

# Platforma Kubernetes — Úvodní seznámení

Lukáš Hejtmánek, CERIT-SC



**kubernetes**

# Co se dnes dozvíte

- Úvod do Kubernetes
  - Co to je?
  - Jak to funguje?
  - K čemu lze použít?
- Webové aplikace JupyterHub a BinderHub
  - Krátké ukázky použití
- Interaktivní aplikace
  - Ukázky použití grafických aplikací Matlab, Ansys nebo Rstudio
- Ukázka spuštění vlastní aplikace



# Kubernetes



# Kontejnery

- Stále populárnější způsob pouštění aplikací
  - Kontejner = soubor aplikací a jejich závislostí
  - Uživatel již neřeší chybějící knihovny
- Docker kontejnery
  - Nejpoužívanější formát kontejnerů
  - Lze provozovat na vlastním počítači



# Docker Kontejnery

- Sestavení
  - Pomocí Dockerfile
  - Manuálně s využitím docker build
  - Automatizovaně CI/CD
    - runner z gitlabu/githubu
- Ukládání do registry
  - [hub.docker.com](https://hub.docker.com)
  - gitlab nabízí vlastní registry
  - Veřejný nebo autentizovaný přístup



# Kontejnery — Principy

- Běžící kontejner má obvyklou adresářovou strukturu
- Neběží-li pod root uživatelem
  - Nelze do běžícího kontejneru instalovat další systémový SW (knihovny)
  - Lze instalovat do HOME
  - SW lze instalovat předem při přípravě kontejneru
- Zapisovat lze zpravidla do /tmp a HOME
  - Tato data nejsou persistentní, s restartem kontejneru zmizí
- Lze připojit externí disk (adresář)
  - Změny v něm jsou persistentní



# Kubernetes

- Orchestrátor
  - Vyvinul Google v roce 2014
  - Nástroj na správu běžících kontejnerů
- Zajišťuje
  - Stažení docker image
  - Spuštění kontejneru
  - Síťové propojení
  - Zpřístupnění úložiště
  - ...



# Kubernetes — Principy

- Kubernetes jsou organizovány do clusterů
  - V rámci jednoho clusteru existuje control plane a worker uzly
- Cluster
  - Namespace — prostor pro uživatele, může mít kvóty
    - Pod — nejmenší jednotka, obsahuje jeden nebo i více kontejnerů
    - Controller
      - Job — Obsahuje Pod, který běží a skončí
      - Deployment — Obsahuje Pod, který má běžet stále
      - StatefulSet — Obsahuje Pody s garancí pořadí





# Kubernetes — Principy

- Spuštění úlohy
  - Pomocí *manifestu* — popisuje jeden z typů objektu: Pod, Job, Deployment, ...
  - Jsou-li dostupné zdroje, plánovač vybere uzel, kde úloha poběží
  - Na uzlu je stažen kontejner, připojeny případné síťové disky, úloha běží
  - Úloha implicitně nemá walltime
- Úlohu lze sledovat
  - describe — základní info, kde běží, atd.
  - logs — zobrazí standardní výstup úlohy
  - top — zobrazí aktuálně spotřebovávané zdroje — CPU, Memory
- Úloha může být systémem restartována — např. migrací na jiný uzel
  - Uživatel s tímto musí počítat např. implementací checkpoints



# Kubernetes — Běh kontejneru

- Orchestrátor
  - Sleduje běh kontejnerů
  - Restartuje případné spadlé kontejnery
  - Dle specifikace udržuje jejich repliky
- Nezajišťuje
  - Pořadí běhu kontejnerů
    - Neexistuje before/after ok varianta zadání
    - Nutno realizovat přes přídatný workflow manager



# Kubernetes — Zdroje

- Zdroje se specifikují pomocí dvou hodnot
  - Requests
    - Garantovaný limit
    - Zdroje jsou na uzlu rezervovány
  - Limits
    - Nepřekročitelný limit
    - Zdroje mezi Requests a Limits nejsou garantované
- Uzlu zdroje mohou dojít
  - Některé Pody jsou přesunuty jinam



# Kubernetes — Úložiště

- Kubernetes poskytuje celou řadu možností
- V rámci e-INFRA jsou nabízeny tři
  - /tmp — není nutné přímo specifikovat v manifestu, s restartem zmizí obsah
    - Nelze sdílet mezi kontejnery
  - emptyDir — musí se uvést v manifestu, s restartem může zmizet obsah
    - Může být v paměti nebo na lokálním disku
    - emptyDir lze sdílet mezi kontejnery v rámci jednoho manifestu
  - PVC — musí se uvést v manifestu, je persistentní
    - Realizováno většinou jako síťový disk přes NFS, CIFS, ...
    - Lze sdílet mezi kontejnery i přes různé manifesty



# Kubernetes — PVC

- PVC — Persistent Volume Claim
  - Používá se prostřednictvím Storage Class
  - Uživatel si vybírá Storage Class dle potřeb
  - Základní typy
    - ReadWriteOnce — lze připojit pouze k jednomu Podu
    - ReadWriteMany — lze připojit k mnoha Podům
- Storage Class
  - Reprezentuje typ úložiště
  - NFS
  - CIFS
  - SSHFS
  - CEPH RBD



# Kubernetes — Ingress, LoadBalancer

- Podpora vystavování kontejnerů do sítě
  - Síť do Podu je filtrovaná
  - Ingress
  - LoadBalancer
- Ingress
  - Pro webové aplikace na bázi virtualhostu
  - Sdílí IP adresu, rozlišování podle DNS jména kontejneru, pouze HTTP protokol
- LoadBalancer
  - Pro ostatní typy
  - Každý LoadBalancer má vlastní IP



# Kubernetes — Ingress

- Princip
  - Pod vystaví Port
  - Objekt typu Service se napojí na Port Podu
  - Ingress je napojen na Service
  - Propojení lze realizovat přes symbolická jména, např. port pojmenuji HTTP
- TLS
  - Ingress podporuje SSL terminaci
  - Pro zvolené jméno je schopen automaticky zajistit Let's Encrypt certifikát
  - Pro konkrétní doménu zapíše do DNS jméno ([rstudio.dyn.cloud.e-infra.cz](https://rstudio.dyn.cloud.e-infra.cz))



# Kubernetes — LoadBalancer

- Princip stejný jako u Ingress
  - Ingress objekt se vynechá
  - Service objekt je rovnou typu LoadBalancer
  - Lze specifikovat konkrétní IP adresu (je-li volná)
- TLS
  - Neumí zajistit SSL terminaci ani vydat certifikát
- Umí zapsat DNS jméno





# Rancher



# Rancher — Dashboard

- Grafické rozhraní ke Kubernetes
- Umožňuje přímo spravovat a používat kontejnery
- Nabízí předpřipravené aplikace
- Poskytuje API pro ovládání z příkazové řádky
- Mezi cluster a namespace zavádí koncept Projektu
  - Projekt umožňuje nastavení přístupových práv a kvóty
  - Uživatel může být v několika projektech
  - Projekt může obsahovat několik namespaces
  - Projekt není přímo vidět v Kubernetes



# Rancher



Welcome to Rancher



Learn more about the improvements and new capabilities in this version.

[What's new in 2.6](#)

Getting Started



Take a look at the the quick getting started guide. For Cluster Manager users, learn more about where you can find you favorite features in the Dashboard UI. [Learn More](#)

Community Support



[File an Issue](#)

What do you want to see when you log in?



You can change where you land when you login:

- Take me to the home page
- Take me to the area I last visited
- Take me to cluster:

kuba-cluster



Clusters 1

[Import Existing](#)

[Create](#)

State	Name	Provider	Kubernetes Version	CPU	Memory	Pods
Active	kuba-cluster	rke2	v1.21.9+rke2r1	175.3/2026 cores	923 GiB/7.78 TiB	216/2560

Operated by CERIT-SC, ICS MUNI



# Co je k dispozici?

- Každému uživateli je vytvořen Personal projekt
  - Request 20 CPU, 40 GB Memory
  - Limit 32 CPU, 64 GB Memory
- Pro větší zdroje nutno požádat o explicitní projekt
- Lze využít GPU — žádá se jako další zdroj
- Podpora pro MPI úlohy
- Částečná podpora ukládání dat v e-INFRA
- Podpora IPv6



# Existující příklady použití

- Binderhub, Jupyterhub (vč. instancí “na míru”)
- Nextflow, Snakemake
- Farma KNIME desktopů
- Tensorflow aplikace — rozpoznávání buněčné smrti
- EGA — úložiště pro velmi citlivá data
- FN Brno — konverze patologických snímků
- Galaxy portál
- Magic Force Field
- Sequia portál
- Ansys, Matlab, RStudio server



# Praktické ukázky



<https://rancher.cloud.e-infra.cz>

<https://docs.cerit.io>

<https://docs.cerit.io/docs/webinar1.html>

[k8s@ics.muni.cz](mailto:k8s@ics.muni.cz)

