Infrastructure as Code a GitOps pomocí Terraformu

Ondřej Šika

ondrej@sika.io
@ondrejsika

Cloud Computing Conference, 12. 5. 2022

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Ondřej Šika

Jsem DevOps lektor, architekt a konzultant z Prahy.

Navrhnu a implementuji Vám na míru DevOps architekturu od verzování v Gitu po provoz v Cloudu.

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

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Můj Opensource DevOps Stack

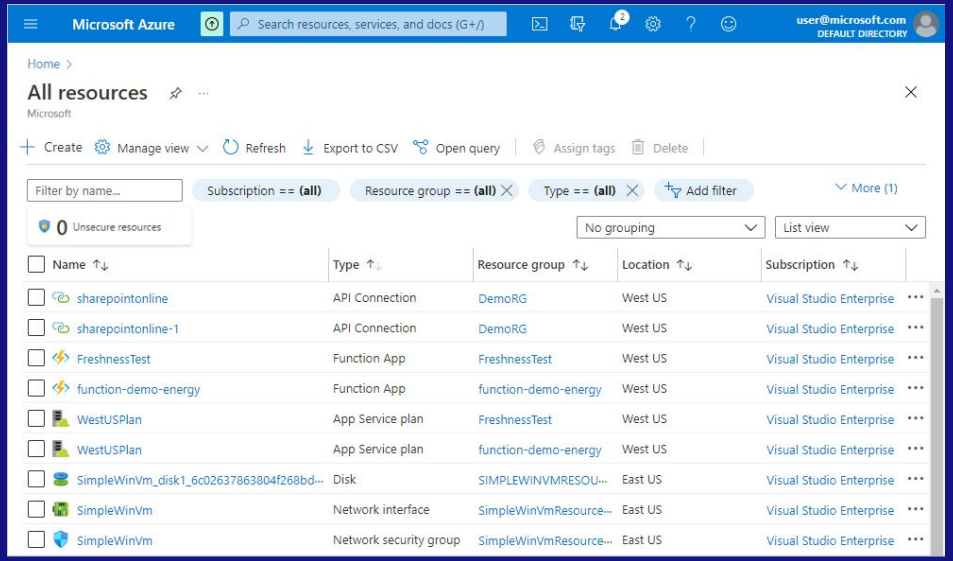
- **Git**, **Gitlab** - Versioning & Collaboration
- **Gitlab CI**, ArgoCD - Continuous Integration, Continuous Deployment
- Docker, Kubernetes - Containers & Orchestration
- RKE & Rancher - Kubernetes Provisioning
- **Terraform** - Infrastructure management
- Prometheus, Alertmanager, Grafana - Monitoring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

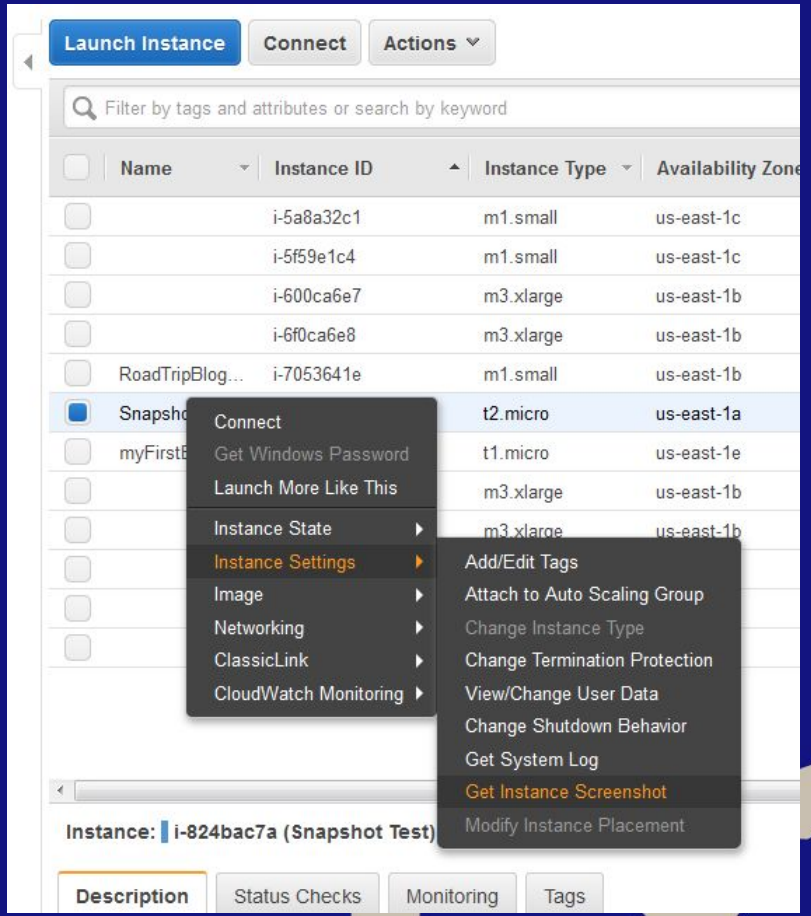
...

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Cloud is hard

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika





@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Cloud is hard

- Rozsáhlé a ne vždy přehledné UI
- Časté změny (nejen v UI)
- Manuální práce - klikání
- Těžko udržovaná dokumentace projektu
- Nevíme, co nám přesně běží a jak je to nastavené
- Obtížné audity
- Nejasný zdroj pravdy (dokumentace vs skutečnost)

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Řešení?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

IaC & GitOps

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Co je IaC?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Co je IaC?

Infrastructure as code (**IaC**) je způsob, jakým spravovat veřejné i privátní cloudy pomocí **deklarativně definovaných** konfiguračních souborů, které používají nástroje pro správu infrastruktury jako zdroj pravdy.

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Co je GitOps?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

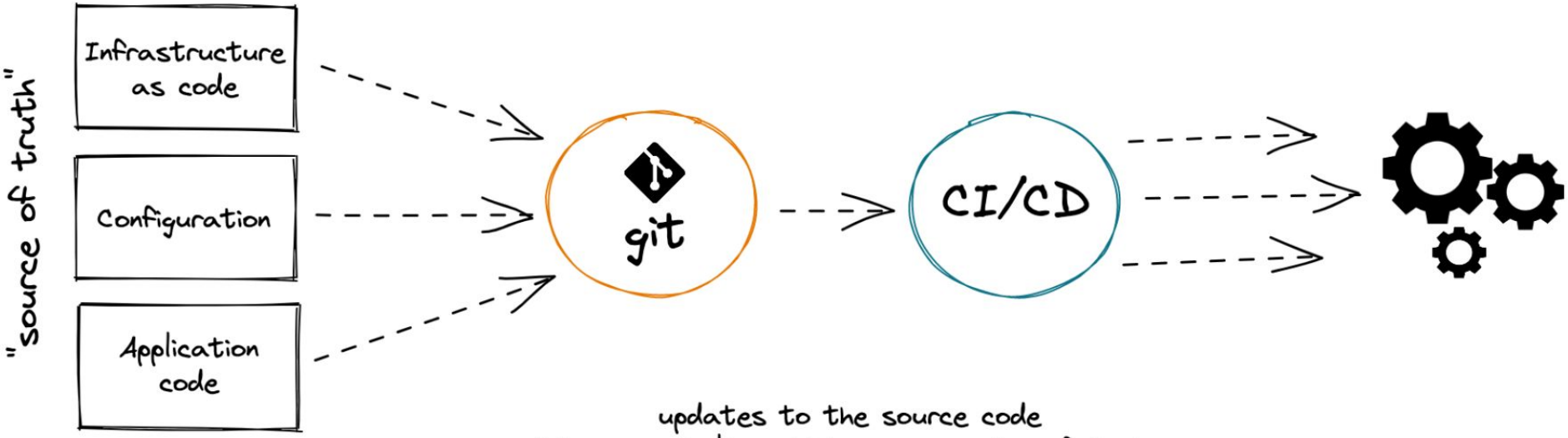
Co je GitOps?

GitOps je přístup, kdy máme jako **jediný zdroj pravdy Git repozitář** a vše (infrastruktura i aplikace) jsou v něm deklarativně definované. Podle toho víme, kdo kdy a co nasadil a můžeme efektivně spolupracovat.

GitOps = IaC + MRs + CI/CD

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

GitOps in a nutshell



updates to the source code
trigger a pipeline, which runs a series of tasks
to update runtime environments so they match the source

Infrastructure as Code & GitOps

Přístup IaC a GitOps nám umožňuje:

- Jediný zdroj pravdy
- Jasná a přehledná historie
- Spolupráce
- Merge requests & Code review
- CI/CD Automatizací
- Dynamické prostředí
- Jednoduchý audit
- Recyklace předchozí práce

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

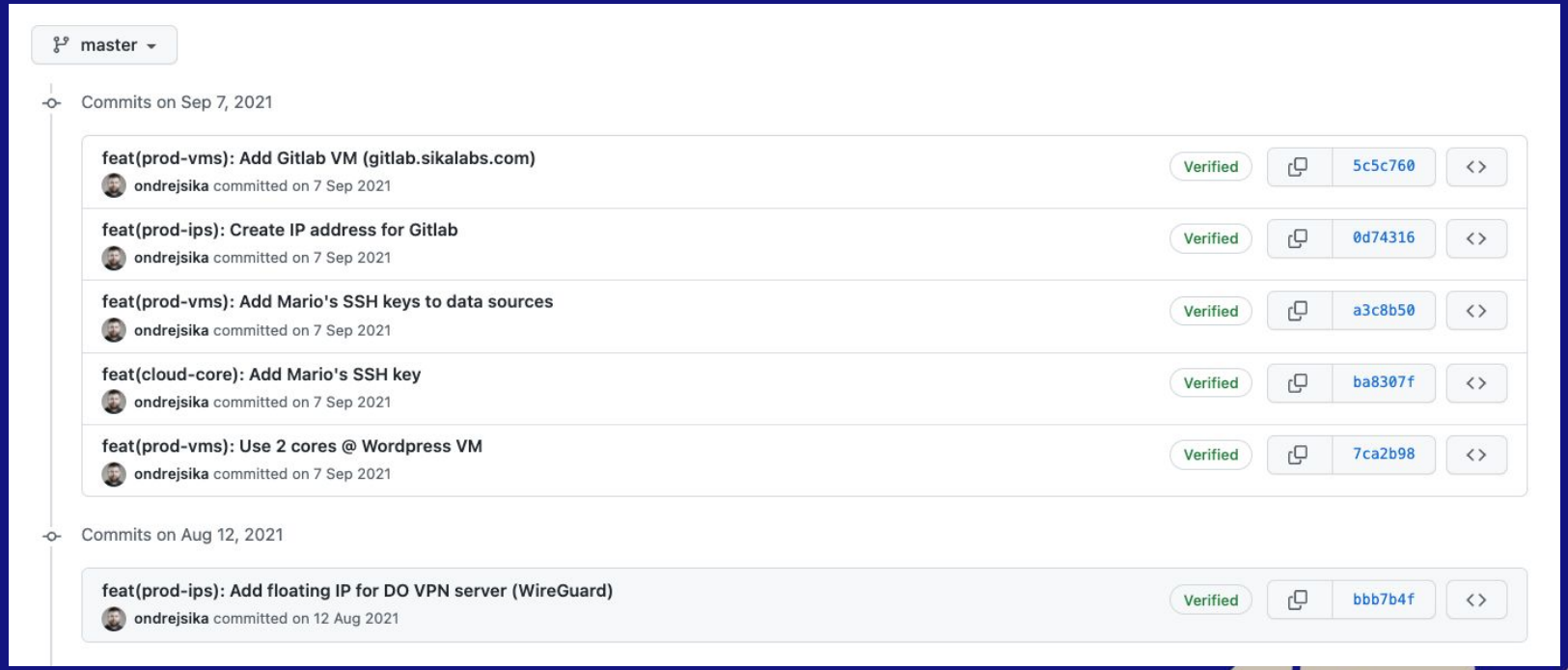
Jediný zdroj pravdy

- Git repozitář určuje, co a jak má být nastavené
- Terraform (případně jiný nástroj) tyto zdrojové kódy přímo aplikuje, nelze aby vznikl rozdíl, co je deklarováno a co je nasazeno.
- Při manuálním nasazování z dokumentace se jednoduše udělá chyba
- Není možné nic měnit jinou formou, to znamená, že vše, co se aplikuje, musí jít přes Git

Jasná a přehledná historie

- Každá změna je commit (vytvořený člověkem nebo strojem (bot))
- Pomocí běžných nástrojů pro práci s Gitem vidíme historii - jak a co bylo nasazováno a upravováno
- Můžeme se kdykoliv vrátit do historie nebo porovnat různé verze co se změnilo

Historie změn v Gitu



@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

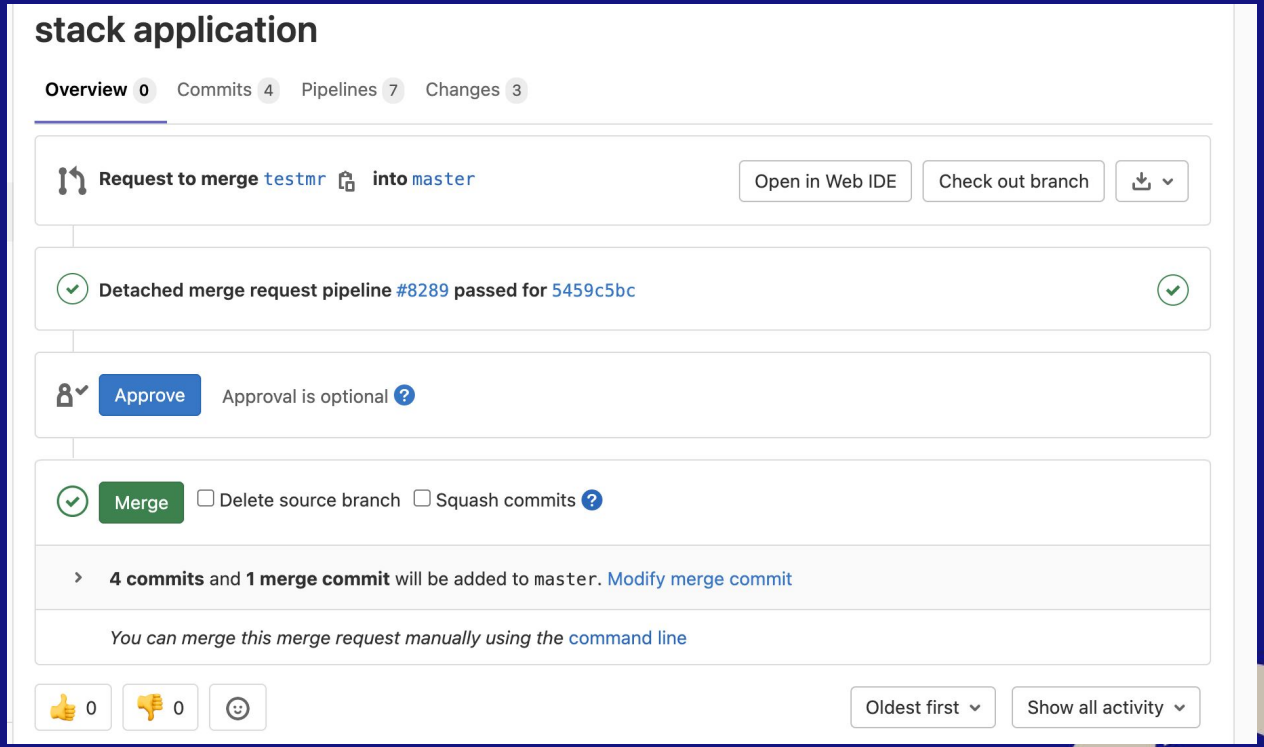
Spolupráce, Merge Requesty a Code Review

Díky Gitu můžeme vyvíjet infrastruturu v cloudu stejně jako software:

- Merge Requesty
- Testy
- Code review

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Spolupráce, MRs, Code Review

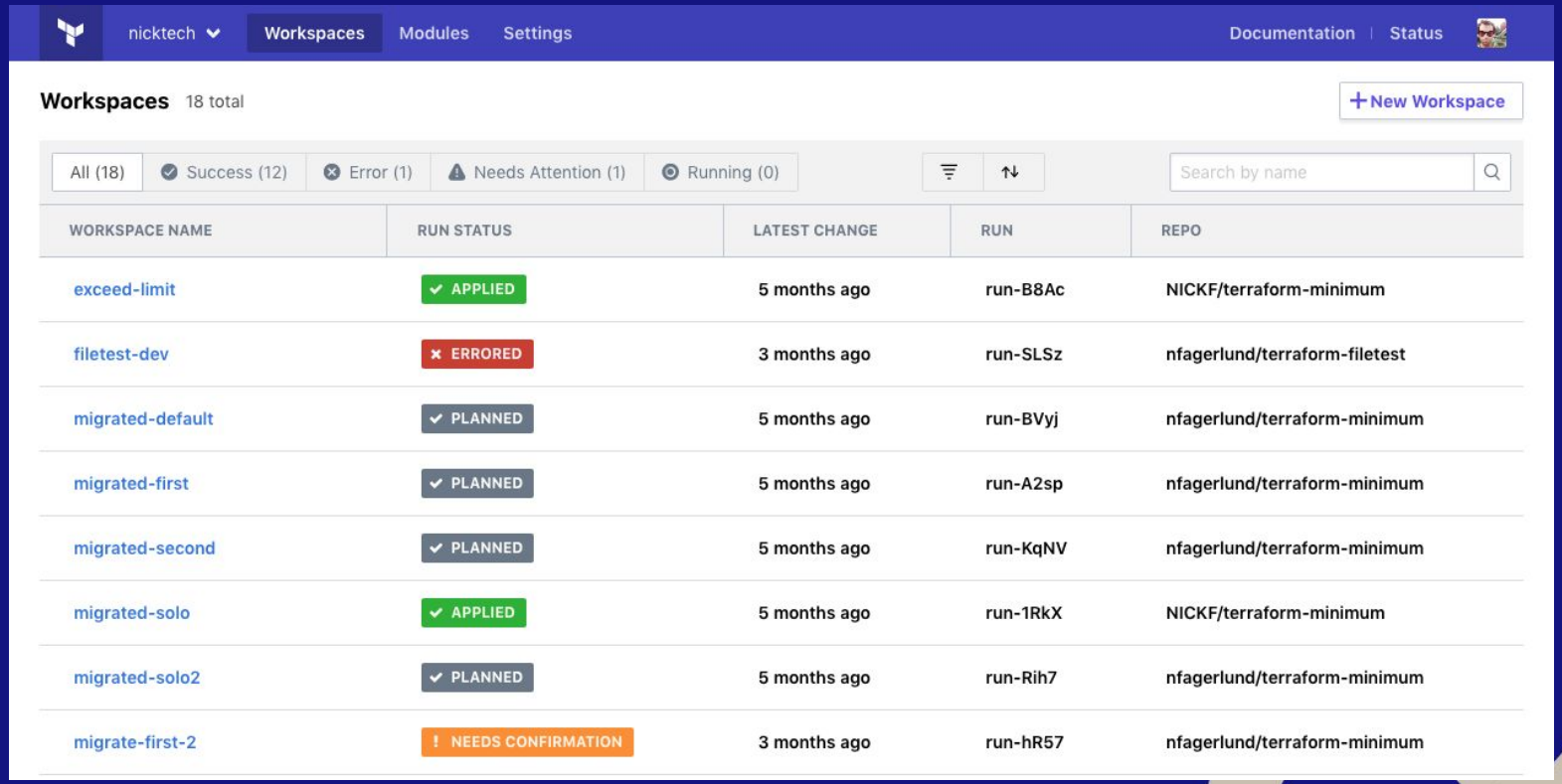


@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Dynamické prostředí

- Z jedněch zdrojových kódu můžeme pustit více prostředí
- Prostředí mohou být různá nebo identická
- Prostředí můžeme jednoduše dynamicky zapínat a vypínat podle potřeby

Dynamické prostředí



@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Nástroje IaC

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Terraform

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Co je Terraform?

Terraform je management tool který umožňuje spravovat **Infrastrukturu formou kódu**

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

```
resource "digitalocean_droplet" "example" {
  image    = "debian-10-x64"
  name     = "example"
  region   = "fra1"
  size     = "s-1vcpu-1gb"
}
```

```
resource "digitalocean_record" "example" {
  domain = "example.com"
  type   = "A"
  name   = digitalocean_droplet.example.name
  value  = digitalocean_droplet.example.ipv4_address
}
```

Vlastnosti Terraformu

- Nezavislý na cloud provideru - pracuje se všemi cloudy
- Podpora multicloud řešení
- Dekarativní přístup
- Full state management
- Open source & Free
- Podpora vlastních pluginů a rozšíření
- De facto standart
- Hodně rozšíření

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Teraform a ostatní nástroje

- Terraform
- Cloudformation, AzureRM, ...
- Ansible, Puppet, Chef, ...

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Cloudformation, AzureRM, …

- Nástroje určené na správu cloudu
- Jsou svázané s konkrétním cloud providerem

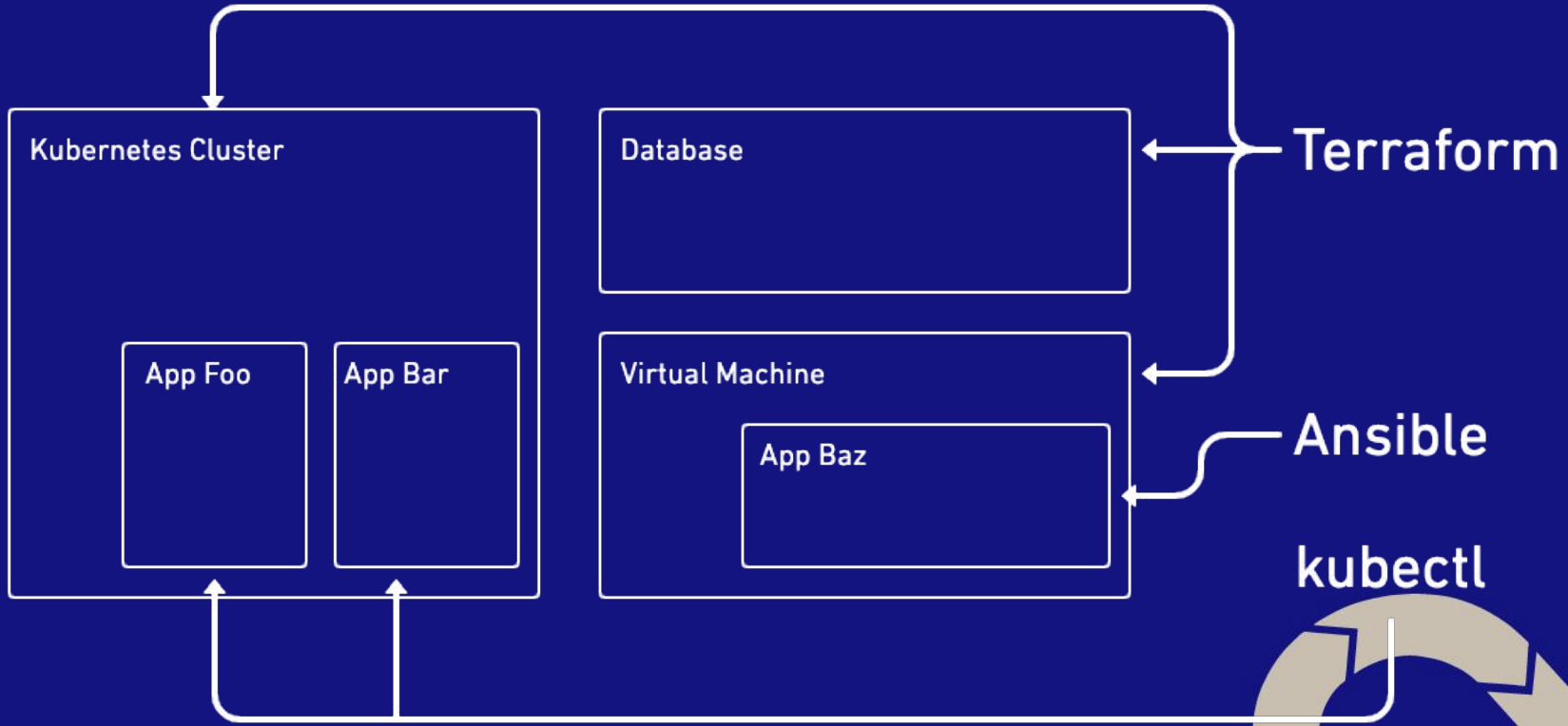
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Ansible, Puppet, Chef, …

- Nástroje určené primárně pro konfiguraci severu
- Nejsou plně deklarativní
- Absence state - neefektivní mazání
- Pomalé

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Terraform, Ansible & Application Deployment



@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Terraform + GitOps

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

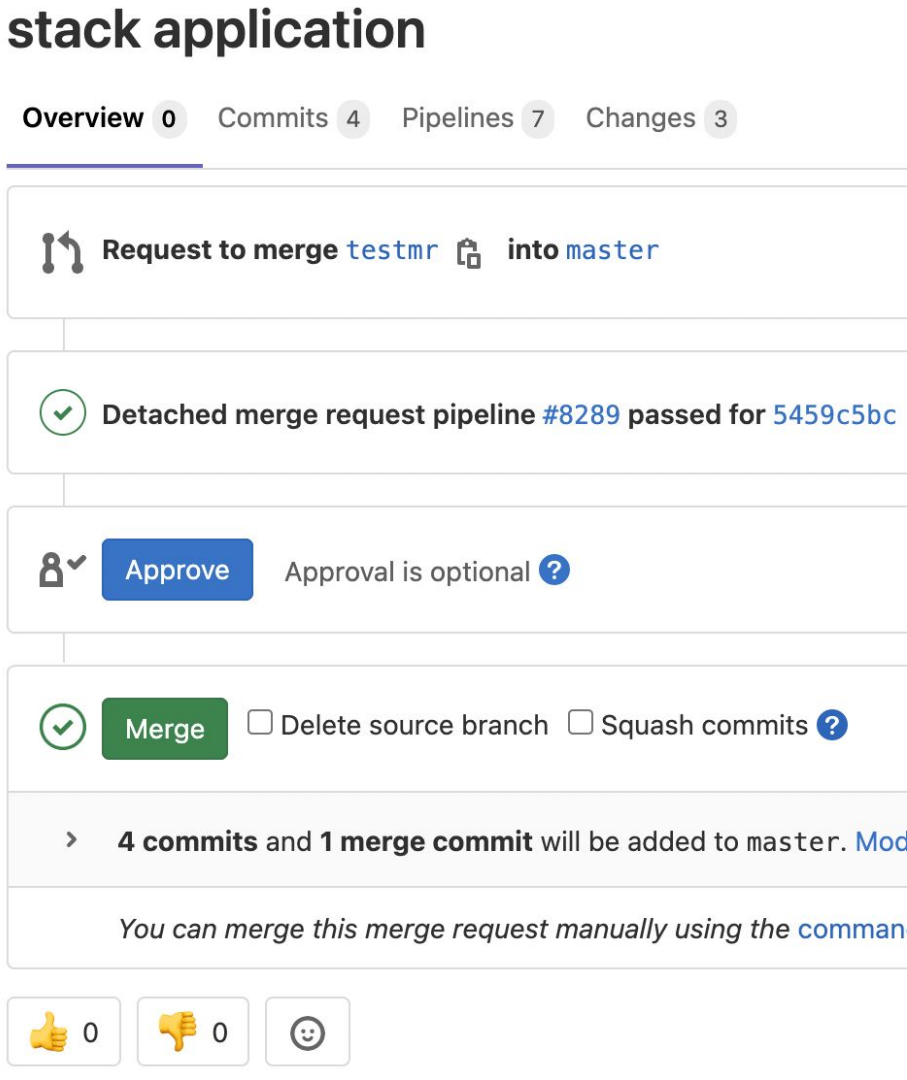
Terraform + Gitlab CI/CD

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

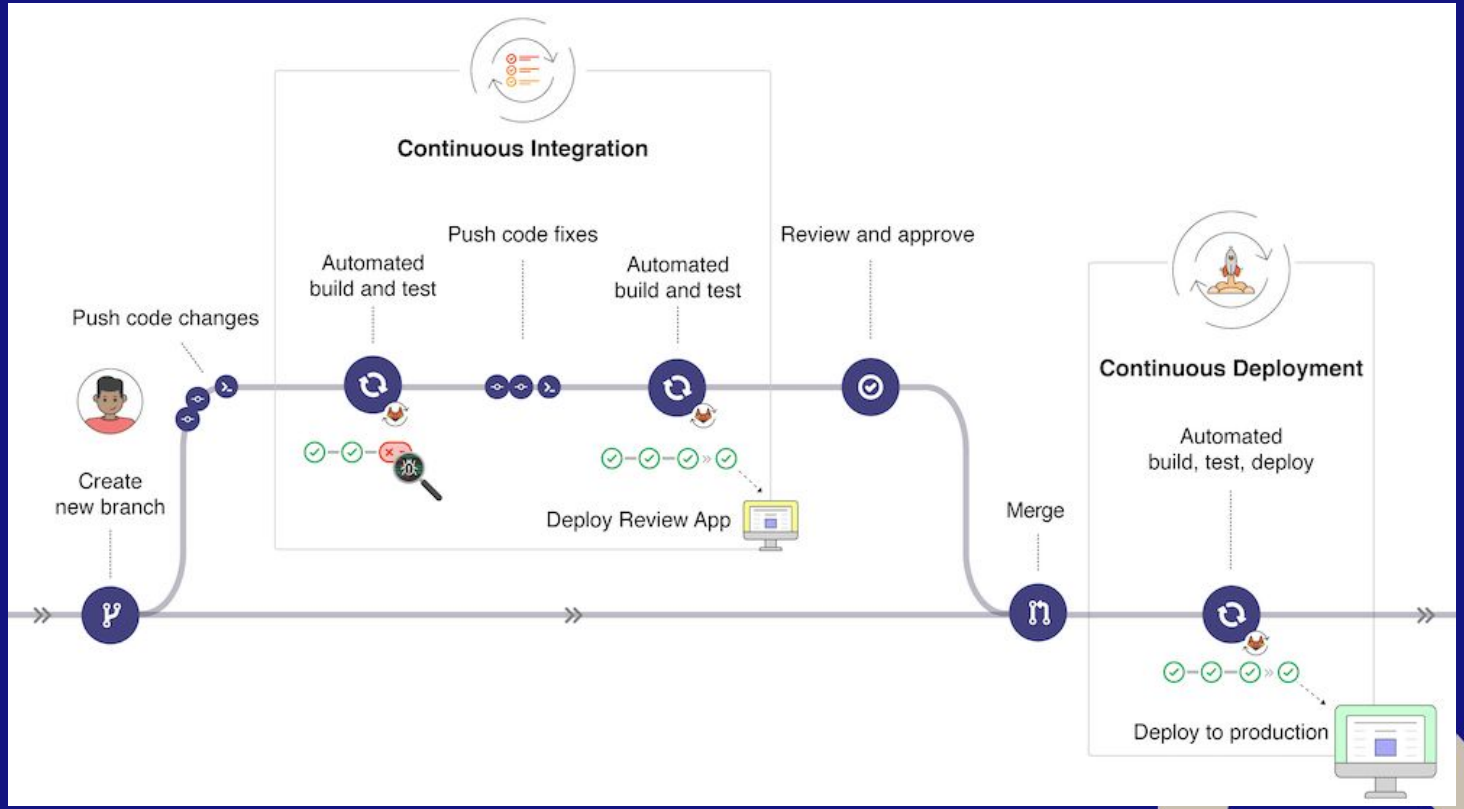
Gitlab CI + Terraform

- Velmi dobrý CI/CD nástroj
- Nativní integrace s Gitlabem
  - merge requesty
  - code reviews
- Nativní podpora Terraformu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika



Gitlab CI + Terraform Workflow



@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Alternativy ke Gitlab CI

- Github Actions - prakticky stejné, akorát pro Github
- Terraform Cloud - CD nástroj nezavislý na Git hostingu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Práce s Terraformem

- Terraform je plně deklarativní
- Podpora cloudu pomocí provideru
- Moduly & Terraform Registry
- Linter, Formater
- Podpora externích (nebo ručně vytvořených) cloud resourcu
- Import stávající infrastruktury

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Imperativní vs Deklarativní přístup

Imperativní přístup

- sada příkazů, co se mají vykonat
- příklad: Pokud neexistuje server, tak ho vytvoř v zóně us-east

Deklarativní přístup

- popisuje finální stav
- příklad: chci server v zóně us-east

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

```
resource "digitalocean_droplet" "example" {
  image    = "debian-10-x64"
  name     = "example"
  region   = "fra1"
  size     = "s-1vcpu-1gb"
}
```

```
data "digitalocean_ssh_key" "default" {
  name = "default"
}

data "digitalocean_domain" "default" {
  name = var.base_domain
}
```

```
resource "digitalocean_record" "ex
  domain = "example.com"
  type   = "A"
  name   = digitalocean_droplet.example.name
  value  = digitalocean_droplet.example.ipv4_address
}
```

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Další výhody Terraformu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Infracost

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Infracost

- Nástroj na odhadování ceny v cloudu
- Prochází Terraform zdrojové kódy a pomocí pricing API spočítá odhadované náklady
- Ukazuje, jak konkrétní změny (commity a merge requesty) mají vliv na cenu

4 terraform/main.tf

```
@@ -17,8 +17,8 @@ resource "aws_instance" "web_app" {
17 17     ebs_block_device {
18 18       device_name = "my_data"
19 19       volume_type = "io1"
20    -     volume_size = 1000
21    -     iops        = 800
   20 +     volume_size = 3000
   21 +     iops        = 1500
22 22     }
23 23   }
24 24
```

github-actions bot commented 15 minutes ago •

💰 Infracost estimate: **monthly cost will increase by $512 (+25%)** 📈

Project	Previous	New	Diff
infracost/ci-demo/dev	$267	$423	+$156 (+58%)
infracost/ci-demo/prod	$1,786	$2,142	+$356 (+20%)
All projects	$2,053	$2,565	+$512 (+25%)

▶ **Infracost output**

Rekapitulace

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Rekapitulace

- **IaC** + **GitOps** jsou obecné principy, které nám ulehčují správu velkých cloudových prostředí
- Jediný zdroj pravdy
- Jednoduchá spolupráce (merge requesty, code review, ...)
- **Terraform** je nejpoužívanější nástroj na IaC
- **GitOps** nám pro Terraform řeší **Gitlab CI/CD**, případně jeho alternativy

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Díky za pozornost

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Otázky?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Email

ondrej@sika.io

Twitter

@ondrejsika

LinkedIn

/in/ondrejsika

Slides

sika.link/slides

What's next?

sika.link/next

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika