

Abstract geometric lines in the top-left corner of the slide, consisting of several thin black lines forming overlapping, irregular shapes.

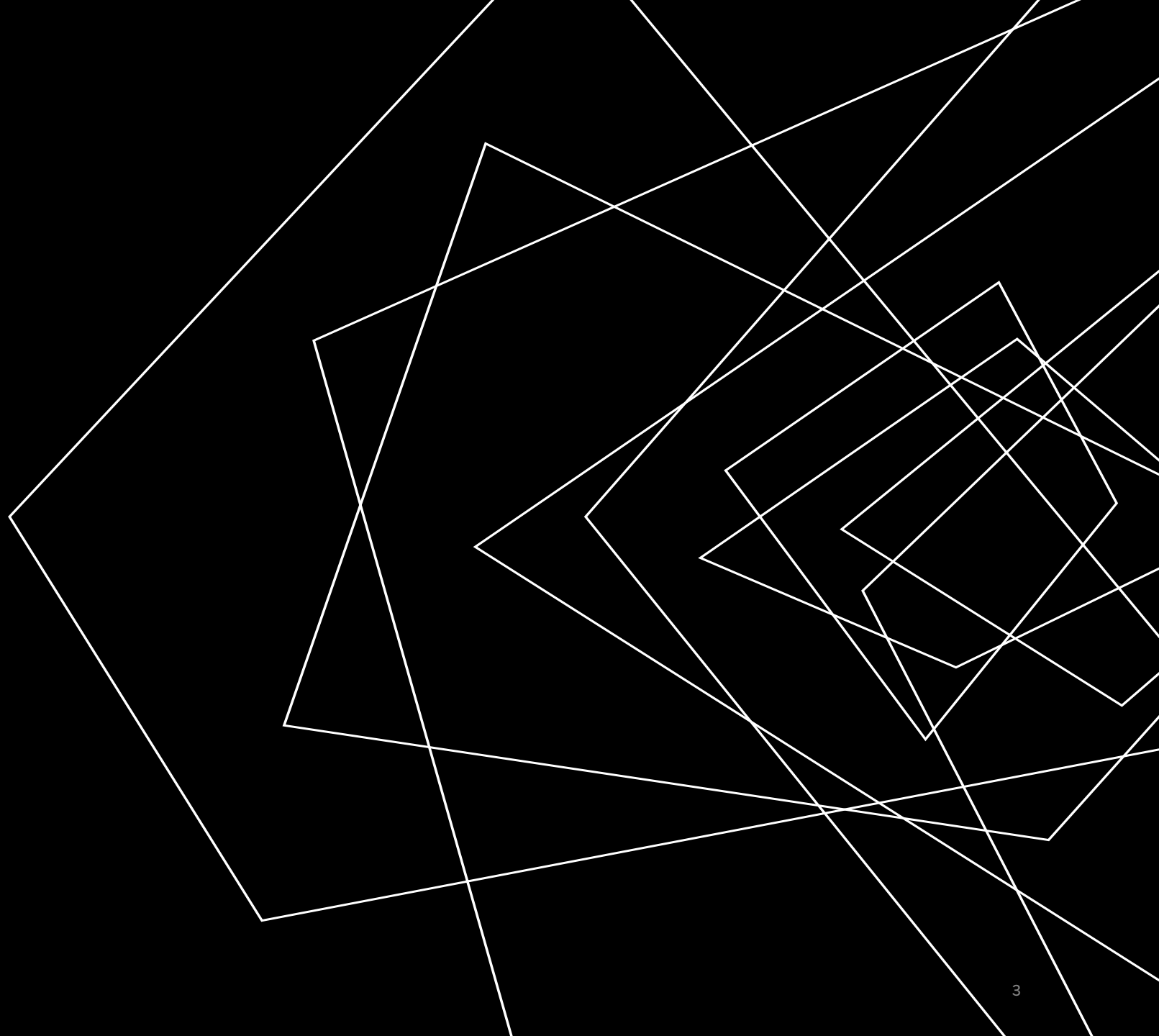
- TRAINY (KBS610)-
NON-AI-PRO
CLOUD SERVICES

GLIEDERUNG

- 1. Was ist Trainy**
- 2. Vorgehensweise**
- 3. Unsere Infrastruktur**
- 4. Probleme und Entscheidungen**
- 5. Live Demo**

TRAINY

Was ist Trainy?





TRAINY

- Check-in-Dienst für ÖP(N)V
- Fahrten loggen, z.B. für Dienstreisen oder persönliche Statistiken
- Globaler Feed mit allen öffentlichen Check-Ins



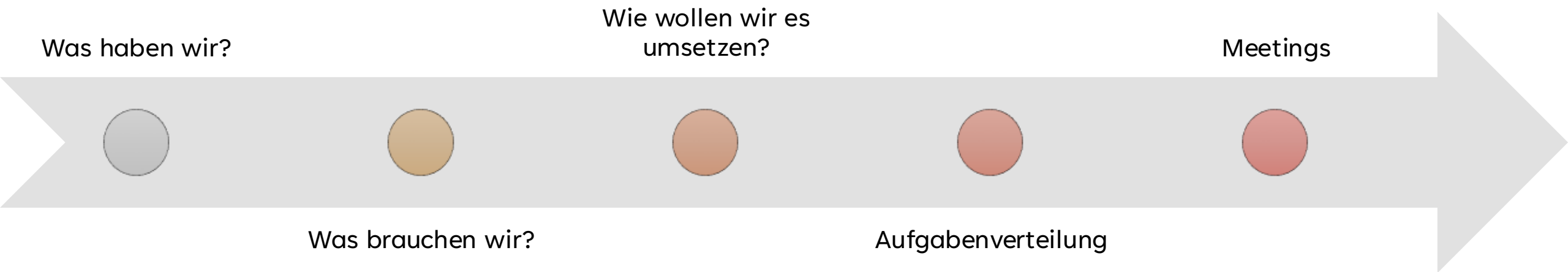
TRAINY

- Custom Backend
- Custom Worker
- Postgres
- Dragenfly (Redis)
- MongoDB
- RabbitMQ

VORGEHENSWEISE

Welche Gedanken haben
wir uns gemacht?

VORGEHENSWEISE



INFRASTRUKTUR

Welche Besonderheiten hat
unsere Infrastruktur

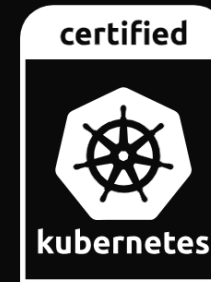
Talos

```
talos-controlplane-0 (v1.12.2): uptime 96h13m15s, 2x2.5GHz, 3.8 GiB RAM, PROCS 34, CPU 24.2%, RAM 52.9%

UUID      82445e55-2702-4513-a163-f97bb7a0b681 TYPE      controlplane HOST      talos-controlplane-0
CLUSTER   talos-controlplane-0 (6 machines) KUBERNETES v1.35.0   IP        192.168.2.97/24
SIDEROLINK n/a KUBELET    J Healthy  GW        192.168.2.1
STAGE     J Running APISERVER  J Healthy  CONNECTIVITY J OK
READY     J True   CONTROLLER-MANAGER J Healthy  DNS        8.8.8.8, 8.8.4.4
SECUREBOOT x False SCHEDULER  J Healthy  NTP        time.cloudflare.com

Logs
user: warning: [2026-02-06T20:08:39.283806259Z]: [talos] service[trustd](Running): Health check successful
user: warning: [2026-02-06T20:08:39.322027259Z]: [talos] service[cril](Running): Health check successful
user: warning: [2026-02-06T20:08:39.324596259Z]: [talos] service[etcd](Preparing): Running pre state
user: warning: [2026-02-06T20:08:39.325607259Z]: [talos] service[ext-cloudflared](Preparing): Running pre state
user: warning: [2026-02-06T20:08:39.328744259Z]: [talos] service[kubelet](Preparing): Running pre state
user: warning: [2026-02-06T20:08:39.329939259Z]: [talos] service[ext-cloudflared](Preparing): Creating service runner
user: warning: [2026-02-06T20:08:39.381971259Z]: [talos] service[kubelet](Preparing): Creating service runner
user: warning: [2026-02-06T20:08:39.384831259Z]: [talos] service[etcd](Preparing): Creating service runner
user: warning: [2026-02-06T20:08:39.502086259Z]: [talos] service[ext-cloudflared](Running): Started task ext-cloudflared (PID 2208) for container ext-cloudflared
kern: notice: [2026-02-06T20:08:39.513590259Z]: XFS (vda1): Mounting U5 Filesystem 16309966-831b-4fd5-b411-d8ba7fc8e925
kern: info: [2026-02-06T20:08:39.531815259Z]: XFS (vda1): Ending clean mount
user: warning: [2026-02-06T20:08:39.537540259Z]: [talos] volume mount {"component": "controller-runtime", "controller": "block.MountController", "volume": "STATE", "source": "/dev/vda1", "target": "/system/state", "filesystem": "xfs", "read_only": false, "detached": true}
kern: notice: [2026-02-06T20:08:39.564790259Z]: XFS (vda1): Unmounting Filesystem 16309966-831b-4fd5-b411-d8ba7fc8e925
user: warning: [2026-02-06T20:08:39.597034259Z]: [talos] volume unmount {"component": "controller-runtime", "controller": "block.MountController", "volume": "STATE", "source": "/dev/vda1", "target": "/system/state", "filesystem": "xfs"}
user: warning: [2026-02-06T20:08:39.697284259Z]: [talos] service[etcd](Running): Started task etcd (PID 2302) for container etcd
user: warning: [2026-02-06T20:08:39.725277259Z]: [talos] service[kubelet](Running): Started task kubelet (PID 2301) for container kubelet
user: warning: [2026-02-06T20:08:41.387520259Z]: [talos] service[kubelet](Running): Health check successful
user: warning: [2026-02-06T20:08:46.452429259Z]: [talos] service[etcd](Running): Health check successful
user: warning: [2026-02-06T20:08:46.453611259Z]: [talos] task startAllServices (1/1): done, 8.366818231s
user: warning: [2026-02-06T20:08:46.459225259Z]: [talos] phase startEverything (9/9): done, 8.368682748s
user: warning: [2026-02-06T20:08:46.467756259Z]: [talos] boot sequence: done: 8.82249034s
user: warning: [2026-02-06T20:08:46.468469259Z]: [talos] rendered new static pod {"component": "controller-runtime", "controller": "k8s.StaticPodServerController", "id": "kube-apiserver"}
user: warning: [2026-02-06T20:08:46.471061259Z]: [talos] rendered new static pod {"component": "controller-runtime", "controller": "k8s.StaticPodServerController", "id": "kube-controller-manager"}
user: warning: [2026-02-06T20:08:46.472671259Z]: [talos] rendered new static pod {"component": "controller-runtime", "controller": "k8s.StaticPodServerController", "id": "kube-scheduler"}
user: warning: [2026-02-06T20:09:30.468197259Z]: [talos] controller failed {"component": "controller-runtime", "controller": "k8s.NodeApplyController", "error": "1 error(s) occurred:\n\ttimeout"}
user: warning: [2026-02-06T20:09:43.144167259Z]: [talos] machine is running and ready {"component": "controller-runtime", "controller": "runtime.MachineStatusController"}

[local] --- [Summary] --- [F2: Monitor]
```



Talos Linux is a Certified Kubernetes
distribution

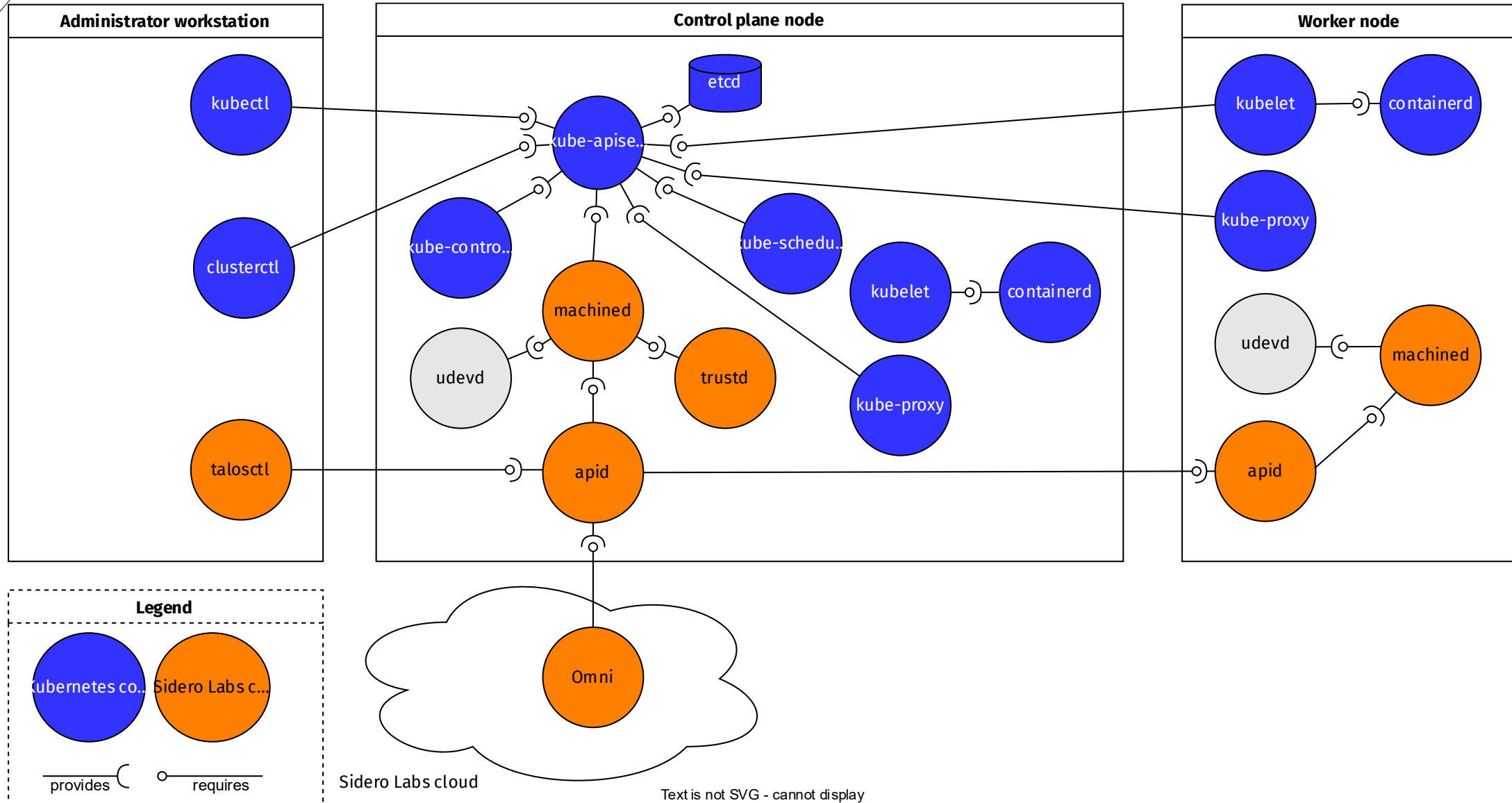


Sidero is a proud CNCF member

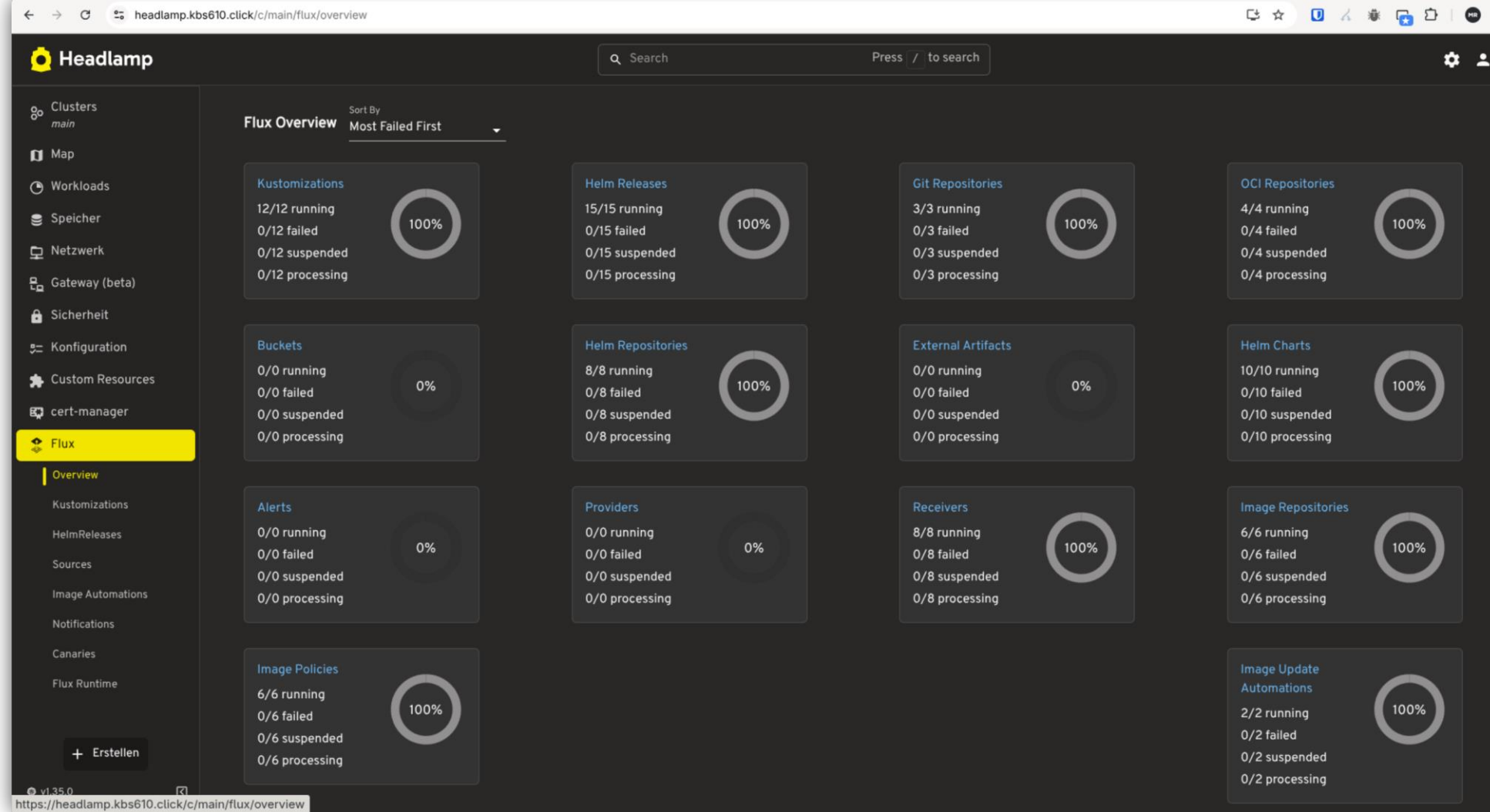


TALOS LINUX

Talos



FLUXCD



FluxCD

Source

Definiert Quellen

- HelmRepository/OCIRepository
- HelmChart
- GitRepository
- Bucket (S3)

Helm & Kustomize

Vergleichbar mit ArgoCD Projekten

- Besitzt Referenz zu einer Source
- Können verschlüsselt sein
- Im selben Namespace wie Bestandteile

Image

Image Update automation

- ImageRepository
- ImagePolicy
- ImageUpdateAutomation

Notification

Definiert Kommunikationspunkte

- Alerts
- Providers
- Receivers

Gateway API



Gateway API

Was ist die Gateway API?

- Nachfolger der Ingress-Ressource
- Soll Ingress langfristig ersetzen
- Regelt das Routing von externem Traffic zu Services im Cluster

Warum die Gateway API?

- Empfehlung eines EA-Mitarbeiters
- Rollenbasiert: Gateway vs. HTTPRoute

Gateway API

GatewayClass

Definiert den Controller Typ

- Verweist auf den Gateway-Controller

Gateway

Konfiguriert Listener (Ports, TLS)

- Bindet an eine GatewayClass
- Definiert Listener (Port 80, 443, ...)

HTTPRoute

Definiert den Controller Typ

- Matched auf Host, Path, Header
- Verweist auf Backend-Services

Gateway API

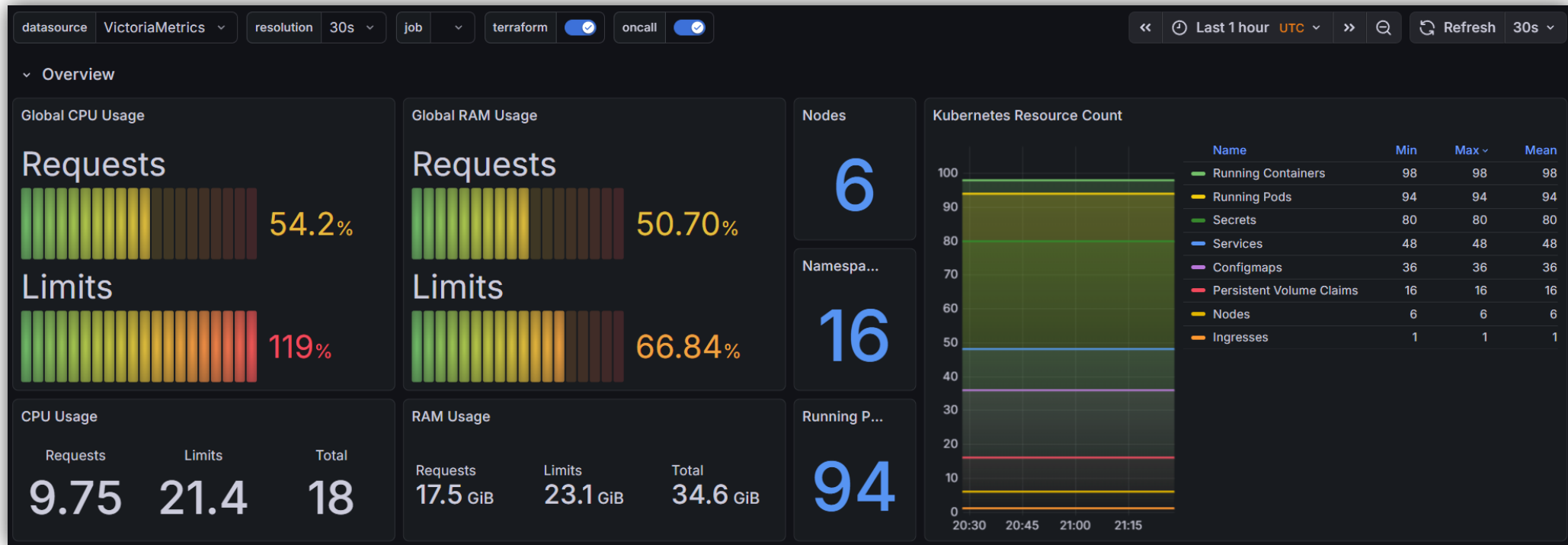
```
apiVersion: gateway.networking.k8s.io/v1
kind: Gateway
metadata:
  name: cloudflare
  namespace: ingress
  annotations:
    cert-manager.io/issuer: cloudflare
    cert-manager.io/issuer-kind: ClusterOriginIssuer
    cert-manager.io/issuer-group: cert-manager.k8s.cloudflare.com
spec:
  gatewayClassName: traefik

  listeners:
    - name: web
      hostname: "*.kbs610.click"
      port: 80
      protocol: HTTP
      allowedRoutes:
        namespaces:
          from: All
    - name: websecure
      hostname: "*.kbs610.click"
      port: 443
      protocol: HTTPS
      allowedRoutes:
        namespaces:
          from: All
      tls:
        mode: Terminate
        certificateRefs:
          - name: cloudflare-cert
```

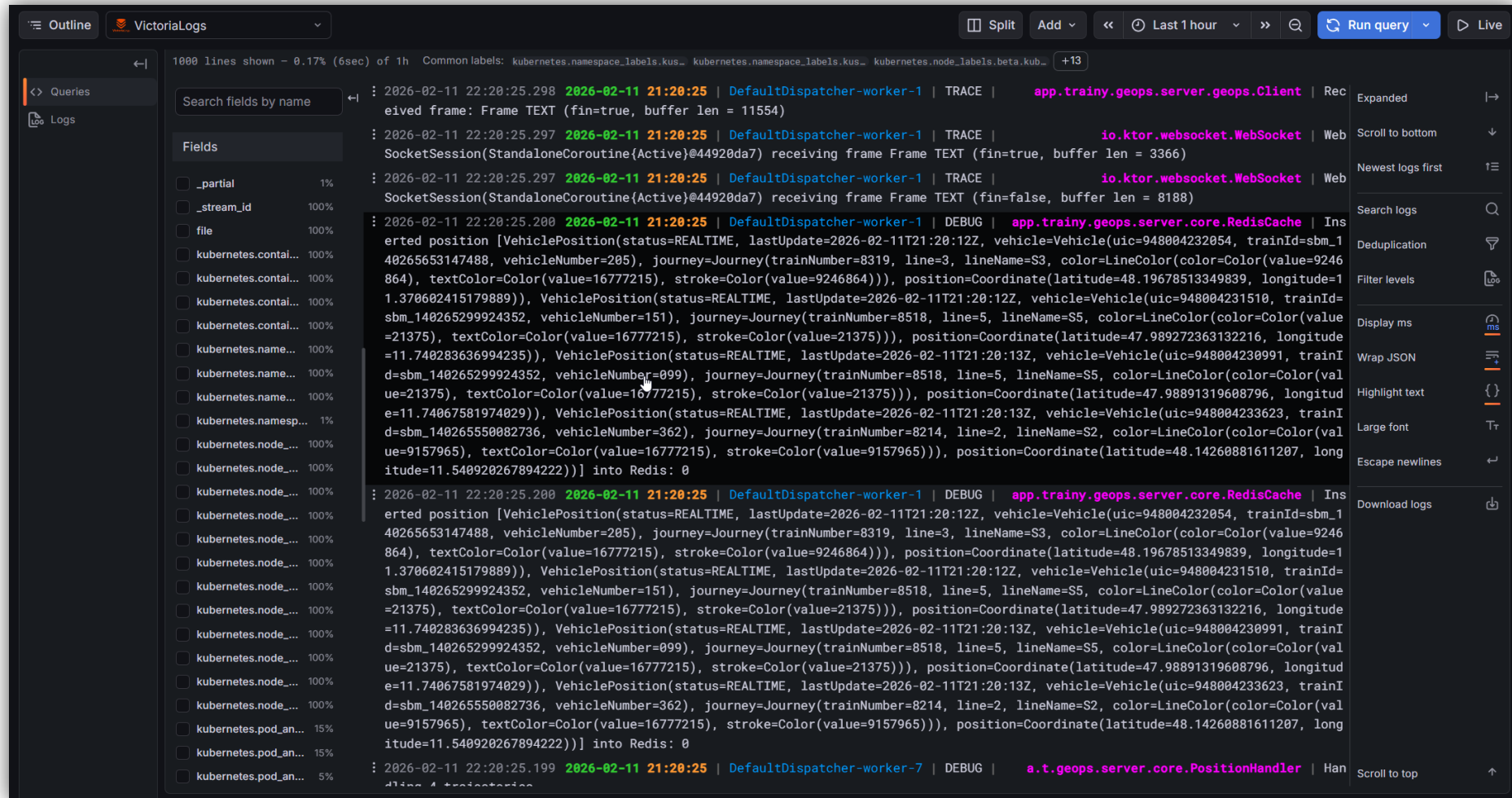


```
kind: HTTPRoute
apiVersion: gateway.networking.k8s.io/v1
metadata:
  name: trainy
spec:
  parentRefs:
    - name: cloudflare
      namespace: ingress
  hostnames:
    - "rbc.kbs610.click"
  rules:
    - backendRefs:
        - name: trainy-service
          port: 8080
```


Grafana mit Victoria Metrics



Grafana mit Victoria Logs



GitLab of the RWTH Aachen University

Willkommen beim GitLab der RWTH Aachen!

Angehörige der RWTH Aachen (Studierende und Mitarbeitende), sowie Angehörige von Universitäten aus dem NFDI4Ing nutzen bitte ausschließlich den **DFN AAI Single Sign-On** und wählen im darauffolgenden Fenster ihre Heimatuniversität aus. Nur über den Login über den Single Sign-On besteht die Möglichkeit, Projekte und Gruppen anzulegen.

Externe Nutzende können sich über **GitHub** authentifizieren, können aber keine Gruppen und Projekte anlegen.

Sie befinden sich auf der GitLab Instanz *git-ce.rwth-aachen.de* der RWTH Aachen University. Weitere Informationen zur Unterscheidung der GitLab Instanzen finden Sie auf unseren Hilfeseiten.

- [Nutzungsbedingungen](#)
- [Nutzungsberechtigungen](#)
- [IT Center Help - GitLab](#)

Weitere Informationen zum Dienst finden Sie im [Dokumentationsportal des IT Centers](#)

Welcome to the GitLab of the RWTH Aachen University!


Members of the RWTH Aachen University (students and staff) please only use the **DFN AAI Single Sign-On** and select the RWTH Aachen University in the following window. Only then will users be able to create projects and groups. External users can authenticate via **GitHub**, but cannot create groups and projects.

You are on the GitLab instance *git-ce.rwth-aachen.de* of RWTH Aachen University. For more information on how to distinguish between GitLab instances, please see our help pages.

- [Terms of Use](#)
- [Usage Permissions](#)
- [IT Center Help - GitLab](#)

For further information about the GitLab service please visit the [documentation portal of the IT Center](#)

Mit deiner Anmeldung akzeptierst du die [Nutzungsbedingungen](#) und erkennst die [Datenschutz-](#) und [Cookie-Richtlinien](#) an.

 GitHub

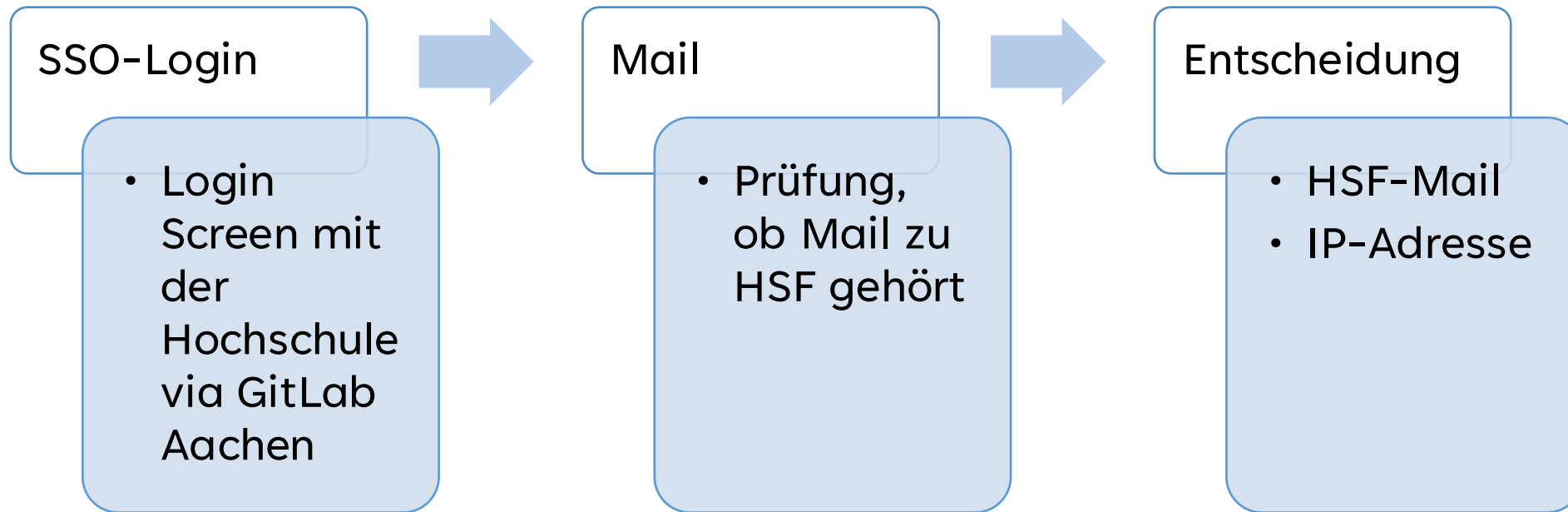
DFN-AAI Single Sign-On

☐ Login merken

SSO IM CLUSTER

- **Generell zur Anmeldung im Netzwerk**
- **Intern zu verschiedenen Tools: Whitelist relevant**
- **Headlamp: Mitglied GitLab Gruppe**
- **Grafana: GitLab Gruppe für Admin**

SSO IM CLUSTER

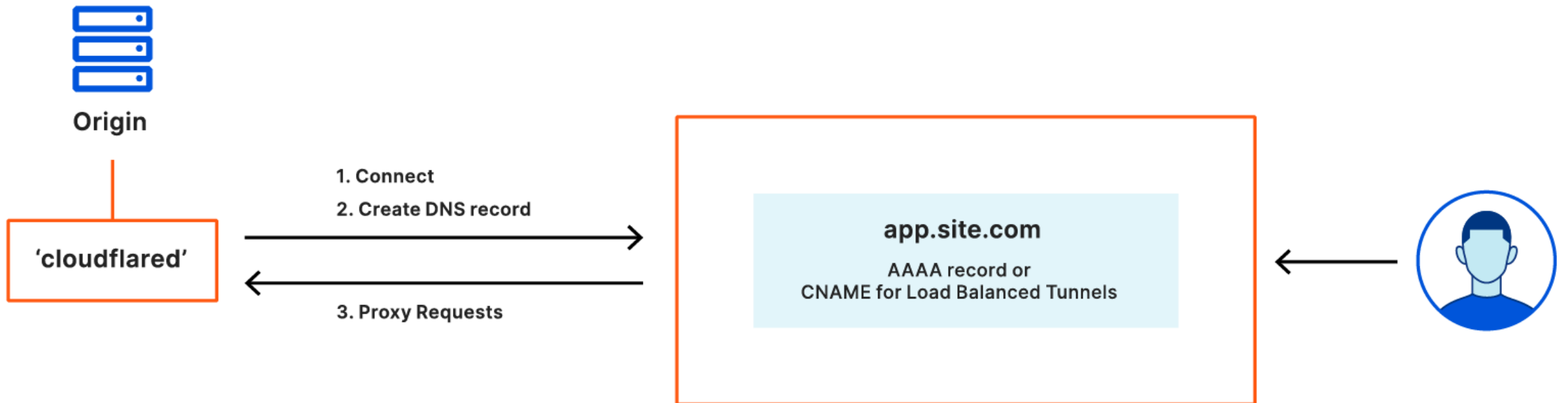


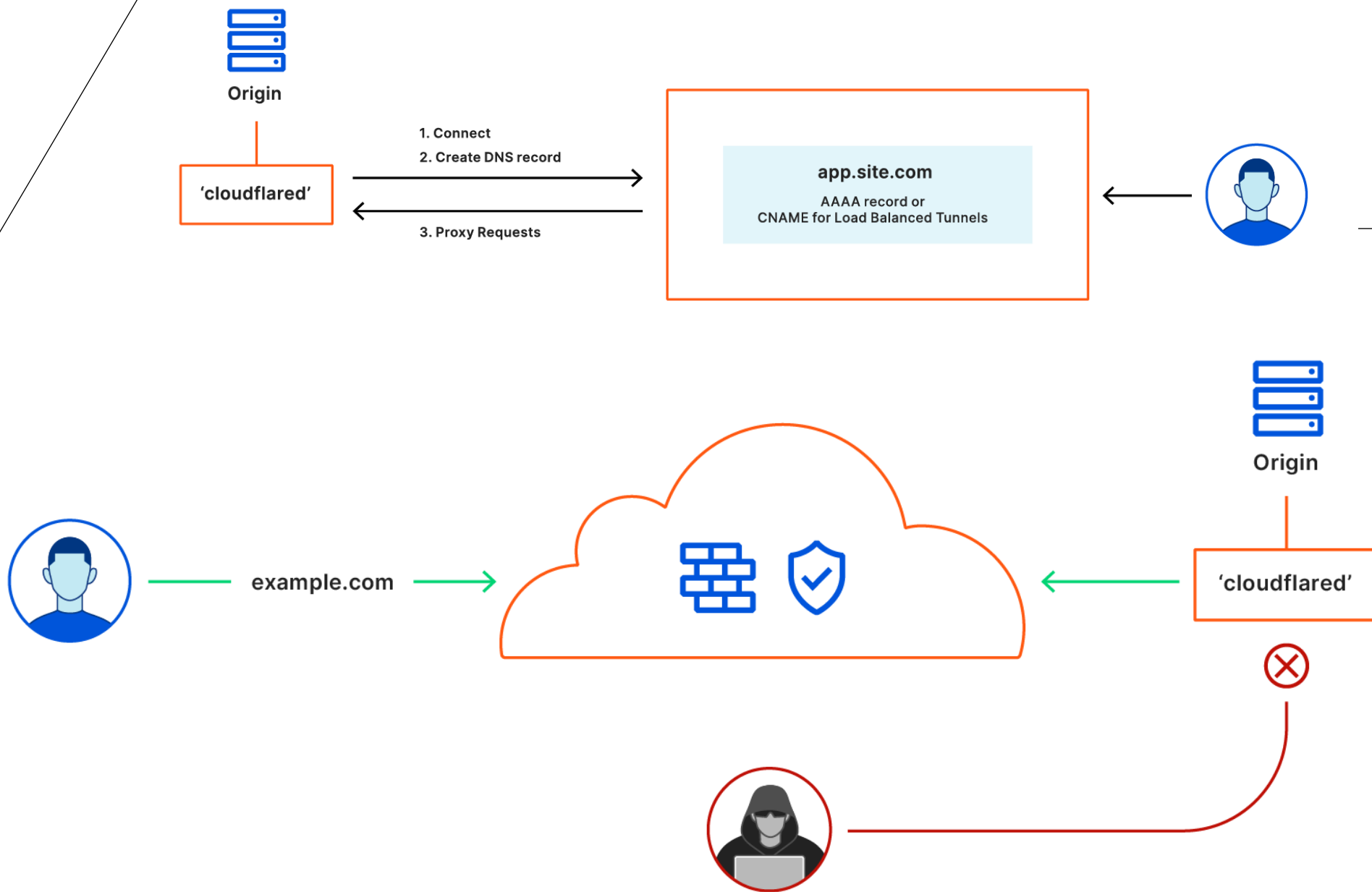


CLOUDFLARE

CLOUDFLARE

- **Cloudflare Argo Tunnel – Externer Zugriff**
- **Sicherheit**
- **Versteckte IP-Adresse**
- **Verbesserte Performance**






PROBLEME ENTSCHEIDUNGEN

Welche Probleme und
welche Entscheidungen
wurden getroffen?


RESSOURCENVERTEILUNG

6 Einträge werden angezeigt

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	talos-worker-2	Talos	192.168.2.55, 10.32.7.76	m1.large
<input type="checkbox"/>	talos-worker-1	Talos	192.168.2.95, 10.32.6.234	m1.large
<input type="checkbox"/>	talos-worker-0	Talos	192.168.2.135, 10.32.7.226	m1.large
<input type="checkbox"/>	talos-controlplane-1	Talos	192.168.2.202, 10.32.6.132	m1.small
<input type="checkbox"/>	talos-controlplane-2	Talos	192.168.2.200, 10.32.7.122	m1.small
<input type="checkbox"/>	talos-controlplane-0	Talos	192.168.2.97, 10.32.6.57	m1.small

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk
> m1.small	1	2 GB	20 GB	20 GB	0 GB
> m1.large	4	 8 GB	80 GB	80 GB	0 GB

RESSOURCENVERTEILUNG

 **Lele1409** 06.02.26, 20:55
hmm

API Server - Health Status

192.168.2.200:6443	UP
192.168.2.202:6443	DOWN
192.168.2.97:6443	DOWN

API Server - HTTP Requests by code

Deprecation version v1

API Server

RESSOURCENVERTEILUNG

6 Einträge werden angezeigt

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	talos-worker-2	Talos	192.168.2.55, 10.32.7.76	m1.large
<input type="checkbox"/>	talos-worker-1	Talos	192.168.2.95, 10.32.6.234	m1.large
<input type="checkbox"/>	talos-worker-0	Talos	192.168.2.135, 10.32.7.226	m1.large
<input type="checkbox"/>	talos-controlplane-1	Talos	192.168.2.202, 10.32.6.132	m1.medium
<input type="checkbox"/>	talos-controlplane-2	Talos	192.168.2.200, 10.32.7.122	m1.medium
<input type="checkbox"/>	talos-controlplane-0	Talos	192.168.2.97, 10.32.6.57	m1.medium

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk
➤ m1.medium	2	4 GB	40 GB	40 GB	0 GB

RESSOURCENVERTEILUNG

Übersicht Kontingente

Compute



Instanzen

Benutzt 6 von 10



VCPUs

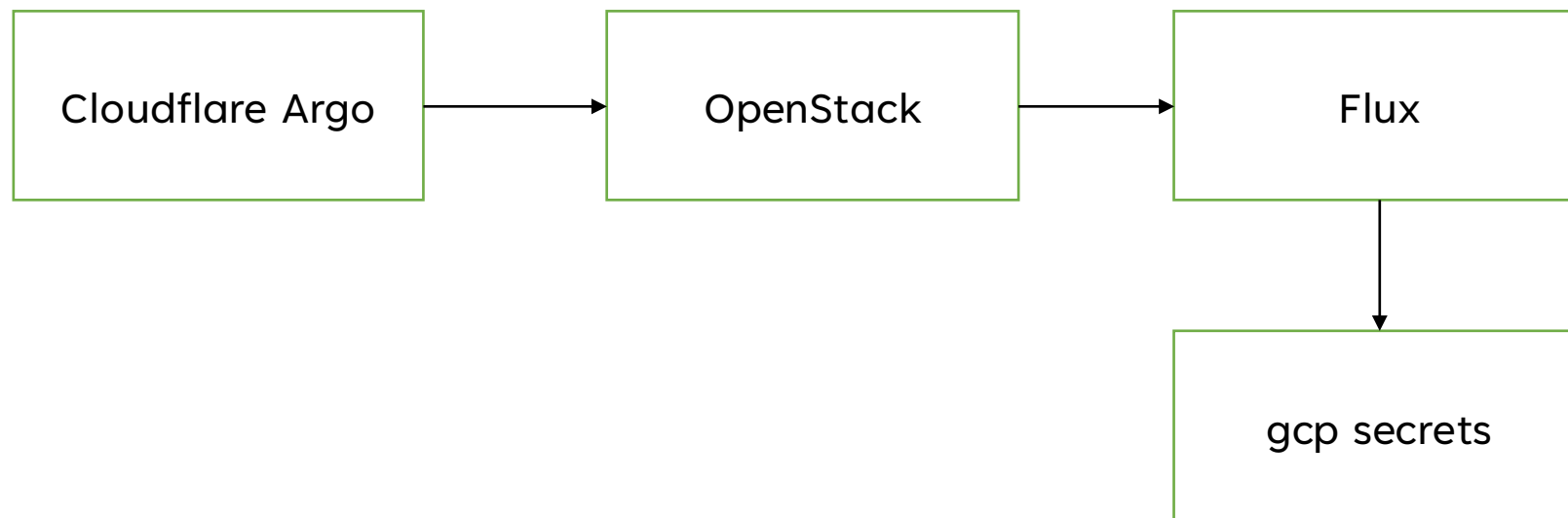
Benutzt 18 von 30



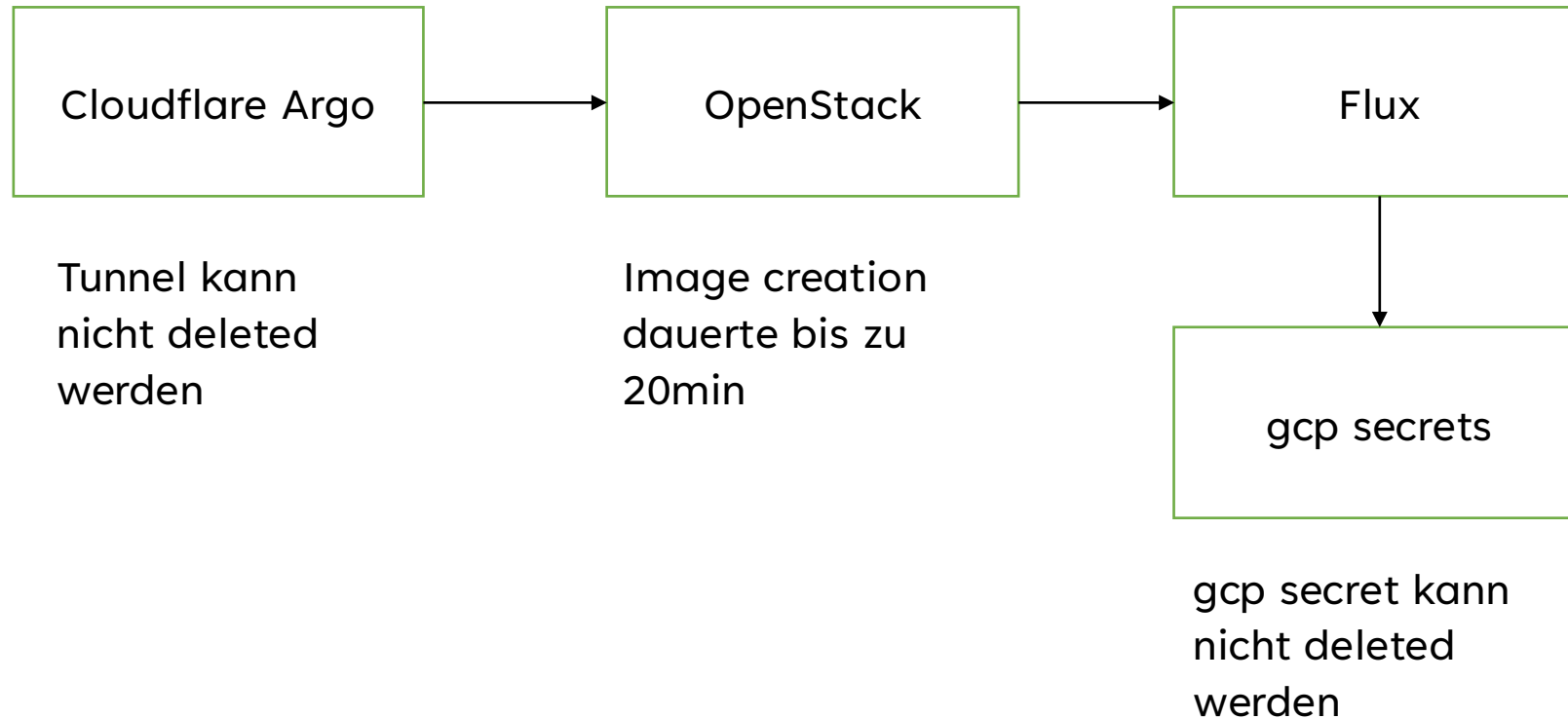
RAM

Benutzt 36GB von 40GB

TERRAFORM MODULES



TERRAFORM MODULES - PROBLEME



```
15  
16 resource "google_iam_workload_identity_pool" "kubernetes" {  
17     # Deleting just marks them as deleted, but they actually still exist, so we need to rename it each time  
18     workload_identity_pool_id = "kubernetes-v12"  
19 }  
20
```

KUSTOMIZATIONS

Kustomizations		12 items		All namespaces		Search Kustomizat	
<input type="checkbox"/>	Name	Namespace	Source	Revision	Resumed	Condition	Status
<input type="checkbox"/>	cloudflare-orign-ca-crds	ingress	cloudflare-orign-ca	trunk@sha1:77fabb29a04c0188e...	True	Ready	Applied revision: trunk@sha1:77fabb29...
<input type="checkbox"/>	flux-system	flux-system	flux-system	main@sha1:2d63ede7fab4a9ef8...	True	Ready	Applied revision: main@sha1:2d63ede...
<input type="checkbox"/>	grafana	grafana	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'operators/operators' is no...
<input type="checkbox"/>	headlamp	headlamp	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'ingress/ingress' is not rea...
<input type="checkbox"/>	ingress	ingress	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'kube-system/kube-system...
<input type="checkbox"/>	ingress-config	ingress	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'flux-system/secrets' is no...
<input type="checkbox"/>	kube-system	kube-system	flux-system	main@sha1:2d63ede7fab4a9ef8...	True	Ready	Applied revision: main@sha1:2d63ede...
<input type="checkbox"/>	operators	operators	flux-system	main@sha1:2d63ede7fab4a9ef8...	True	Ready	Applied revision: main@sha1:2d63ede...
<input type="checkbox"/>	rabbitmq-operator	rabbitmq-system	rabbitmq-operator	v2.19.1@sha1:231b13db9070e9d...	True	Ready	Applied revision: v2.19.1@sha1:231b1...
<input type="checkbox"/>	secrets	flux-system	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'flux-system/flux-system' r...
<input type="checkbox"/>	trainy	trainy	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'ingress/ingress' is not rea...
<input type="checkbox"/>	victoria-metrics	victoria-metrics	flux-system	main@sha1:89e0fd4752aed75e1...	True	Not Ready	dependency 'ingress/ingress' is not rea...

FLUX HELM CONTROLLER

Helm Install

Timeout von 5 Minuten

=> Helm Controller killen



Delete Pod **flux-system/helm-controller-645dcb7d8d-5x875** from **admin@talos-controlplane-0?**

Cancel

Delete

LIVE DEMO

Unsere Anwendung in live

- Trainy (Handy Stream)
- [Grafana](#)
- Freelens

