

MUNI

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



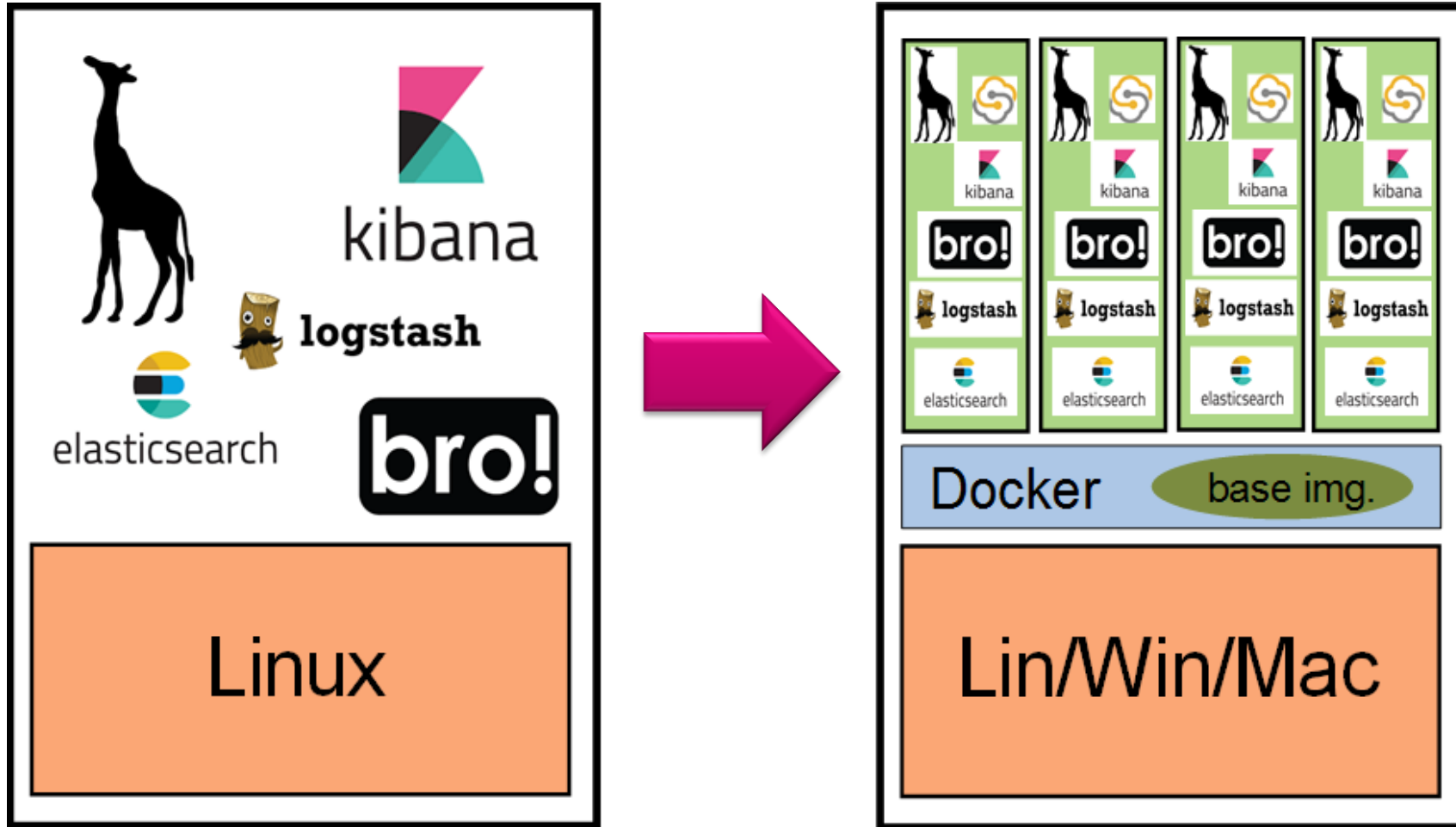
CopAS (do verze 3.1)

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

CopAS (do verze 3.1)



CopAS – správa kontejnerů (do verze 3.1)

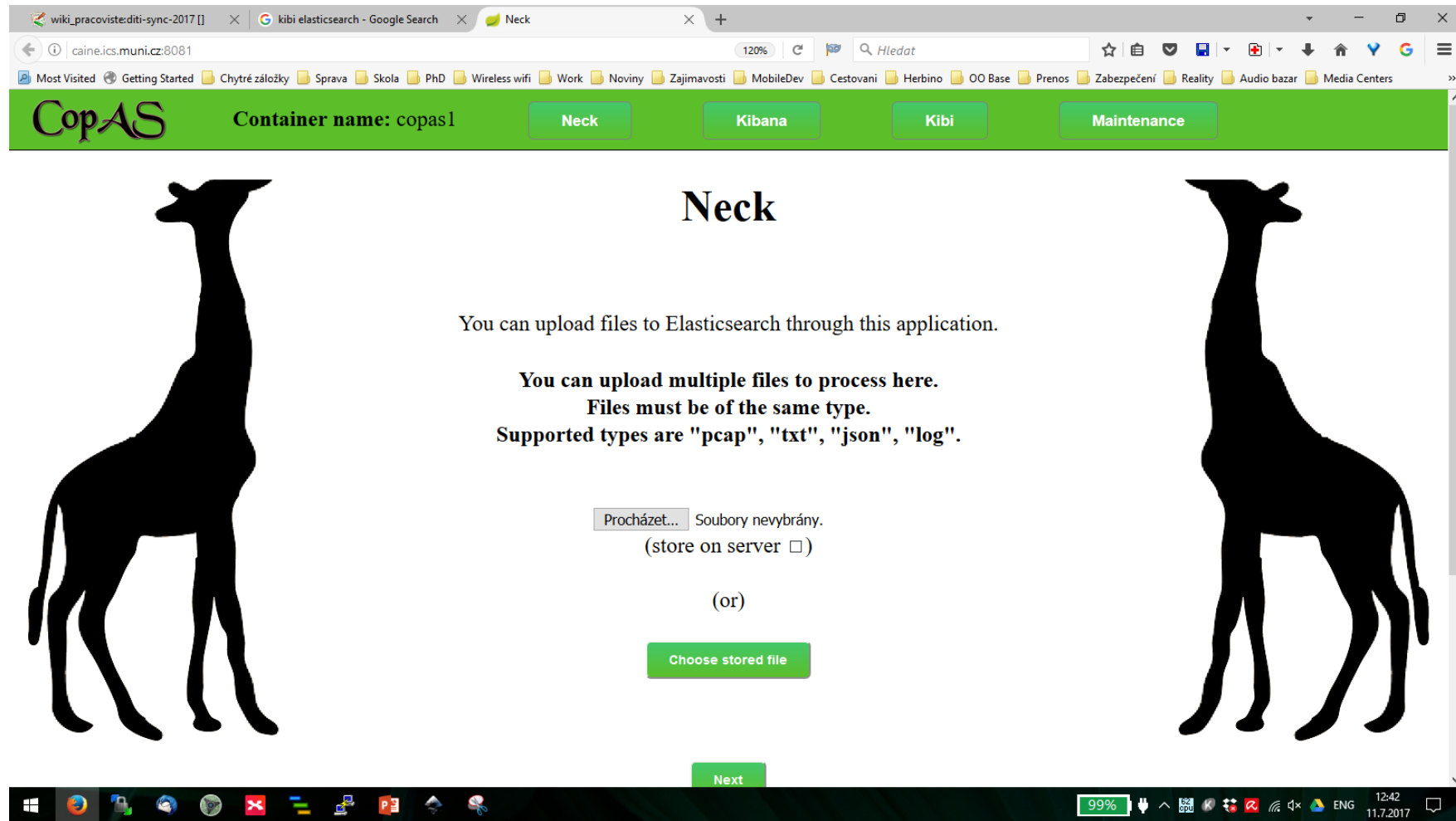
copas ACTION [container name]

- *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
```


CopAS – uživatelské prostředí (verze 1.0)



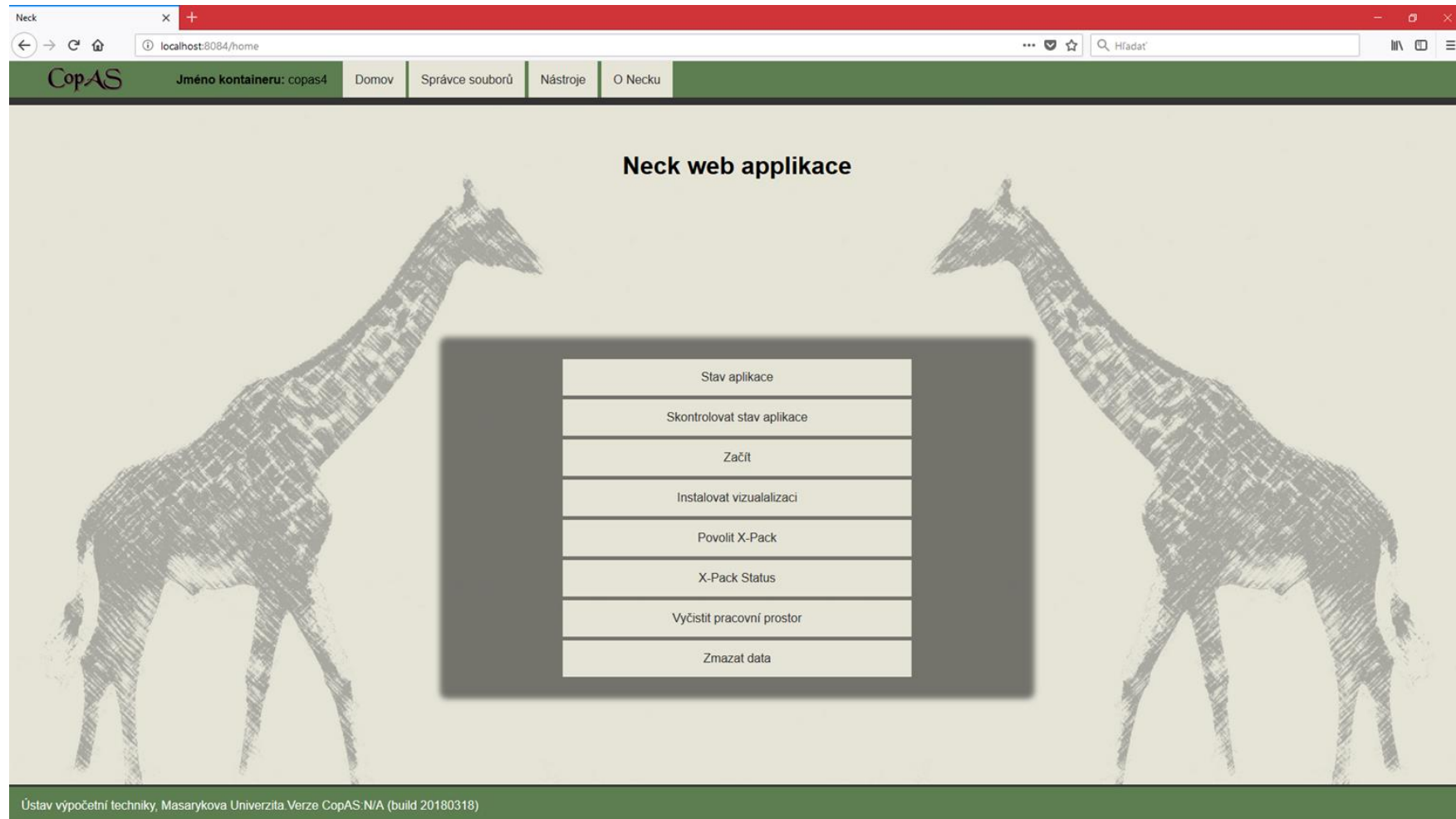
The screenshot shows a web browser window with the CopAS application. The browser tabs include 'wiki_pracovistediti-sync-2017', 'kibi elasticsearch - Google Search', and 'Neck'. The address bar shows 'caine.ics.muni.cz:8081'. The application header is green and contains the CopAS logo, the container name 'copas1', and buttons for 'Neck', 'Kibana', 'Kibi', and 'Maintenance'. The main content area is titled 'Neck' and contains the following text:

You can upload files to Elasticsearch through this application.

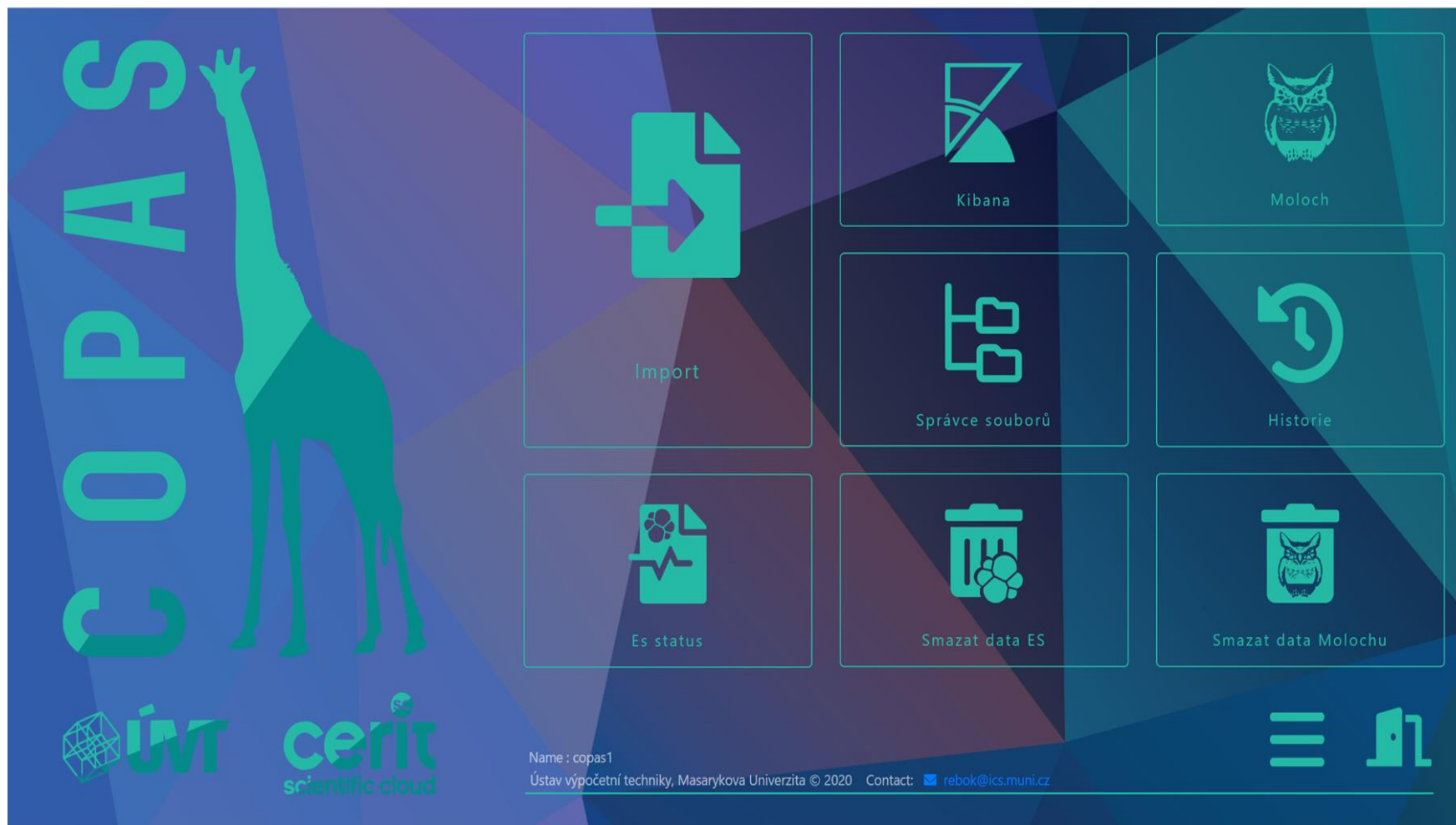
You can upload multiple files to process here.
Files must be of the same type.
Supported types are "pcap", "txt", "json", "log".

Below the text is a file upload area with a 'Procházet...' button, the text 'Soubory nevybrány.', and '(store on server)'. Below this is '(or)' and a green 'Choose stored file' button. At the bottom of the main content area is a green 'Next' button. The browser's taskbar at the bottom shows the Windows logo, several application icons, a 99% battery indicator, and the date and time '12:42 11.7.2017'.

CopAS – uživatelské prostředí (verze 2.0)



CopAS – uživatelské prostředí (verze 3.1)



CoPAS verze 4.0

modulární datově-analytické řešení



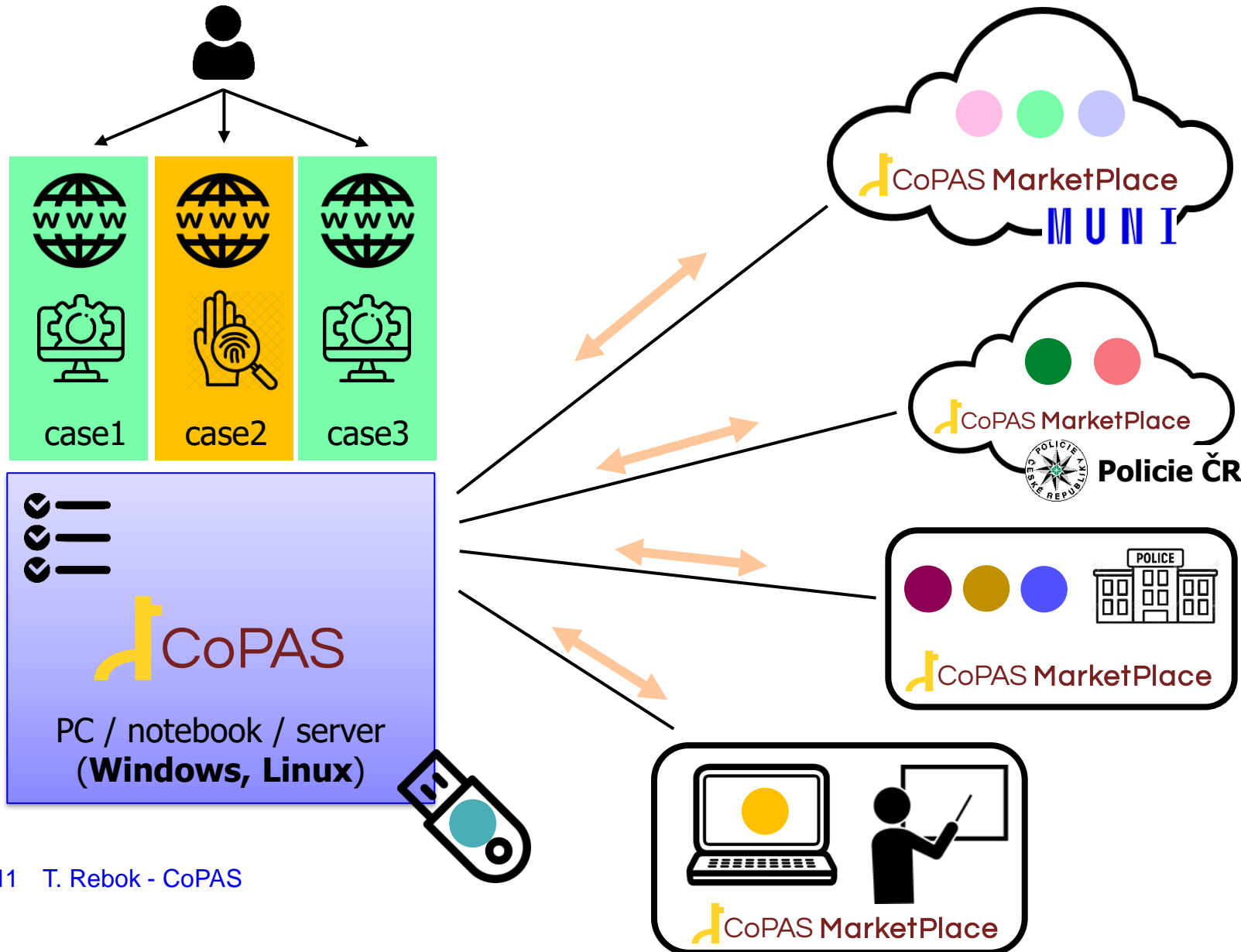
CoPAS (*Cop's Personal Analytic System*)

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*

CoPAS – ilustrace funkcionality



1. Instalace CoPAS
2. Napojení na repositáře
 - externí (např. MUNI)
 - centrální (PCR, ...)
 - lokální (útvár, 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.

CoPAS – hlavní myšlenka I.

Typické formy realizace (nejen forezních) IT řešení:

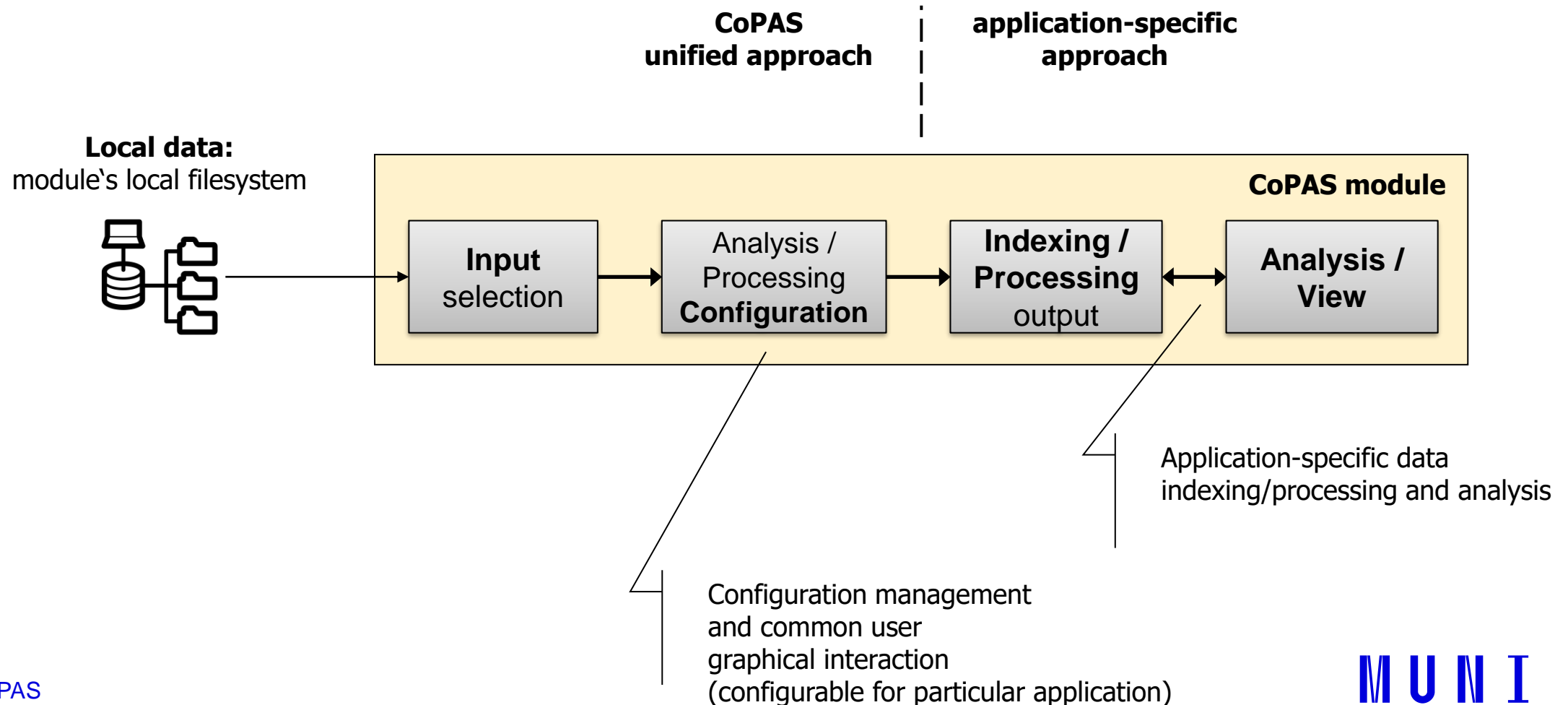
- **cloudová řešení** – výhodou škálovatelnost a „on-click“ řešení, nevýhodou omezená transparentnost práce s daty
 - pro bezpečnostní složky typicky zcela nevhodné
- **izolované on-premise nástroje** – výhodou kontrolovaná práce s daty (privátnost), nevýhodou složitá příprava prostředí a omezená škálovatelnost
 - 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

CoPAS – hlavní myšlenka II.

Separace jednotlivých datově-analytických kroků:



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 řídicím prvkem – školitel)
- **cíl:** týmové hry s využitím uživatelských zařízení a kontejnerizovaných modulů
– první hru představíme během podzimu 2023 (*Capture the Flag!*)

CoPAS – analytická šablona

CoPAS module template
This is a template for other copas modules

LOGO

John Doe
john@mail.com
Institution
Website

Files Import Analysis

Config Watchdog History

Powered by **CoPAS**
data processing & analytics environment

MUNI
CERIT-SC

CERIT-SC Centre
Institute of Computer Science
Masaryk University, Czechia
<https://www.cerit-sc.cz>
<https://ics.muni.cz>

service-1 service-2 Profile: Low

<https://copas.cerit-sc.cz> rebok@ics.muni.cz kajinek [copas-template : 0.3.0]

CoPAS – analytická šablona

Home Files Import Analysis Config Watchdog History

1 SELECT FILES 2 SELECT CONFIG 3 MODIFY CONFIG 4 SUMMARY

Back Hidden files Grid List file name

bin	21. 03. 2023 10:05
boot	15. 04. 2020 13:09
copas-data	20. 03. 2023 23:09
copas-data-shared	20. 03. 2023 15:40
copas-template	21. 03. 2023 10:05
copas-ui	22. 03. 2023 06:31
dev	22. 03. 2023 06:31
etc	22. 03. 2023 06:31
home	15. 04. 2020 13:09
lib	21. 03. 2023 10:05
lib32	30. 11. 2022 03:04
lib64	30. 11. 2022 03:06
libx32	30. 11. 2022 03:04
media	30. 11. 2022 03:04
mnt	30. 11. 2022 03:04
opt	30. 11. 2022 03:04
proc	22. 03. 2023 06:31

2 selected 25 total

Selected files

copas-data	0 / 0	<input checked="" type="checkbox"/>	×
copas-data-shared	1 / 1	<input checked="" type="checkbox"/>	×
test		<input checked="" type="checkbox"/>	

Confirm

service-1 service-2 Profile: Low <https://copas.cerit-sc.cz> rebok@ics.muni.cz kajinek [copas-template : 0.3.0]

CoPAS – aplikační šablona

CoPAS Linux Application's Template

Module template providing web GUI to Linux Desktops (basis for specific Linux applications)

Files App

Powered by **CoPAS**
data processing & analytics environment

MUNI
CERIT-SC

CERIT-SC Centre
Institute of Computer Science
Masaryk University, Czechia
<https://www.cerit-sc.cz>
<https://ics.muni.cz>

<https://copas.cerit-sc.cz> rebok@ics.muni.cz test [copas-linux-app : 0.3.0]

CoPAS – aplikační šablona

Warning: you are using the root account. You may harm your system.

```
root@kajinek:/copas-ui#  
root@kajinek:/copas-ui#  
root@kajinek:/copas-ui# apt update  
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease [110 kB]  
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [119 kB]  
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]  
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]  
Get:5 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [944 kB]  
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [971 kB]  
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [683 kB]  
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [656 kB]  
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [58.5 kB]  
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [197 kB]  
Fetched 4847 kB in 1s (3628 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
All packages are up to date.  
root@kajinek:/copas-ui#
```

Settings Manager
Accessibility
Appearance
Color Profiles
Default Applications
Desktop
Display
File Manager Settings
Keyboard
Mouse and Touchpad
Panel
Removable Drives and Media
Screensaver
Session and Startup
Settings Editor
Window Manager
Window Manager Tweaks
Workspaces

Applications | File System | root@kajinek: /copas-ui

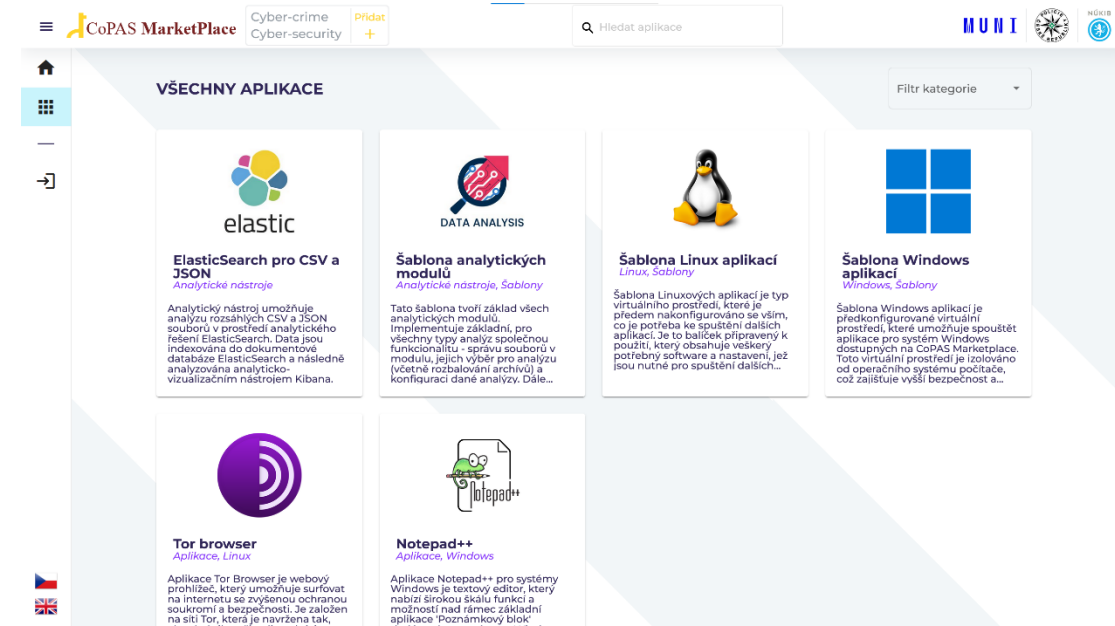
Fri 7 Jul, 07:11

CoPAS MUNI CERIT-SC

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

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

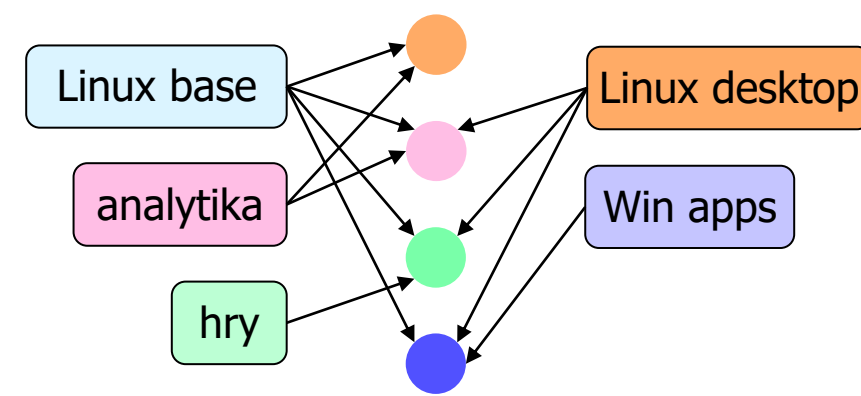
▪ nezávislost na hostitelském OS a HW

- 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

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 uložení modulů (repositáře)
- **open-source nástroje**
 - veškeré využívané nástroje jsou open-source
 - CoPAS samotný bude také uvolněn pod vhodnou open-source licenci

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

