

Beskar Cloud: GitOps-Based OpenStack on Kubernetes

Klára Moravcová
Cloud Engineer at **CESNET**

7.11.2023, LinuxDays 2023, Praha

Proč řešíme cloudy?

Metacentrum (MetaVO)

- projekt pro podporu vědy a výzkumu v ČR
- provoz služeb nabízející výpočetní výkon
 - Grid (PBS)
 - MetaCloud
- pro všechny akademické pracovníky, zaměstnance a studenty vědeckovýzkumných institucí v České republice
- používání MetaCentra je zdarma, podmínkou členství je souhlas s pravidly, uvádění poděkování v publikacích a dodání výroční zprávy



- **Openstack** - open-source platforma pro cloud computing
 - Implementace z roku 2016 (puppet-kolla)
- Public cloud pro národní výzkumnou infrastrukturu
 - 600 uživatelských projektů “free tier”
 - 200 projektů zabývajících se výzkumem
 - 50+ mezinárodních (přes EGI a ELIXIR)
- 300 HV, 10K CPU, 300TB RAM, 80 GPU
- Podpora pro HPC
 - velké flavors (až 128 CPU), GPUs (NVIDIA A40) a rychlé úložiště (local NVMEs)



Proč nové řešení?

- Konec životnosti stávajícího řešení
- Vlastní custom řešení (puppet-kolla) - složité na správu a další vývoj
- Chtěli jsme
 - zlepšit odolnost a provozovatelnost
 - mít možnost snadnějšího upgradu
 - stavět/provozovat **více instancí openstacku** - Cloud as a service
 - snížit náklady na vývoj a provoz
 - poladit dřívější rozhodnutí v cloudu (jmenná konvence flavoru, přidělování veřejných IP adres, MTU,..)

Co s tím dál? Jak by měl vypadat nový openstack?



Spojení s TAIKUN Cloud

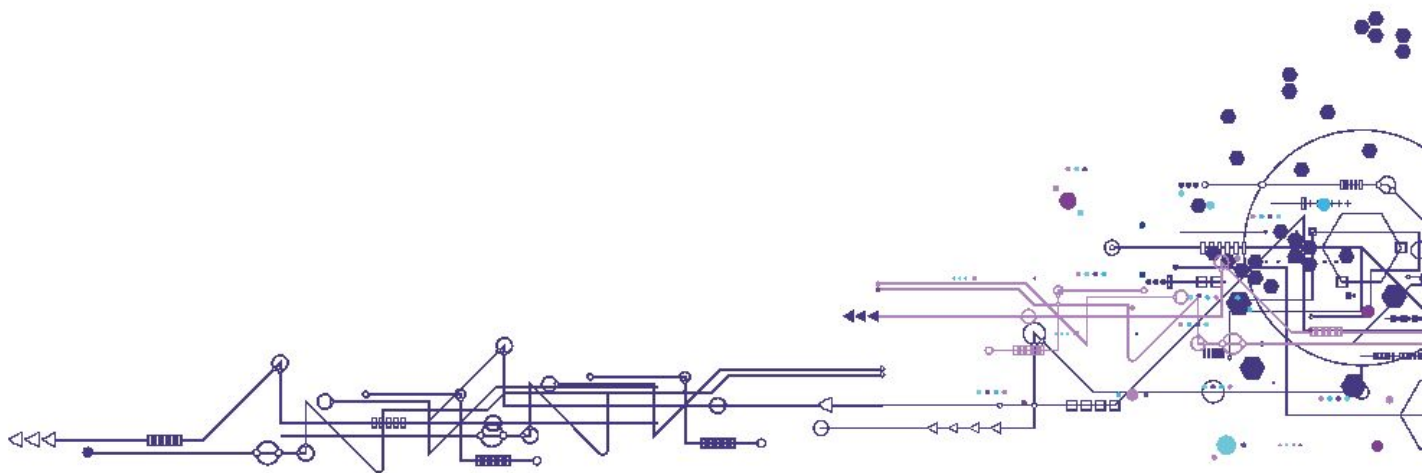


- Zeloženo v 2018 v Praze
- Tým 30 lidí
- Produkt Taikun - SaaS DevOps nástroj na management Kubernetes clusterů
- Provoz on-premise openstack u sebe i u zákazníků
- Zákazníci z oblasti telco, bankovníctví and Enterprise customers





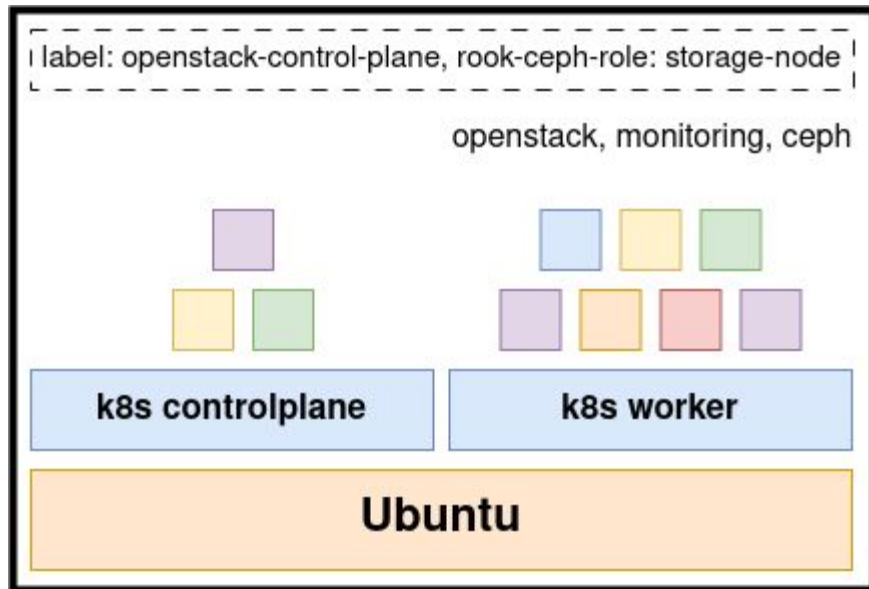
Beskar Cloud



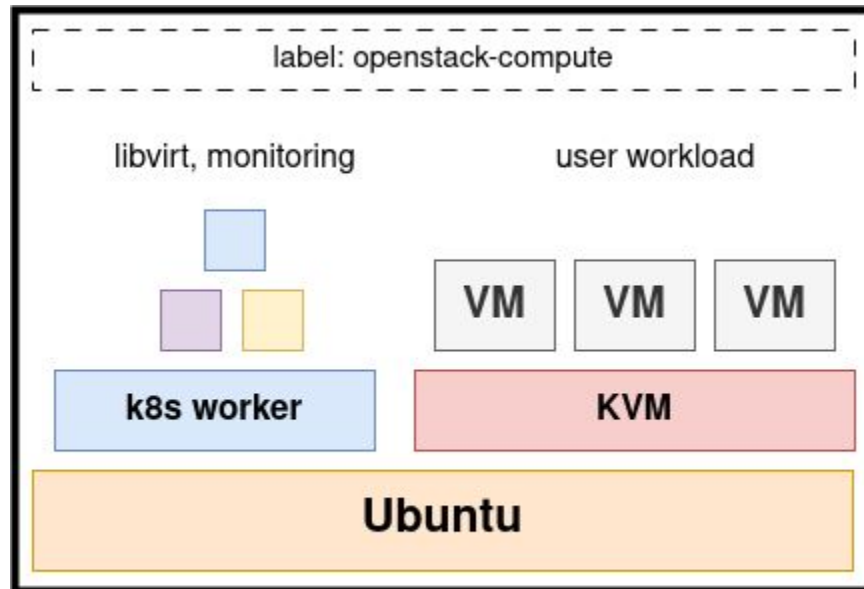
- **Openstack distribuce nad Kubernetes**
 - Cluster řešení pro orchestraci openstack kontejnerů
- Využití **open-source projektů** (minimum vlastního vývoje)
 - MAAS, Ubuntu OS
 - Ansible (infra-config)
 - Kubernetes (Kubespray)
 - Openstack-helm a openstack-helm-infra
 - FluxCD
 - Prometheus, Grafana,..
 - CEPH storage
- **Automatizace** (IaC, GitOps)
- Sdílení provozních zkušeností přes komunitu (<https://github.com/beskar-cloud/>)
 - Kód - fluxcd manifest, values pro kubespray, custom helm charty, infra-config
 - Knowledgebase
 - Pravidelné cally
 - Komunikační kanál přes discord (WIP)



Architektura



OpenStack controlplane node

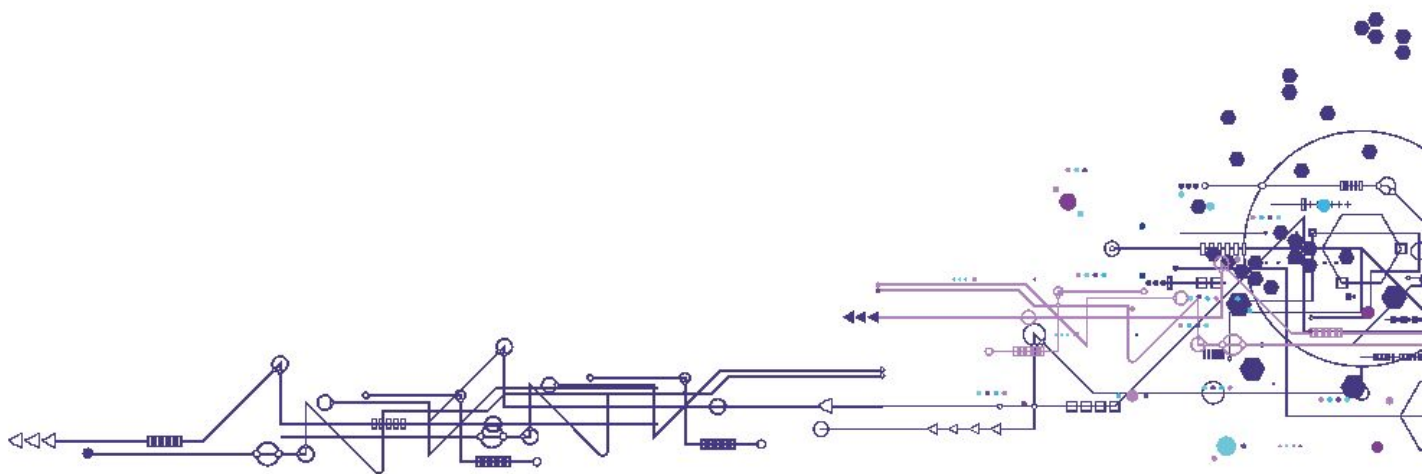


OpenStack compute node





Instalace a management



Hardware a operační system



- **MAAS** - Debian/Ubuntu
 - Instalace OS na HV
 - Počáteční síťová konfigurace
 - Přizpůsobení deploymentu přes cloud-init
 - Není součástí distribuce
- **Infra-config Ansible** kongurace Ubuntu
 - Úklid po MAAS instalaci
 - Základní konfigurace OS
 - Ssh kklíče, síťování, balíčky ...
 - Příprava na libvirt VMs, kubespray



MAAS

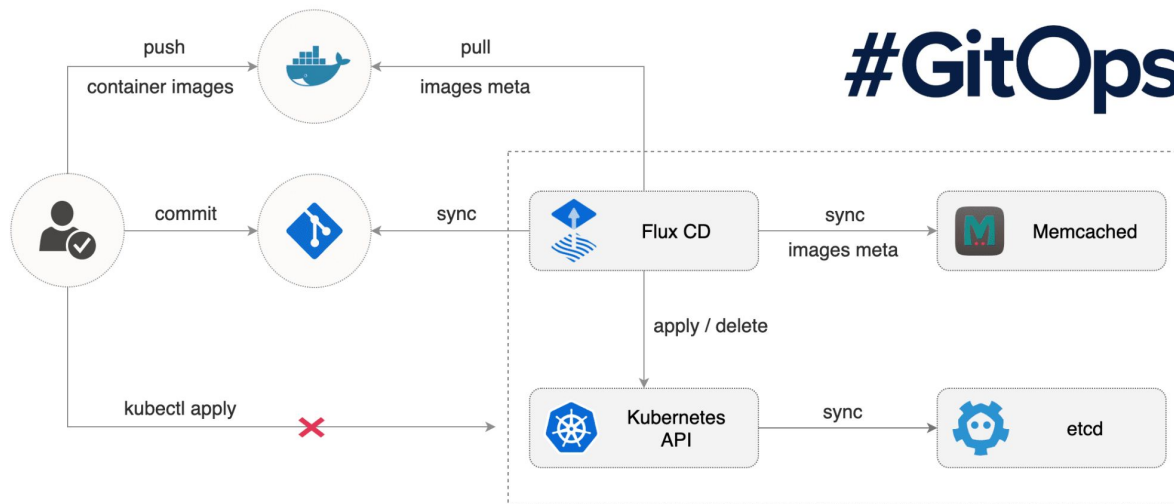


ANSIBLE



Kubernetes + HELM + Flux CD

- **Kubespray** (ansible vanilla kubernetes)
 - Cluster dedikovaný pouze pro openstack
- Deployment openstack a dalších aplikací přes **Helm (openstack-helm)** a **Flux CD**
- **Gitlab** jako jediný zdroj pravdy
 - Deklarativní popis infrastruktury



downstream ▾

ceph-openstack-lma / apps /

+ ▾

Lock

History

Find file

Name	Last commit
..	
📁 base	remove bidirectional mount from openstack nova
📁 freznicek-cluster-10a	feat: move namespace outside from infrastructure ks close to apps definition
📁 freznicek-cluster-10b	feat: move namespace outside from infrastructure ks close to apps definition
📁 prod-brno	refactor: drop nova in custom-helm-charts in favor of standard openstack-helm one
📁 prod-ostrava	refactor: revert API endpoint to oauth20



downstream ▾

ceph-openstack-lma / apps / prod-ostrava / 03-openstack / 03-openstack.base / + ▾

Lock



















History

Find file

Edit ▾

↓ ▾

Clone ▾

Name	Last commit	Last update
..		
 00-common-configmap.yaml	refactor: rename cinder backend and re-enable	3 months ago
 00-common-encryptedsecret.yaml	#1097 introducing mariadb-backup	2 months ago
 00-namespace.yaml	feat: move namespace outside from infrastructure ks close to apps definition	3 months ago
 01-ingress-controller.yaml	refactor: yoga upgrade ostack/00-05 components	3 months ago
 02-ceph-cluster-config.yaml	refactor: yoga upgrade ostack/00-05 components	3 months ago
 02-ceph-rgw-users-encryptedsecret.yaml	fix: re-add ostack	5 months ago
 03-mariadb-backup.yaml	#1097 introducing mariadb-backup	2 months ago
 03-mariadb.yaml	refactor: upgrade monitoring/mariadb	3 months ago
 04-memcached.yaml	Update apps/prod-ostrava/03-openstack/03-openstack.base/04-memcache...	3 months ago
 05-rabbitmq.yaml	Update apps/prod-ostrava/03-openstack/03-openstack.base/04-memcache...	3 months ago
 06-keystone-apache-oidc-metadata-encryptedsecret.yaml	fix: re-add ostack	5 months ago
 06-keystone.yaml	refactor: disable keystone httpd debug logging	1 day ago
 07-radosgw-openstack.yaml	add back the glance, radosgw disabled atm, updated to last yoga, specify re...	3 months ago
 08-ceph-client-glance-key-images-rbd-keyring-encryptedse...	fix: re-add ostack	5 months ago
 08-glance.yaml	feat: add empty glance RBAC rules, add cinder policy rules	2 months ago
 09-ceph-client-cinder-backup-rbd-keyring-encryptedsecre...	fix: re-add ostack	5 months ago
 09-ceph-client-cinder-volume-rbd-keyring-encryptedsecre...	fix: re-add ostack	5 months ago
 09-cinder.yaml	refactor: drop unneeded cinder.conf [nova] entries	1 month ago

FRA
CZ

```
1 kind: HelmRelease
2 apiVersion: helm.toolkit.fluxcd.io/v2beta1
3 metadata:
4   name: nova
5   namespace: openstack
6 spec:
7   interval: 5m
8   dependsOn:
9     - name: "cinder"
10     namespace: "openstack"
11   targetNamespace: openstack
12   storageNamespace: openstack
13   chart:
14     spec:
15       chart: nova
16       sourceRef:
17         kind: GitRepository
18         name: openstack-helm
19         namespace: default
20         interval: 1m
21   install:
22     #timeout: 10s
23     disableWait: true
24     #disableWaitForJobs: false
25     #disableHooks: false
26     #disableOpenAPIValidation: false
27   upgrade:
28     #timeout: 10s
29     disableWait: true
30     #disableWaitForJobs: false
31     #disableHooks: false
32     #disableOpenAPIValidation: false
33   values:
34     images:
35       tags:
36         bootstrap: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__openstackhelm__heat:wallaby-ubuntu_focal
37         db_drop: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__openstackhelm__heat:wallaby-ubuntu_focal
38         db_init: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__openstackhelm__heat:wallaby-ubuntu_focal
39         dep_check: 'registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/quay.io__airshipit__kubernetes-entrypoint:v1.0.0'
40         rabbit_init: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__rabbitmq:3.9-management
41         ks_user: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__openstackhelm__heat:wallaby-ubuntu_focal
42         ks_service: registry.gitlab.ics.muni.cz:443/cloud/g2/container-registry/docker.io__openstackhelm__heat:wallaby-ubuntu_focal
```



Kde Beskar beží teď?

e-infra

- IT4I - 25 HV
- Příprava nového clusteru v Brně - následná migrace

TAIKUN

- Privátní cloud - platforma pro Taikun SaaS
- Jeden z největších operátorů v ČR
- TCPPro - cloud pro koncové zákazníky



This is the cloud way!

Přidejte se k nám
<https://github.com/beskar-cloud>



Děkuji za pozornost!

moravcova@cesnet.cz