

Infrastructure as Code a GitOps pomocí Terraformu

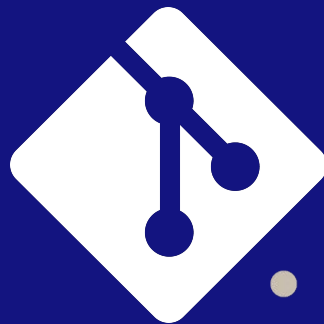
Ondřej Šika

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.

Navrhnou 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
- ...



Cloud is hard

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



Microsoft Azure

Search resources, services, and docs (G+)

user@microsoft.com
DEFAULT DIRECTORY

Home >

All resources

Microsoft

Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter by name... Subscription == (all) Resource group == (all) Type == (all) Add filter More (1)

0 Unsecure resources

No grouping List view

Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
sharepointonline	API Connection	DemoRG	West US	Visual Studio Enterprise
sharepointonline-1	API Connection	DemoRG	West US	Visual Studio Enterprise
FreshnessTest	Function App	FreshnessTest	West US	Visual Studio Enterprise
function-demo-energy	Function App	function-demo-energy	West US	Visual Studio Enterprise
WestUSPlan	App Service plan	FreshnessTest	West US	Visual Studio Enterprise
WestUSPlan	App Service plan	function-demo-energy	West US	Visual Studio Enterprise
SimpleWinVm_disk1_6c02637863804f268bd...	Disk	SIMPLEWINVMRESOU...	East US	Visual Studio Enterprise
SimpleWinVm	Network interface	SimpleWinVmResource...	East US	Visual Studio Enterprise
SimpleWinVm	Network security group	SimpleWinVmResource...	East US	Visual Studio Enterprise

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone
	i-5a8a32c1	m1.small	us-east-1c
	i-5f59e1c4	m1.small	us-east-1c
	i-600ca6e7	m3.xlarge	us-east-1b
	i-6f0ca6e8	m3.xlarge	us-east-1b
RoadTripBlog...	i-7053641e	m1.small	us-east-1b
Snapshot		t2.micro	us-east-1a
myFirst		t1.micro	us-east-1e
		m3.xlarge	us-east-1b
		m3.xlarge	us-east-1b

- Connect
- Get Windows Password
- Launch More Like This
- Instance State
- Instance Settings
- Image
- Networking
- ClassicLink
- CloudWatch Monitoring
- Add/Edit Tags
- Attach to Auto Scaling Group
- Change Instance Type
- Change Termination Protection
- View/Change User Data
- Change Shutdown Behavior
- Get System Log
- Get Instance Screenshot
- Modify Instance Placement

Instance: i-824bac7a (Snapshot Test)

Description Status Checks Monitoring Tags

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)



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.



Co je GitOps?

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



Co je GitOps?

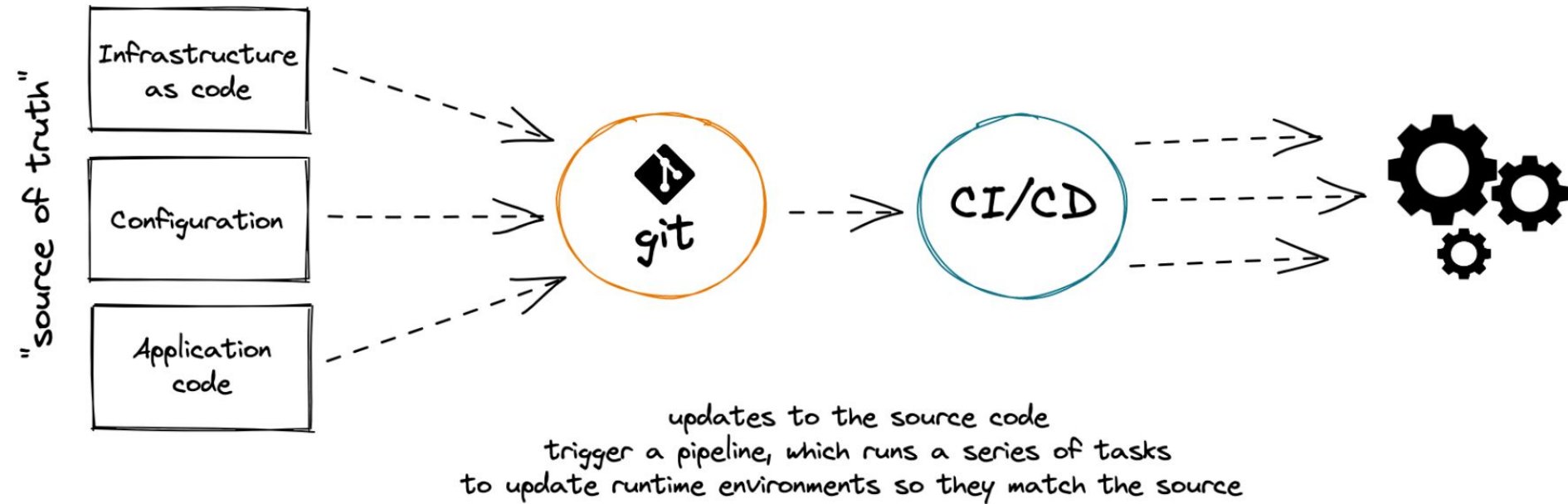
GitOps je přístup, kdy máme jako **jediný zdroj pravdy Git repozitář** a vše (infrastruktura i aplikace) jsou v něm deklarativně definované. Podle toho víme, kdo kdy a co nasadil a můžeme efektivně spolupracovat.



GitOps = IaC + MRs + CI/CD



GitOps in a nutshell



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



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

master ▾

Commits on Sep 7, 2021

feat(prod-vms): Add Gitlab VM (gitlab.sikalabs.com) ondrejsika committed on 7 Sep 2021	Verified		5c5c760	<>
feat(prod-ips): Create IP address for Gitlab ondrejsika committed on 7 Sep 2021	Verified		0d74316	<>
feat(prod-vms): Add Mario's SSH keys to data sources ondrejsika committed on 7 Sep 2021	Verified		a3c8b50	<>
feat(cloud-core): Add Mario's SSH key ondrejsika committed on 7 Sep 2021	Verified		ba8307f	<>
feat(prod-vms): Use 2 cores @ Wordpress VM ondrejsika committed on 7 Sep 2021	Verified		7ca2b98	<>

Commits on Aug 12, 2021

feat(prod-ips): Add floating IP for DO VPN server (WireGuard) ondrejsika committed on 12 Aug 2021	Verified		bbb7b4f	<>
---	----------	---	---------	----

Spolupráce, Merge Requesty a Code Review

Díky Gitu můžeme vyvíjet infrastrukturu v cloudu stejně jako software:



- Merge Requesty
- Testy
- Code review






Spolupráce, MRs, Code Review



stack application



Overview 0 Commits 4 Pipelines 7 Changes 3

 Request to merge `testmr`  into `master`

Open in Web IDE Check out branch  ▾




 Detached merge request pipeline #8289 passed for 5459c5bc 

 Approve Approval is optional 

 Merge ☐ Delete source branch ☐ Squash commits 

> 4 commits and 1 merge commit will be added to master. [Modify merge commit](#)

You can merge this merge request manually using the [command line](#)

 0  0 

Oldest first ▾ Show all activity ▾




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

Dynamické prostředí





- Z jedné zdrojové kódu můžeme pustit více prostředí
- Prostedí mohou být různá nebo identická
- Prostedí můžeme jednoduše dynamicky zapínat a vypínat podle potřeby






Dynamické prostředí









 nicktech  Workspaces Modules Settings Documentation | Status 

Workspaces 18 total [+ New Workspace](#)

All (18)  Success (12)  Error (1)  Needs Attention (1)  Running (0)

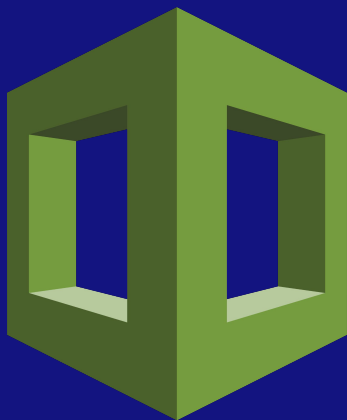
Search by name 

WORKSPACE NAME	RUN STATUS	LATEST CHANGE	RUN	REPO
exceed-limit	 APPLIED	5 months ago	run-B8Ac	NICKF/terraform-minimum
filetest-dev	 ERRORED	3 months ago	run-SLSz	nfagerlund/terraform-filetest
migrated-default	 PLANNED	5 months ago	run-BVyj	nfagerlund/terraform-minimum
migrated-first	 PLANNED	5 months ago	run-A2sp	nfagerlund/terraform-minimum
migrated-second	 PLANNED	5 months ago	run-KqNV	nfagerlund/terraform-minimum
migrated-solo	 APPLIED	5 months ago	run-1RkX	NICKF/terraform-minimum
migrated-solo2	 PLANNED	5 months ago	run-Rih7	nfagerlund/terraform-minimum
migrate-first-2	 NEEDS CONFIRMATION	3 months ago	run-hR57	nfagerlund/terraform-minimum

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





```
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  
}
```

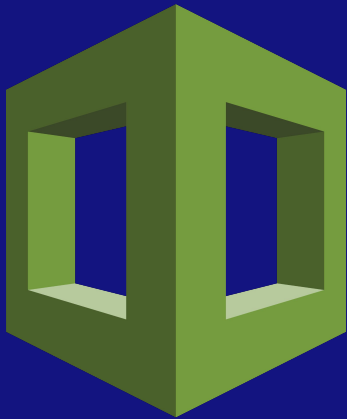
Vlastnosti Terraformu

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



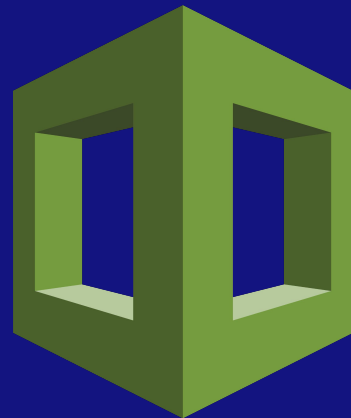
Terraform a ostatní nástroje

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



Cloudformation, AzureRM, ...

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

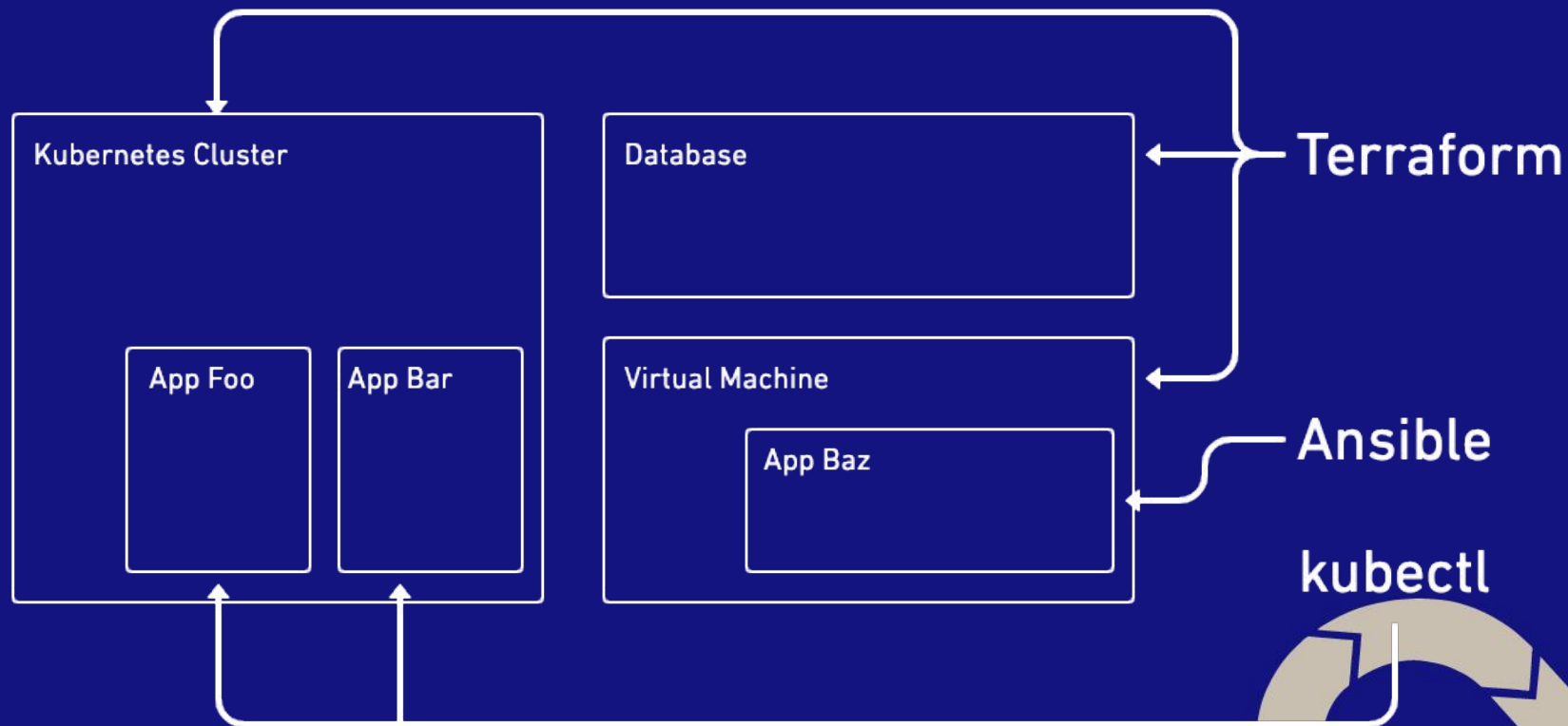


Ansible, Puppet, Chef, ...

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



Terraform, Ansible & Application Deployment



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

stack application

Overview 0 Commits 4 Pipelines 7 Changes 3

 Request to merge [testmr](#)  into [master](#)

 Detached merge request pipeline [#8289](#) passed for [5459c5bc](#)

  [Approve](#) Approval is optional 

 [Merge](#) ☐ Delete source branch ☐ Squash commits 

> **4 commits** and **1 merge commit** will be added to master. [Mod](#)

You can merge this merge request manually using the [command](#)



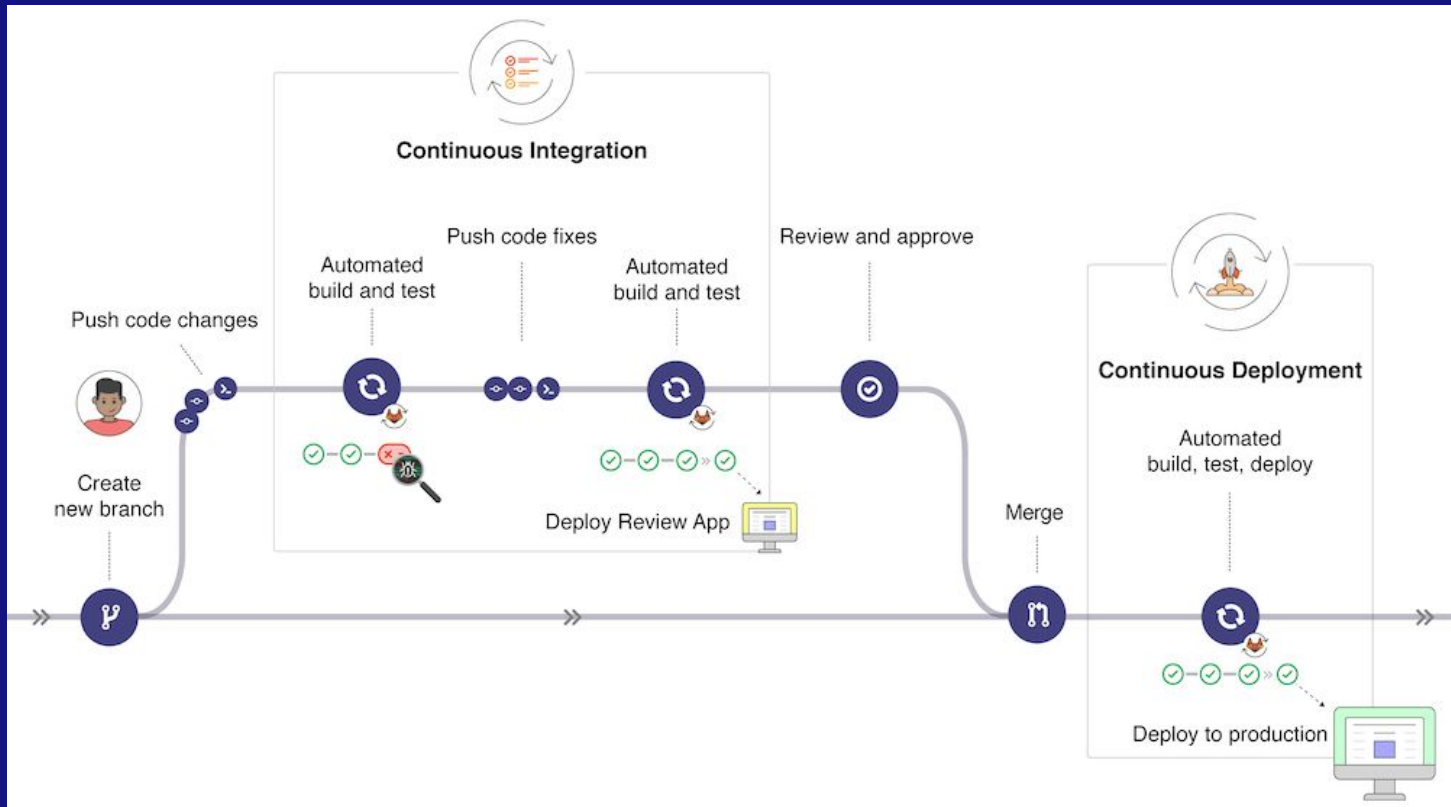
0



0



Gitlab CI + Terraform Workflow



Alternativy ke Gitlab CI

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



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



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





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


Další výhody Terraformu



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



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

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



Slides

sika.link/slides

What's next?

sika.link/next

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

