Beskar Cloud: Status Update

Klara Moravcova <moravcova@cesnet.cz>
& Adrian Rosinec <adrian@muni.cz>
Cloud Engineer at CESNET

1.10.2024, EGI Conference 2024

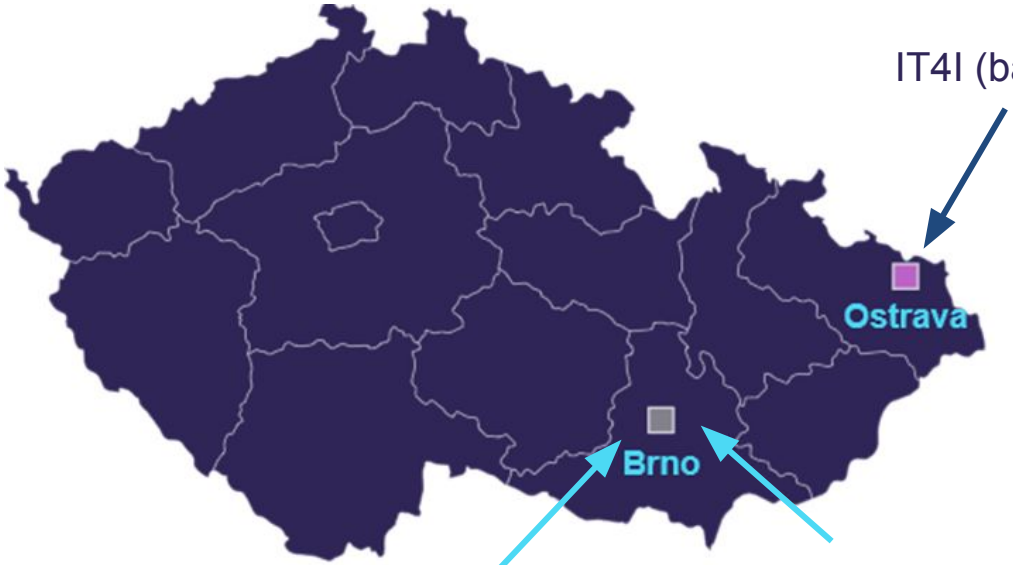
Quick recap

- The **Beskar.cloud OpenStack distribution**
  - **new architecture** with improved deployment process and lifecycle support
  - **GitOps**-based approach with underlying **Kubernetes for better automation and operation**
  - set of **open-source projects**, documented and **prepared to deploy OpenStack** cluster
- Community endeavour
  - **share and unify** experience of **operating and managing** OpenStack clusters
  - Regular bi-weekly community calls
- Documentation and code:
  https://github.com/beskar-cloud/

What is new since the last year

- Management stack - HA Kubernetes, rook ceph, fluxcd
- Full openstack for user workload - Nova, Keystone, Glance, Cinder, Swift, Neutron, Horizon
- Octavia (for loadbalancer as a service)
- Designate + PowerDNS (for DNS as a service)
- Monitoring + runbooks
- penetration tests (CENSET flab)
- Keystone federation - multiple OIDC support, project mappings, application credentials
- **EGI services support** (esaco, accounting, cloudkeeper)
- Openstack entity management - cloud-entities (include **personal projects**)

Beskar implementation



Migration from G1 to G2

- more than 200 group projects
- requires downtime for user workload - collaboration with users needed
- **Organization**
  - pre-migration communication
    - determine migration date
    - agree on the migration parametres
  - tools:
    - email_tool - sending personalised emails to selected users
    - detailed spreadsheet table about status of migration
- **migration itself**
  - create new project in the G2
  - migrate the workload
  - tools:
    - migration_script

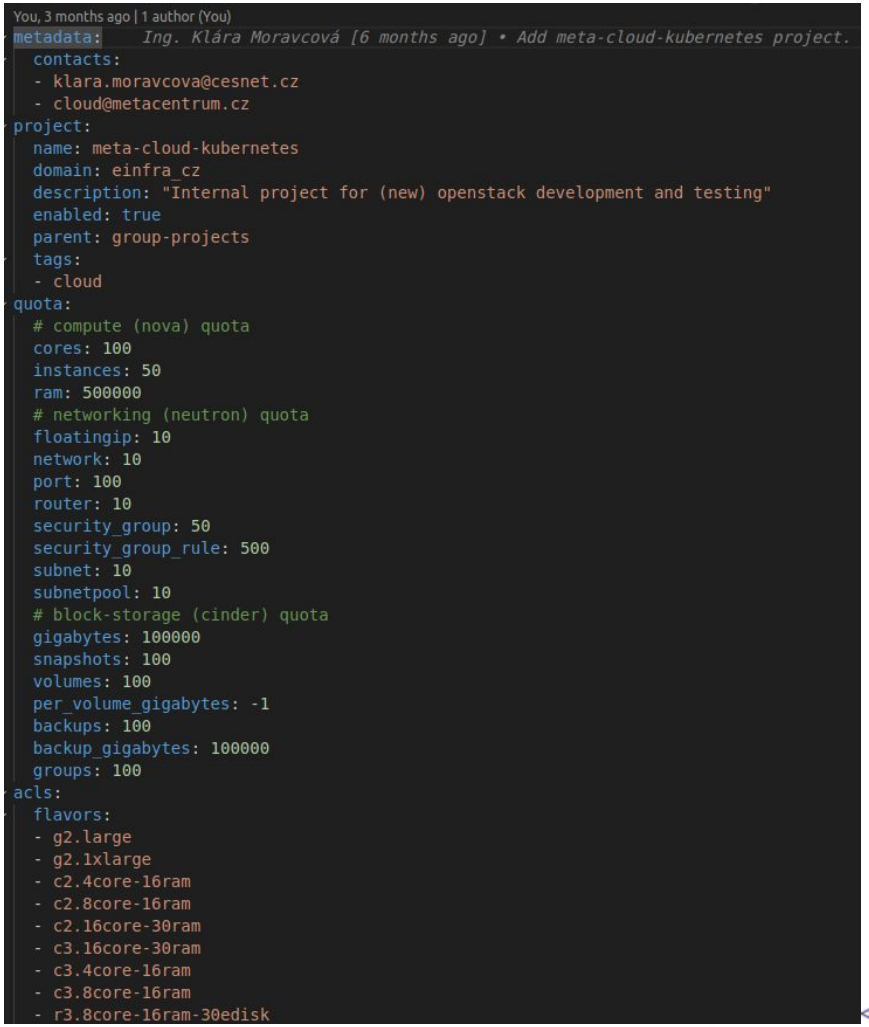
Migration from G1 to G2

Migration script + CI pipeline

- Cloud team or cloud user initiates cloud workload migration
- Migration pipeline is configured and launched
  - Connects to source (G1) and destination (G2) clouds
  - In main loop migrator iterates over source servers and
    - stops the source virtualized server
    - transfers all attached volumes from source (G1) to destination (G2) cloud using low-level ceph RBD operations
    - starts back the source virtualized server
    - starts up the destination server in destination cloud from the cloned volumes (so using mapped flavor, network, volumes, keypair, security-groups)
    - associate FIP address if source VM has one
  - Configured extra volumes are transfered to destination cloud
  - Cloud user validates workload is properly migrated
- Source cloud resources are made inactive for 2-4 weeks by cloud team
- Source cloud resources are archived

Openstack entity management

- openstack entities declaratively stored in git as single point of truth
  - definition of projects with their quotas, network, flavors, images, …
- for openstack administrators
  - observability - what is in git is in openstack database
  - change management
  - auditability - know who changed what
- handled by terraform activated after git push via CI
  - each change triggers update into Openstack
  - no need to have admin (write) roles/credentials on desktop of admins
- lifecycle support
  - automatic deprovisioning resources of projects (based on expiration tag)
- docs


You, 3 months ago | 1 author (You)
metadata: Ing. Klára Moravcová [6 months ago] • Add meta-cloud-kubernetes project.
contacts:
- klara.moravcova@cesnet.cz
- cloud@metacentrum.cz
project:
name: meta-cloud-kubernetes
domain: einfra_cz
description: "Internal project for (new) openstack development and testing"
enabled: true
parent: group-projects
tags:
- cloud
quota:
compute (nova) quota
cores: 100
instances: 50
ram: 500000
networking (neutron) quota
floatingip: 10
network: 10
port: 100
router: 10
security_group: 50
security_group_rule: 500
subnet: 10
subnetpool: 10
block-storage (cinder) quota
gigabytes: 100000
snapshots: 100
volumes: 100
per_volume_gigabytes: -1
backups: 100
backup_gigabytes: 100000
groups: 100
acls:
flavors:
- g2.large
- g2.1xlarge
- c2.4core-16ram
- c2.8core-16ram
- c2.16core-30ram
- c3.16core-30ram
- c3.4core-16ram
- c3.8core-16ram
- r3.8core-16ram-30edisk

Personal project support

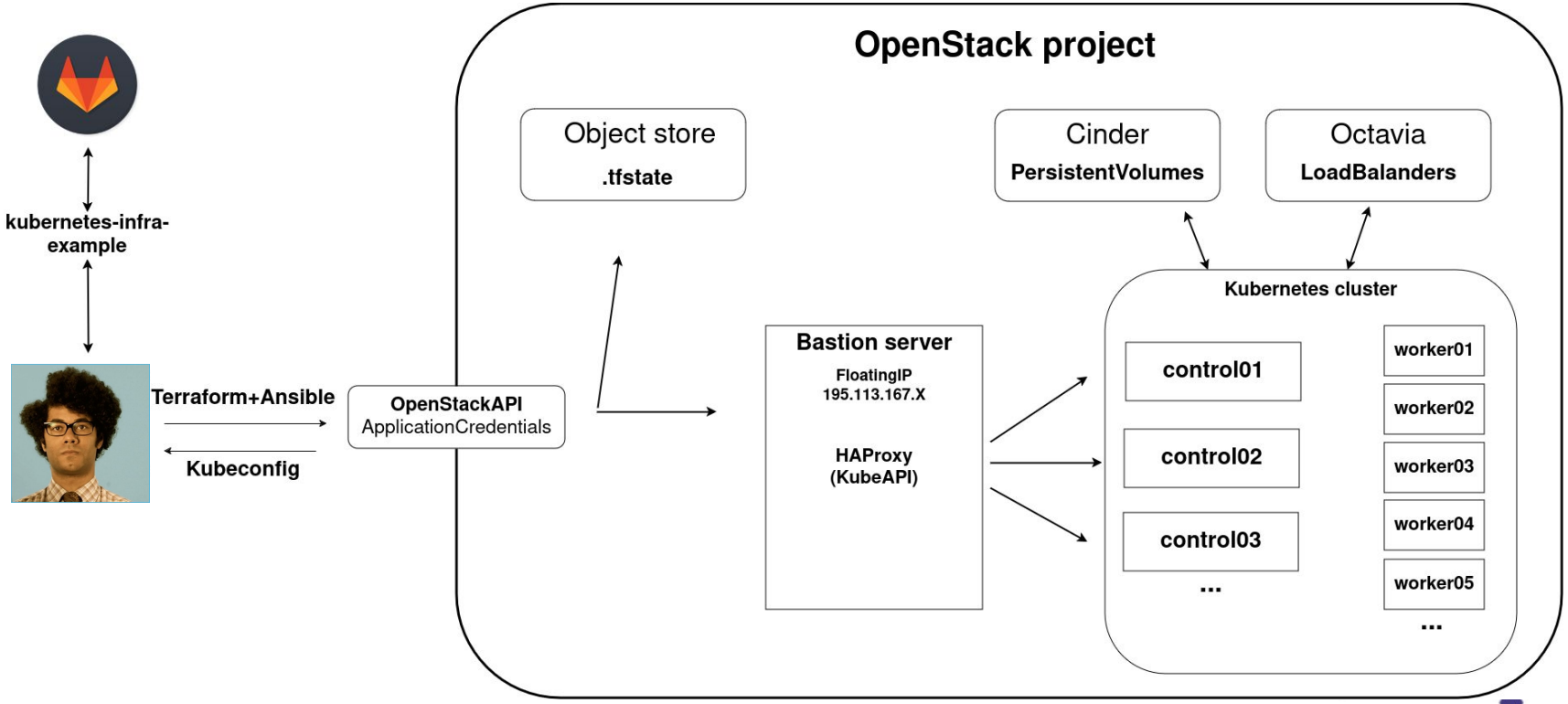
- free-tier OpenStack project (playground)
- limited fixed quota
- using auto-provisioning rules - limited to the specific eduperson entitlement
- automated life-cycle
- VO manager of umbrella project can manage all of the personals project
- in Beskar cloud - via cloud entities
- [knowledgebase]

```
* egi_eu                  # EGI domain
  * personal-projects     # umbrella parent project on top of all personal projects
    * abcd@egi.eu         # personal project granted for EGI identity abcd@egi.eu
    * ...                 # ...
    * dcba@egi.eu         # ...
  * group-projects        # umbrella parent project on top of all group projects
    * ...                 # group projects
```

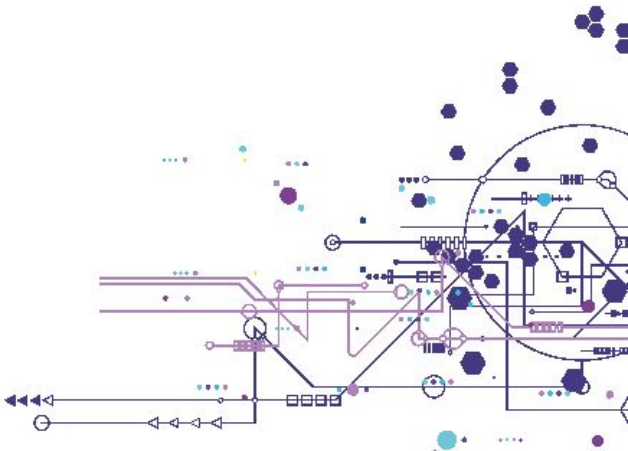
```yaml
metadata:
  contacts:
  - cloud@metacentrum.cz
project:
  name: personal-projects
  domain: egi_eu
  description: "Umbrella project for all personal projects in egi_eu domain"
  enabled: true
  tags:
  - egi                                          # internal cloud statistics tag
  - caso                                         # make sure accounting is enabled
  - children-project-clean-up.enable=true        # project clean-up for children projects & timing
  - children-project-clean-up.pre-shutoff-period-days=160
  - children-project-clean-up.shutoff-period-days=180
  - children-project-clean-up.cleanup-period-days=190
  - project_nested_quota_propagation.enable=true     # ostack quota (*) propagation to children projects
  - egi.AppDB.project_nested_propagation.enable=true # AppDB appliances propagation to children projects
quota: # (*)
  instances: 15
acls: {}
```

Kubernetes as a service (unmanaged)

- service on top of Openstack
- Terraform + Ansible (Kubespray)
- binded to **openstack api**
  - application credentials
  - .tfstate in S3 (swift) bucket
  - dynamic volume provisioning (PVC in Kubernetes)
  - Service type loadbalancer via Octavia


kubernetes-infra-example
Terraform+Ansible
Kubeconfig
OpenStackAPI
ApplicationCredentials
OpenStack project
Object store
.tfstate
Cinder
PersistentVolumes
Octavia
LoadBalanders
Bastion server
FloatingIP
195.113.167.X
HAProxy
(KubeAPI)
Kubernetes cluster
control01
control02
control03
...
worker01
worker02
worker03
worker04
worker05
...

Thank you for the attention!



cesnet

MUNI CERIT-SC

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | IT4INNOVATIONS NÁRODNÍ SUPERPOČÍTAČOVÉ CENTRUM