# Secure Cloud-Native Infrastructure for AI-Based Tumor Tissue Analysis: A Collaborative Approach


## Authors

**Francesco Sinisi** (INFN)
Tomáš Brázdil (Faculty of Informatics, Masaryk University)
Alessandro Costantini (INFN)
Jacopo Gasparetto (INFN)
Lukáš Hejtmánek (Institute of Computer Science, Masaryk University)
Petr Holub (BBMRI-ERIC & Institute of Computer Science, Masaryk University)
Jiří Horák (BBMRI-ERIC & Faculty of Informatics and Institute of Computer Science, Masaryk University)
Barbara Martelli (INFN)
Vit Musil (Faculty of Informatics, Masaryk University)
Giusy Sergi (INFN)
Andreas Tuerk (BBMRI)

# Outline

## Context

- Scientific purpose: MCVAL use case
- Scientific collaboration

## Infrastructure and architecture

- Secure cloud
- Kubernetes cluster
- NFS Storage
- Authentication and logging
- Automation

## Software involved

- Data elaboration and visualization
- Authentication

## Conclusion

- Summary, issues and future prospects

# Context

DARE

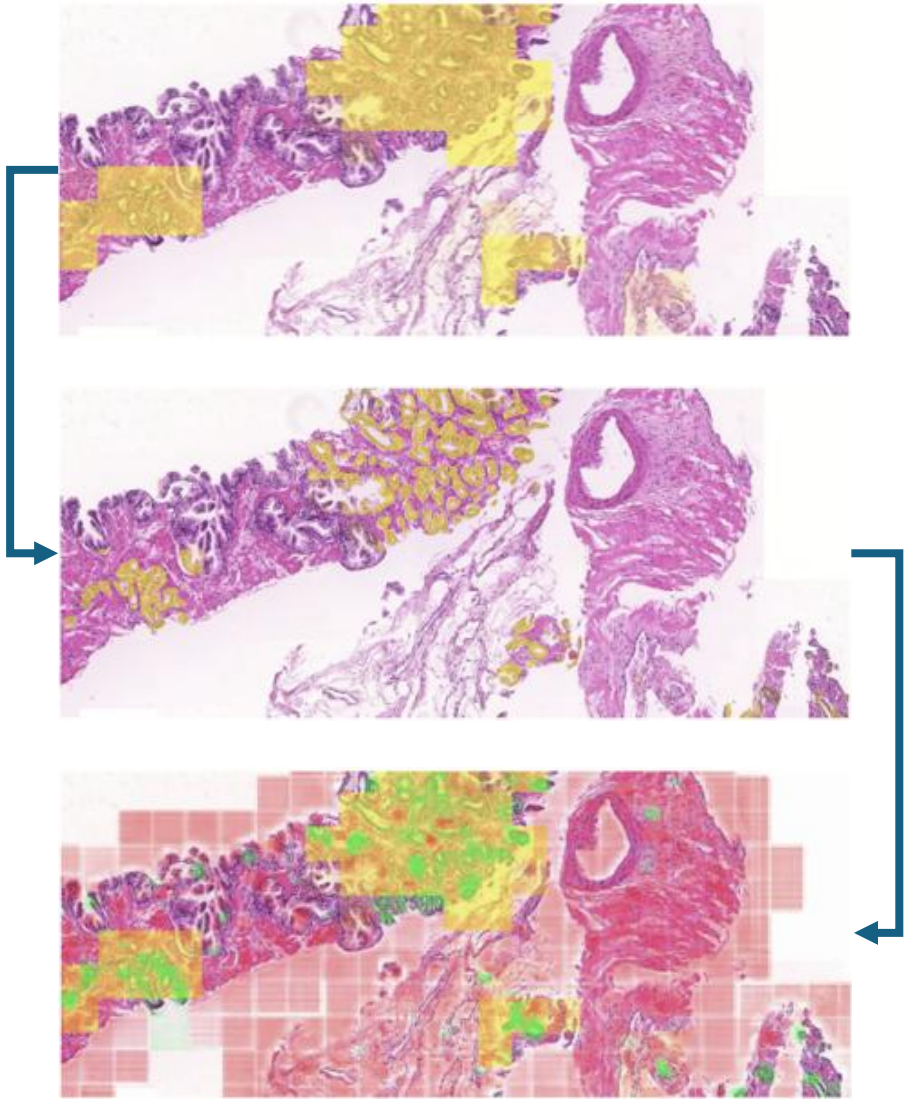
# Scientific purpose: MCVAL use case

**Problem**

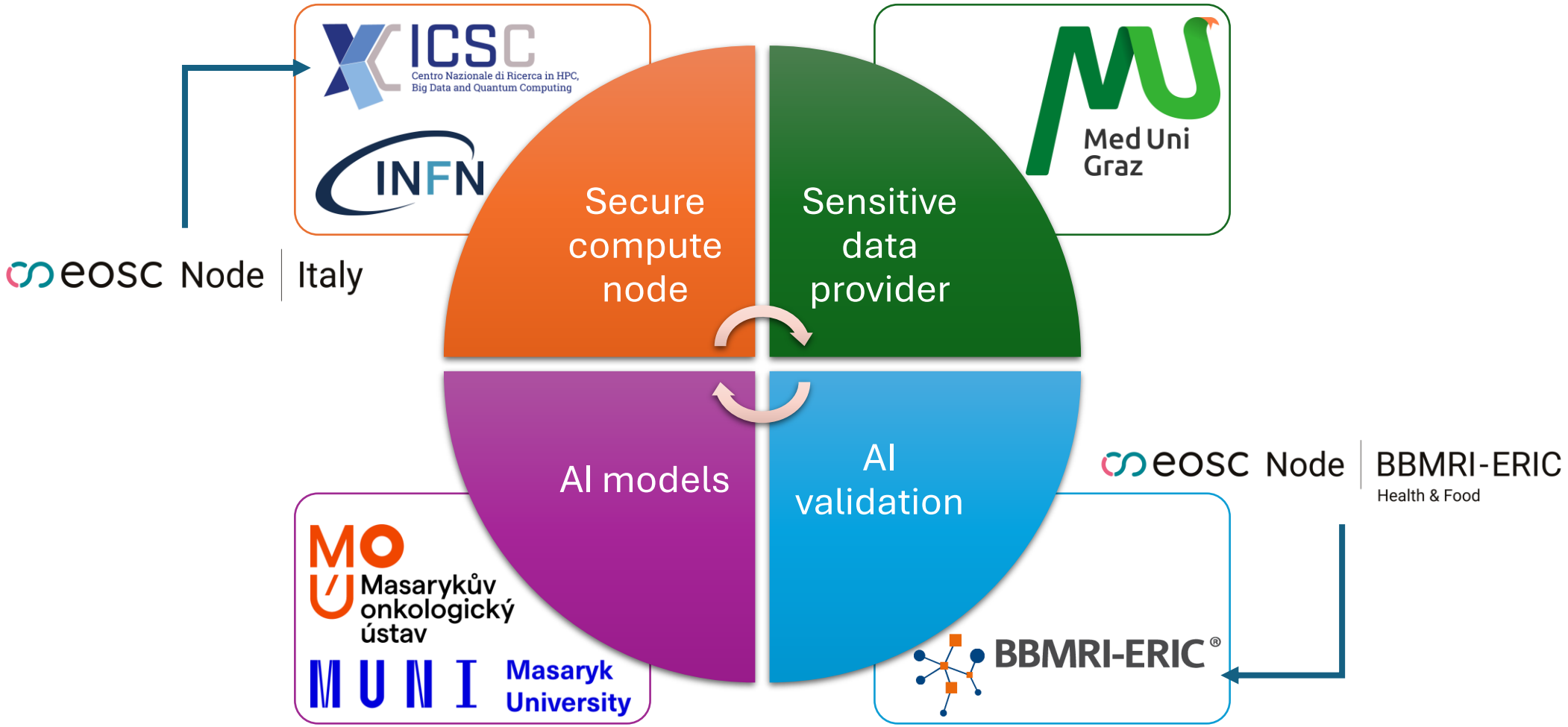
- AI models are often trained using data from a single healthcare institution, so they are not easily transferable
- Define Legal and Ethical frameworks

**Purpose**

- Develop a tool for validating AI models used in prostate cancer screening (**M**ulti-**C**entric **VAL**idation)



# Scientific collaboration






Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Infrastructure and architecture

DARE

# Secure Cloud

## Cloud

- Vertical and orizontal scaling
- Backups and volumes management
- Network segregation
- VM migration

## EPIC

- ISO certifications
- Access granted only to authorized personnel
- System administrator certification
- VPN and 2FA
- Reliable software

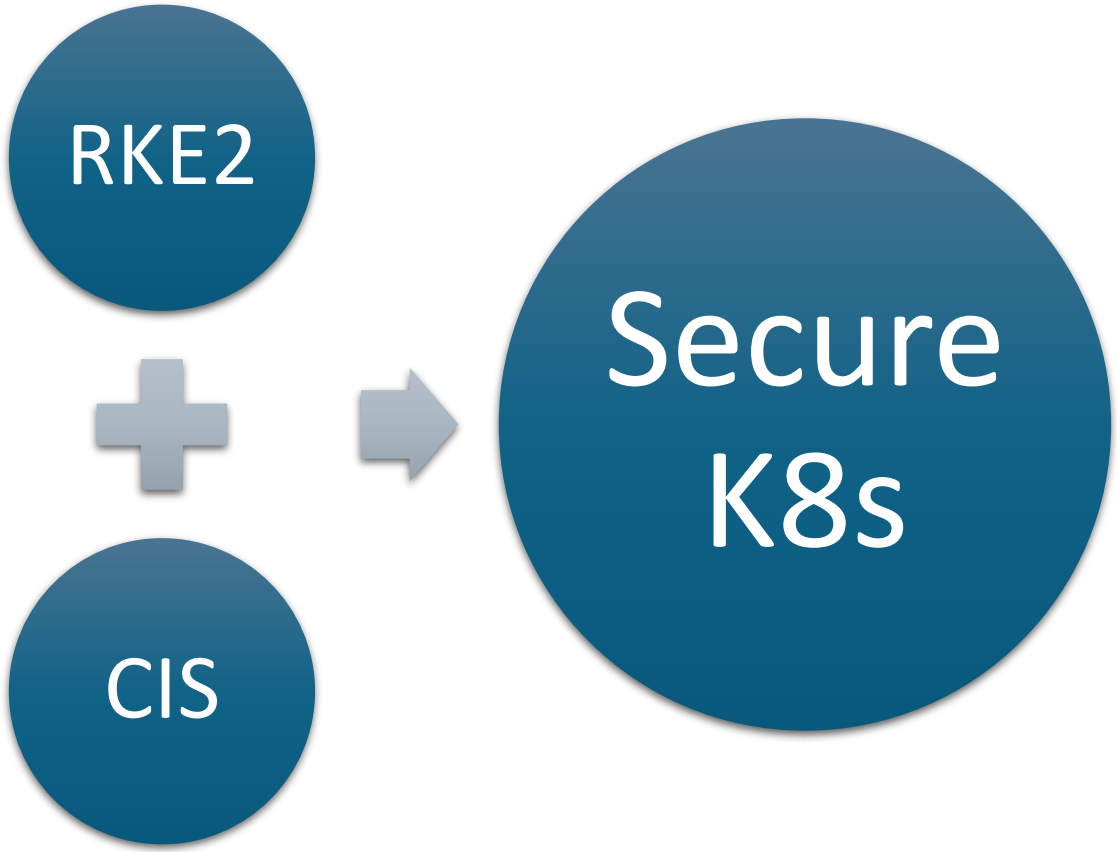
# Kubernetes cluster

## RKE2

- Enterprise-ready Kubernetes distribution
- Large community (sponsored by SUSE)
- CIS benchmark

## CIS

- Recommended secure configurations
- Disabling of risky features
- Several best practices






Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

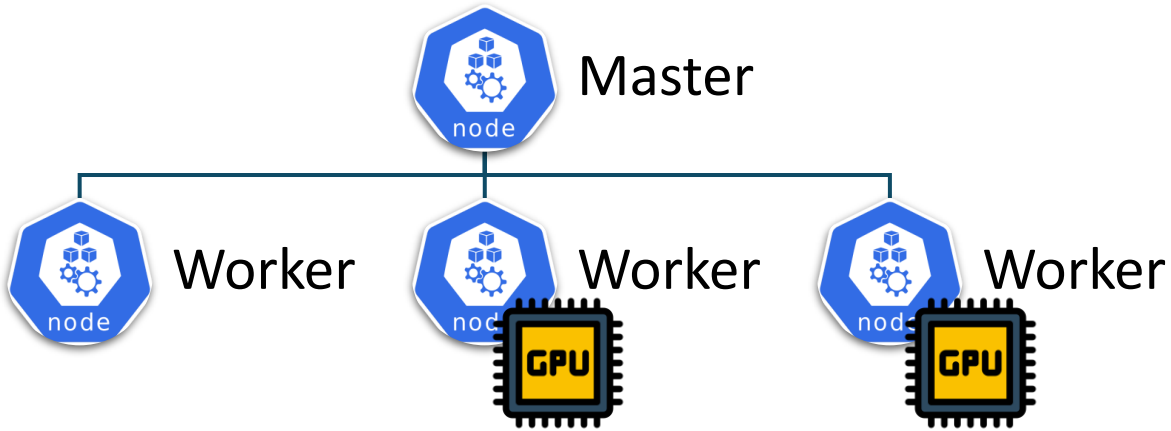
# Kubernetes cluster

## RKE2

- Enterprise-ready Kubernetes distribution
- Large community (sponsored by SUSE)
- CIS benchmark

## CIS

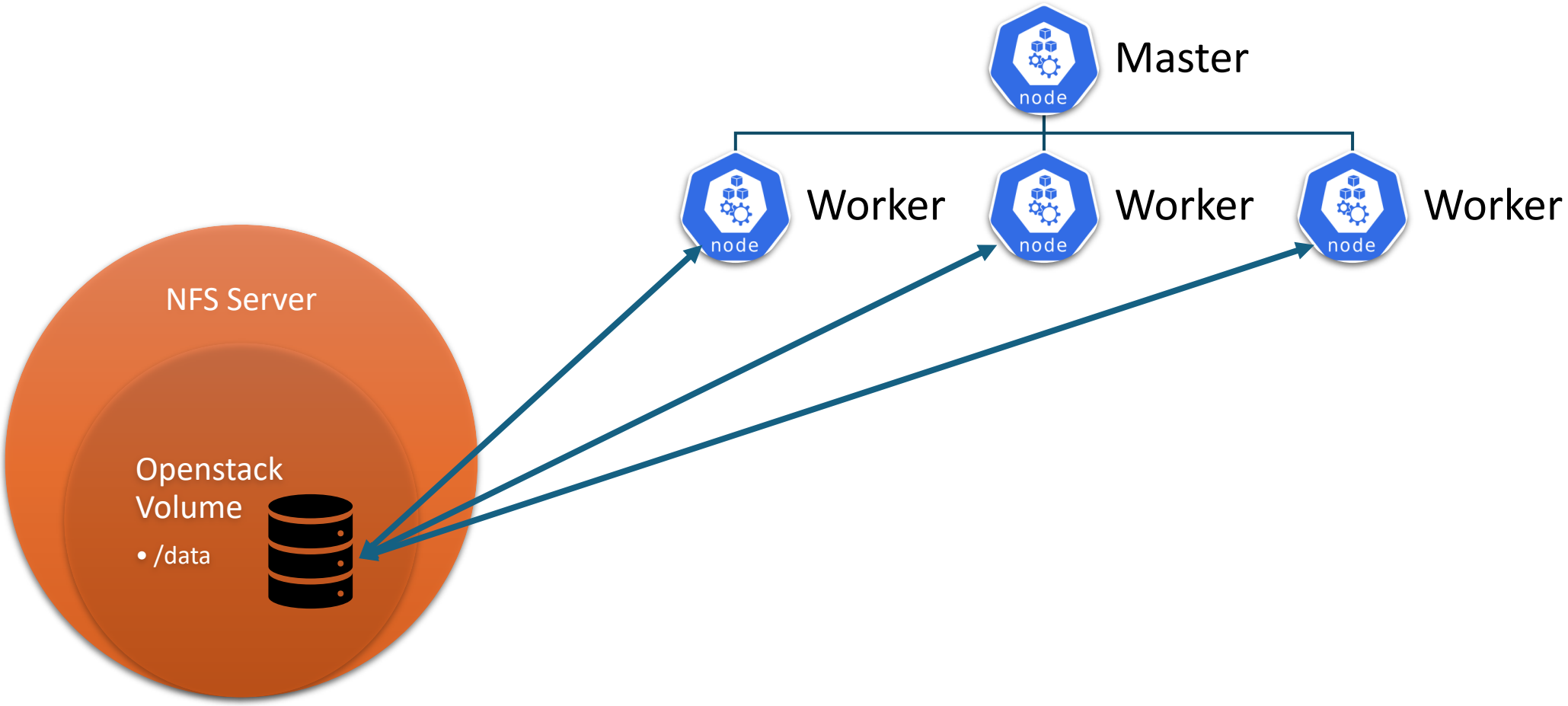
- Recommended secure configurations
- Disabling of risky features
- Several best practices



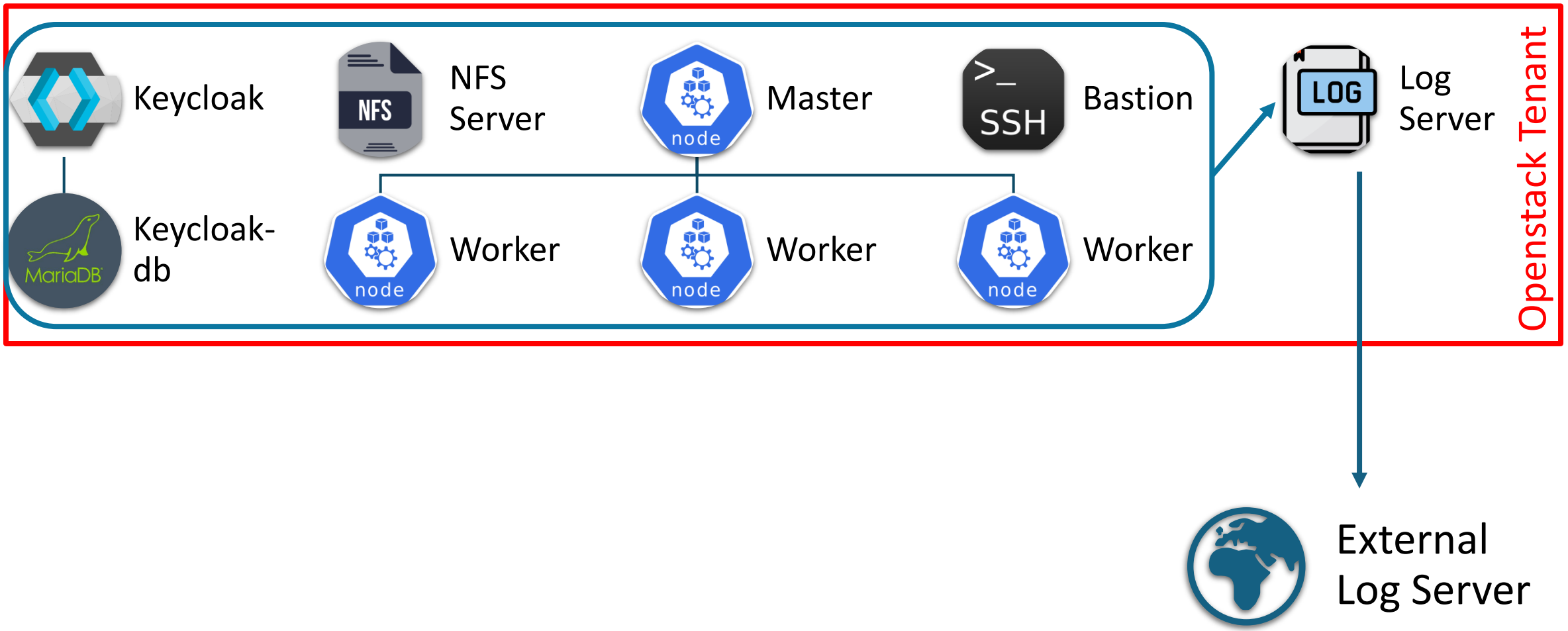



Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

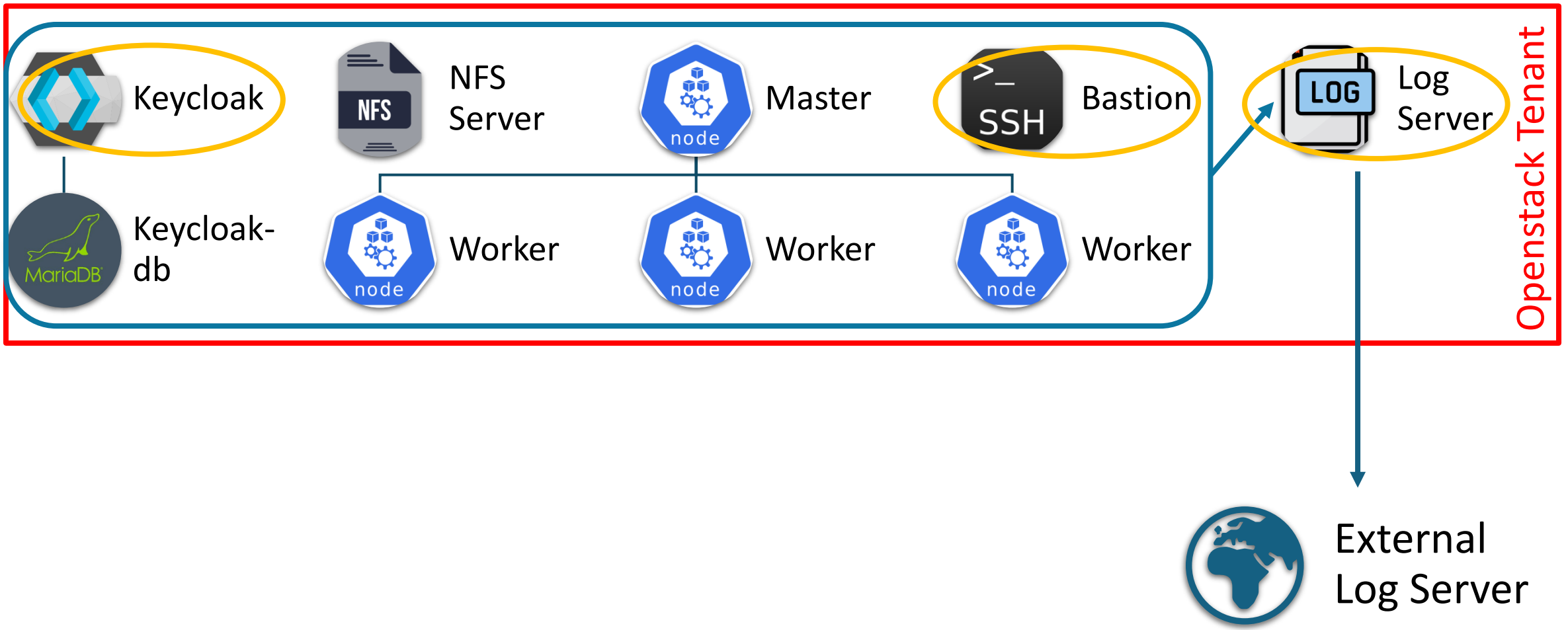
# NFS Storage



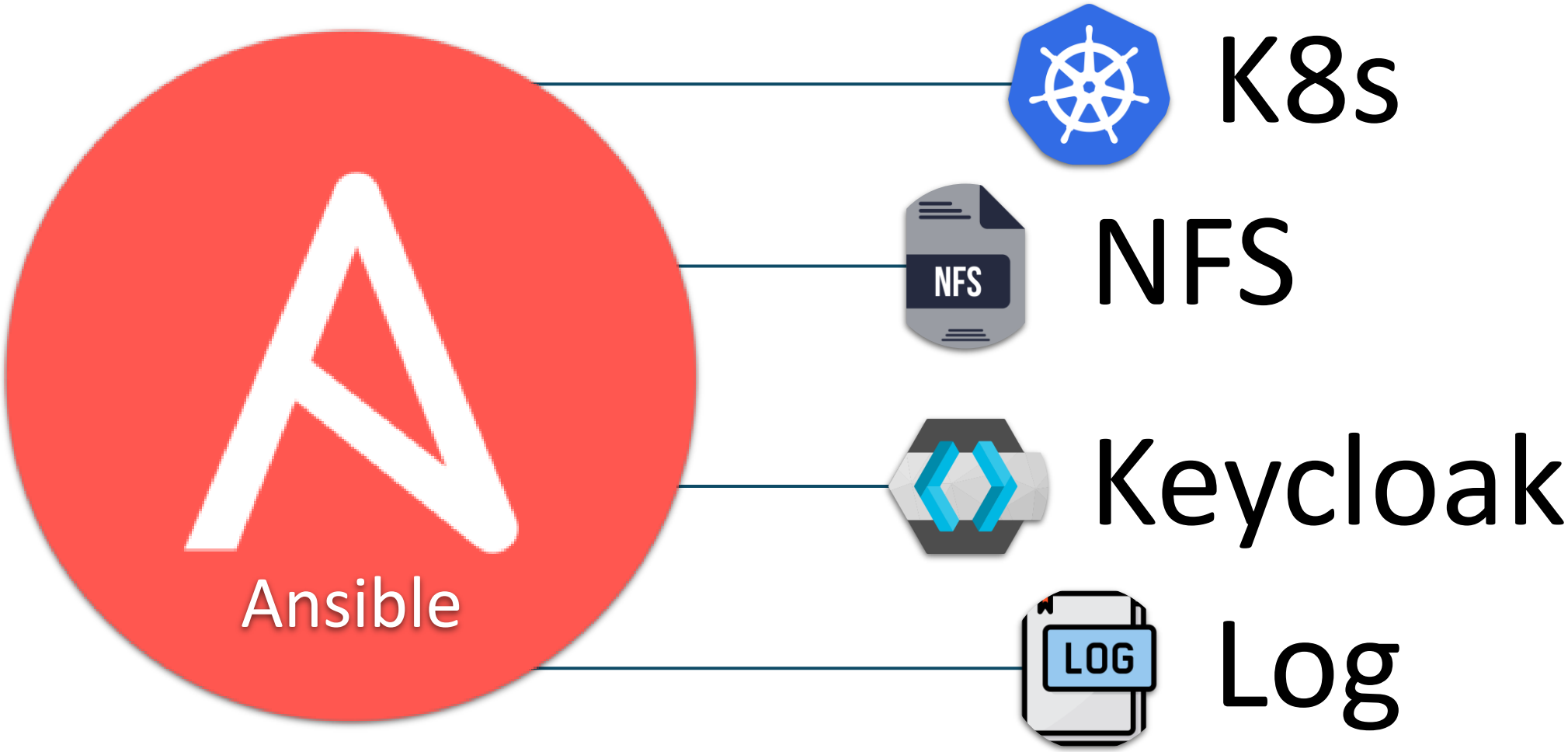
# Authentication and logging



# Authentication and logging



# Automation






Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Software involved

DARE

# Data elaboration and visualization

Jupyter

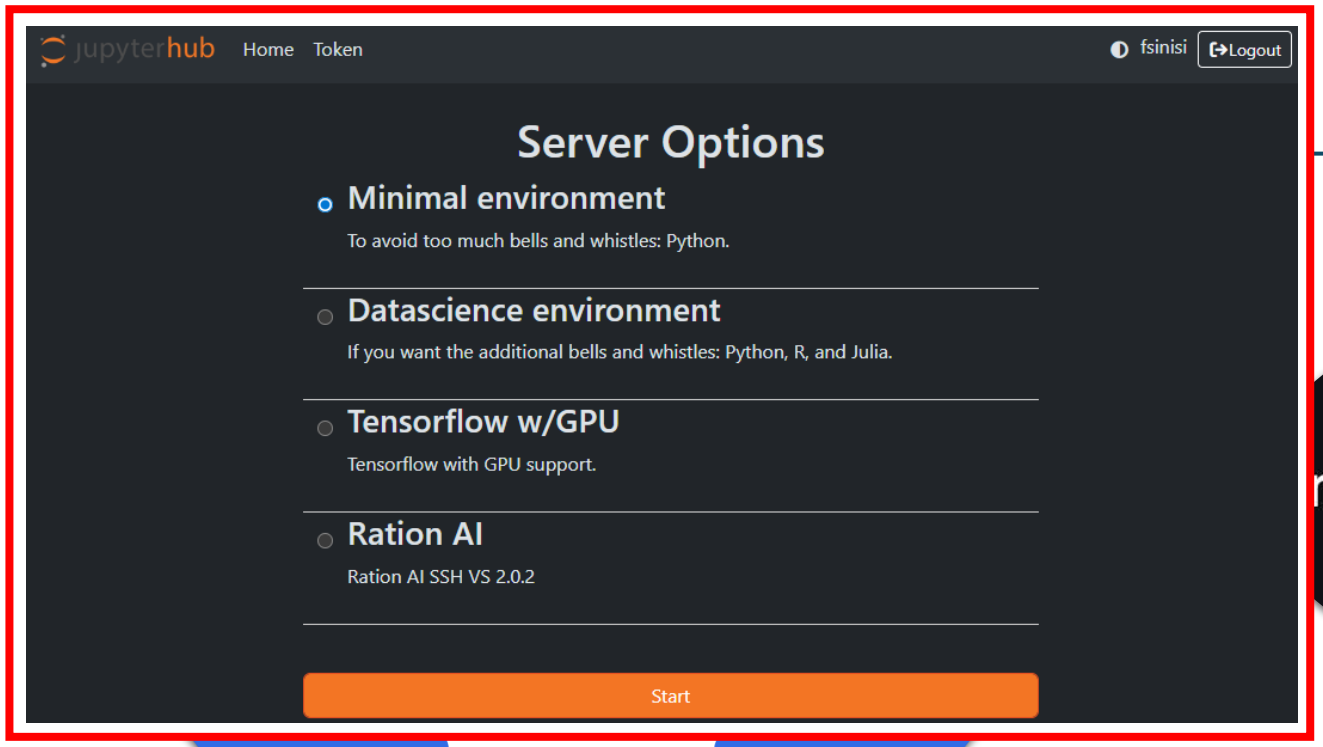
MLflow

Viewer



Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Data elaboration and visualization




jupyter Jupyter

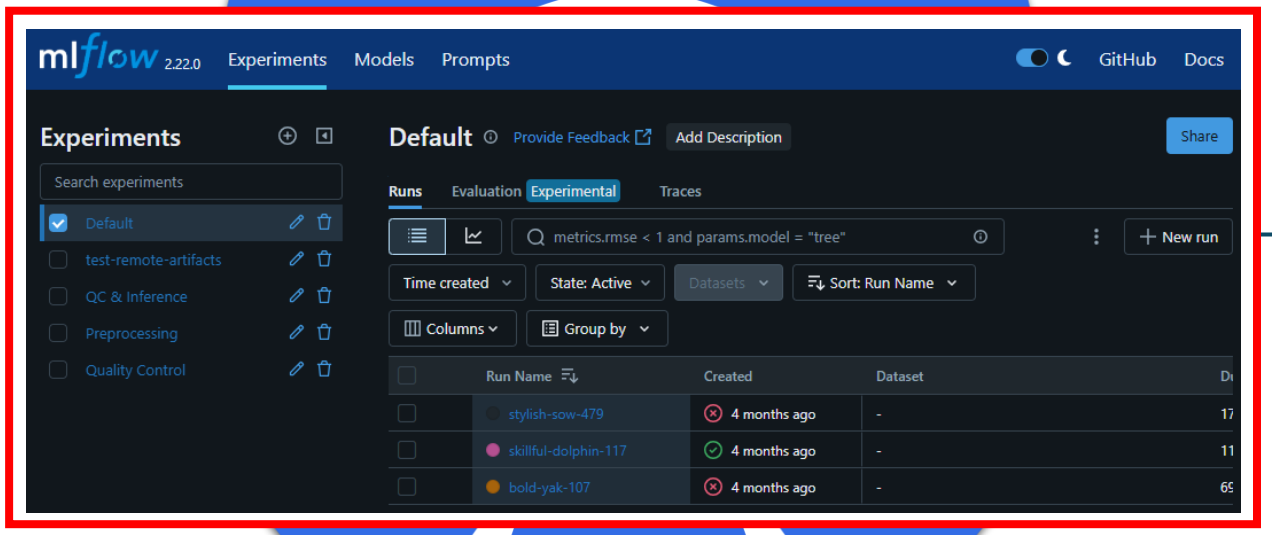
mlflow MLflow

Viewer



Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Data elaboration and visualization




jupyter Jupyter

mlflow MLflow

Viewer



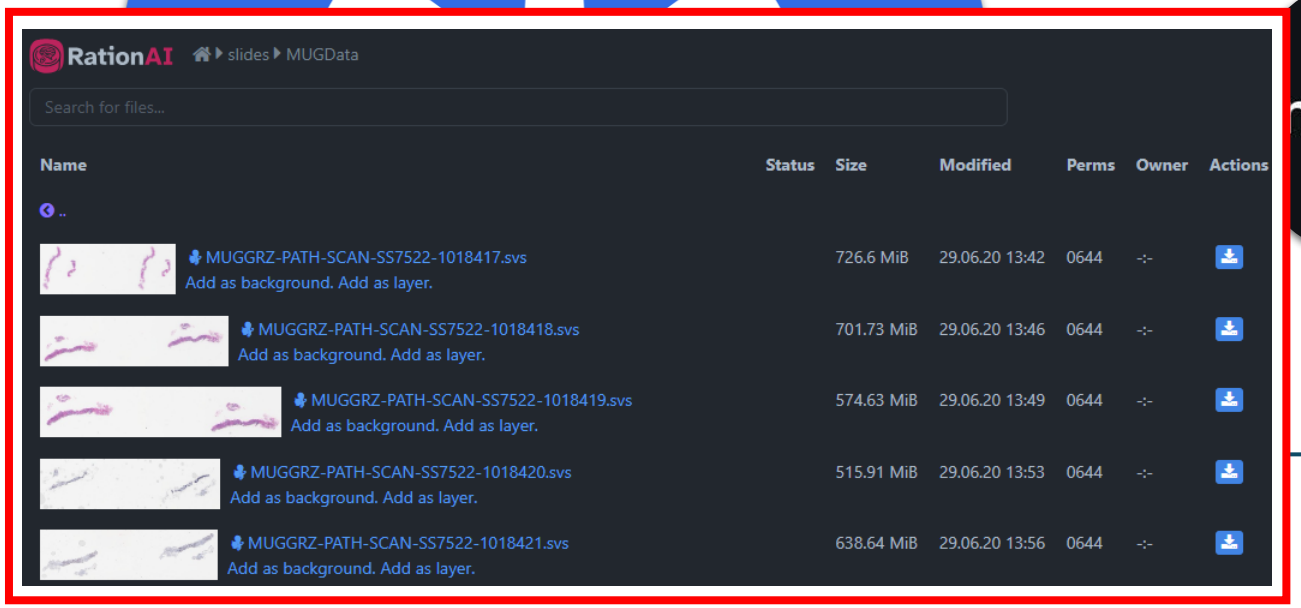
Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Data elaboration and visualization

Jupyter

MLflow

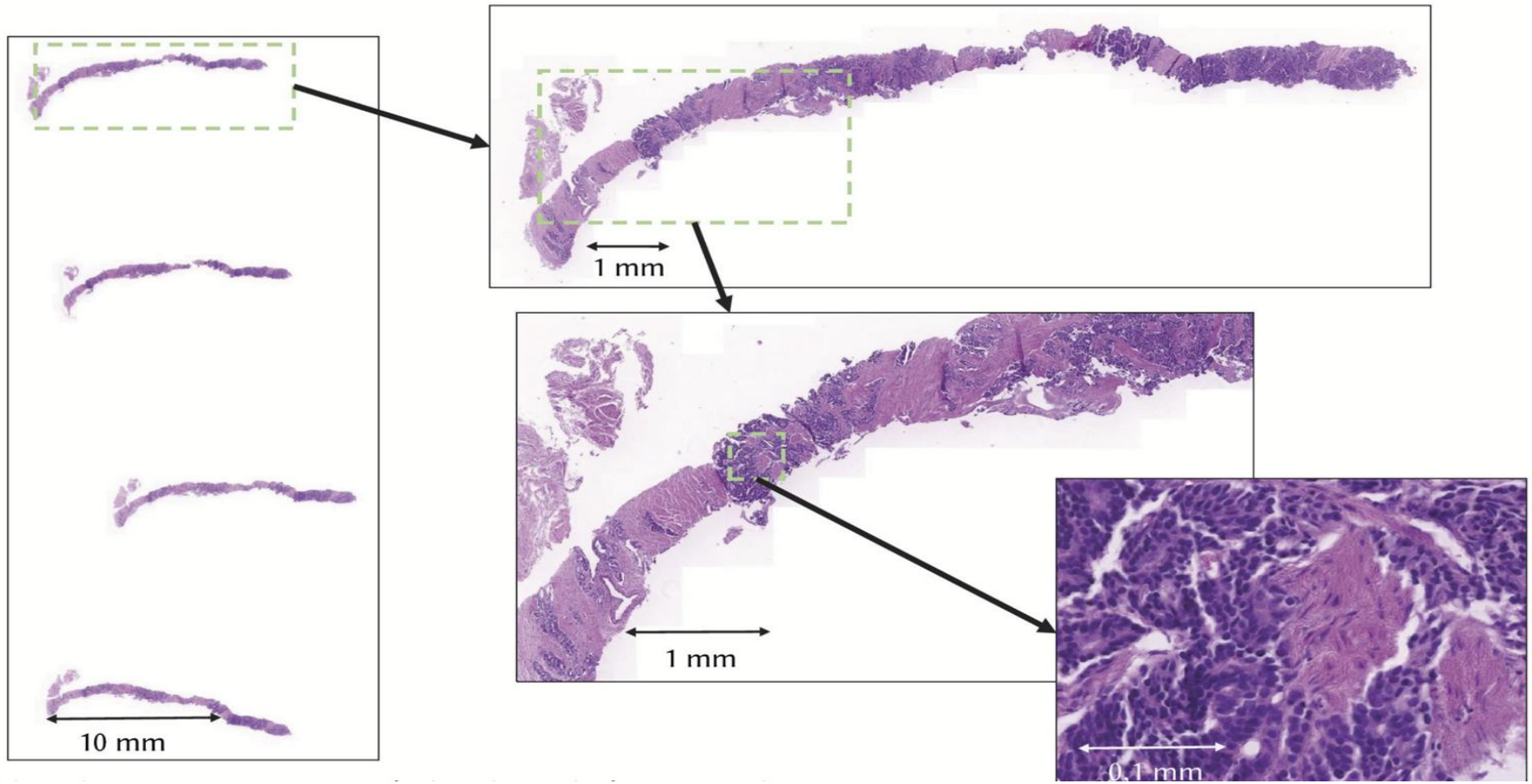
Viewer






Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | INFN | DARE DIGITAL LIFELONG PREVENTION

# Data elaboration and visualization

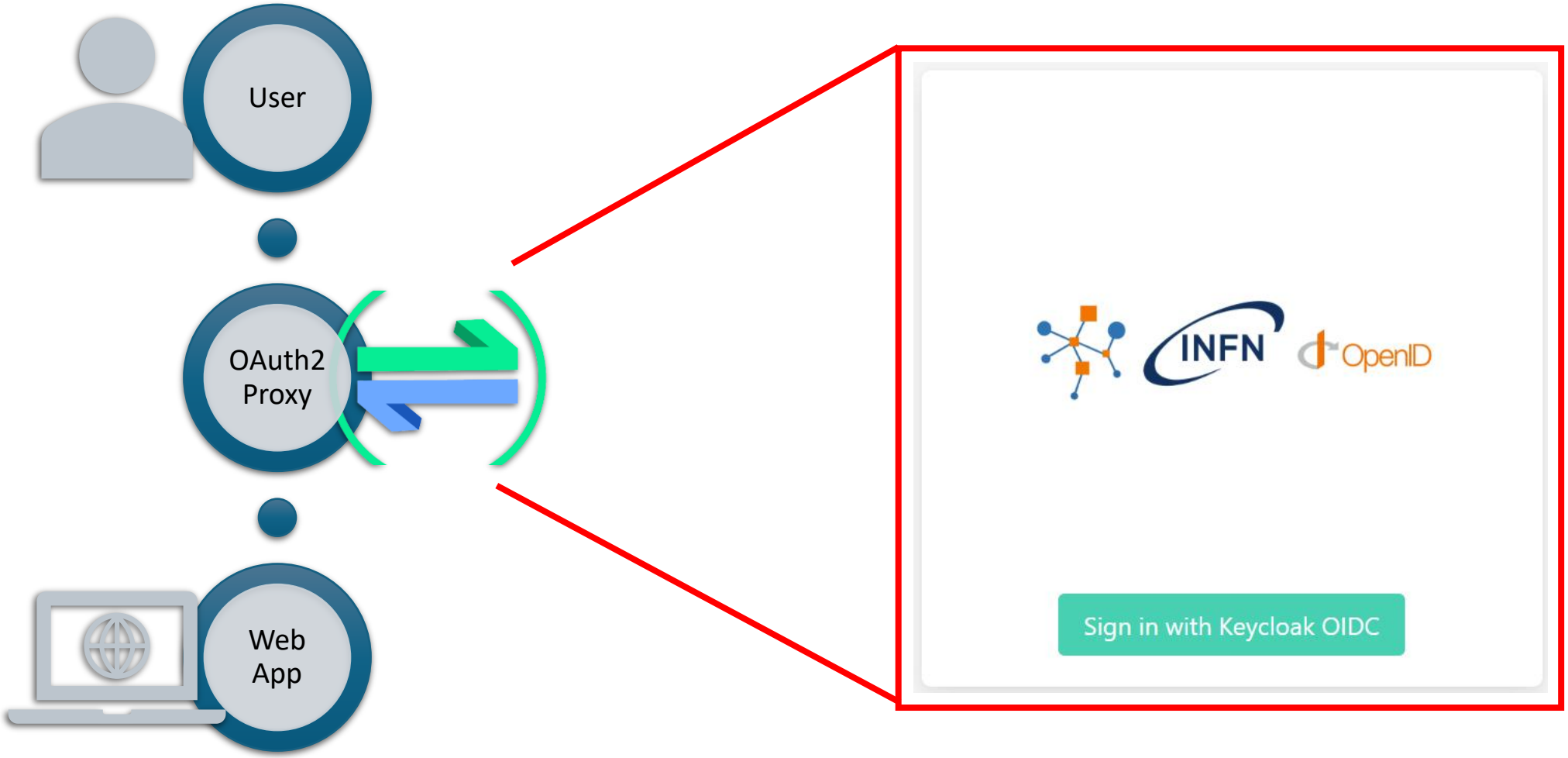



upyter

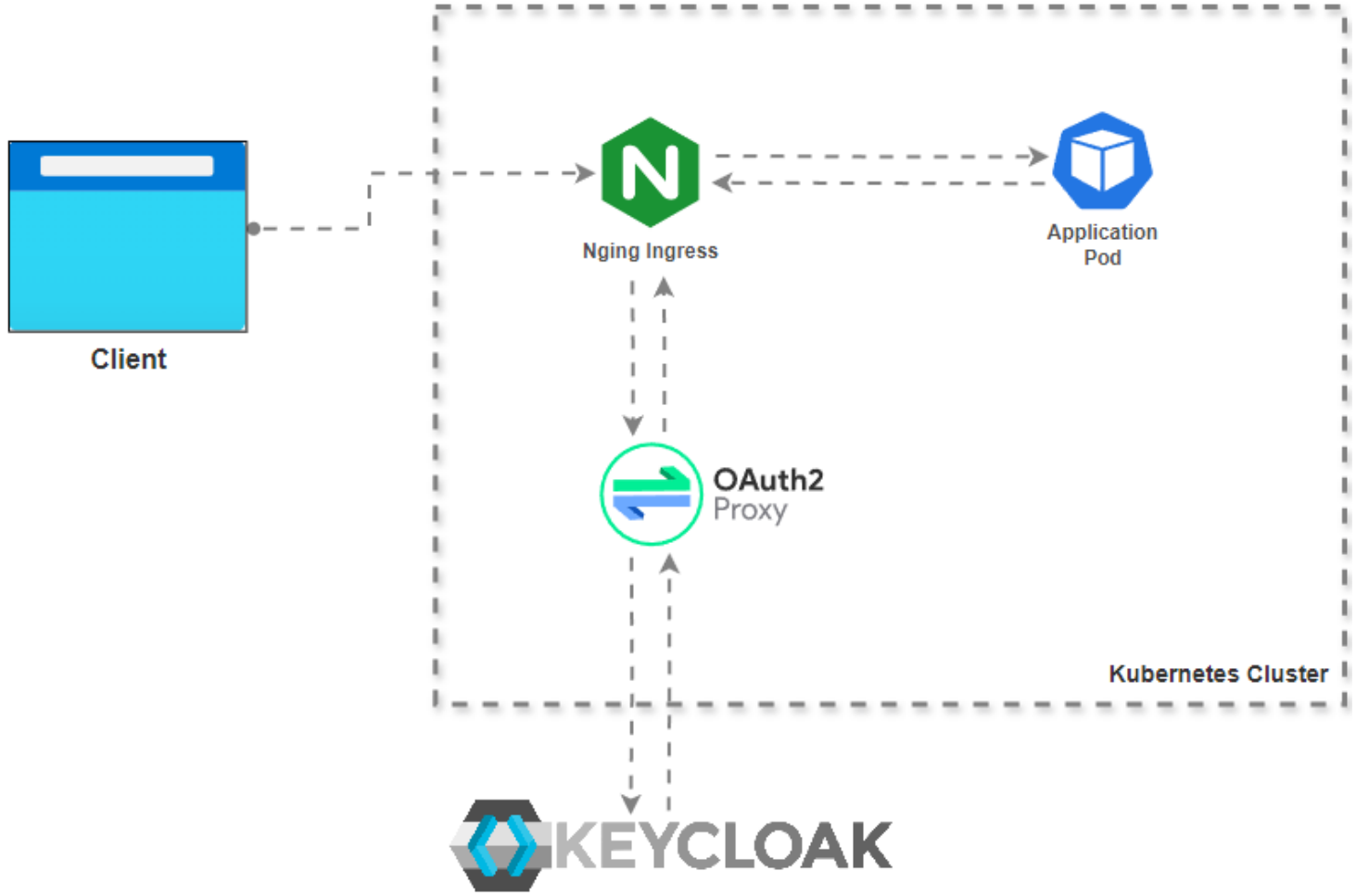
flow

iewer

# Authentication



# Authentication



# Conclusion

DARE

# Summary, issues and future prospects

## Summary

- Modern research requires collaboration

## Federation

- To facilitate collaboration, it would be beneficial to have unique authentication system o federation
- There are obvious implementation difficulties

## Improvements

- Use software that natively integrates authentication and authorization
- Best storage solutions
- Automate the infrastructure part

# Thank you

This research was co-funded by the Italian Complementary National Plan PNC-I.1 "Research initiatives for innovative technologies and pathways in the health and welfare sector" D.D. 931 of 06/06/2022, "DARE - DigitAI lifelong pRevEntion" initiative, code PNC0000002,
CUP: B53C22006450001