

Sovereign Cloud Stack

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

Using Sovereign Cloud Stack to Achieve Digital Sovereignty

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

project@scs.sovereignit.de

Cloud Expo Europe, 2022-05-11

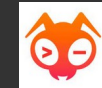
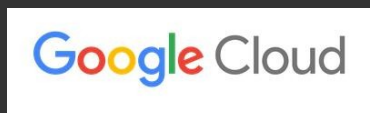
Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

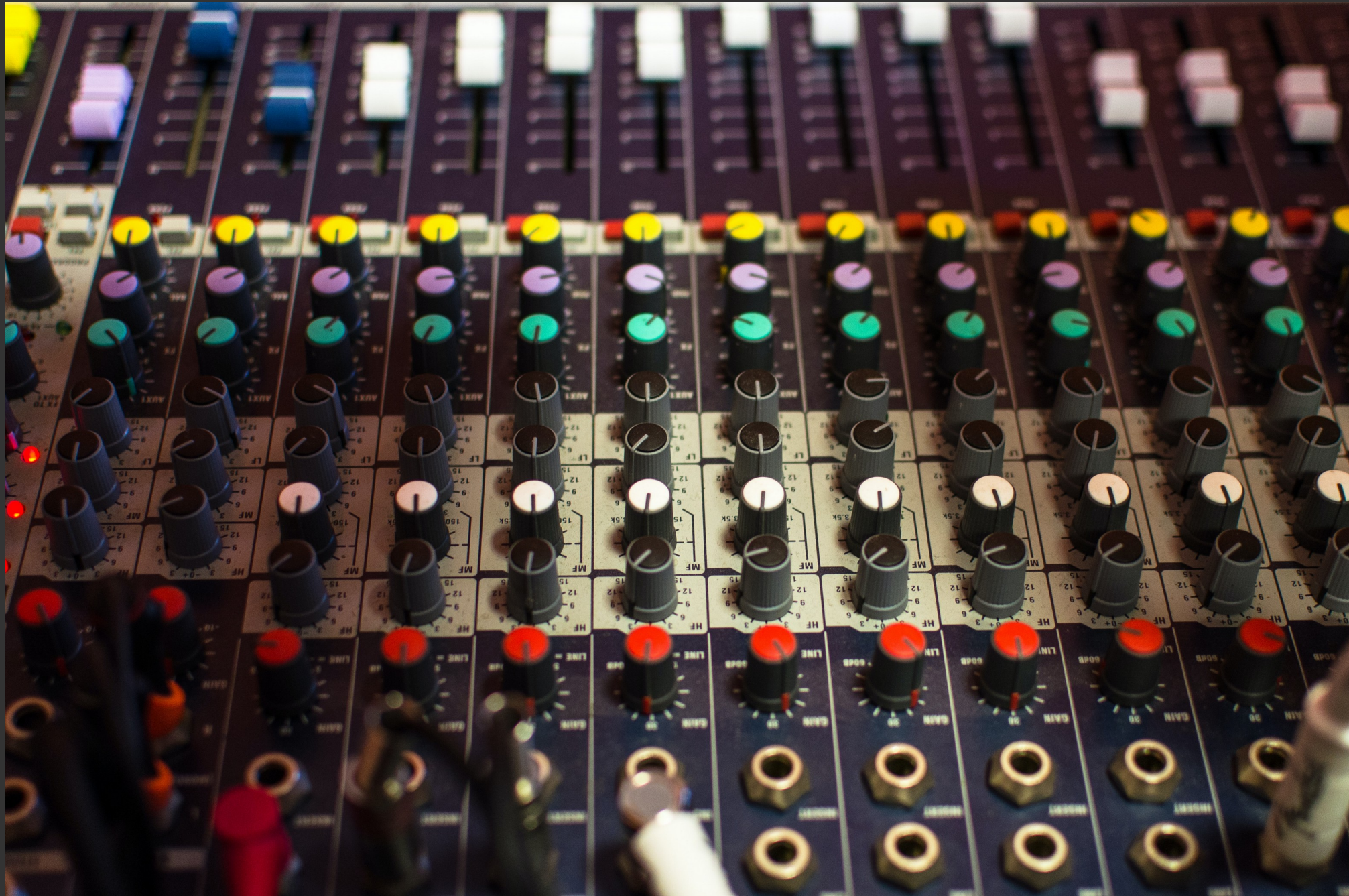


Digital Sovereignty ... What?



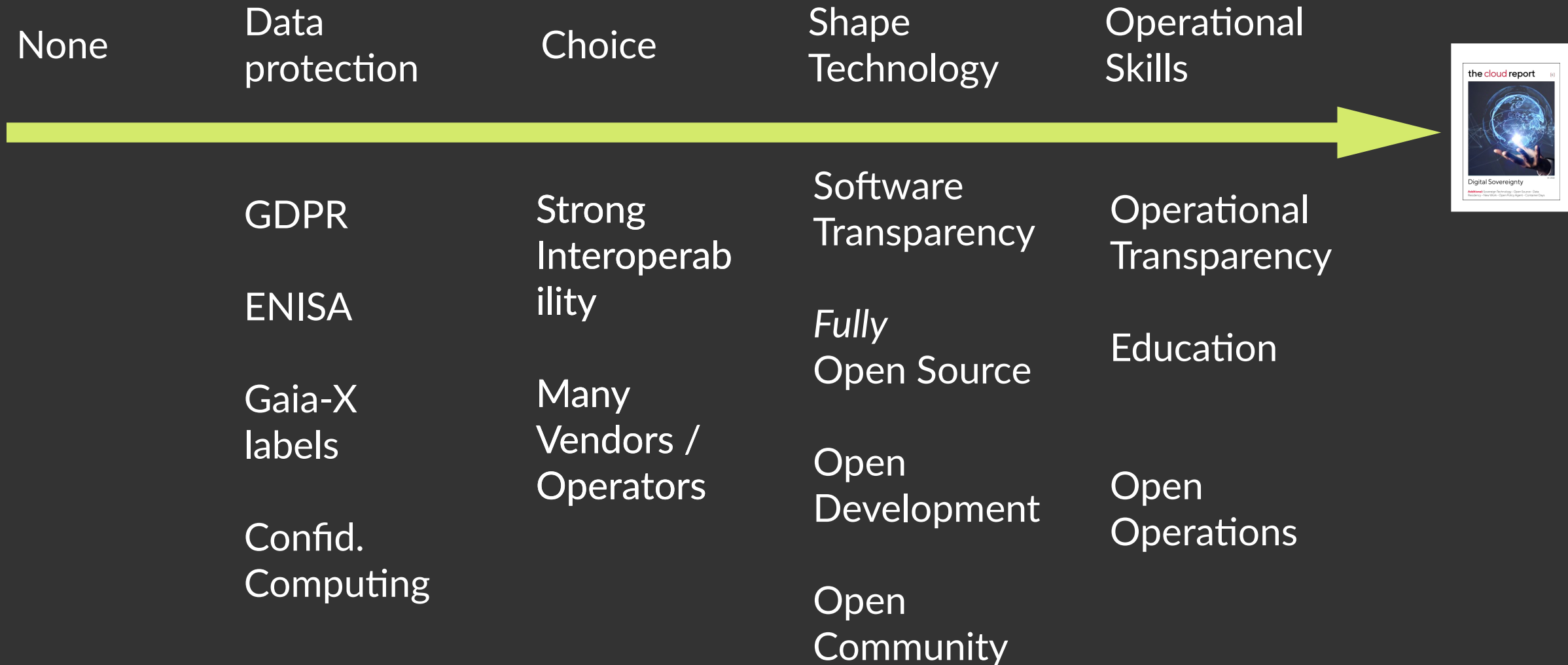


Who is in control?





Levels of sovereignty



Recommendation: Thu, 11:15, Digi Trans Keynote Theatre:
Peter Ganten: Digital Sovereignty and the Cloud: Everything is at stake



Openness?



Transparency?





Sovereign Data requires ...





... sovereign infrastructure ...





and it'd better be solid



2018

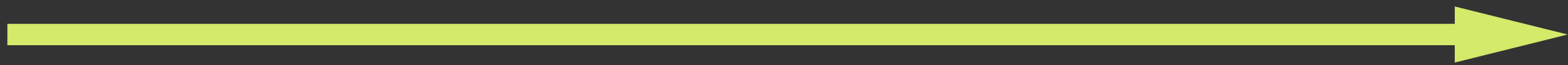
gaia-x



Sovereign Cloud Stack vision

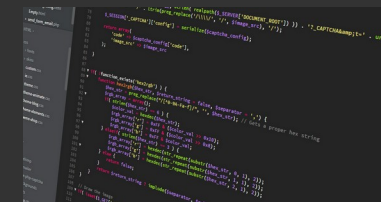


None Data protection Choice Shape Technology Operational Skills



Achieve all levels of digital sovereignty

- 1) GDPR / Data protection / Data security
- 2) Real choice by many (collaborating!) providers with strong interoperability: Standardization & Certification
- 3) Fully open functional stack (Four Opens, OSS Health Check) as reference implementation
- 4) Full transparency over operations stack, operational practices (Open Operations)





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/>





1 - Security by Design

Using strong isolation for container clusters

- Different tenants receive their own Kubernetes clusters; by default, no cluster sharing happens
- Underlying 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 registry solution

Daily patching supported

- The architecture is built for daily patching (or redeployment) without noticeable 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 ecosystem

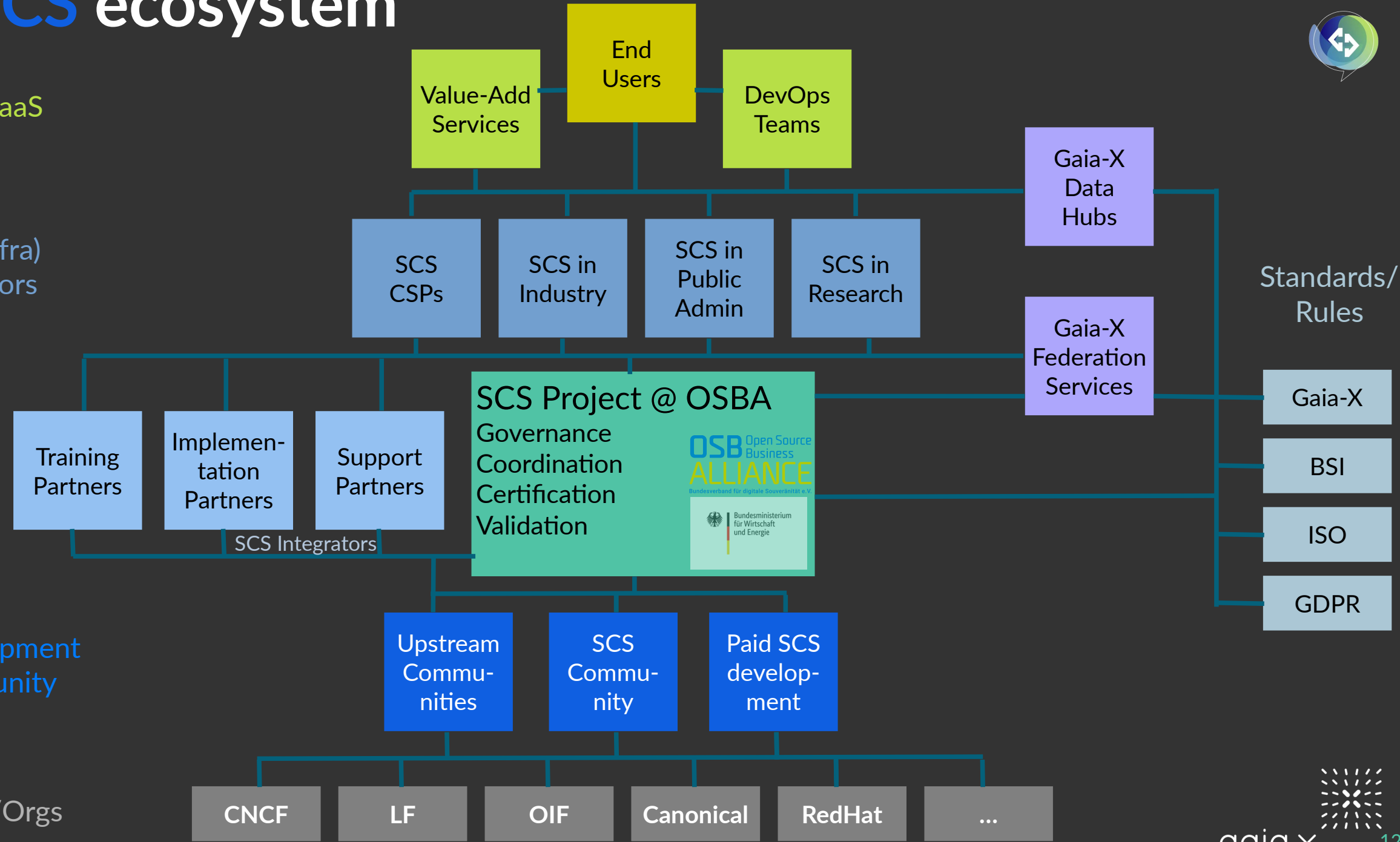
SaaS/PaaS

SCS (Infra) Operators

Services

Development Community

Found/Orgs

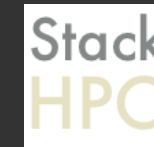
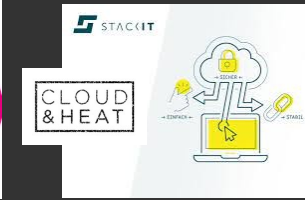
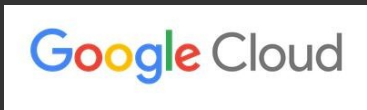




2 - SCS choice ...



SCS





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)

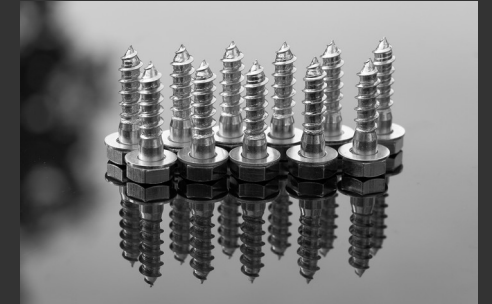
- Done: IaaS flavor naming and standard flavors
- Done: Image metadata
- WIP: Definition of regions, availability zones, ...
- WIP: k8s cluster management (k8s cluster-API)

Federation

- Allow OIDC user federation

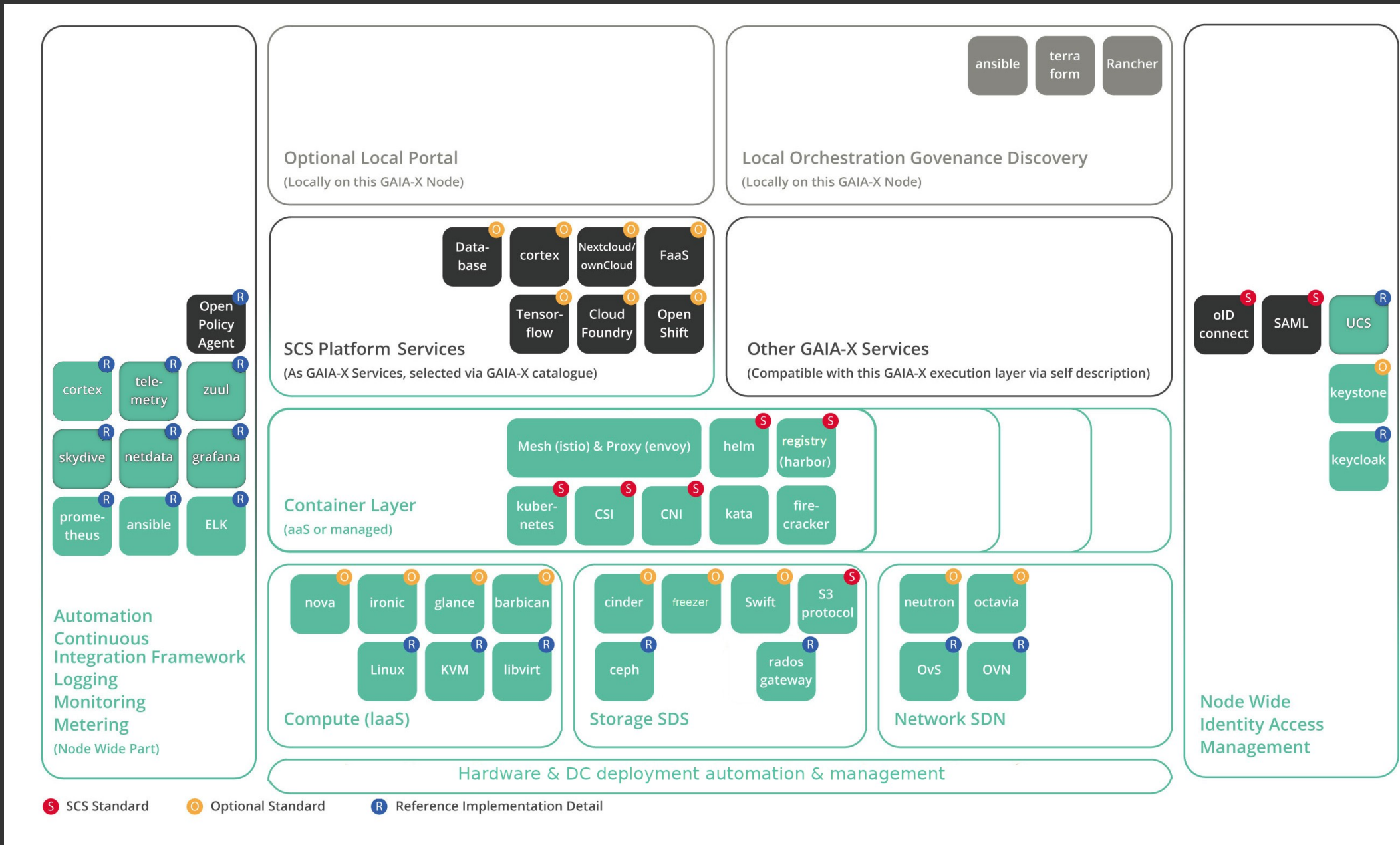
Formal SCS certification program to be launched this summer for CSPs

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





3 - SCS reference implementation architecture





3 - SCS reference implementation status

Consists of OSI compliant (OSS health 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, ...



3 - SCS reference implementation adoption

Two public clouds in production with complete SCS stacks since > 1 year



PlusCloud achieved a BSI C5 certification in Nov '21

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

Adoption continues...

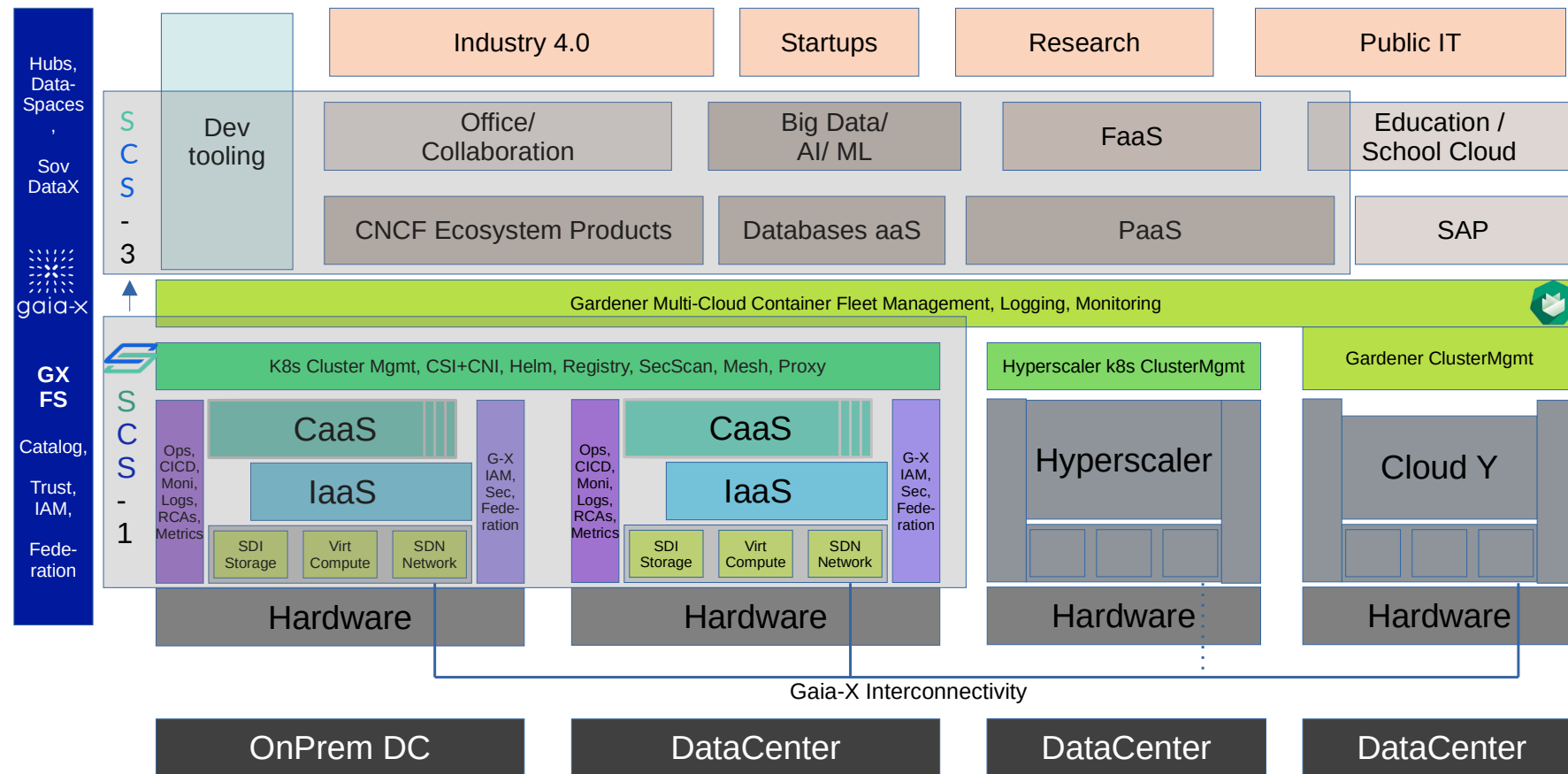
- Soon: Third public cloud (with full SCS)
- PoCs in industry and with public sector IT providers (DE)
- Modules used by various partners (see logos on homepage)
- Ecosystem of service companies emerging (training, consulting, implementation, support, ...)
- Standards adoption via certification program

Gaia-X

- Collaboration with Gaia-X Federation Services
- Usage in Gaia-X projects

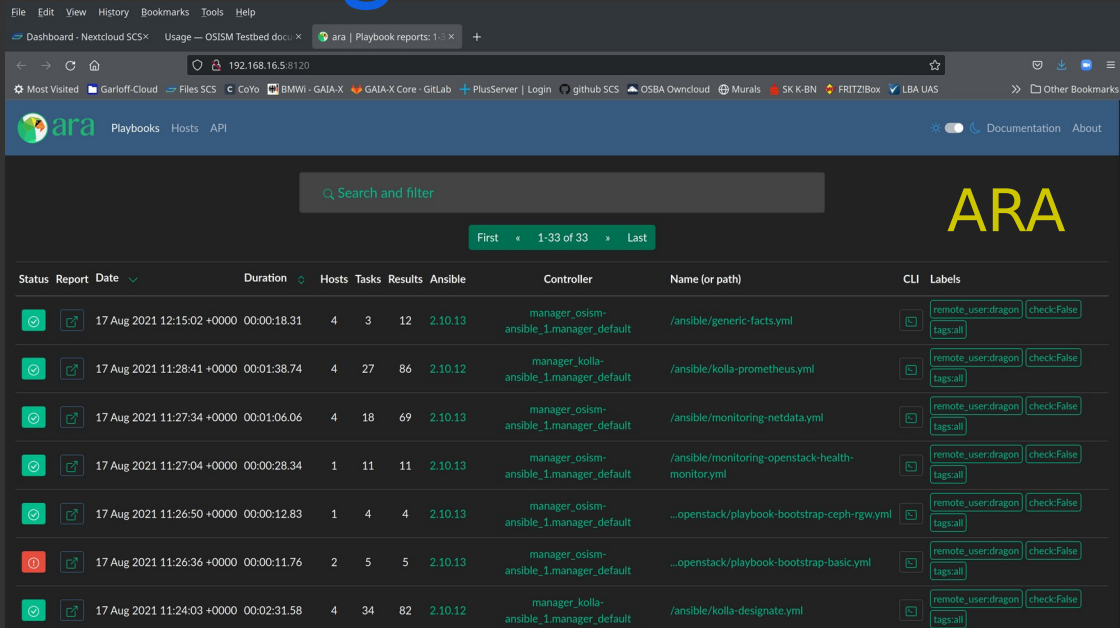


2/3 - Building federated clouds



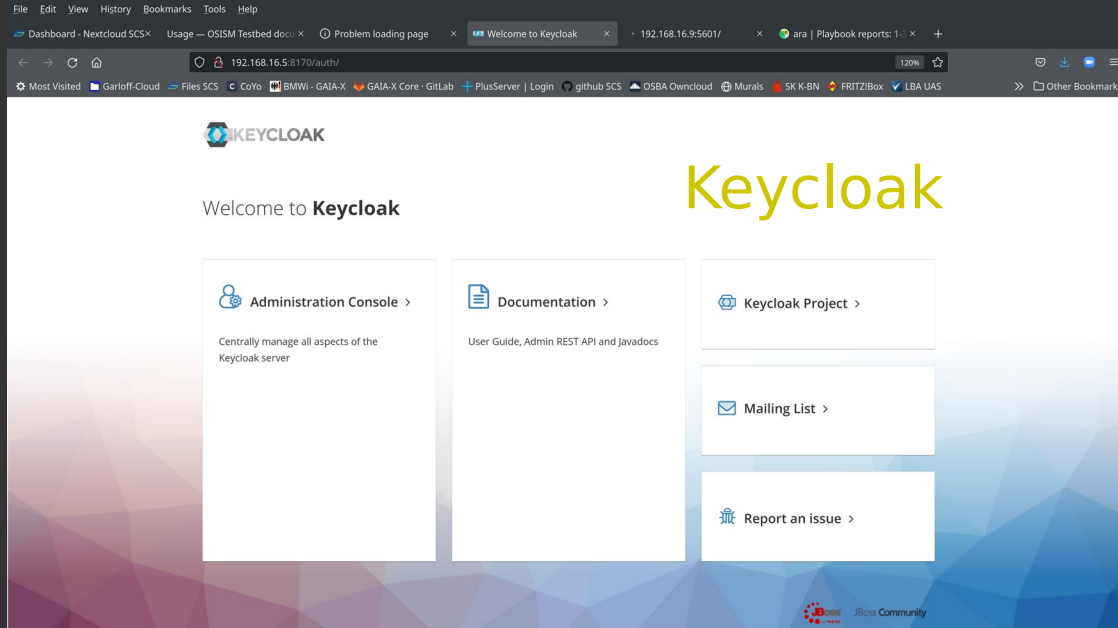
Adapted from Acatech Whitepaper on Digital Sovereignty (3/2021)

4 - Addressing the Operations challenge: Tooling



ARA

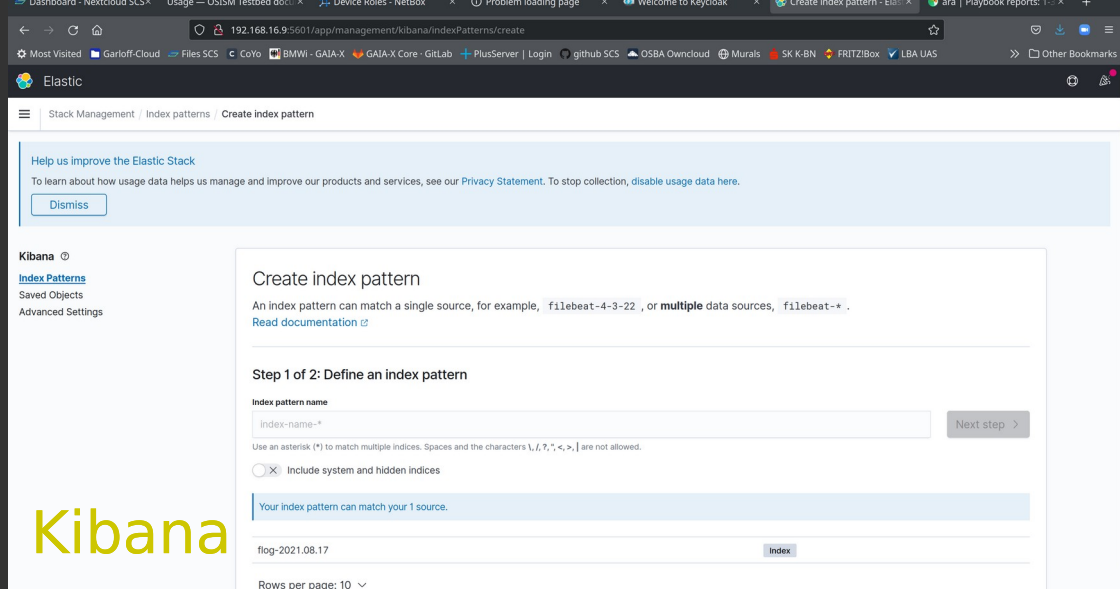
Status	Report	Date	Duration	Hosts	Tasks	Results	Ansible	Controller	Name (or path)	CLI	Labels
Success		17 Aug 2021 12:15:02 +0000	00:00:18.31	4	3	12	2.10.13	manager_osism-ansible_1.manager_default	/ansible/generic-facts.yml	remote_user:dragon	check:False tags:all
Success		17 Aug 2021 11:28:41 +0000	00:01:38.74	4	27	86	2.10.12	manager_kolla-ansible_1.manager_default	/ansible/kolla-prometheus.yml	remote_user:dragon	check:False tags:all
Success		17 Aug 2021 11:27:34 +0000	00:01:06.06	4	18	69	2.10.13	manager_osism-ansible_1.manager_default	/ansible/monitoring-netdata.yml	remote_user:dragon	check:False tags:all
Success		17 Aug 2021 11:27:04 +0000	00:00:28.34	1	11	11	2.10.13	manager_osism-ansible_1.manager_default	/ansible/monitoring-openstack-health-monitor.yml	remote_user:dragon	check:False tags:all
Success		17 Aug 2021 11:26:50 +0000	00:00:12.83	1	4	4	2.10.13	manager_osism-ansible_1.manager_default	...openstack/playbook-bootstrap-ceph-rgw.yml	remote_user:dragon	check:False tags:all
Failure		17 Aug 2021 11:26:36 +0000	00:00:11.76	2	5	5	2.10.13	manager_osism-ansible_1.manager_default	...openstack/playbook-bootstrap-basic.yml	remote_user:dragon	check:False tags:all
Success		17 Aug 2021 11:24:03 +0000	00:02:31.58	4	34	82	2.10.12	manager_kolla-ansible_1.manager_default	/ansible/kolla-designate.yml	remote_user:dragon	check:False tags:all



Keycloak

Welcome to Keycloak

- Administration Console > Centrally manage all aspects of the Keycloak server
- Documentation > User Guide, Admin REST API and Javadocs
- Keycloak Project >
- Mailing List >
- Report an issue >



Kibana

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or multiple data sources, `filebeat-*`.
[Read documentation](#)

Step 1 of 2: Define an index pattern

Index pattern name

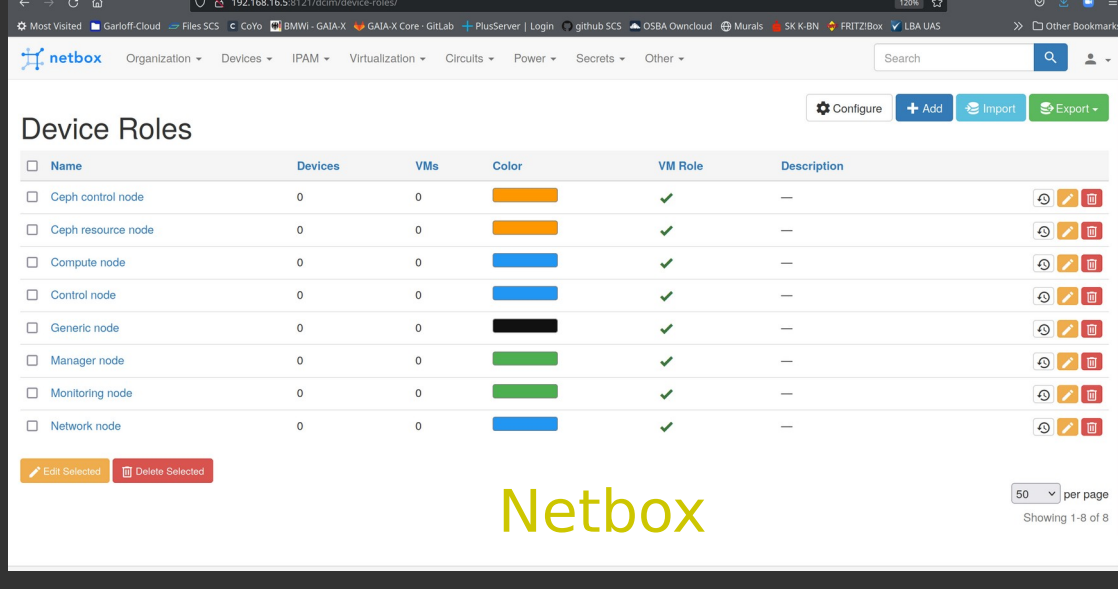
Use an asterisk (*) to match multiple indices. Spaces and the characters `\, /, ?, <, >` are not allowed.

Include system and hidden indices

Your index pattern can match your 1 source.

log-2021.08.17

Rows per page: 10



netbox

Device Roles

Name	Devices	VMs	Color	VM Role	Description
Ceph control node	0	0	Orange	✓	—
Ceph resource node	0	0	Orange	✓	—
Compute node	0	0	Blue	✓	—
Control node	0	0	Blue	✓	—
Generic node	0	0	Black	✓	—
Manager node	0	0	Green	✓	—
Monitoring node	0	0	Green	✓	—
Network node	0	0	Blue	✓	—

50 per page
Showing 1-8 of 8

Kibana

Netbox

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



openstack-health-monitor: Black-box monitoring

4 - Addressing the Operations challenge: Towards fully Open Operations



More tooling (well documented and configured)

- Monitoring, Alerting, Trending
- Patching (LCM) & CI/CD

Documenting and sharing best practices

Transparent Issue resolution

- Public RCAs

Public dashboard / status page

- e.g. OpenStack Health Monitor (or successor from TSI)





Join the growing SCS community!

As CSP or industry IT department

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

As OSS infrastructure software developer

- Contribute / Participate in community
- Deploy SCS testbeds (or use comm. hardware)
- 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

More information:

Homepage:

<https://scs.community/>

Github:

<https://github.com/SovereignCloudStack>

Booth E155 (3.1) at CEE

(Other Confs: 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>