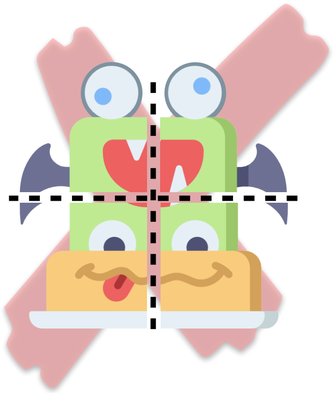


Service Mesh Architektur

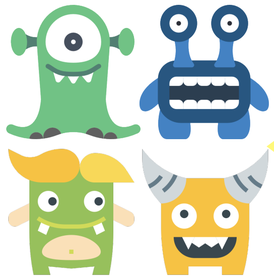
Monolith



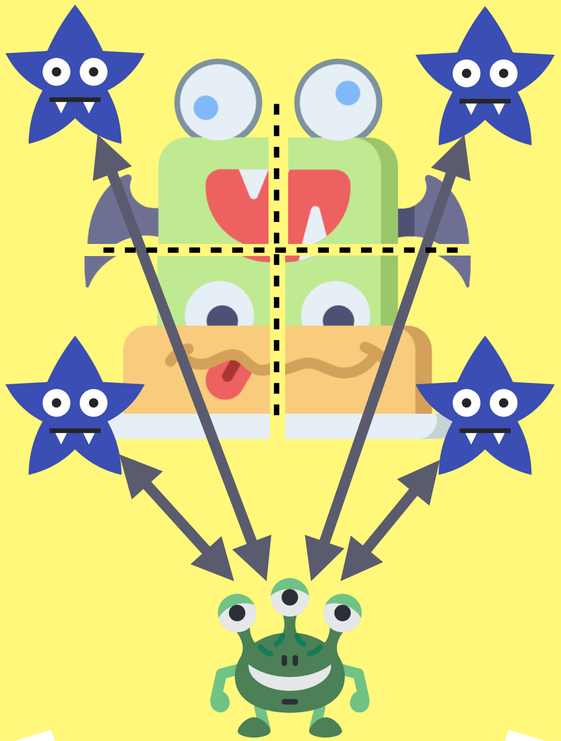
Microservices Theorie



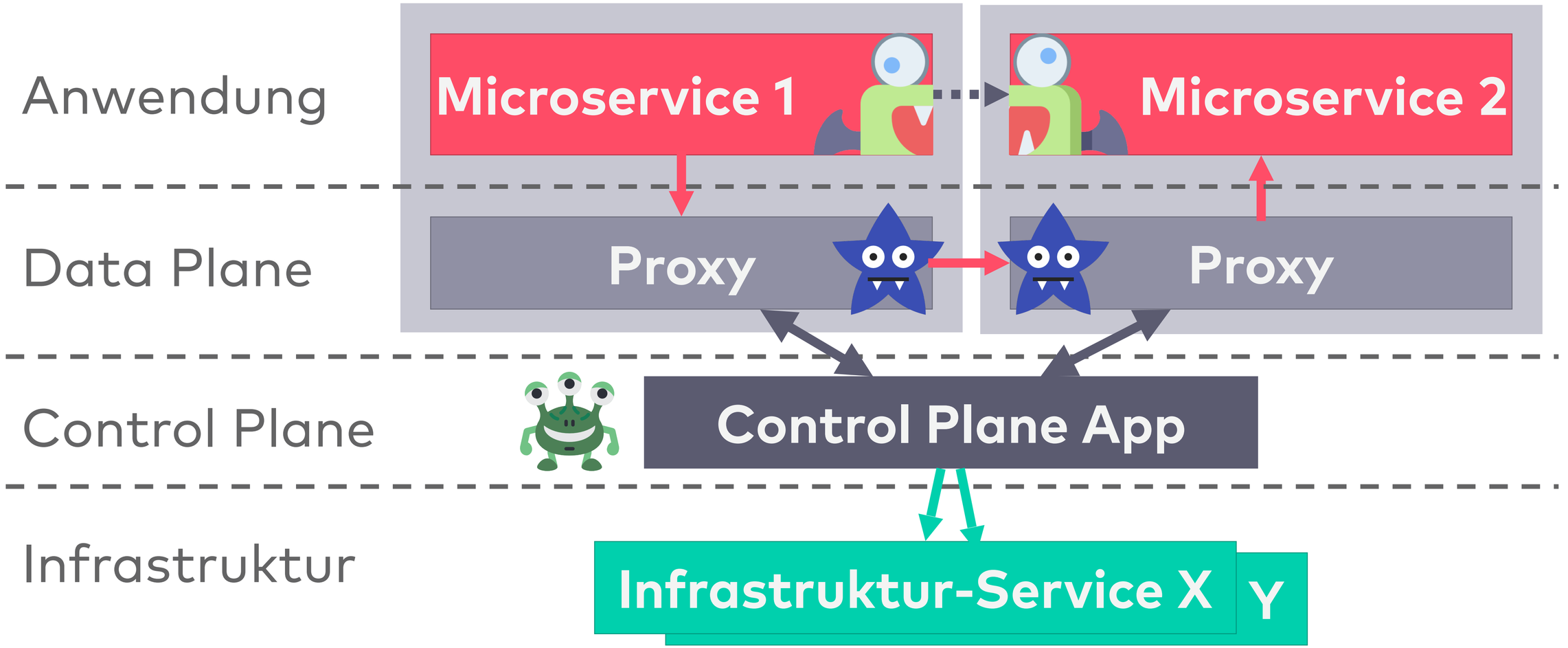
Microservices Praxis



Microservices mit Service Mesh



Service Mesh Architektur



Was kann ein Service Mesh?

Service Mesh Features

Observability

Routing

Resilience

Security

Beispiele mit dem Istio Service Mesh

Monitoring

Ein Service Mesh kann automatisch Daten für alle 4 "Golden Signals" liefern:

Latenz

Requests/Sekunde

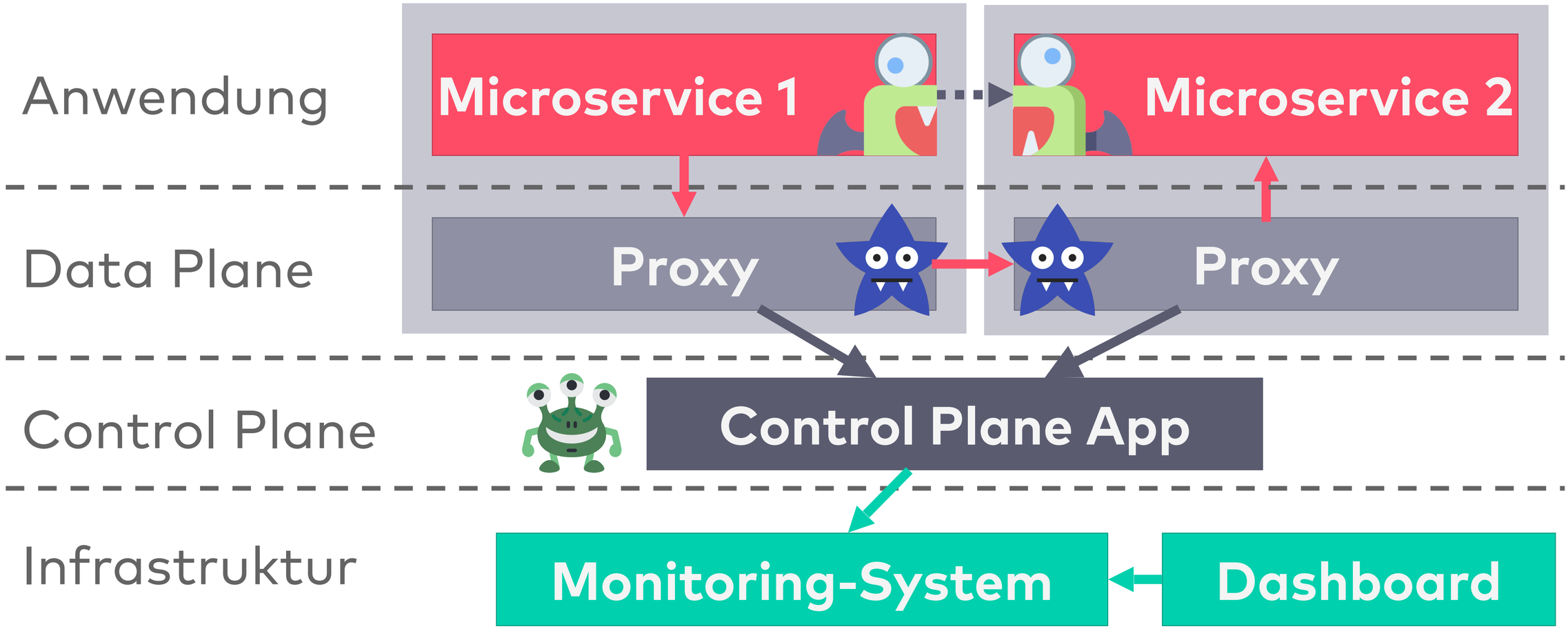
Status Codes (Fehler)

Auslastung

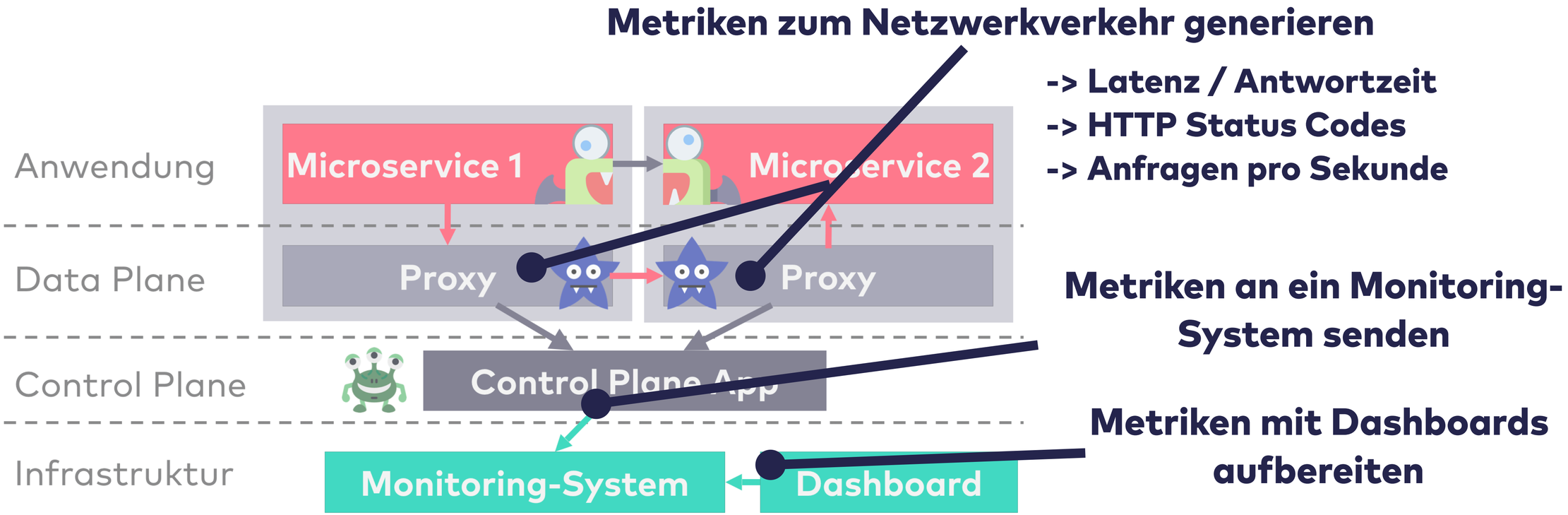
... es hat aber keinen Einblick in die Microservices

https://landing.google.com/sre/sre-book/chapters/monitoring-distributed-systems/#xref_monitoring_golden-signals

Monitoring mit Service Mesh



Monitoring mit Service Mesh



Monitoring mit Istio

Monitoring mit Istio

basiert auf...

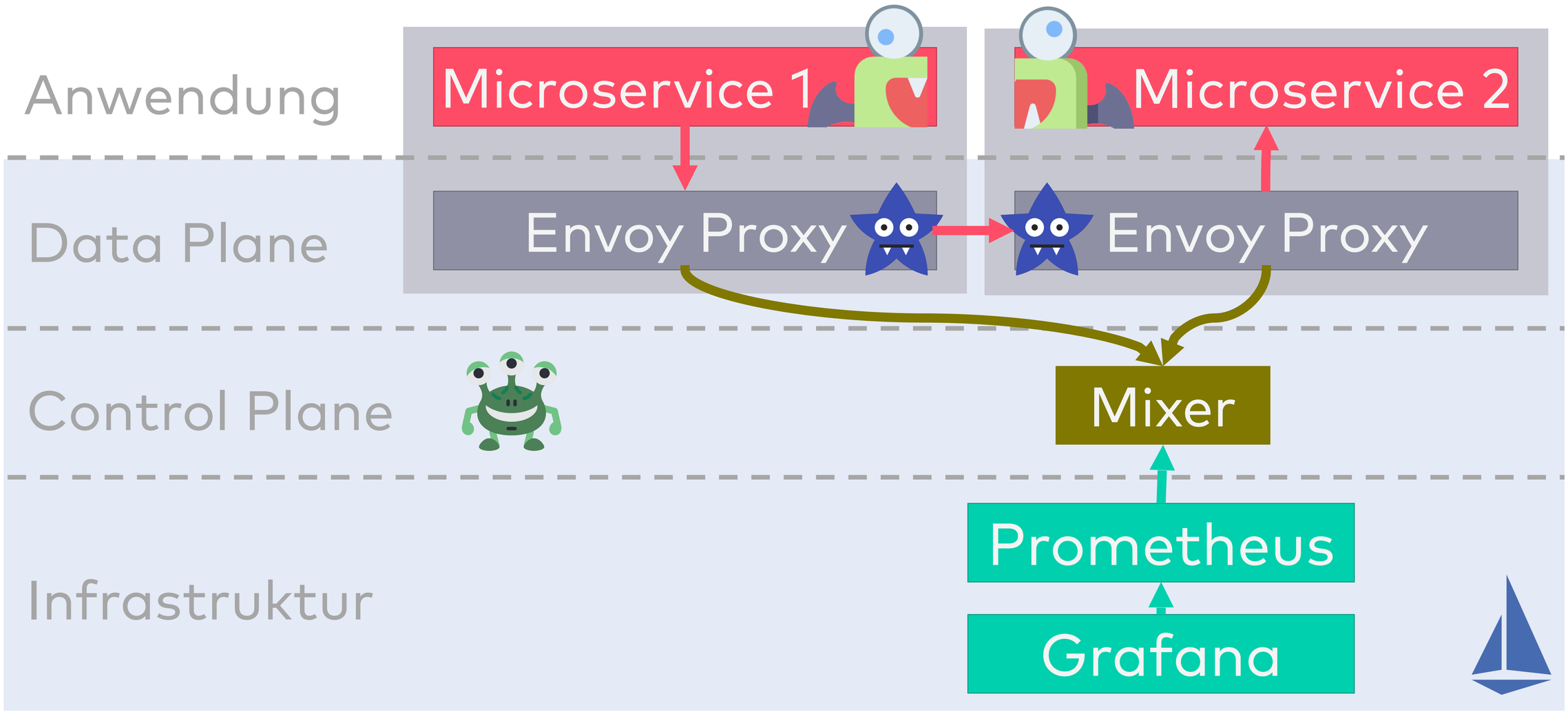
Prometheus

- Monitoring-System
- Pull-basiert
- Erfasst multi-dimensionale Daten pro Microservice
- z.B. HTTP-Statuscode, Latenz, URL, Path-Parameter,, ...

Grafana

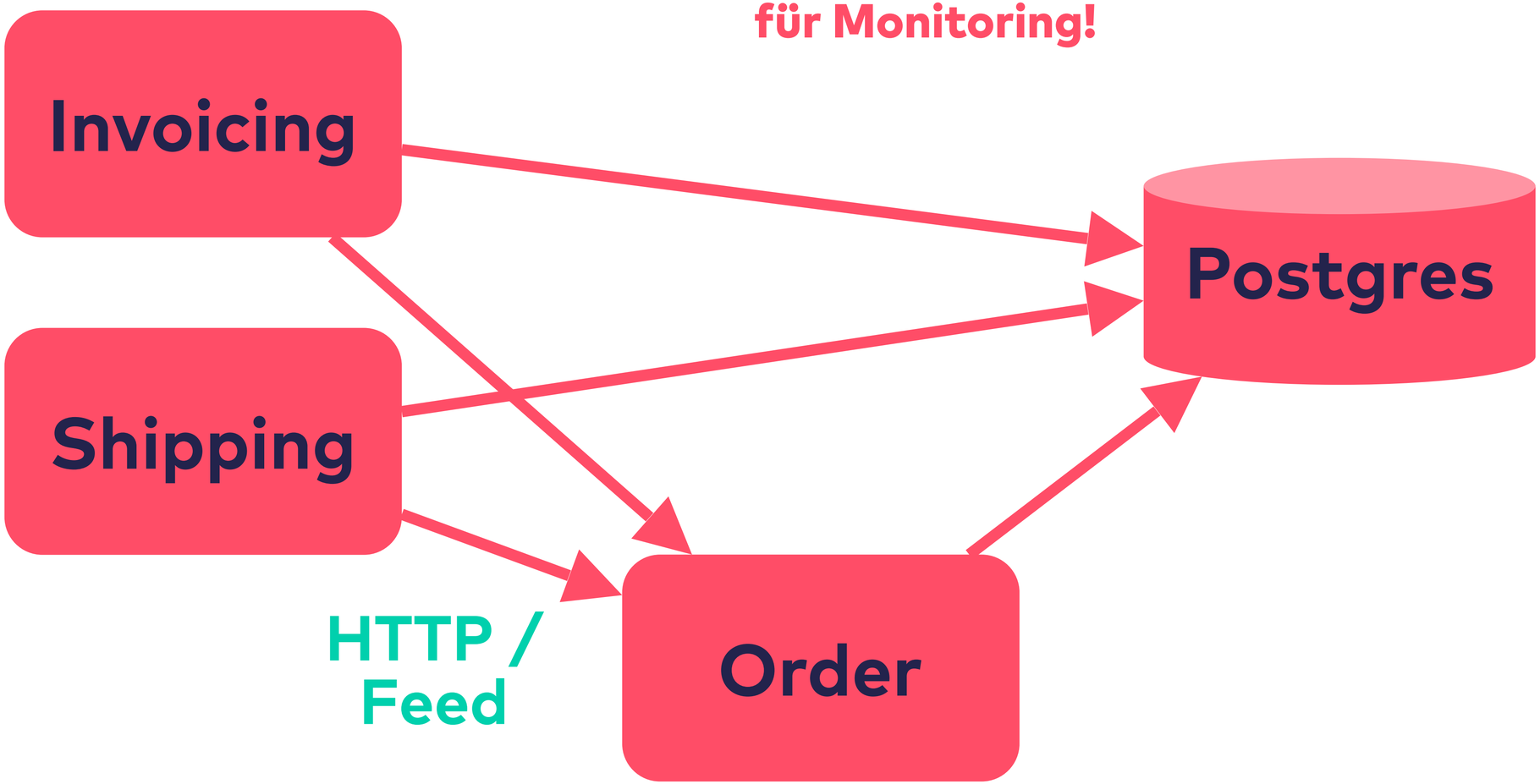
- Analyse von Monitoring-Daten
- Dashboards
- Alerting
- Istio bietet default Dashboards

Monitoring mit Istio



Beispiel

Service nutzen weder
Code noch Bibliotheken
für Monitoring!



https://github.com/ewolff/microservice-istio

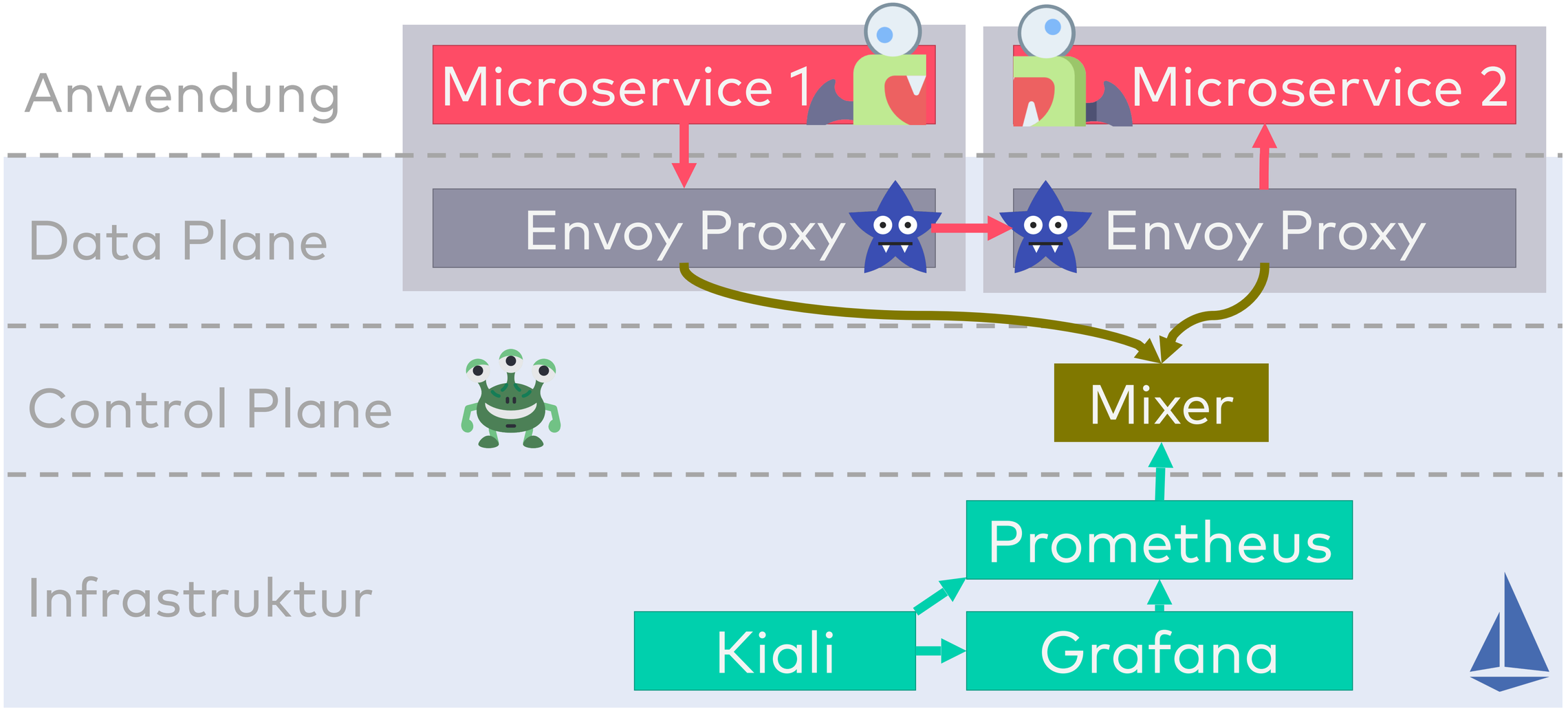
Order, Shipping, Invoicing

Order	Create an order
Shipping	Display shipping information
Invoicing	Display invoices

Istio Dashboard: Kiali

- Bereitet Prometheus-Metriken zu einem **Echtzeit-Service-Graph** auf:
  - Protokolle & Verschlüsselung
  - Latenz
  - Prozentuale Verteilung der Anfragen
  - Fehlerquoten
- Weitere Funktionen
  - Ansicht der Istio Konfiguration
  - Konfigurations-Wizards für Routing
  - Integration von Grafana und Jaeger

Istio Dashboard: Kiali

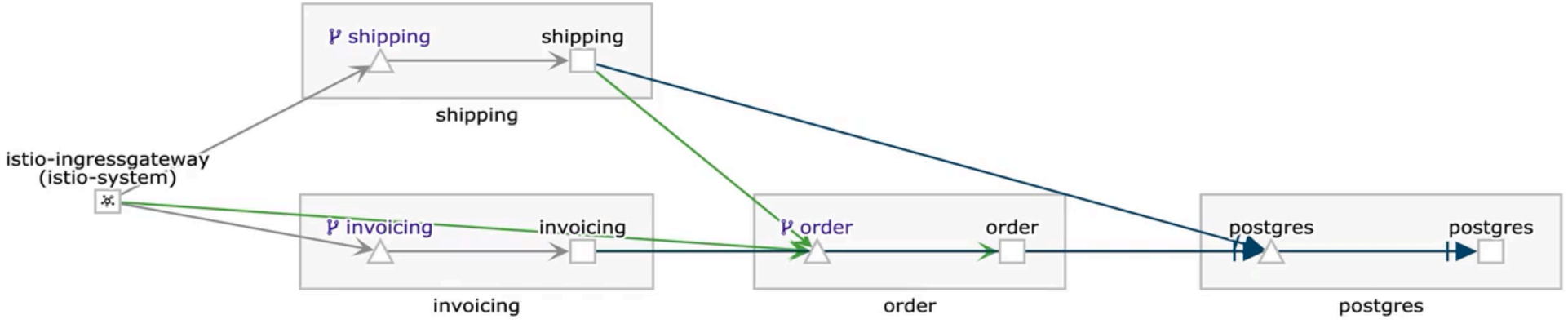


Namespace: default

Graph

23. Aug., 11:39:57 ... 23. Aug., 11:40:57

App graph | No edge labels | Display | Find... | Hide... | Last 1m | Every 10s



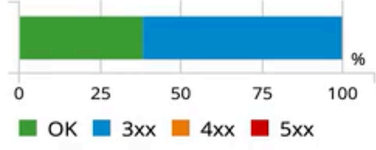
Hide

Namespace: default
applications, services, workloads

Current Graph:
5 apps
4 services
12 edges

HTTP Traffic (requests per second):

Total	%Success	%Error
0.13	100.00	0.00



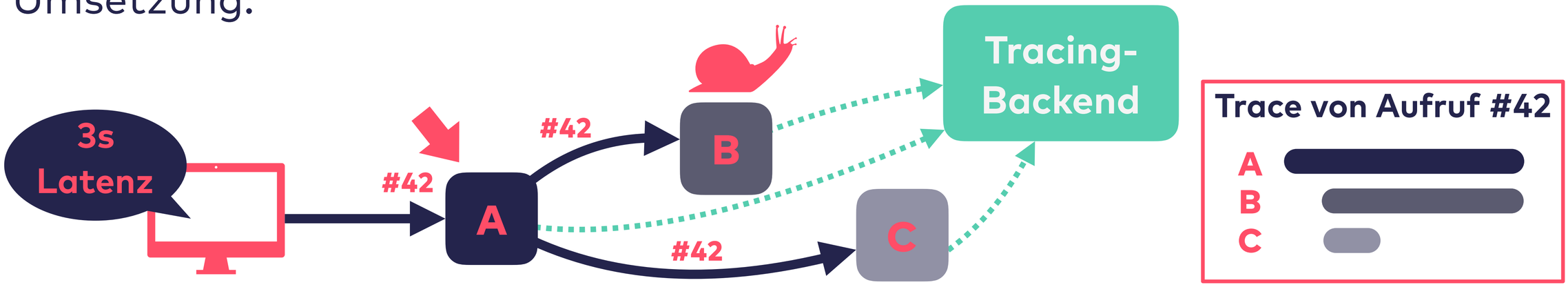
Loading chart...

Legend

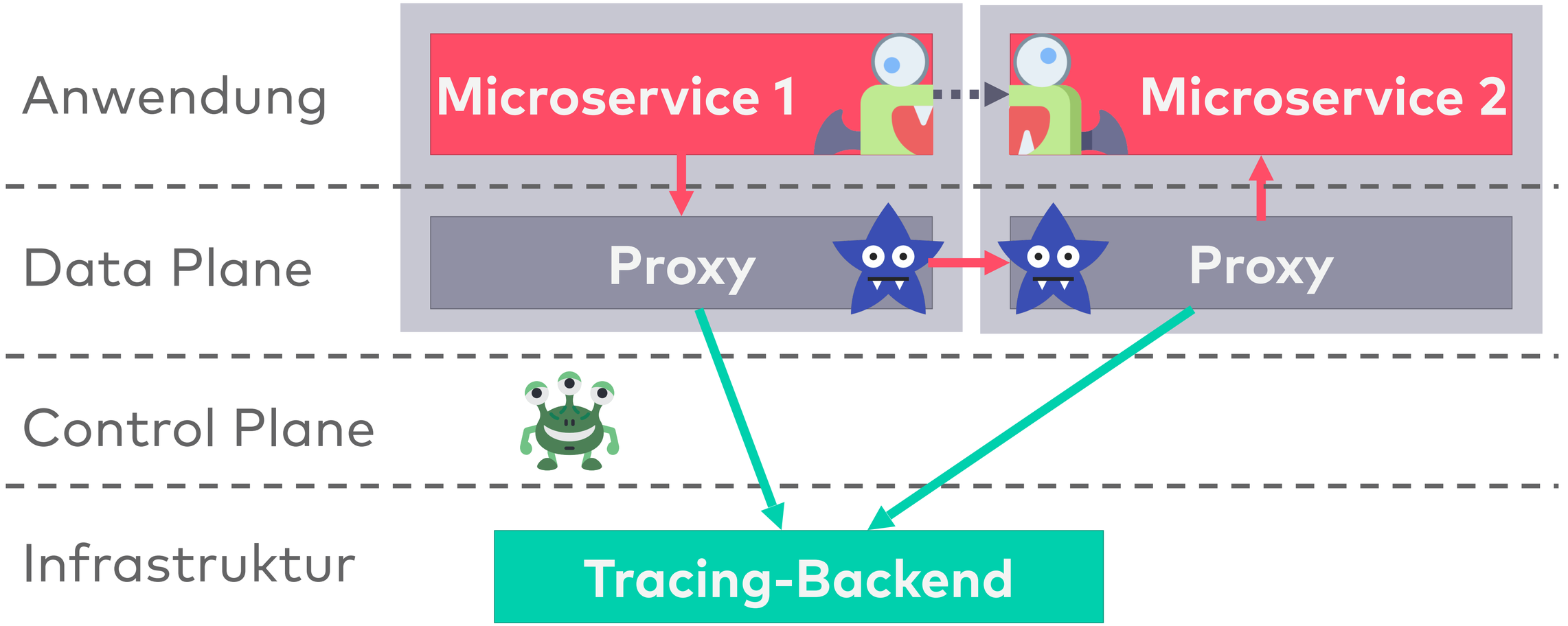
kiali

Tracing

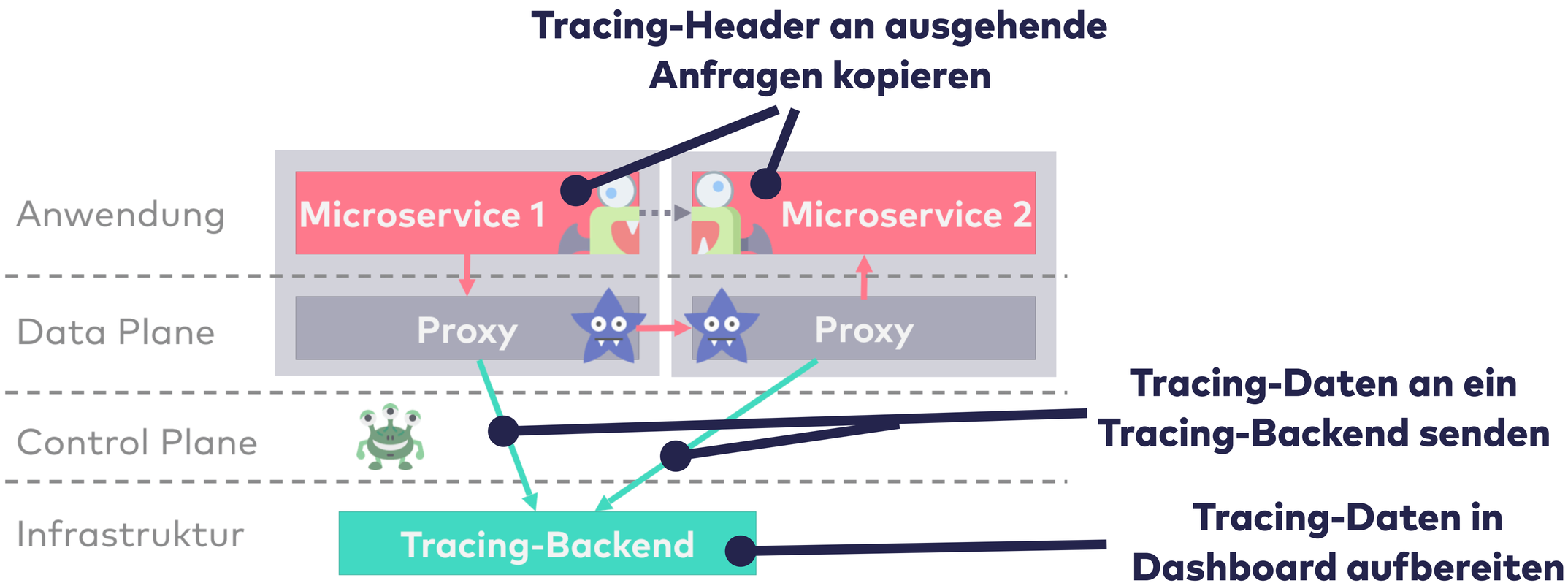
- Beantwortet…
  - Welcher Aufruf erzeugt welchen **Folgeaufruf**?
  - Welchen Anteil hat jeder Teilaufruf an der **Latenz**?
  - Wo ist ein **Fehler** entstanden?
- Umsetzung:



Tracing mit Service Mesh | Config



Tracing mit Service Mesh



Service Mesh Features

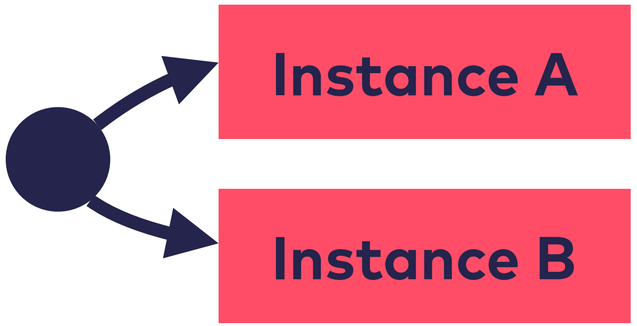
Observability

Routing

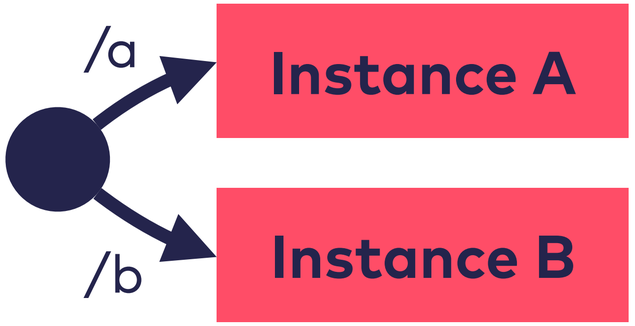
Resilience

Security

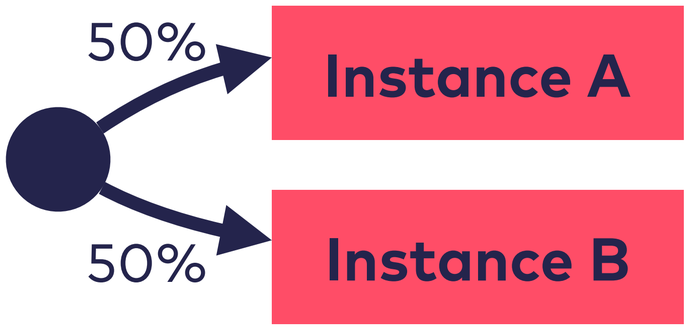
Routing



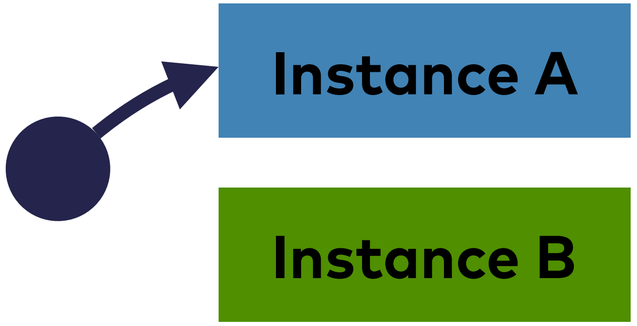
Load Balancing



Pfad-basiertes Routing



A/B-Testing

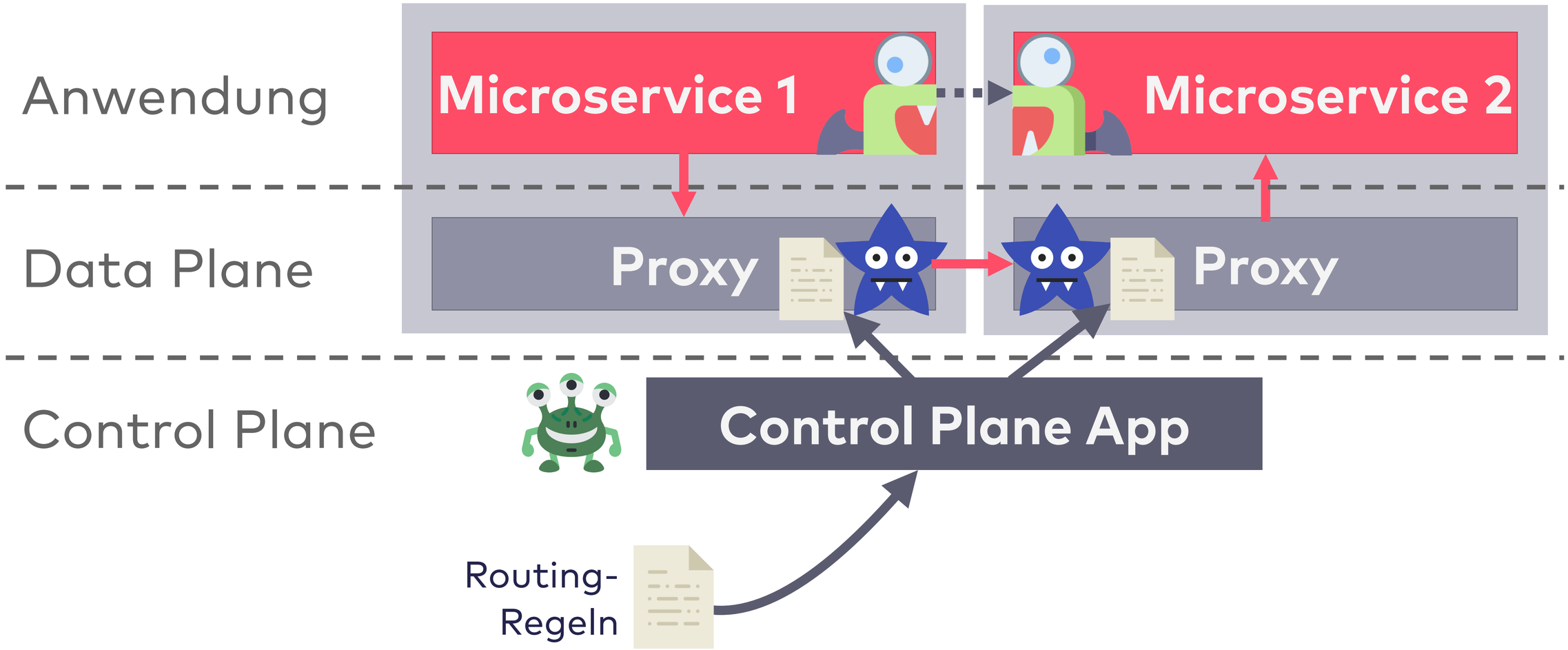


Blue/Green Deployment

Canary Releasing

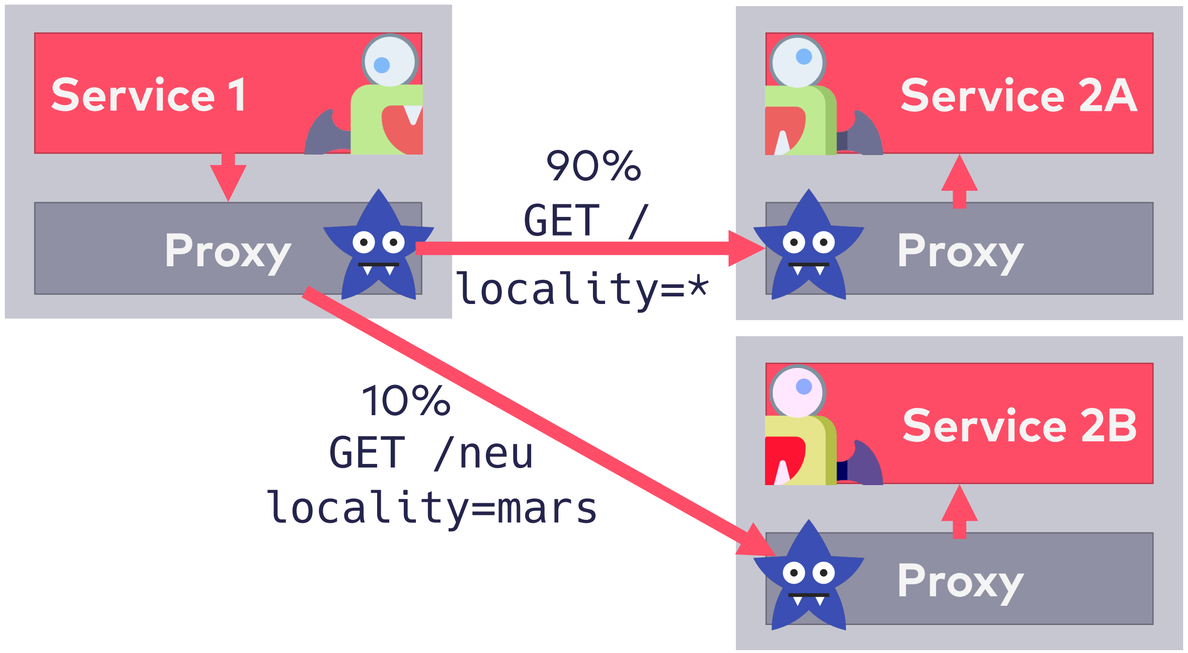
Typischerweise im **Edge Router / API-Gateway** implementiert
z.B. NGINX, Kong, Ambassador, Traefik

Routing mit Service Mesh | Config

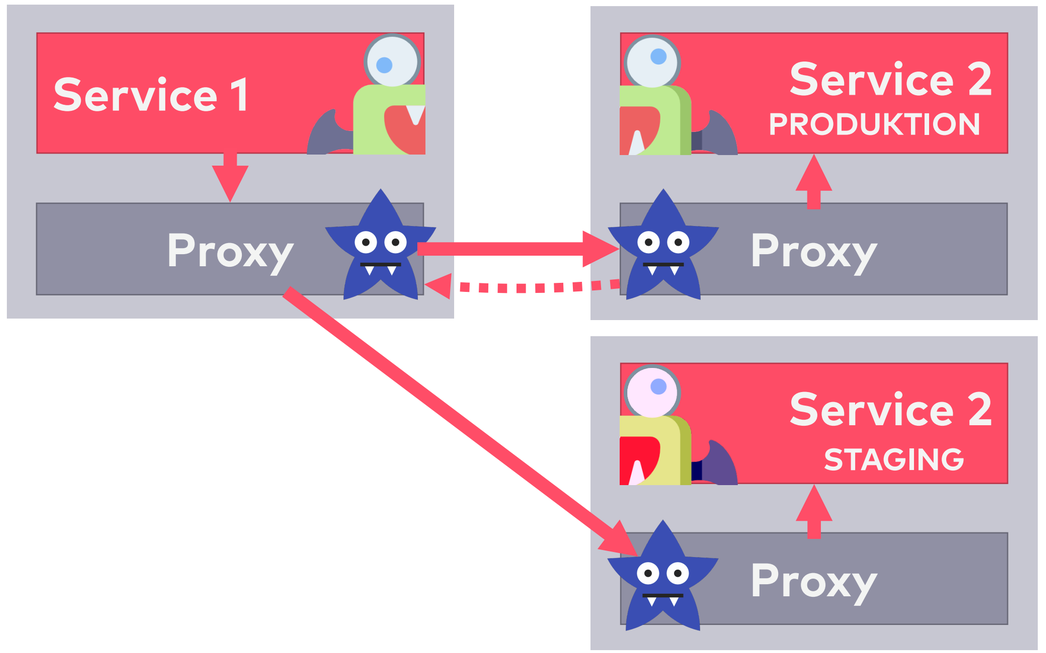


Routing mit Service Mesh

Komplexe Routing-Regeln
für A/B Testing und Canary Releasing

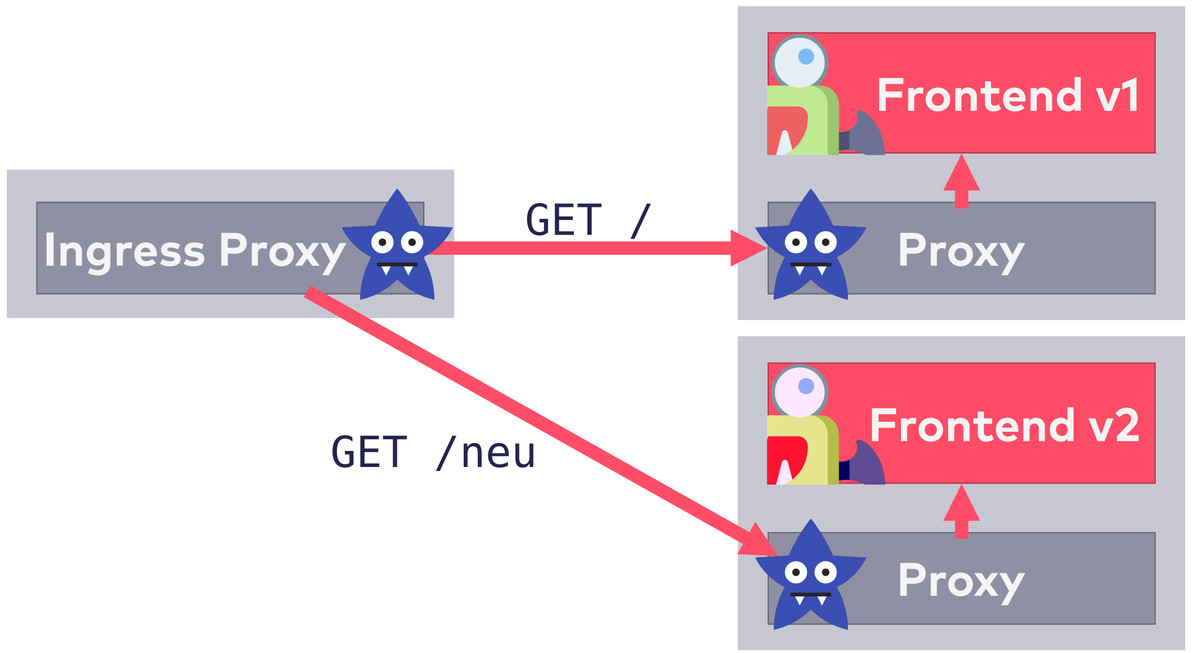


Traffic Mirroring



Routing mit Istio

Beispiel-Routing mit Istio



Routing Config

```yaml
apiVersion: networking.istio.io/…
kind: DestinationRule
metadata:
  name: frontend

spec:
  host: frontend
  subsets:
  - name: v2
    labels:
      version: "2"
  - name: v1
    labels:
      version: "1"
```

Subset "**v2**":
Alle Pods mit Label `version: "2"`

Subset "**v1**":
Alle Pods mit Label `version: "1"`

```yaml
apiVersion: networking.istio.io/…
kind: VirtualService
metadata:
  name: frontend-ingress
spec:
  hosts:
  - "*"
  http:
  - match:
    - uri:
        prefix: "/neu"
    route:
    - destination:
        host: frontend
        subset: v2
  - route:
    - destination:
        host: frontend
        subset: v1
```

Regel 1:
Wenn die **URI** `"/neu"` **enthält**, dann leite an `frontend` **v2** weiter

Regel 2:
Ansonsten leite an `frontend` **v1** weiter

Service Mesh Features

Observability

Routing

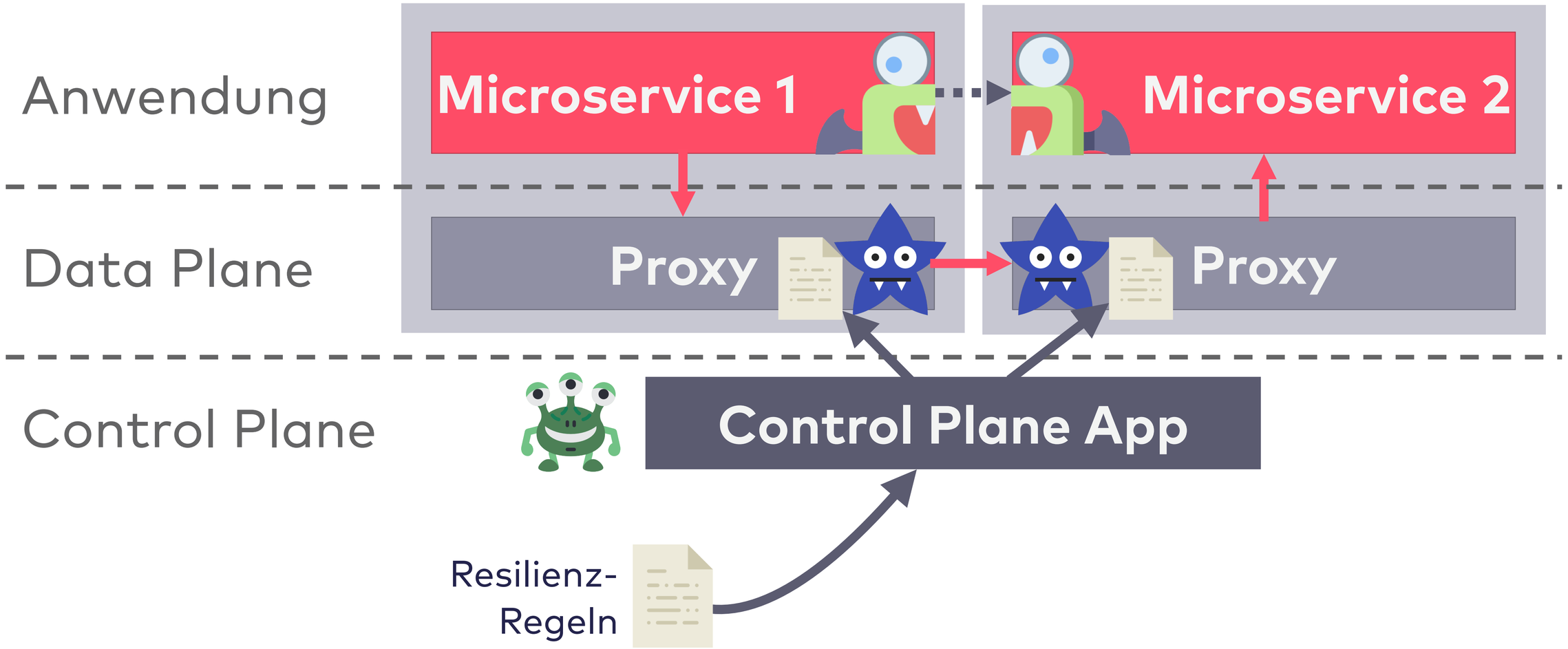
Resilience

Security

Resilience

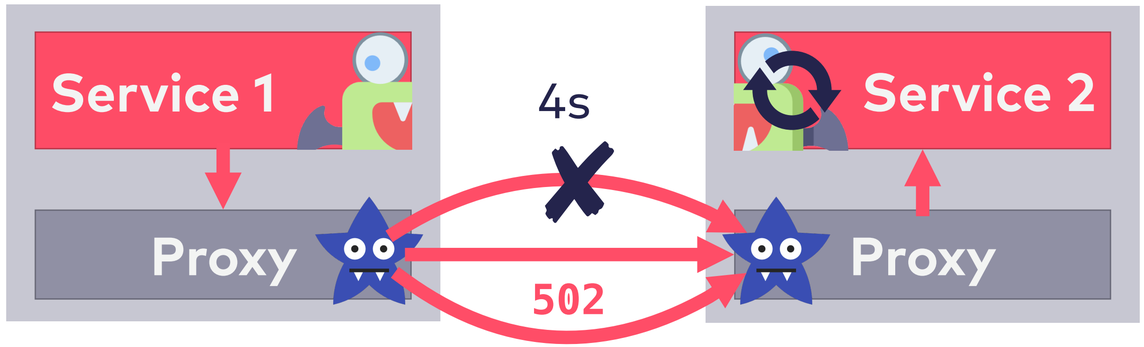
- Was wenn ein Service nicht wie erwartet zur Verfügung steht?
  - Fehler (5xx)
  - Delay
- Ziel: **Gesamtsystem funktioniert weiter**
  - ggf. mit Einschränkungen
- **Resilience-Maßnahmen**: Retry, Timeout, Circuit Breaking

Resilience mit Service Mesh | Config

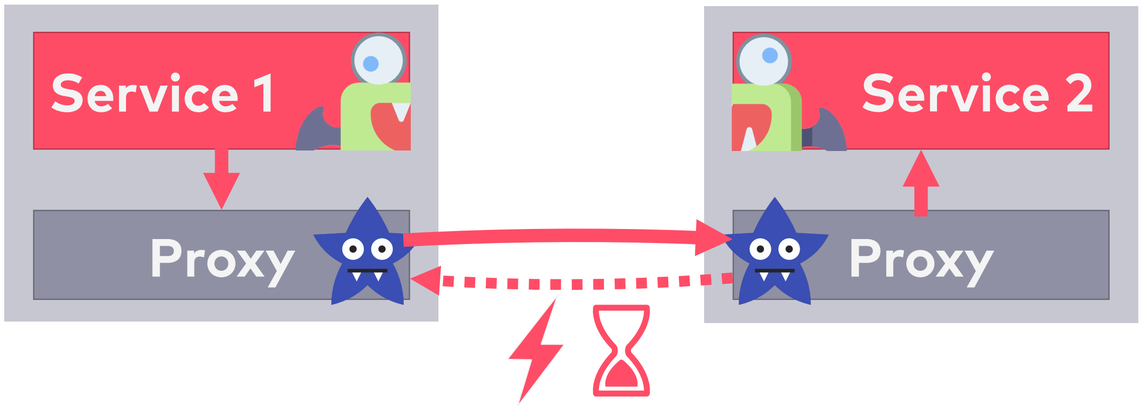


Resilience mit Service Mesh

Timeout
Retry



Fault Injection
Delay Injection



Resilience mit Istio

Timeout & Retry

hosts: Zieladresse des Client-Requests

max. Anzahl der Retrys

Timeout pro Retry

Bedingungen für ein Retry

Timeout für alle Retrys zusammen

destination: Wo der Request tatsächlich hingeht

```yaml
apiVersion: networking.istio.io/...
kind: VirtualService
metadata:
name: order-retry
spec:
  hosts:
  - order
  http:
  - retries:
      attempts: 20
      perTryTimeout: 5s
      retryOn: connect-failure,5x
    timeout: 10s
    route:
    - destination:
        host: order
```

```
wolff@BLACK-HARDWARE:~/win/microservice-istio/microservice-istio-demo$
```

Service Mesh Features

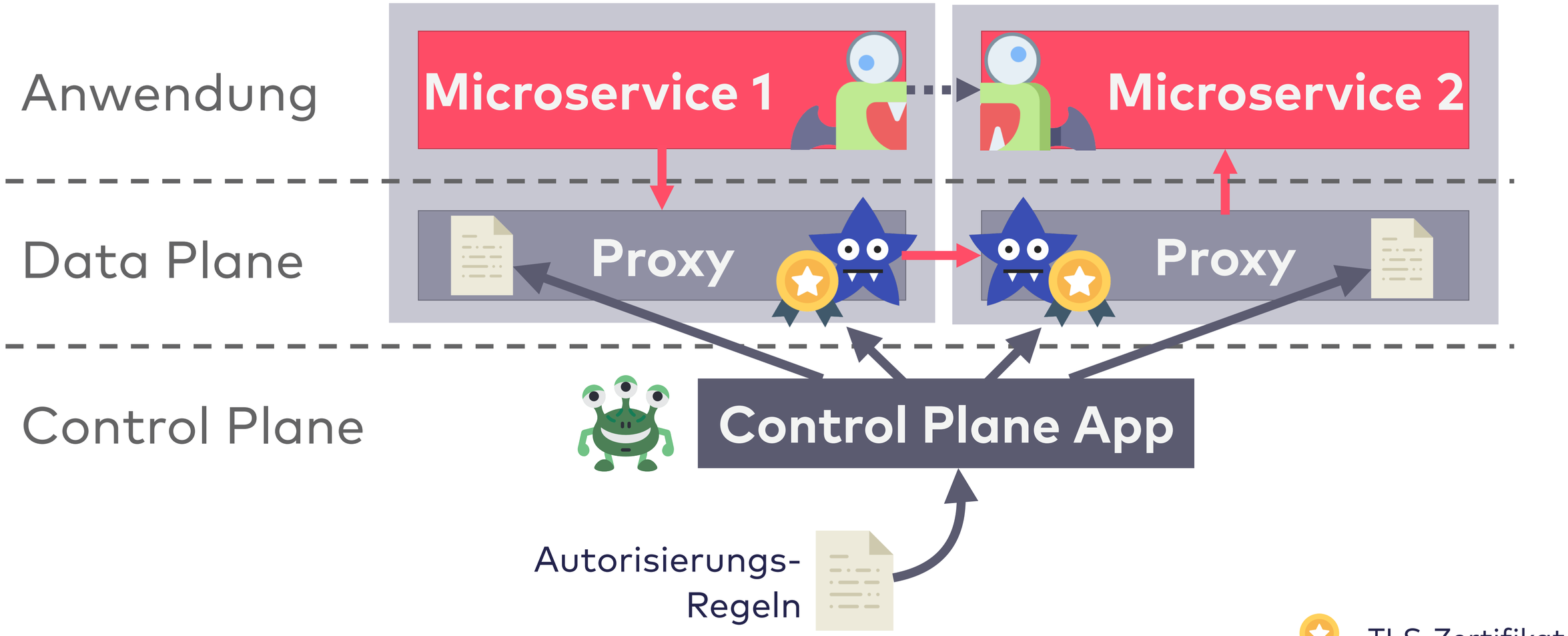
Observability

Routing

Resilience

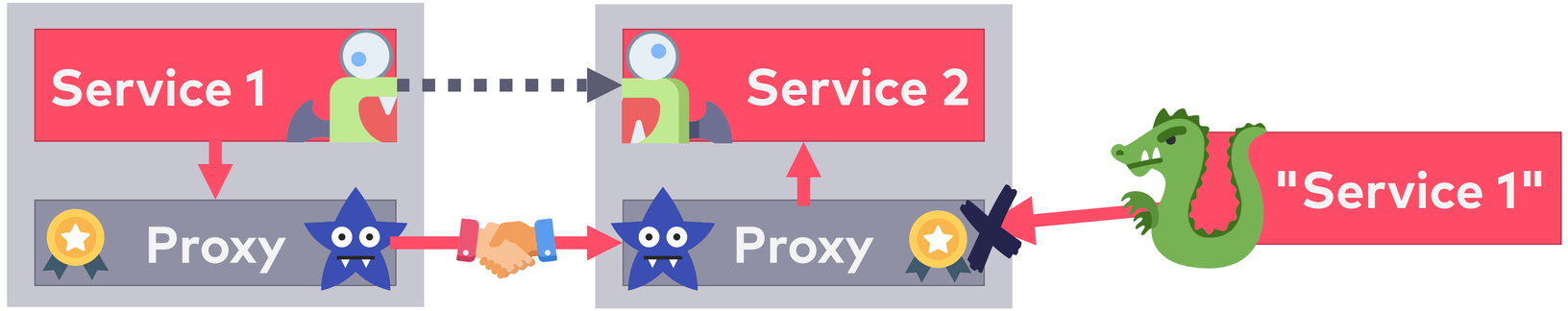
Security

Security mit Service Mesh | Config

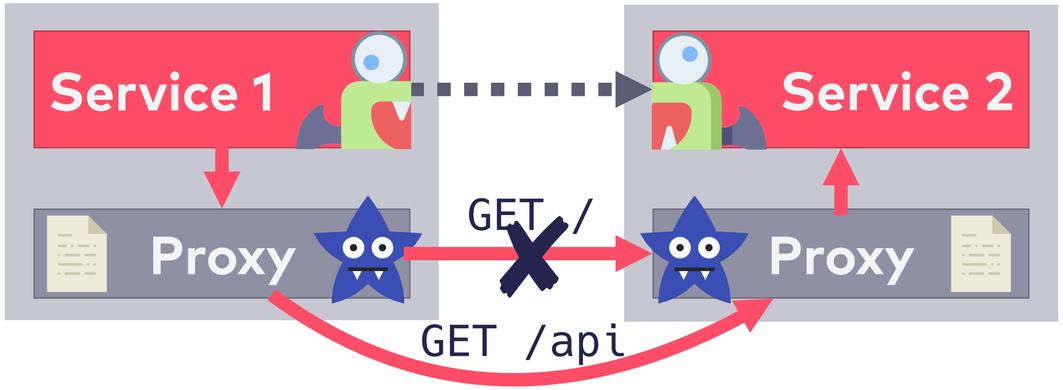


Security mit Service Mesh

Authentifizierung mit mTLS



Autorisierung




TLS-Zertifikat


Autorisierungs-Regel

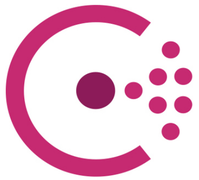
Service Mesh Features

Telemetrie-Metriken und -Logs Daten an Tracing-Backend senden	 Observability	Business-Metriken oder -Logs Weitergabe von Tracing-Headern
Komplexe Routing-Regeln Canary Releasing & A/B-Testing	 Routing	Routing anhand von Request Body Automatisierung Canary Releasing
Automatische Timeouts & Retrys Automatisches Circuit Breaking	 Resilience	Cache oder Standardantworten in Circuit Breaker nutzen
Authentifizierung mit mTLS Autorisierung	 Security	

Service Mesh = Istio?

Service Mesh Implementierungen

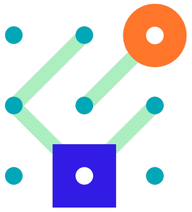
LINKERD



AWS App Mesh

mæsh

Istio



Service
Mesh
Interface

Kuma

Vergleich auf servicemesh.es

Was ist wichtig für die Auswahl eines Service Mesh?

Features

Kompatibilität

Performance

Usability

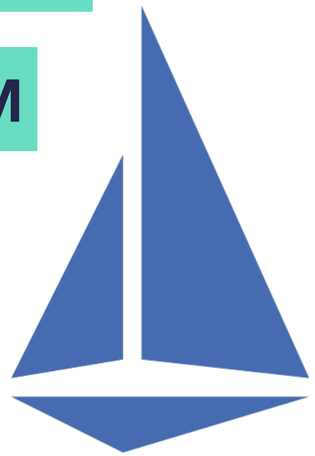
Istio VS Linkerd 2

*2017

von **Google & IBM**

optimiert auf **Featureanzahl** und **Konfigurierbarkeit**

optimiert für Kubernetes, aber nicht exklusiv



*2017

von **Buoyant**

optimiert auf **Usability** und **Performance**

Kubernetes only

Features

		Istio 1.3	Linkerd 2.6
Generell	**Plattform**	Verschiedene	Kubernetes
	Automatische Sidecar-Injektion	✓	✓
Monitoring	**Metriken**	✓	✓
	Tracing	✓	(✓)
	Dashboard mit Service Graph	✓	✓
Routing	**Load Balancing**	✓	✓
	Routing-Regeln	✓	✓
Resilienz	**Timeouts & Retrys**	✓	✓
	Circuit Breaker	✓	✘
Sicherheit	**Authentifizierung via mTLS**	✓	✓
	Autorisierung	✓	✘

Performance & Ressourcen

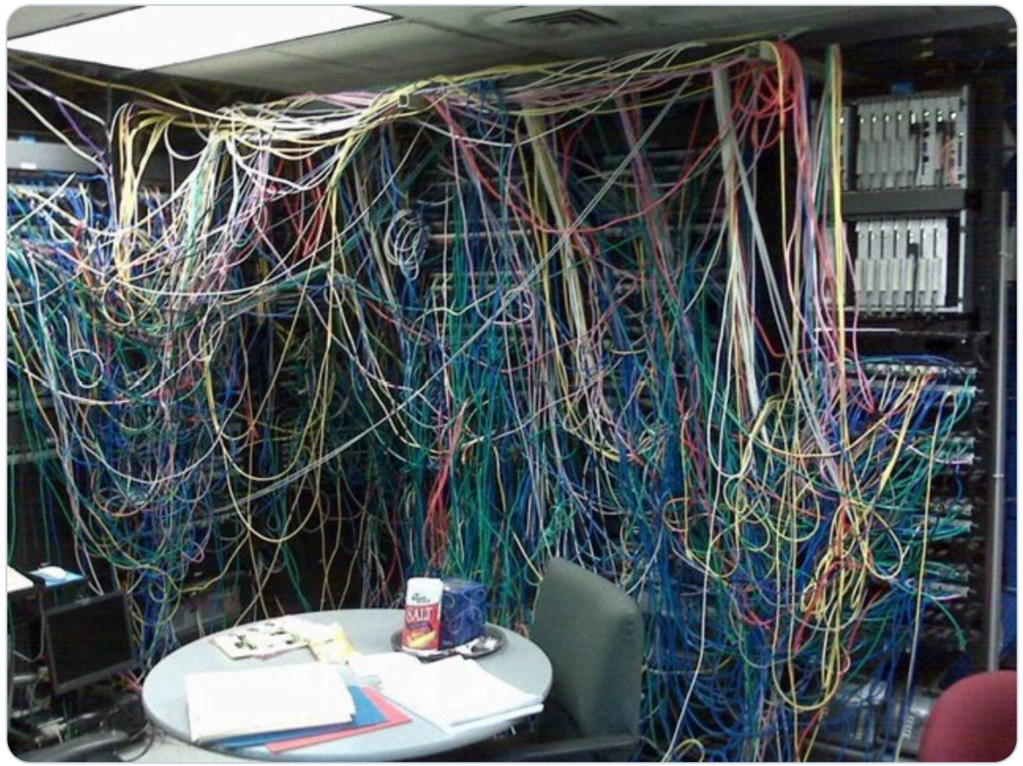
- **Latenz**
  - **Istio**: zusätzlich ca. 8ms Latenz - pro Aufruf zwischen Services!
  - **Linkerd 2**: ähnlich, mit weniger starken Schwankungen
- **Ressourcen**
  - Zusätzliche Container für Control Plane & jedes Sidecar
  - → Erhöhter CPU- & Arbeitsspeicher-Verbrauch

Aber: Abhängig von konkretem Setting
→ eigenen Benchmark machen!

Usability

Dave Strebel
@dave_strebel

"Finally got Istio into production"



2:21 AM · Sep 18, 2019 from Apple Valley, MN · Tweetbot for iOS

322 Retweets **1.2K** Likes

Service Mesh Fazit

+

Löst viele wesentliche Probleme von Microservices

... ohne Codeänderungen!

-

Eine weitere komplexe Technologie

Latenz- und Ressourcen-Overhead

Entscheidungshilfe

Mesh oder kein Mesh?

- **Service Mesh** wenn:
  - Großteil in Kubernetes läuft
  - Viele Microservices, viele synchrone Aufrufe
  - Viele ungelöste Probleme beim Monitoring, Routing, Resilienz und/oder Security

Istio oder Linkerd 2?

- **Istio nur** wenn Komplexität und Flexibilität nötig ist:
  - Teilsystem bleibt außerhalb von Kubernetes
  - Circuit Breaking und Autorisierung unverzichtbar
  - Ausreichend zeitliche und kognitive Kapazität im Team

Mehr Mesh

- Artikel Brauchen asynchroner Microservices und Self-Contained-Systems ein Service Mesh?
- Artikel Alle 11 Minuten verliebt sich ein Microservice in Linkerd
- Service Mesh Vergleich auf servicemesh.es
- Podcast zu Service Meshes
- Beispiel-Anwendung auf GitHub
- Tutorial von Linkerd
- Tutorial von Istio

Kostenloser Service Mesh Primer auf
leanpub.com/service-mesh-primer

... oder gedruckt am INNOQ-Stand!

Danke! Fragen?

Hanna Prinz
hanna.prinz@innoq.com
@HannaPrinz

INNOQ
www.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