CoPAS

aneb „Pohádka o Popelce“

Tomáš Rebok
Ústav výpočetní techniky
Masarykova univerzita

CopAS historicky (do verze 3.1)

datově-analytické řešení

pro analýzu síťových záchytů

CopAS (do verze 3.1)

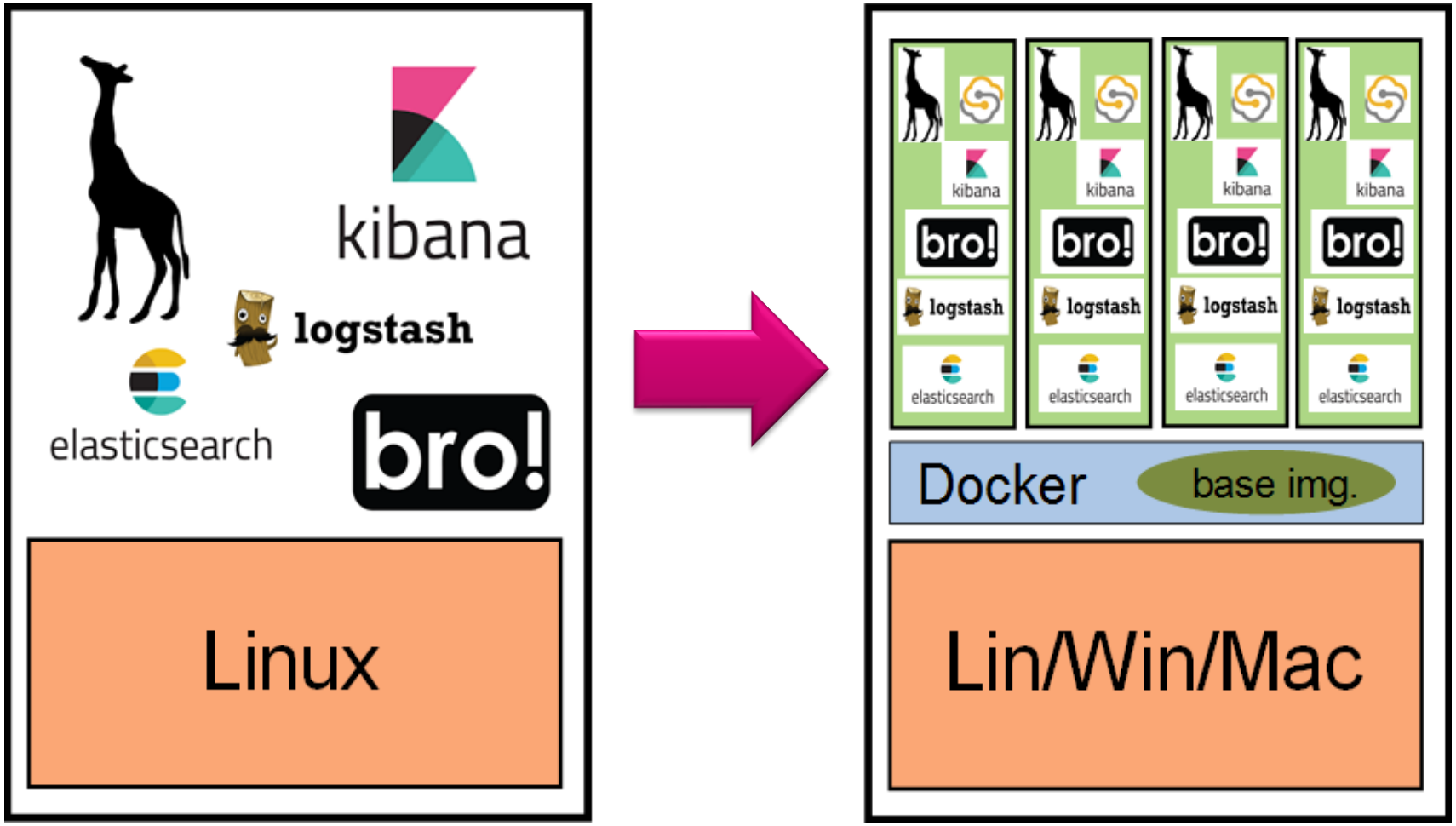
CopAS – *Cops Analytic System*

- vyladěné prostředí analytických řešení ElasticSearch (+ Kibana) a Moloch/Arkime
  - určené pro analýzu síťových záchytů
  - Bro/Zeek, LogStash, ElasticSearch, Kibana a Moloch/Arkime
- + webové GUI (vlastní implementace – Neck)
- + sada předpřipravených dashboardů a vizualizací

- hlavní důraz na uživatelskou přívětivost, snadnost nasazení a používání
  - využití Dockeru pro snadnější nasazení

MUNI

CopAS (do verze 3.1)



MUNI

CopAS – správa kontejnerů (do verze 3.1)

`copas ACTION [container name]`

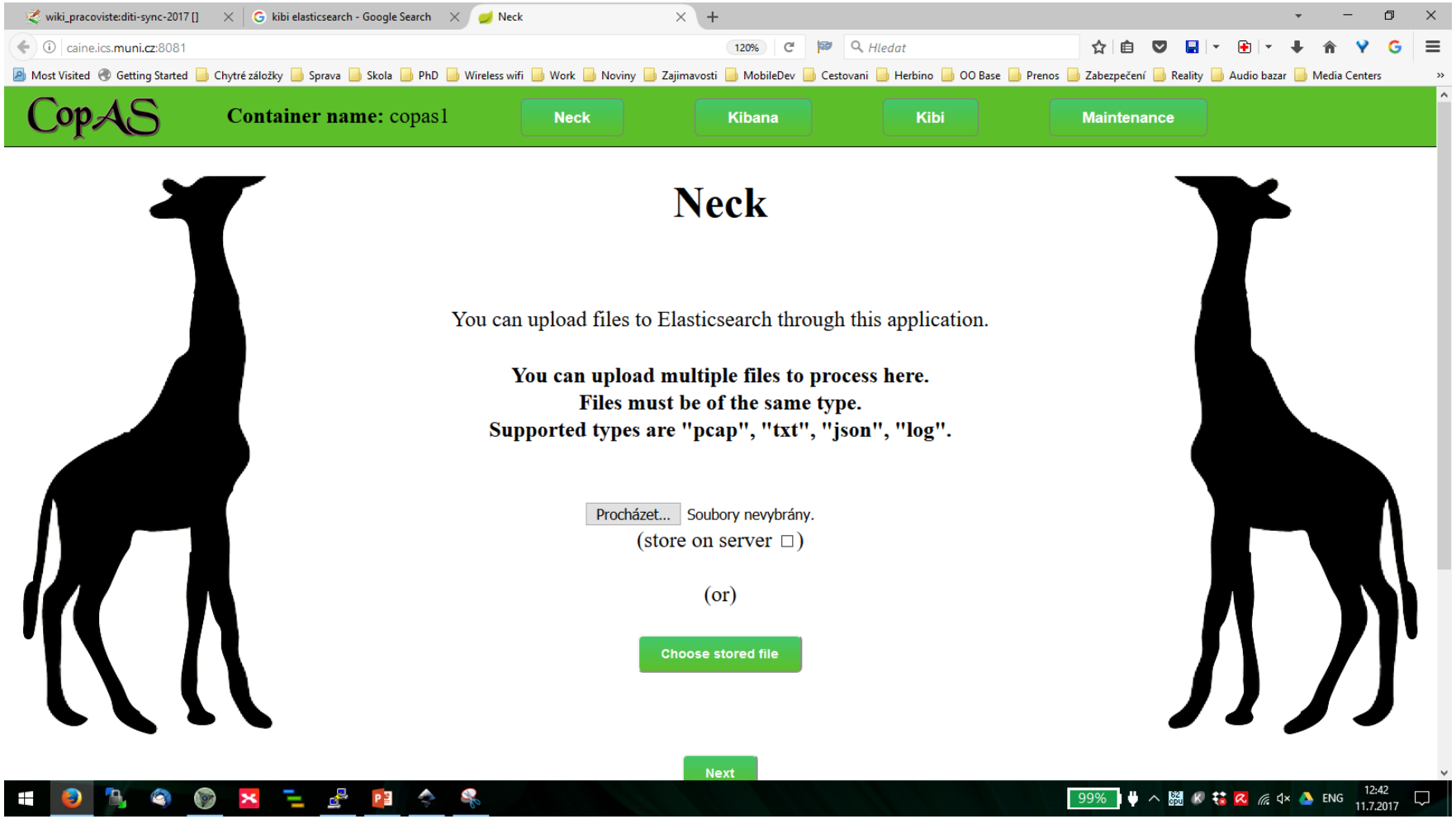
- *nástroj pro správu CopAS kontejnerů*

```
[jeronimo@caine /home/jeronimo]$ copas -h
**************************************************************************
* CopAS (Cops Analytic System) -- a system for data analyses using Elastic stack *
*       Created by Institute of Computer Science, Masaryk University, 2017       *
**************************************************************************

Usage: copas ACTION [container_name]
       Available actions:
          create  ... creates a CopAS container (named 'container_name', if provided)
          start   ... starts a CopAS container (named 'container_name', if provided)
          stop    ... stops a CopAS container (named 'container_name', if provided)
          destroy ... destroys a CopAS container (named 'container_name', if provided)
          info    ... shows information about available CopAS containers
          monitor ... monitors the resource usage of CopAS containers
                      (if -l|--live option provided, shows live resource usage)
          enter   ... enters a CopAS container (named 'container_name', if provided)
          update  ... updates the CopAS base image
                      if a filename is provided, updates from the local image
```

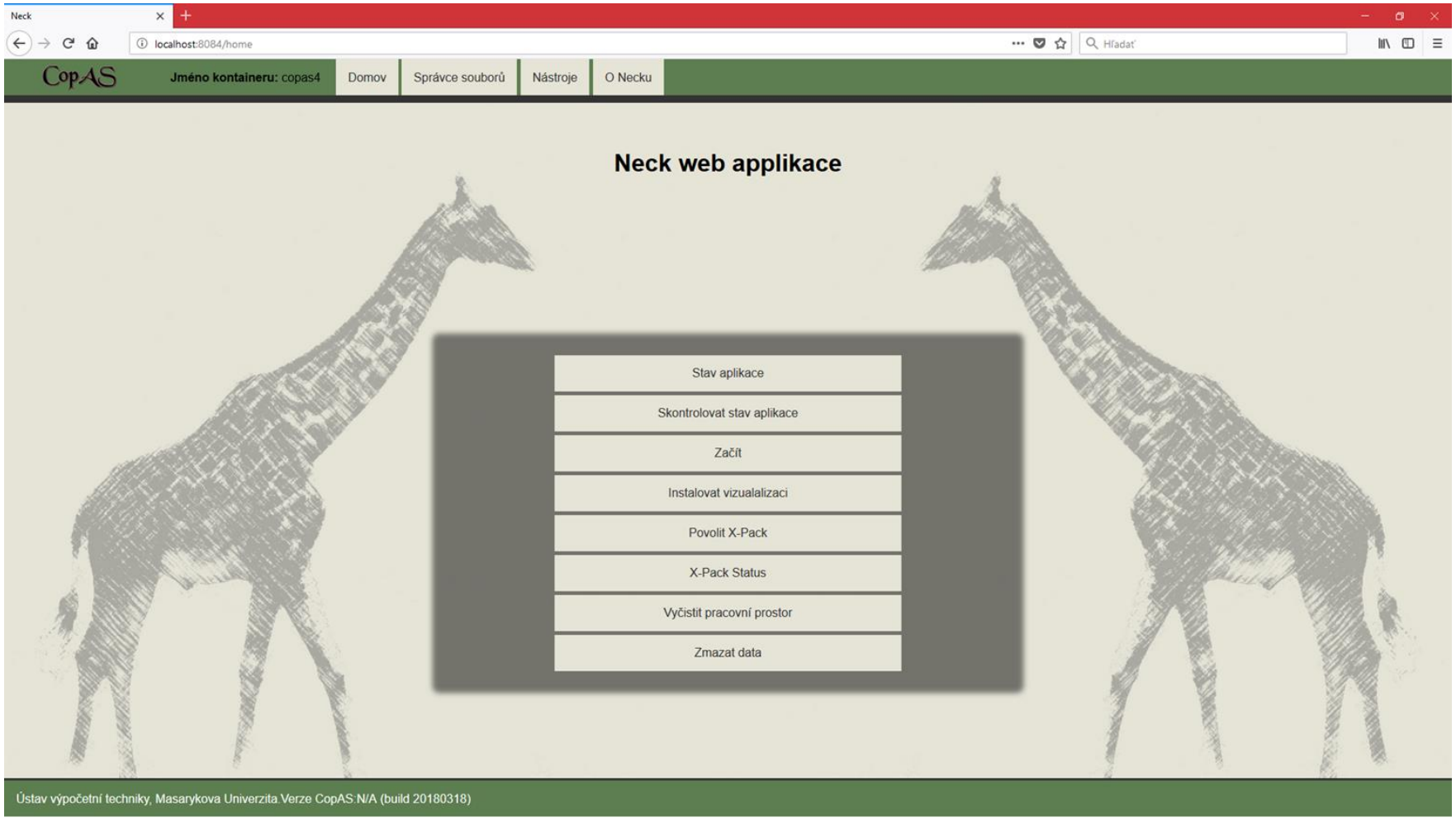

MUNI

CopAS – uživatelské prostředí (verze 1.0)



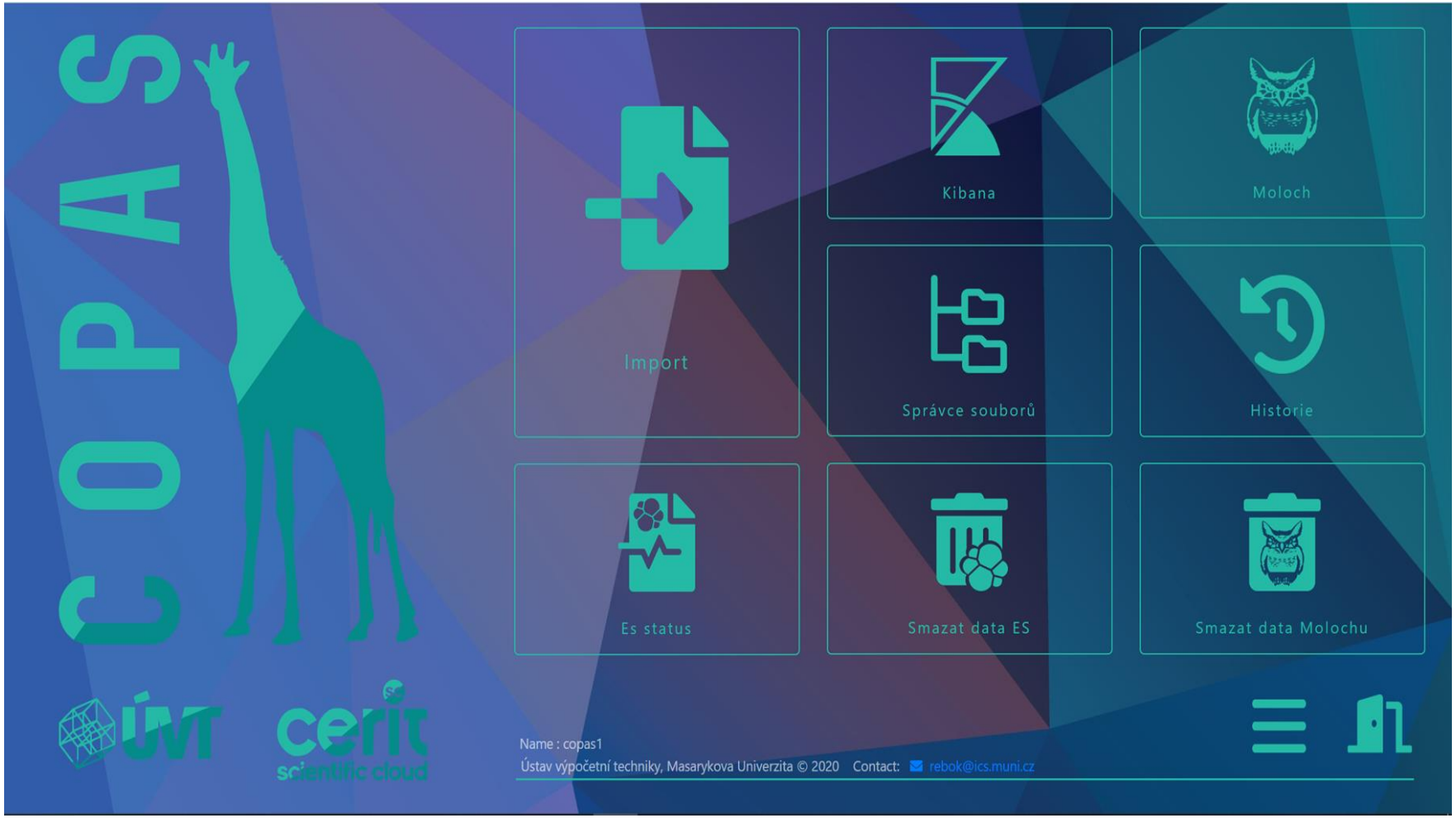
MUNI

CopAS – uživatelské prostředí (verze 2.0)



MUNI

CopAS – uživatelské prostředí (verze 3.1)



MUNI

CoPAS verze 4.0

modulární datově-analytické řešení

CoPAS *(Cop's Personal Analytic System)*

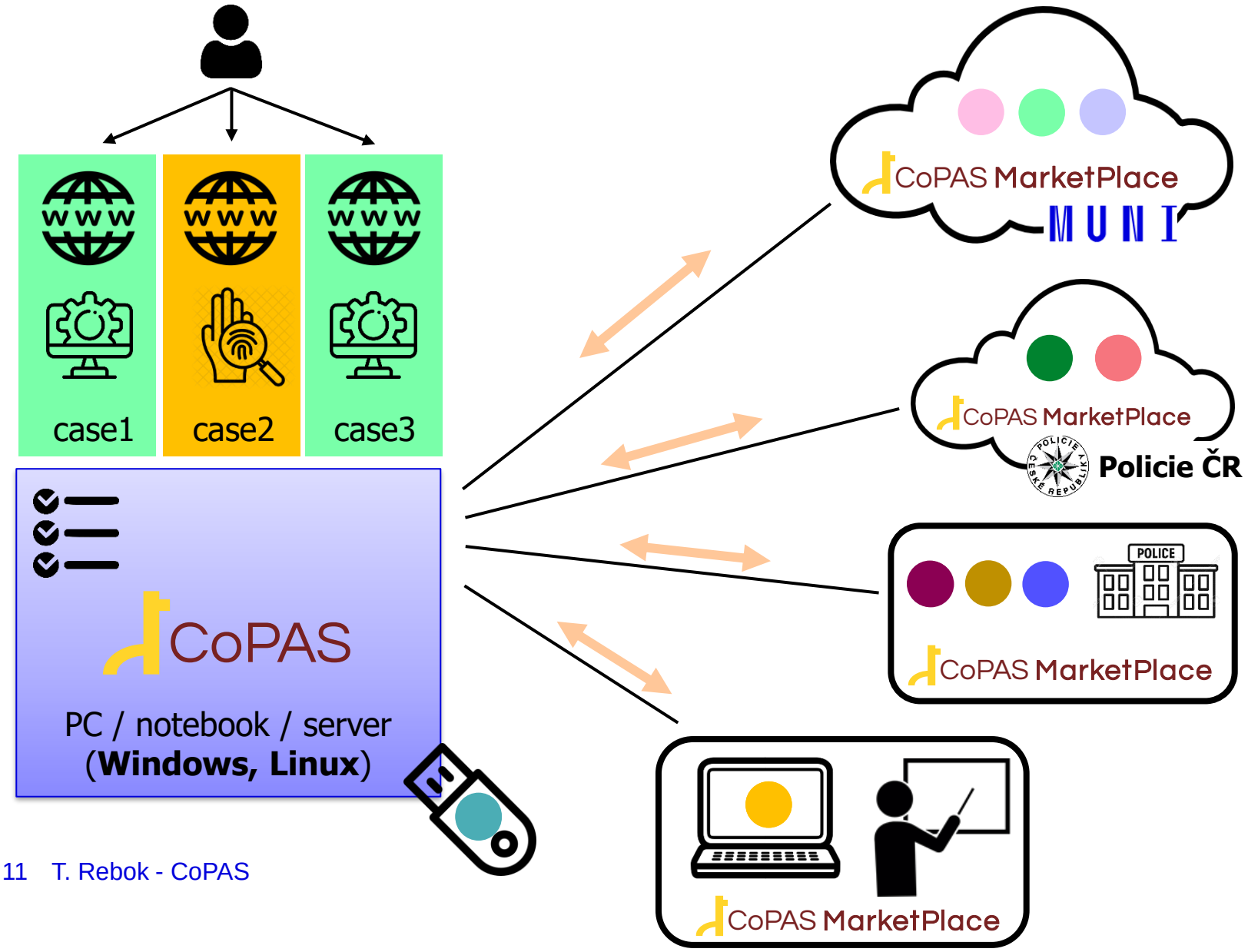
Modulární datově-analytické řešení …

které:

- umožňuje **lokální datové analýzy a zpracování dat** prostřednictvím kontejnerizovaných modulů
  - včetně podpory běhu **kontejnerizovaných aplikací**
- umožňuje budování **tematicky-zaměřených repositářů**
  - *CoPAS Marketplace*
- poskytuje **podporu pro vývoj a integraci nových modulů**
  - staví na značce *„Powered by CoPAS“*
    - *tj. nepřivlastňuje, ale naopak podporuje integraci externích řešení*

MUNI

CoPAS – ilustrace funkcionality



1. Instalace CoPAS
2. Napojení na repositáře
   - externí (např. MUNI)
   - centrální (PCR, …)
   - lokální (útvar, tým)
   - cestovní (školení)
3. Zjištění dostupných modulů
4. Stažení vybraných modulů
   - nebo offline instalace z přenosného disku
5. Spuštění kontejnerů z vybraných modulů
   - lze kombinovat
   - i více instancí z jednoho modulu
6. Připojení a práce s kontejnery
   - WWW prohlížeč
7. Zálohy či výmaz kontejnerů, přenos na silnější HW, atp.

MUNI

CoPAS – hlavní myšlenka I.

Typické formy realizace (nejen forenzních) IT řešení:

- **cloudová řešení** – výhodou škálovatelnost a „on-click“ řešení, nevýhodou omezená transparentnost práce s daty
  - pro bezpečnostní složky typicky zcela nevhodné
- **izolované on-premise nástroje** – výhodou kontrolovaná práce s daty (privátnost), nevýhodou složitá příprava prostředí a omezená škálovatelnost
  - časově i zdrojově náročné, ne vždy dostupné pro koncový OS
    - platí i v případě dostupnosti kontejnerů

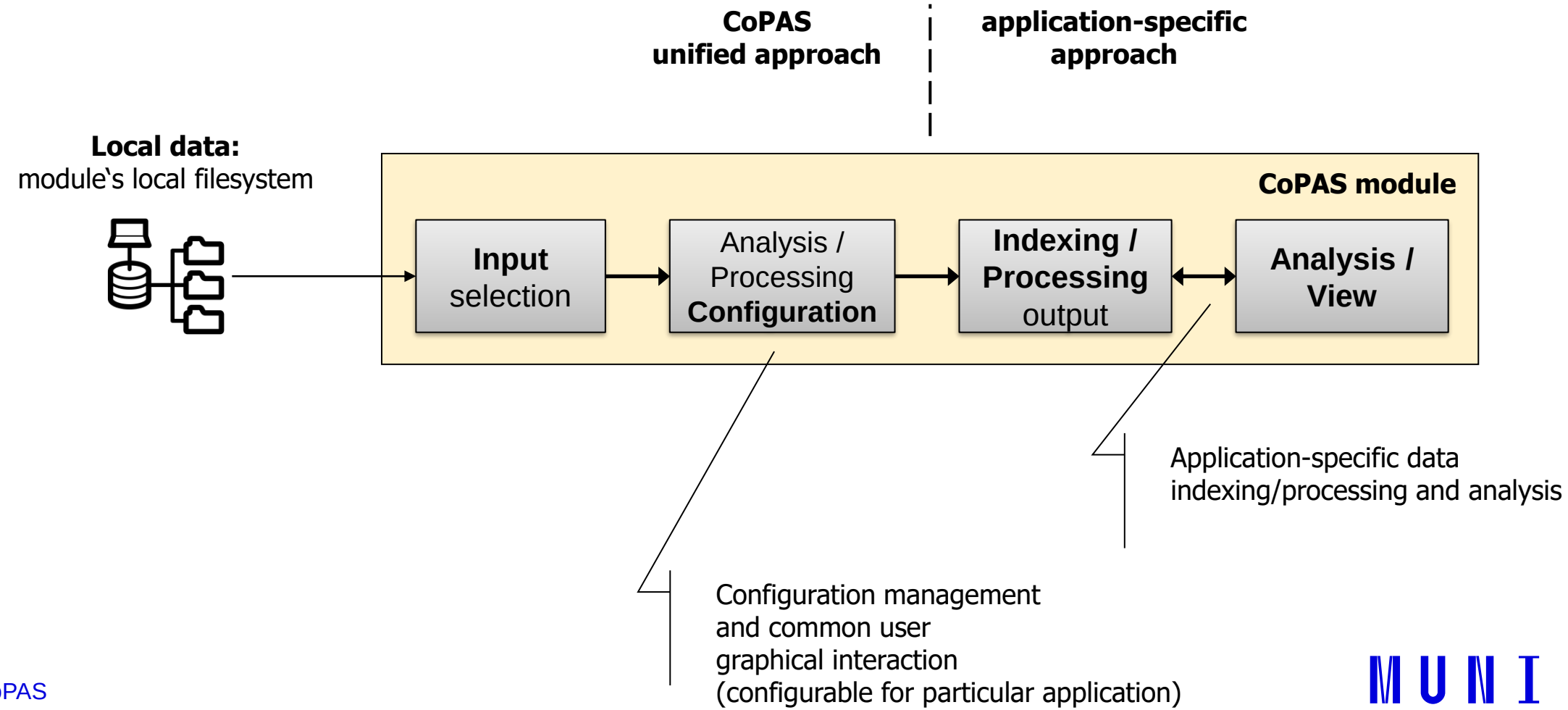
CoPAS tyto nenahrazuje, ale rozšiřuje o další možnost:

- **cloudová řešení na koncových stanicích**
  - „velká řešení na malých datech“
- **jednotné (unifikované) prostředí pro zpracování, sdílení a analýzu dat**
  - decentralizovaný (distribuovaný) model

MUNI

CoPAS – hlavní myšlenka II.

Separace jednotlivých datově-analytických kroků:



MUNI

CoPAS – možnosti využití (šablony)

Datově-analytický nástroj

- ***šablona:*** jednotné webové rozhraní, správa souborů, správa konfigurací, správa zdrojů, práce s archívy, sledování adresářů, historie analýz, …
- ***cíl:*** snaha o minimalizaci požadavků na tvůrce nových analytických modulů

Nástroj pro podporu školení (a práce s aplikacemi)

- ***šablona:*** jednotné webové rozhraní, Linuxový desktop, Linuxový desktop s podporou Windows aplikací
- ***cíl:*** jednotlivé aplikace nebo sady aplikací ve vyladěném prostředí

Nástroj pro podporu infrastrukturních školení a her

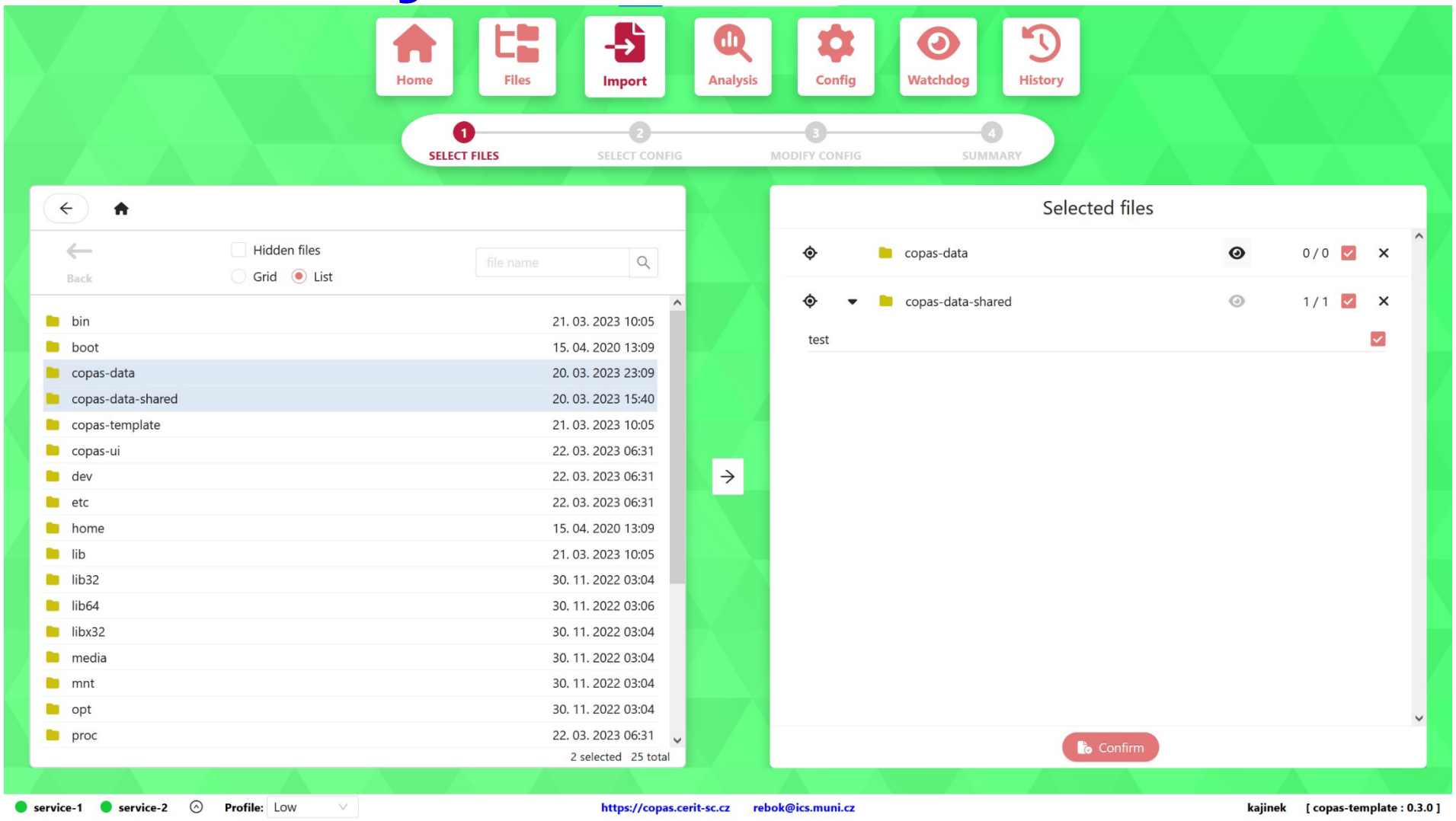
- ***šablona:*** jednotné webové rozhraní, podpora týmových her (s řídícím prvkem – školitel)
- ***cíl:*** týmové hry s využitím uživatelských zařízení a kontejnerizovaných modulů
  - první hru představíme během podzimu 2023 (*Capture the Flag!*)

MUNI

CoPAS – analytická šablona

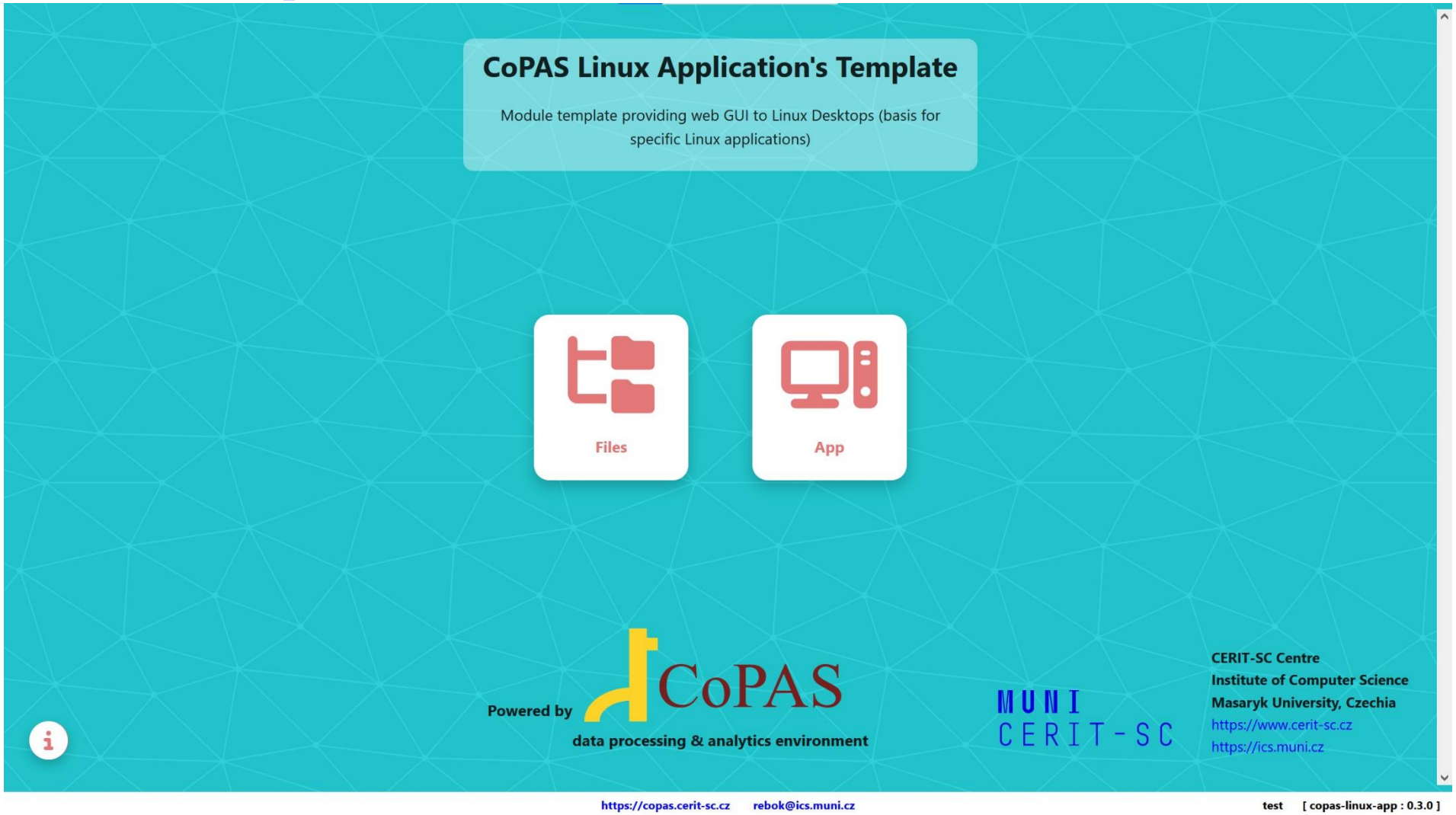
MUNI

CoPAS – analytická šablona



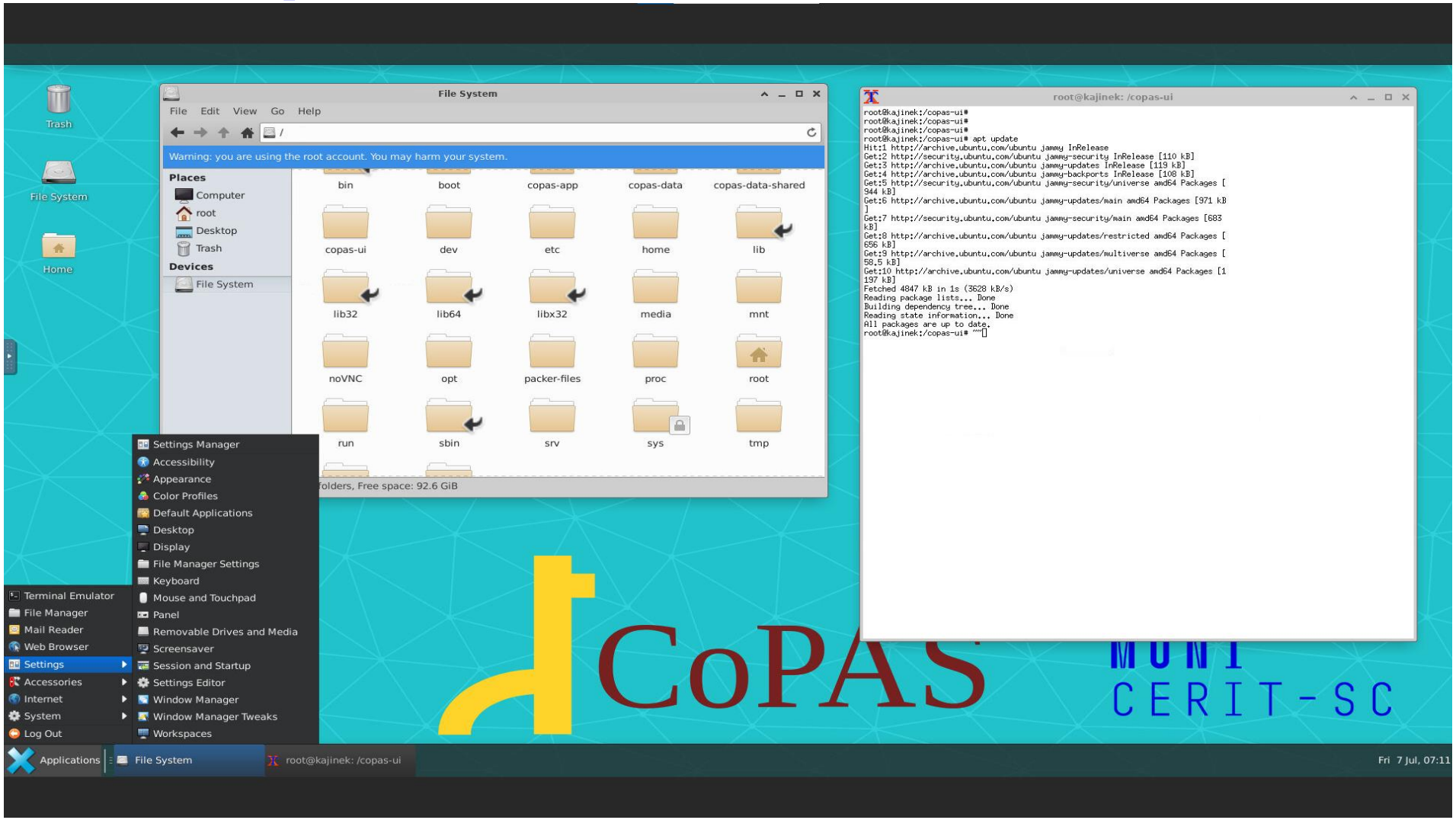
MUNI

CoPAS – aplikační šablona



MUNI

CoPAS – aplikační šablona

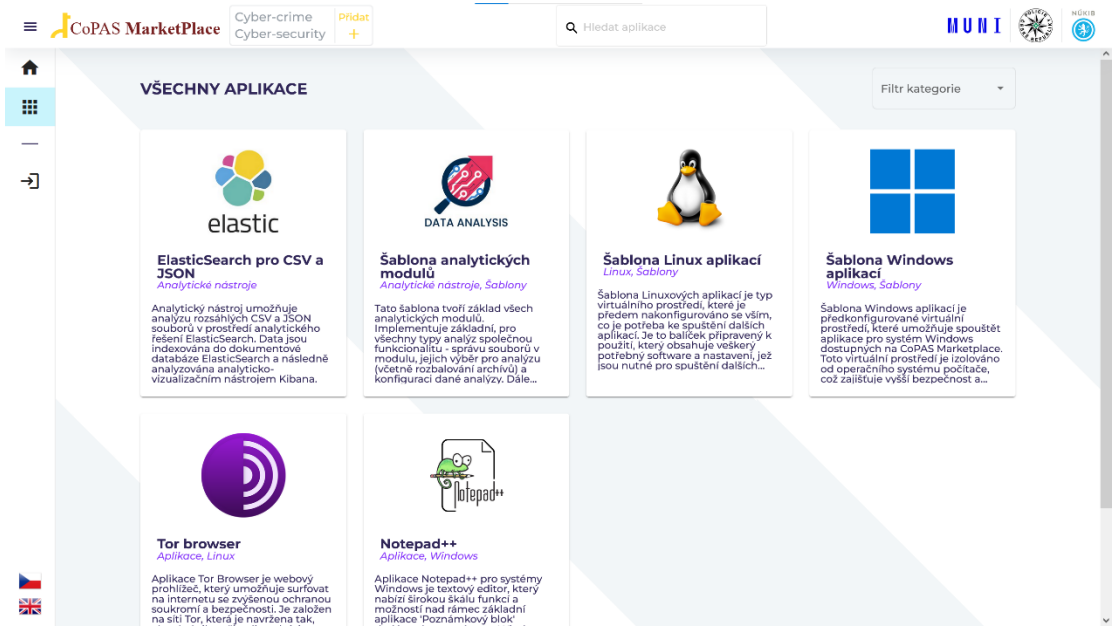


MUNI

CoPAS Marketplace

Grafické rozhraní prezentující moduly (aplikace) v repositáři

- aktuálně v první verzi
  - jednoduchá prezentace modulů
- **cílový stav:** rozšíření o funkcionalitu pro podporu sdílení informací
  - včetně informací o verzích modulů, jejich hodnocení, komentáře, návody, atp.
    - adaptace podle potřeb uživatelů
- součástí i funkcionalita **přehrávání modulů mezi repositáři**
  - podpora pro „cestovní“ repositáře
    - nahrání modulů potřebných pro dané školení
- rozšířená verze 1.0 cca konec 2023



CoPAS – hlavní výhody

Obecné:

- **modularita** a **flexibilita**
  - každý modul specializován pro konkrétní funkcionalitu
  - možnost stažení pouze vybraných modulů (podle zájmu uživatele)
    - a vícenásobné instanciace (z jednoho modulu více instancí-kontejnerů)
- **repositáře modulů**
  - podpora napojení na více repositářů současně
  - možnost vybudování a udržování tematicky či odborně zaměřených repositářů
    - např. repositář pro forenzní aplikace, repositář pro konkrétní tým, repositář pro potřeby školení, ...
- **šablony modulů**
  - podpora vytváření nových modulů prostřednictvím připravených šablon
    - snaha o minimalizaci nároků na vývojáře
    - poskytování hotových (a vyladěných) společných vlastností

MUNI

CoPAS – hlavní výhody

Obecné:

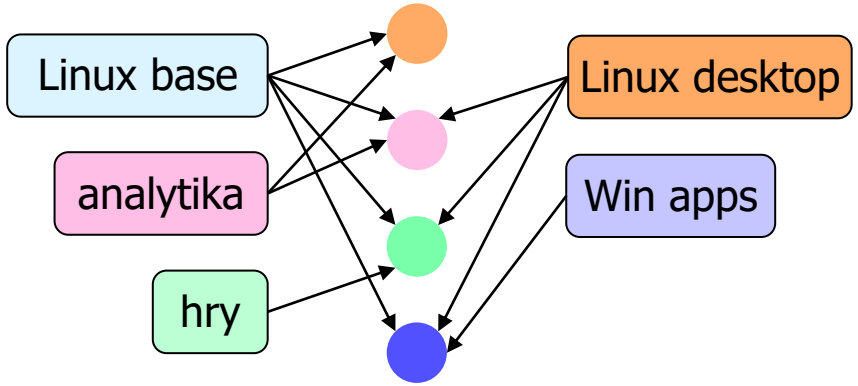
- **bezpečnost**
  - aplikace uvnitř kontejneru nemá (jednoduchý) přístup do hostitelského systému
    - zabezpečení lze dále posilovat (Minikube)
- **privátnost**
  - možnost analýzy a zpracování citlivých informací
    - data zůstávají na zařízení (může být zcela odříznuto od sítě)
  - možnost vybudování vlastních (privátních) repositářů
    - včetně možnosti práce na zcela uzavřené síti
- **definovaný stav** a **„čistota“**
  - nová instance (kontejner) každého modulu vždy v definovaném (nezměněném) stavu
    - změny však udržovány až do jeho smazání
  - počet instancí (kontejnerů) každého z modulů omezen pouze dostupným HW
    - instance různých modulů mohou běžet souběžně
  - po smazání kontejnerů/modulů je hostitelský systém v původním stavu
    - nedochází k zásahům do hostitelského systému

CoPAS – hlavní výhody

Obecné:

- **přenositelnost**
  - možnost přenosu kontejnerů mezi hostitelskými počítači
    - např. při nedostatku zdrojů na notebooku přenos rozdělané práce na výkonnější server
    - možnost sdílení práce mezi spolupracovníky
- **nezávislost na hostitelském OS a HW**
  - odstínění od konkrétního OS a HW zajišťuje kontejnerová vrstva
    - přenositelnost rozpracované práce i mezi různým OS a HW
  - testováno na OS Linux a OS Windows, mělo by fungovat i na MacOS
- **jednoduchost vzdálené práce**
  - běh instancí na výkonnějším serveru a vzdálený přístup k němu
    - prostřednictvím webového prohlížeče
    - identický způsob práce jako s lokální instancí

CoPAS – hlavní výhody



Obecné:

- **automatizované sestavování a správa modulů**
  - kompletní příprava modulů prostřednictvím Ansible
    - plně automatizovaný proces sestavení
  - komponentová struktura modulů
    - moduly sestávají z vybraných (předpřipravených) komponent
    - izolace jejich vývoje, testování a nasazení
- **efektivní využívání zdrojů hostitelského systému**
  - kontejnerové aplikace zabírají pouze ty zdroje, které skutečně využívají

MUNI

CoPAS – hlavní výhody

Obecné:

- **iluze virtuálního stroje**
  - možnost příkazové řádky a instalace vlastních aplikací
    - avšak pouze OS Linux
- **minimální infrastrukturní nároky**
  - prakticky „neomezená“ škálovatelnost
    - zpracování probíhá na lokálních stanicích
    - centrální infrastruktura poskytuje pouze uložiště modulů (repositáře)
- **open-source nástroje**
  - veškeré využívané nástroje jsou open-source
  - CoPAS samotný bude také uvolněn pod vhodnou open-source licencí

CoPAS Education

CoPAS Education – hlavní výhody

Další výhody z pohledu potřeb školení:

- možnost **vybudování specializovaných repositářů** se školícími aplikacemi
  - možnost přípravy **repositáře i na HW lektora**
    - účastníci získávají moduly po lokální (uzavřené) síti
- schopnost **využití klientského hardware** (notebooky, PC)
  - není zapotřebí drahá cloudová infrastruktura (a její náročná správa a údržba)
- možnost poskytnout **prostor pro práci studentům i po školení**
  - zprostředkováním repositáře (nezatěžují HW pro školení)
  - moduly mohou využívat i po školení pro vlastní práci
    - případně se připravovat na další dny školení
- schopnost naučit se ovládat „**velká řešení na malých datech**“
  - a následně tyto znalosti analogicky využít na datech velkých (reálných)
- možnost hromadné **demonstrace pracovní plochy vybraného účastníka**
  - vzdálené připojení z lektorského PC přes prohlížeč

MUNI


thank you
danke
рахмат
謝謝
ngiyabonga
teşekkür ederim
spas
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
gracias
хвала
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràçie
hvala
enkosi
dankon
akun
aċiū
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
chokrane
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
sobodi
děkuji
obrigado
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercé
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

MUNI