IT-IMPRESSIVE

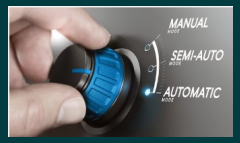
SIMPLIFYNOW

DevOps Automation

The New Way of Working

Speaker:
Dinant Paardenkooper – Architect/Consultant

Topics:
- Containerized app
- Kubernetes
- Container Security
- Container straat CI/CD
- Infra as Code



Introductie

Dinant Paardenkooper

Rol: Handson Cloud Native Solution Architect (Azure, VMWare)
Cloud Native | Kubernetes | Automation | IaC | Spreker

Drive: Innoveren, Business requirements omzetten naar praktische technische oplossingen

Hobby's: Gitaar spelen, innoveren, hardlopen, squash
E-mail: d.paardenkooper@IT-Impressive.nl
LinkedIn: www.linkedin.com/in/dinantpaardenkooper

Agenda

IT Trends	-	Modern Development en bijbehorende producten uit de Markt
Container App	-	Wat is een container en hoe gaat de creatie van een containerized applicatie
Kubernetes	-	Wat is het en waarom is het zo populair
Security	-	Wat zijn de risico's en hoe containerized applicaties te beschermen
CI/CD	-	Hoe wordt de uitrol van applicaties geautomatiseerd
Infra as code	-	Hoe wordt de provisioning van de Kubernetes laag gerealiseerd


IT Trends

IT Trends

Volgens Gartner…

Data Fabric
Cybersecurity Mesh
Privacy-Enhancing Computation
Cloud-Native Platforms

Composable Applications
Decision Intelligence
Hyperautomation
AI Engineering

Distributed Enterprise
Total Experience
Autonomic Systems
Generative AI

IT Trends

Volgens Gartner…

Composable Applications

Decision Intelligence

CI/CD

Hyperautomation

AI Engineering

Infra As Code

Data Fabric

Cybersecurity Mesh

Privacy-Enhancing Computation

Cloud-Native Platforms

Kubernetes en security

Distributed Enterprise

Total Experience

Autonomic Systems

Generative AI

Producten uit de markt

Kubernetes

RED HAT OPENSHIFT Container Platform

RANCHER

VMware Tanzu

Security

Twistlock

aqua

sysdig

RedLock

CI/CD

GitLab

Azure DevOps

GitHub Actions

vRealize Automation 8.0

Infrastructure as Code

Scripting

+

HashiCorp Terraform

PowerShell

Producten uit de markt

Kubernetes

Security

CI/CD

Infrastructure as Code

Containers


L M S
CONTAINER
ERVICE
AHK 315
L N S
Image courtesy : shippingcontainers.co.nz

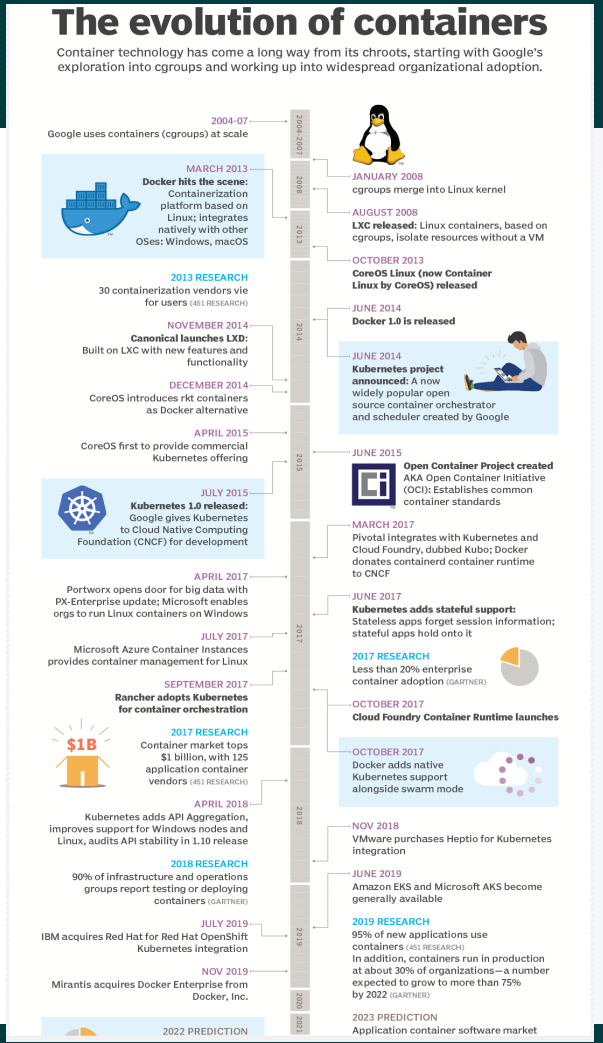
Historie

Intro containers (docker)

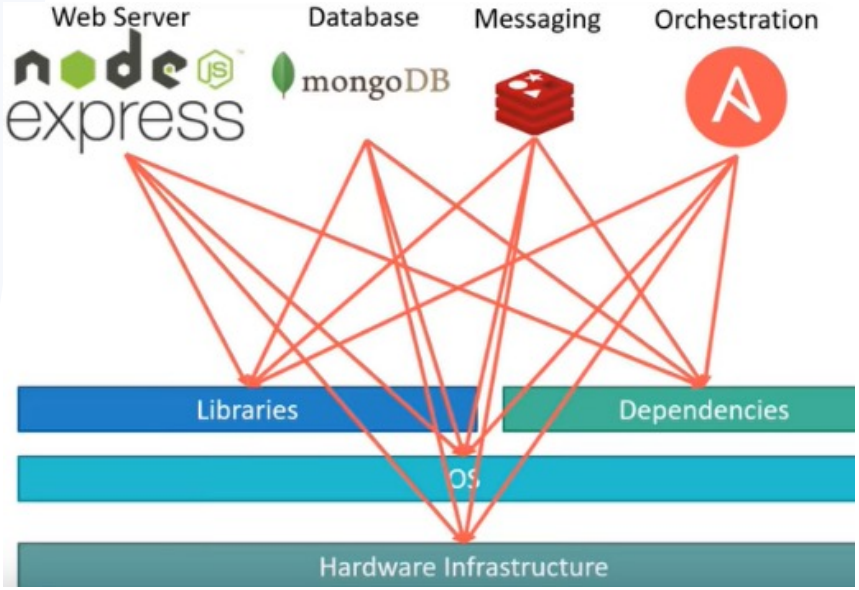
Wat is een container en wat zijn de voordelen

Waarom zo interessant

Historie – 1970

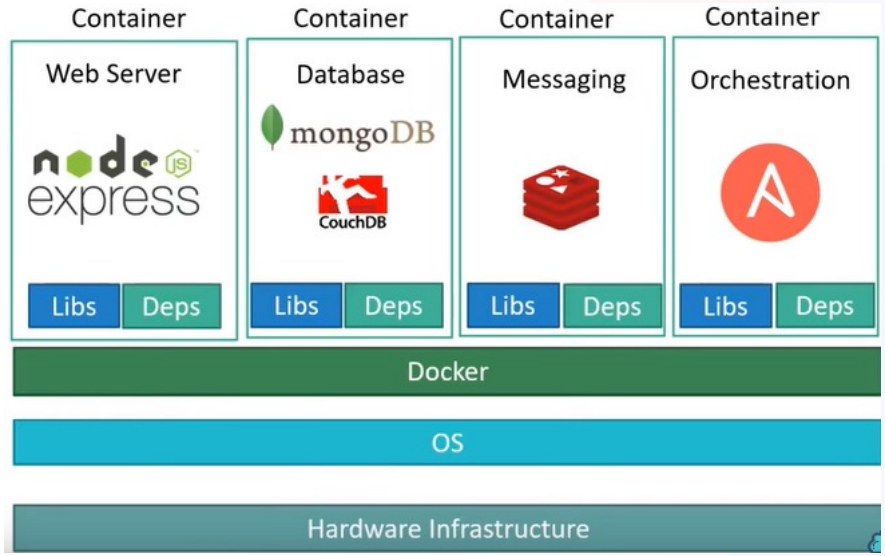


Kracht van containers



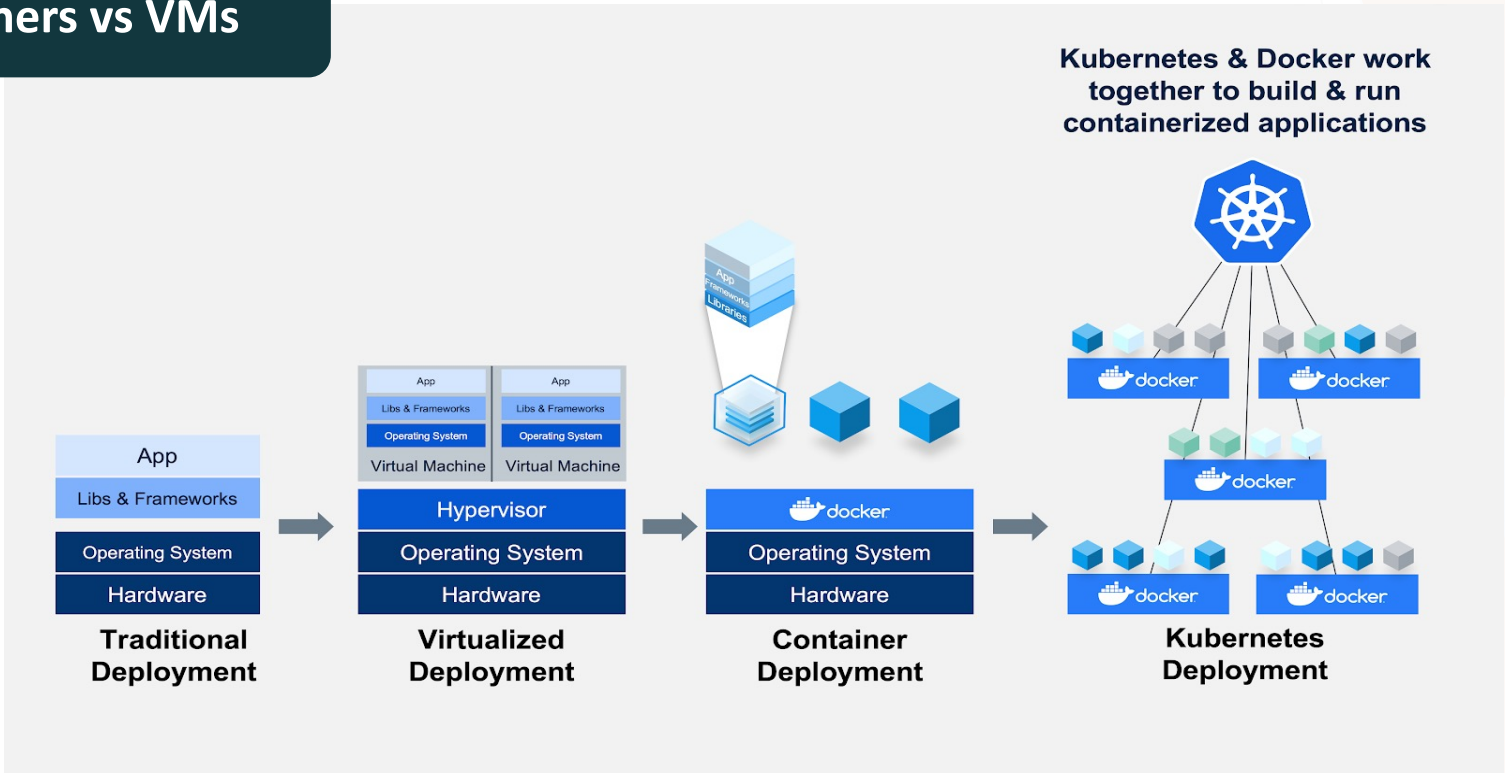
Traditioneel

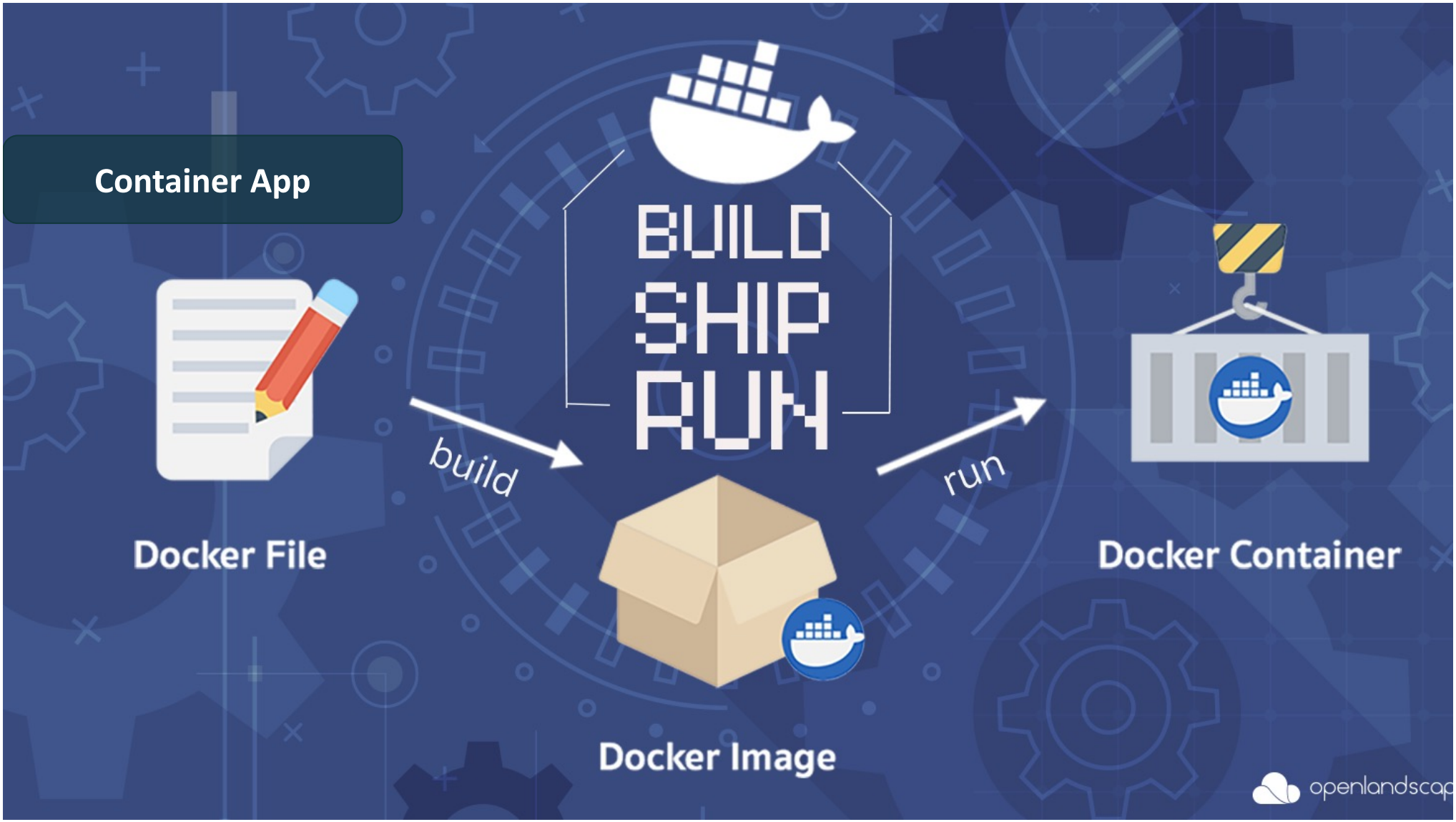
VS



Containerized

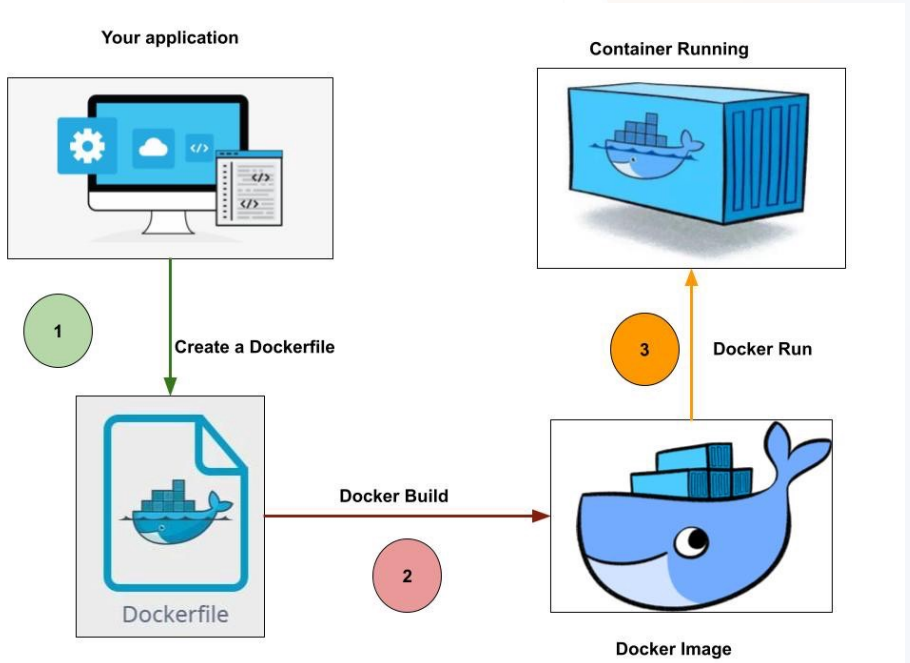
Containers vs VMs




Container App
BUILD
SHIP
RUN
build
run
Docker File
Docker Image
Docker Container
openlandscap

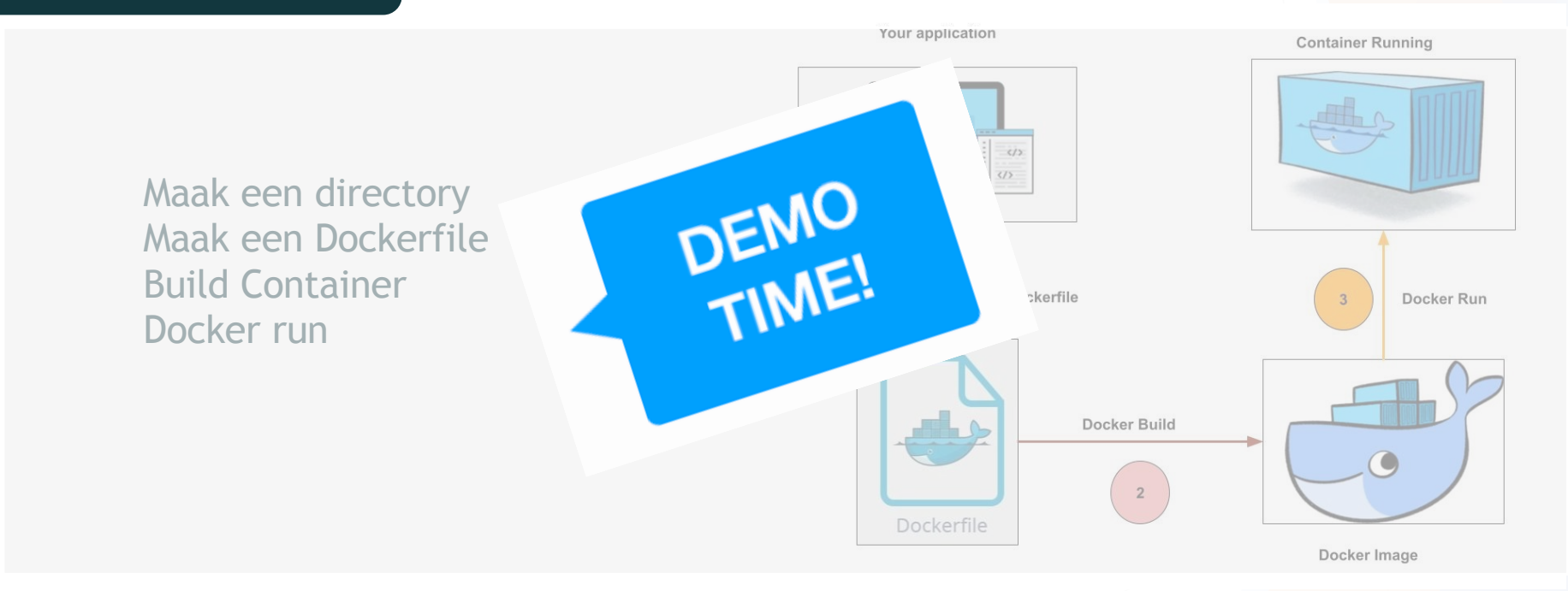
Simpele Web app

Maak een directory
Maak een Dockerfile
Build Container
Docker run



Simpele Web app

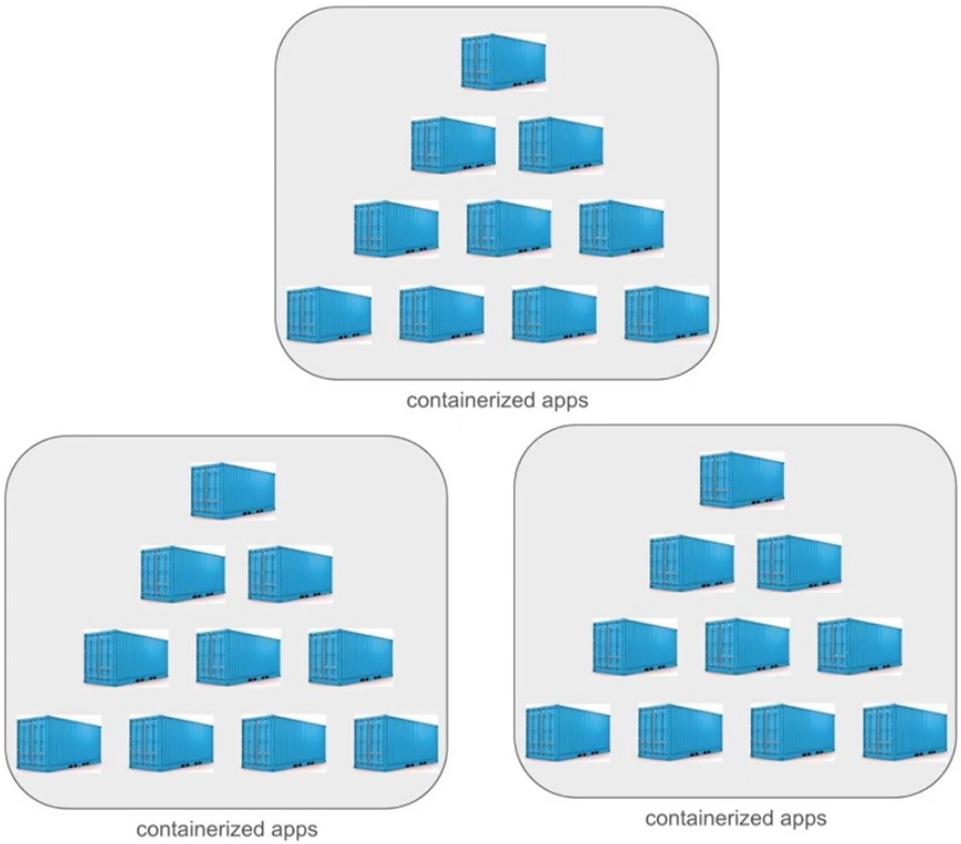
Maak een directory
Maak een Dockerfile
Build Container
Docker run



Container uitdagingen

Hoe op te lossen?

- Schalen
- Beheren
- Loadbalancing
- Storage
- Security
- RBAC




Kubernetes

Use cases

Landingsplaats voor gecontaineriseerde apps

Op en afschalen applicaties

Gestandaardiseerde uitwisselbare applicaties

Applicatie isolatie en identieke OTAP straat

Tool selectie

VS

RANCHER

Pro's
- Azure Integrated
- Built in Storage, IAM
- Doorontwikkeling hoog

Cons
- Azure Only
- Geen Multicloud
- Niet opensource

Pro's
- Opensource
- Multicloud /OnPrem
- Multi integraties

Cons
- Configure IAM, Storage
- Doorontwikkeling laag

Tool selectie

Pro's

- Azure Integrated
- Built in Storage, IAM
- Doorontwikkeling hoog

Cons

- Azure Only
- Geen Multicloud
- Niet opensource

VS

RANCHER

Pro's

- Opensource
- Multicloud /OnPrem
- Multi integraties

Cons

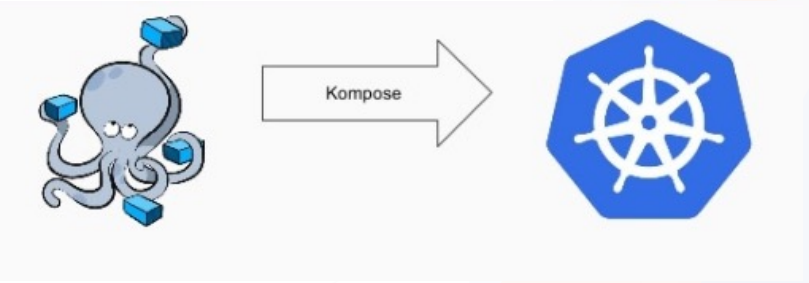
- Configure IAM, Storage
- Doorontwikkeling laag

Docker file vs Manifest files

Uitdaging:

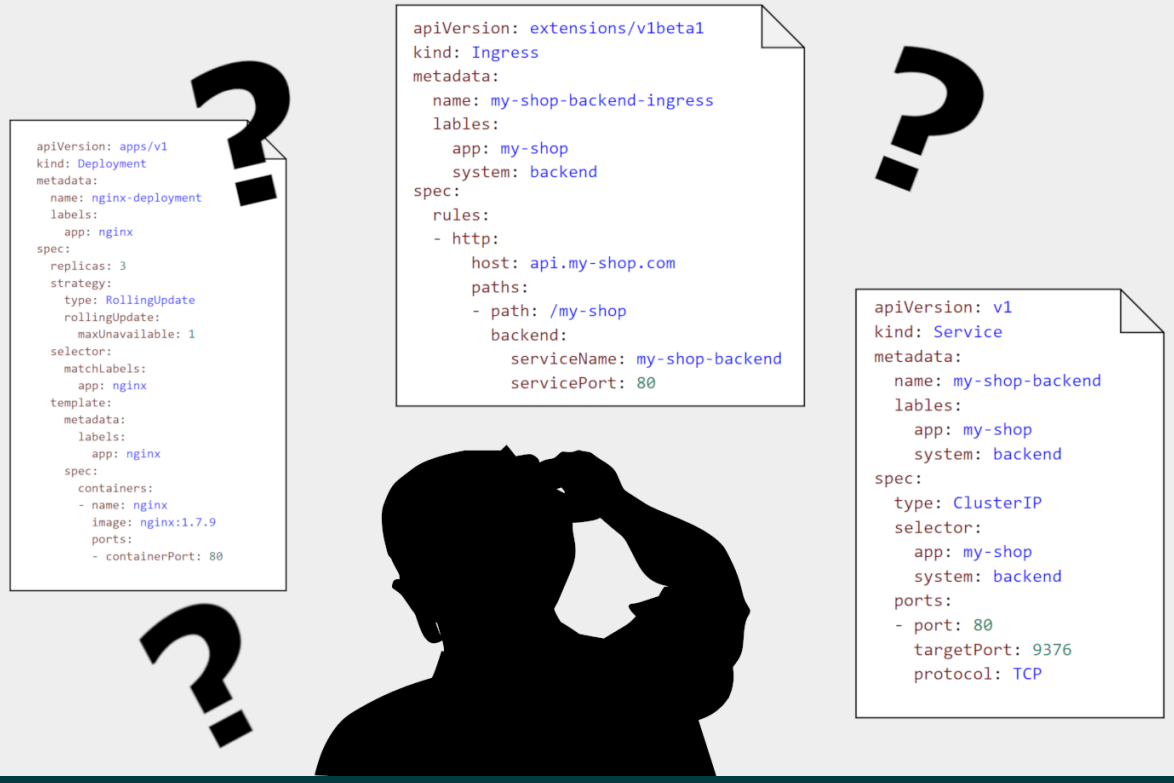
Leverancier Docker-compose

Omzetten tot Kubernetes



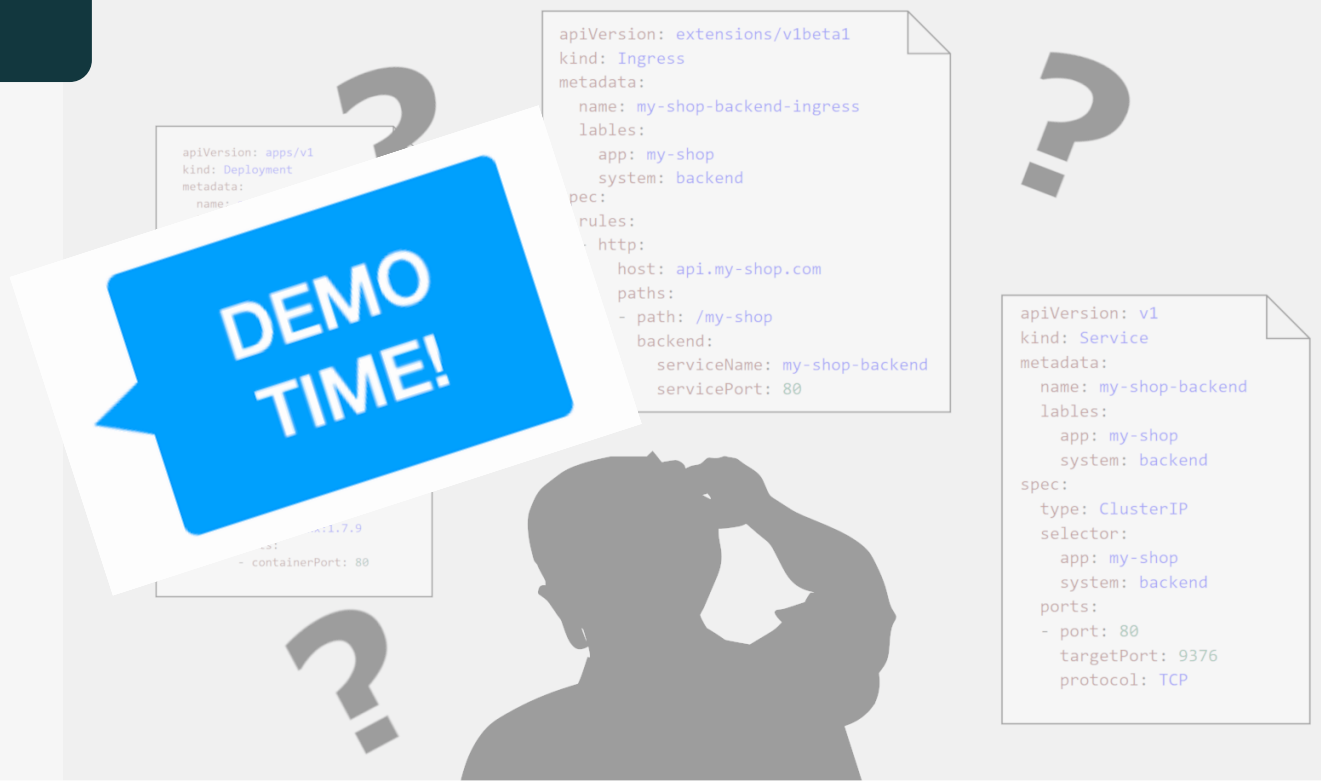
Wat zijn Manifest files?

- Containers
- Images
- Netwerken
- Secrets
- Poortnummers



Wat zijn Manifest files?

- Containers
- Images
- Netwerken
- Secrets
- Poortnummers

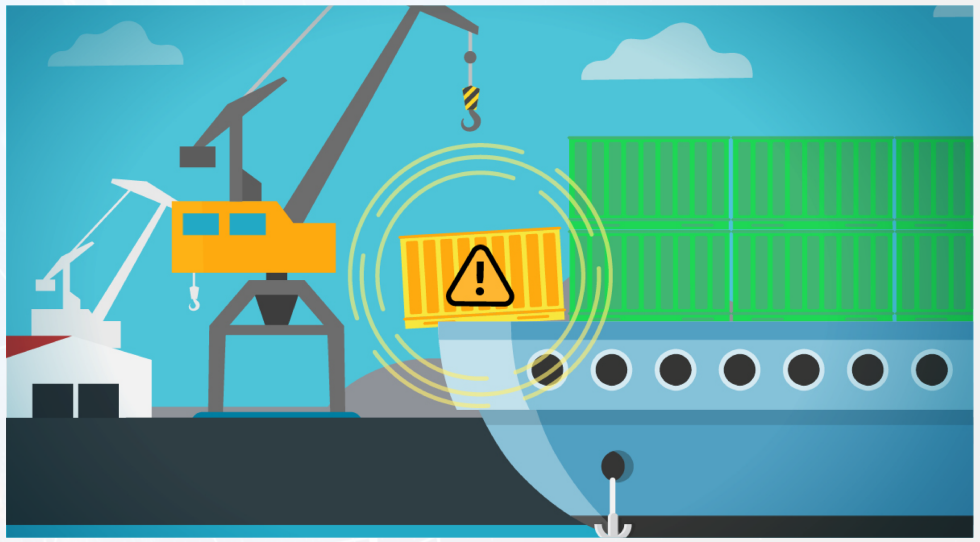



Kubernetes Security

Welke Risico’s

Type Risico’s

- Container image;
- Container Registry;
- Kubernetes orchestratie laag;
- Container (runtime);
- Operating System Kubernetes Nodes;



Welke Risico’s

Container image risico’s

- Vulnerabilities (CVE’s);
- Configuration defects;
- Embedded malware;
- Embedded clear text secrets;
- Untrusted images.

Mitigerende maatregelen

- Aqua can scan during build time (integration with Azure DevOps);
- Aqua can scan your Azure Container Registry;
- Aqua scans images on AKS hosts;
- Each image is scanned for vulnerabilities both in its OS packages and development language files.

Risico's

Container Registry van risico's

- Insecure connections;
- Stale images;
- Insufficient authentication and authorization restrictions.

Mitigerende maatregelen

- Only allow images from specific (trusted) container registries;
- Allows daily scans of images to alert on out-of-date vulnerable packages, base-images and versions;
- Allows the admin to define stale images via custom checks and block them from running;
- Can integrate automated scans into your CI processes to ensure only authorized images can be used.

Risico's

Kubernetes Orchestratie risico's

- Unbounded administrative access;
- Unauthorized access;
- Poorly inter-container connectivity;
- Mixing of workload sensitivity levels;
- Node trust.

Mitigerende maatregelen

- Audit logging;
- Set and enforce user access policies to container resources;
- Monitor user access, blocks, alerts unauthorized access attempts;
- Container Firewall limits network connectivity between workloads;
- Host integrity checks, including vulnerability scan, malware and CIS test to ensure nodes are secured.

Risico's

Container risico's

- Vulnerabilities within runtime software;
- Unbounded network access from containers;
- Insecure container runtime configuration;
- Application vulnerabilities.

Mitigerende maatregelen

- Threat mitigation defenses detect and prevent port scanning;
- Threat mitigation defenses to detect and prevent connections to IP addresses with poor reputation;
- Real-time audit events on policy violations, report to SIEM tooling;
- Check for configuration drift;
- Block non-compliant images
- Block/allow certain executables;
- Prevent certain volumes to be mounted in a container;
- Manage and enforce seccomp profiles to unwanted syscalls;
- Log all container events.

Risico's

Operating system risico's

- Attack surface;
- Shared kernel;
- Host OS component vulnerabilities;
- Improper user access rights;
- Host file system tampering.

Mitigerende maatregelen

- Scans host for vulnerabilities and malware against the Center for Internet Security (CIS) benchmarks (Docker, K8s);
- Logs user login and logout events on the host, including invocation of sudo programs;
- Scans hosts for configuration issues per the CIS Docker Benchmark;
- Restrict containers from specific mounting volumes or from writing into specific volumes or directories.

Tool selectie

VS

Pro's
- Azure Integrated
- Built in Storage, IAM
- Doorontwikkeling hoog

Cons
- Azure Only
- Geen Multicloud
- Niet opensource

Pro's
- Opensource
- Multicloud /OnPrem
- Multi integraties

Cons
- Configure IAM, Storage
- Doorontwikkeling laag

Tool selectie

Pro's

- Forensics
- Investigation
- Doorontwikkeling

Cons

- AWS/Google Focussed
- Meer focus op Cloud

VS

Pro's

- More scan capabilities
- Multicloud /OnPrem
- Multi integraties

Cons

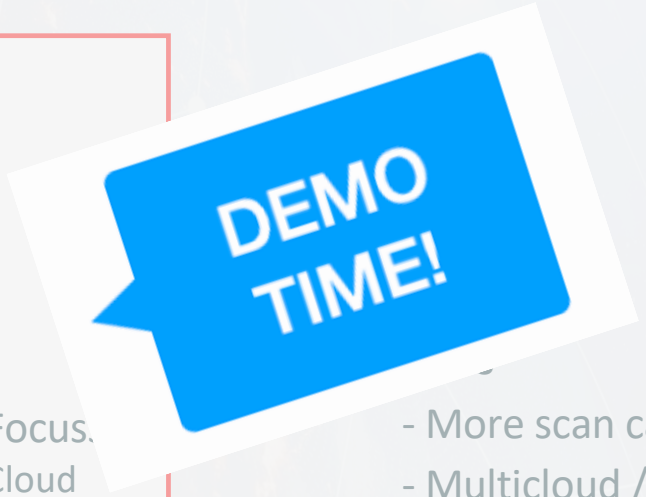
- Doorontwikkeling laag

Tool selectie

sysdig

Pro's
- Forensics
- Investigation
- Doorontwikkeling

Cons
- AWS/Google Focus
- Meer focus op Cloud



aqua

Cons
- Doorontwikkeling laag

- More scan capabilities
- Multicloud /OnPrem
- Multi integraties

CI/CD - App Container straat

Use cases

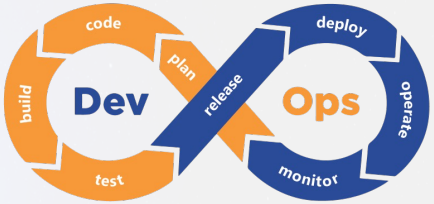
Geautomatiseerde uitrol van applicaties

Versiebeheer en audit trails

Code opslag collaboratie mogelijkheden

Werkwijze gevisualiseerd in Dashboards

Tool selectie



Azure DevOps

VS

GitHub Actions

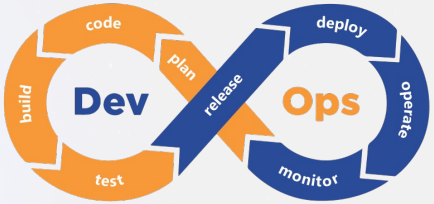
Pro's
- Gates
- Stages defined in Yaml
- Also On-prem build agents

Cons
- non

Pro's
- Opensource

Cons
- Self-hosted agents only

Tool selectie



Azure DevOps

Pro's

- Gates
- Stages defined in Yaml
- Also On-prem build agents

Cons

- non

VS

GitHub Actions

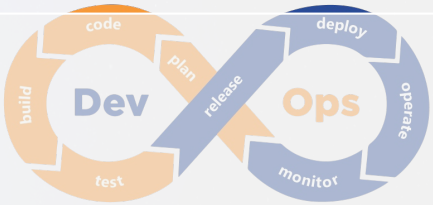
Pro's

- Opensource

Cons

- Self-hosted agents only

Tool selectie



Azure DevOps

Pro's
- Gates
- Stages defined in Yaml
- Also On-prem build agents

Cons
- non

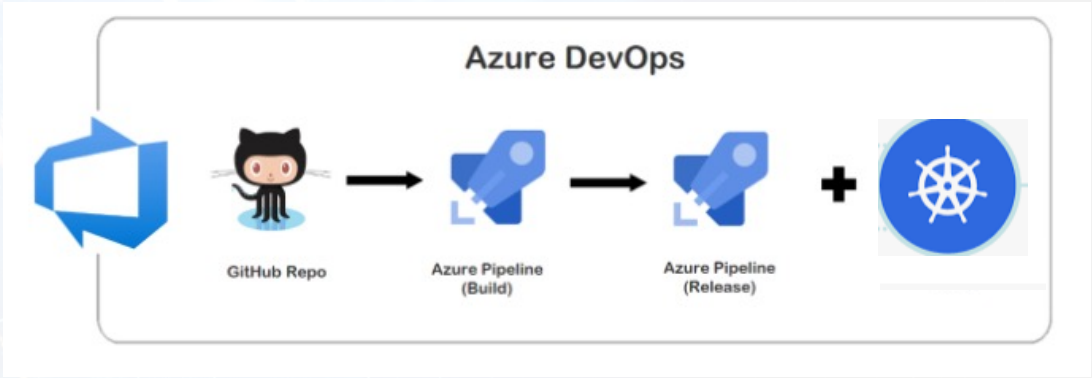
GitHub Actions

- Opensource

Cons
- Self-hosted agents only

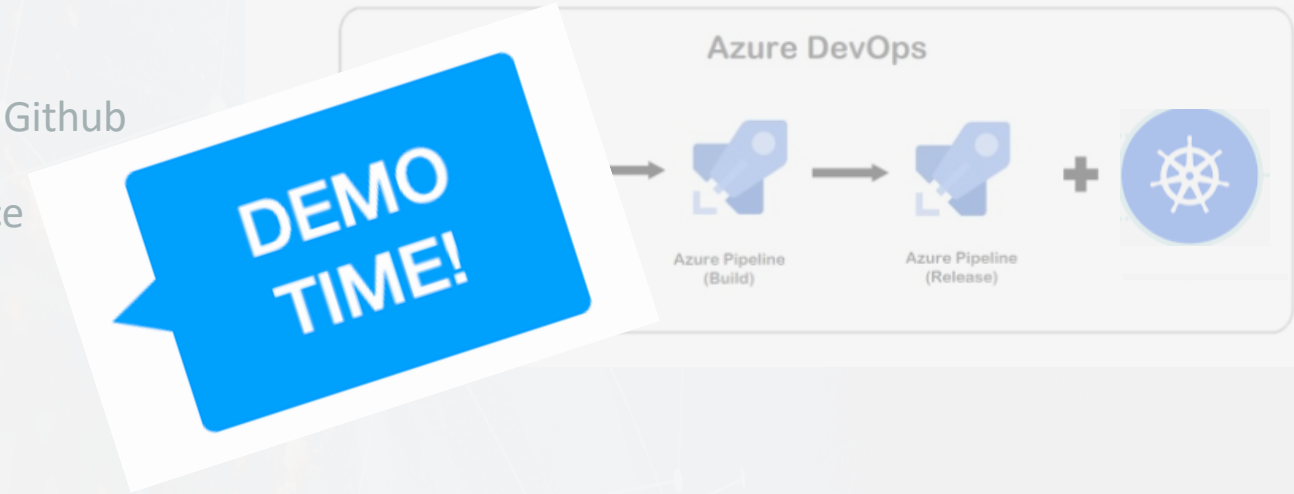
Simpele CI/CD pipeline

Code opslag vanuit Github
Azure Pipeline
Deploy een resource



Simpele CI/CD pipeline

Code opslag vanuit Github
Azure Pipeline
Deploy een resource




Infrastructure as Code
Provisioning de infra

Use cases

Geautomatiseerde uitrol van infra (bouw)blokken

Versiebeheer en audit trails

Proof of Concepts

Automatiseren gebruikers aanvragen

Tool selectie


+


VS

Pro's
- Dichtst bij Azure
- Geen State File
- Preview features

Cons
- Geen delete/destroy
- Azure specifiek
- Json format

Pro's
- Cloud agnostisch
- Multi Provider plugins
- Delete/Destroy

Cons
- State File
- Geen Preview features
- HCL format

Tool selectie


+


VS

HashiCorp Terraform

Pro's

- Dichtst bij Azure
- Geen State File
- Preview features

Cons

- Geen delete/destroy
- Azure specifiek
- Json format

Pro's

- Cloud agnostisch
- Multi Provider plugins
- Delete/Destroy

Cons

- State File
- Geen Preview features
- HCL format

Uitrol AKS cluster

- Resource groep
- LoadBalancer
- AKS cluster

Uitrol AKS cluster

Resource groep
LoadBalancer
AKS cluster

Take aways

- Begin klein
- Kies een usecase
- Toegevoegde waarde zien
- DRY-Principe
- Herhaling? Automatiseer
- Build & Test
- Gewoon doen!
- Blijf Innoveren


Next Time ...
Q3 2022
Workshop Apps bouwen
Workshop Azure Pipelines
Q4 2022
Worskhop IaC met Terraform

IT-IMPRESSIVE

SIMPLIFYNOW

Thanks for your attention