



Belastingdienst

Container Chaos to Platform Power

de Engineering reis van
de Belastingdienst

Jeroen Wolff

Platform Architect

Belastingdienst

j.wolff@belastingdienst.nl

Gerben Welter

Platform Specialist

HCS Company



van één
(overloaded)
container
cluster



Naar...





Belastingdienst

Container Hosting Platform

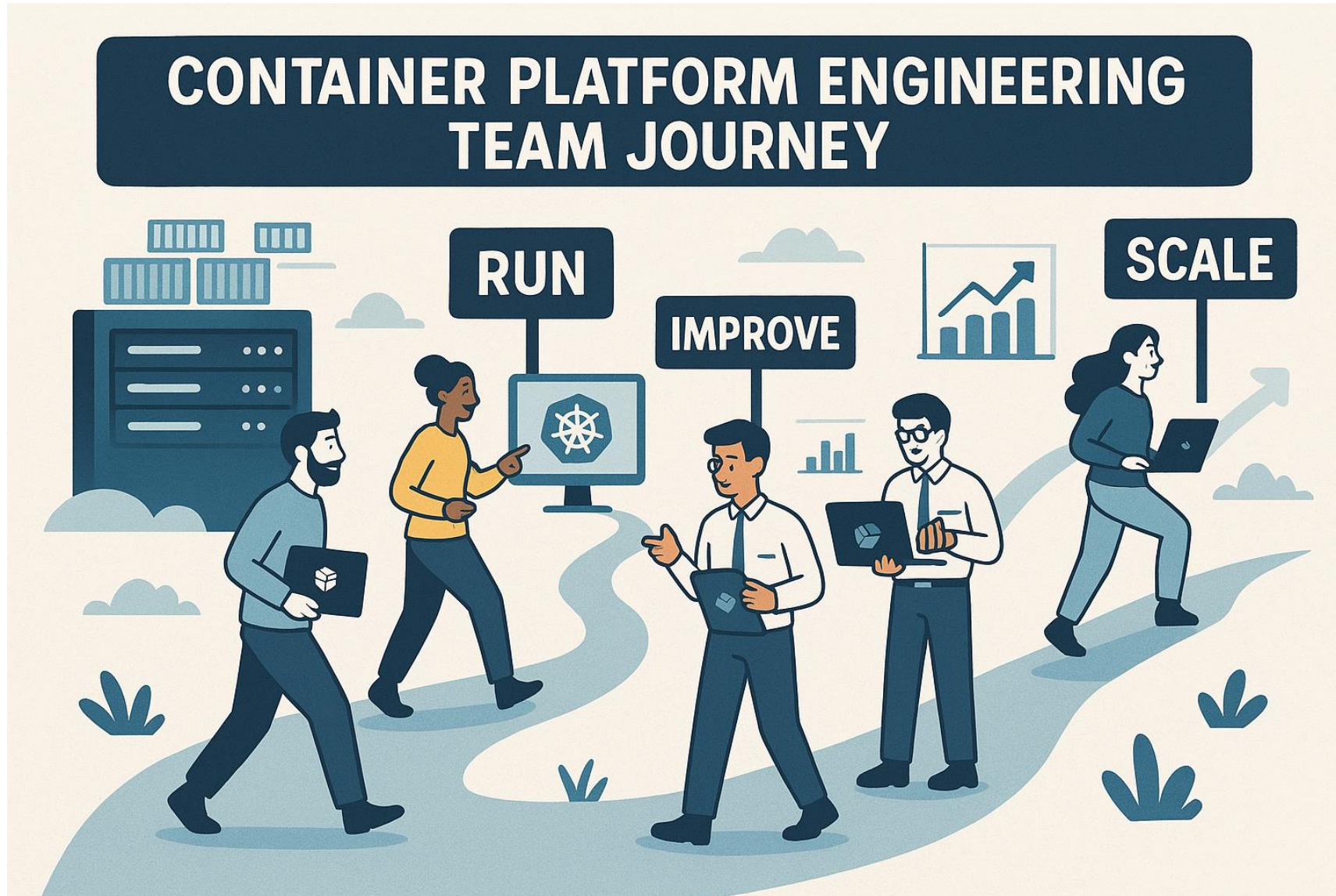
&

Container Platform Engineering



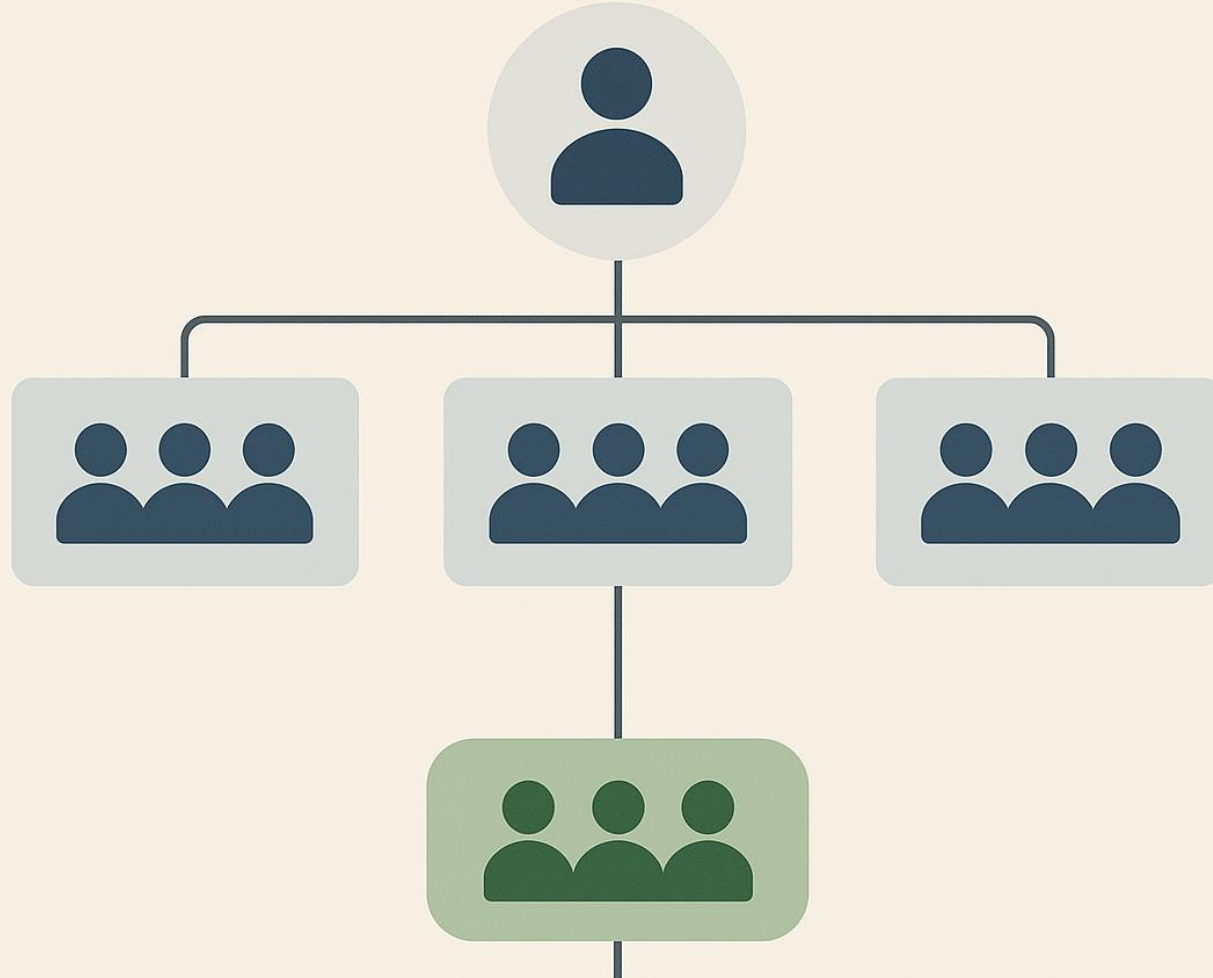
CONTAINER PLATFORM ENGINEERING TEAM JOURNEY

2021



2025

Organisatie



Organisatie



* De directeur van de Chief Technology Officer Office fungeert in de rol van Chief Technology Officer.



Wat is dan WEL belangrijk...

Team CHP⁽⁸⁾

Leveren clusters/infra

&

Team CPET⁽²⁴⁾

Managed clusters
Onboarding
Leveren capabilities
 Path

Organisatie

CHPET

Hoe?

Focus on self-service voor
DevOps teams

Platform Engineering Team

Team CHP(8)

Leveren clusters/infra

&

Team CPET(24)

Managed clusters
Onboarding
Leveren capabilities
 Path



Hoe?

**Cluster (6)
Infra (8)**

Tooling (6)

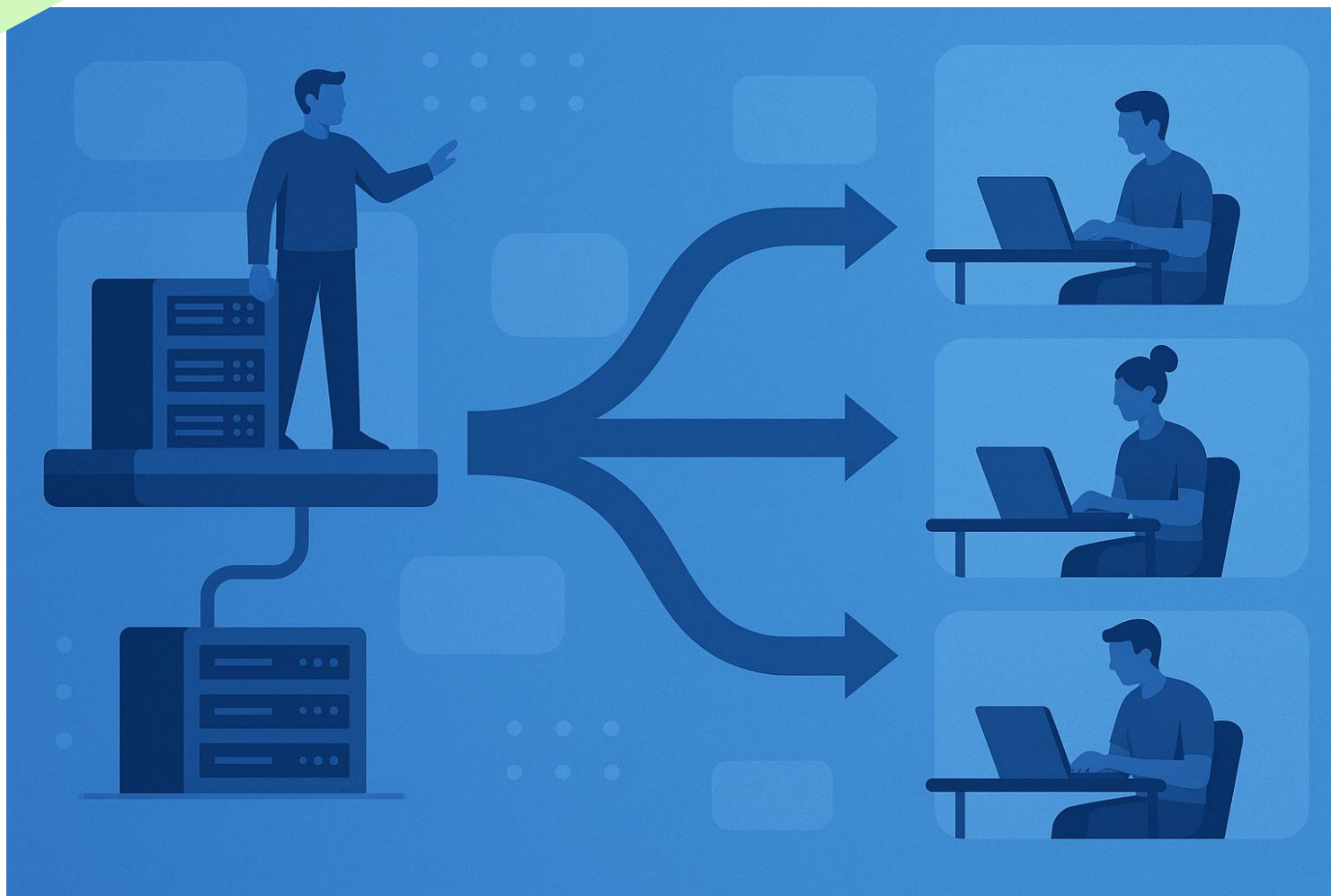
**DevOps
Capabilities (8)**

**Service
& Enablement
(4)**

CHPET subteams (32)



Aanbod



De 3 lagen van CHPET



Guardian

Cloud Native way of working



(Platform) Engineering

Cloud Native Content / Golden Path



Project As A Service™

Provider

Cloud Native Platform



Product Teams



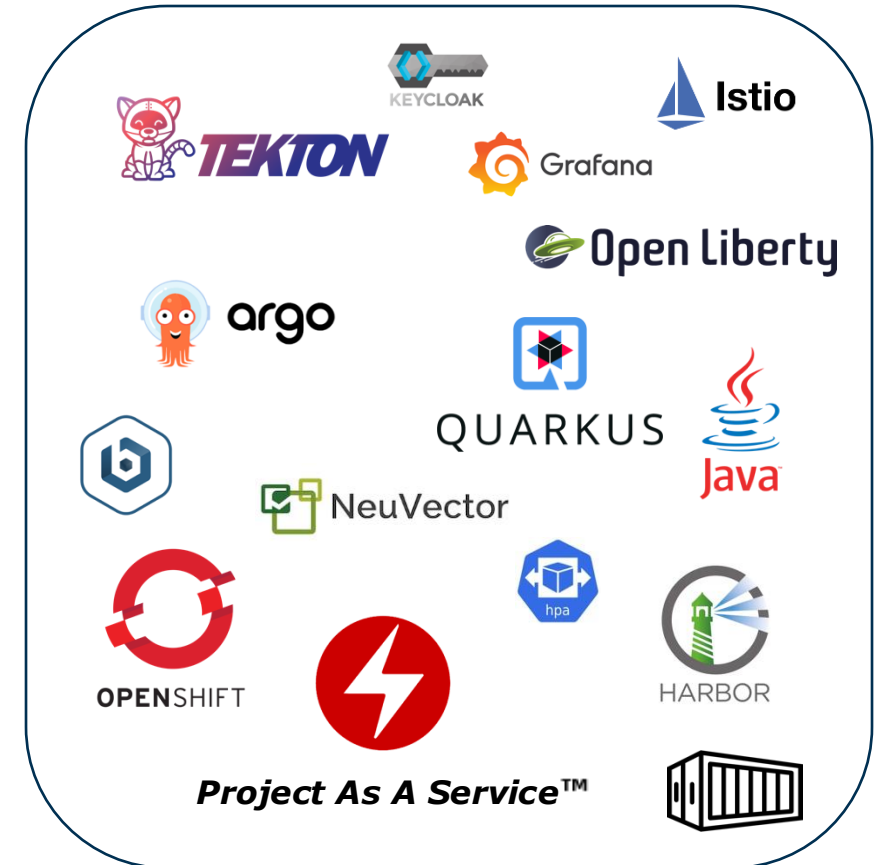
***Integratie
product team***



***APM
product team***

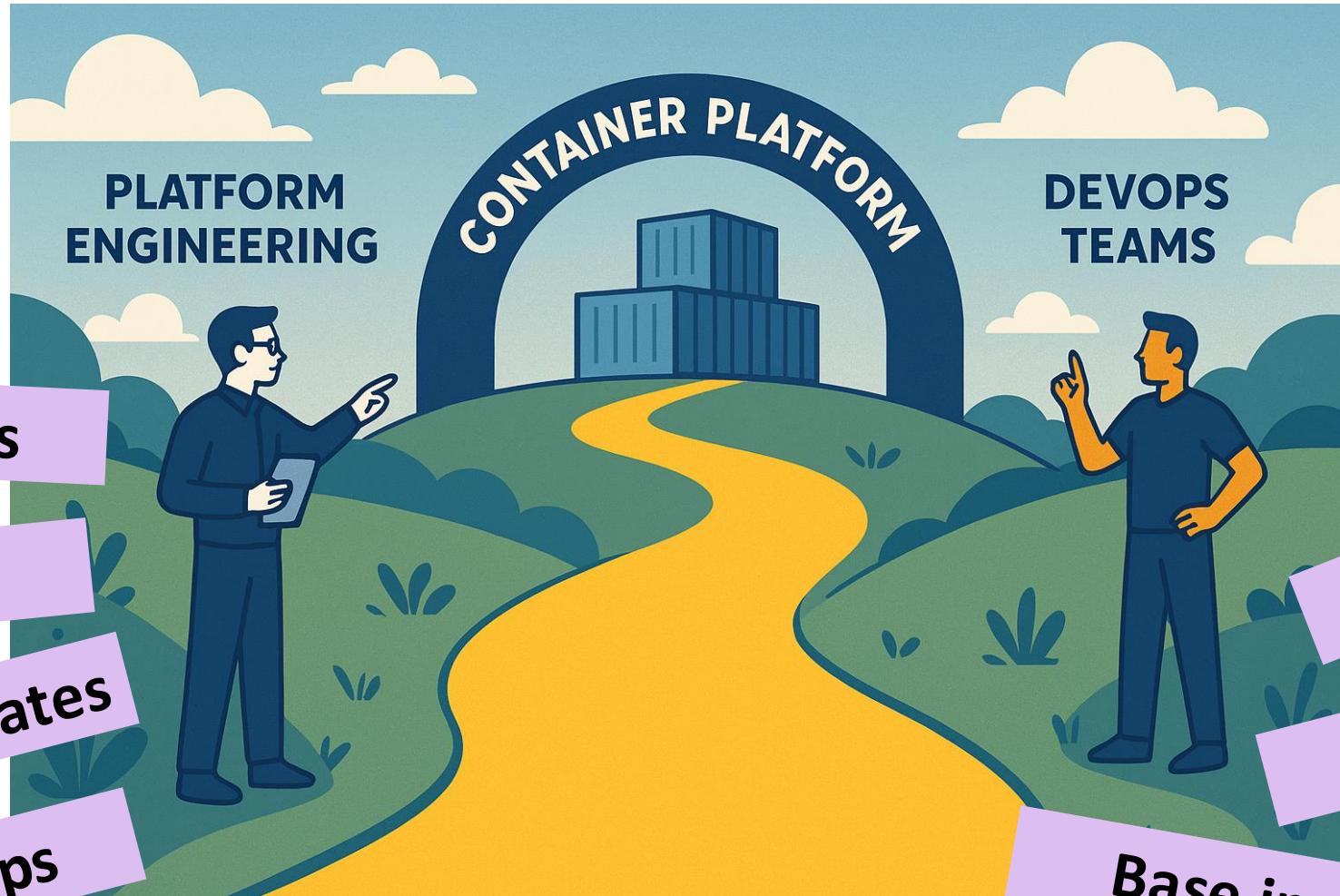


***Databases
product team***



CHPET

Golden Path



White papers

Snippets

Pipeline templates

Example apps

Dashboards

Recipes

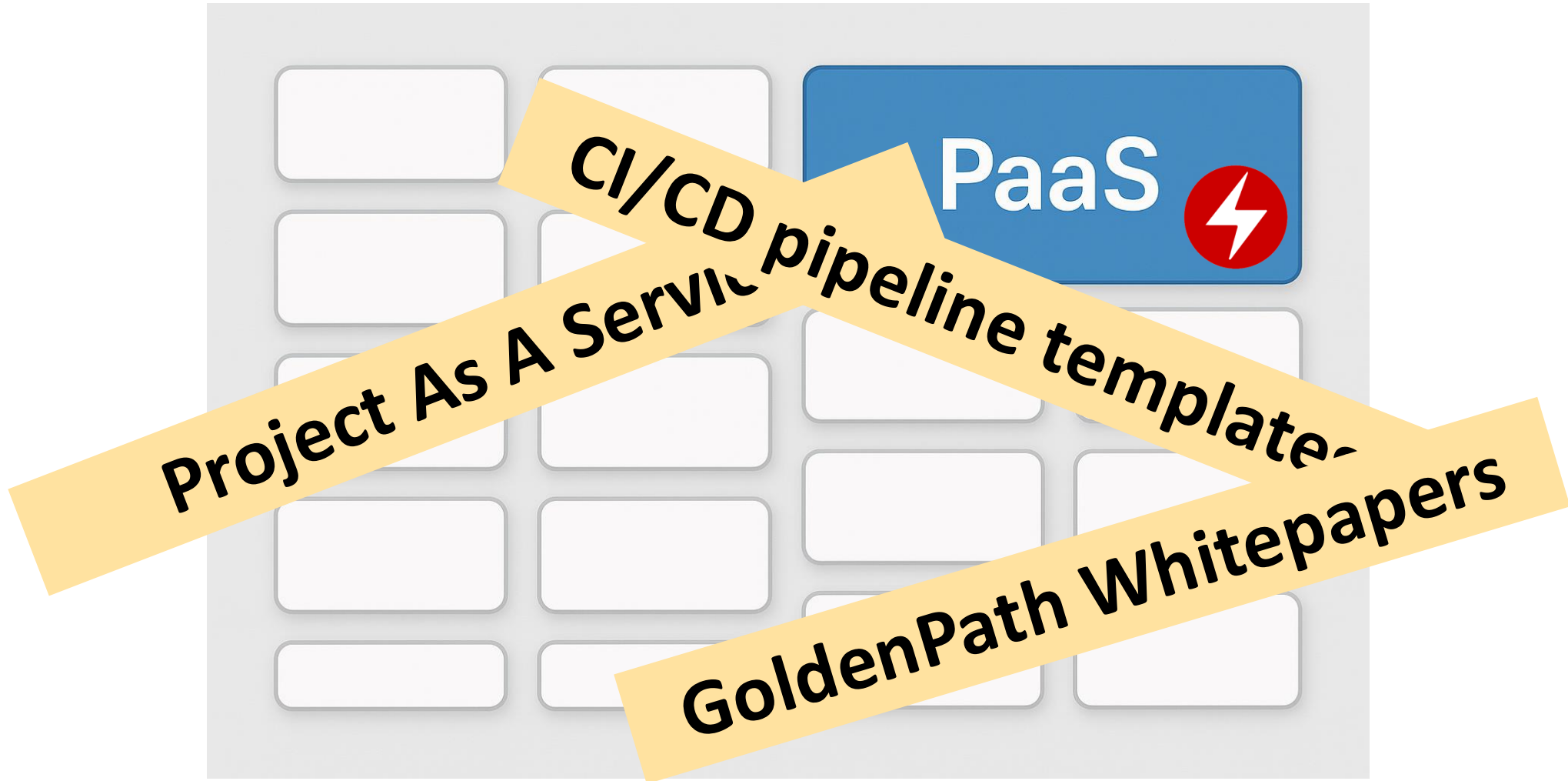
Base images

Onboarding / Workshops

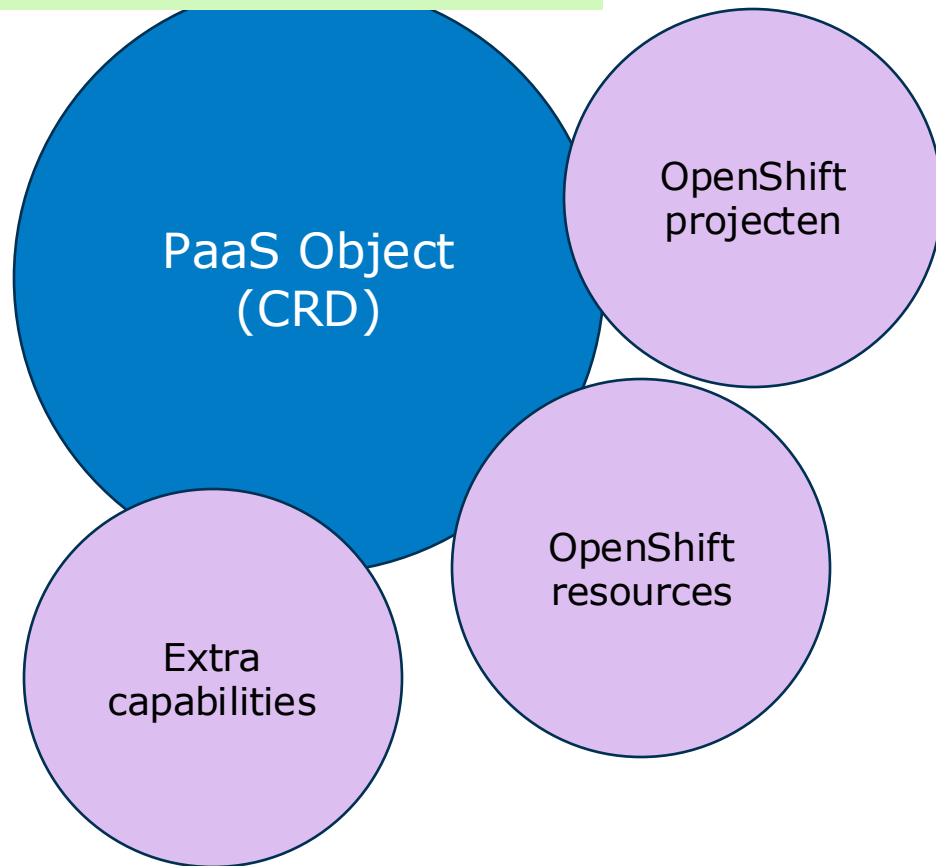




Internal Developer Portal



PaaS Operator



Configuratie PaaS

```
1 ---
2 apiVersion: cpet.belastingdienst.nl/v1alpha1
3 kind: Paas
4 metadata:
5   labels:
6     app.kubernetes.io/part-of: opr-paas
7     app.kubernetes.io/managed-by: kustomize
8     app.kubernetes.io/created-by: opr-paas
9   name: abc-def
10 spec:
11   requestor: CA0XXXXXX
12   groups:
13     aug_abc_def: # <-- naam van group
14       query: CN=aug_abc_def,OU=paas,OU=caas,OU=corp,DC=prod,DC=acme,DC=org # <-- query van de ldap group voor synchronisatie van users naar de CN=groep
15       users: # <-- userid's die aan de CN=groep worden toegevoegd los van de ldap synchronisatie
16         - doej01
17   quota:
18     limits.cpu: "9"
19     limits.memory: 10Gi
20     requests.cpu: "3"
21     requests.memory: 5Gi
22     requests.storage: 50Gi
23   capabilities:
24     argocd: # 1)
25       sshSecrets:
26         'ssh://git@git.belastingdienst.nl:7999/xxx/xxx-demo-deploy.git': >~
27           29jo0Ew54/6D9VEB/wbBz7e8IXqtTf17m1CKvgJXp6+rIGdG0c+FnuIPyY/mIk2+E4WtL+Qj+NMa ... 5jjYyCKhc9SugCG+sVPeTJY0DInbMaZ0pjEf6aCU58GqQdAXj4A==
28       enabled: true
29       gitUrl: ssh://git@git.belastingdienst.nl:7999/abc/def.git
30       gitRevision: develop
31       gitPath: argocd
32   tekton: # 2)
33     enabled: true
```

PaaS Operator



Configuratie PaaS

```
1 ---
2 apiVersion: cpet.belastingdienst.nl/v1alpha1
3 kind: Paas
4 metadata:
5   labels:
6     app.kubernetes.io/part-of: opr-paas
7     app.kubernetes.io/managed-by: kustomize
8     app.kubernetes.io/created-by: opr-paas
9   name: abc-def
10 spec:
11   requestor: CA0XXXXXX
12   groups:
13     aug_abc_def: # <-- naam van group
14       query: CN=aug_abc_def,OU=paas,OU=caas,OU=corp,DC=prod,DC=acme,DC=org # <-- query van de ldap group voor synchronisatie van users naar de CN=groep
15       users: # <-- userid's die aan de CN=groep worden toevoegegd los van de ldap synchronisatie
16         - doej01
17   quota:
18     limits.cpu: "9"
19     limits.memory: 10Gi
20     requests.cpu: "3"
21     requests.memory: 5Gi
22     requests.storage: 50Gi
23   capabilities:
24     argocd: # 1)
25       sshSecrets:
26         'ssh://git@git.belastingdienst.nl:7999/xxx/xxx-demo-deploy.git': >-
27           29jo0Ew54/6D9VEB/wbBz7e8IxtuTf17miCKvgJXp6+rIGdG0c+FnUIPyY/mIk2+E4WtL+Qj+NMaa ... 5jjYyCKhc9SUGCG+sVPeTJY0DInbMaZ0pjEf6aCU58GqQdAXj4A==
28         enabled: true
29       gitUrl: ssh://git@git.belastingdienst.nl:7999/abc/def.git
30       gitRevision: develop
31       gitPath: argocd
32   tekton: # 2)
33     enabled: true
```

PaaS Capabilities



IBM Cloudpak
Business Automation



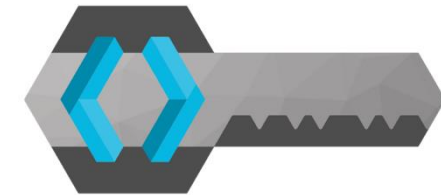
Tekton



ArgoCD



Grafana



KEYCLOAK

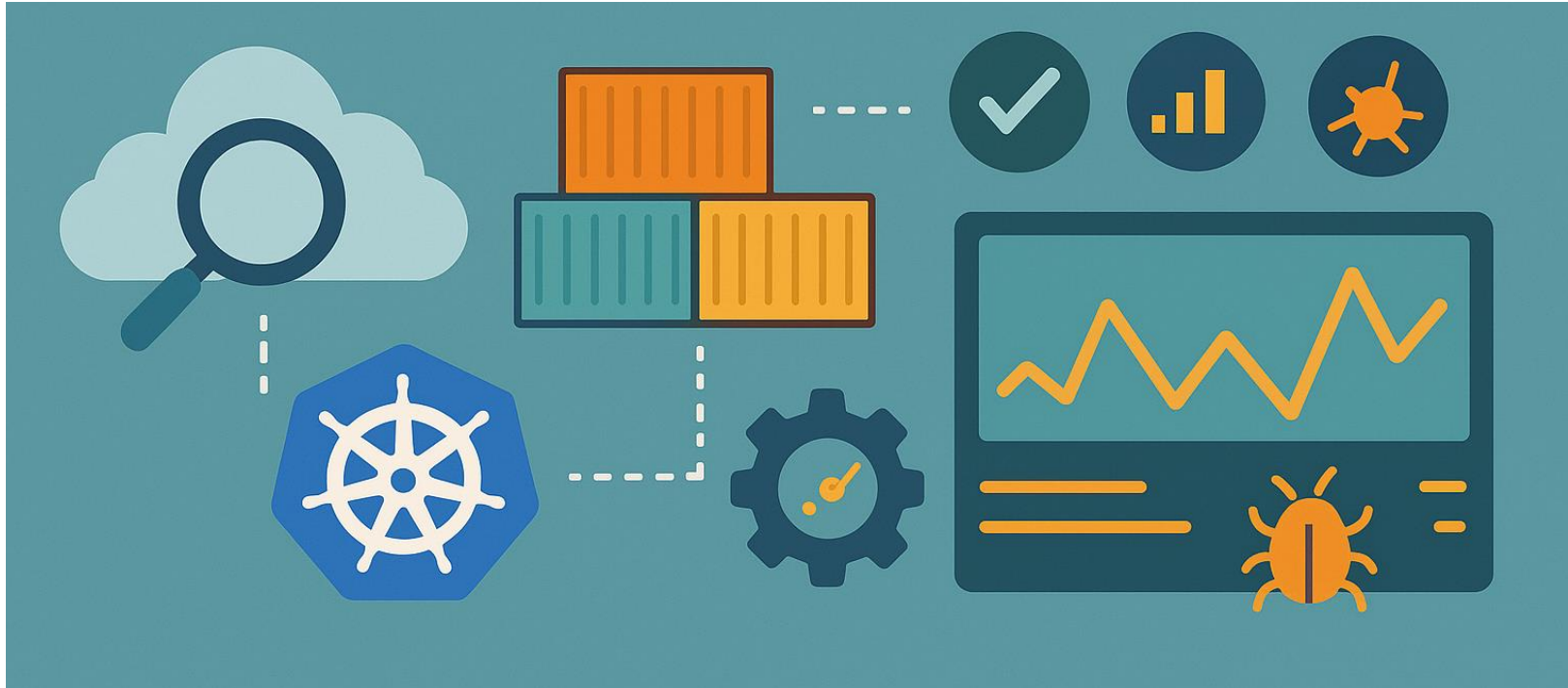


Custom Capabilities 19

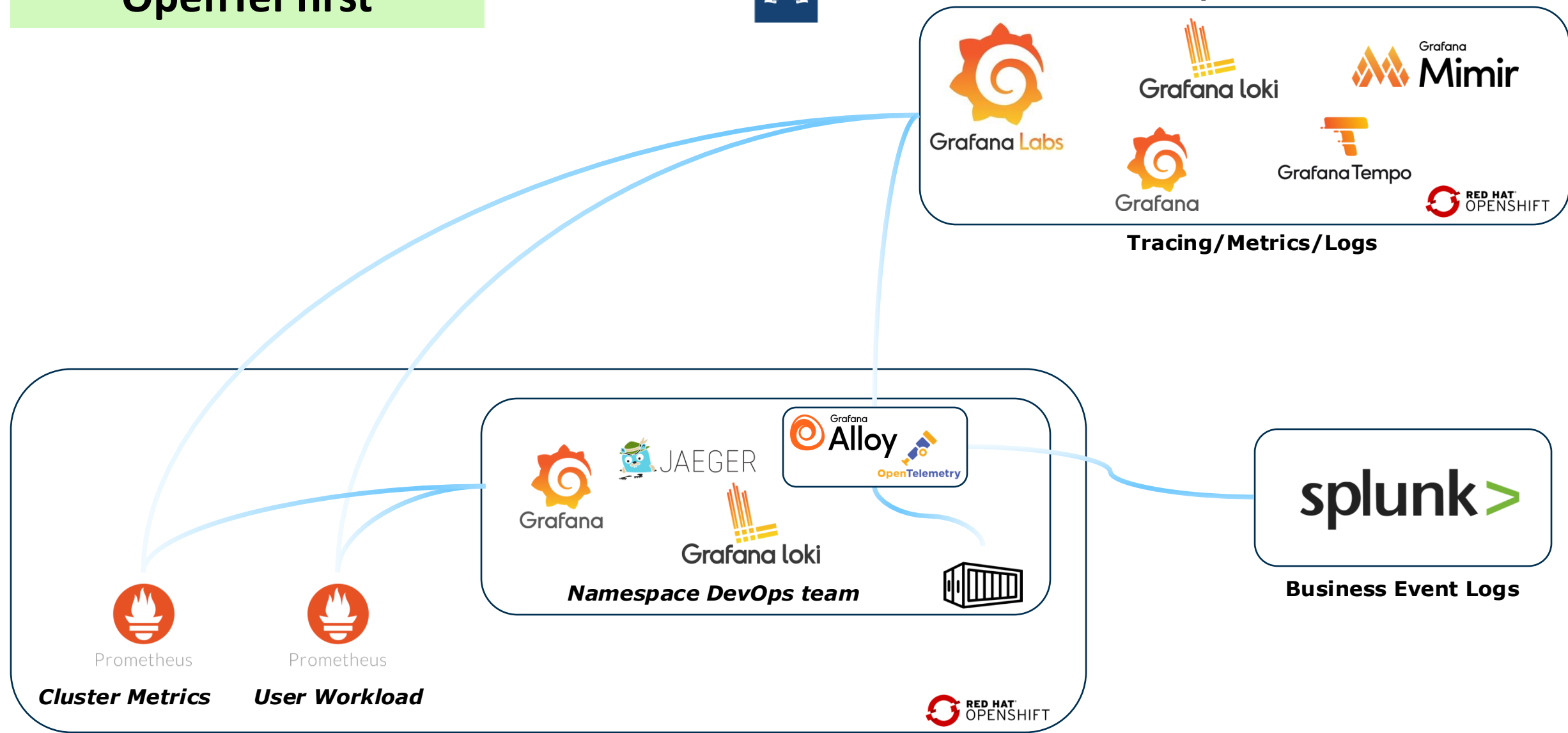


<https://github.com/belastingdienst/opr-paas>

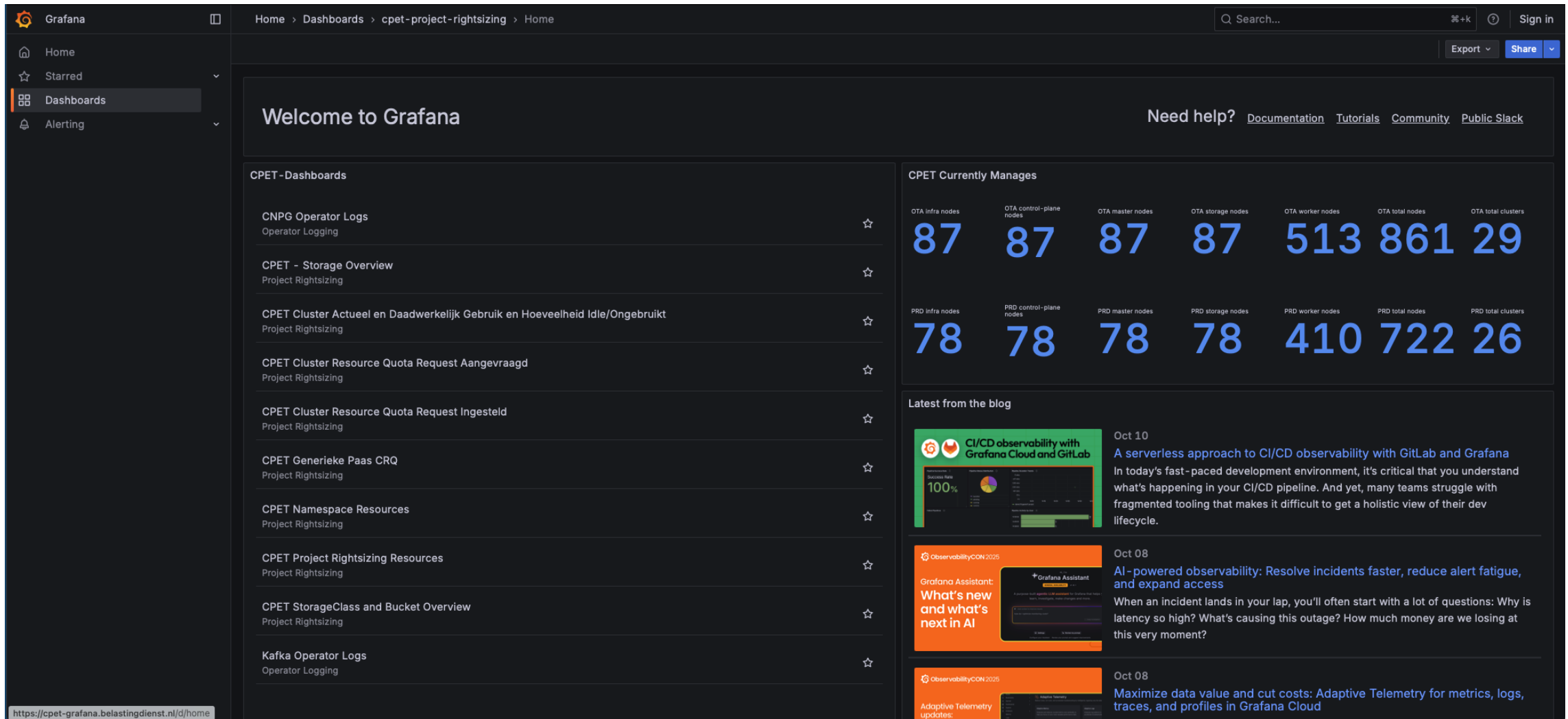
Observability



OpenTel first



Monitoring



Grafana dashboard voor iedereen in de organisatie

Cluster Types



Internet facing

Cloud Native

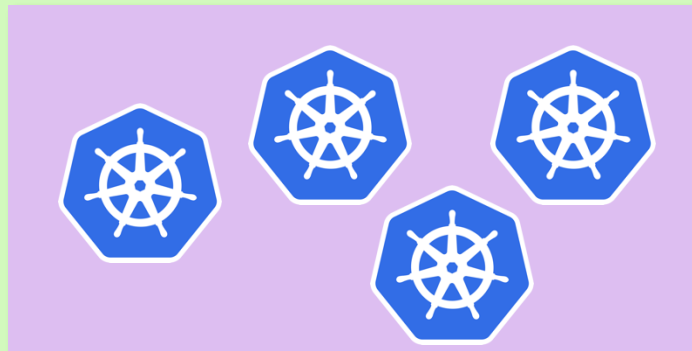
Commercial Of
The Shelf

Type workload cluster



**CloudNative
Clusters**

OTA (29)



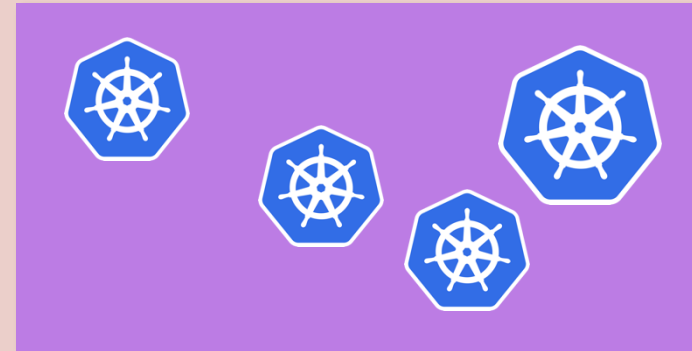
Shared & Dedicated clusters

**Common of
the Shelf
Clusters**



Dedicated clusters

P (26)

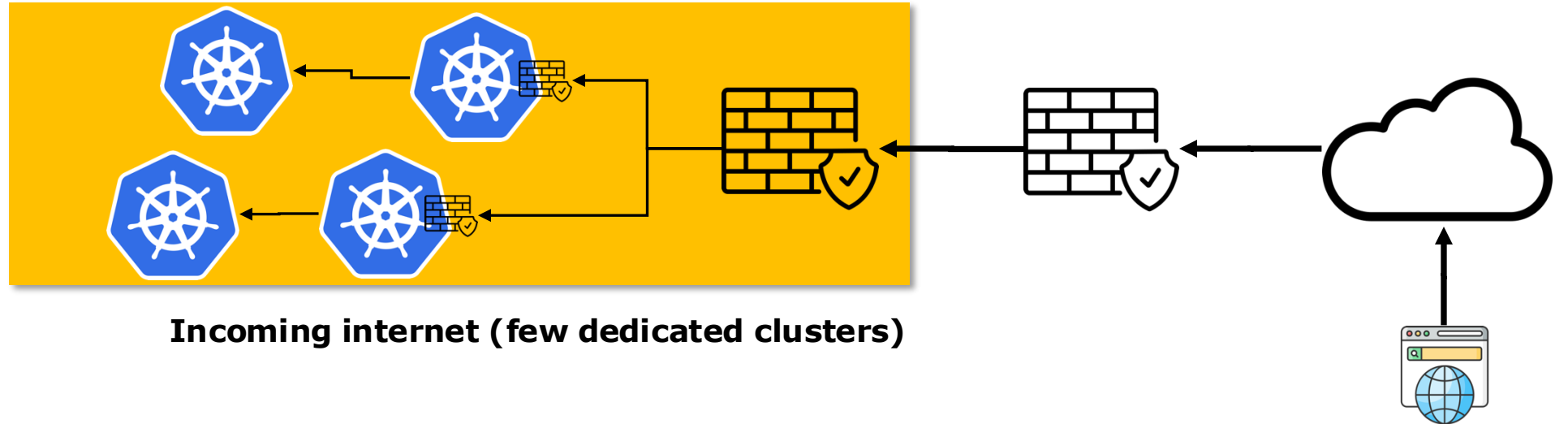


Shared & Dedicated clusters

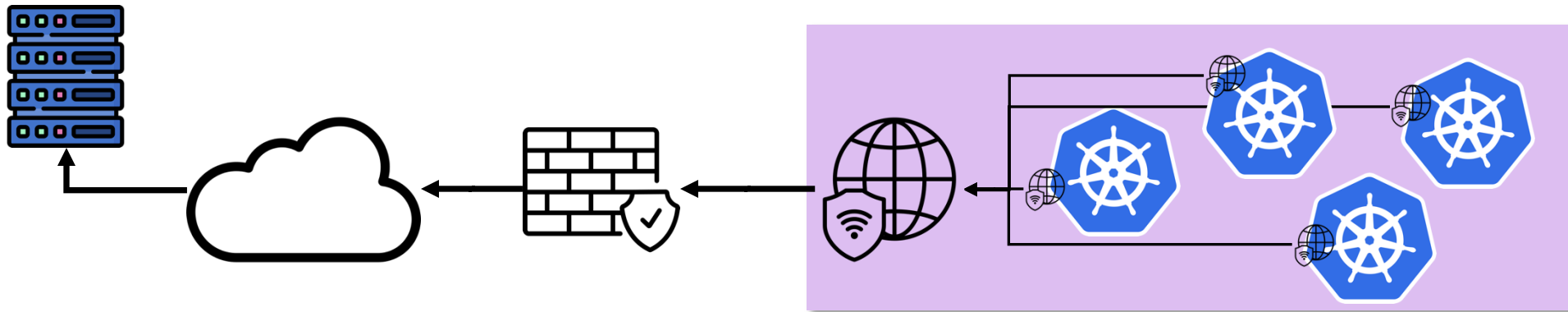


Dedicated clusters

Internet facing



Incoming internet (few dedicated clusters)



Outgoing internet (all clusters)

Internet



Alleen CHPET

(op CHPET beheerde clusters)

Air-gapped

**Eén cluster
met Internet
via proxy**

Renovate

Image mirror

**Helm charts
(incl. images)
mirror**

Klassieke proxy oplossing



Niet container aware

Voordelen:

Teams kunnen zelf:

- allowlist aanmaken
- IP-adressen toevoegen

Nadelen:

Teams kunnen zelf:

- allowlist aanmaken
- IP-adressen toevoegen

Teams kunnen Worker nodes toevoegen

Team A zet destination ook voor Team B,C, etc open

Geen traceerbaarheid door ontbreken authenticatie.



Uitdagingen



Vertraging:

- Afdeling Netwerken kon niet beslissen over oplossing
- Andere projecten hadden meer prio

Techniek:

- IP-adressen hebben geen eigenaar

Proces:

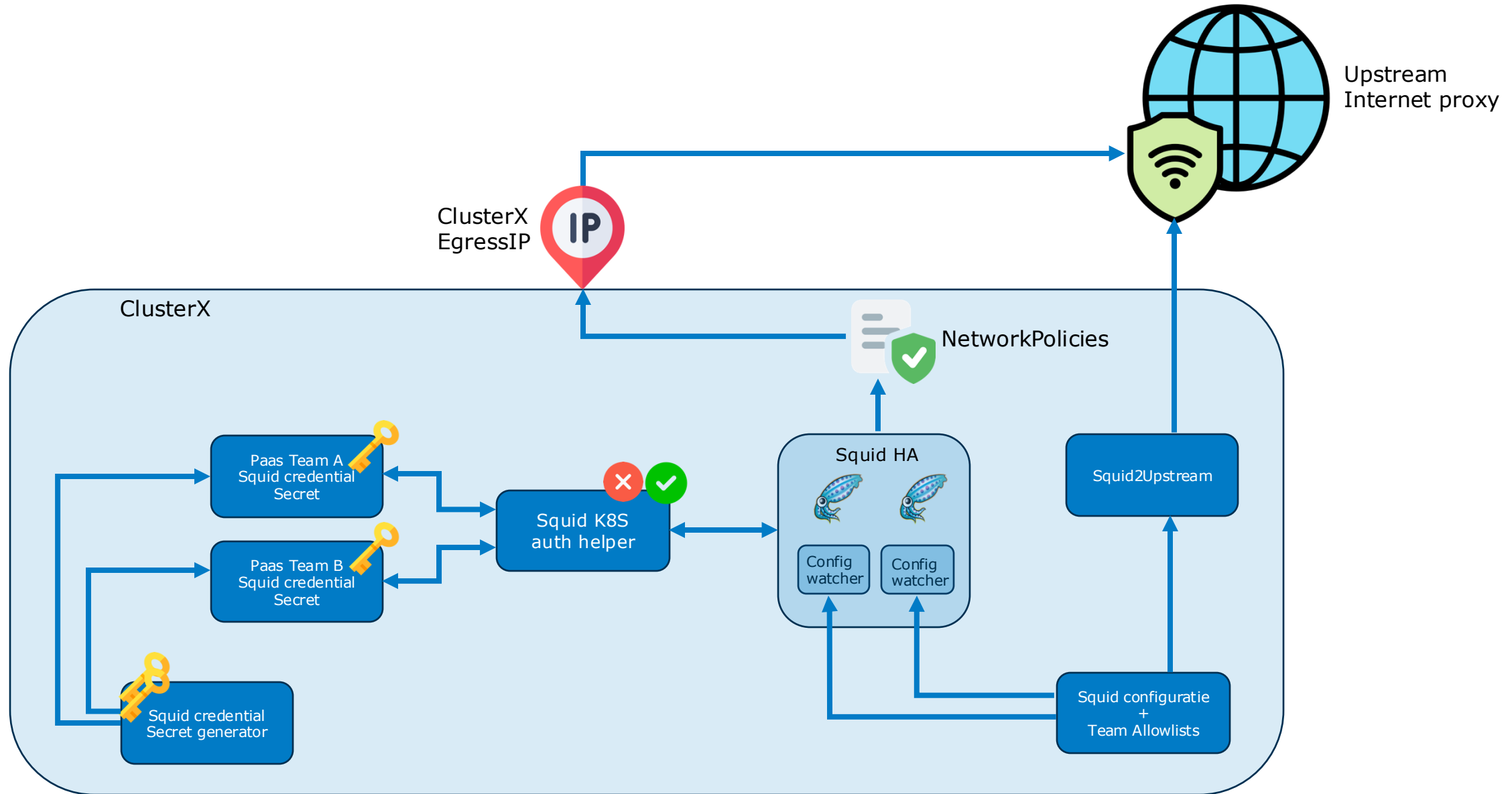
- Aanvragen losse IP-adressen paste niet in proces.
- Proces verandert



Pakket van eisen:

- Verkeer vanaf OpenShift onder controle van CHPET
- Teams kunnen zelf allowlist aanmaken dmv Pull Request
- Allowlist per team
- Team overstijgende allowlist
- Allowlist zonder authenticatie
 - Uitzondering
 - Niet-Paas gerelateerde workload
 - Applicatieconfiguratie
- Content Scanning standaard
 - Mogelijkheid tot uitschakelen
- Compleet geautomatiseerd







Wat getallen

55 Clusters (29 OTA, 26 PROD)

513 OTA worker nodes

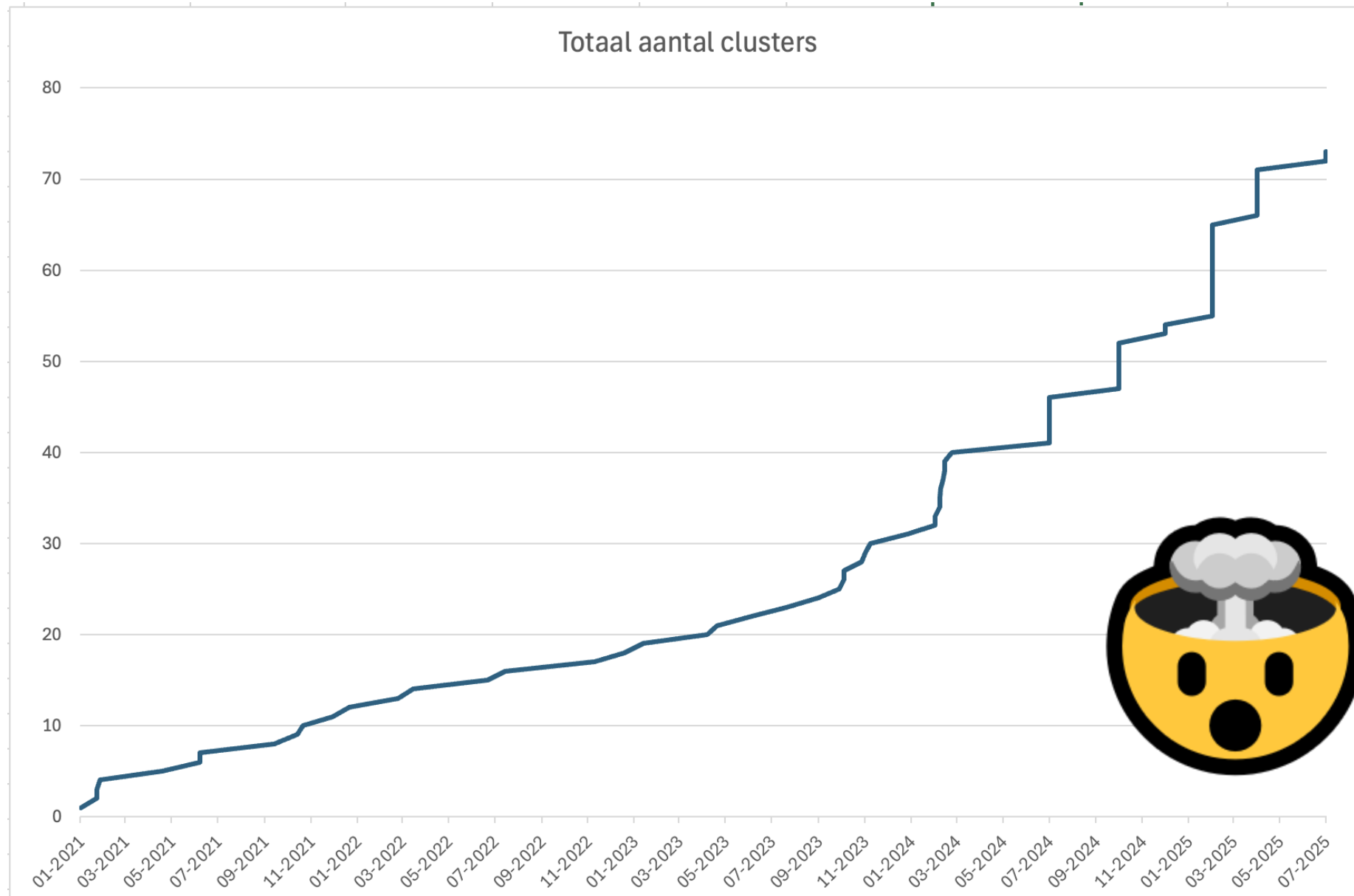
410 PROD worker nodes

Incl. overhead: 1583 nodes

1 Node (16 CPU, 64 Gb)

Totaal: 25.3k CPU & 101.3 TB

Cluster groei!



teams



OTA

223 PaaS objecten

5.3k namespaces

45k pods

82 DevOps teams/Oplogsgroepen

160+ Applicaties/Services

50+ DevOps teams in de queue

PROD

105 PaaS objecten

2.8k namespaces

21k pods

Thanks Team! 🐾



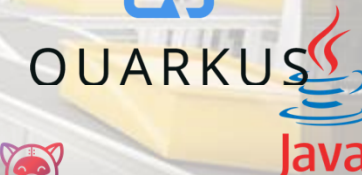
Dagelijks rollen we een cluster
(opnieuw) uit



Uitrollen nieuw cluster

PaaS

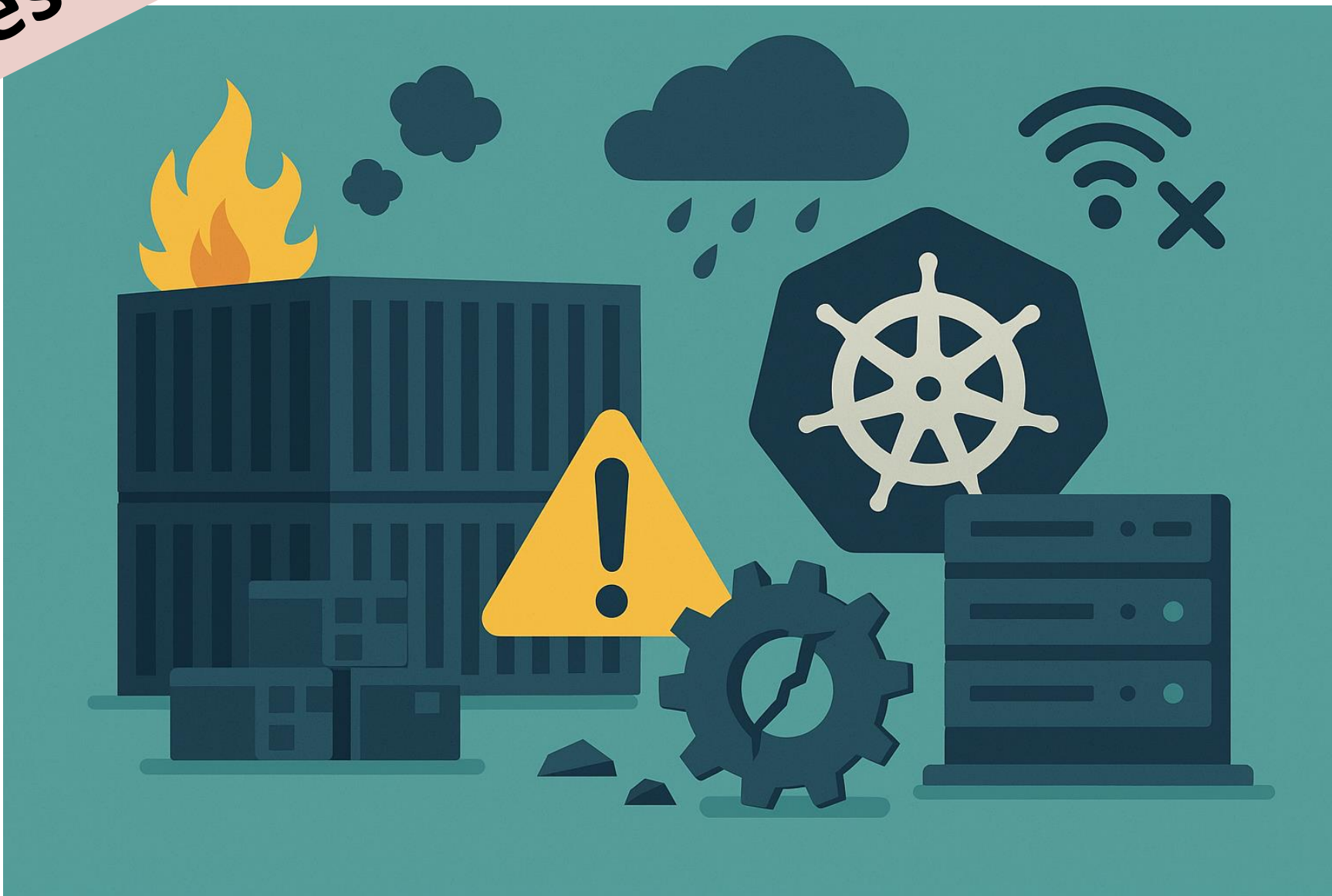
**Bootstrapping
capabilities / operators**



**Uitrollen pipelines die
voorbeeld/test
applicaties bouwen,
testen en voortbrengen**



Issues



Manifesto



Immutable Infrastructure

Environment Parity

Stateless Applications

Declarative Configuration

(Micro)services Architecture

Resiliency en high availability

Agility

Connectiviteit

Health Checks

**Platform
Awareness**

Logging and
Monitoring

NodePorts



Pod Disruption
Budget (PDB)

Resource
Management

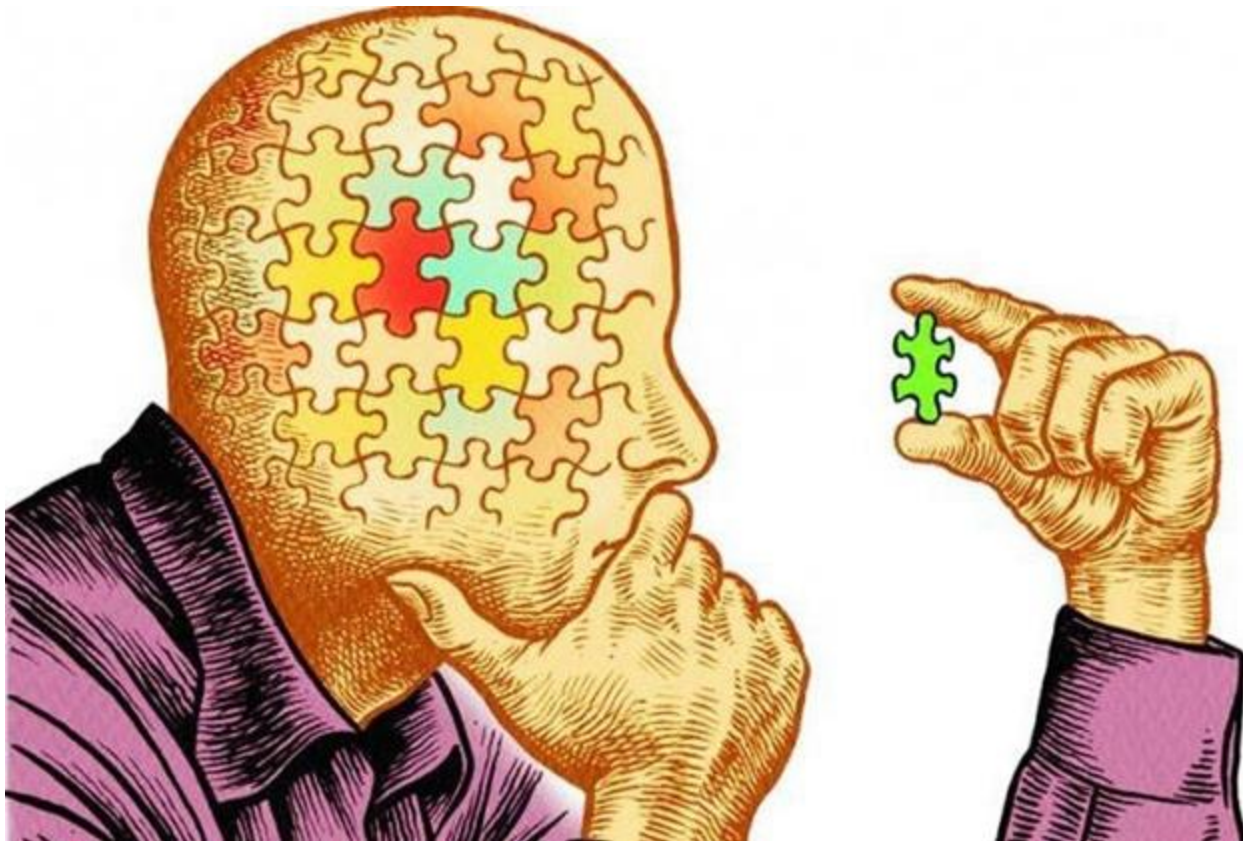
CI/CD

DevOps verantwoordelijkheid

Security Best
Practices

Service Discovery

Platform Awareness



**Normaal gedrag: POD herstart bij re-schedule
(bijvoorbeeld bij platform upgrade)**

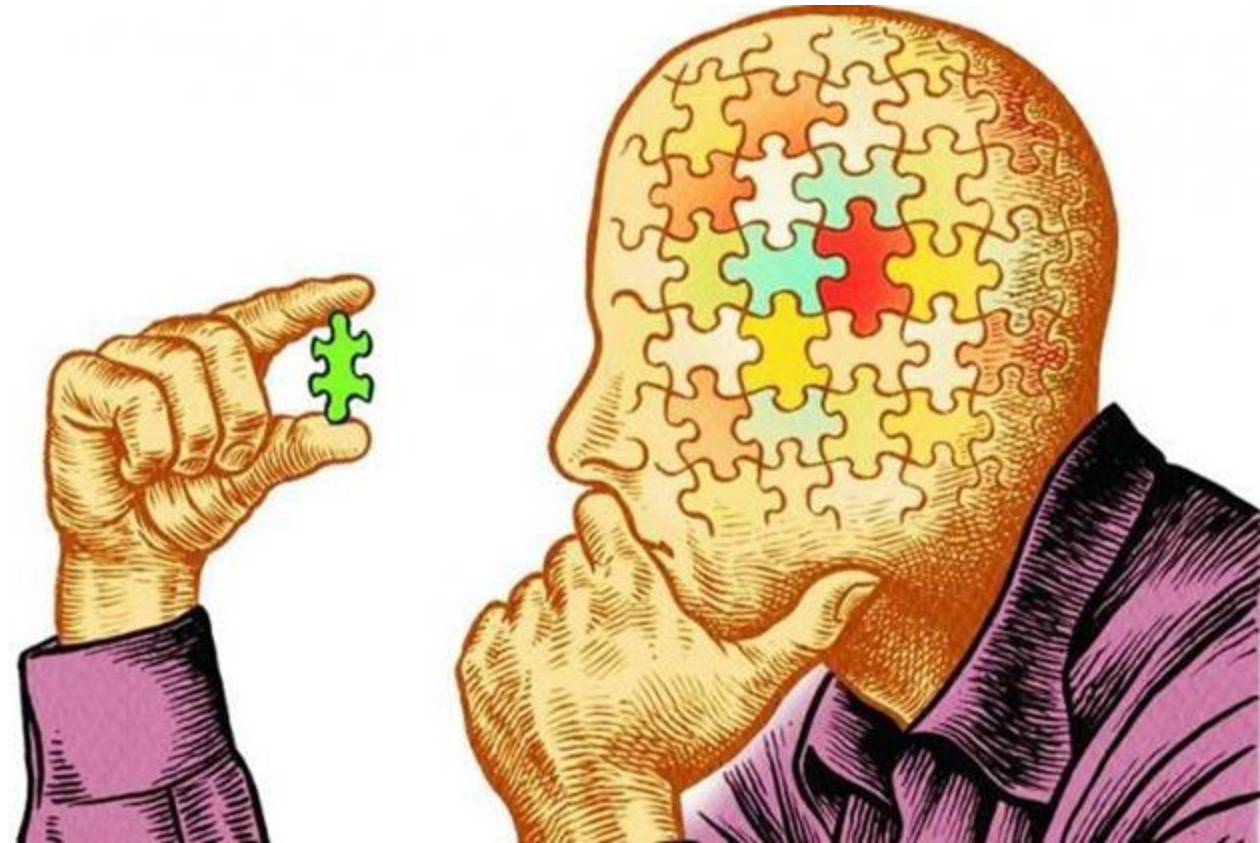
**OpenLiberty app met Message Driven Bean welke
je netjes wilt een JVM shutdown wilt geven:**

```
spec:
  containers:
    - image: openliberty-app-container:latest
      lifecycle:
        preStop:
          exec:
            command:
              - /liberty/bin/server
              - stop
```

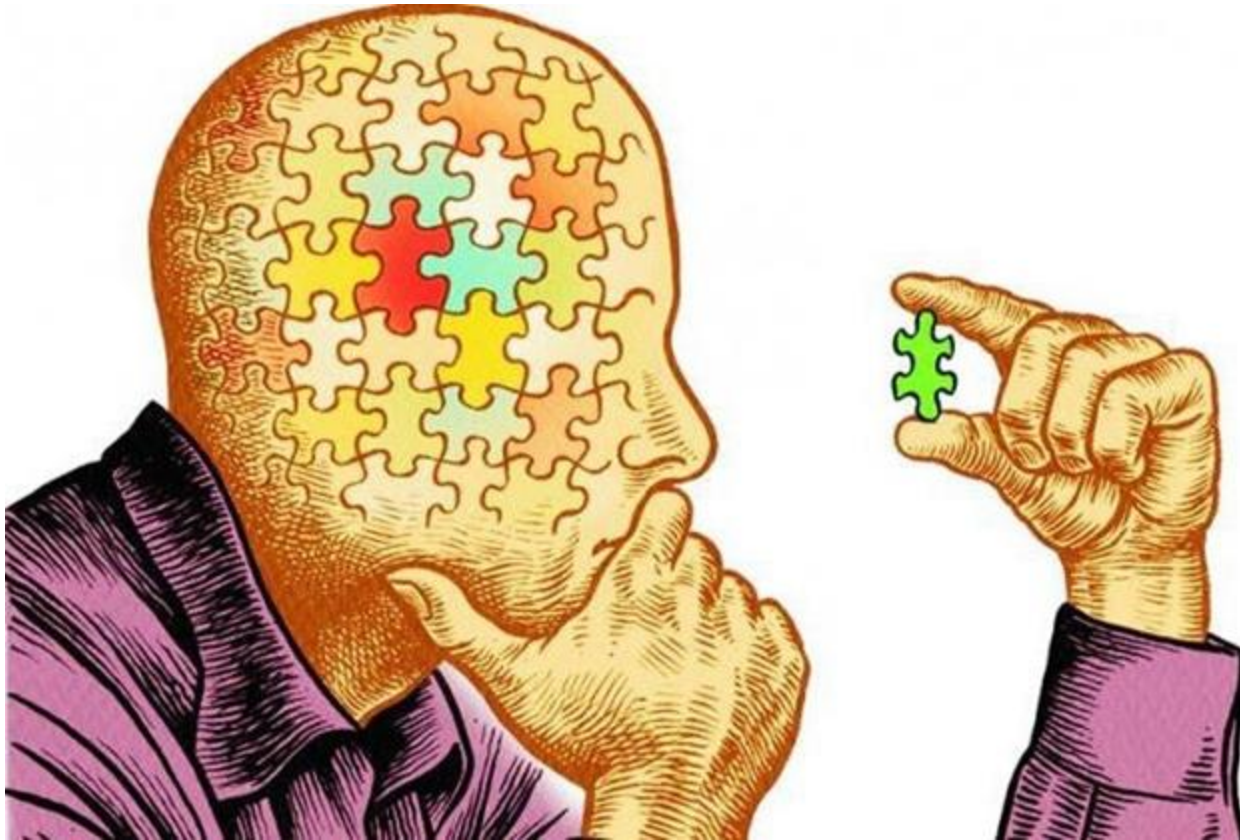


Een team maakt 32 workspaces aan zodat testers weken lang in aparte omgevingen kunnen testen.
Ze maken 32 kopieën met verschillende database state

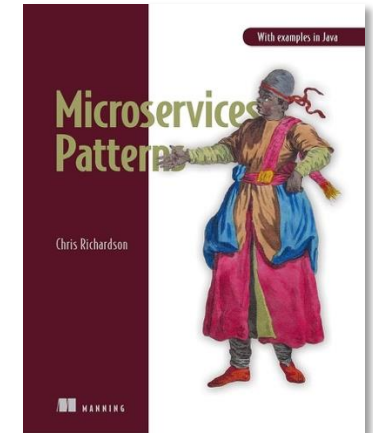
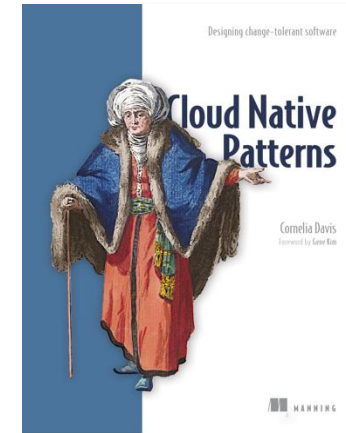
***Dit vraagt om (betere)
geautomatiseerde testen met
dynamische workspaces!!***



Platform Awareness



“Het platform zorgt toch voor transactionaliteit?! Dat was bij iPAS & WebSphere/JHOP toch ook zo!”



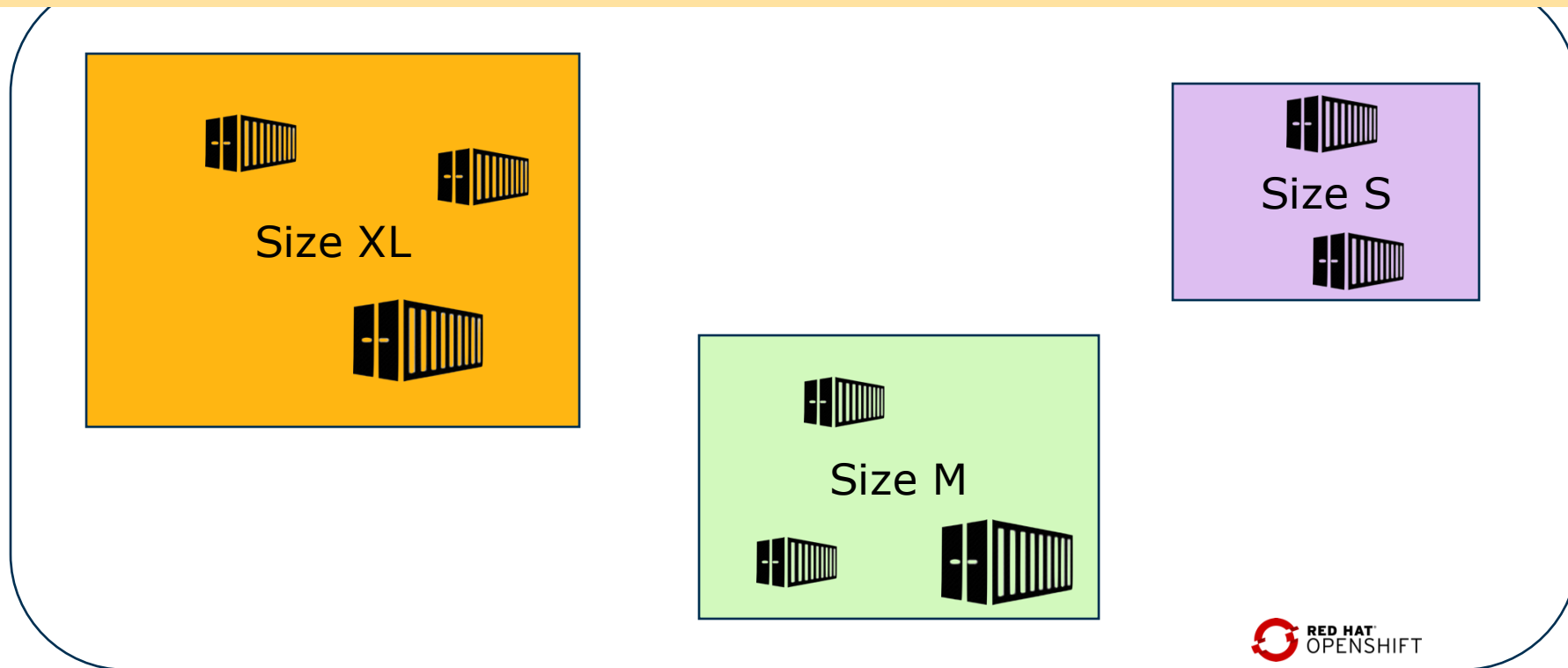
<https://microservices.io/patterns/microservices.html>

Right Sizing





CPU-limieten zijn opgeheven om performance bursts toe te staan.



Elk team kan middels PaaS Quota aanvragen (via Git PR => PaaS Operator)

Handdoekje leggen



We bieden t-shirt sizes, laat zien met je dashboard dat je eruit groeit

Re-Platforming Lift & Shift

Van iPAS & Websphere naar
OpenLiberty in containers in meer
dan alleen de Java code migreren:

CI/CD (Jenkins + DINQ) =>
Tekton + ArgoCD

Over de muur gooien => DevOps

DSC => Infrastructure as Code

Zelf monitoren / alerts

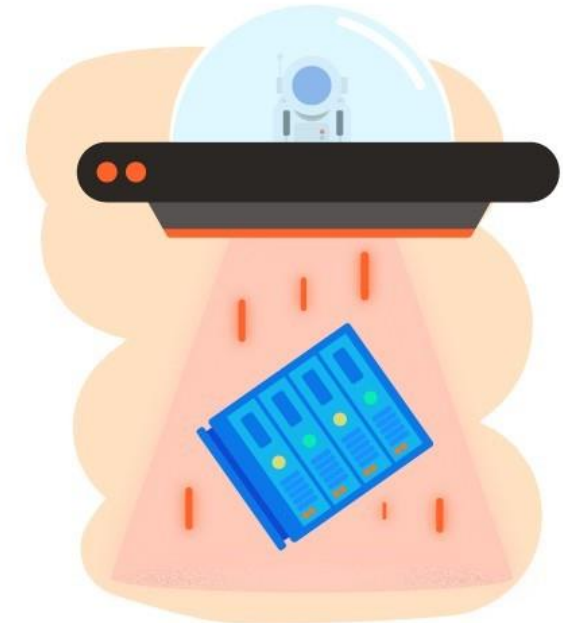
Je bent zelf van
jouw containers!

Andere architectuur
patronen

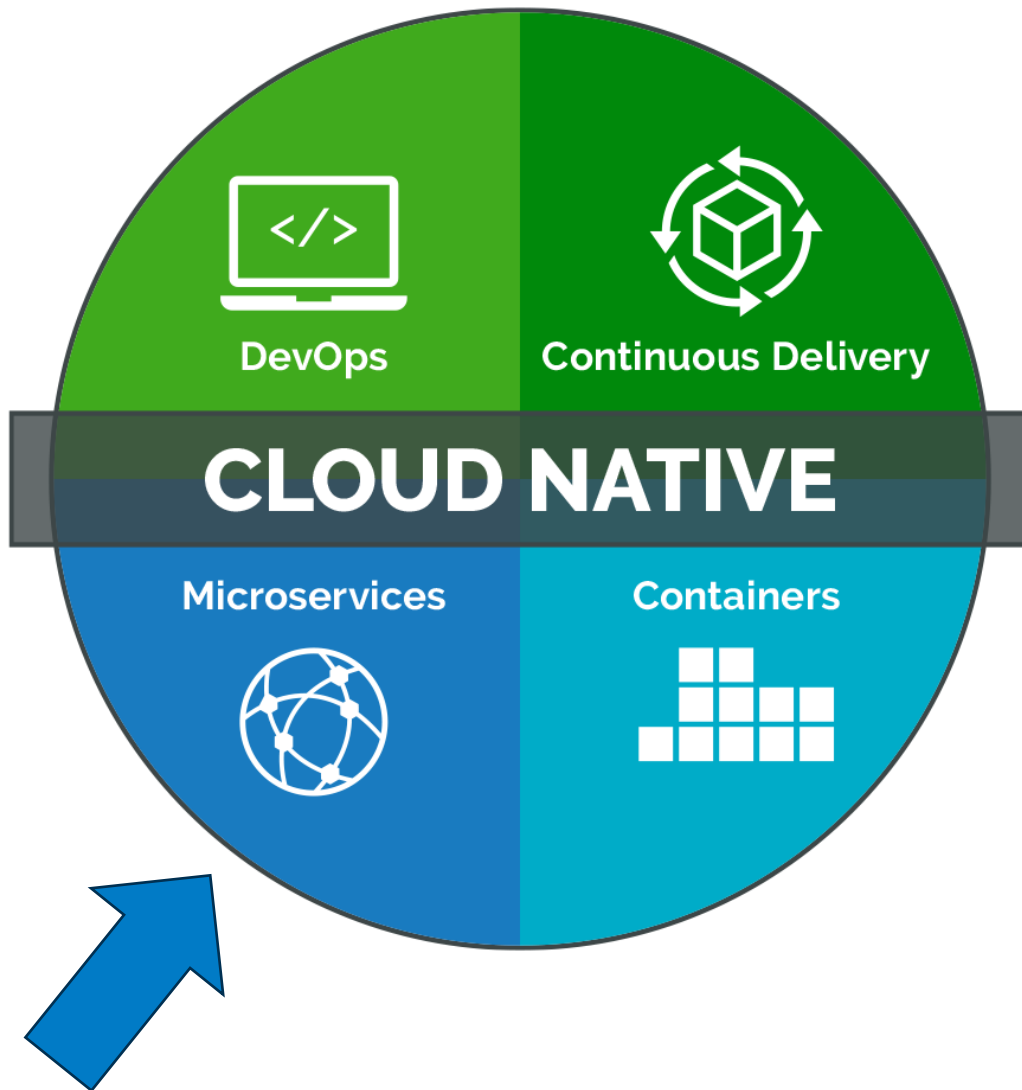
Lift & Shift



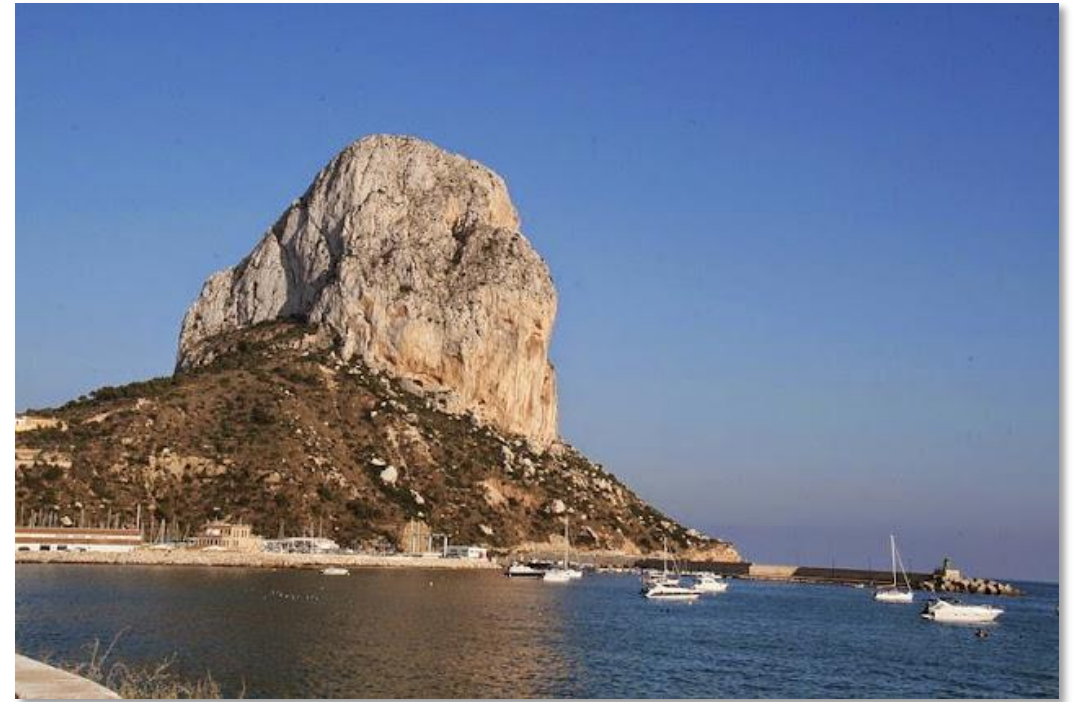
Cloud-Native



Cloud Native workload only?



Mag het dan geen monoliet zijn?



“Alleen (meer) services als het iets oplevert!!”



Roadmap

ROLLING ROADMAP CONTAINER PLATFORM ENGINEERING



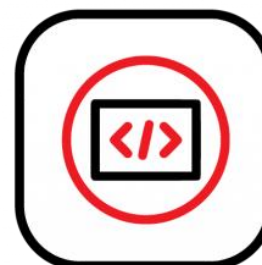
Roadmap focus



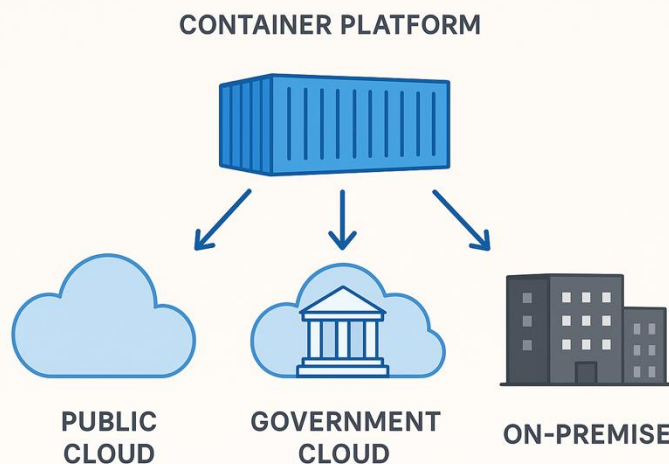
**Backstage as
Selfservice Portal**



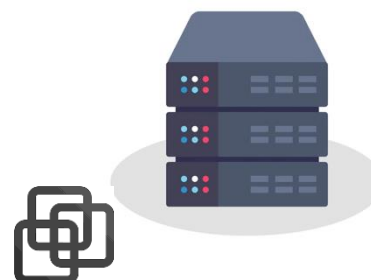
Golden Path up2date (Kargo / Kepn?)



**DevSpaces
Clusters**



Meer capaciteit / locaties



vmware => Bare Metal?



Secret Managent Oplossing

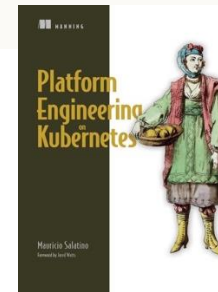
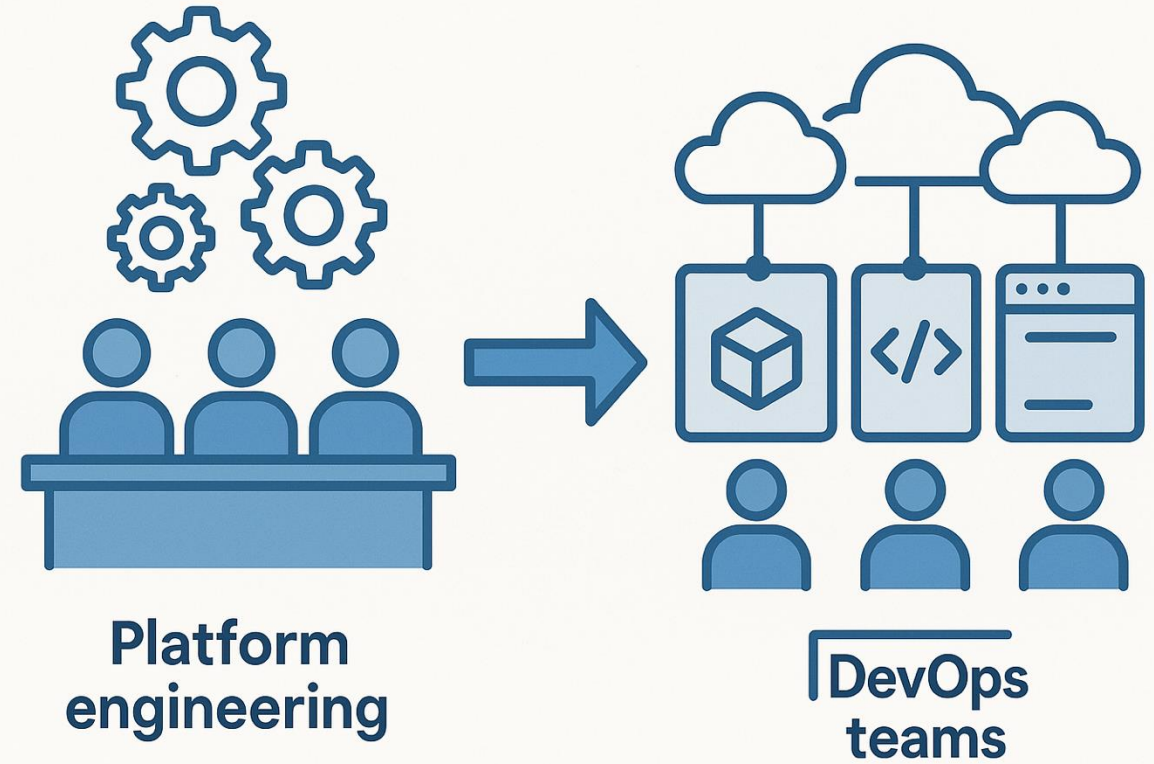
Wat hebben we geleerd?



Platform Engineering

- **DevOps** is een cultuur en samenwerking tussen development en operations.
- **Platform engineering** bouwt *het gereedschap* waar DevOps-teams mee werken.

Je kunt zeggen dat platform engineering de “enablement” laag is die DevOps mogelijk maakt op schaal.



Take aways



**We dachten
stateless te
blijven....duh!**

**State (storage) op
platform? Doe het
in 1x goed!**

**Golden Path altijd te
laat en updates niet
snel genoeg ;)**

**Het oude
denken is
HARDNEKKIG!**

**DevOps kent
VELE
interpretaties**

**Cognitieve load (te) hoog
voor (Java) developers en
Architecten**

**Pure Cloud Native
workloads only? You wish!**



Vragen?