





Peter Bult

Lead Consultant

p.bult@previder.nl

<https://www.linkedin.com/in/peterbult/>

it starts here.

Agenda

- ✧ Waarom Containers
- ✧ Historie
- ✧ Eigenschappen
- ✧ Kubernetes as a Service
- ✧ Haven/Commonground



it starts here.

Pets and Cattle

Pets

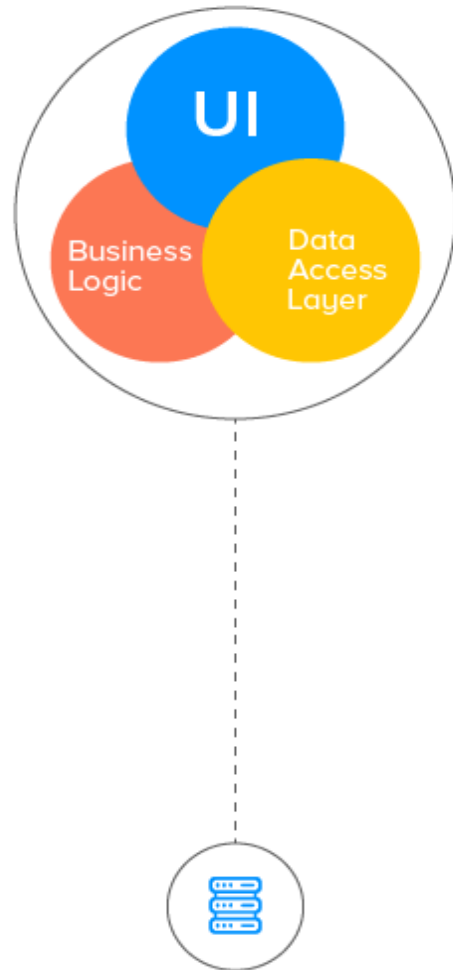
- Hebben namen als `mustang.previder.nl`
- Zijn uniek, worden vertroeteld en er wordt voor gezorgd
- Als er wat mee is, verzorg je ze of “repareer” je ze

Cattle

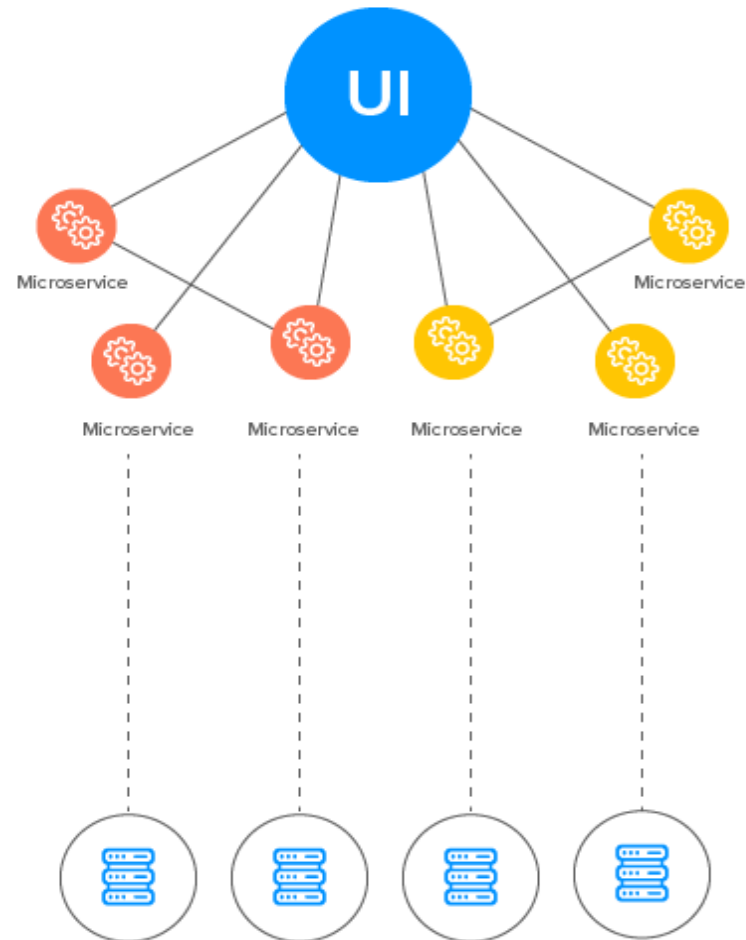
- Heeft nummers als `svr0123.previder.nl`
- Zijn nagenoeg gelijk aan ander cattle
- Als er wat mee is vervang je ze met een nieuwe



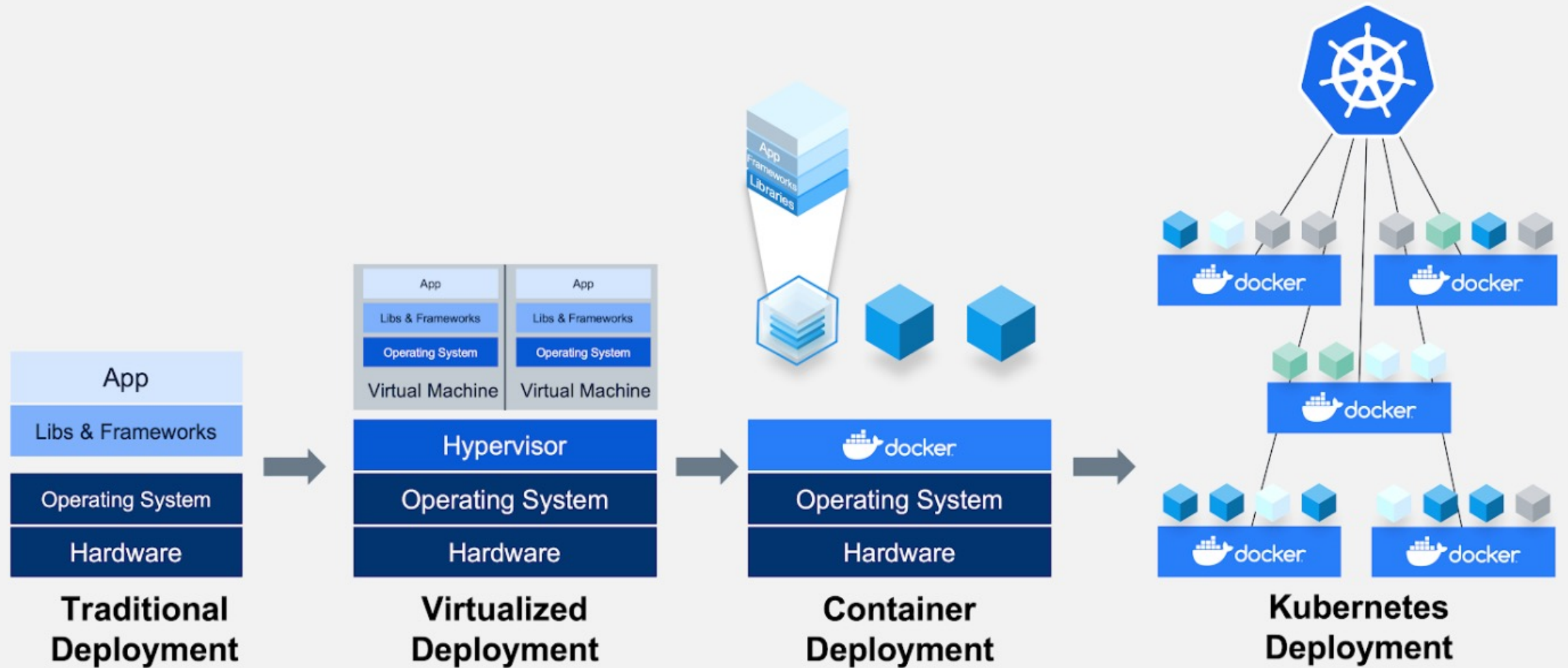
Monolithic Architecture



Microservice Architecture



Ontwikkeling virtualisatie web apps



previder

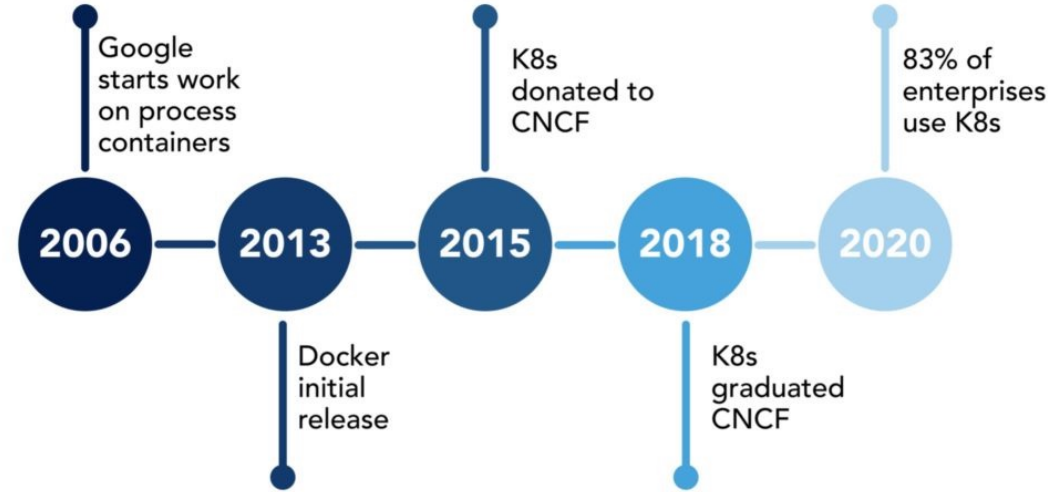
κυβερνήτης

Kubernetes

K8s



Coo-ber-net-ees



it starts here.

previder



Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications

We bring together the world's top developers, end users, and vendors and run the largest open source developer conferences. CNCF is part of the nonprofit Linux Foundation.

it starts here.

The screenshot displays the 'Application Definition & Image Build' section of the AWS IAM console. It features a grid of 48 application logos, each accompanied by a status label. The logos are arranged in 6 rows and 8 columns. The status labels include 'ONCE INSTALLED', 'ONCE CONFIGURED', 'ONCE DELETED', and 'ONCE INSTALLED'. The applications shown are: Helm, ArgoCD, Backstage, Buildpacks.io, dapr, KubeVela, CANVEL, KubeVirt, Karpenter, Pulumi, and many others. The page is titled 'Application Definition & Image Build' and includes a search bar and a filter icon.

[illegible][illegible]

The grid displays 24 logos for various security and compliance products, organized into two rows and eight columns. Each logo is accompanied by a status label: 'NOT GRADUATED', 'NOT INCUBATING', or 'INCUBATING'.

Logo	Status
Falco	NOT GRADUATED
Open Policy Agent	NOT GRADUATED
Open	NOT GRADUATED
Open	NOT GRADUATED
in-toto	NOT GRADUATED
KEYCLOAK	NOT GRADUATED
Kyverno	NOT GRADUATED
clair	NOT GRADUATED
Open Policy Agent	NOT GRADUATED
Open	NOT GRADUATED
Open	NOT GRADUATED
in-toto	NOT GRADUATED
KEYCLOAK	NOT GRADUATED
Kyverno	NOT GRADUATED
clair	NOT GRADUATED
Open Policy Agent	NOT GRADUATED
Open	NOT GRADUATED
Open	NOT GRADUATED
in-toto	NOT GRADUATED
KEYCLOAK	NOT GRADUATED
Kyverno	NOT GRADUATED
clair	NOT GRADUATED
Open Policy Agent	NOT GRADUATED
Open	NOT GRADUATED
Open	NOT GRADUATED
in-toto	NOT GRADUATED
KEYCLOAK	NOT GRADUATED
Kyverno	NOT GRADUATED

[illegible]

The screenshot shows the CNCF Landscape website. The top navigation bar includes filters for 'Projects and products', 'Members', 'Certified partners and providers', 'Serverless', 'Wasm', and 'CNAI'. The main section is titled 'Certified Kubernetes - Distribution' and displays a grid of logos for various Kubernetes distributions. The logos are arranged in a grid, with each logo representing a different distribution. The logos include AWS, Azure, Google Cloud, IBM, and many others. The grid is organized into rows and columns, with each logo being a square icon.

[illegible]

starts here.

Eigenschaften K8s



Container Orchestration

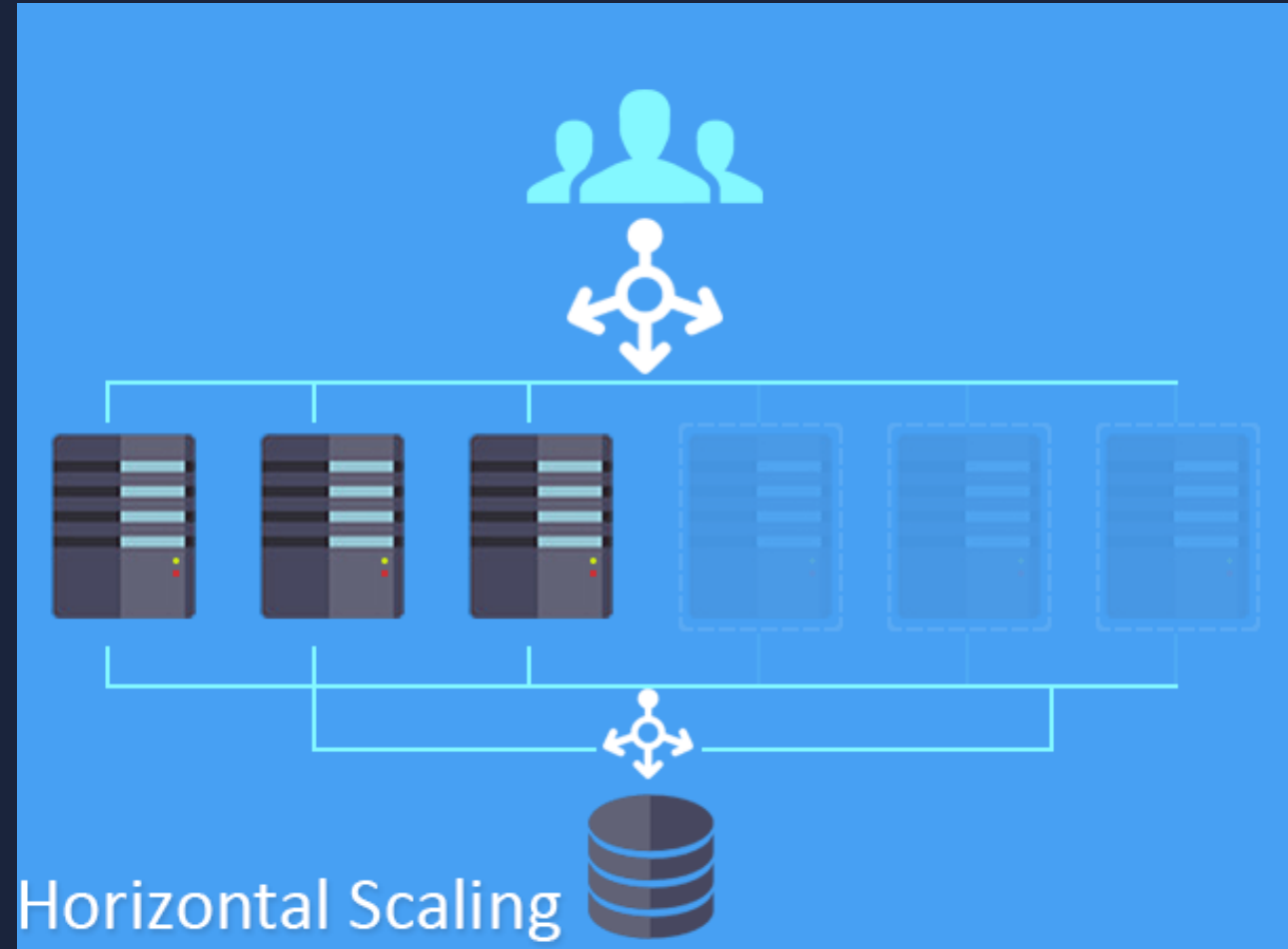
Kubernetes helpt bij het beheren van containers in een cluster

Het stelt ontwikkelaars in staat om containers te definiëren en te declareren die vervolgens geautomatiseerd kunnen worden beheerd



Schaalbaarheid

Kubernetes is ontworpen om hoog schaalbaar te zijn, zodat u gemakkelijk toepassingen kunt implementeren en beheren over een cluster van hosts. Je kunt opschalen of terugschalen zoals nodig is.



Automatisering

Kubernetes biedt volledige automatisering van het implementatieproces van applicaties
Ontwikkelaars kunnen eenvoudig applicaties declareren en Kubernetes doet de rest



Service Discovery en Load Balancing

Kubernetes biedt krachtige service discovery en load balancing-functies waarmee verkeer eenvoudig naar de juiste container of service kan worden geleid. Dit maakt het mogelijk dat applicaties naadloos kunnen worden uitgevoerd over meerdere nodes en datacenters.



Self-healing

Kubernetes heeft de mogelijkheid tot zelfherstel, wat betekent dat als een container of node faalt, Kubernetes automatisch de container kan herstarten of verplaatsen naar een andere node, zodat de applicatie beschikbaar en responsief blijft. Deze functie helpt om downtime te verminderen en zorgt ervoor dat de applicatie blijft functioneren zoals bedoeld.

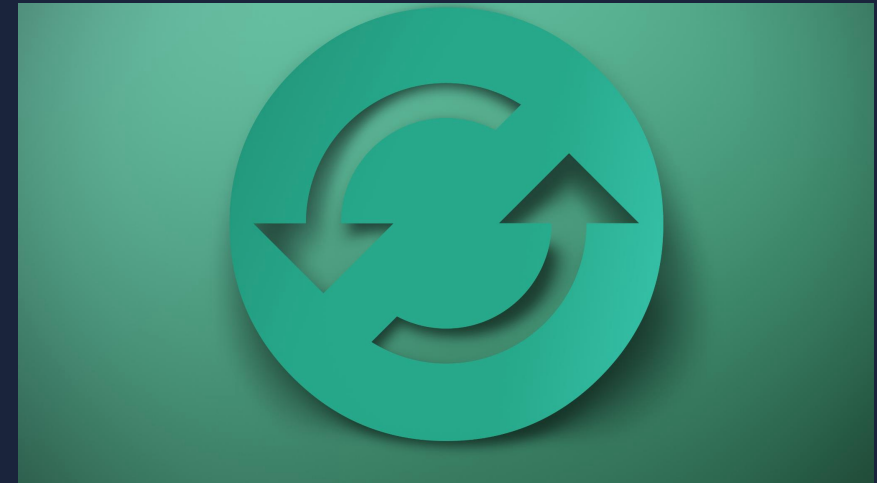


Rolling Updates en Rollbacks

Kubernetes biedt ingebouwde functies voor Rolling Updates en Rollbacks

Ontwikkelaars kunnen eenvoudig nieuwe versies van hun applicaties implementeren zonder downtime

Kubernetes biedt de mogelijkheid om snel terug te gaan naar een vorige versie van een applicatie als dat nodig is



Declaratieve Configuratie

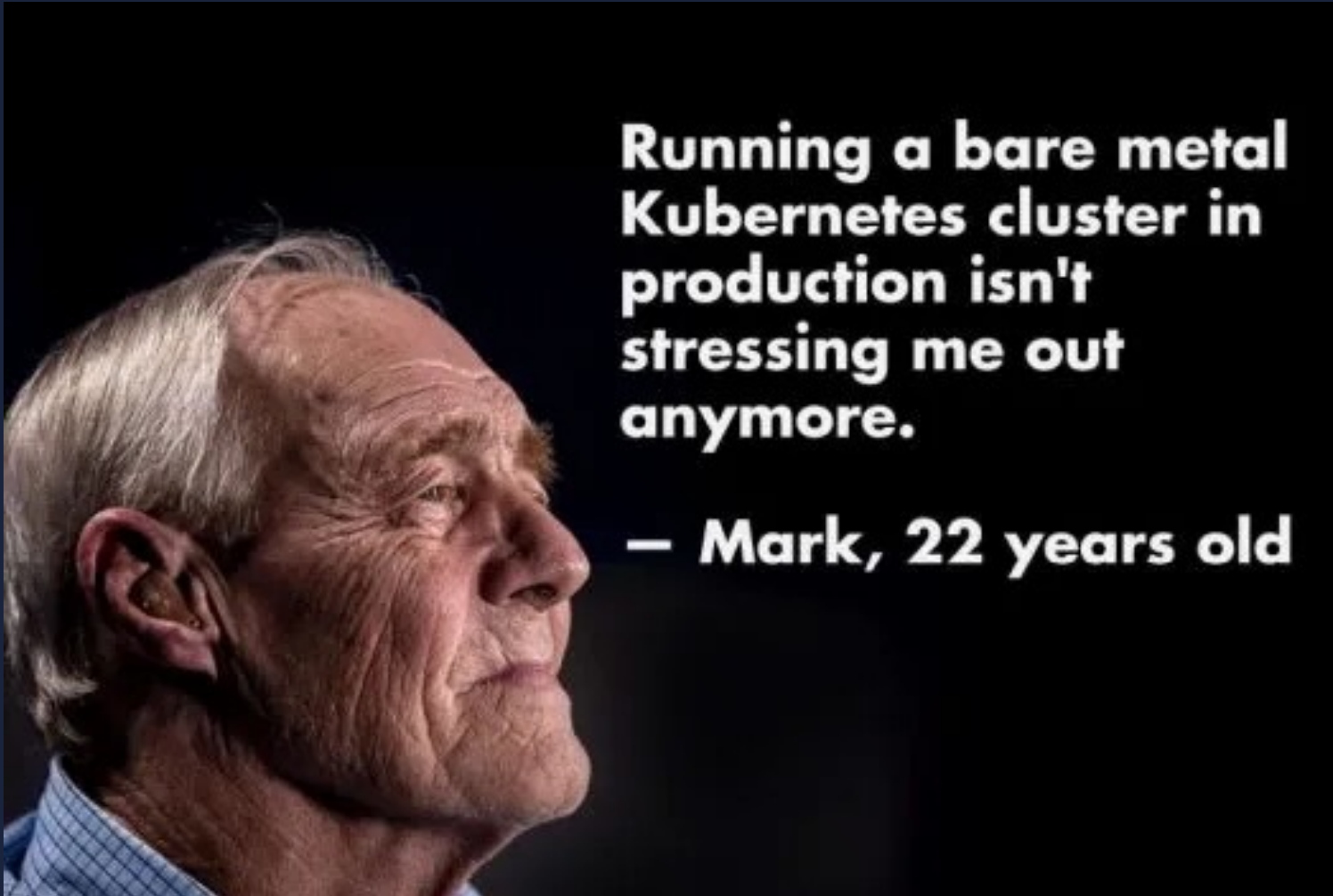
Ontwikkelaars kunnen eenvoudig de gewenste staat van hun infrastructuur definiëren

Kubernetes zorgt voor het beheer van de infrastructuur en past deze automatisch aan aan de gewenste staat



```
# deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.14.2
          ports:
            - containerPort: 80
```

Is K8s complex?



Wat ervaren bedrijven als de grootste uitdaging bij het opzetten en onderhouden van Kubernetes Clusters. Geef puntsgewijs de drie grootste uitdagingen.



Bij het opzetten en onderhouden van Kubernetes-clusters ervaren bedrijven de volgende drie grootste uitdagingen:

1. **Complexiteit en Leercurve:** Kubernetes vereist diepgaande kennis van containerisatie, configuratiebeheer, en netwerkbeheer, wat voor veel bedrijven een steile leercurve betekent.
2. **Beveiliging en Compliance:** Het correct implementeren van beveiligingsmaatregelen zoals RBAC en netwerkpolities, en het voldoen aan compliance-eisen, is vaak ingewikkeld en tijdrovend.
3. **Schaalbaarheid en Betrouwbaarheid:** Het beheren van schaalbare Kubernetes-clusters, inclusief automatisering en monitoring, vereist geavanceerde tools en strategieën, wat bedrijven voor grote uitdagingen stelt.

Previder KaaS

previder portal

Maak een Kubernetes cluster

1. Kies type

Express

- Web- en applicatiehosting
- Selectie voor 1 datacenter
- Limiet tot 5000 IOPS

PDCT & PDC2

Performance

- Database hosting
- Selectie voor 1 datacenter
- Limiet tot 20000 IOPS

Maak een keuze

Premium

- Bedrijfskritische hosting
- 2 Datacenters
- Limiet tot 20000 IOPS
- Realtime replicatie

Maak een keuze

2. Configureer je control planes

Hoge beschikbaarheid

☐ Uitgeschakeld

☒ Deze optie maakt 3 control planes aan.

Geavanceerde instellingen

☐ Uitgeschakeld

3. Configureer je worker nodes

Kies een standaard grootte of stel deze zelf in

Geavanceerde instellingen

☐ Uitgeschakeld

Small

- CPU cores: 2
- RAM: 4GB
- Opslag: 25GB

Medium

- CPU cores: 4
- RAM: 8GB
- Opslag: 50GB

Minimum aantal worker nodes

Minimum: 1, Maximum: 10, Stel in: 3

Maximum aantal worker nodes dat via autoscaling kan worden aangemaakt.

Minimum: 1, Maximum: 10, Stel in: 6

4. Globale instellingen

Cluster naam

Cluster naam

Autoscaling

☒ Aan

Previder zal ervoor zorgen dat de cluster periodiek zal worden geupdate naar de meest recente Kubernetes versie.

Verwijderingsbescherming

☐ Voorkom dat het cluster per ongeluk wordt verwijderd

5. Eenmalige instellingen

Installeer een CNI in het cluster

Wanneer je een CNI kiest zal deze automatisch worden geïnstalleerd in je cluster. Selecteer Geen als je een eigen CNI wilt installeren.

Cilium

Netwerk

Dit netwerk zal worden gekoppeld aan alle nodes. Netwerken zijn te vinden onder IaaS.

☒ Ik heb een netwerk aangemaakt waarin DHCP (of een IP pool) is geconfigureerd en waarin DNS beschikbaar is.

Kubenetwork

VIP

Je cluster zal beschikbaar zijn op dit VIP in het gekozen netwerk.

Voorbeeld: 192.168.1.10

Item toevoegen

192.168.2.10

Endpoints

Deze hostnames zullen worden toegevoegd aan het cluster certificaat en kan worden gebruikt om verbinding te maken met het cluster.

Voorbeeld: cluster01.customer.dev

Item toevoegen

kubecuster.previder.nl

Eigenschappen KaaS

- ✧ Automatische uitrol
- ✧ Autoscaling Workernodes (optie)
- ✧ Automatische updates (optie)
- ✧ Eigen keuze in CNI
- ✧ Hybrid mogelijk met IaaS of fysieke omgeving
- ✧ Redundantie over meerdere Datacenters 🇳🇱🇪🇺
- ✧ Gebouwd op bewezen stabiele infrastructuur



Digitale autonomie



Bijeenkomst Cloud en Digitale Open Strategische Autonomie

Mar 29 2024

Op 27 maart was er een mooi gesprek over de Nederlandse en Europese afhankelijkheid van "de cloud". Het gesprek vond plaats op het ministerie van Economische Zaken en Klimaat, en deelnemers waren onder andere minister Micky Adriaansens en staatssecretaris van digitalisering Alexandra van Huffelen. Het onderwerp wordt dus (terecht) serieus genomen.

Dit artikel is onderdeel van een groter reeks Engelstalige reeks over Europese innovatie en digitale afhankelijkheden.

De bijeenkomst werd gehouden onder Chatham House Rule, wat inhoudt dat we niet ga verklappen wie precies wat heeft gezegd. Op deze pagina vat ik dingen samen die mij zi opgevallen, waarbij ik benadruk dat dit dus geen set conclusies uit de bijeenkomst is. Er besproken dan ik hier beschrijf, en ik voeg onderstaand ook dingen toe die in de bijeen (ruim) genoemd zijn. Zie dit meer als mijn reflectie op het gesprek.

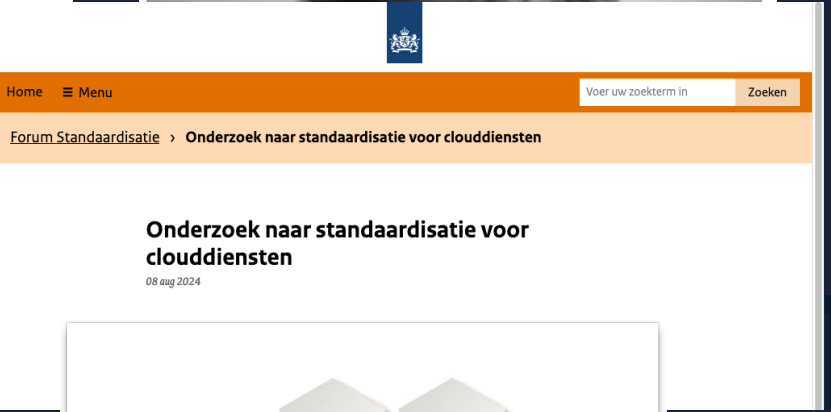
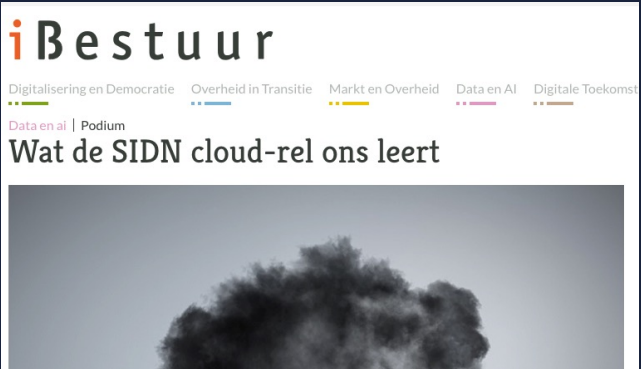
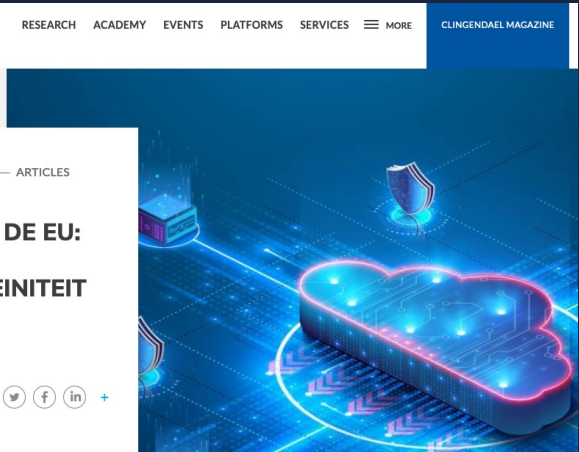
Ook BNR besteedde tijdens de bijeenkomst aandacht aan dit onderwerp (op minuut 37).



RESEARCH — CYBER SECURITY — ARTICLES

NEDERLAND EN DE EU: ZET IN OP CLOUDSOEVEREINITEIT

16 APR 2024 - 10:39



Open brief CIO-verenigingen aan EC voor een 'digitale interne markt' voor clouddiensten en oplossingen met een hoog niveau van zekerheid

previder

it starts here.

Digitale auton



- ✈ Haven als sta
 - ✈ CompliancyChecks op basis van script
 - ✈ Security/authorisatie/redundantie
 - ✈ Referentieimplementaties
 - ✈ Previder eerste NL partij met referentie implementatie
- previder

Result

[I] Results: 16 out of 16 checks passed, 0 checks skipped, 0 checks unknown. This is a Haven Compliant cluster.

[I] Compliancy checks results:

CATEGORY	NAME	PASSED
Fundamental	Self test: HCC version is latest major or within 3 months upgrade window	YES
Fundamental	Self test: does HCC have cluster-admin	YES
Infrastructure	Multiple availability zones in use	YES
Infrastructure	Running at least 3 master nodes	YES
Infrastructure	Running at least 3 worker nodes	YES
Infrastructure	Nodes have SELinux, Grsecurity, AppArmor, LKRG, Talos or Flatcar enabled	YES
Infrastructure	Private networking topology	YES
Cluster	Kubernetes version is latest stable or max 3 minor versions behind	YES
Cluster	Role Based Access Control is enabled	YES
Cluster	Basic auth is disabled	YES
Cluster	ReadWriteMany persistent volumes support	YES
External	CNCF Kubernetes Conformance	YES
Deployment	Automated HTTPS certificate provisioning	YES
Deployment	Log aggregation is running	YES
Deployment	Metrics-server is running	YES
Validation	SHA has been validated	YES

Haven compliant oplossingen

Alles Cloud On-premise

**Amazon Elastic Kubernetes Service (EKS)** - Cloud
Amazon Elastic Kubernetes Service (Amazon EKS) is a managed container service to run and scale Kubernetes applications in the cloud or on-premises.
[Referentie Implementatie](#) [Contactgegevens](#)

**Edgeless Systems Constellation** - Cloud
Constellation is the secure, always-encrypted Kubernetes that shields all clusters from the infrastructure and makes sure that cloud admins and hackers cannot access your data.
[Referentie Implementatie](#) [Contactgegevens](#)

**Google Kubernetes Engine (GKE)** - Cloud
Google Kubernetes Engine (GKE) is a managed, production-ready environment for running containerized applications.
[Referentie Implementatie](#) [Contactgegevens](#)

**Kops op OpenStack** - Cloud
Kops will not only help you create, destroy, upgrade and maintain production-grade, highly available, Kubernetes cluster, but it will also provision the necessary cloud infrastructure.
[Referentie Implementatie](#) [Contactgegevens](#)

**Microsoft Azure Kubernetes Service (AKS)** - Cloud
Deploy and manage containerized applications more easily with a fully managed Kubernetes service.
[Referentie Implementatie](#) [Contactgegevens](#)

**Previder** - Cloud
Previder Kubernetes Engine wordt uitsluitend in eigen Nederlandse datacenters gehost en beheerd, waarbij redundantie over meerdere datacenterlocaties hoge beschikbaarheid garandeert.
[Referentie Implementatie](#) [Contactgegevens](#)

**Red Hat OpenShift** - Cloud + On-premise
Red Hat® OpenShift® is an enterprise-ready Kubernetes container platform built for an open hybrid cloud strategy.
[Referentie Implementatie](#) [Contactgegevens](#)

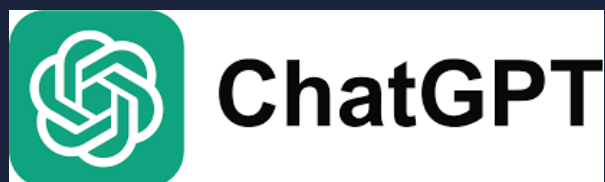
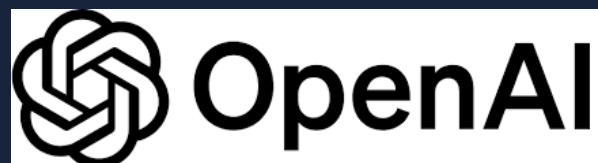
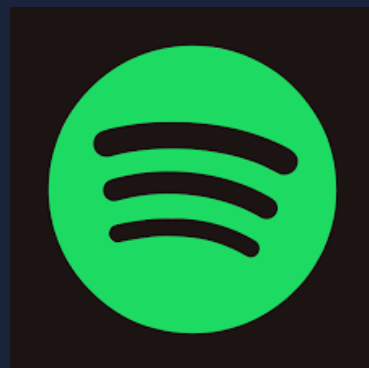
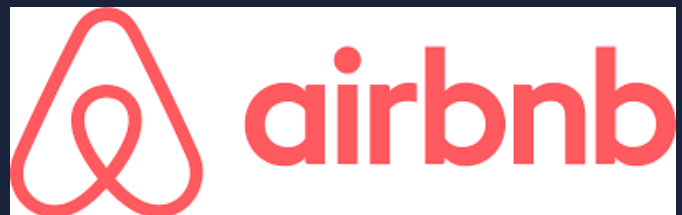
**SUSE Rancher Kubernetes Engine (RKE)** - Cloud + On-premise
RKE is a CNCF-certified Kubernetes distribution that solves common installation complexities of Kubernetes by removing most host dependencies, presenting a stable path for deployment, upgrades & rollbacks.
[Contactgegevens](#)

**VMware Tanzu Kubernetes Grid** - Cloud + On-premise
Reliably deploy and run containerized workloads across private and public clouds.

it starts here.

Use cases

- ✈ ISV'ers. Partijen die vanuit Previder datacenters hun software als SaaS dienst aan hun klanten aanbieden.
- ✈ Organisaties met eigen softwareontwikkeling (intern of extern)
- ✈ Keywords: DevOps, CI/CD, Containers



Vragen?

