

Jak Kubernetes zrychlilo nasazování aplikací do Drážního Úřadu a zjednodušilo jejich provoz

Ondřej Šika

Freelance & SikaLabs s.r.o.

ondrej@sika.io
@ondrejsika

Kontejnery v praxi
Praha, 27. 2. 2024

SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



Ondřej Šika

Jsem DevOps lektor, architekt a konzultant z Prahy.

Navrhnu a implementuji Vám na míru DevOps architekturu od verzování v Gitu po provoz kontejneru v Kubernetes v Cloutu.



Moje DevOps školení

Dělám populární školení, kde své znalosti předávám tak, abyste si mohli vše udělat sami a bez zbytečných přešlapů a slepých cest.

- Úvod do DevOps
- Docker
- Kubernetes

Kubernetes



Terraform



Docker



Prometheus



Rancher



ArgoCD



Gitlab CI



Git



Ansible



Elk



DigitalOcean



Proxmox



SikaLabs

Mám skvělé kolegy

Postaráme se Vám o zavedení DevOps technologií do firmy nebo o kompletní správu DevOps.



SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



Our DevOps Stack

- **Git**, Gitlab - Versioning & Collaboration
- Gitlab CI, **ArgoCD** - Continuous Integration, Continuous Deployment
- Docker, **Kubernetes** - Containers & Orchestration
- **RKE2** & Rancher - Kubernetes Provisioning
- Terraform - Infrastructure management
- Prometheus, Alertmanager, Grafana - Monitoring Stack
- Elastic Stack / **Loki** - Log Management
- AWS, Azure, DigitalOcean, Proxmox - Public or Private Cloud



Problém



Provoz aplikací v DÚ



Drážní Úřad

Správní úřad, který vykonává státní správu v oblasti drah.

Zabývá se dráhou železniční, tramvajovou, trolejbusovou, lanovou a speciální (metrem).

Celkový počet zaměstnanců je 113.

© 2023 Google



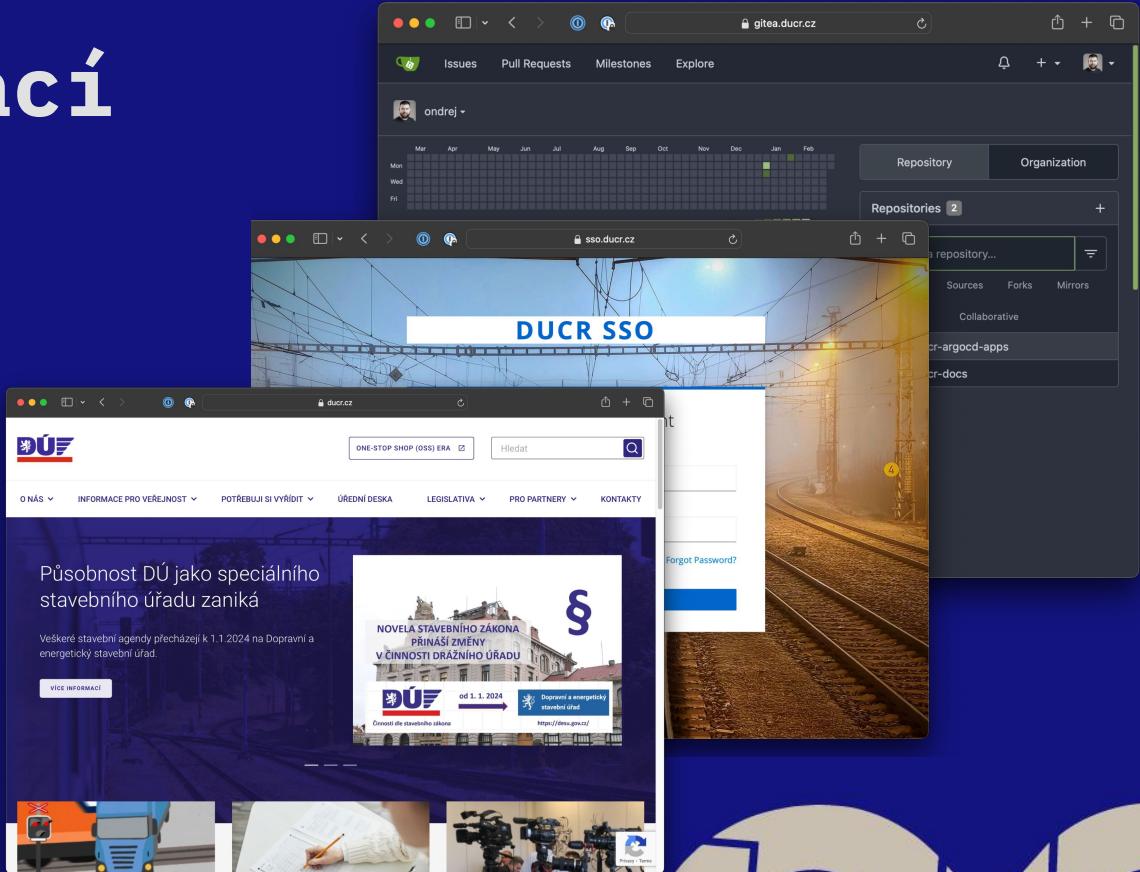
Problémy provozu aplikací v DÚ

- Omezené zdroje
 - Finance
 - Manpower
- Různé aplikace - každá se provozuje jinak
 - Běžný Open Source
 - Custom Development
 - ...



Ukázky aplikací

- Weby
 - ducr.cz, ...
- Open Source
 - Keycloak SSO
 - Zammad Helpdesk
 - ...
- Interní Systémy



Problémy nasazování v DÚ

- Rychlosť nasazení aplikace
 - Je potřeba vytvořit prostředí - VMs
 - Správa infra byla manuální
 - Instalace poskytovatelem / manuálně podle dokumentace
- => Pro každou aplikaci stavíme prostředí znovu (ručně) a pokaždé jinak
- => velmi pomalé



Problémy provozu v DÚ



- Každá aplikace se provozuje různě
 - PHP + Apache, Node.js, Tomcat, Docker Compose, ...
- Aktualizace se prováděly manuálně (dodavatel, podle docs)
- Manuální přidávání do monitoringu, ...
- Absence centrálního log managementu - každá aplikace logovala k sobě a dost různě
 - => velmi náročné zvládnout všechny rozdílné technologie
 - => obzvlášť ve velmi malém teamu





Řešení?

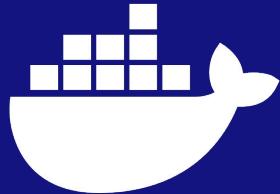
SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



Kontejnery + Kubernetes



- Unifikace prostředí
- Definice hranice zodpovědnosti
- Automatizace



Unifikace prostředí

- Je potřeba co nejvíce věcí dělat stejně
- Musíme používat jednotné nástroje a procesy při provozu a nasazování různých aplikací
- Nesmíme pokaždé vše tvořit od začátku - musíme používat to, co máme
- Musíme využívat existující (open source) tooling



Hranice Dodavatel / Provozovatel

Musíme vyjasnit hranici mezi dodavatelem a provozovatelem aplikace

Díky kontejnerům je hranice jasná, dodavatel připraví Docker image a Helm balíček pro Kubernetes

O běh clusteru, sběr logu, monitoring, storage backupy, ... se stará DÚ



Automatizace

- Malý team nedokáže dělat věci ručně, musíme tedy automatizovat
- Nechceme manuálně řešit proces nasazování & upgrade
- Chceme co nejméně nutnosti manuálních zásahů při provozu aplikací



Kontainery

SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



“A container is a lightweight, stand-alone, executable package that includes everything needed to run a piece of software, including the code, runtime, system tools, libraries, and settings.“



Kubernetes

SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



**“Kubernetes is an platform designed to
automate deploying, scaling, and operating
application containers.“**



Proč tedy Kubernetes?

- De-facto standard provozu software
- Unifikace prostředí pro provoz aplikací
- Ovládání pomocí YAML souboru / Helm balíčku
- Deployment (deklarativní) požadovaného stavu
- Přístup ke clusteru místo k jednotlivým serverům
- Automatizace manuálních tasků
- Opensource, pod CNCF
- Velký ekosystém kolem Kubernetes



Naše řešení

SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



Goal

- On-premise Kubernetes environment
- Infrastructure as Code
 - Všechno chceme mít v Gitu, žádné manuální úpravy
- Postavené na OpenSource



Naše řešení

Řešení je postaveno nad fyzickými stroji v DC Drážního Úřadu

Tech stack

- RKE2 Kubernetes (Rancher Kubernetes Engine)
- Longhorn Storage
- ArgoCD
- Observability
 - Prometheus, Grafana, Loki
- Keycloak SSO, SSO Proxy
- ...



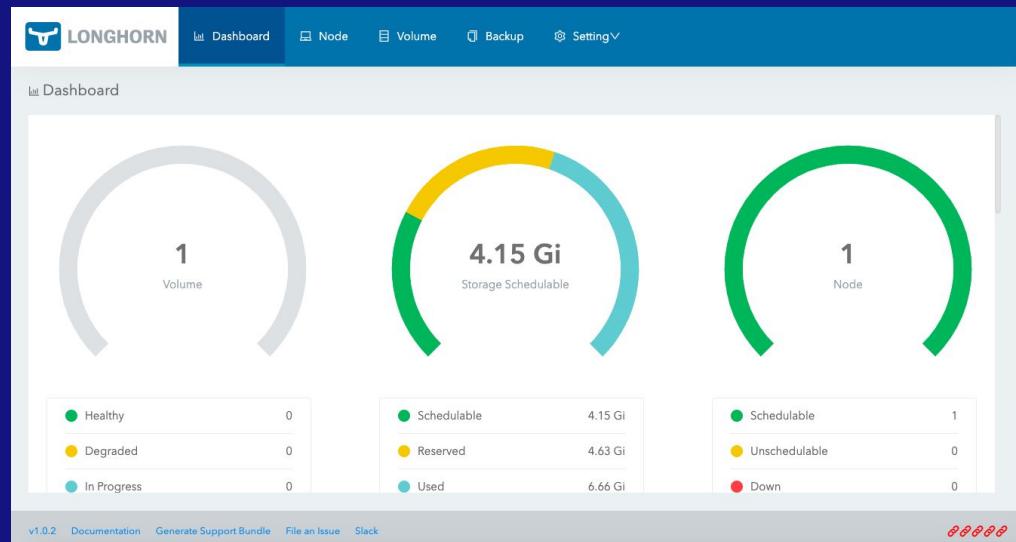
Rancher Kubernetes Engine / RKE2

- Kubernetes distribuce vhodná pro on-premise
- Od SUSE (v roce 2020 koupili Rancher)



Longhorn

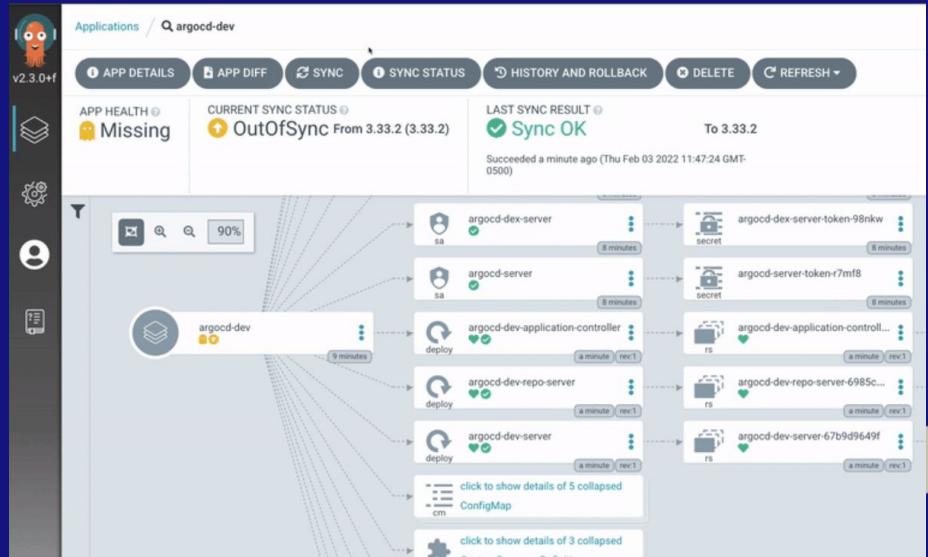
- Nativní Kubernetes storage od Rancheru
- Jednoduchý setup
- Nativní podpora zálohování
 - S3
 - NFS
- UI



ArgoCD

GitOps pro Kubernetes

- Nasazujeme deklarativně z Gitu
- UI pro Kubernetes



Prometheus, Loki, Grafana

- Moderní observability stack
- Light weight



Čeho jsme tedy dosáhli

- Nasazení aplikace se zkrátilo z řádů týdnů na dny
- Staráme se o provoz jedné platformy, ne o každou aplikaci zvlášť
- Zálohování je unifikované - řešíme na úrovni Longhornu
- Sjednocený a automatizovaný monitoring
 - napojený na service discovery v Kubernetes
- Centrální správa logů v Grafana Loki



Proces nasazení aplikace

1. Dodavatel dodá Docker Images + Helm Balíček (případně mu pomůžeme)
2. V ArgoCD Repozitáři vytvoříme objekt s konfigurací aplikace pro různá prostředí (test, stage, prod)
3. Commitneme do Gitu

Vše ostatní se provede samo.

- Aplikace se nasadí a automaticky se přidá do monitoring
- Zálohy, sběr logů a metric je by default nad celou platformou





Díky za pozornost



Otázky

SikaLabs s.r.o.

hi@sikalabs.com

sikalabs.com



Email

ondrej@sika.io

Twitter

@ondrejsika

LinkedIn

/in/ondrejsika

Slides

sika.link/slides

