

Rancher managed Kubernetes for Helmholtz users

Container Orchestration



Tim Wetzel, Michael Schuh, Johannes Reppin, Patrick Fuhrmann, Uwe Jandt
HEPiX workshop 2023, Academia Sinica, Taipei, Taiwan

What is HIFIS?

Helmholtz federated IT services

- Helmholtz Association with 18 autonomous research centres in Germany
- Incubator platforms for better collaboration between centres
 - Using synergies is key!
- HIFIS is the central IT service federation platform in Helmholtz
- Very good review last year from international experts
- Centres make web services and resources available for all other Helmholtz members
- Central AAI with community attributes and integration
 - Helmholtz, EGI, eduGAIN, ...

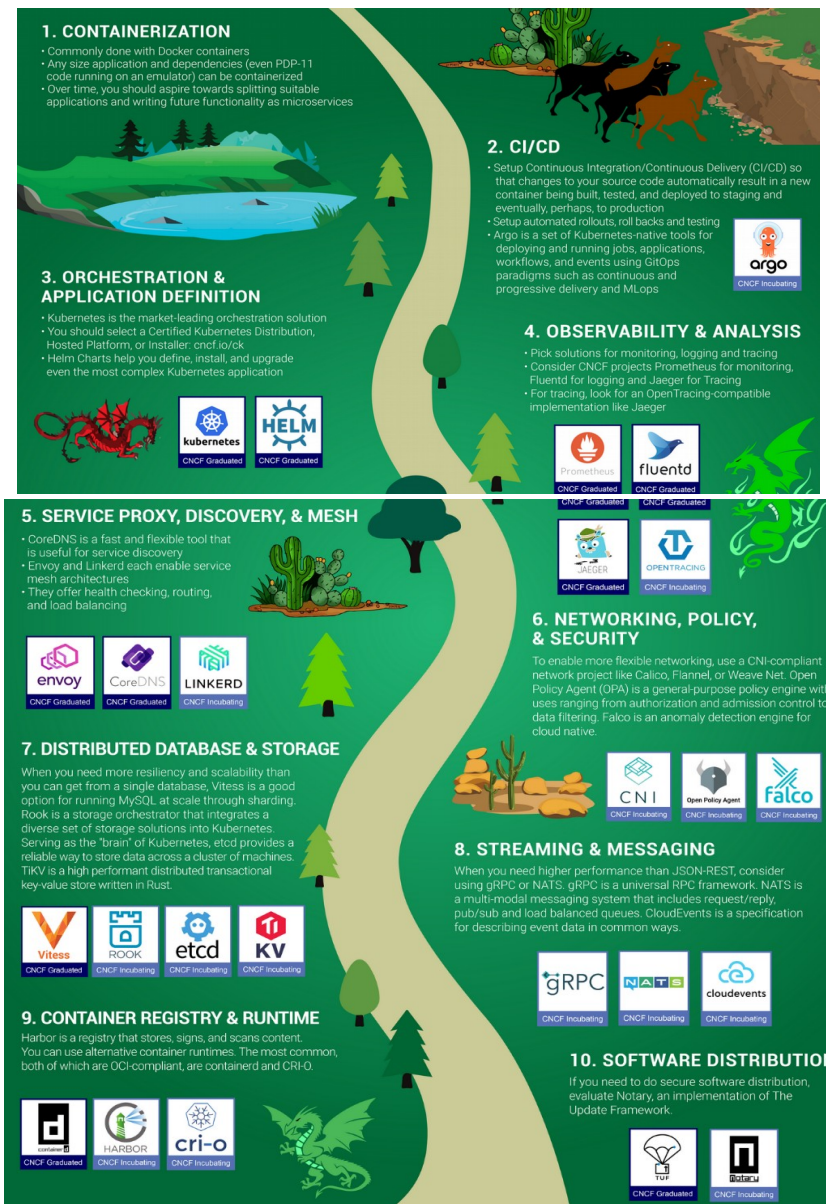


The Cloud Native Landscape

The Cloud Native Trail Map

Container orchestration

1. Containerize applications
2. CI/CD - robust automation
3. Orchestration
4. Monitoring & Analysis



Integration with research infrastructure

5. DNS, Load Balancing
6. Network Operations
 - Software-defined networking
 - Firewall
 - Dynamic certificates
7. Scientific data storage
 - dCache
 - High performance storage
 - DBaaS
8. Event streaming platforms
 - Data acquisition streams
 - Function as a service (FaaS)
9. Scale container registry
 - HPC & HTC
 - Docker / Singularity Registry
10. Software Repository
 - CVMFS
 - NIMS

Source: trailmap.cncf.io

Software stack container orchestration

Infrastructure as a Service
Cloud Computing
Infrastructure as code



Software stack container orchestration

Container as a Service

Cloud Native CI/CD

Container registry



GitLab



Infrastructure as a Service

Cloud Computing

Infrastructure as code



openstack®

Software stack container orchestration

Kubernetes as a Service

Container Orchestration

Kubernetes Package Manager



Container as a Service

Cloud Native CI/CD

Container registry



GitLab



Infrastructure as a Service

Cloud Computing

Infrastructure as code



openstack®

Software stack container orchestration

Software as a Service

Container-based environments

App deployments as code



Kubernetes as a Service

Container Orchestration

Kubernetes Package Manager



Container as a Service

Cloud Native CI/CD

Container registry



Infrastructure as a Service

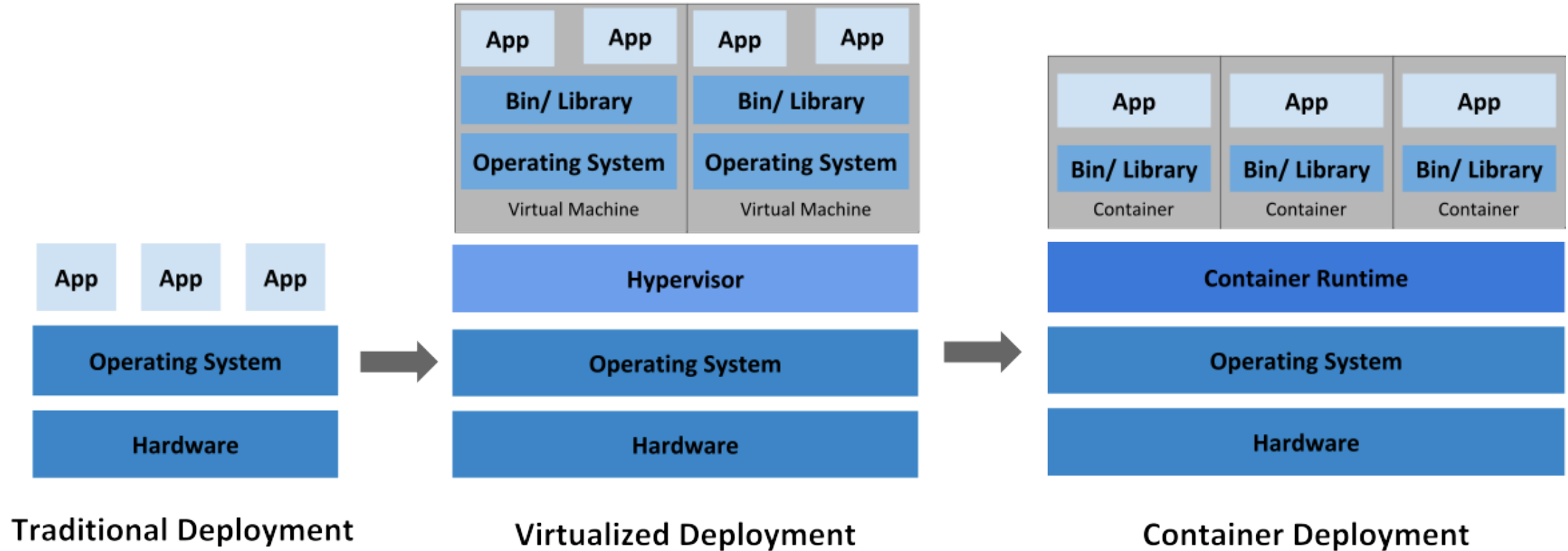
Cloud Computing

Infrastructure as code



Architecture

Infrastructure concepts

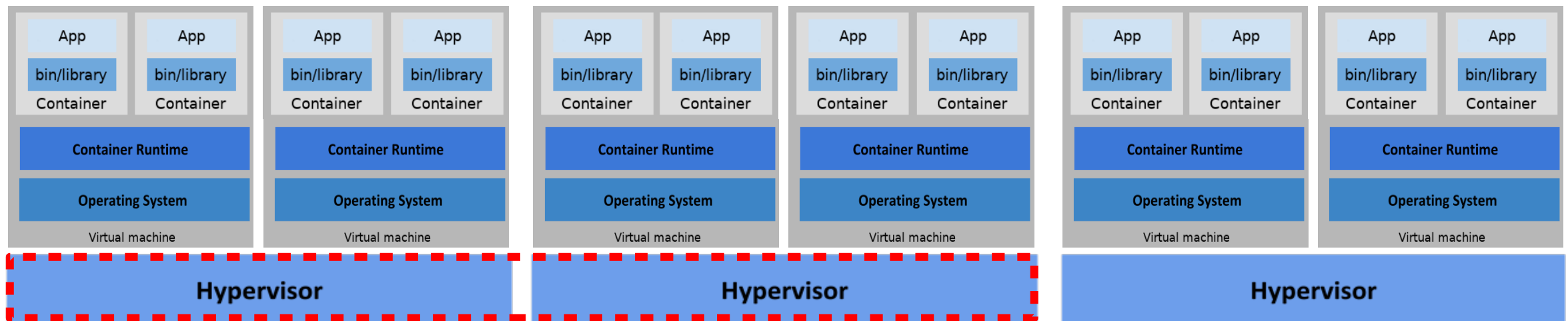


- A container image is a standalone, executable package of software that includes everything needed to run an application: code, application runtime, system tools, system libraries and settings.
- **Container images become containers at run time** and are processes (or group of processes) running in a cgroup, where the Kernel restricts resource usage (CPU, memory, disk I/O, network)

Architecture

Clusters and Schedulers

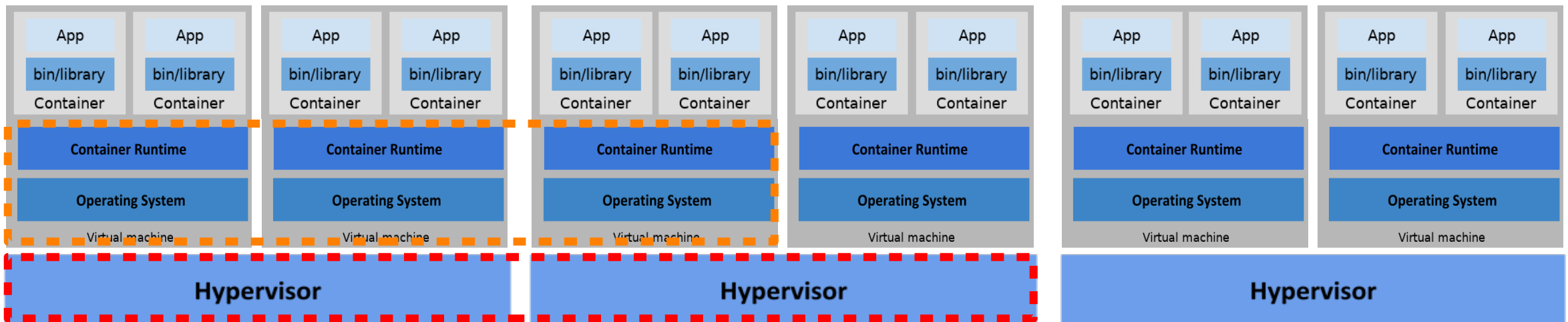
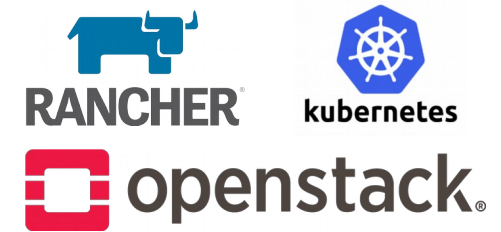
- Openstack Hypervisors organized as **Host Aggregates**
 - Openstack Nova (compute scheduler) places VMs on Hypervisors (hosts)



Architecture

Clusters and Schedulers

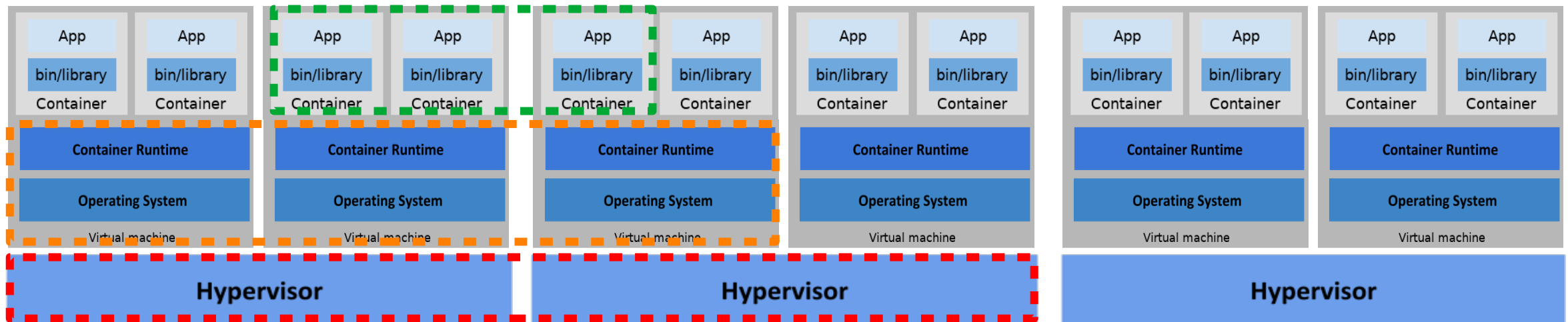
- VMs configured as Kubernetes nodes form a **Kubernetes Cluster**
 - Dynamically created by Rancher Kubernetes management platform
- Openstack Hypervisors organized as **Host Aggregates**
 - Openstack Nova (compute scheduler) places VMs on Hypervisors



Architecture

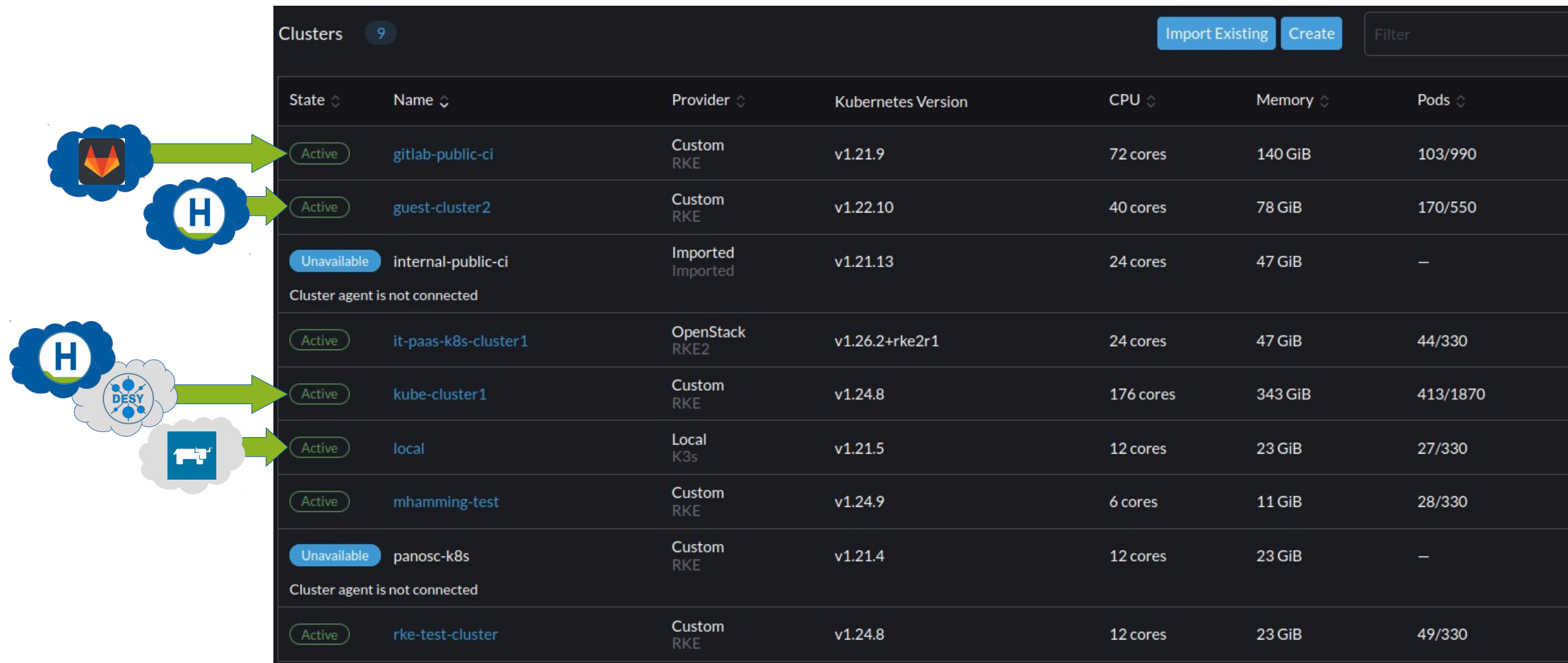
Clusters and Schedulers

- Kubernetes scheduler places containers on Kubernetes Nodes
 - Application Deployments form **Container Clusters**
- VMs configured as Kubernetes nodes form a **Kubernetes Cluster**
 - Dynamically created by Rancher Kubernetes Management platform
- Openstack Hypervisors organized as **Host Aggregates**
 - Openstack Nova (compute scheduler) places VMs on Hypervisors



Rancher

K8s cluster management and additional RBAC



The screenshot displays the Rancher Clusters management interface. At the top, there are buttons for 'Import Existing' and 'Create', and a 'Filter' input field. The main content is a table listing 9 clusters. The table columns are State, Name, Provider, Kubernetes Version, CPU, Memory, and Pods. The clusters are as follows:

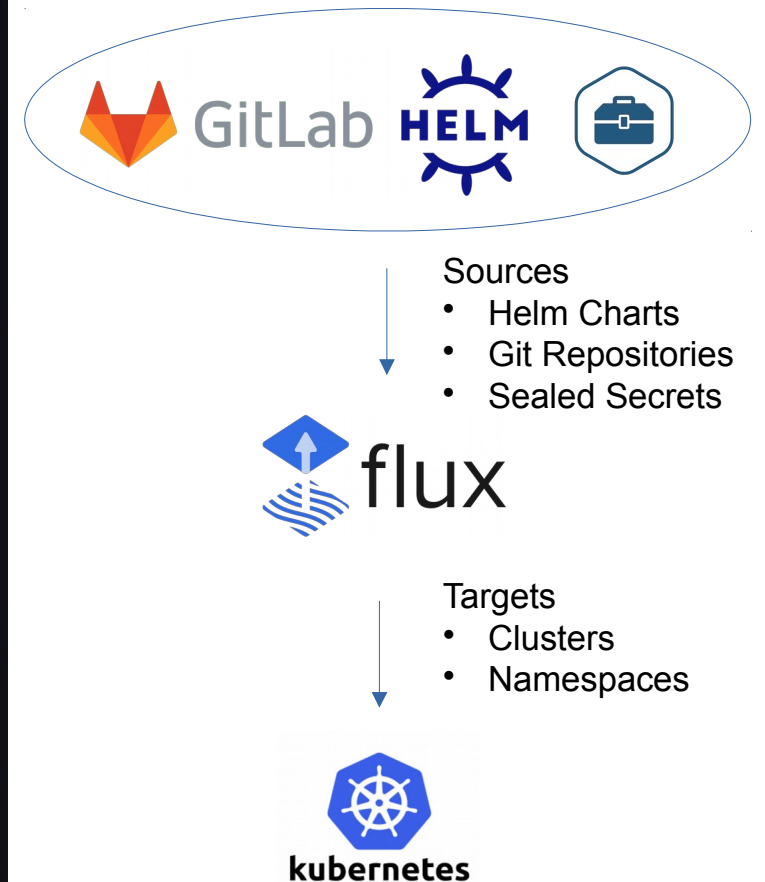
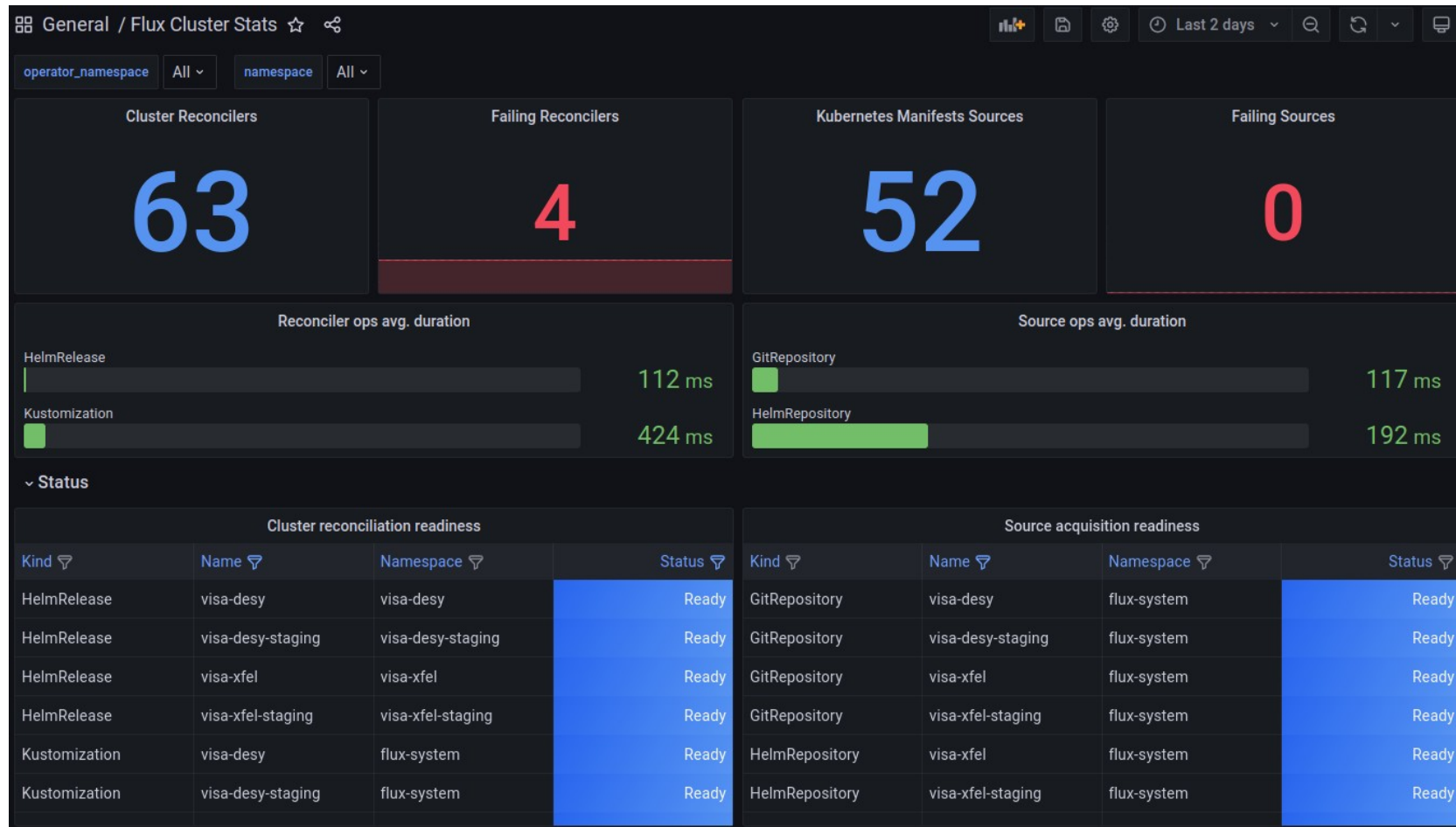
State	Name	Provider	Kubernetes Version	CPU	Memory	Pods
Active	gitlab-public-ci	Custom RKE	v1.21.9	72 cores	140 GiB	103/990
Active	guest-cluster2	Custom RKE	v1.22.10	40 cores	78 GiB	170/550
Unavailable	internal-public-ci	Imported Imported	v1.21.13	24 cores	47 GiB	—
Cluster agent is not connected						
Active	it-paas-k8s-cluster1	OpenStack RKE2	v1.26.2+rke2r1	24 cores	47 GiB	44/330
Active	kube-cluster1	Custom RKE	v1.24.8	176 cores	343 GiB	413/1870
Active	local	Local K3s	v1.21.5	12 cores	23 GiB	27/330
Active	mhamming-test	Custom RKE	v1.24.9	6 cores	11 GiB	28/330
Unavailable	panosc-k8s	Custom RKE	v1.21.4	12 cores	23 GiB	—
Cluster agent is not connected						
Active	rke-test-cluster	Custom RKE	v1.24.8	12 cores	23 GiB	49/330

Annotations on the left side of the screenshot include:

- A cloud icon with the GitLab logo and an arrow pointing to the 'gitlab-public-ci' cluster.
- A cloud icon with the Helm logo and an arrow pointing to the 'guest-cluster2' cluster.
- A cloud icon with the DESY logo and an arrow pointing to the 'kube-cluster1' cluster.
- A cloud icon with the Rancher logo and an arrow pointing to the 'local' cluster.

GitLab Integration

Flux CD and Helm Releases



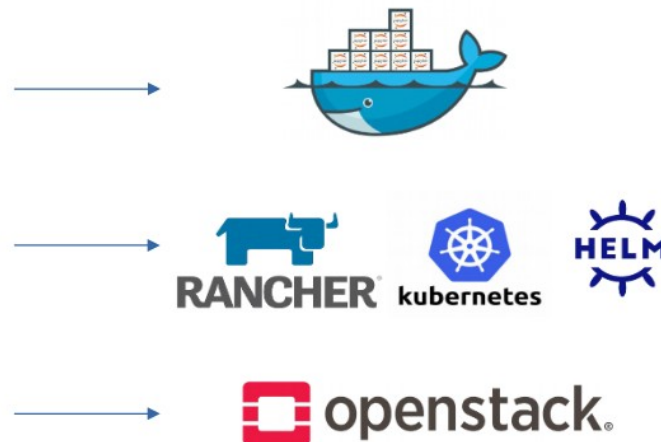
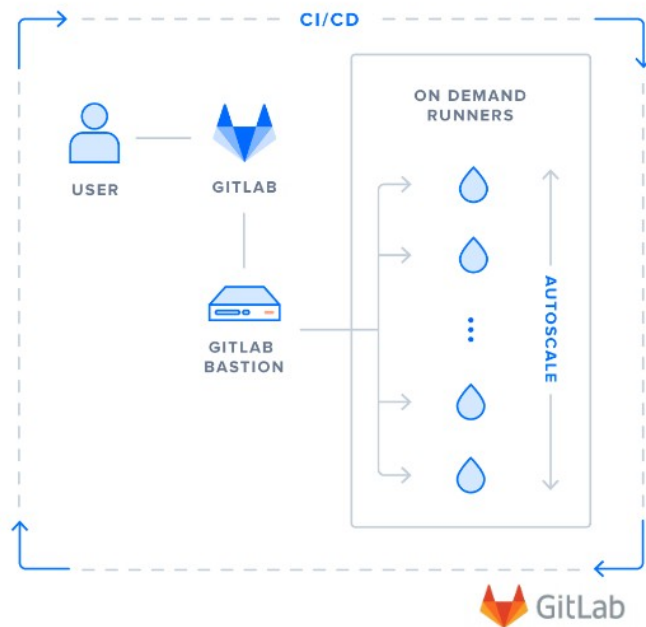
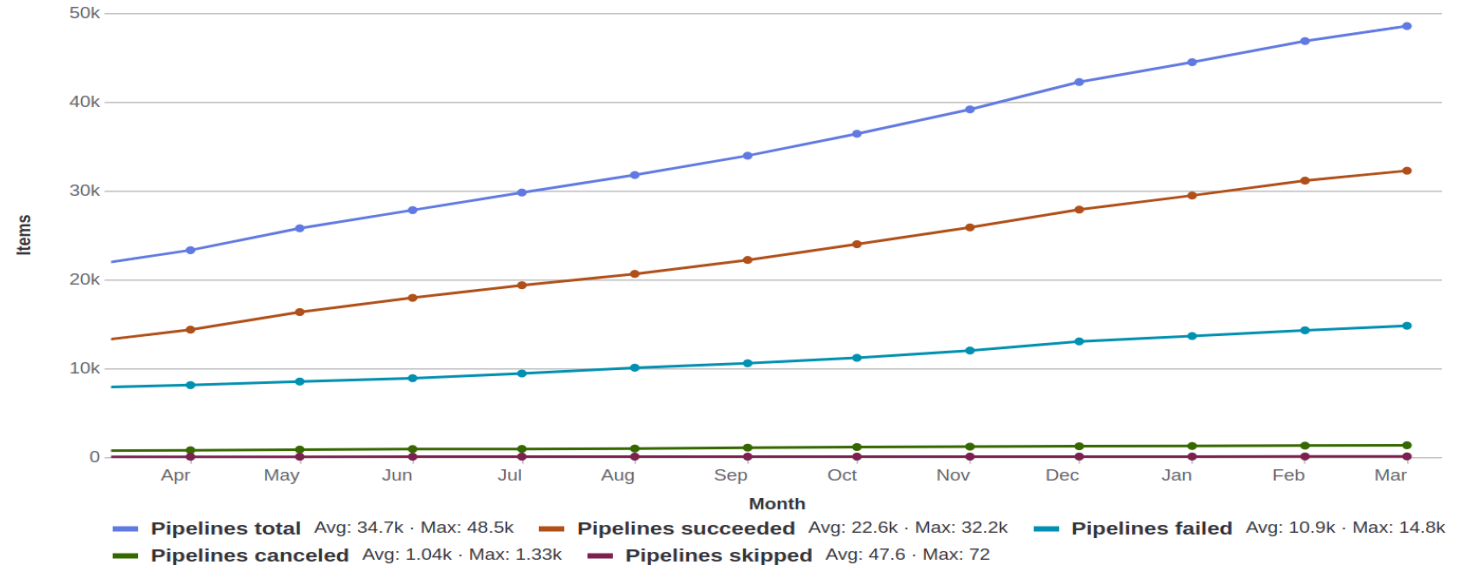
Gitlab Runners for gitlab.desy.de



Johannes Reppin, Michael Schuh – DESY IT / HIFIS, PaNOSC, ExPaNDS

Helm Deployment

- Gitlab CI/CD pipelines / jobs
- Autoscaling service
- Shared runner pilot for gitlab.desy.de
- At ~ 50k pipelines per month



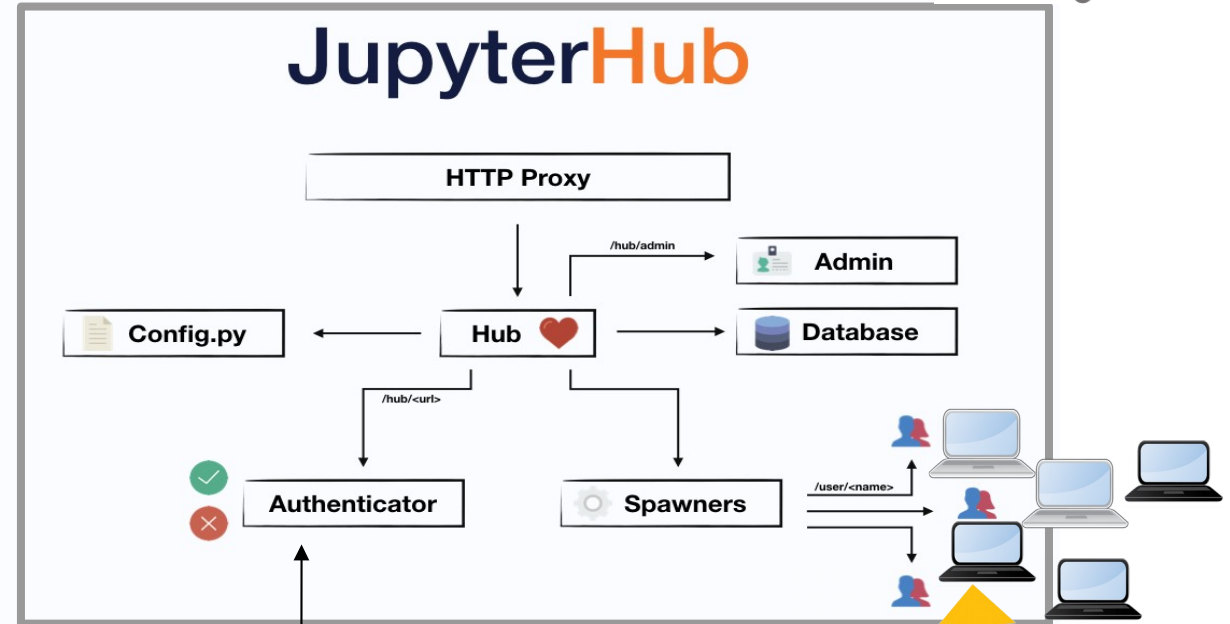
JupyterHub - jupyter.desy.de

Johannes Reppin, Tim Wetzel – DESY IT / HIFIS



Helm Deployment with Flux CD

- Merge group memberships from Helmholtz AAI in Keycloak
- Run Jupyter Servers, set UID/GIDs
- Integrate with dcache-demo.desy.de



All icons where obtain on Flaticon (<https://www.flaticon.com/packs/essential-collection>)



User Federation

- LDAP (DESY)
- OIDC (EGI Check-in)
- OIDC (Helmholtz AAI)



PetaByte Storage

- NFS Mounts

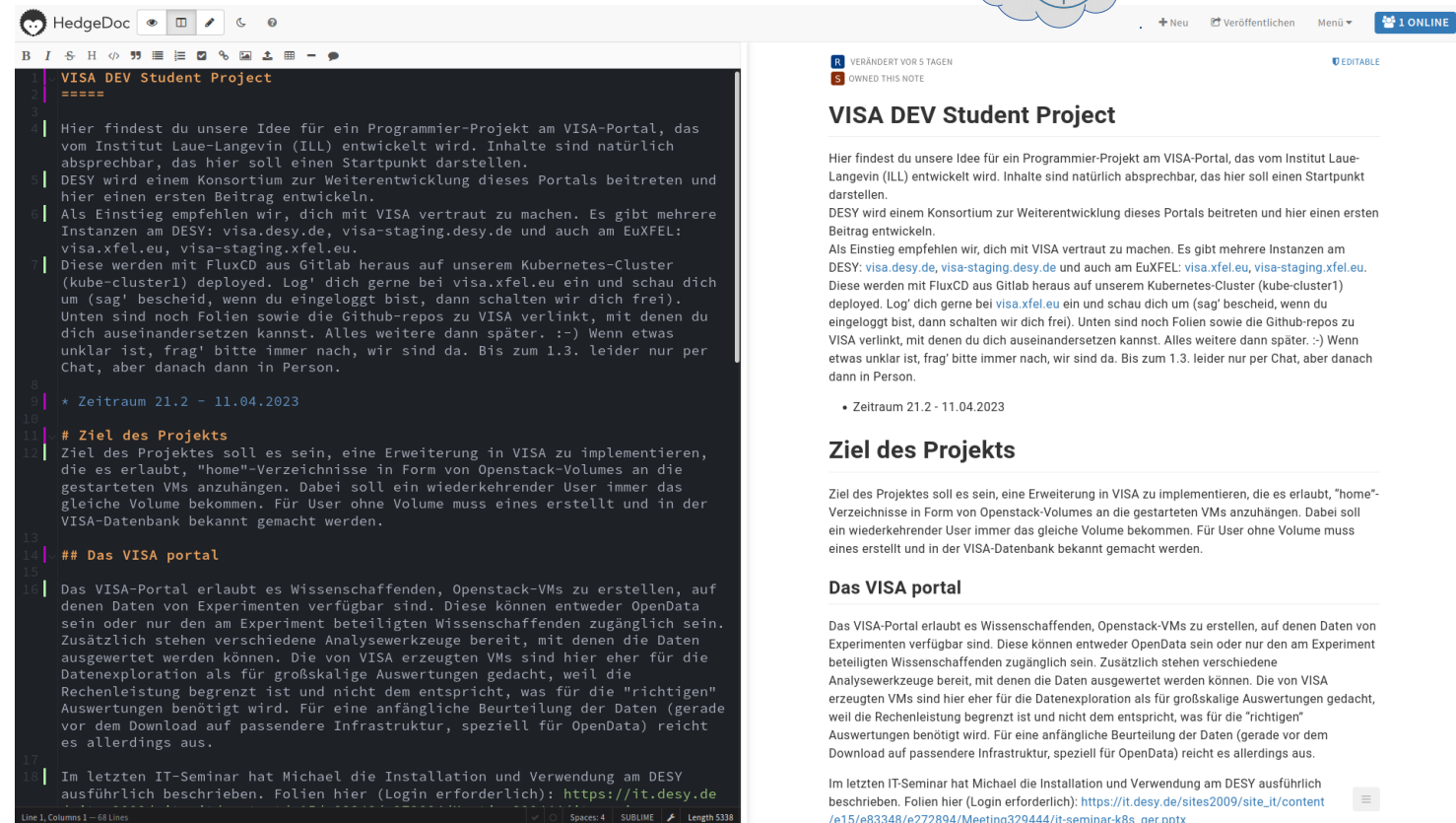
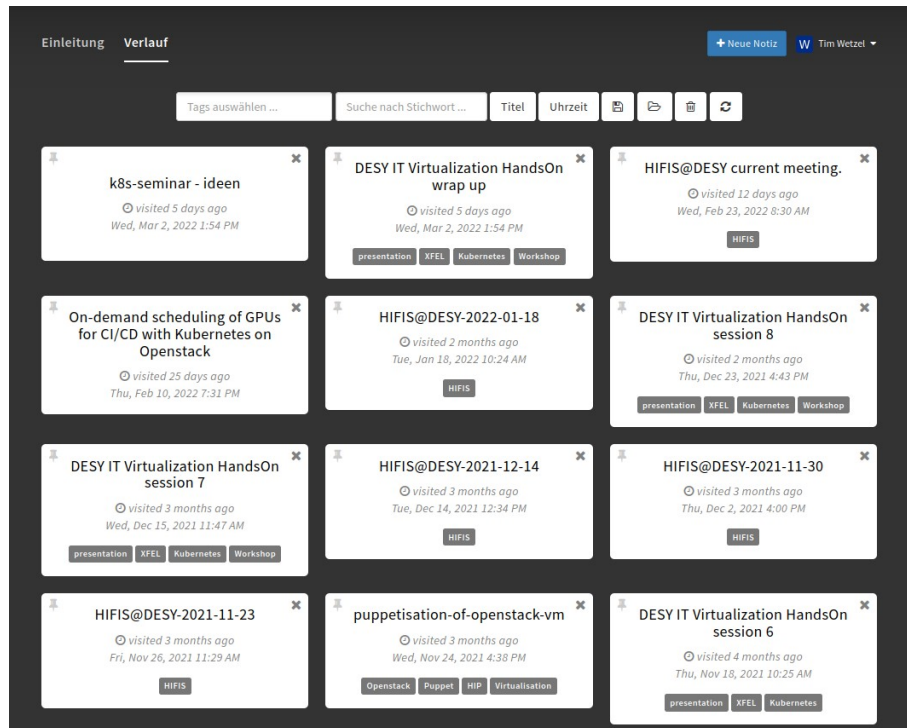
Collaborative document editing - notes.desy.de



Johannes Reppin – DESY IT / HIFIS

Helm Deployment with Flux CD

- HedgeDoc instance
- Collaborative note taking for Helmholtz
- Storage and backups via S3 on CEPH

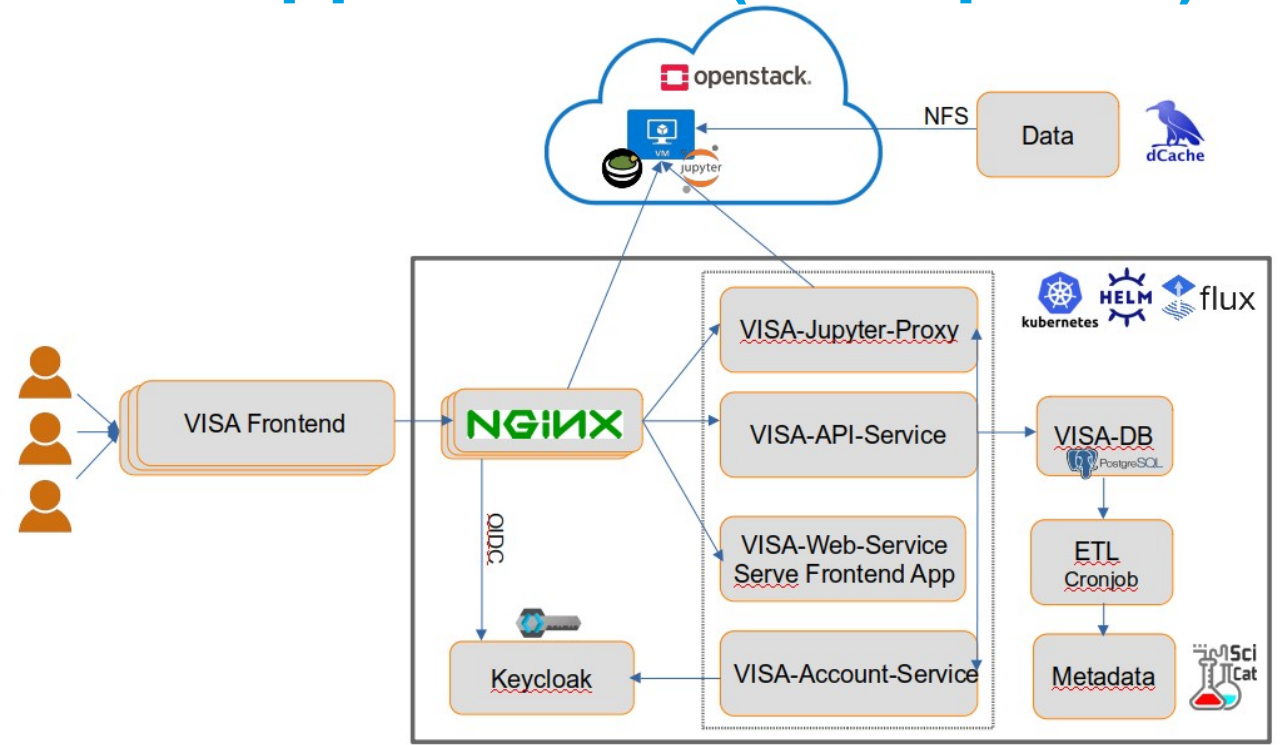


Collaborative note taking, presentation generation, LaTeX-like mathematical notation and more. More than 1.5k AAI-registered users from all Helmholtz and beyond.

Virtual Infrastructure for Scientific Applications (VISA portal)

Michael Schuh, Tim Wetzel – DESY IT

- Developed at ILL, France
- Deployed at 6+ institutes in Europe
- Scientists can spawn VMs with specific datasets mounted for data exploration after experiments
- Applications and workflows integrated into the infrastructure according to user needs



Experiments

Select the experiments you wish to associate with your compute resource.

Search for experiments

Search for your experiments using the filters below

Instrument: All instruments | between: 2017 and 2021 | with open data: included | sort by: date (newest first)

Proposal	Title	Instrument	Start Date	End Date	
p700002	FXE example data	EUXFEL-XMPL	27 Sept 2021	30 Dec 2021	SELECT
p700001	Detector Calibration Test Data	EUXFEL-XMPL	19 Jan 2019	20 Jan 2019	SELECT
CXIDB-ID-98	ExPaNDS Reference Data for Serial Crystallography	EUXFEL-SPB/SFX	30 Aug 2018	03 Sept 2018	SELECT
CXIDB-ID-103	Advances in long-wavelength native phasing at X-ray free-electron lasers	SwissFEL-Alvra	07 Aug 2018	10 Aug 2018	SELECT
p700000	Example Data	EUXFEL-XMPL	08 Nov 2017	31 Dec 2017	SELECT

Results per page: 5 | 1 - 5 of 5 experiments

VISA_Apptainer

VISA Image with Apptainer (former Singularity) preinstalled.

VISA_CrystFEL

VISA Image with latest CrystFEL installed.

Choose hardware requirements

4 Cores

8GB memory

Large

8 Cores

16GB memory

XLarge

Helmholtz Cloud Portal - cloud.helmholtz.de



Thomas Beermann, Sebastian Wagner - DESY IT / HIFIS

- Service discovery portal for Helmholtz federated web service
- Allows users to find, understand and access services in Helmholtz
- Service quotas, access, monitoring to be integrated into portal
- Communication channel between services and portal in development
- Developed and hosted at DESY
- Code available on Helmholtz codebase
- Deployed on k8s via CI/CD pipelines
- Testing, monitoring, dependency management & error detection integrated into pipelines

Helmholtz Cloud

In the Helmholtz Cloud, members of the Helmholtz Association of German research centers provide selected IT-Services for joint use.

Note: Helmholtz Cloud is currently in pilot phase and will go in production when the legal framework is finalised.

[BROWSE ALL SERVICES](#)

Find more information at hifis.net

HELMHOLTZ CLOUD

Services Team News Helpdesk About Sign in

Search services Select Keywords Select Providers Select Software Sort Services

B2Share B2SHARE, based on Invenio Research Data (+ corresponding Metadata) Publishing service. JÜLICH Storage Description Go to service	bwSync&Share Nextcloud File Sync and Share, Groupware-Functionalities: Files, Fotos, Calendar, etc. KIT Collaboration Sync & Share Description Go to service	Collabtext Overleaf Collaborative document writing with LaTeX HZDR Collaboration Information Description Go to service	Compute Projects Slurm Apply for Computing Time at Jülich Supercomputing Centre (JSC). JÜLICH Infrastructure Supercomp... Description Go to service
Container-Runtime Aptainer Container runtime environment on HPC systems at FZJ / Jülich Supercomputing Centre (JSC). JÜLICH Infrastructure Supercomp... Description Go to service	Data Projects (HDF) JARDS Apply for data projects at FZJ / Jülich Supercomputing Centre (JSC). JÜLICH Infrastructure Supercomp... Storage Description Go to service	GPU compute Service Jupyter Jupyter Notebooks on GPU Nodes containing Nvidia A100 GPUs. HZDR Infrastructure Supercomp... Description Go to service	HAICORE HAICORE Dedicated Computing Resources for the Helmholtz AI community. KIT Infrastructure Supercomp... Description Go to service
HAICORE HAICORE Dedicated Computing Resources for the Helmholtz AI community. JÜLICH Infrastructure Supercomp... Description Go to service	Helmholtz Codebase GitLab A web-based DevOps lifecycle tool that provides a Git-repository manager. HZDR Infrastructure Collaboration Description Go to service	Helmholtz RSD Research Software Directory Promote and discover research software developed in the Helmholtz Association. GFZ Science Database Description Go to service	HIFIS Events Indico An Events Management service for everyone within Helmholtz and their partners, based on Indico. Indico Collaboration Description Go to service

PIA eResearch system (<https://info-pia.de>)



Castell, Heise, Klett-Tammen, Barohn, Jemric, Steguweit – Helmholtz Centre for Infection Research (HZI); Xapling and Inqode

- System for conducting epidemiologic studies and repetitive surveys
- Available as web and mobile application for participants
- Currently built on docker-compose (see figure)
- Development for k8s-ready version facilitated with HIFIS resources
- Onboarding and introduction to the infrastructure via video call between project lead, developers and DESY team
- Access to Rancher / k8s cluster given live
- Ticket queue and chat for support by DESY
- Colleagues at HZI satisfied by onboarding and platform stability

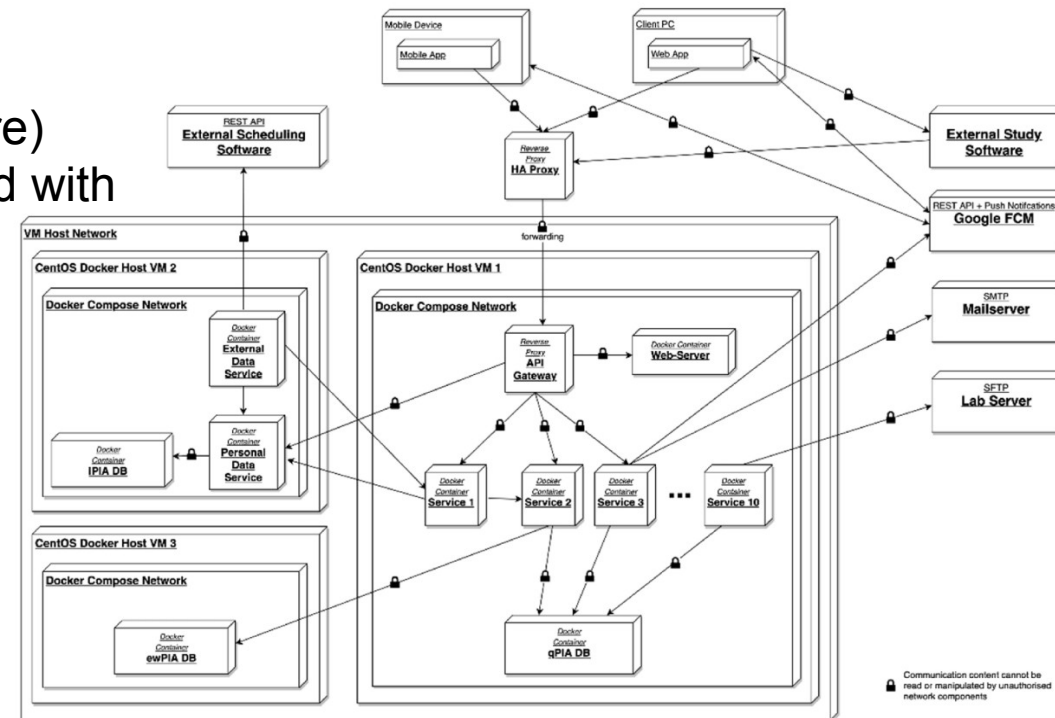
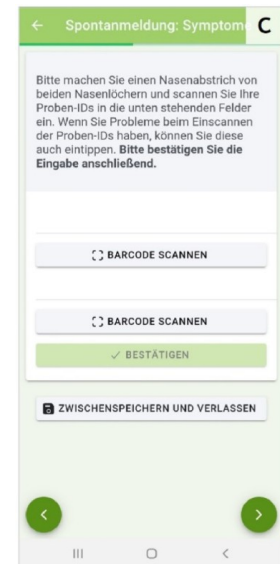
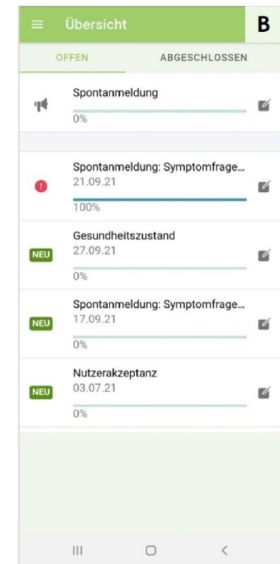


Fig. 1. Formalisation of network environment of PIA (basic version without connection to SORMAS).

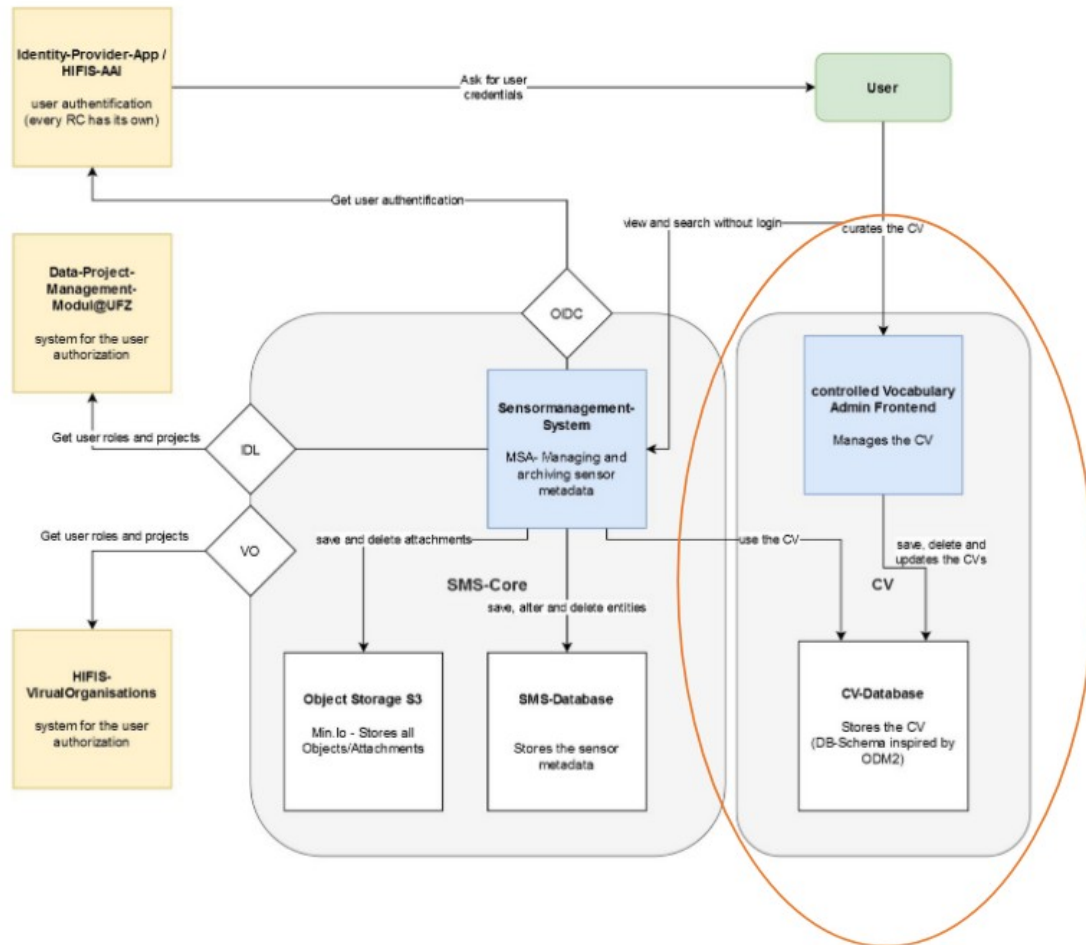
Heise et al. „Putting digital epidemiology into practice: PIA- Prospective Monitoring and Management Application“, 2022 Informatics in Medicine Unlocked 30



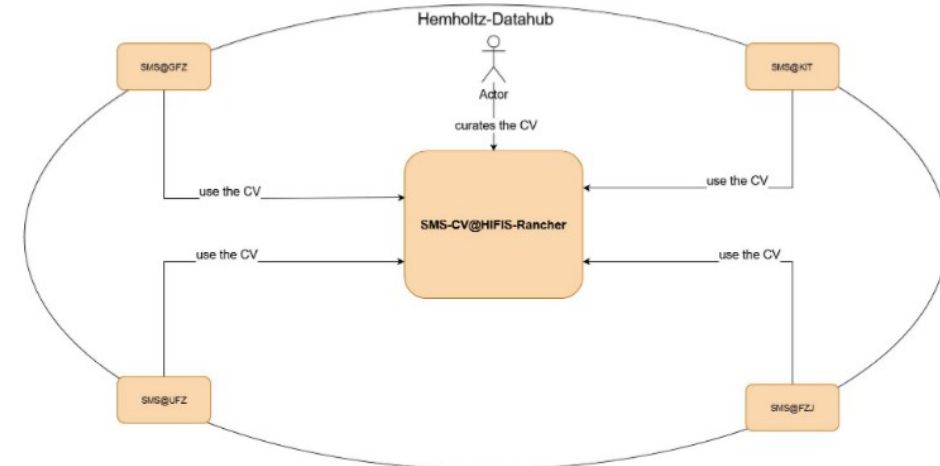
Sensor Management System – Controlled Vocabulary



Norman Ziegner, Daniel Sielaff – Helmholtz Centre for Environmental Research (UFZ)



- Sensor Management for environmental research
- Distributed systems for measurement campaigns
- Sensor metadata administrated in SMS
- Metadata is shaped by controlled vocabulary (CV)
 - Ensures FAIRness
 - Instance hosted in Kubernetes@DESY

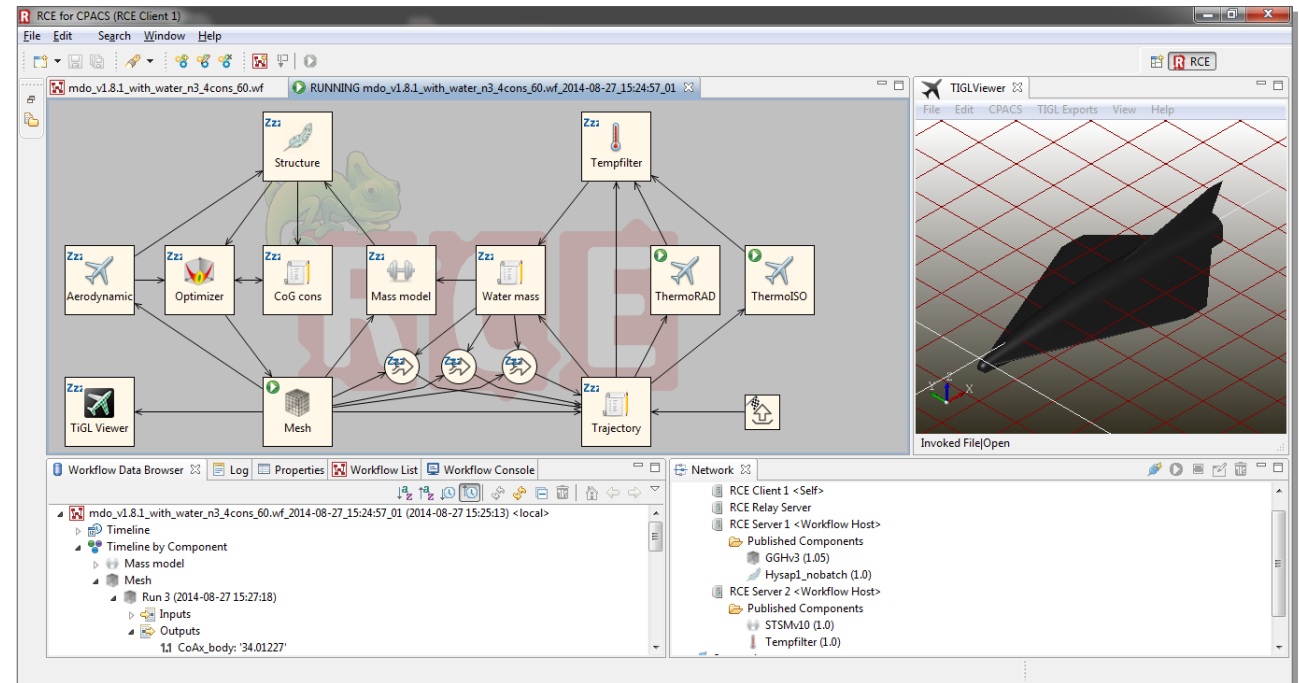
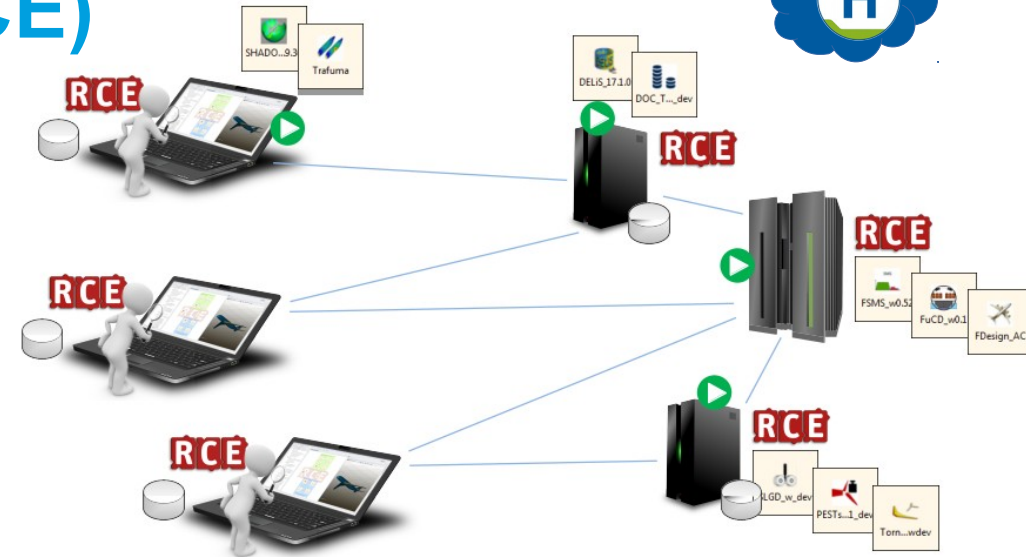


Remote Component Environment (RCE)

Robert Mischke – German Aerospace Center (DLR)



- Open Source integration environment for distributed workflows (<https://rcenvironment.de/>)
- Comes with GUI, batch mode, external tool integration, ...
- Used for simulation and design of aircraft, ships and their impact on climate and environment
- Automated creation and disposal of test networks of distributed software (like RCE) for automated system testing on Kubernetes@DESY
- Automated deployments and chaos testing for resiliency optimization



Summary

- Kubernetes clusters for use within DESY as well as for Helmholtz users via HIFIS
- Managed by Rancher instance for dynamical cluster deployments and additional RBAC
- Many internal & external use cases already hosted on clusters
 - Jupyter, Keycloak, HedgeDoc, Gitlab runners, ...
 - Helmholtz Cloud Portal, VISA Portal, SciCat, ...
 - Use cases from 5 other Helmholtz Centres

Outlook

- Exploring feasibility of k8s deployments on bare metal by DESY colleagues
- Better integration with Gitlab-agent (currently only for cluster admins)
- Optimization of cluster deployments with Terraform for easy base cluster spawning
- Strategy development for individual service backups
- Monitoring solution for external users' services
- ...

Thank you

Contact

DESY.

Michael Schuh

IT-RIC

michael.schuh@desy.de

Tim Wetzel

IT-RIC

tim.wetzel@desy.de

Johannes Reppin

IT-INFA

johannes.reppin@desy.de

Deutsches Elektronen Synchrotron

www.desy.de