

Kubernetes v e-INFRA CZ

Operované CERIT-SC

Co a k čemu jsou Kubernetes?

- Co jsou Kubernetes?
 - „Dirigent“ pro kontejnery
 - Automatizuje běh a správu Docker kontejnerů
- K čemu jsou Kubernetes?
 - Jednoduché spouštění Docker kontejnerů
 - Bez nutnosti se starat o zbytek komponent (OS, Docker)
 - Snadná integrace do infrastruktury
 - Napojení na úložiště, certifikáty, DNS

Pro koho a jak přístupné jsou Kubernetes?

- Pro koho?
 - Pro všechny 😎
 - Služba v rámci e-INFRA CZ a MetaCentra
 - Pro použití stejná pravidla, zejména platný účet v MetaCentru
- Jak přístupné?
 - Webové rozhraní: rancher.cloud.e-infra.cz
 - API: `kubectl`, `helm`
 - Bez instalace vlastního clusteru – rovnou připravené prostředí

Existující Instance

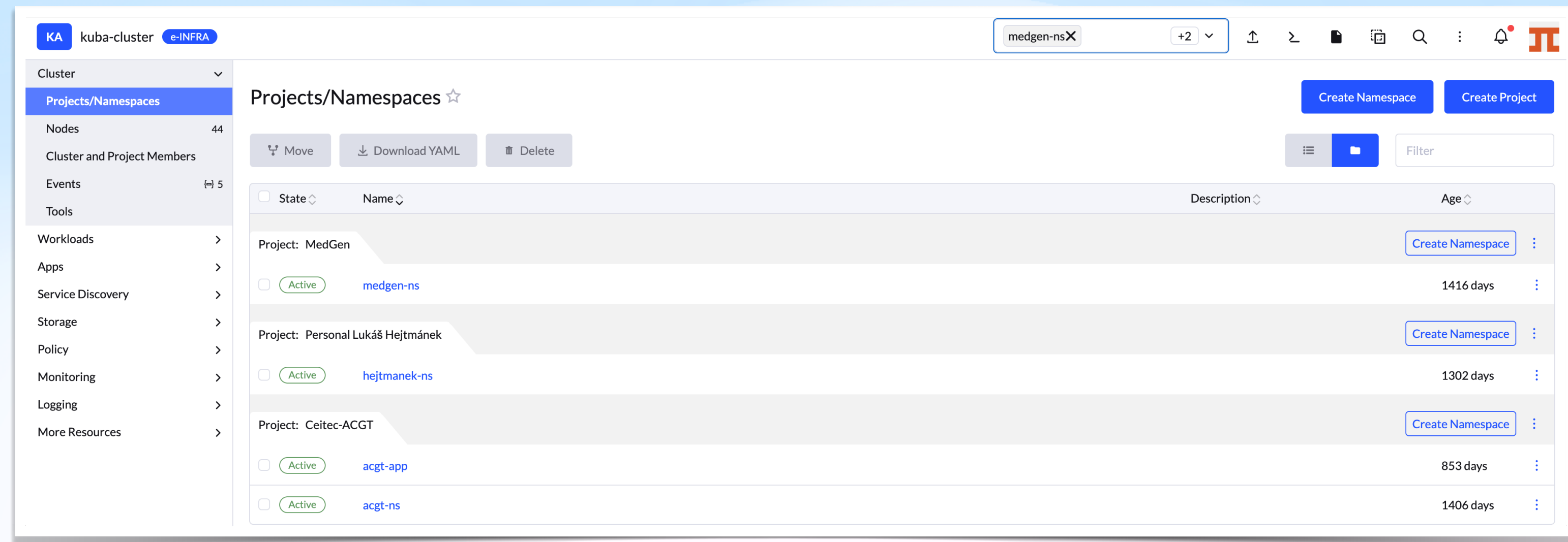
- Public Cluster (kuba-cluster)
 - ~3000 CPU jader, 30 TB paměti, 41 GPU karet, 1.2PB flash úložiště
 - Otevřený pro obecné použití
- Sensitive Cloud (kubas-cluster)
 - ~1000 CPU jader, 13 TB paměti, 20 GPU karet, 4PB úložiště
 - NVIDIA DGX B200
 - Přístup pouze přes VPN (pro citlivá data)
- NRP Kubernetes
 - Vznikající platforma
 - Napojená primárně na úložiště NRP
- Společné rysy
 - Stejná architektura → jednotný způsob použití
 - Rozdíly pouze ve výkonu a zabezpečení



NVIDIA DGX B200

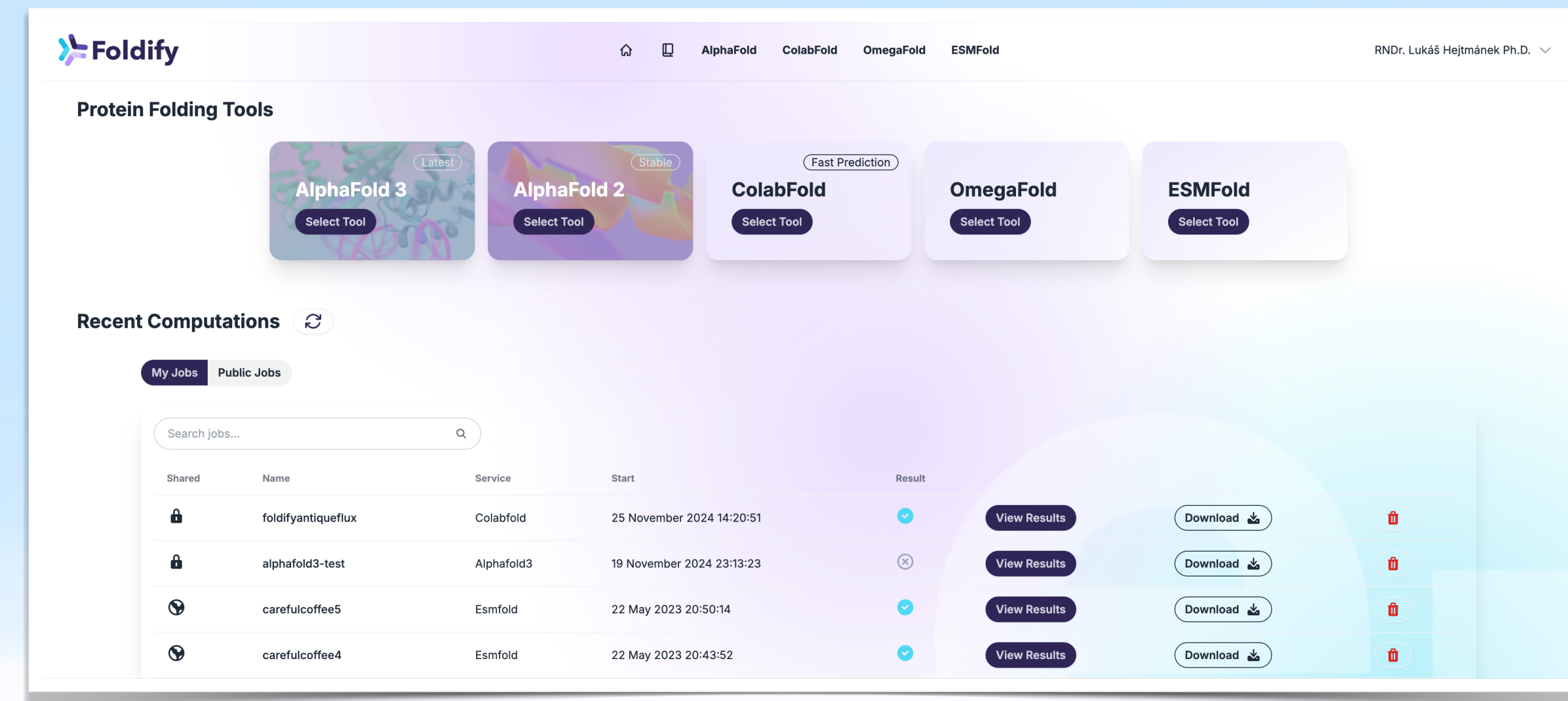
Přístup a Zdroje

- kuba-cluster
 -  Personal projekt (automaticky pro každého)
 - 20–32 CPU, 40–64 GB RAM
 - Neomezený disk, přístup ke GPU
 -  Skupinový projekt
 - Na žádost, vyšší kapacity
- kuba-cluster a NRP
 - Pouze skupinové projekty
 - Kapacita dojednána individuálně
- Jak získat projekt?
 - Připravuje se webové rozhraní
 - Do té doby: e-mail na k8s@cerit-sc.cz



Způsoby Použití Kubernetes

- Hotové služby běžící na Kubernetes
 - Foldify → foldify.cloud.e-infra.cz
 - Harbor → hub.cerit.io
 - JupyterHub → hub.cloud.e-infra.cz
 - Cryosparc
 - AI nástroje (následující přednáška)
- Rancher UI (nejjednodušší)
 - Webové rozhraní
 - Předpřipravené aplikace: RStudio, Matlab, Ansys, Code-Server, Blender
 - Další aplikace na žádost
- API (flexibilní)
 - Přímé: `kubectl`, `helm`
 - Nepřímé: workflow systémy (např. Nextflow)
- Operátory (zjednodušují konkrétní operace)
 - CloudNativePG, MinIO, Logging



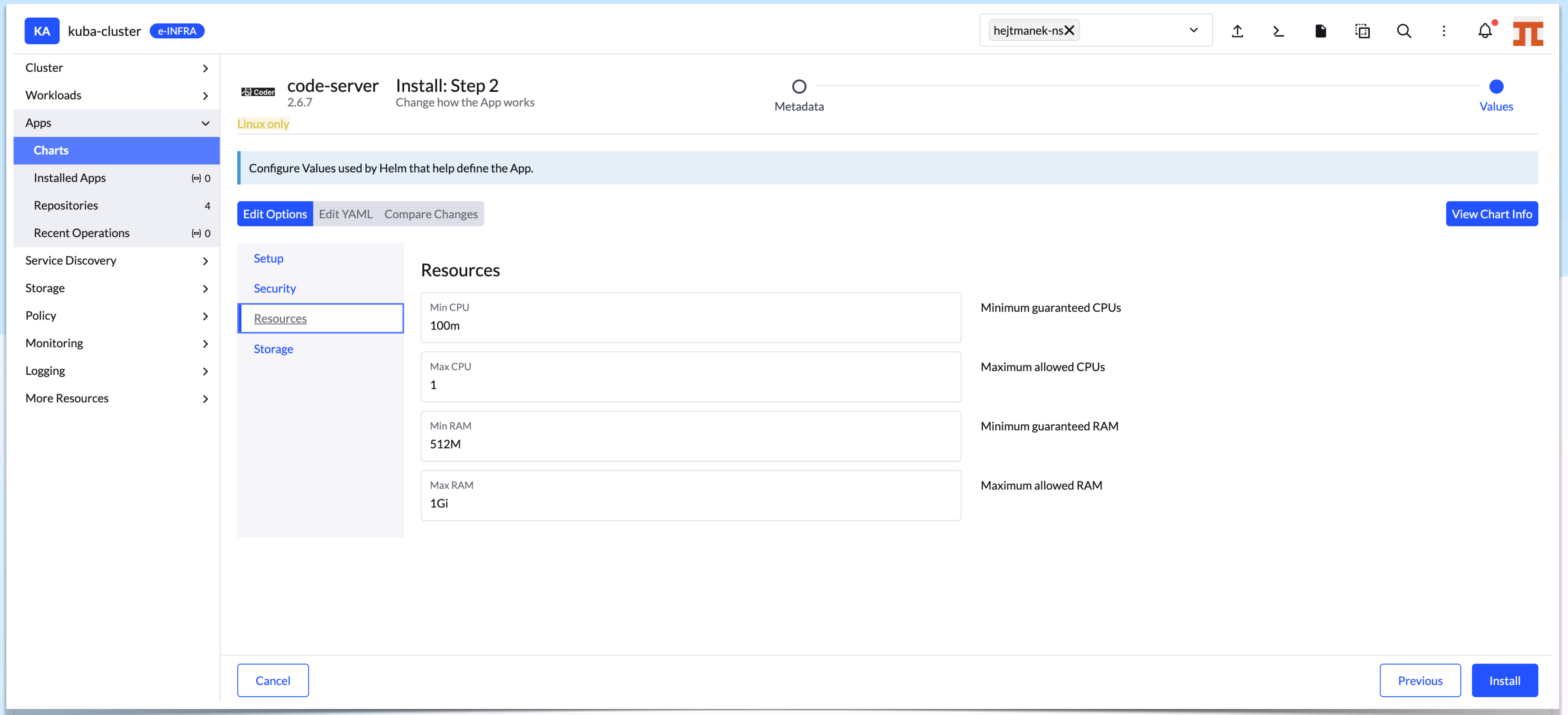
Hotové služby v Kubernetes

- Foldify
 - Webové UI pro Alphafold / Colabfold / Omegafold / ESMfold
 - Podpora dávkových úloh (lze zadat sérii vstupů)
 - (V přípravě) ukládání výsledků do S3
- Harbor
 - Docker registry provozovaná na Kubernetes
 - Transparentní zálohování na CESNETu
 - Soukromé repozitáře bez složité konfigurace

Hotové služby v Kubernetes

- JupyterHub
 - Personalizované prostředí nejen pro výuku, kurzy a školení
 - (V přípravě) nové uživatelské rozhraní
 - Integrace s AI nástroji
- CryoSPARC
 - Specializovaný software pro zpracování dat z kryo-EM
 - Provozováno jako instance na žádost pro vědecké skupiny
 - Spouští se po domluvě administrativou

Rancher UI



API

```
anubis: /tmp/helm $ helm install blender -n hejtmanek-ns . -f valuesprivate.yaml
NAME: blender
LAST DEPLOYED: Tue Sep 30 21:44:52 2025
NAMESPACE: hejtmanek-ns
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: blender
CHART VERSION: 1.1
APP VERSION: 4.2.3

** Please be patient while the chart is being deployed **
Navigate browser to: https://blender-hejtmanek-ns.dyn.cloud.e-infra.cz
anubis: /tmp/helm $ █
```

```
anubis: /tmp/helm $ kubectl get pods -n hejtmanek-ns
```

NAME	READY	STATUS	RESTARTS	AGE
blender-0	3/3	Running	0	93s

```
anubis: /tmp/helm $ helm list -n hejtmanek-ns
```

NAME	NAMESPACE	REVISION	UPDATED	STATUS	CHART	APP VERSION
blender	hejtmanek-ns	1	2025-09-30 21:44:52.000849 +0200 CEST	deplaved	blender-1.1	4.2.3

```
anubis: /tmp/helm $ helm uninstall blender -n hejtmanek-ns
release "blender" uninstalled
anubis: /tmp/helm $ kubectl get pods -n hejtmanek-ns
No resources found in hejtmanek-ns namespace.
```

```
anubis: /tmp/helm $ kubectl logs blender-0 -n hejtmanek-ns
Defaulted container "desktop" out of: desktop, pulseaudio, web
mkdir: cannot create directory '/run/dbus': File exists
Updating xorg.conf with NVIDIA device BusId PCI:163:00:00
Waiting for X socket
_XSERVTransmkdir: ERROR: euid != 0,directory /tmp/.X11-unix will not be created.

X.Org X Server 1.21.1.11
X Protocol Version 11, Revision 0
Current Operating System: Linux blender-0 6.14.0-28-generic #28~24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Fri Jul 25 10:47:01 UTC 2 x86_64
Kernel command line: BOOT_IMAGE=/boot/vmlinuz-6.14.0-28-generic root=UUID=5106db16-6ade-419d-b434-16f91ddd40ce ro console=tty0 console=ttyS0,115200 crashkernel=384M-:512M iommu=pt
xorg-server 2:21.1.12-1ubuntu1.2 (For technical support please see http://www.ubuntu.com/support)
Current version of pixman: 0.42.2
  Before reporting problems, check http://wiki.x.org
  to make sure that you have the latest version.
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/home/ubuntu/.local/share/xorg/Xorg.0.log", Time: Tue Sep 30 21:44:57 2025
(==) Using config directory: "/etc/X11/xorg.conf.d"
(==) Using system config directory "/usr/share/X11/xorg.conf.d"
X socket is ready
Waiting for X11 startup
X11 startup complete
Setting resolution
```

```
anubis: /tmp/helm $ kubectl exec -it blender-0 -n hejtmanek-ns -- /bin/bash
Defaulted container "desktop" out of: desktop, pulseaudio, web
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@blender-0:~$ ps fax
  PID TTY          STAT TIME  COMMAND
 2067 pts/1        Ss   0:00 /bin/bash
 2092 pts/1        R+   0:00 \ ps fax
    1 ?            Ss   0:00 dumb-init /entrypoint.sh
   37 ?            Ss   0:00 /bin/bash /entrypoint.sh
   59 ?            Sl   0:01 \ /usr/lib/xorg/Xorg :0 -noreset +extension MIT-SHM
   68 ?            Sl   0:02 \ python3 /opt/selkies_gstreamer/__main__.py --encoder nvfbch264enc --turn_rest_username webrtc --turn_rest_uri http://coturn-web.turnapi.svc.cluster.local --enable_basic_auth false
   74 ?            Sl   0:00 \ xfce4-session
  120 ?            Sl   0:01 \ xfwm4
  319 ?            Sl   0:00 \ xfsettingsd
  323 ?            Sl   0:00 \ xfce4-panel
```

```
anubis: /tmp/helm $ kubectl cp -n hejtmanek-ns logo.svg blender-0:/tmp/
Defaulted container "desktop" out of: desktop, pulseaudio, web
anubis: /tmp/helm $ kubectl exec -it blender-0 -n hejtmanek-ns -- /bin/bash
Defaulted container "desktop" out of: desktop, pulseaudio, web
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
ubuntu@blender-0:~$ ls /tmp
dbus-IaUY1nFoHf  google-chrome-stable_current_amd64.deb  logo.svg  runtime-ubuntu  ssh-wafVNchhX4PM
ubuntu@blender-0:~$
```

API a Workflows – Nextflow

- Co je Nextflow?
 - Workflow engine pro bioinformatiku, AI/ML a datové pipeline
 - Automatizuje spouštění úloh a podporuje Kubernetes
- Jak funguje v Kubernetes
 - Spuštění příkazem: `nextflow-go`
 - Řídicí kontejner: např. *happy-einstein*
 - Úlohy jako kontejnery `nf-[hash]`
 - Sdílený souborový systém nutný pro všechny kontejnery
 - Řešeno pomocí PVC (PersistentVolumeClaim)
- Konfigurace pro Kubernetes
 - Specifická sekce `k8s` v konfiguraci Nextflow
 - Definuje adresáře, typ zdrojů, limity CPU, PVC

```
nextflow-go run nf-core/sarek -v 'pvc-acgt-beegfs:/mnt' \  
  --input /mnt/GIAB_bench/GIAB_AshkenaziTrio_son.tsv \  
  --genome GRCh38 --tools HaploTypeCaller,VEP,Manta \  
  --annotation_cache --vep_cache /mnt/shared/vep_cache \  
  --igenomes_base /mnt/igenome/
```

```
k8s {  
  launchDir = /storage2/variantbenchmark  
  computeResourceType = 'Job'  
  cpuLimits = true  
  storageMountPath = '/storage2'  
  storageClaimName = 'pvc-shared'  
}
```

Operátory

CloudNativePG

- Operátor pro Postgres SQL databázi
- Umí:
 - spustit a nakonfigurovat DB cluster
 - zajistit replikaci a správu certifikátů (SSL/TLS)
 - volitelně provádět zálohy do S3
- Nasazení:
 - `kubectl create -f cluster.yaml -n hejtmanek-ns`
- Přihlašovací údaje jsou uloženy v **Secret** objektu

```
anubis: /tmp $ kubectl get pods -n hejtmanek-ns
NAME                                READY   STATUS    RESTARTS   AGE
test-cluster-1-initdb-zhhn9        0/1     Init:0/1   0           7s
anubis: /tmp $ kubectl get pods -n hejtmanek-ns
NAME                                READY   STATUS    RESTARTS   AGE
test-cluster-1                      1/1     Running    0           41s
test-cluster-2                      1/1     Running    0           16s
anubis: /tmp $
```

```
apiVersion: postgresql.cnpg.io/v1
kind: Cluster
metadata:
  name: test-cluster
spec:
  instances: 2
  enableSuperuserAccess: true
  imageName: 'cerit.io/cloudnative-pg/postgresql:15.0'
  bootstrap:
    initdb:
      database: mydb
      owner: myowner
  resources:
    limits:
      memory: "4096Mi"
      cpu: 1
  storage:
    size: 10Gi
    storageClass: zfs-csi
```

cluster.yaml

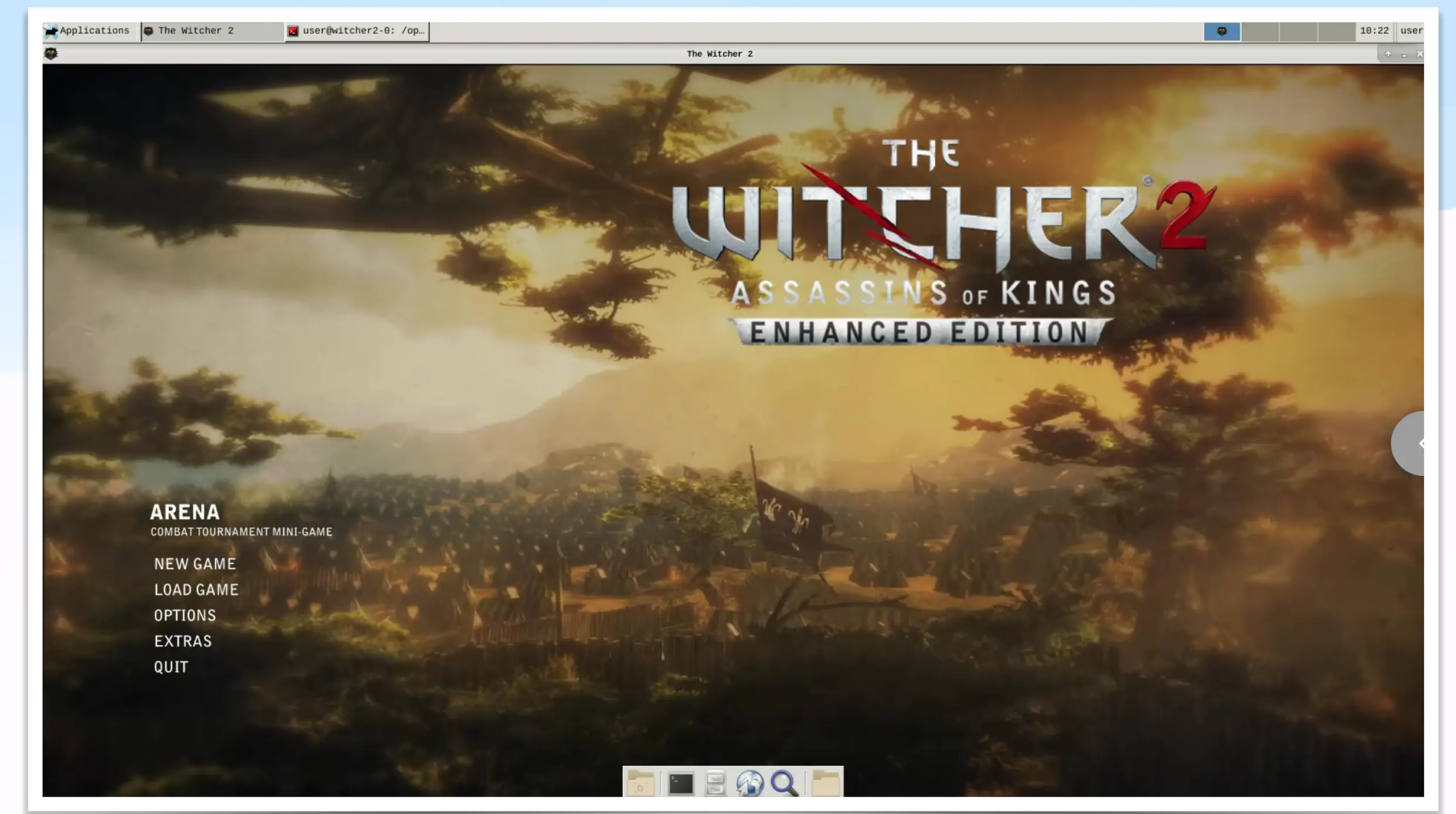
Operátory

MinIO a Logging

- MinIO Operator
 - Spustí a spravuje S3-kompatibilní objektové úložiště (MinIO cluster)
 - Sleduje stav clusteru a zajišťuje jeho dostupnost
 - Umožňuje vytvořit uživatele a bucket
- Logging Operator
 - Usnadňuje konfiguraci sběru logů z kontejnerů
 - Poskytuje možnosti filtrování a směrování logů
 - Ukládání/odesílání do externího agregátoru (Elastic, Loki, apod.)

K čemu to celé je?

- Spouštění Docker kontejnerů bez časových limitů
- Workflow orchestrace (např. Nextflow)
- Kombinace dlouho běžících služeb a výpočetních úloh
- Webové aplikace pro vědce a studenty
 - JupyterHub, CryoSPARC, Foldify ...
- Vzdálené desktopy
 - Včetně funkční 3D akcelerace
- Provoz databází
 - včetně webových frontendů a integrací



Děkuji za pozornost!

k8s@cerit-sc.cz
<https://docs.cerit-sc.cz>
<https://blog.e-infra.cz>