Sovereign Cloud Stack

gaia-x

Sovereign Cloud Stack

Open Source Cloud & Container Stack for Federated Sovereign Infrastructure (Gaia-X)

Sovereign Infrastructure for Sovereign Data Processing

Dr. Manuela Urban, **Kurt Garloff**, Dirk Loßack, Eduard Itrich,
Felix Kronlage-Dammers, Bianca Hollery-Pfister (OSB Alliance e.V.)

project@scs.sovereignit.de

CloudLand, Brühl, 2022-06-29

CloudLand

OSB Open Source Business ALLIANCE
Bundesverband für digitale Souveränität e.V.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Sovereign Cloud Stack

An OSB ALLIANCE project

CloudLand

GCC

SUSE

T-Systems

Open Telekom Cloud

OSB Open Source Business ALLIANCE

Bundesverband für digitale Souveränität e.V.

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

openstack.

OSISM

EFF

guug

German Unix User Group

LINUX VERBAND

SPRIN-D

DPG

gaia-x

Mainstream truth in EU, mid 2015

A big war in Europe in inconceivable. We don’t need well-working defense.

It’s OK for Europe to strongly depend on natural gas from Russia.

Britain won’t leave the European Union.

The Americans won’t elect an immature bully.

It’s OK for Euope to strongly depend on US IT platforms.

Safe Harbor sufficiently protects personally-identifiable data transferred to the US.

.

.

.

.

Mid 2017

A big war in Europe in inconceivable. We don’t need well-working defense.

It’s OK for Europe to strongly depend on natural gas from Russia.

~~Britain won’t leave the European Union.~~

~~The Americans won’t elect an immature bully.~~

It’s OK for Euope to strongly depend on US IT platforms.

~~Safe Harbor sufficiently protects personally-identifiable data transferred to the US.~~

Privacy Shield sufficiently protects personally-identifiable data transferred to the US.

.

.

.

Mid 2020

A big war in Europe in inconceivable. We don't need well-working defense.

It's OK for Europe to strongly depend on natural gas from Russia.

~~Britain won't leave the European Union.~~

The Americans won't elect an immature bully again.

It's OK for Euope to strongly depend on US IT platforms.

~~Safe Harbor sufficiently protects personally-identifiable data transferred to the US.~~

~~Privacy Shield sufficiently protects personally-identifiable data transferred to the US.~~

US clouds hosted in European Data Centers are safe to use for personally identifiable data

.

.

Sovereign Cloud Stack
An OSB ALLIANCE project

CloudLand

Mid 2022

~~A big war in Europe in inconceivable. We don't need well-working defense.~~

~~It's OK for Europe to strongly depend on natural gas from Russia.~~

~~Britain won't leave the European Union.~~

??? The Americans won't elect an immature bully again.

??? It's OK for Euope to strongly depend on US IT platforms.

~~Safe Harbor sufficiently protects personally-identifiable data transferred to the US.~~

??? Privacy Shield 2.0 sufficiently protects personally-identifiable data transferred to the US.

~~US clouds hosted in European Data Centers are safe to use for personally identifiable data~~

??? Trustee models (EU operated "sovereign" clouds with US tech) fulfill GDPR and sovereignty

??? Confidential Computing avoid all these problems with trust and sovereignty requirements.

We love illusions …

… to avoid cognitive dissonance
… to avoid questioning taken decisions

Digital Sovereignty ... What?

aws

Google Cloud

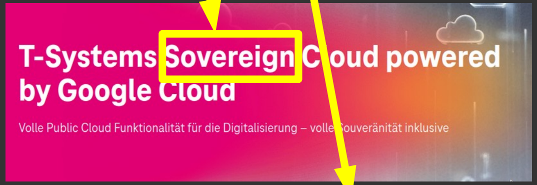
Azure

Alibaba Cloud

HUAWEI

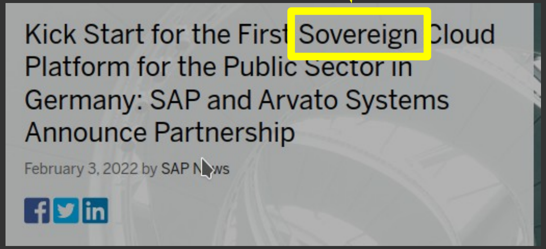
ORACLE CLOUD

HETZNER



T-Systems Sovereign Cloud powered by Google Cloud

Volle Public Cloud Funktionalität für die Digitalisierung – volle Souveränität inklusive



Kick Start for the First Sovereign Cloud Platform for the Public Sector in Germany: SAP and Arvato Systems Announce Partnership

February 3, 2022 by SAP News

vmware vCloud

NUTANIX

STACKIT

CLOUD & HEAT

IONOS

Open Telekom Cloud

OVH.com

Stack HPC

WAVECON

cleura

gridscale

plusserver

DigitalOcean

VEXXHOST

Fragmentation

Digital Sovereignty

„There must [...] be a sovereign government. Sovereignty is supreme authority, an authority which is independent of any other earthly authority. Sovereignty in the strict and narrowest sense of the term includes, therefore, independence all around, within and without the borders of the country.“

- LFL Oppenheim, 1905

“Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf. Sie umfasst weiterhin die Fähigkeit, technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen.

– Digitale Souveränität und Künstliche Intelligenz, Digitalgipfel 2018

https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5

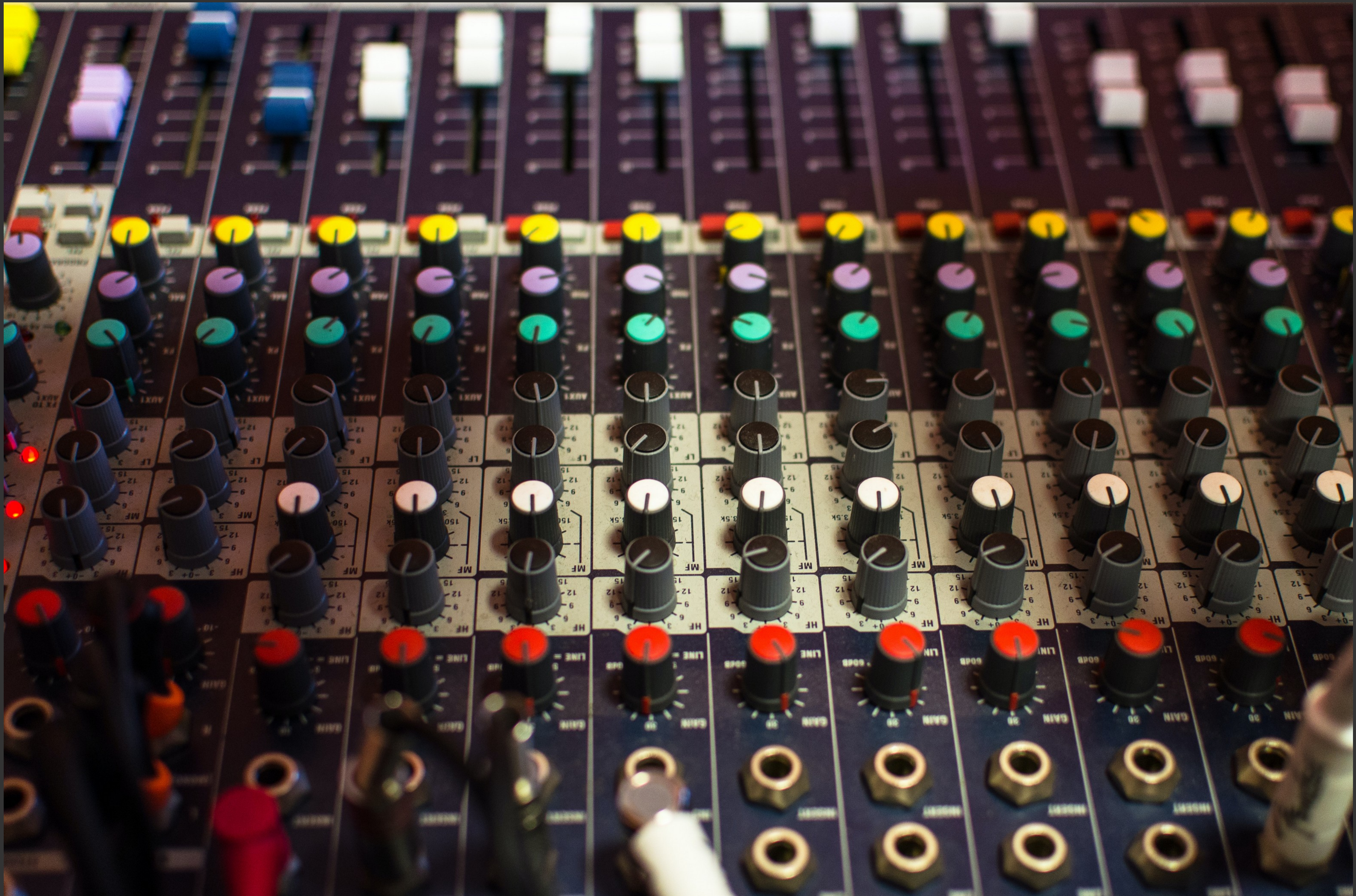
Digital Sovereignty – Open Source

OpenInfra SUMMIT · BERLIN '22
THE INTERSECTION OF OPEN SOURCE TECHNOLOGIES AND DIGITAL SOVEREIGNTY
FREDERIC LARDINOIS
TECHCRUNCH
>> AND
DR. FRANZISKA BRANTNER
FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION
OpenInfra SUMMIT >
OpenInfra SUMMIT > BERLIN '22

“Digital Technology and Digital Sovereignty […] and we define it as the capacity to be able to act and to reduce vulnerabilities.
So it’s twofold. The one is really to reduce your weaknesses, where others can attack you.
And the other side is to be able to innovate, to develop by yourself, to set your own standards, to define the values you want to see in technology.
[…]
[Sovereign Tech Fund is specifically for open source software?] Only!”

https://www.youtube.com/watch?v=ZlPLGmBfaVc

Who is in control? Who can act?



Levels of sovereignty

0	1	2	3	4
None	Data security & protection	Choice	Shape Technology	Operational Skills
	GDPR ENISA Gaia-X labels	Strong Interoperability Many Vendors / Operators	Software Transparency *Fully* Open Source Open Development Open Community	Operational Transparency Education Open Operations

the cloud report

Digital Sovereignty

The Cloud Report 1/2022 https://the-report.cloud/
https://scs.community/de/2022/03/18/digital-sovereignty-whitepaper/

A pig with a lipstick …

Image used with friendly permission from Massively Overpowered

Local data centres of non-EU platforms

- Cloud Act

Confidential Computing

- Data decrypted for processing (exc homomorphic)
- Availability issue remains

Local operations (with partner)

- Availability issue only partially solved
- No choice, no ability to shape

“Open”

- Open Standards w/o Open Ref Implementation
- Open Core / partial Open Source
- Closed communities
- No Operational knowledge sharing

“Transparent”

- No public Root Cause Analysis
- Very filtered public monitoring / status

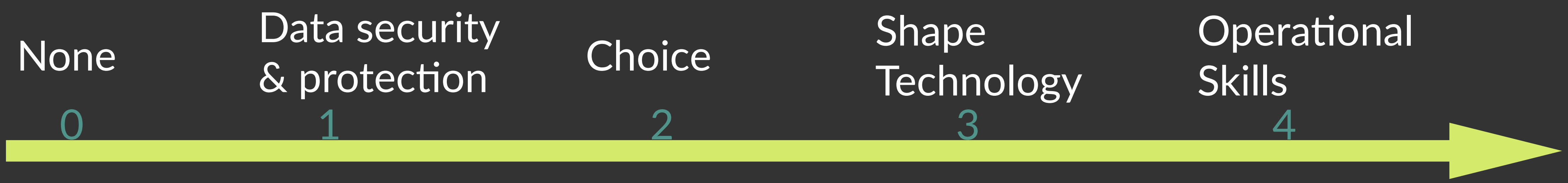
Regulation meets reality

Regulation alone won’t cut it

Sovereign Cloud Stack
An OSB ALLIANCE project

CloudLand

Sovereign Cloud Stack vision



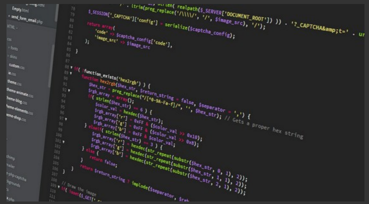
the cloud report

Digital Sovereignty

Achieve all levels of digital sovereignty

1) GDPR / Data protection / Data security / availability

2) Real choice by many (collaborating!) providers with strong interoperability: Standardization, Certification, Federation



3) Fully open functional stack (Four Opens, OSS Health Check) as modular reference implementation

4) Full transparency over operations stack, operational practices, status, RCAs (Open Operations)

Avoiding fragmentation

gaia-x

Sovereign Cloud Stack project

Started end of 2019

Funded by BMWK (German Fed. Min. for Economic Affairs & Climate Action) since summer 2021

Run by Open Source Business Alliance e.V. with half a dozen employees (growing to a dozen)

Open Community contributions

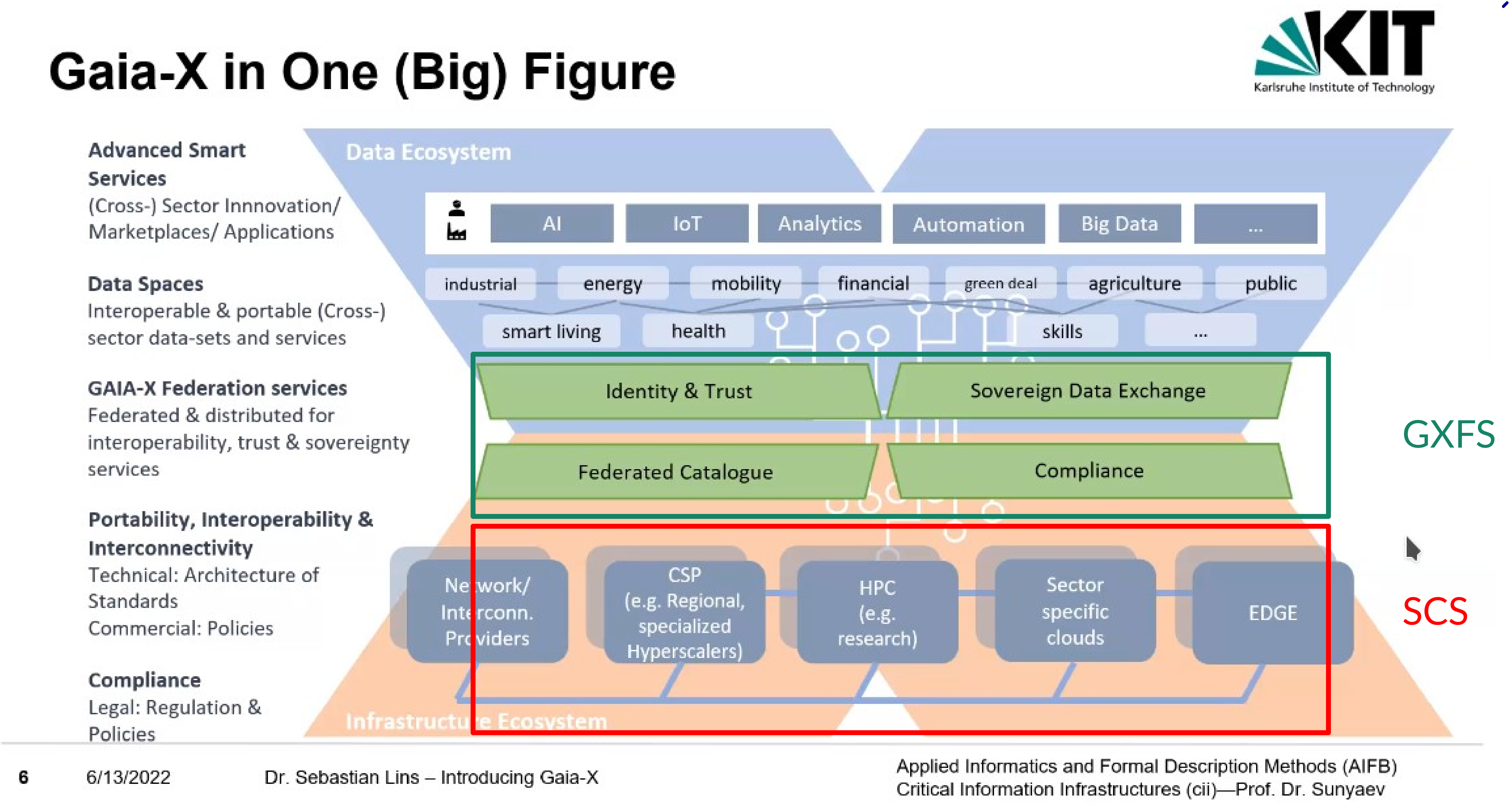
Paid contractor work (awarded via public tenders)

Closely working with Gaia-X

SCS project is neutral orchestrator within the SCS ecosystem, partners do business as CSP, services providers, etc.

Project page: https://scs.community/

Sovereign Cloud Stack and Gaia-X



Gaia-X in One (Big) Figure

Advanced Smart Services
(Cross-) Sector Innnovation/ Marketplaces/ Applications

Data Spaces
Interoperable & portable (Cross-) sector data-sets and services

GAIA-X Federation services
Federated & distributed for interoperability, trust & sovereignty services

Portability, Interoperability & Interconnectivity
Technical: Architecture of Standards
Commercial: Policies

Compliance
Legal: Regulation & Policies

6 6/13/2022 Dr. Sebastian Lins – Introducing Gaia-X

Applied Informatics and Formal Description Methods (AIFB)
Critical Information Infrastructures (cii)—Prof. Dr. Sunyaev

Sovereign Cloud Stack deliverables

Make it easy to provide a modern sovereign platform

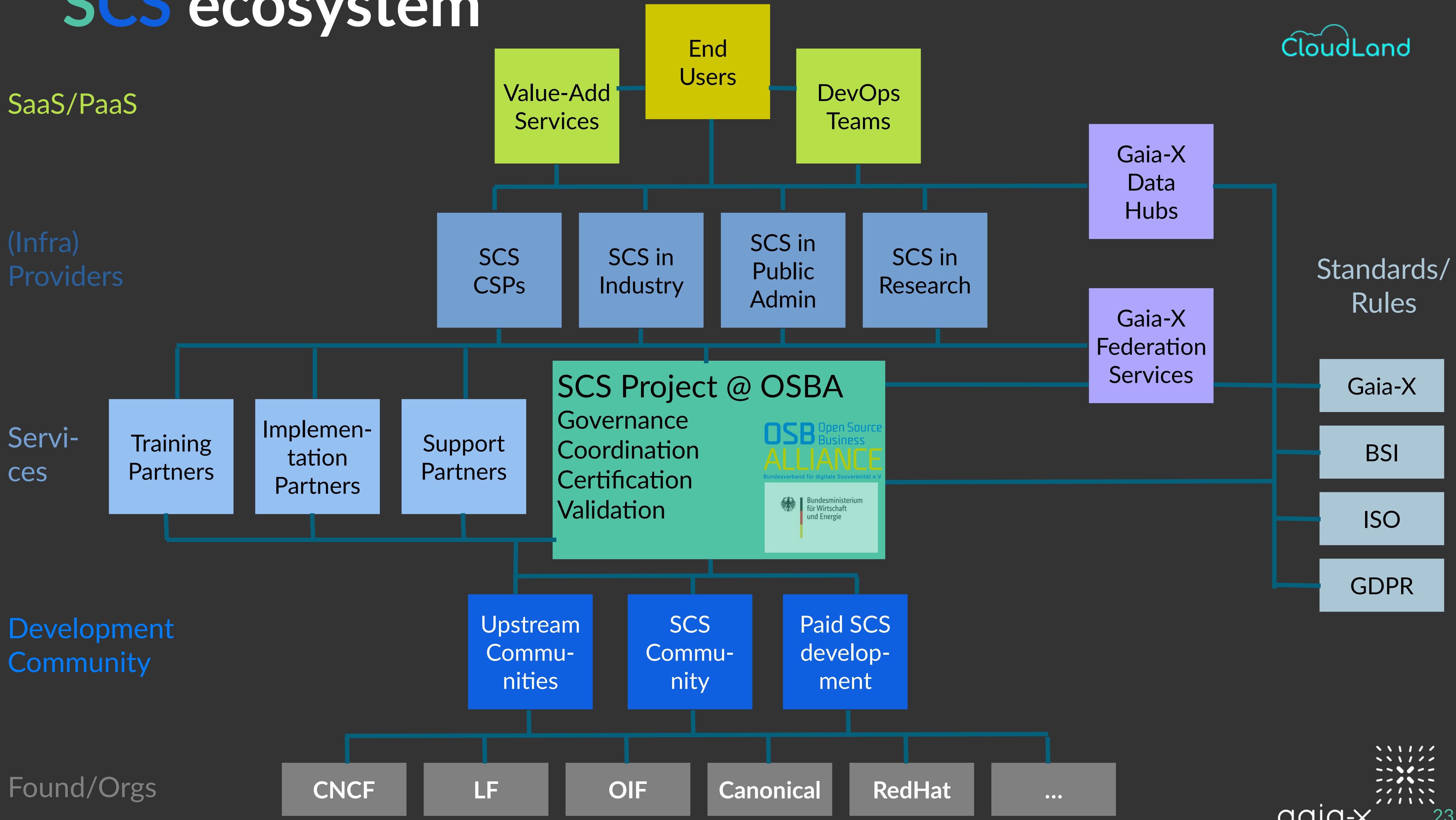
Project to create an open ecosystem & community to deliver a

1. Secure platform
2. that delivers certifiable compatible standards for federatable cloud & container platforms
3. with a complete, fully (4x) open, modular, automated reference implementation
4. along with tools, best practices and transparency for operating these dynamic distributed platform

Sovereign Cloud Stack
An OSB ALLIANCE project

CloudLand

SCS ecosystem



SaaS/PaaS

Value-Add Services

End Users

DevOps Teams

Gaia-X Data Hubs

(Infra) Providers

SCS CSPs

SCS in Industry

SCS in Public Admin

SCS in Research

Standards/ Rules

Gaia-X Federation Services

Servi-ces

Training Partners

Implemen-tation Partners

Support Partners

SCS Project @ OSBA
Governance
Coordination
Certification
Validation

OSB Open Source Business ALLIANCE
Bundesverband für digitale Souveränität e.V.

Bundesministerium für Wirtschaft und Energie

Gaia-X

BSI

ISO

GDPR

Development Community

Upstream Commu-nities

SCS Commu-nity

Paid SCS develop-ment

Found/Orgs

CNCF

LF

OIF

Canonical

RedHat

...

gaia-x

1 - Security by Design

Using strong isolation for container clusters

- Different tenants receive their own Kubernetes clusters; by default, no cluster sharing happens
- Underlaying VMs, network, storage are separated by strong virtualization barriers

Private registry for users

- Make it easy for DevOps teams to enforce their own security vetting processes and control their supply chain
- Vulnerability scanning included in regristry solution

Daily patching supported

- The architecture is built for daily patching (or redeployment) without noticable customer impact
- This creates a practice of keeping the systems up to date especially with respect to security patches

Secure Operational practices

- Document updating, patching, security response, … processes to help with secure operations

Air gap mode supported

- Deploying and updating without internet connection possible
- Leveraging an internal registry and patch distribution mechanism (includes vulnerability scanning)

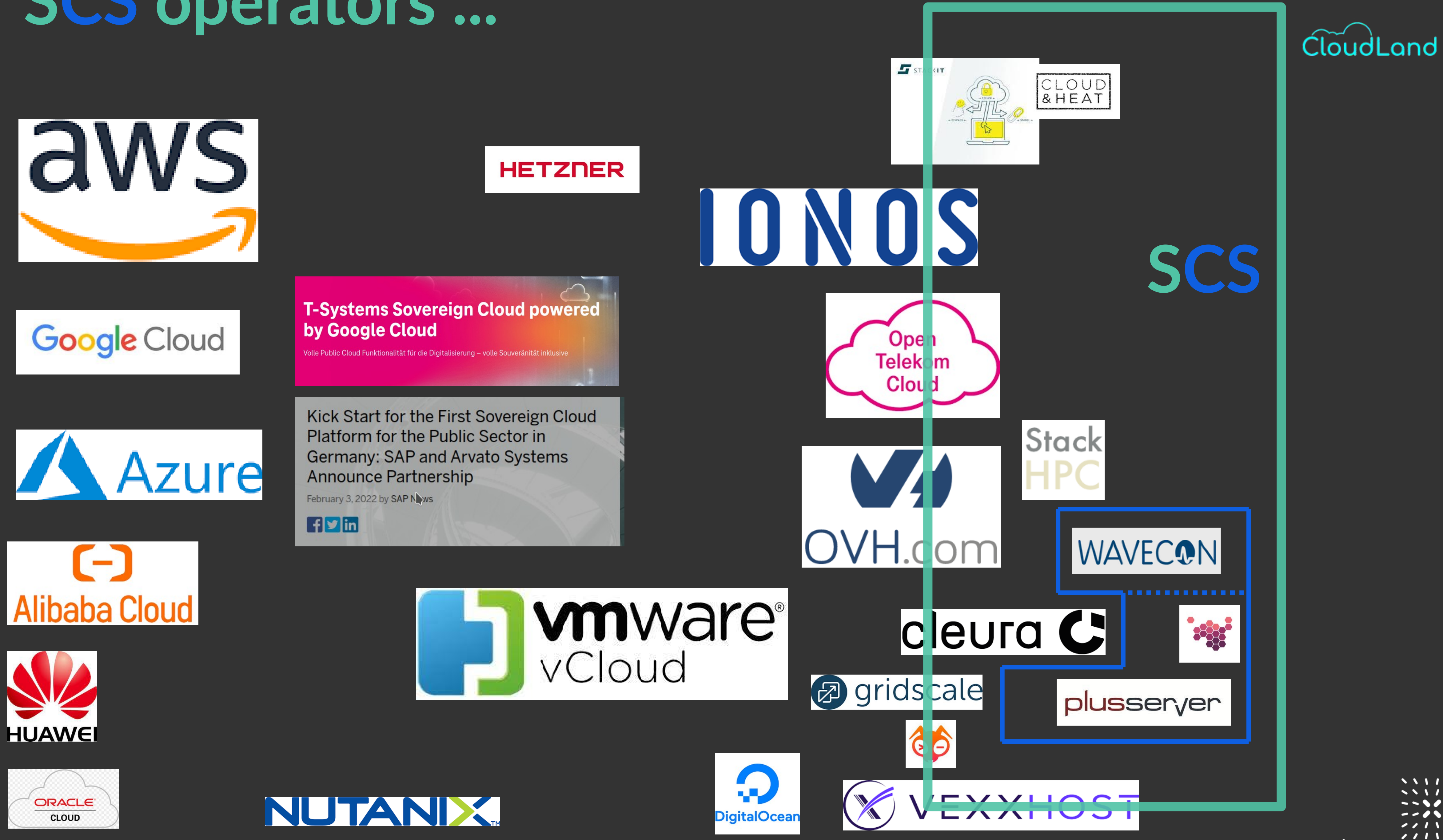
Certification

- Budget for security certifications (BSI) with partners – SCS based PlusCloud Open achieved BSI C5 in Nov 2021
- Pen testing planned (and budget allocated)

Supply chain security

- Work with researchers on further improving supply chain security (reproducible builds, scanning, …)

SCS operators ...



T-Systems Sovereign Cloud powered by Google Cloud

Volle Public Cloud Funktionalität für die Digitalisierung – volle Souveränität inklusive

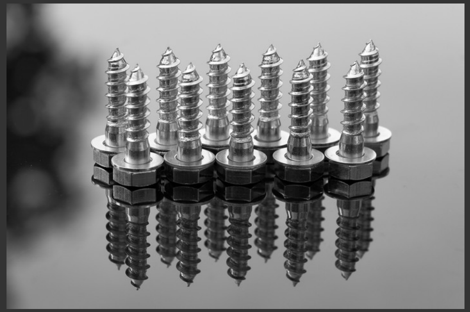
Kick Start for the First Sovereign Cloud Platform for the Public Sector in Germany: SAP and Arvato Systems Announce Partnership

February 3, 2022 by SAP News

2 - SCS standards & certification

Reuse existing Open Standards

- Must have a fully open and capable (reference) implementation
- Ideally with conformance tests
- Examples: CNCF conformance tests, S3, OIDC, OpenStack powered trademark tests
- Contribute improvements (e.g. tests) back upstream
- Gaia-X self-descriptions (in development)



SCS: Fill gaps (for PaaS/SaaS DevOps teams)

- Done: IaaS flavor naming and standard flavors
- Done: Image metadata
- WIP: Definition of regions, availability zones, …
- WIP: k8s cluster management (k8s cluster-API)

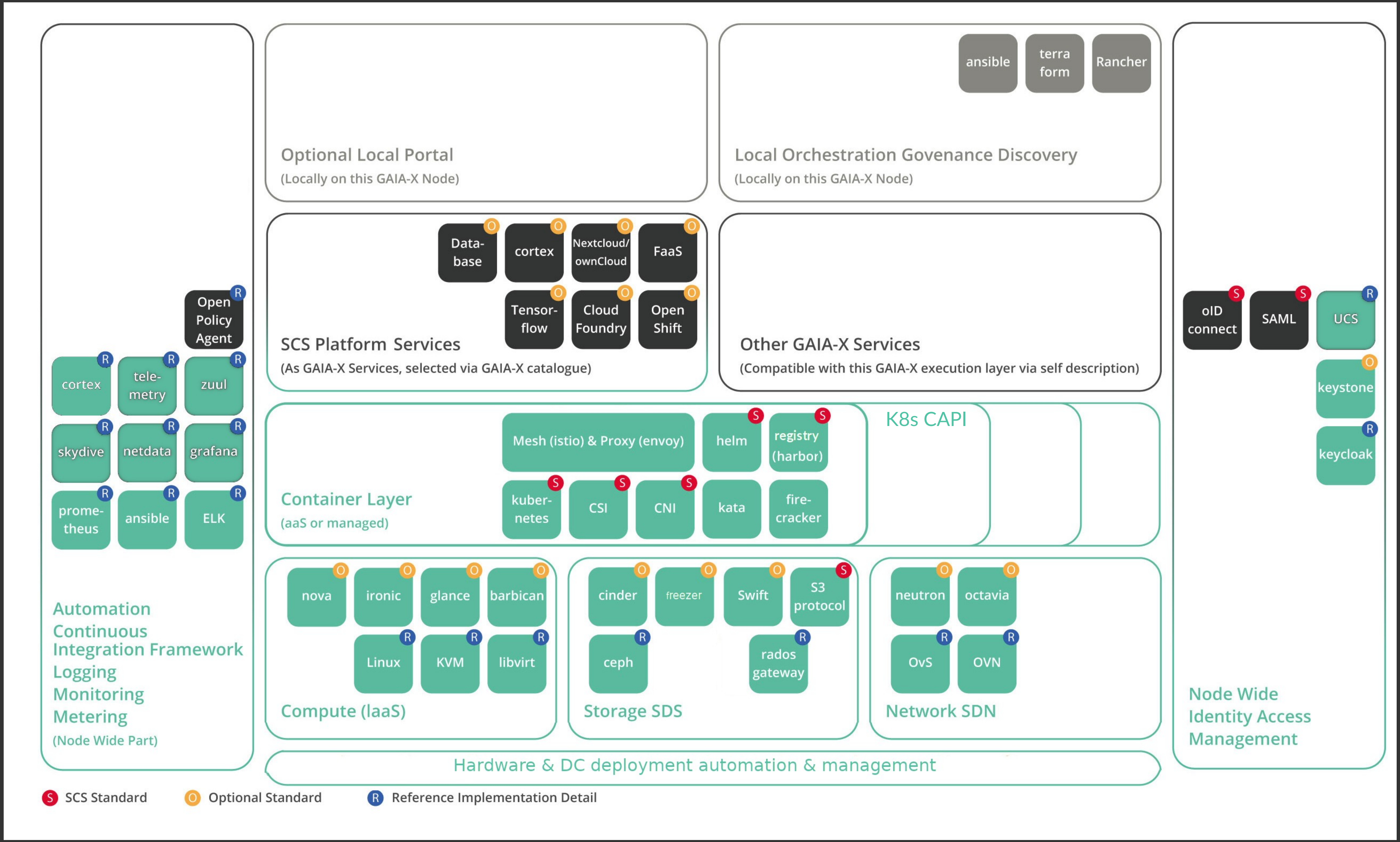
Federation

- Allow OIDC user federation

Formal SCS certification program to be launched this summer for CSPs

- SCS compatible: Compatibility / Interoperability testing
- SCS open: Technological transparency (fully open functional stack)
- SCS sovereign (later): Operational transparency

3 - SCS reference implementation architecture



LOKI

=

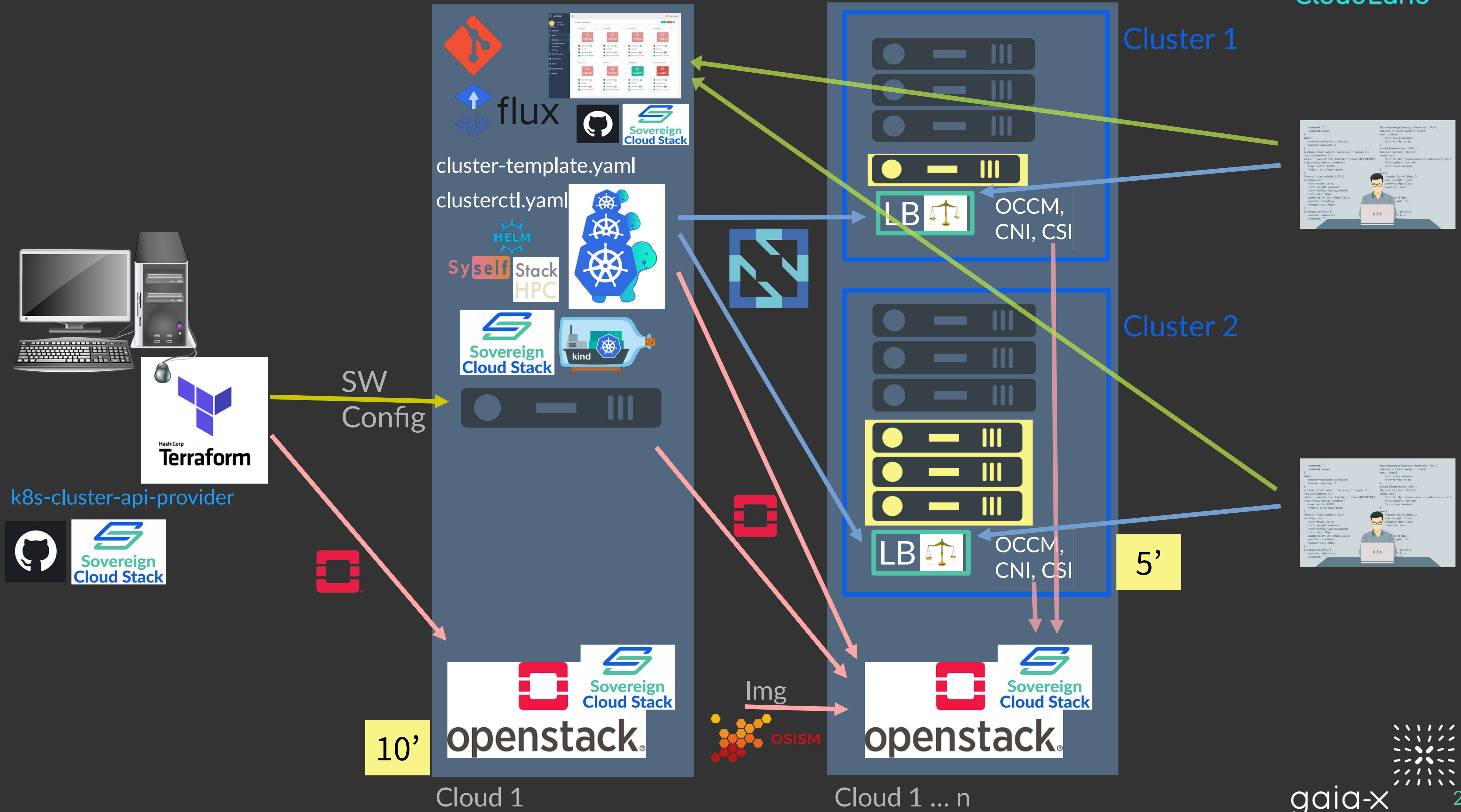
Linux

OpenStack

Kubernetes

Infra-
structure

K8s Cluster deployment structure - gitops



flux

cluster-template.yaml

clusterctl.yaml

HELM

Syself Stack HPC

kind

SW Config

HashiCorp Terraform

k8s-cluster-api-provider

Cluster 1

LB

OCCM, CNI, CSI

Cluster 2

LB

OCCM, CNI, CSI

5’

10’

openstack

Img

OSISM

openstack

Cloud 1

Cloud 1 … n

3 - SCS reference implementation status

Consists of OSI compliant (OSS helath check surviving) upstream components

- Participating in & contributing to upstream communities

All SCS work fully OSS (github.com/SovereignCloudStack)

- Modular code, developed by growing community in an agile way

Release R2 (v3.0.0) from 2022-03-23

- Secure, Stable & sustainable base layer (OSISM) w/ Bare Metal automation
- Complete IaaS stack (includes OpenStack Xena)
- Ready for federation (OIDC) & GXFS
- Operational stack (Lifecycle Management, Monitoring, Alerting, …) included
- K8s Cluster-API based container cluster management (KaaS) – API/CLI only

Roadmap for R3 (Sept 2022)

- Encrypt all data at rest (opt-out possible)
- Standardize k8s cluster management across providers (also for non-SCS IaaS)
- Strengthen CI framework and coverage
- Conformance tests (IaaS)
- Document and validate a set of IAM federation use cases
- Later: PaaS, Edge setups, Network encryption, …

SCS adoption

Two public clouds in production with complete SCS IaaS/Ops/IAM stacks since > 1 year

PlusCloud achieved BSI C5 certification in Nov ‘21

Adoption continues…

- Soon (2022-08): Third public cloud (with full SCS); TLRZ in 2023
- PoCs in industry and with public sector IT providers (DE: dataport, DVS = Deutsche Verwaltungscloud Strategie)
- Gaia-X lighthouse projects
- Modules used by various partners (see logos on homepage)
- Ecosystem of service companies emerging (training, consulting, implementation, support, …)
- Standards adoption via certification program (WIP)
- SCS Gitops Container Management definition also with non-SCS-IaaS providers (WIP)

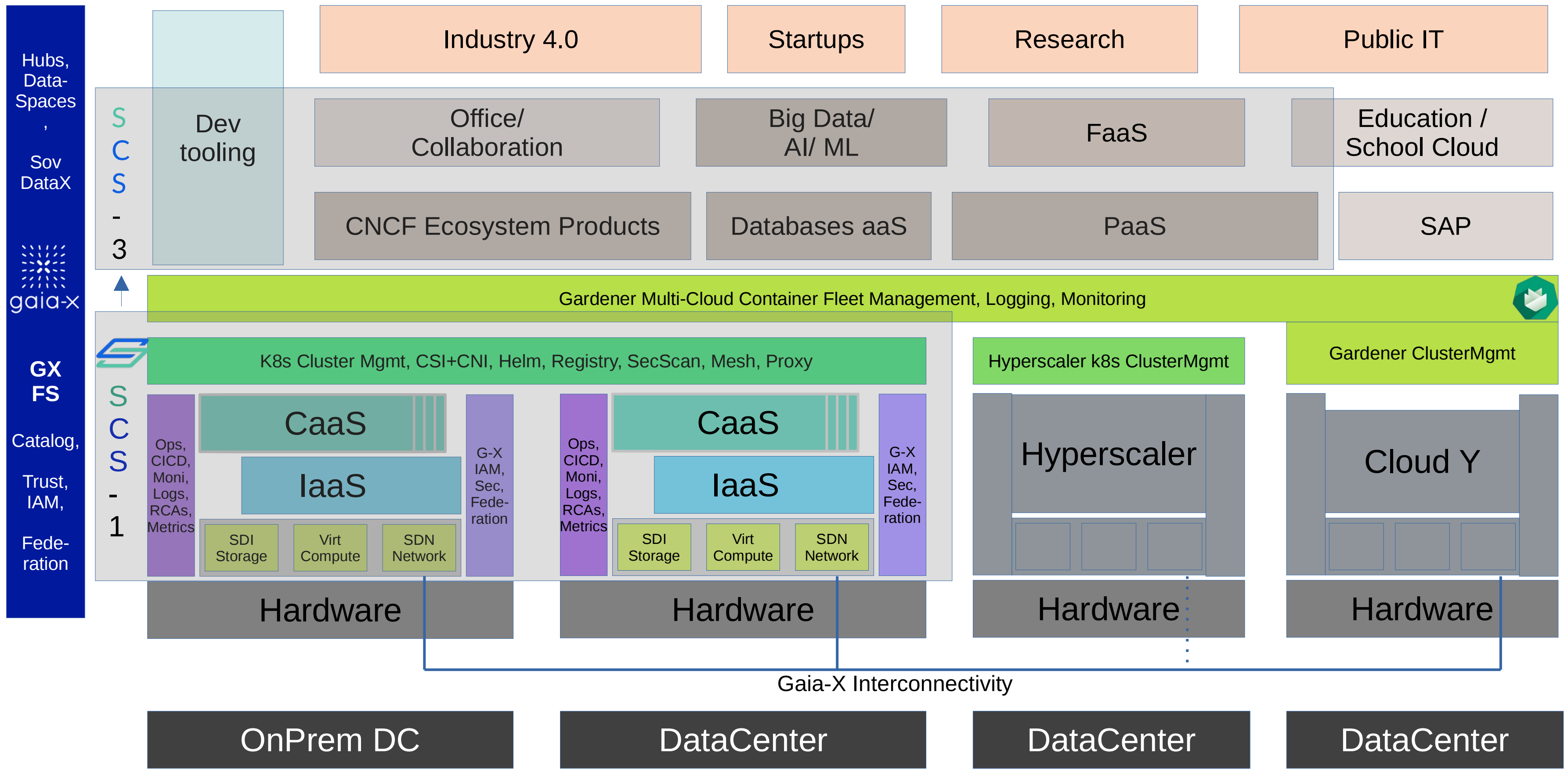
SCS validated in Gaia-X Hackathons and Betacloud and PlusCloud customers

- Gaia-X Self-Descriptions developed and provided (Srv. Char. WG / Bachelor thesis @ C&H)

Gaia-X Federation Services

- SCS used as Dev and Validation platform for Gaia-X Federation Services, integrated offerings planned

2/3 - Building federated clouds



Hubs, Data-Spaces, Sov DataX

gaia-x

GX FS

Catalog, Trust, IAM, Fede-ration

Industry 4.0

Startups

Research

Public IT

SCS - 3

Dev tooling

Office/ Collaboration

Big Data/ AI/ ML

FaaS

Education / School Cloud

CNCF Ecosystem Products

Databases aaS

PaaS

SAP

Gardener Multi-Cloud Container Fleet Management, Logging, Monitoring

SCS - 1

K8s Cluster Mgmt, CSI+CNI, Helm, Registry, SecScan, Mesh, Proxy

Ops, CICD, Moni, Logs, RCAs, Metrics

CaaS

IaaS

SDI Storage

Virt Compute

SDN Network

G-X IAM, Sec, Fede-ration

Ops, CICD, Moni, Logs, RCAs, Metrics

CaaS

IaaS

SDI Storage

Virt Compute

SDN Network

G-X IAM, Sec, Fede-ration

Hyperscaler k8s ClusterMgmt

Hyperscaler

Gardener ClusterMgmt

Cloud Y

Hardware

Hardware

Hardware

Hardware

Gaia-X Interconnectivity

OnPrem DC

DataCenter

DataCenter

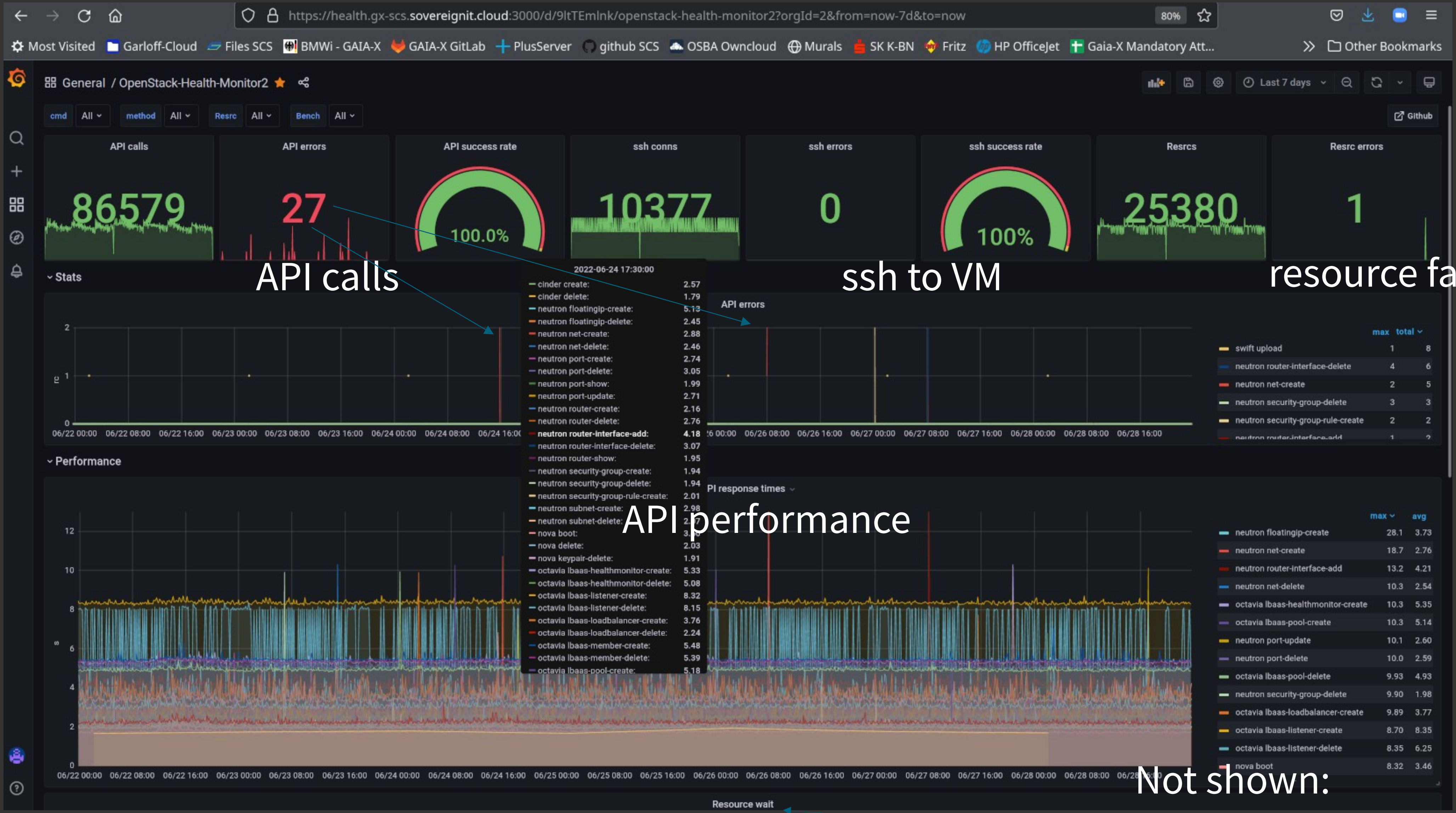
DataCenter

Adapted from Acatech Whitepaper on Digital Sovereignty (3/2021)

Sovereign Cloud Stack
An OSB ALLIANCE project

CloudLand

4 - Operations:
Measure what you want to manage ...



https://health.gx-scs.sovereignit.cloud:3000/d/9ltTEmlnk/openstack-health-monitor2?orgId=2&from=now-7d&to=now

API calls	API errors	API success rate	ssh conns	ssh errors	ssh success rate	Resrcs	Resrc errors
86579	27	100.0%	10377	0	100%	25380	1

2022-06-24 17:30:00

cinder create:	2.57
cinder delete:	1.79
neutron floatingip-create:	5.13
neutron floatingip-delete:	2.45
neutron net-create:	2.88
neutron net-delete:	2.46
neutron port-create:	2.74
neutron port-delete:	3.05
neutron port-show:	1.99
neutron port-update:	2.71
neutron router-create:	2.16
neutron router-delete:	2.76
neutron router-interface-add:	**4.18**
neutron router-interface-delete:	3.07
neutron router-show:	1.95
neutron security-group-create:	1.94
neutron security-group-delete:	1.94
neutron security-group-rule-create:	2.01
neutron subnet-create:	2.98
neutron subnet-delete:	[illegible]
nova boot:	[illegible]
nova delete:	2.03
nova keypair-delete:	1.91
octavia lbaas-healthmonitor-create:	5.33
octavia lbaas-healthmonitor-delete:	5.08
octavia lbaas-listener-create:	8.32
octavia lbaas-listener-delete:	8.15
octavia lbaas-loadbalancer-create:	3.76
octavia lbaas-loadbalancer-delete:	2.24
octavia lbaas-member-create:	5.48
octavia lbaas-member-delete:	5.39
octavia lbaas-pool-create:	5.18

API errors

	max	total
swift upload	1	8
neutron router-interface-delete	4	6
neutron net-create	2	5
neutron security-group-delete	3	3
neutron security-group-rule-create	2	2
neutron router-interface-add	1	2

	max	avg
neutron floatingip-create	28.1	3.73
neutron net-create	18.7	2.76
neutron router-interface-add	13.2	4.21
neutron net-delete	10.3	2.54
octavia lbaas-healthmonitor-create	10.3	5.35
octavia lbaas-pool-create	10.3	5.14
neutron port-update	10.1	2.60
neutron port-delete	10.0	2.59
octavia lbaas-pool-delete	9.93	4.93
neutron security-group-delete	9.90	1.98
octavia lbaas-loadbalancer-create	9.89	3.77
octavia lbaas-listener-create	8.70	8.35
octavia lbaas-listener-delete	8.35	6.25
nova boot	8.32	3.46

API calls

ssh to VM

resource fails

API performance

Not shown:
resource performance

openstack-health-monitor: Behavior-based monitoring

gaia-x

Wanted: Open Operations culture
You’re not alone in operating your stack!

Share knowledge

e.g. monitoring setup and config

Share status

e.g. health & performance monitoring

Share challenges

e.g. fraud detection

Public Root Cause Analysis

e.g. outages

SCS resources:

Blog

OperationalDocs

Operator Lean Coffee

Tools:
e.g. Health-mon dashboard

Next: RCA templates
Link collection

Join the growing SCS community!

As CSP or industry IT department

- Join discussions / community
- Adopt standards and/or technology (code)

As OSS infrastructure software developer

- Contribute / Participate in community
- Apply for a job in our OSB Alliance team

As interested company

- Build SCS expertise, respond to tenders
- Build business model around SCS expertise

As PaaS/SaaS developer

- Develop / Test against SCS standards

As IT consumer

- Request true sovereignty from your platform
- Avoid the pitfall of reinterpreting reality to make it feel better

More information:

Homepage:
https://scs.community/
Github:
https://github.com/SovereignCloudStack
https://github.com/OSISM
Upstream: OIF, CNCF, LF

(CloudExpo, OIF summit, CloudLand, …)

Gaia-X: MVG OWP, Hackathons, WGs FS/OSS, Svc. Char.

Email: project@scs.sovereignit.de
Matrix: SCS rooms
https://matrix.to/#/#scs-general:matrix.org

Predicting the future (2024)

~~A big war in Europe in inconceivable. We don’t need well-working defense.~~

~~It’s OK for Europe to strongly depend on natural gas from Russia.~~

~~Britain won’t leave the European Union.~~

??? ~~The Americans won’t elect an immature bully again.~~

??? ~~It’s OK for Euope to strongly depend on US IT platforms.~~

~~Safe Harbor sufficiently protects personally-identifiable data transferred to the US.~~

??? ~~Privacy Should 2.0 sufficiently protects personally-identifiable data transferred to the US.~~

~~US clouds hosted in European Data Centers are safe to use for personally identifiable data~~

??? Trustee models (EU operated “sovereign” clouds with US tech) fulfill GDPR ~~and sovereignty~~

??? ~~Confidential Computing avoid all these problems with trust and sovereignty requirements.~~