

Kubernetes



Chemnitzer Linux Tage 2025

Thomas Güttler, Sysself

[Samstag, 11:00 - Raum V7 - Dauer 90 Min](#)

[\[me: Next Version\]](#)

Intro

Managed Kubernetes vs DIY

Cloud Native

Tools

GitOps / RMP

Cluster API

Tipps

Tun

Grenzen

Brauche ich das?

Outro



Ich freue mich über
Fragen (am Ende)

Evolution, Server Config

- Turnschuhe und YaST (Bekannter: Registry+MS ist besser als Linux)
- ssh + vi
- Bash Scripts
- Saltstack/Ansible
- Terraform
- Kubernetes

Was ist Kubernetes?

Container Orchestrierung

...

Kubernetes Resource Model + CRD

Ziele

Hardware effizient nutzen

No Vendor-Lock-in

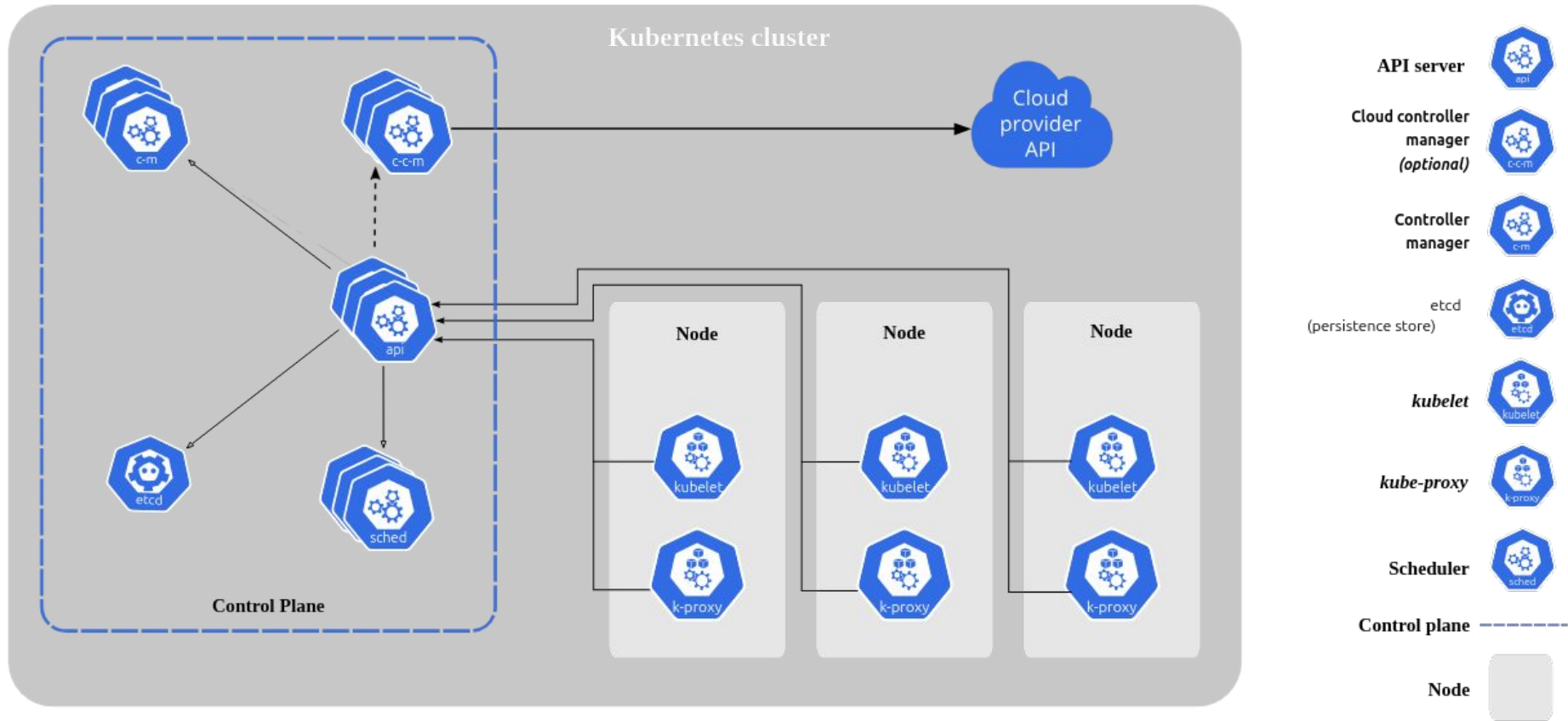
Klare Schnittstellen

Validierung

Autoscaling

Deklarativ

Resilienz



<https://kubernetes.io/docs/concepts/overview/components/>

Operator pattern

vgl Heizung

Desired State

Controller

Reconcile

```
kubectl apply -f deployment.yaml
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: foo-deployment
spec:
  replicas: 3
  selector:
    matchLabels:
      app: foo
  template:
    metadata:
      labels:
        app: foo
    spec:
      containers:
        - name: foo
          image: ...
```



Desired State

“Manifest”

Control Loop

Du wünschst replicas=3

Kubernetes erstellt 3 Pods

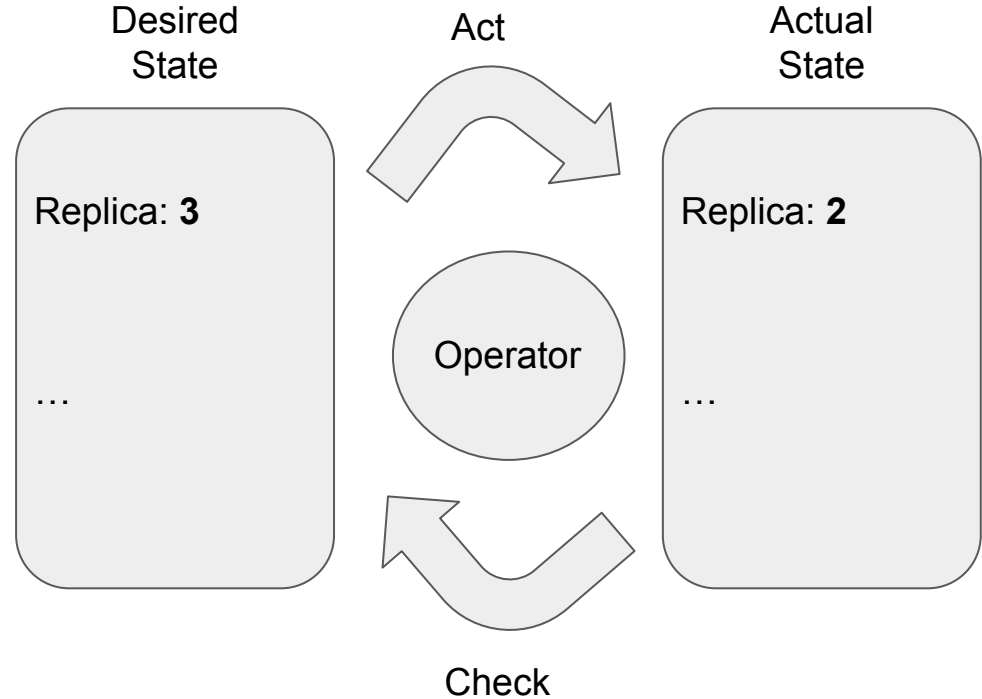
Ein Pod “stirbt”

Aktueller Zustand != Wunsch

Kubernetes erstellt neuen Pod

→ Deklarativ

Endlosschleife (vgl Terraform)



KRM: Resource Typen und Instanzen

Klares Schema 

Vgl SQL: Tabellen / Zeilen

KRM: Deployment

apiVersion: apps/v1

kind: **Deployment**

metadata:

...

spec:

...

status:

....

metadata:

annotations:

foo: bar

creationTimestamp: "2024-11-21T16:52:50Z"

generation: 6

labels:

control-plane: caph-controller-manager

name: caph-controller-manager

namespace: mgt-system

resourceVersion: "227112756"

uid: bdbad897-17c2-473b-9353-1595f75cbc7e

spec:

replicas: 3

template:

spec:

containers:

- image: ghcr.io/sysself/caph:v1.0.1

command: /manager

name: manager

status:

availableReplicas: 2

conditions:

- lastTransitionTime: "2025-03-16T03:56:45Z"

lastUpdateTime: "2025-03-16T03:56:45Z"

message: Deployment has minimum availability.

reason: MinimumReplicasAvailable

status: "True"

type: Available

readyReplicas: 2

apiVersion: apps/v1

kind: Deployment

metadata:

...

spec:

...

status:

....

Resources

Pod

Deployment

Service

Ingress / Gateway API

Resources (2)

ConfigMaps

Secrets

CronJobs

Events

Namespace

Namespace

Per Team, Anwendung, Kunde, ...

Nicht Namespaced:

- Node
- CustomResourceDefinition
- PersistentVolume
- StorageClass

Requests & Limits

- Per Container
- Per Pod (alpha seit 1.32)
- Per Namespace (ResourceQuota)

Requests:

Mindestanforderung

Limits:

Max. Ggf Throttling (CPU), OOMKill (Mem)

Probes

Liveness Probe

Readiness Probe

Startup Probe

CRD: Custom Resource Definition

Controller Entwicklung mit Kubebuilder in Golang.

Kubebuilder Book

CRDs Beispiele

ArgoCD: Application

Prometheus: ServiceMonitor

Cluster API: Cluster (apiVersion: cluster.x-k8s.io/v1beta1)

cnPG: Cluster (apiVersion: postgresql.cnpg.io/v1)

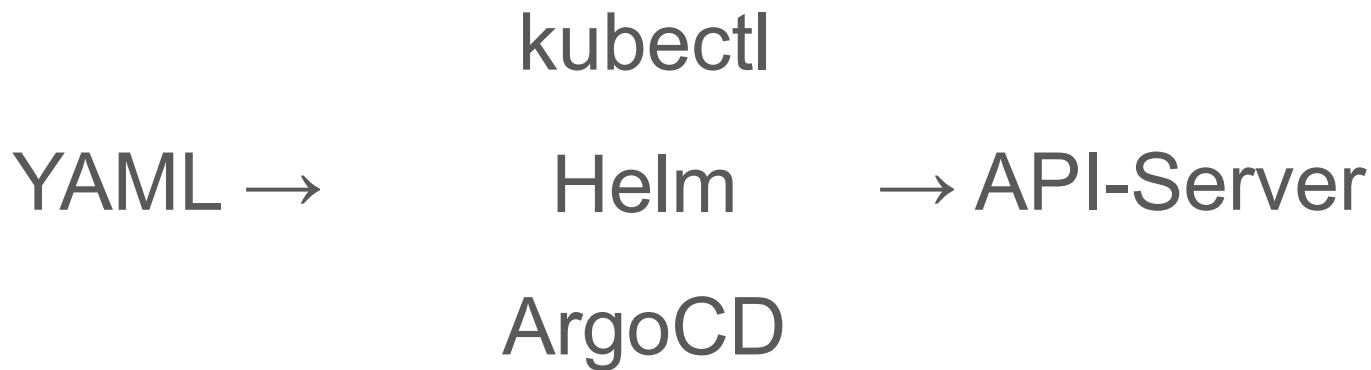
Minio: Bucket

Ein Resource-Typ, ein Controller

Deployment → Deployment Controller

MyCRD → MyCRD Controller

Validierung



OpenAPI, CEL & Web-hooks

Vgl ssh+vi

Data Plane vs Control Plane

Data Plane: Highspeed

Control-Plane: Kurze Downtime, keine Auswirkung

HTTP Request Handling

Data Plane

HTTP Request → Loadbalancer

Loadbalancer → IP+Port

IP+Port → Linux Process

Control Plane (Config)

Ingress / Gateway API → Service

Service → Pod

Pod → Container

Data Plane

HTTP Request → Loadbalancer

Loadbalancer → IP+Port

IP+Port → Linux Process

Control Plane (Config)

Ingress / Gateway API → Service

Service → Pod

Pod → Container

Data Plane

HTTP Request → Loadbalancer

Loadbalancer → IP+Port

IP+Port → Linux Process

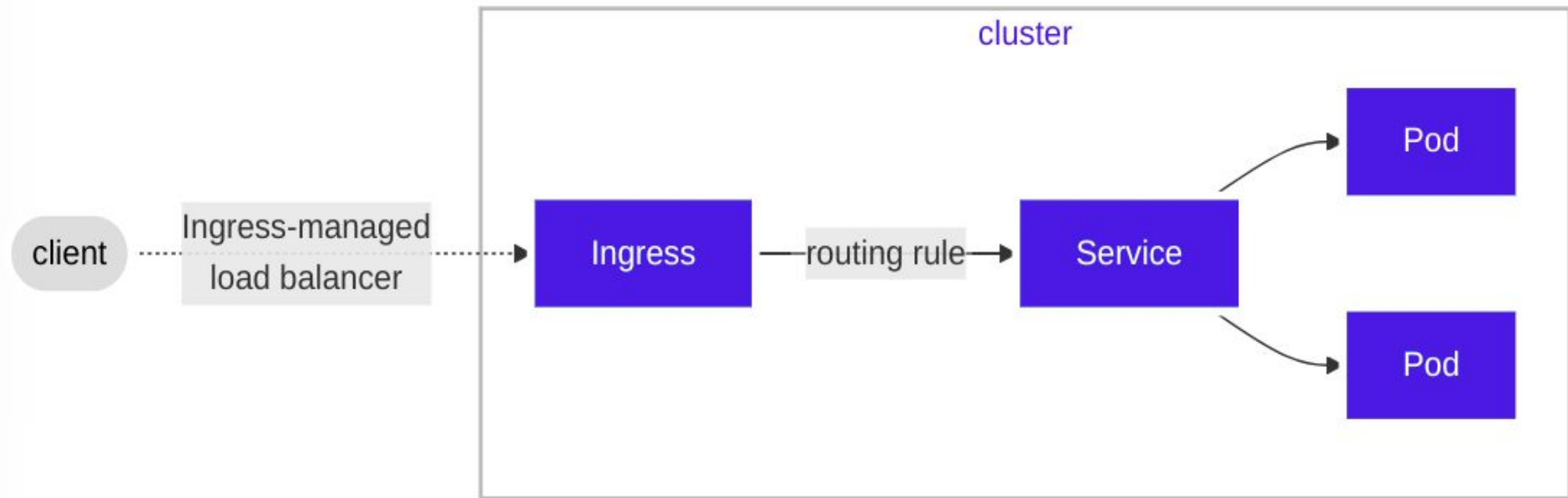
Control Plane (Config)

Ingress / Gateway API → Service

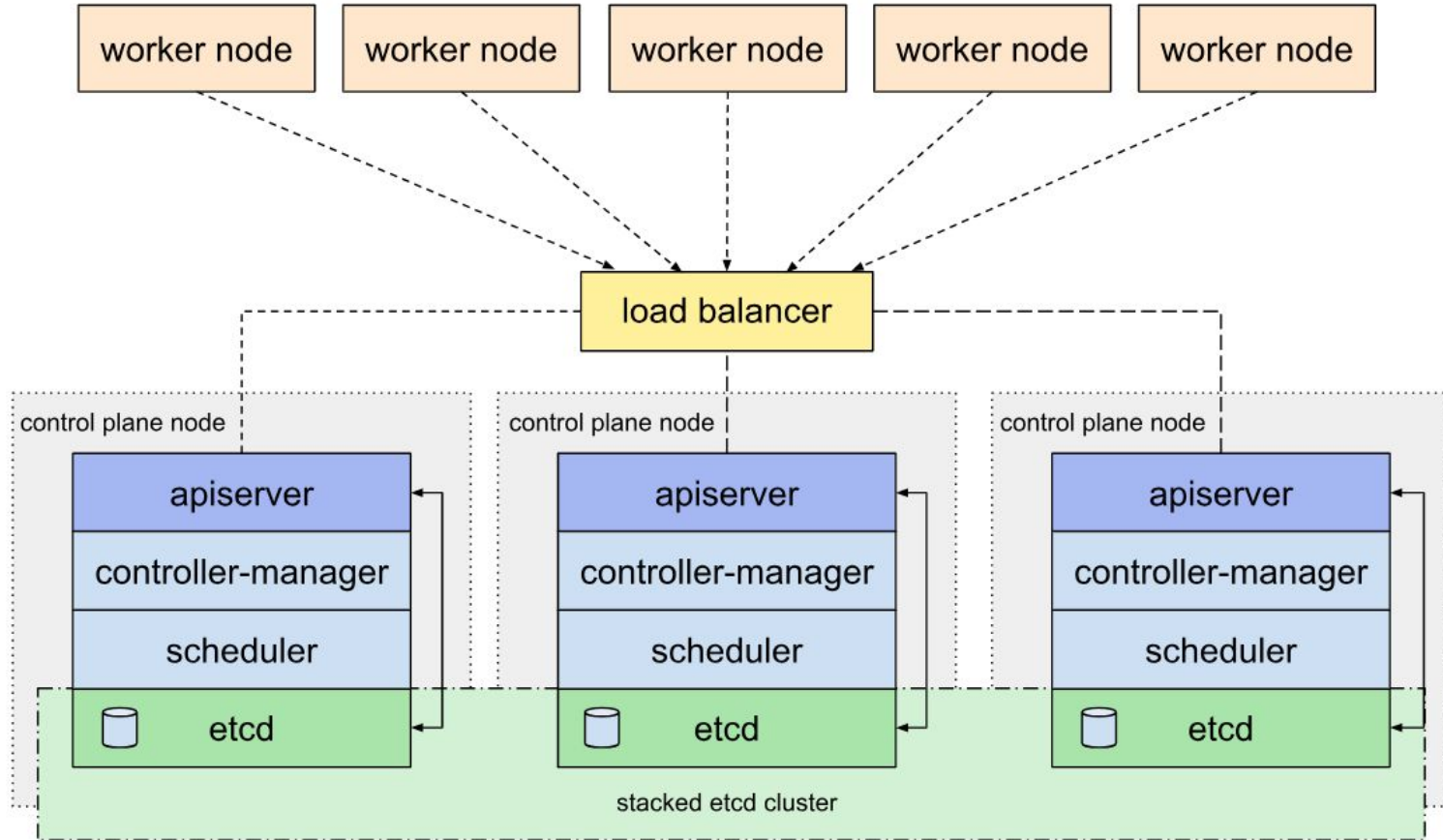
Service → Pod

Pod → Container

Data Plane: Ingress, Gateway API



HA: LoadBalancer mit 3 Control Planes



RBACs

Role (namespaced)

ClusterRole

Bsp: Nutzer “foo” darf nur Namespace “foo-ns” nutzen.

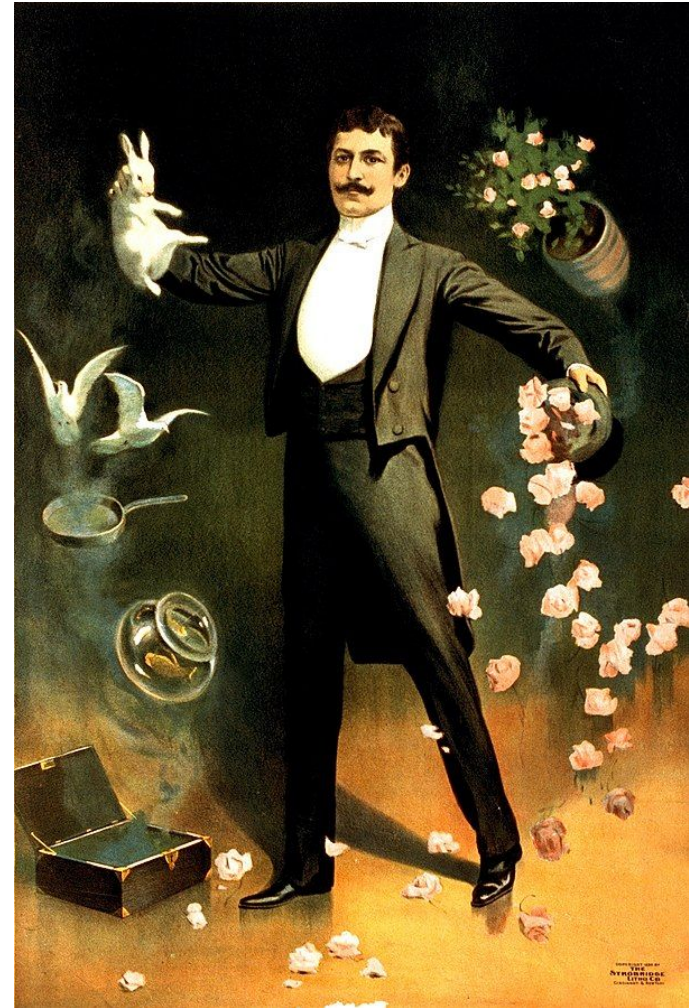
Resource Model

+

Operator Pattern

=

magic



Intro

Managed Kubernetes vs DIY

Cloud Native

Tools

GitOps / RMP

Cluster API

Tipps

Tun

Grenzen

Brauche ich das?

Outro

K8s nutzen oder verwalten?

Managed K8s nutzen: leicht!

DIY? Zeit, hit by bus, ...

(Mein Job by Sysself)

(simplified)

Managed
K8s

PaaS

vendor
lock-in 👎

\$\$\$

easy

\$

hard

DIY

Intro
Managed Kubernetes vs DIY

Cloud Native

Tools
GitOps / RMP
Cluster API
Tipps
Tun
Grenzen
Brauche ich das?
Outro



Netz von Abhängigkeiten?

Frontend Service braucht Backend Service

Backend Service braucht DB

DB braucht Storage

Wie deklarativ?

→ Gleichzeitig starten!

Kein RWX

Read Write Many (NFS)

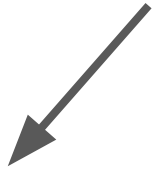
→ Object-Storage (s3)

To DB or not to DB?

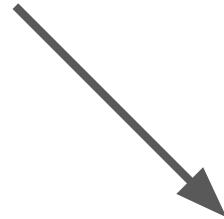
Stateless

XOR

Stateful?



Application



DB/s3

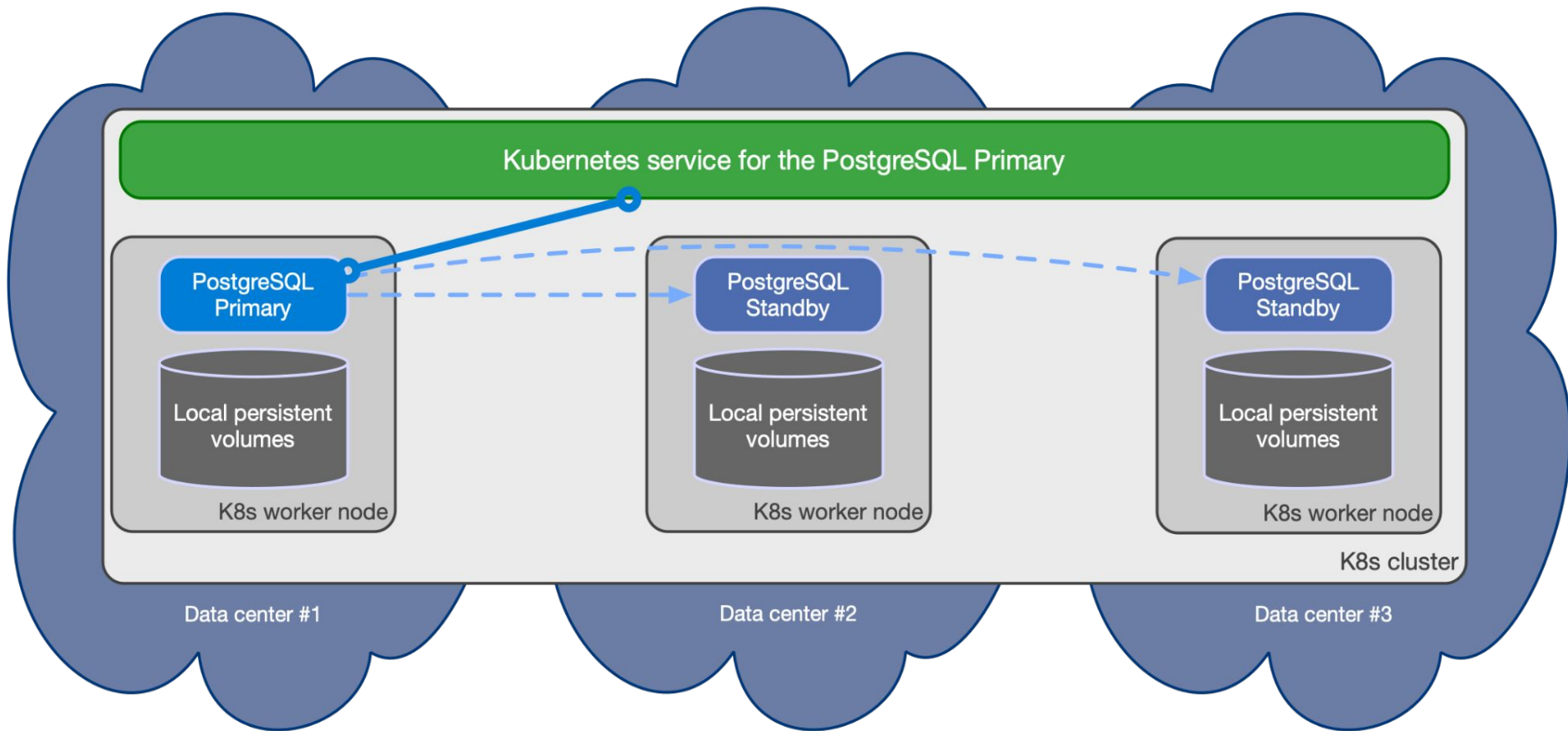
Application

Anwendung nutzt DB (cnPG, ...) und s3 (minio, seaweedfs)

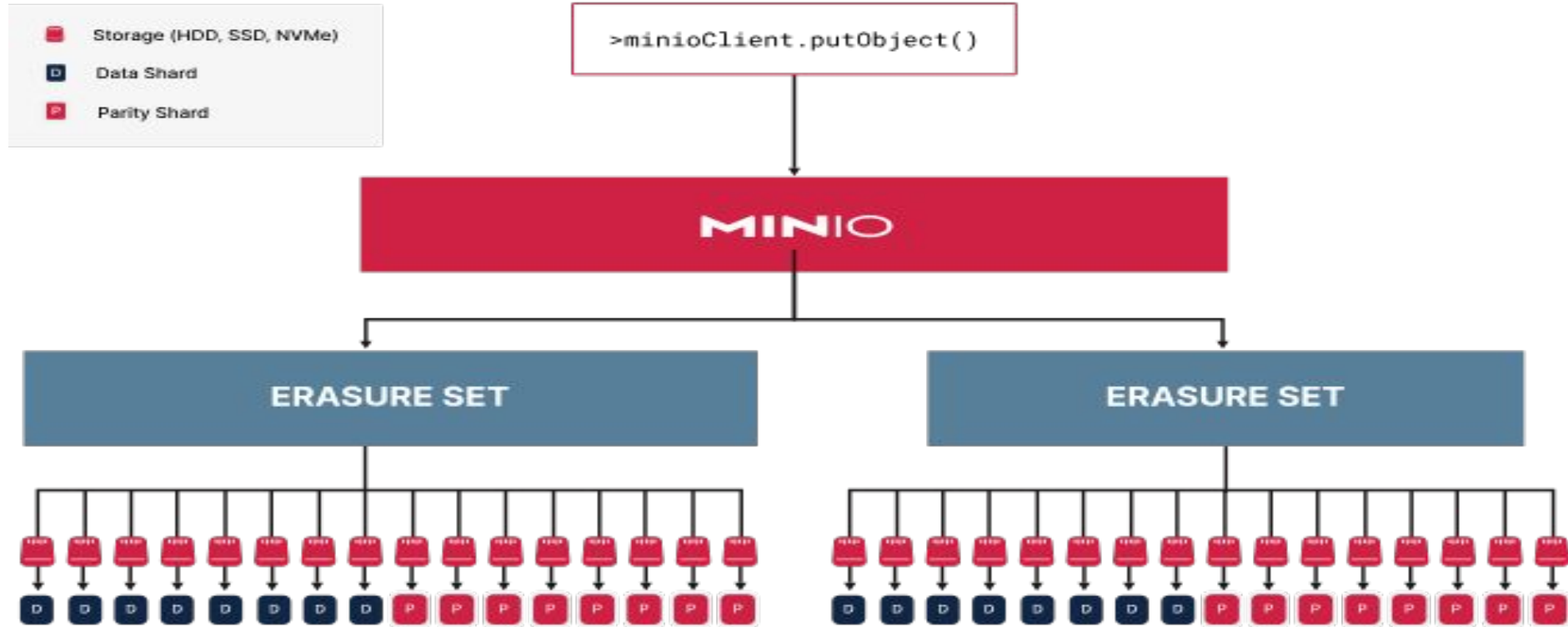
DB nutzt Storage

s3 nutzt Storage

Stateful DB: cnPG



Stateful Object Storage (Minio)



Local Storage

TopoLVM

DirectPV

Replication durch DB/s3 (cnPG, Minio)

Anwendung ist ephemeral/stateless

Anwendung nutzt DB/s3

DB/s3 nutzen local Storage und Replication



Remote Storage (Longhorn, Ceph, ...)

nicht nötig. (meine Meinung)

Alternativ: DB/s3 vom Cloud Provider kaufen

Von Terraform zu CRDs

AWS Controllers for Kubernetes

Azure Service Operator

Google Config Connector

Crossplane

Pro CRDs/KRM: Drift correction

Contributions by Company



Make code,
not war.



Source:

<https://k8s.devstats.cncf.io/d/9/companies-table?orgId=1>

Kubernetes Companies statistics (Contributions, Range: Last decade),

Rank ^ Company

	All
1	Google LLC
2	Red Hat Inc.
3	VMware Inc.
4	Microsoft Corporation
5	Independent
6	International Business Machines Corporation
7	Amazon
8	DaoCloud Network Technology Co. Ltd.
9	Intel Corporation
10	The Scale Factory Limited
11	Huawei Technologies Co. Ltd
12	NEC Corporation
13	CNCF
14	SUSE LLC
15	Sangfor Technologies
16	Red Hat Inc
17	Kubermatic GmbH
18	ZTE Corporation
19	Fujitsu Limited
20	Apple Inc.
21	Weaveworks Inc.

Autoscaling

HPA: +/- Pods

VPA: +/- Limits

CAS: +/- Nodes

Intro
Managed Kubernetes vs DIY
Cloud Native

Tools

GitOps / RMP
Cluster API
Tipps
Tun
Grenzen
Brauche ich das?
Outro

kubectl

kubectl api-resources

Autocomplete

kubectl **[apply | get | delete | edit]** deployment -n my-ns foo

k9s

Context: test-alm-thomas-admin@test-alm-thomas
Cluster: test-alm-thomas
User: test-alm-thomas-admin
K9s Rev: v0.40.8 < v0.40.10
K8s Rev: v1.31.6
CPU: 6%
MEM: 25%

<0> all
<1> default
<a> Attach
<ctrl-d> Delete
<d> Describe
<e> Edit
<?> Help
<shift-j> Jump Owner
<ctrl-k> Kill
<l> Logs
<p> Logs Previous
<shift-f> Port-Forward
<z> Sanitize
<s> Shell

<0> Show...
<f> Show
<t> Trans
<y> YAML



🔒 v1/pods(all) [41]

NAMESPACE↑	NAME	PF	READY	STATUS	RESTARTS	CPU	MEM	%CPU/R	%CPU/L	%
cert-manager	cert-manager-974444f45-dhzvn	●	0/1Δ	TerminatingΔ	0	0	0	n/a	n/a	
cert-manager	cert-manager-974444f45-rnbj7	●	0/1	ContainerCreating	0	0	0	n/a	n/a	
cert-manager	cert-manager-cainjector-857964b486-jw58f	●	1/1	Running	0	2	32	n/a	n/a	
cert-manager	cert-manager-webhook-755d476bb8-4svv5	●	1/1	Running	0	1	11	n/a	n/a	
kube-system	ccm-776db75c68-59btl	●	1/1	Running	0	4	17	20	n/a	
kube-system	ccm-proportional-autoscaler-7799686bbb-7mtrt	●	1/1	Running	0	1	8	10	n/a	
kube-system	cilium-4mzkl	●	1/1	Running	0	46	235	92	n/a	
kube-system	cilium-envoy-2zrjk	●	1/1	Running	0	5	12	n/a	n/a	
kube-system	cilium-envoy-v2vwk	●	1/1	Running	0	5	12	n/a	n/a	
kube-system	cilium-h7dgs	●	1/1	Running	0	53	240	106	n/a	
kube-system	cilium-operator-7ffc74976f-9kssp	●	1/1	Running	0	2	25	20	n/a	
kube-system	cilium-operator-7ffc74976f-vzv64	●	1/1	Running	0	4	30	40	n/a	
kube-system	coredns-7c65d6cfc9-8nmkx	●	1/1	Running	0	3	35	3	n/a	
kube-system	coredns-7c65d6cfc9-dwlsm	●	1/1	Running	0	4	39	4	n/a	
kube-system	coredns-proportional-autoscaler-6858fccf67-pmv8l	●	1/1	Running	0	1	8	10	n/a	
kube-system	csi-controller-55d4c45b4d-4bs45	●	5/5	Running	0	8	46	16	n/a	
kube-system	csi-controller-55d4c45b4d-9ptq5	●	5/5	Running	0	8	46	16	n/a	
kube-system	csi-node-hffnl	●	3/3	Running	0	3	21	10	n/a	
kube-system	etcd-test-alm-thomas-rzd76-7qs9x	●	1/1	Running	0	72	101	72	n/a	
kube-system	hubble-relay-76b5675448-xhhvl	●	1/1	Running	0	1	14	5	n/a	
kube-system	hubble-ui-564c675b98-ns9fk	●	2/2	Running	0	1	20	n/a	n/a	
kube-system	konnectivity-agent-67cc897b84-pwmd4	●	1/1	Running	0	2	41	20	n/a	
kube-system	konnectivity-agent-proportional-autoscaler-6bd88595d7-hk8ln	●	1/1	Running	0	1	8	10	n/a	
kube-system	konnectivity-server-test-alm-thomas-rzd76-7qs9x	●	1/1	Running	0	3	47	12	n/a	

<pod>

🗑 Delete resource v1/pods cert-manager/cert-manager-974444f45-dhzvn

KUBECONFIG mit direnv

```
export KUBECONFIG=my-kubeconfig.yaml
```

Datei: .envrc

Tool: direnv

```
cd ~/clusters/foo/
```

→ automatisch KUBECONFIG gesetzt

Starship k8s Prompt



user@mycluster

› kubectl get ...

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools

GitOps / RMP

Cluster API
Tipps
Tun
Grenzen
Brauche ich das?
Outro



GitOps

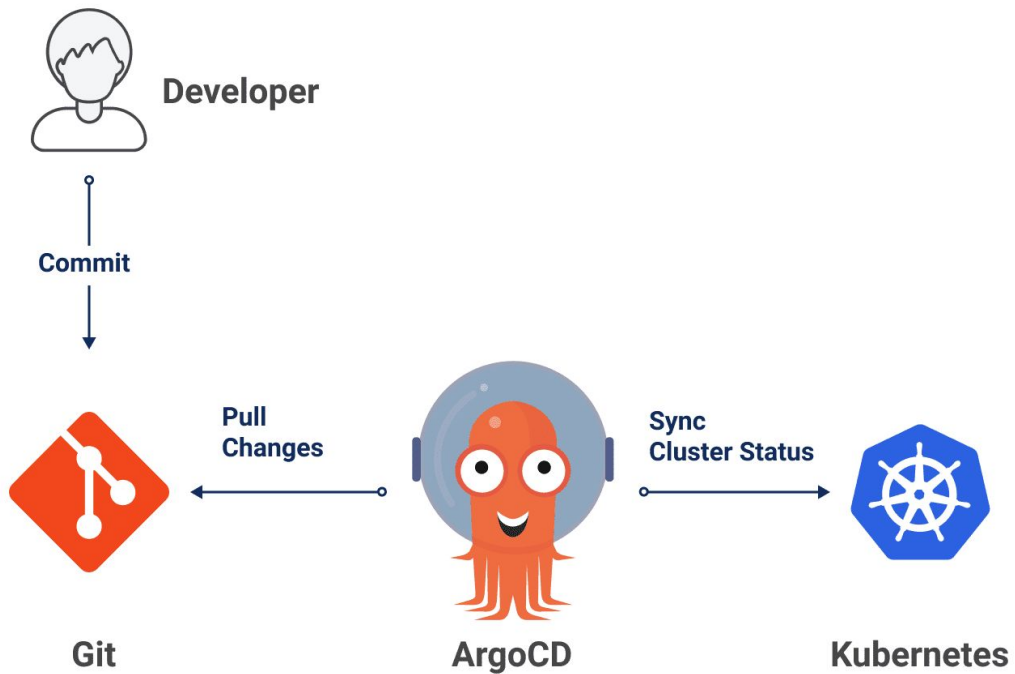
Config in Git.

Tool applies config to cluster.

ArgoCD, Flux

kubectl (only readonly)

Drift Correction



Ohne “Rendered Manifest Pattern”

Helm + Kustomize → YAML

In Git: Helm Referenz + values.yaml, kustomization.yaml

Schön Schlank

Mit “Rendered Manifest Pattern”

Helm Referenz + values.yaml, kustomization.yaml

Plus Rendered Manifests

“hundert” YAML Dateien

Aber: Änderungen sind deutlich sichtbar.

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP

Cluster API

Tipps
Tun
Grenzen
Brauche ich das?
Outro

Cluster API (capi)

SIG Cluster Lifecycle

Management-Cluster: N Workload-Cluster

Infra-Providers:

Azure, DigitalOcean, GCP, Hetzner (Sysself), OpenStack,
VMWare, ...

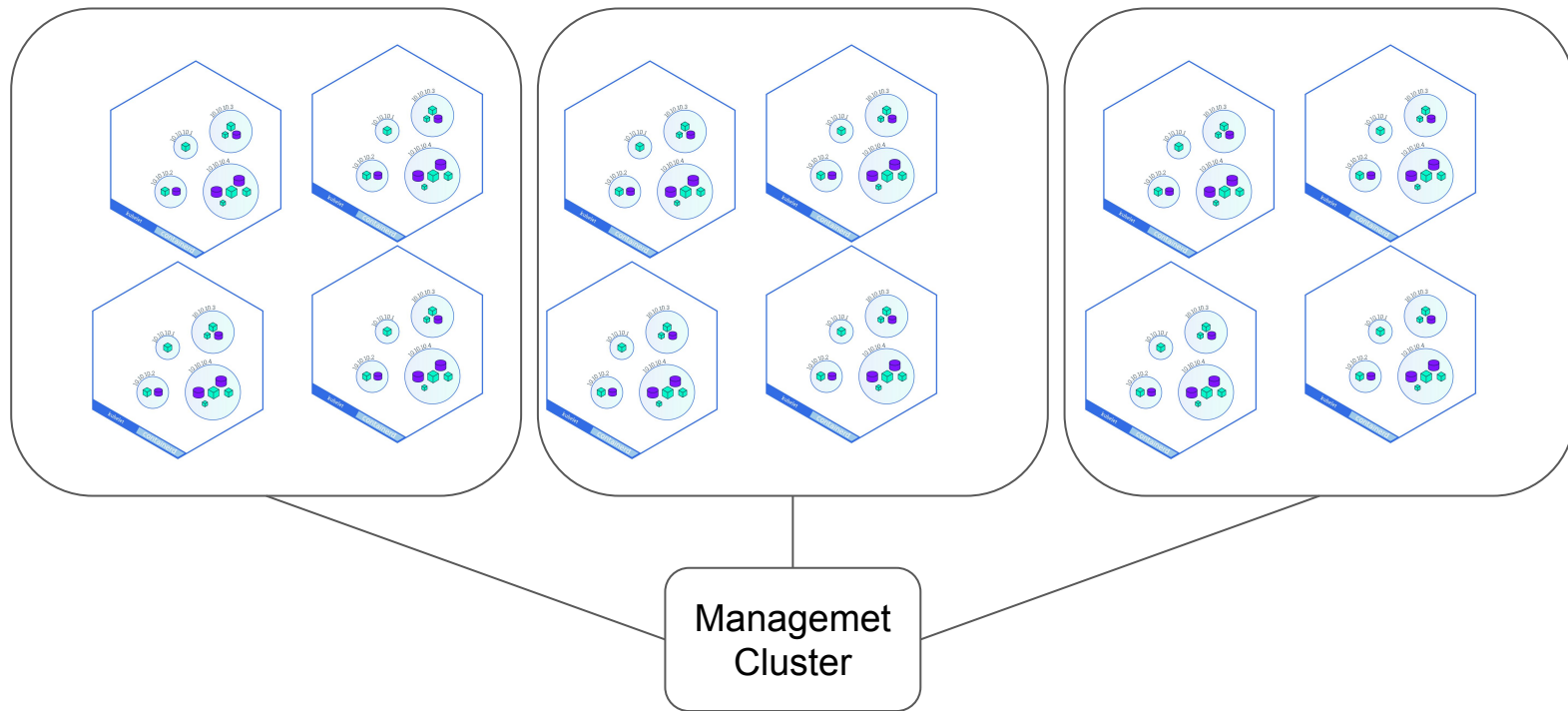
Cluster API

Cluster A

Cluster B

Cluster C

← ***“Workload” Cluster***



(simplified)

K8s
managed

PaaS
(vendor lock-in)

\$\$\$

easy



hard

Cluster
API

\$

MachineDeployment

CRD von Cluster-API

```
{  
  apiVersion: cluster.x-k8s.io/v1beta1  
  kind: MachineDeployment  
}
```

metadata:

labels:

nodepool: host-cluster-md-0

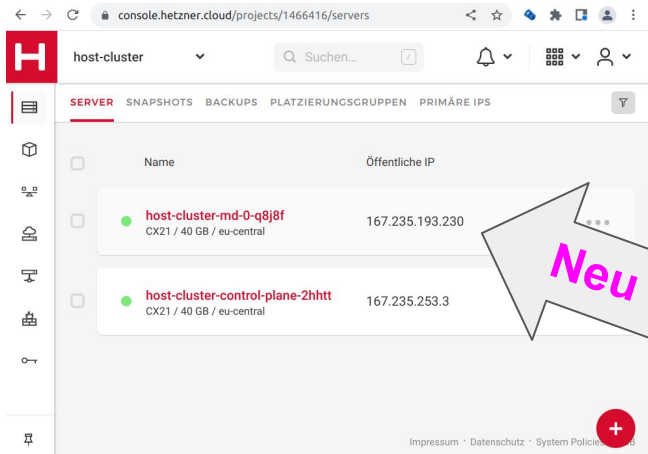
name: host-cluster-md-0

namespace: default

spec:

clusterName: host-cluster

replicas: 1 → 2



```
• > k get clusters -A
```

NAMESPACE	NAME	CLUSTERCLASS	PHASE	AGE	VERSION
my-workspace	my-cluster	hetzner-apalla-1-30-v6	Provisioned	20d	v1.30.8

> kubectl-tree -n my-workspace cluster my-cluster

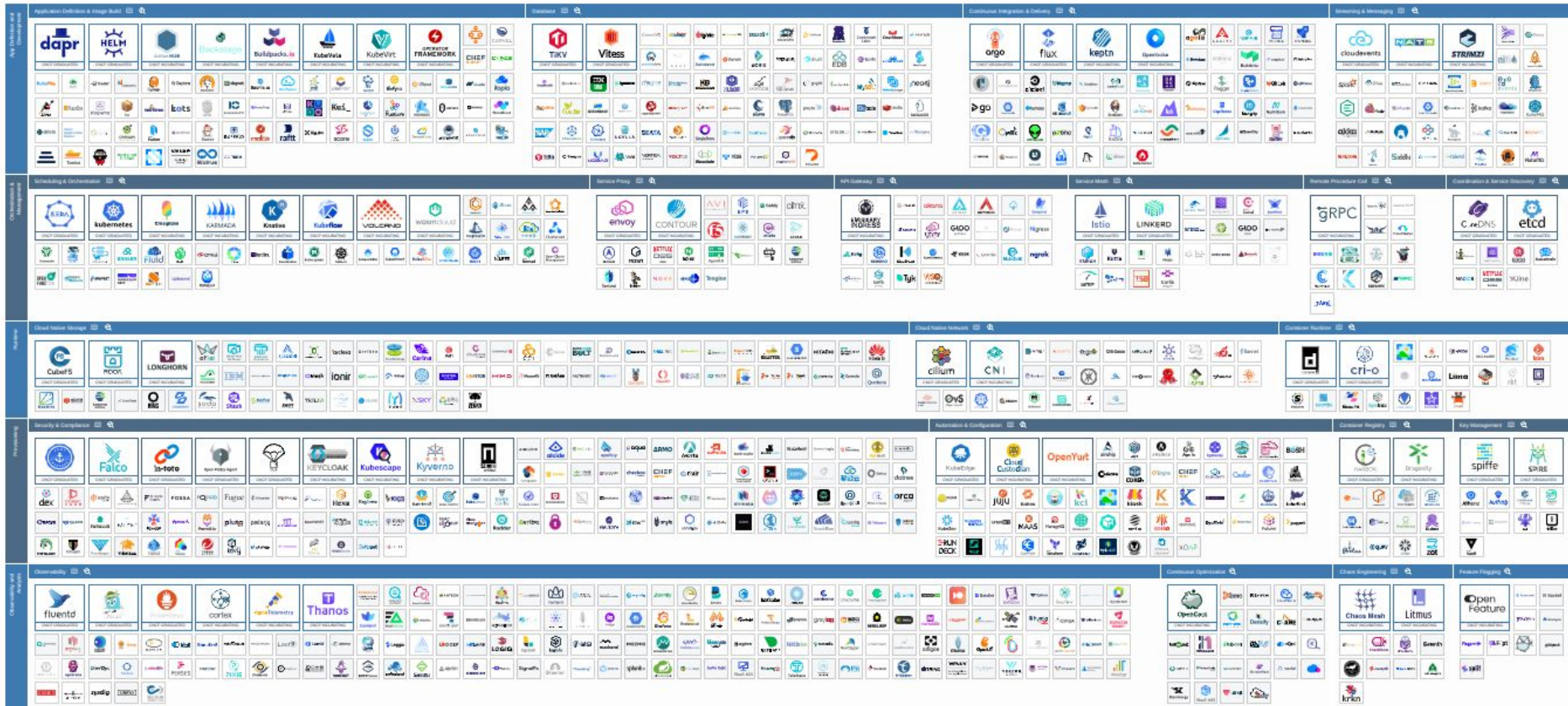
NAMESPACE	NAME	READY	REASON	AGE
my-workspace	Cluster/my-cluster	True		7d2h
my-workspace	ClusterAddon/cluster-addon-my-cluster	True		7d2h
my-workspace	HCloudMachineTemplate/my-cluster-2gxrq	-		7d2h
my-workspace	HCloudMachineTemplate/my-cluster-md-hcloud-1-hm4rf	-		7d2h
my-workspace	HetznerCluster/my-cluster-8vkxn	True		7d2h
my-workspace	Secret/hetzner	-		7d23h
my-workspace	Secret/my-cluster-kubeconfig	-		7d2h
my-workspace	KubeadmConfigTemplate/my-cluster-md-hcloud-1-2fqhf	-		7d2h
my-workspace	KubeadmControlPlane/my-cluster-dcx5w	True		7d2h
my-workspace	Machine/my-cluster-dcx5w-7crhr	True		7d2h
my-workspace	HCloudMachine/my-cluster-dcx5w-7crhr	True		7d2h
my-workspace	Secret/my-cluster-dcx5w-7crhr	-		7d2h
my-workspace	KubeadmConfig/my-cluster-dcx5w-7crhr	True		7d2h
my-workspace	Secret/my-cluster-dcx5w-7crhr	-		7d2h
my-workspace	Secret/my-cluster-ca	-		7d2h
my-workspace	Secret/my-cluster-etcd	-		7d2h
my-workspace	Secret/my-cluster-kubeconfig	-		7d2h
my-workspace	Secret/my-cluster-proxy	-		7d2h
my-workspace	Secret/my-cluster-sa	-		7d2h
my-workspace	MachineDeployment/my-cluster-md-hcloud-1-m9kqq	True		7d2h
my-workspace	MachineSet/my-cluster-md-hcloud-1-m9kqq-rs6lk	True		7d2h
my-workspace	Machine/my-cluster-md-hcloud-1-m9kqq-rs6lk-b48hw	True		7d2h
my-workspace	HCloudMachine/my-cluster-md-hcloud-1-m9kqq-rs6lk-b48hw	True		7d2h
my-workspace	Secret/my-cluster-md-hcloud-1-m9kqq-rs6lk-b48hw	-		7d2h
my-workspace	KubeadmConfig/my-cluster-md-hcloud-1-m9kqq-rs6lk-b48hw	True		7d2h
my-workspace	Secret/my-cluster-md-hcloud-1-m9kqq-rs6lk-b48hw	-		7d2h
my-workspace	MachineHealthCheck/my-cluster-dcx5w	-		7d2h
my-workspace	MachineHealthCheck/my-cluster-md-hcloud-1-m9kqq	-		7d2h

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP
Cluster API

Tipps

Tun
Grenzen
Brauche ich das?
Outro

CNCF Landscape



Sane Defaults

CRI → containerd

CNI → Cilium

Metrics → Prometheus

GitOps → ArgoCD

Bootstrap → kubeadm / Cluster-API

Terminal → kubectl, k9s

Local Playground → kind

PostgreSQL → cloudnativePG

CRD dev → Golang and Kubebuilder

FOMO?

Service Mesh

OpenTelemetry

flatcar, talos

Wasm

FaaS, PaaS

CUE

External Secrets Operator

Rancher, OpenShift

.... meist nicht nötig. Lieber kubernetes.io lesen.

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP
Cluster API
Tipps

Tun

Grenzen
Brauche ich das?
Outro

Raspberry Pi (Joy-it RB-Case)

(not me, I hate hardware)



kind: Kubernetes in Docker

```
> kind create cluster
```

```
Creating cluster "kind" ...
```

- ✓ Ensuring node image (kindest/node:v1.30.0) 
- ✓ Preparing nodes 
- ✓ Writing configuration 
- ✓ Starting control-plane 
- ✓ Installing CNI 
- ✓ Installing StorageClass 

```
Set kubectl context to "kind-kind"
```

```
You can now use your cluster with:
```

```
kubectl cluster-info --context kind-kind
```

```
Not sure what to do next? 😊 Check out https://kind.sigs.k8s.io/docs/user/quick-start/
```

VPS + kubeadm

Cluster mit einer Node

kubeadm

Taints entfernen

fertig ist die **Spielwiese**

Hetzner CX32, 4 CPU, 8 GB, 6,80 €

tun

kubernetes.io lesen

#kubernetes-users (Slack), Reddit r/kubernetes.

CKA

Golang (CLT 2025, Sonntag 10 Uhr)

... Geduld! (vgl Fremdsprache)

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP
Cluster API
Tipps
Tun

Grenzen

Brauche ich das?
Outro

Nodes: Erstellen/Entfernen

→ kubeadm, Cluster API

Controlplane LoadBalancer

LoadBalancer für Data-Plane (via Service Type=LB) ✓

LoadBalancer für ControlPlane



`kubectl apply` easy ... aber

Tag1: Apply von 5 Manifesten

Tag2: Apply/Update

Tag3: Nur noch 4 Manifests ... nun?

Prune?

Nicht in Kubernetes

GitOps (ArgoCD)

Cert-Manager

Applikationen (DB, persistent Storage, ...)

Monitoring/Alerting

OOMKilled



Pods/Container “verschieben” ...

Delete + Re-Create

Namespace Isolation

Dev, Staging, Prod in einem Cluster? Nein!

CRDs are cluster-scoped

ThirdPartyCRD v1



ThirdPartyCRD v2

Helm

Text Templating....

Alle Werte im YAML zu Werten in values.yaml ?

Good: ArgoCD, Helm + Kustomize

[fancy: CUE, jsonnet, ...]

Verknüpfen der Anwendungen...

Pod $\rightarrow$ Token $\rightarrow$ DB

(vgl PaaS)

Grenzen

Max. 110 Pods pro Node

Max. 5k Nodes

—

Max Object Size: 3 MByte (Yaml)

Max etcd Size: 8 GByte

Global Scale!

... nein

Alternativen?

Docker

Docker Swarm

Mesos

Kamal (DHH)

—

AWS ECS

Nomad, business source license

PaaS (Heroku, fly.io, ...)

Linux

git

Bash

systemd

OpenSSH

sqlite

PostgreSQL

alternativos

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP
Cluster API
Tipps
Tun
Grenzen

Brauche ich das?

Outro

Vielleicht brauche ich es gar nicht...

Legacy Applications ...

containerisierbar ?

N Worker?

Ein VM reicht?

Prima!

Lass es so.

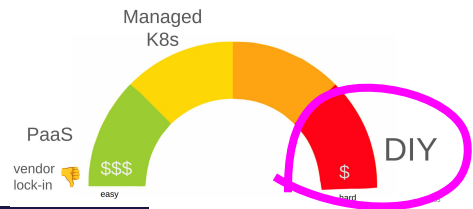
(Spaß am Lernen?)

Intro
Managed Kubernetes vs DIY
Cloud Native
Tools
GitOps / RMP
Cluster API
Tipps
Tun
Grenzen
Brauche ich das?

Outro

Sysself Cluster API Provider Hetzner

CAPH: Open Source



Syself CAPH

Search

Ctrl K

Getting Started

Introduction

> Quickstart

Hetzner project preparation

Topics

SSH key management

High availability setup

Node Images

Upgrading the Kubernetes
Cluster API Provider Hetzner

> Baremetal

> Advanced

Reference

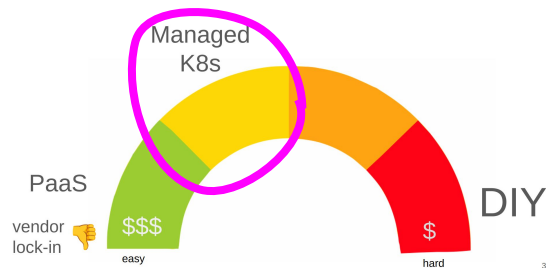
Introduction

Welcome to the official documentation for the Cluster API Provider Hetzner (CAPH). If you are new to it, you can keep reading the Getting Started section, the Quickstart guide will walk you through your first cluster setup.

What is the Cluster API Provider Hetzner

CAPH is a Kubernetes Cluster API provider that facilitates the deployment and management of self-managed Kubernetes clusters on Hetzner infrastructure. The provider supports both cloud and bare-metal instances for consistent, scalable, and production-ready cluster operations.

It is recommended that you have at least a basic understanding of Cluster API before getting started with CAPH. You can refer to the Cluster API Quick Start Guide from its [official documentation](#).



Get Started for Free

Get everything you need to run your personal Kubernetes projects

- ✓ Production-Ready Kubernetes
- ✓ Full Lifecycle Management
- ✓ Self-Healing Capabilities
- ✓ Autoscaling Capabilities
- ✓ 1 Cluster With Up to 5 Nodes

Email*

Join Waitlist

Don't want to wait? [Book a Demo](#) and Explore the Platform with a 14-Day Trial!

Cloud Native Chemnitz



Chemnitz Cloud Native Meetup

📍 Chemnitz, Deutschland

👤 128 Mitglieder · Öffentliche Gruppe ⓘ

👤 Organisiert von **Andreas Siegel** and **3 others**

Teilen:     

[Info](#)[Events](#)[Mitglieder](#)[Fotos](#)[Diskussionen](#)

Du bist Mitglied ▼

Kubernetes



Chemnitzer Linux Tage 2025

Thomas Güttler, Sysself

[Samstag, 11:00 - Raum V7 - Dauer 90 Min](#)

Fragen?