Folien zum Mitlesen
slides.aditsystems.de/ittage_2026



Kevin Honka

Kubernetes-Management mit Cluster API

WER BIN ICH

- Kevin Honka
- CTO @ AD IT Systems GmbH
- Seit mehr als 20 Jahren in der IT unterwegs





IT SYSTEMS

WER IST AD IT SYSTEMS

- Kleiner MSP aus Nürnberg
- Spezialisiert auf Webshops, Hidden Champions Europas, Gesundheits- und Telco-Anwendungen
- Eigene Cloud mit OpenStack, Ceph und Kubernetes

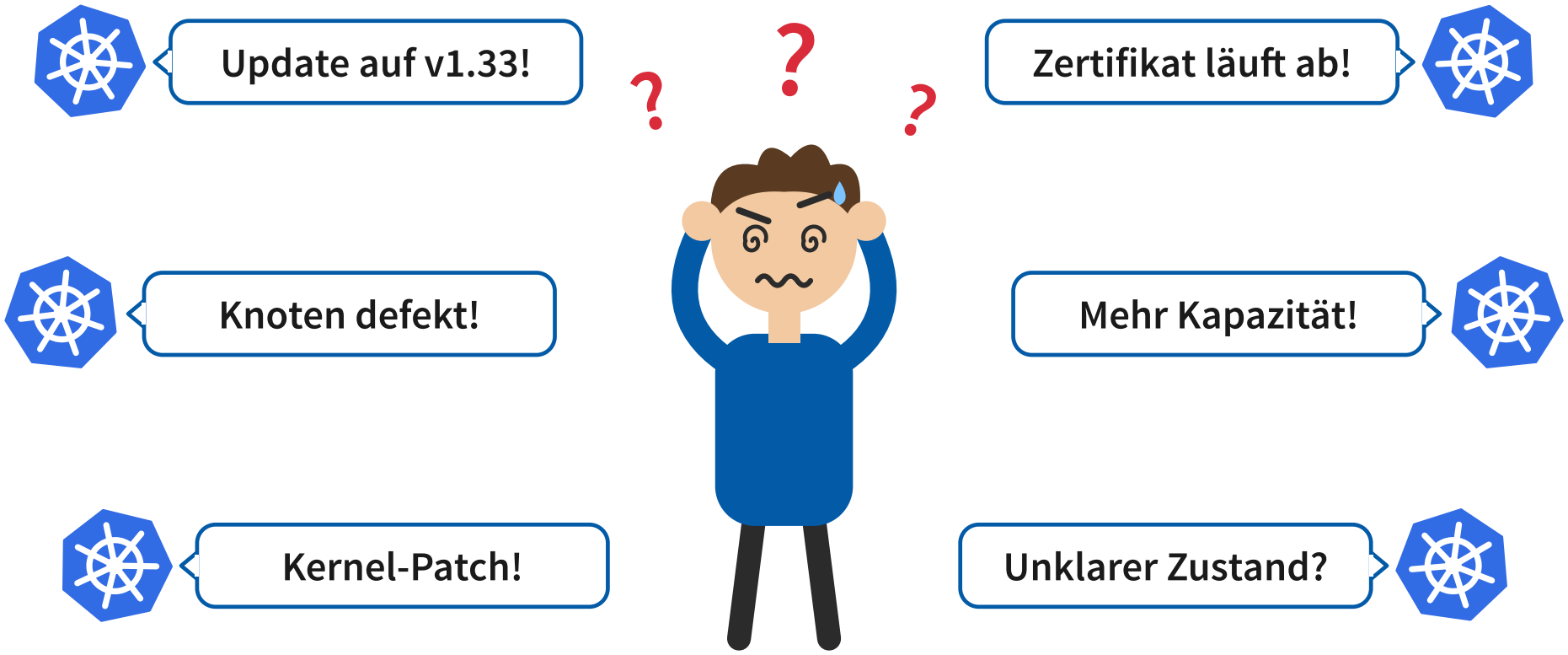
aditsystems.de

LinkedIn

Mastodon

IT SYSTEMS

DAS PROBLEM

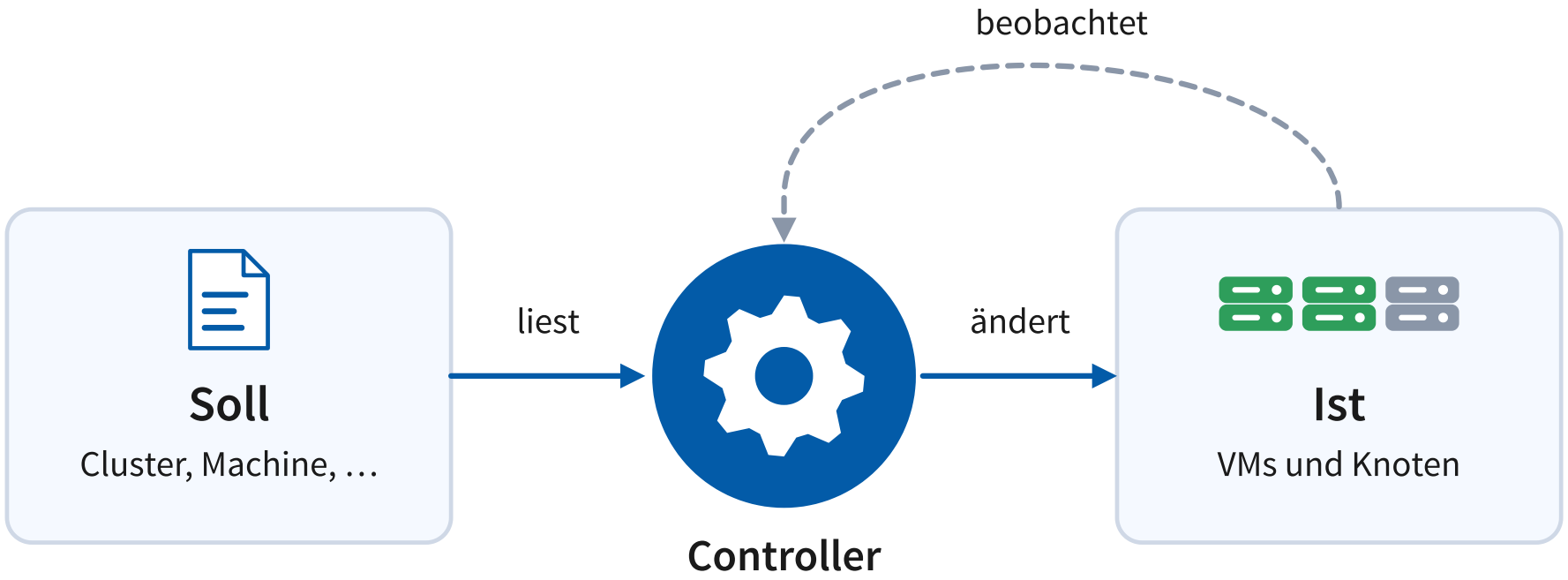


Viele Cluster. Handarbeit skaliert nicht.

IT SYSTEMS

WAS IST CLUSTER API?

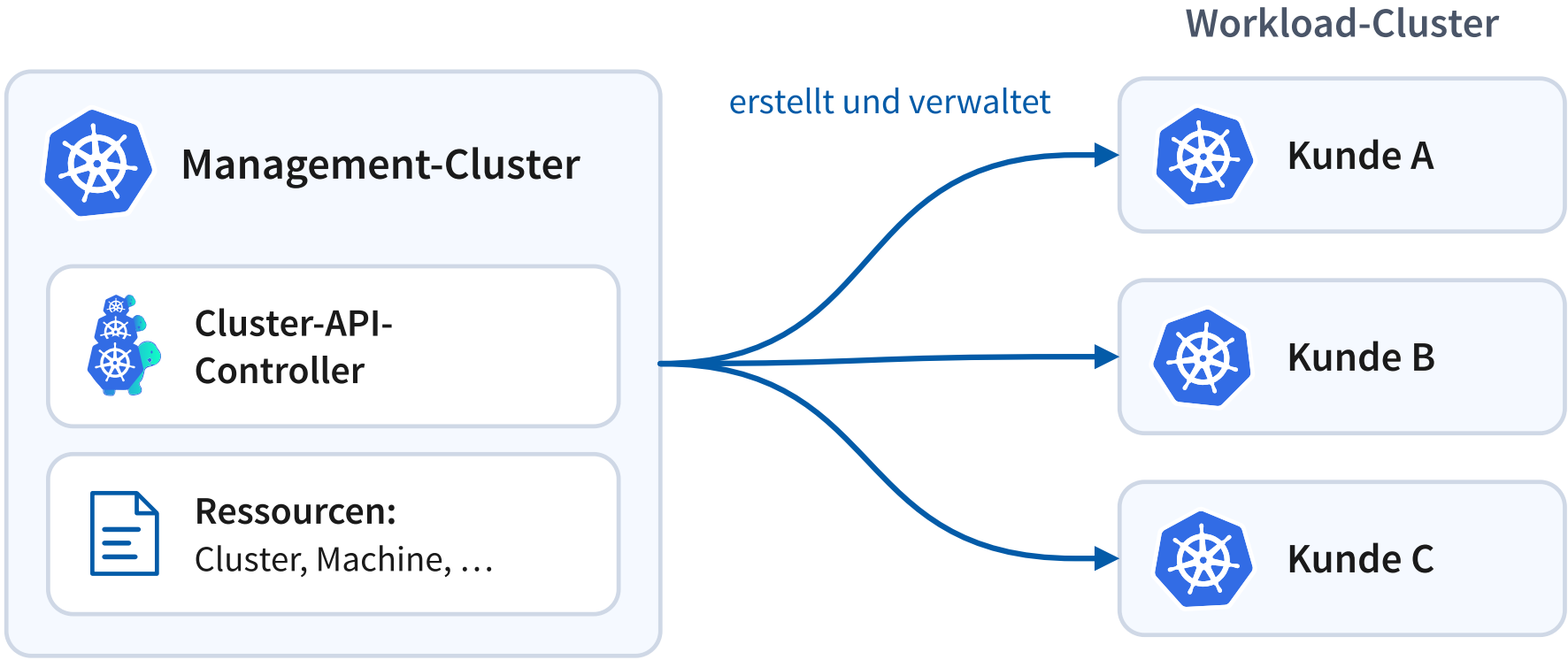
Kubernetes verwaltet Kubernetes



Soll ≠ Ist → Controller handelt. Immer wieder.

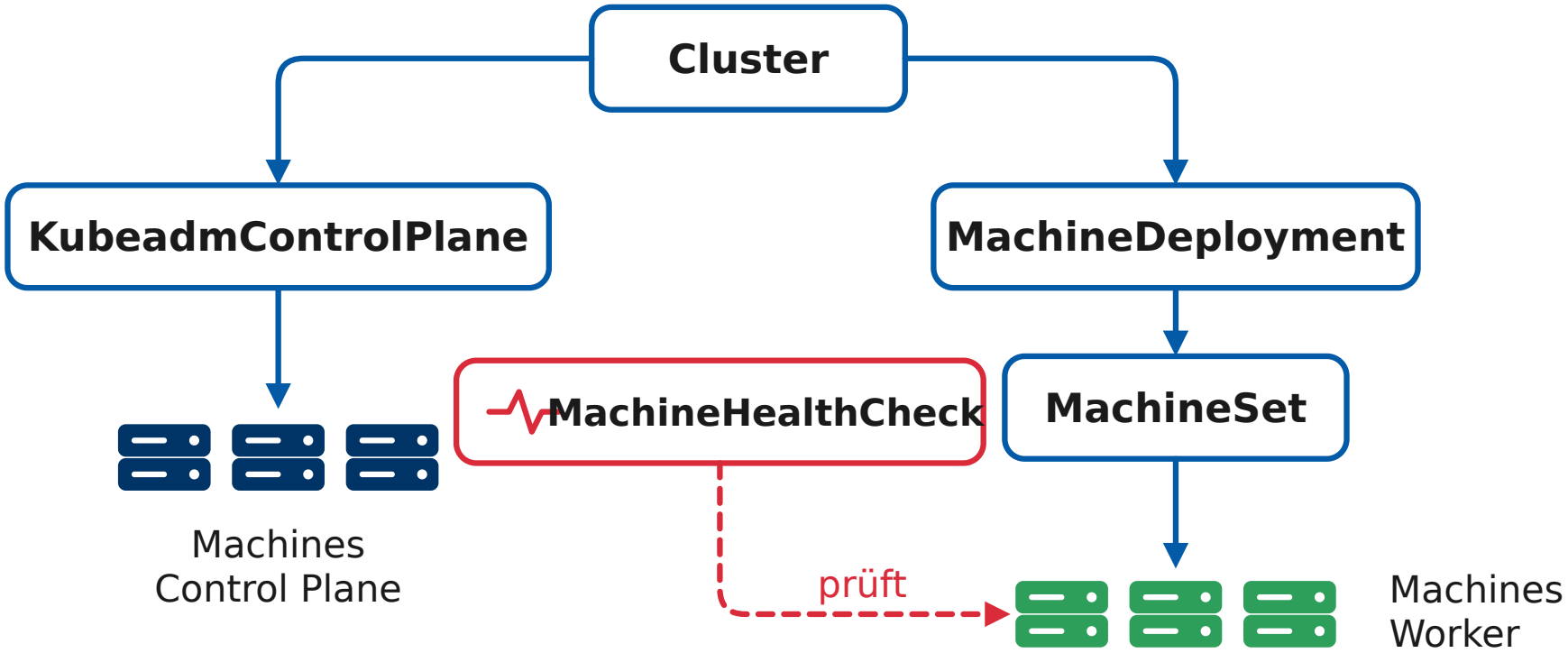
IT SYSTEMS

MANAGEMENT- UND WORKLOAD-CLUSTER



IT SYSTEMS

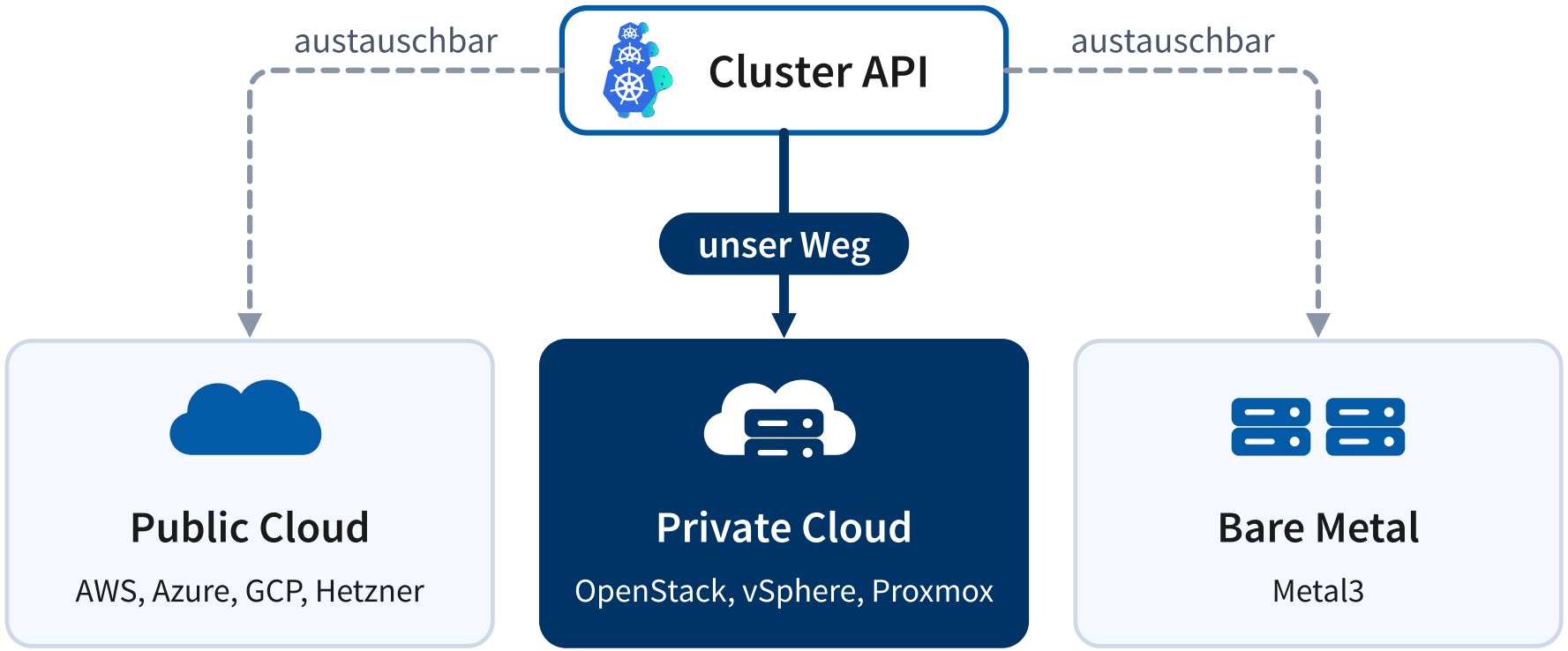
DIE RESSOURCEN



Wie `Deployment` → `ReplicaSet` → `Pod`

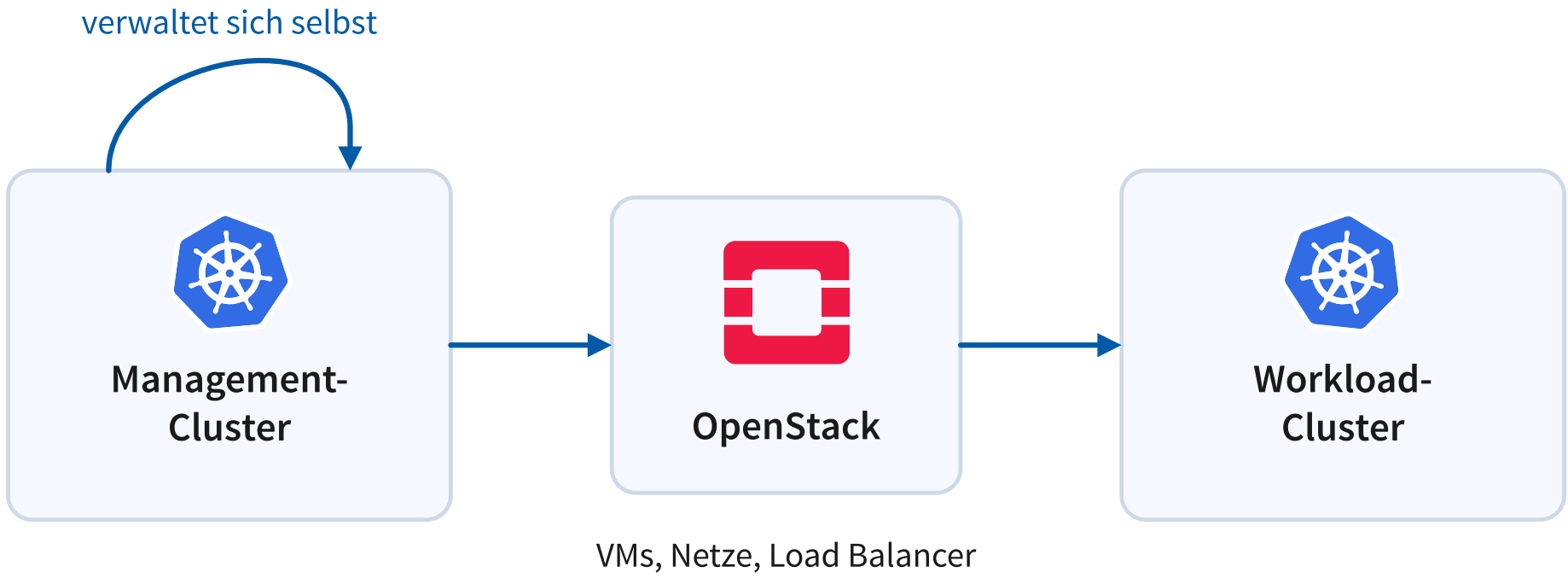
IT SYSTEMS

PROVIDER



IT SYSTEMS

UNSERE ARCHITEKTUR



IT SYSTEMS

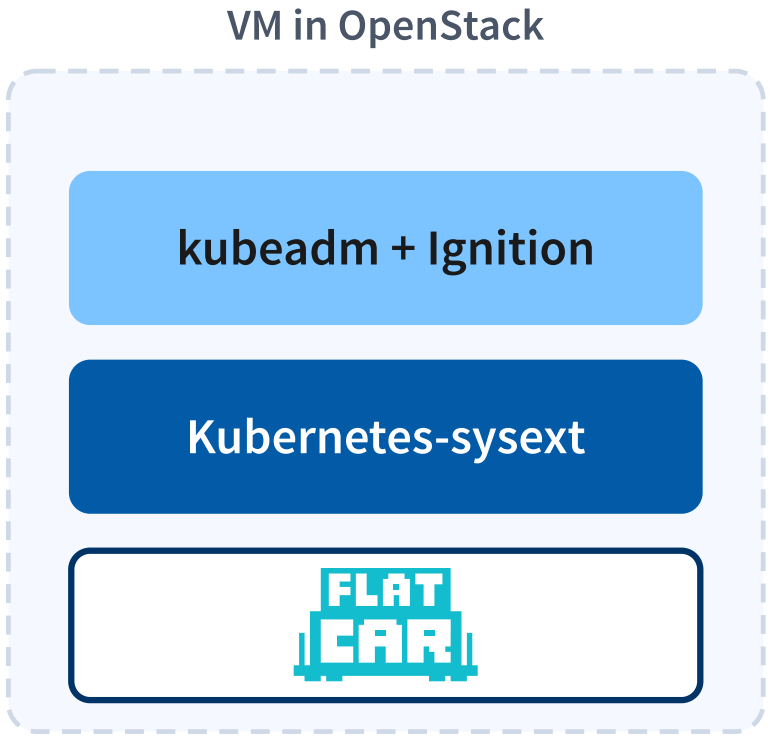
IM MANAGEMENT-CLUSTER

Management-Cluster

CAPI Cluster API	Cluster und Maschinen: Soll gegen Ist
CAPO Provider OpenStack	Erstellt VMs, Netze, Load Balancer
ORC OpenStack Resource Controller	OpenStack-Ressourcen, z. B. Images
CAAPH Addon Provider Helm	Installiert Helm-Charts im Cluster

IT SYSTEMS

EIN KNOTEN



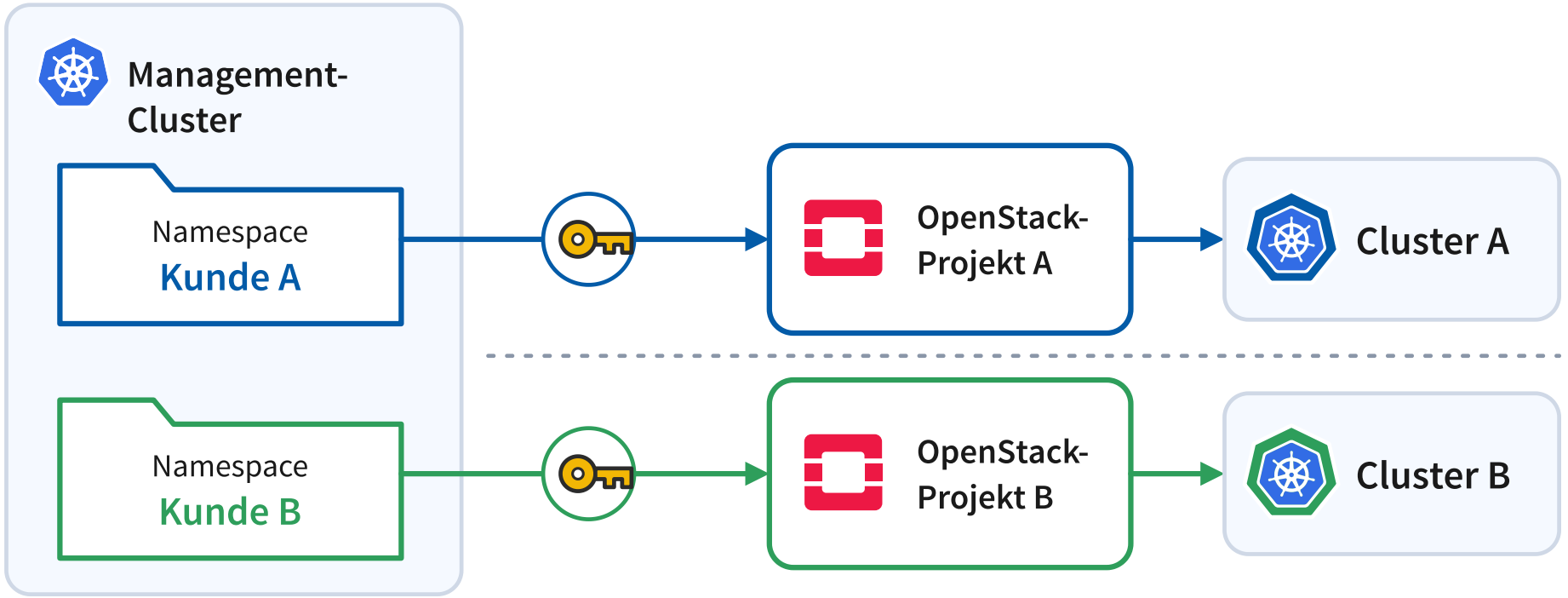
Bootstrap beim ersten Start
Ignition richtet ein, kubeadm tritt bei

Binaries von extensions.flatcar.org
SHA-512 geprüft

Unverändertes Image
Kein eigener Image-Build

IT SYSTEMS

MANDANTEN



Application Credential: Zugang nur zum eigenen Projekt

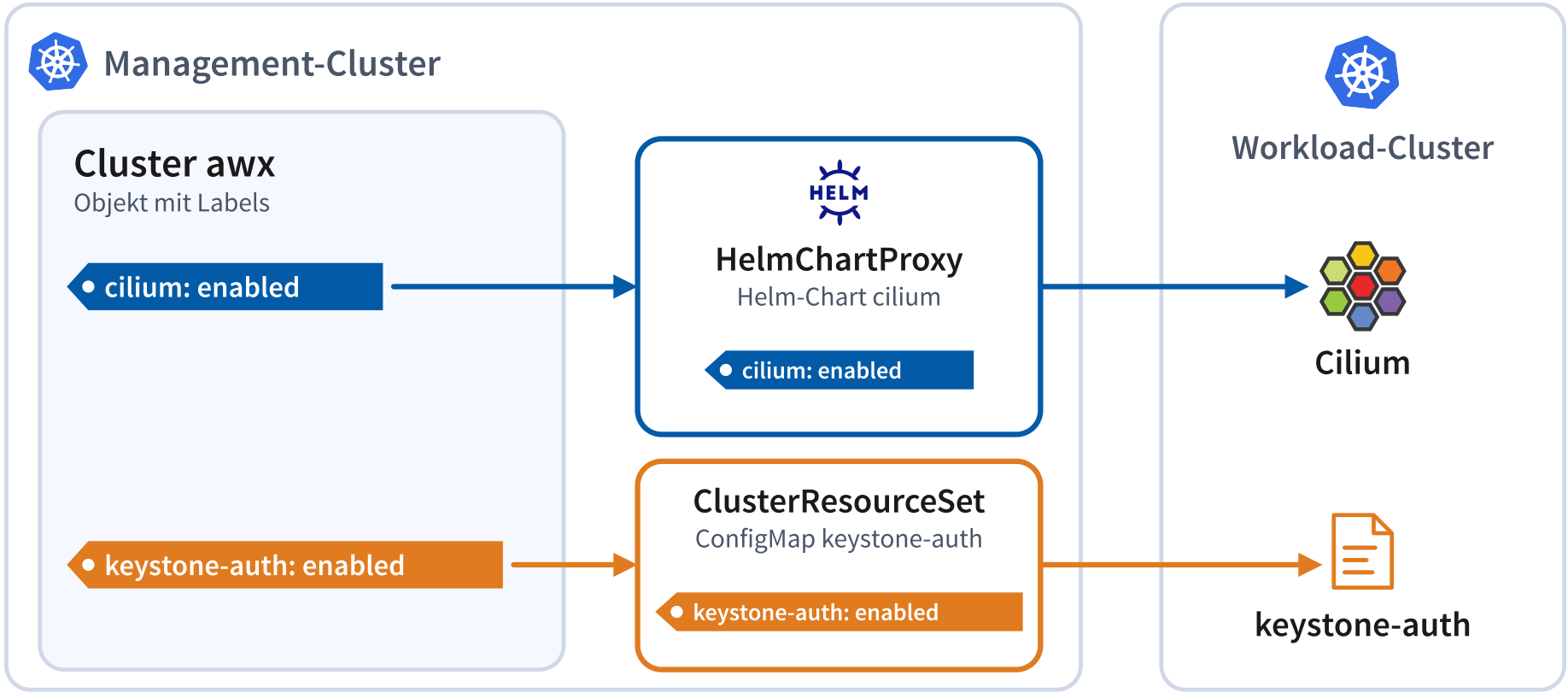
IT SYSTEMS

WAS EIN CLUSTER BRAUCHT



IT SYSTEMS

KOMPONENTEN PER LABEL



Ein Label pro Komponente genügt.

IT SYSTEMS

CLUSTER ALS CODE

Ein OpenTofu-Modul erzeugt alle CAPI-Ressourcen:

```
module "awx_cluster" {
  source  = "git.aditsystems.de/adit/capi-cluster/local"
  version = "5.0.0"

  cluster_name                = "awx"
  control_plane_machine_count = 3
  machine_count               = 3

  worker_templates = {
    "v1" = { flavor = "gp2i.8", image_name = "Flatcar Container Linux" }
  }
  active_worker_template = "v1"
}
```

IT SYSTEMS

DEMO: CLUSTER ERSTELLEN

```
── Terminal ──────────────────────────────────────────────────────────────────────
# Helm-Charts +09:24
$ kubectl get hrp -o custom-columns=CHART:spec.chartName,VERSION:spec.version,STATUS:status.status
CHART                              VERSION   STATUS
cert-manager                       1.21.2    deployed
cilium                             1.20.2    deployed
filebeat                           8.5.1     deployed
helm-exporter                      1.3.0     deployed
kube-prometheus-stack              78.3.2    deployed
kured                              5.11.0    deployed
nginx-gateway-fabric               2.8.0     deployed
openstack-cinder-csi               2.32.0    deployed
openstack-cloud-controller-manager 2.27.1    deployed

# ClusterResourceSets +09:31
$ kubectl get clusterresourcesets
NAME                              APPLIED   AGE
testing-gateway-api-crds          True      6d3h
testing-gateway-resources         True      6d3h
testing-keystone-auth             True      6d3h
testing-nginx-gateway-fabric-crds True      6d3h

# Ende +09:35
```

Demo abspielen
slides.aditsystems.de/ittage_2026

IT SYSTEMS

LEBENSZYKLUS



Upgrade



Patches



Reparatur



Skalierung

IT SYSTEMS

UPGRADE: VERSION ÄNDERN

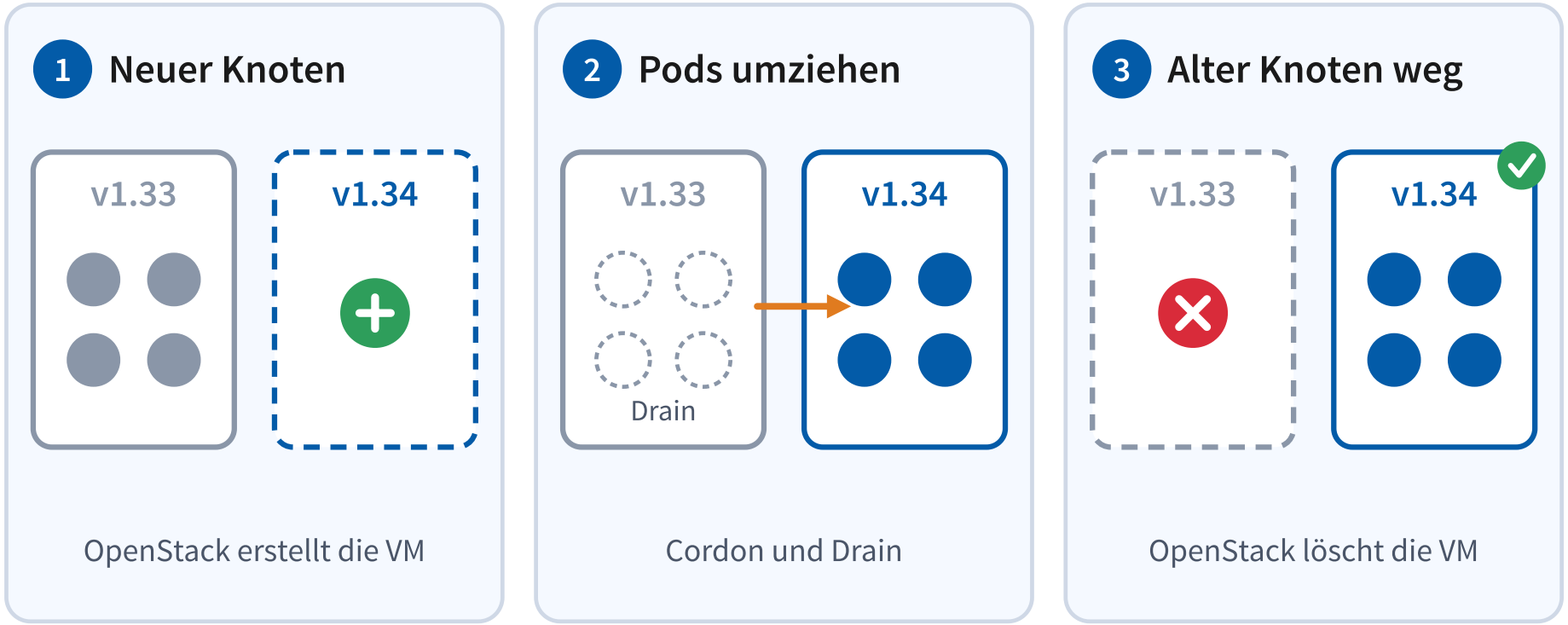
```
kubernetes_version = "v1.33.13"  # war: v1.32.13

worker_templates = {
  "v1" = { flavor = "gp2i.8",  image_name = "Flatcar" }
  "v2" = { flavor = "gp2i.16", image_name = "Flatcar" }
}
active_worker_template = "v2"   # war: "v1"
```

`tofu apply` → CAPI tauscht die Knoten

IT SYSTEMS

ROLLING UPGRADE



IT SYSTEMS

DEMO: UPGRADE

```
── Terminal ──────────────────────────────────────────────────────────────────────

# Neue Version  +15:51
$ kubectl --kubeconfig /tmp/testing-cluster.kubeconfig get nodes
NAME                                  STATUS   ROLES           AGE     VERSION
testing-cluster-control-plane-4qbj6   Ready    control-plane   13m     v1.33.13
testing-cluster-control-plane-7wtqh   Ready    control-plane   7m33s   v1.33.13
testing-cluster-control-plane-m5dtq   Ready    control-plane   10m     v1.33.13
testing-cluster-worker-52znd-bk4rw    Ready    <none>          118s    v1.33.13
testing-cluster-worker-52znd-jxzxv    Ready    <none>          5m3s    v1.33.13

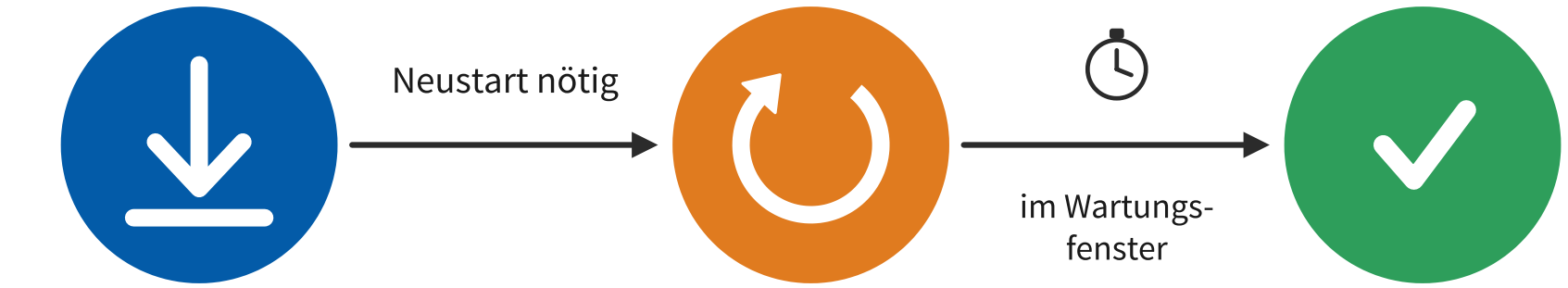
# Ende  +15:56
```



Demo abspielen
slides.aditsystems.de/ittage_2026

IT SYSTEMS

PATCHES OHNE NEUE KNOTEN



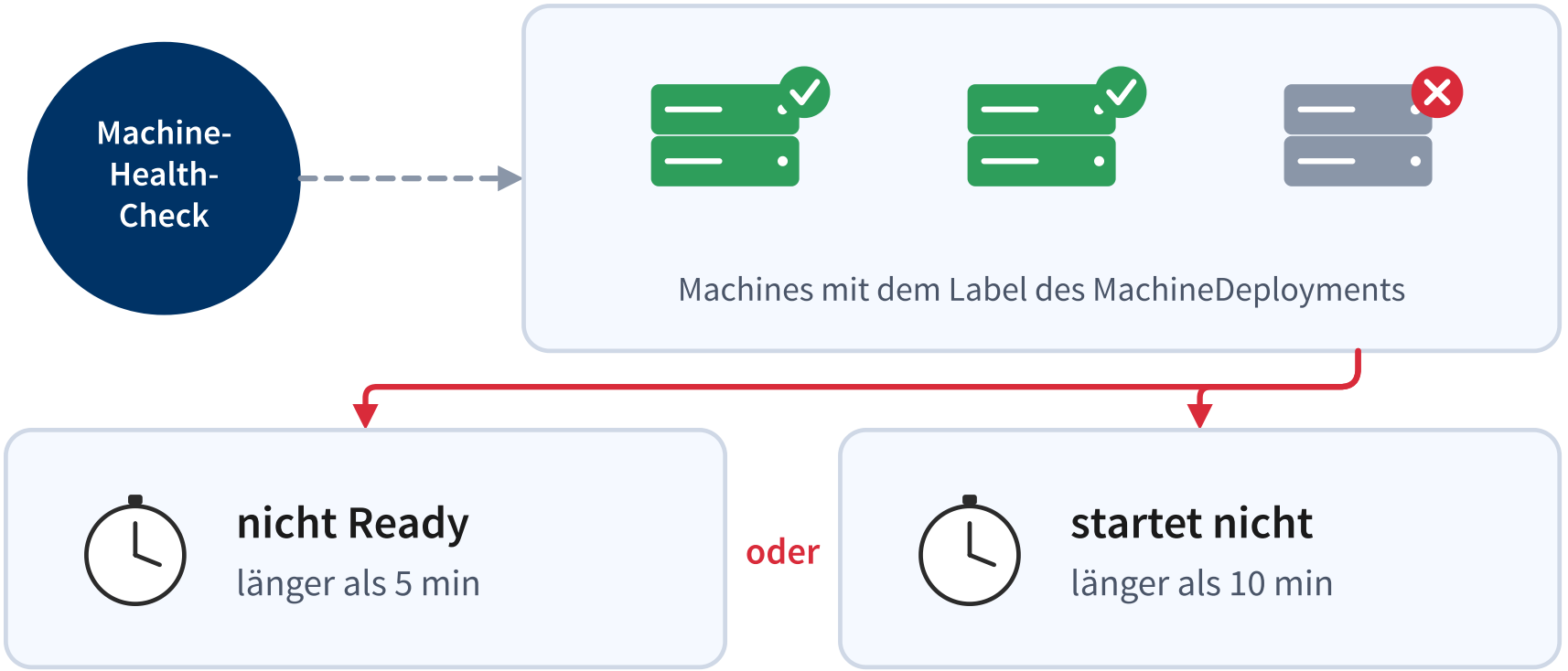
systemd-sysupdate
lädt Patch

kured
Drain und Neustart

Knoten
wieder Ready

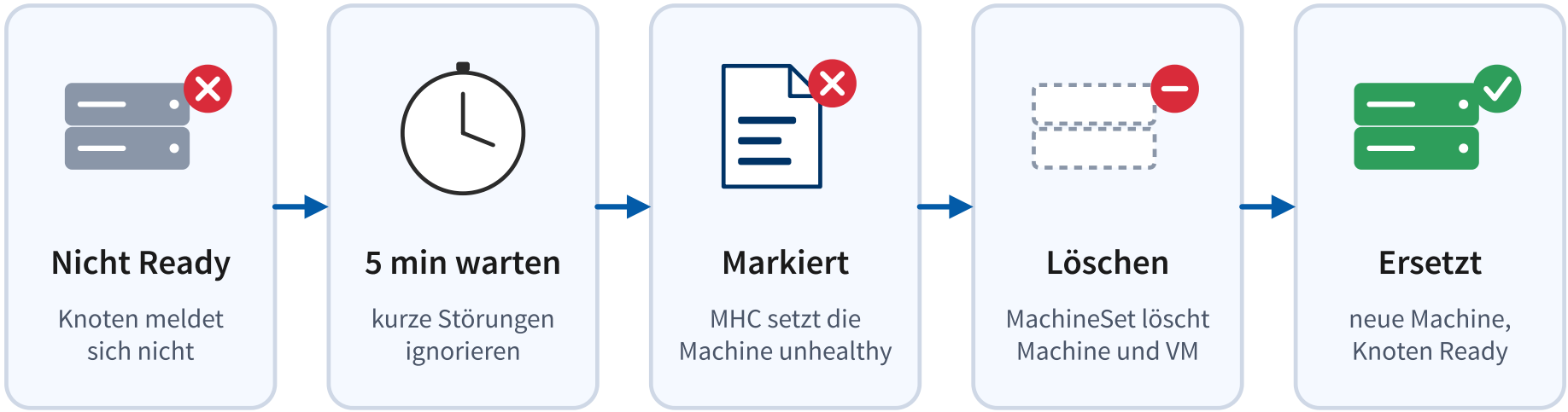
IT SYSTEMS

REPARATUR: MACHINEHEALTHCHECK



IT SYSTEMS

REPARATUR: ERSETZEN



Wie ein Pod im ReplicaSet: weg damit, ein neuer kommt.

IT SYSTEMS

REPARATUR: SICHERUNG

1 von 5 defekt



ersetzen

normaler Ausfall

3 von 5 Unknown





Netzausfall? Mensch prüft

Grenze: höchstens 40 % unhealthy, sonst Stopp

IT SYSTEMS

DEMO: REPARATUR

```
── Terminal ──────────────────────────────────────────────────────────────────────

# Wieder gesund +08:50
$ kubectl --kubeconfig /tmp/testing-cluster.kubeconfig get nodes
NAME                                  STATUS   ROLES           AGE   VERSION
testing-cluster-control-plane-pcl98   Ready    control-plane   13m   v1.33.13
testing-cluster-control-plane-q5ms8   Ready    control-plane   19m   v1.33.13
testing-cluster-control-plane-sw7hl   Ready    control-plane   16m   v1.33.13
testing-cluster-worker-42cpf-7kvkr    Ready    <none>          69s   v1.33.13
testing-cluster-worker-42cpf-w6wtz    Ready    <none>          17m   v1.33.13

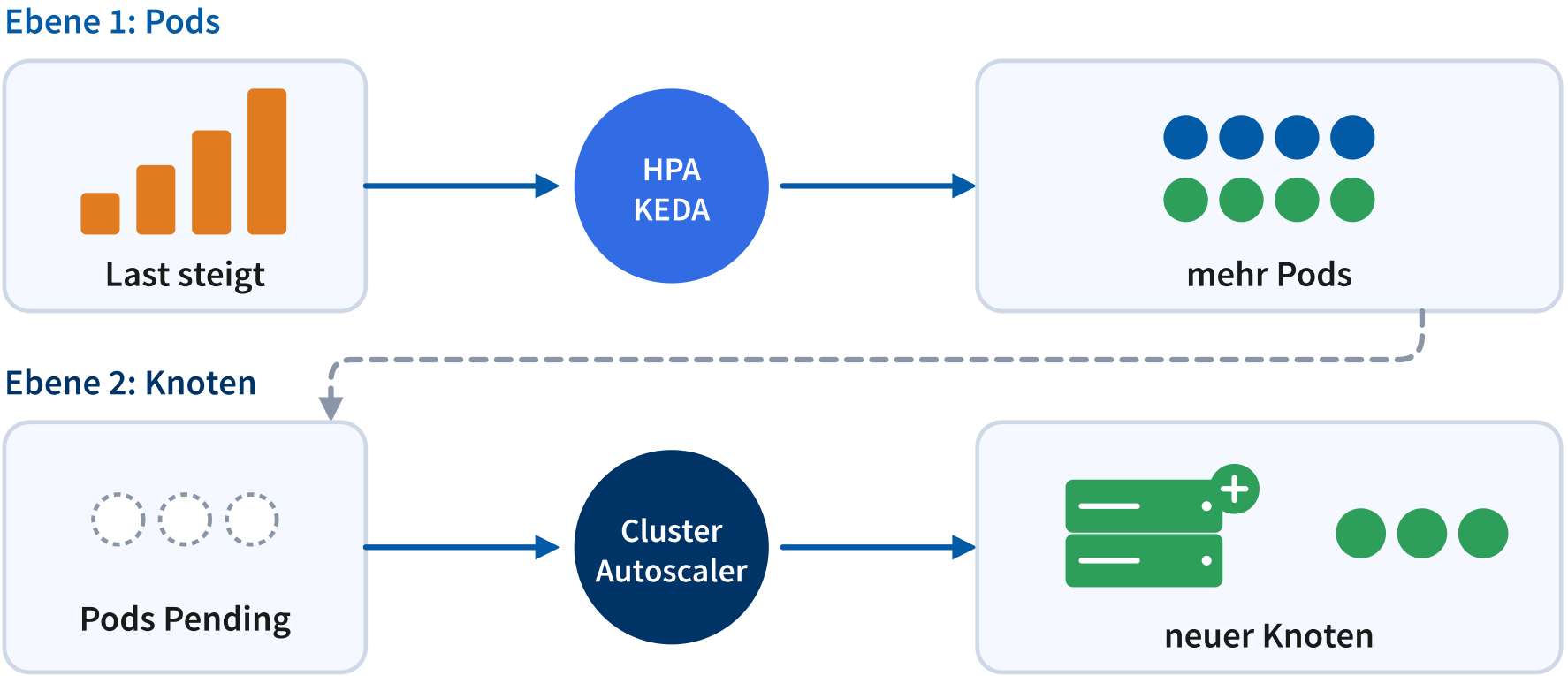
# Ende +08:55
```



Demo abspielen
slides.aditsystems.de/ittage_2026

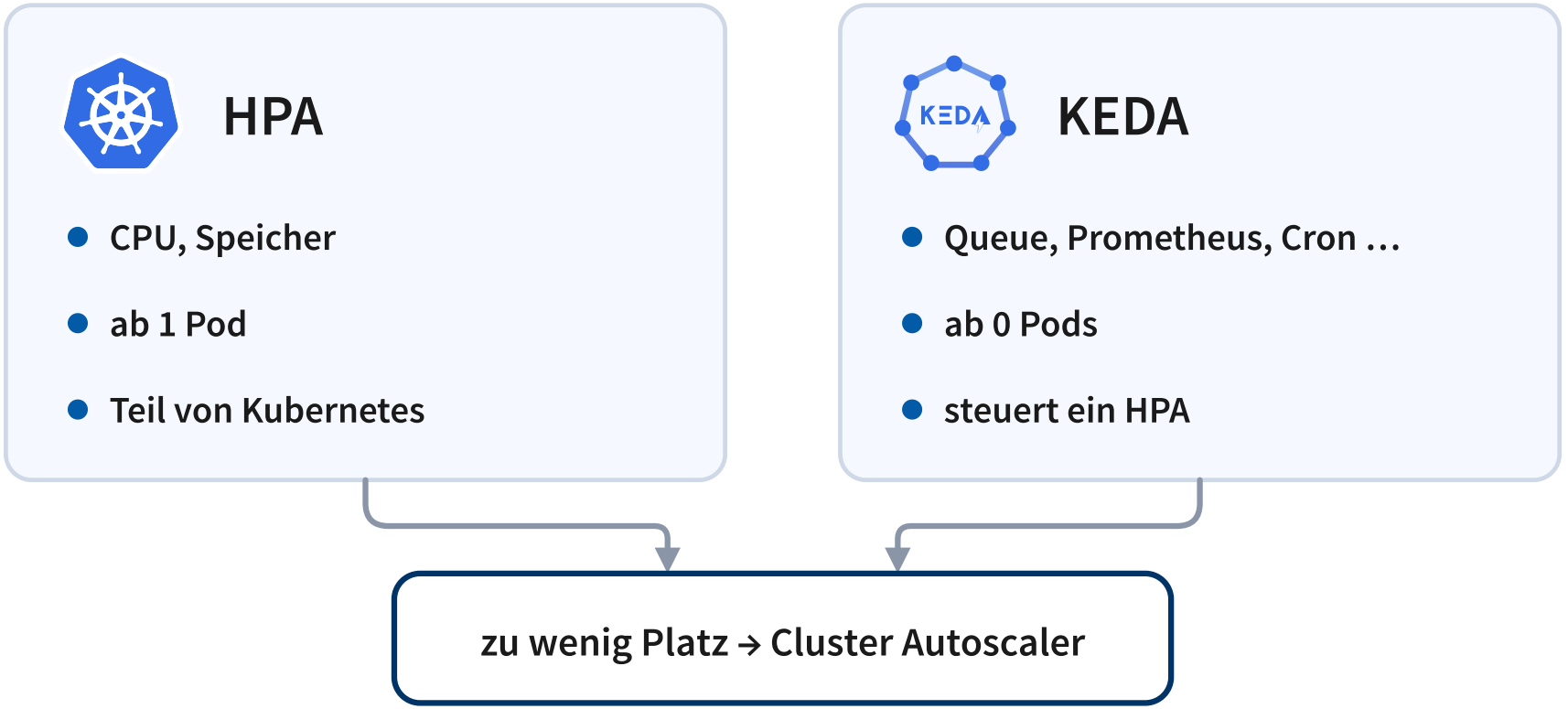
IT SYSTEMS

SKALIERUNG: ZWEI EBENEN



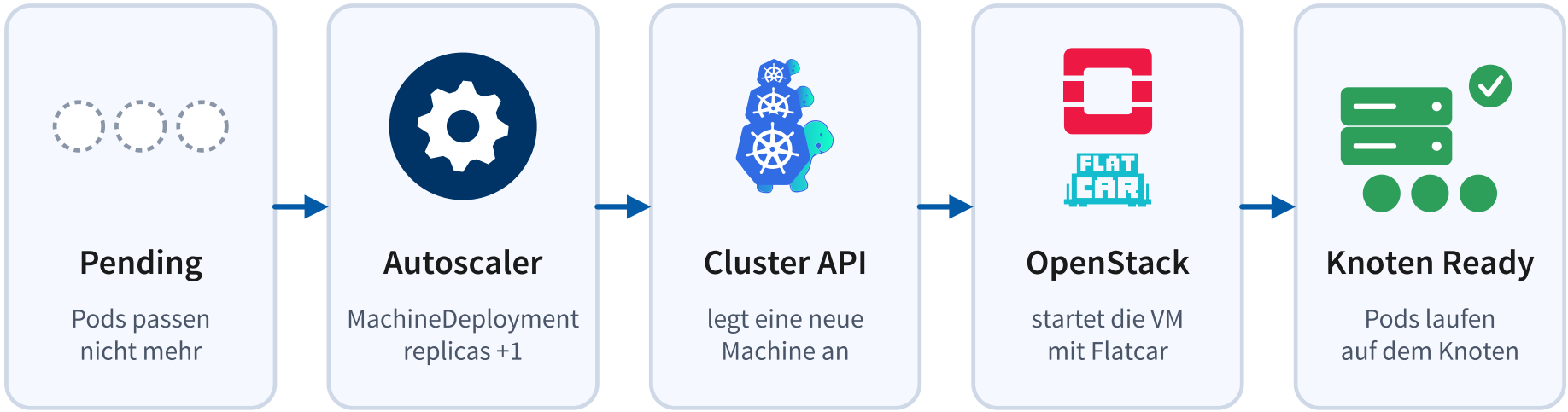
IT SYSTEMS

PODS SKALIEREN: HPA ODER KEDA



IT SYSTEMS

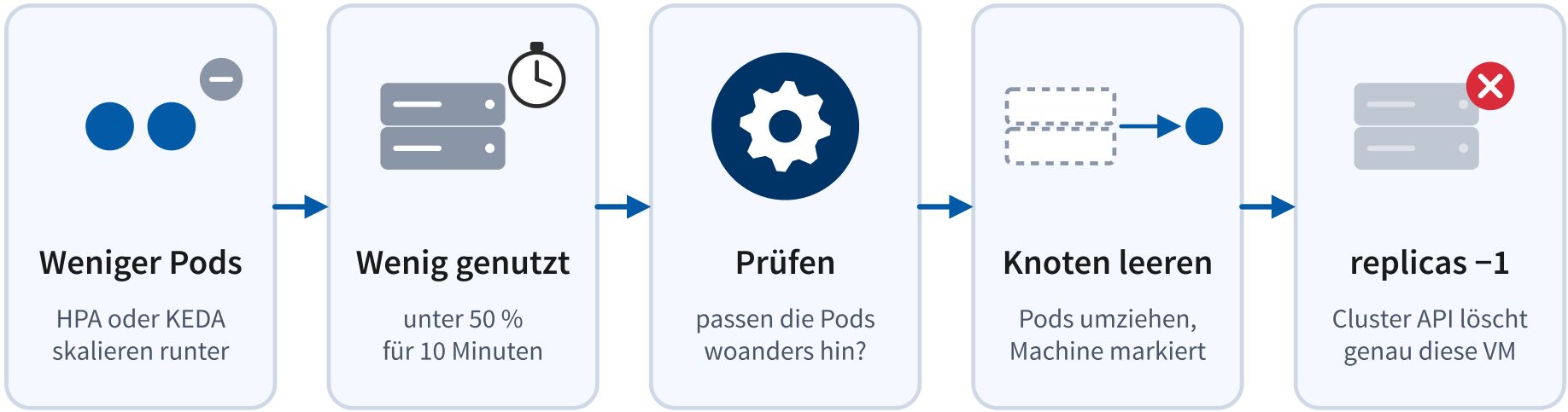
HOCHSKALIEREN



Der Autoscaler ändert nur replicas. Den Rest macht Cluster API.

IT SYSTEMS

HERUNTERSKALIEREN



Grenze nach unten: min-size. PodDisruptionBudgets gelten.

IT SYSTEMS

DEMO: SKALIERUNG

```
── Terminal ──────────────────────────────────────────────────────────────────────

# Alle Pods laufen  +03:10
$ kubectl --kubeconfig /tmp/testing-cluster.kubeconfig get nodes
NAME                                 STATUS   ROLES           AGE   VERSION
testing-cluster-control-plane-pcl98  Ready    control-plane   23m   v1.33.13
testing-cluster-control-plane-q5ms8  Ready    control-plane   29m   v1.33.13
testing-cluster-control-plane-sw7hl  Ready    control-plane   26m   v1.33.13
testing-cluster-worker-42cpf-5w2n9   Ready    <none>          75s   v1.33.13
testing-cluster-worker-42cpf-7kvkr   Ready    <none>          11m   v1.33.13
testing-cluster-worker-42cpf-w6wtz   Ready    <none>          27m   v1.33.13

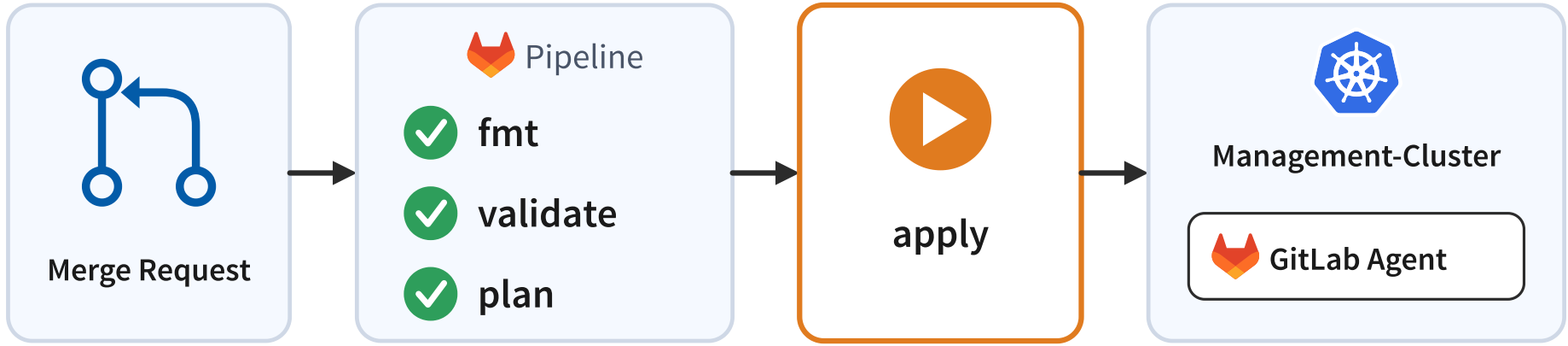
# Aufräumen  +03:15
$ kubectl --kubeconfig /tmp/testing-cluster.kubeconfig delete deployment inflate
deployment.apps "inflate" deleted from default namespace

# Ende  +03:21
```

Demo abspielen
slides.aditsystems.de/ittage_2026

IT SYSTEMS

GITOPS MIT GITLAB



jede Änderung
mit Review

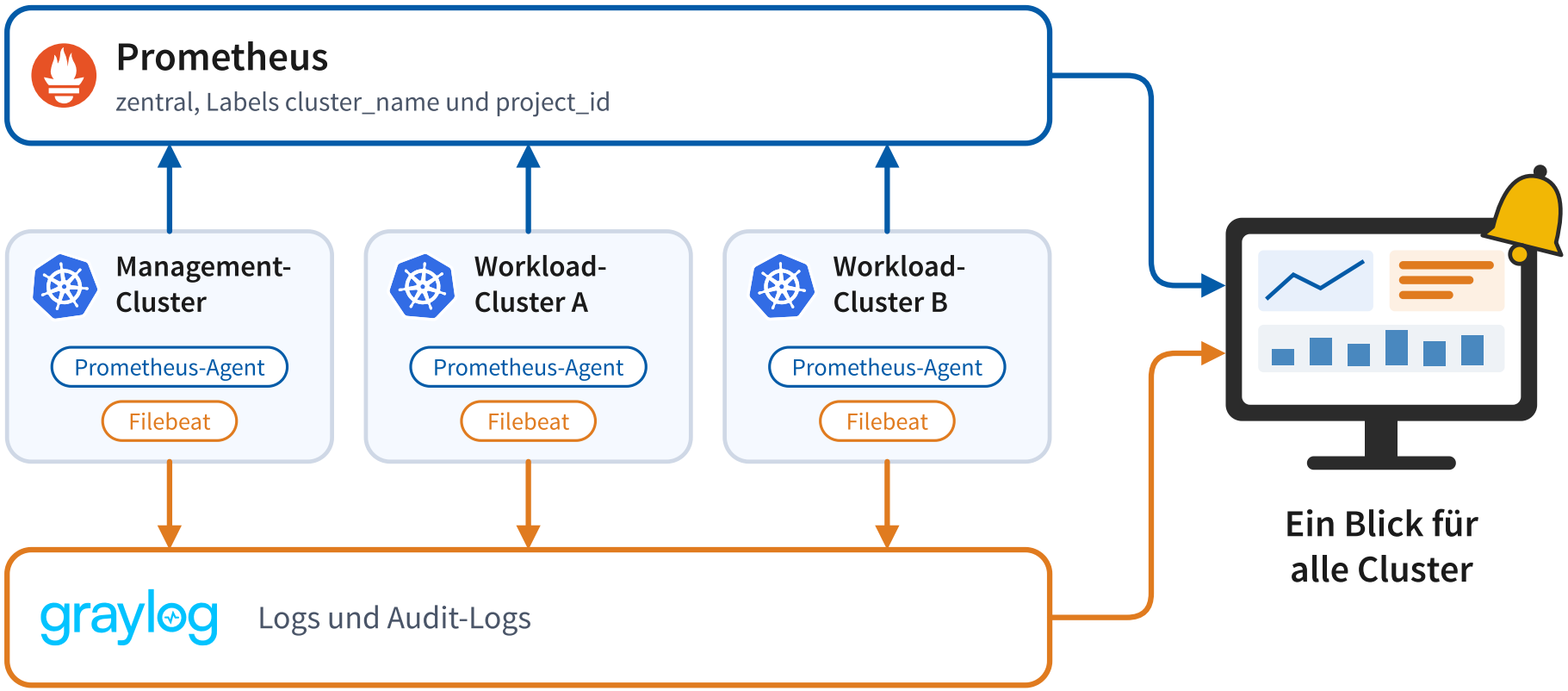
läuft bei
jedem Push

manueller Job
nach dem plan

Agent nimmt die
Änderung an

IT SYSTEMS

MONITORING UND LOGS



IT SYSTEMS

ERFAHRUNGEN

Templates unveränderlich



nicht änderbar

neu anlegen, umschalten

Löschen hängt fest



Abbau hängt für immer

OpenTofu wartet ab

Apply fertig ≠ Cluster bereit



VMs fehlen noch

auf Bereitschaft warten

HA weg nach Upgrade

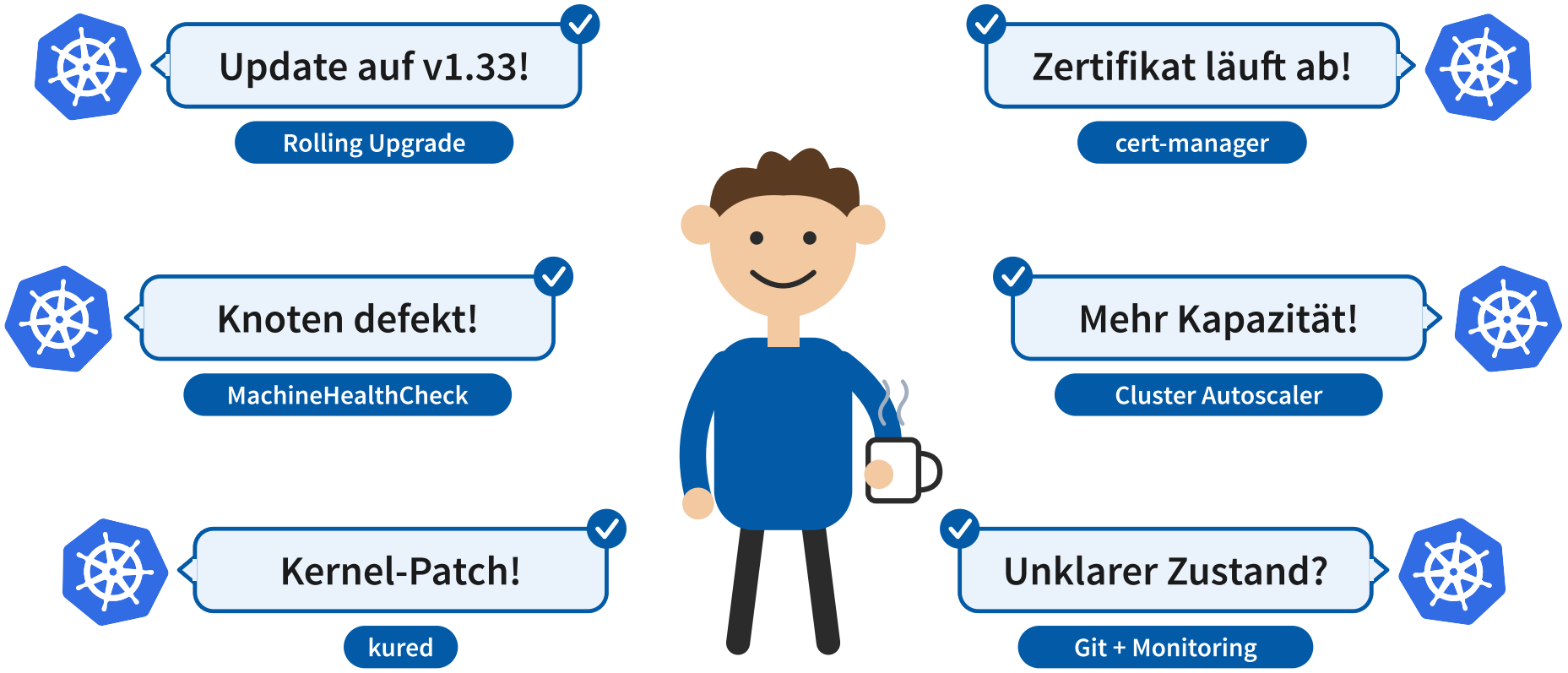


nach clusterctl upgrade: 1

Replicas wieder auf 3

IT SYSTEMS

VORTEILE IM BETRIEB



Einheitlich. Reproduzierbar. Automatisch. Souverän.

IT SYSTEMS

FRAGEN?

Viele Cluster. Wenige Leute. Eigene Infrastruktur.

Folien

Mastodon

LinkedIn

IT SYSTEMS