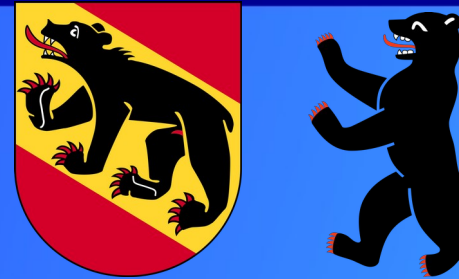


CH Open Business Lunch 25.08.2022



Sovereign Cloud Stack - ein Beitrag zur Verwirklichung digitaler Souveränität

Dr. Manuela Urban, Kurt Garloff, Dirk Loßack,
Eduard Itrich, Felix Kronlage-Dammers, Alexander Diab

project@scs.sovereignit.de

Slides shared under CC-BY-SA-4.0

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

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Agenda

1. Was ist digitale Souveränität? Was bedeutet sie für Cloud-Services?
2. SCS Vision und Ziele
3. Technologie
4. Open Operations
5. Zertifizierung
6. Was wurde bisher erreicht?

Digitale Souveränität

“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 der deutschen Bundesregierung

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

Realität

Hyperscaler dominieren den Markt

USA-EU: Privacy Shield, Schrems II, CLOUD Act...

Vergabekammer Baden-Württemberg, 13.07.2022: Datenschutz bei US-Cloud-Diensten auch dann nicht gewährleistet, wenn über europäisches Tochterunternehmen



ökonomische, strategische Abhängigkeiten:

Peter Ganten, Handelsblatt: <https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-warum-wirtschaft-schnell-eine-digitale-zeitenwende-brauchen/28575768.html>

Alternativen?

- Open Source? Ja, aber:
 - Fragmentierung
 - Betrieb moderner Cloud-Plattformen hochkomplex
 - Fachkräftemangel
 - fehlende Referenzimplementierungen
 - nicht durchgängig “open”
 - OS Governance



Digitale Souveränität



**Kontrolle
wiedererlangen,
Selbstbestimmung**



**Technologische Innovation und
Marktbeteiligung**



**Digitalisierung, Beseitigung
technologischer Rückstände**



Gaia-X

„eine leistungsstarke, wettbewerbsfähige, sichere und vertrauenswürdige Dateninfrastruktur auf der Grundlage europäischer Werte“¹

7 Leitprinzipien:²

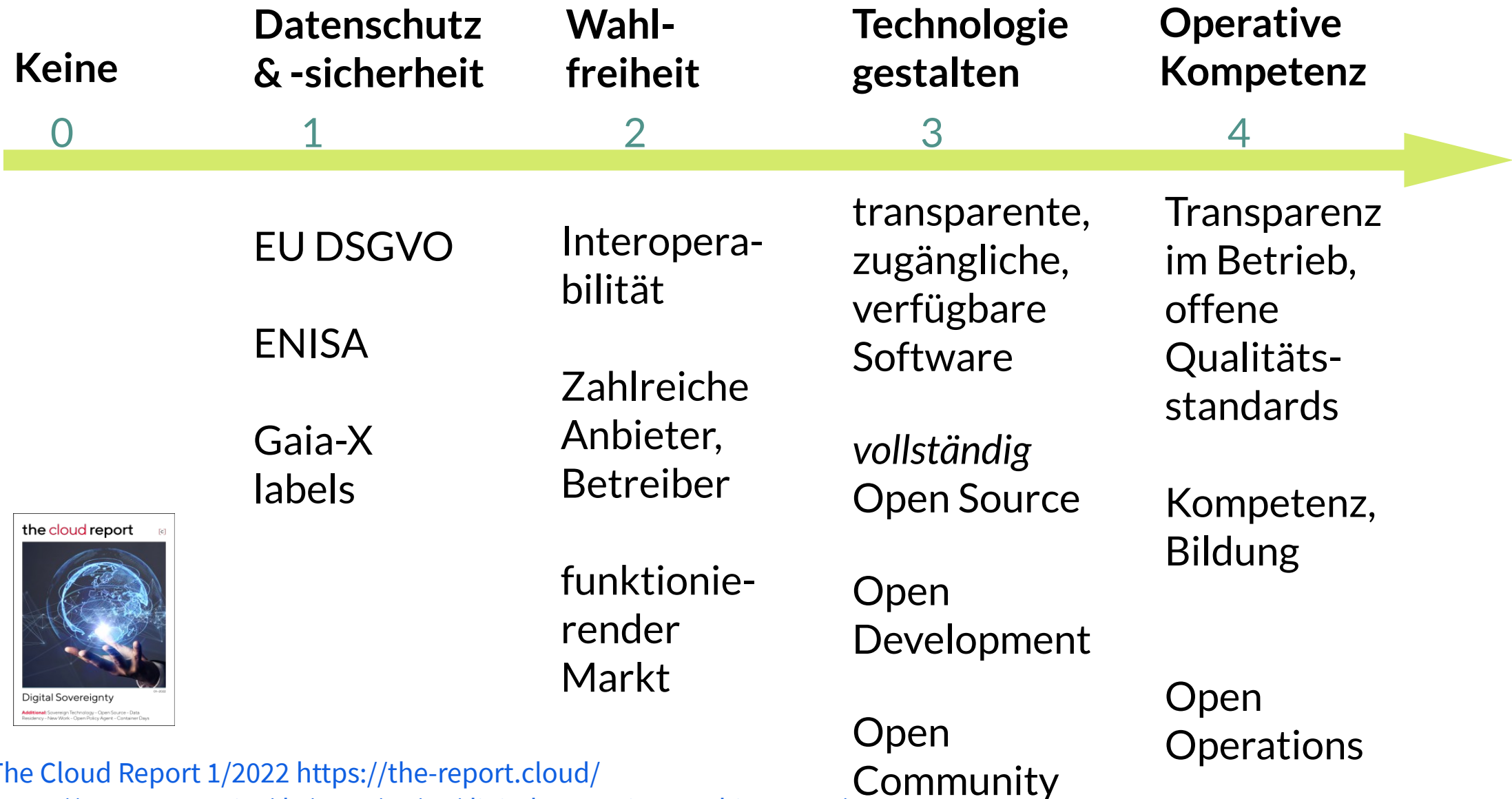
1. Europäischer Datenschutz
2. Offenheit und Transparenz
3. Authentizität und Vertrauen
4. Digitale Souveränität und Selbstbestimmtheit
5. Freier Marktzugang und europäische Wertschöpfung
6. Modularität und Interoperabilität
7. Benutzerfreundlichkeit



¹ BMWi & BMBF 2019

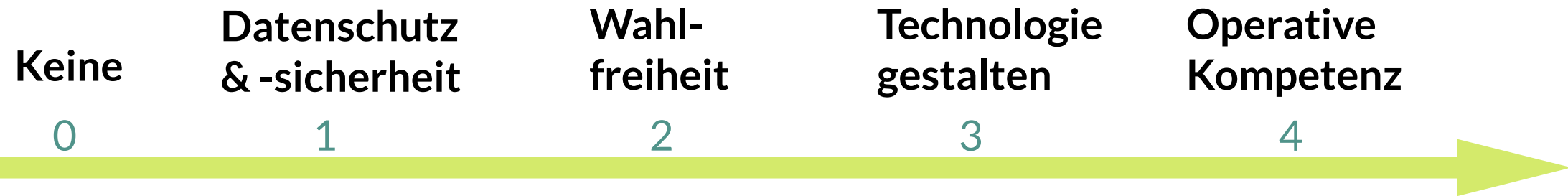
² BMWi 2020

Stufen der Souveränität



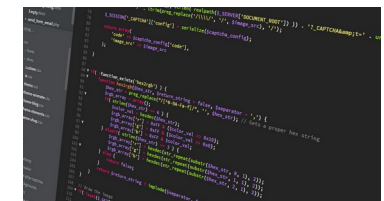
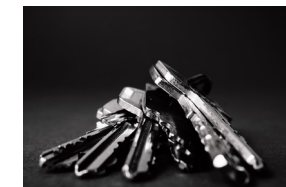
The Cloud Report 1/2022 <https://the-report.cloud/>
<https://scs.community/de/2022/03/18/digital-sovereignty-whitepaper/>

Sovereign Cloud Stack Vision



Alle Stufen der digitalen Souveränität ermöglichen

- 1) Security by design, SBOM, “GOP”, Open Source Governance
- 2) Interoperabilität: Standardisierung, Zertifizierung, Föderation
- 3) vollständig offener funktionaler Cloud- & Container-Stack als modulare Referenzimplementierung
- 4) vollständige Transparenz über die betrieblichen Praktiken und den operativen Status, nachvollziehbare operative Standards, Root Cause Analyses: “Open Operations”



Sovereign Cloud Stack Projekt

- Start Ende 2019
- Gefördert durch Bundesministerium für Wirtschaft und Klimaschutz (BMWK) seit Sommer 2021
- Getragen von Open Source Business Alliance e.V. (mit derzeit 6 Personen, Ziel 12 Personen)
- Beiträge aus und in die Open Source Communities
- Auftragsarbeiten, öffentlich ausgeschrieben
- enge Zusammenarbeit mit Gaia-X
- SCS versteht sich als neutrale Plattform im SCS ecosystem; Partner aus Wirtschaft, Staat und Zivilgesellschaft
- Website: <https://scs.community/>



Sovereign Cloud Stack Ziele

Die Bereitstellung und Nutzung einer modernen, souveränen Cloud- und Container-Infrastruktur einfach machen

1. Ein **Ökosystem** und eine **Community** mit “Good Governance” entwickeln;
wichtig: SCS möchte der weiteren Fragmentierung entgegenwirken und trägt daher aktiv zu den existierenden Communities bei.
 2. Eine Secure-by-design-**Plattform** entwickeln
 3. mit **zertifizierbaren Standards**, die die **Föderierung** ermöglichen,
 4. mit einer vollständigen, durchgängig offenen, modularen, automatisierten **Referenzimplementierung**,
 5. mit einem Open-Source-Werkzeugkasten und Best Practices für den Betrieb moderner Plattformen: Entwicklung von “**Open Operations**”
- ➔ Leitprinzipien: “**Four Opens**” (OIF): Open Source (not: Open Core!), Open Development, Open Community, Open Design

SCS Ecosystem

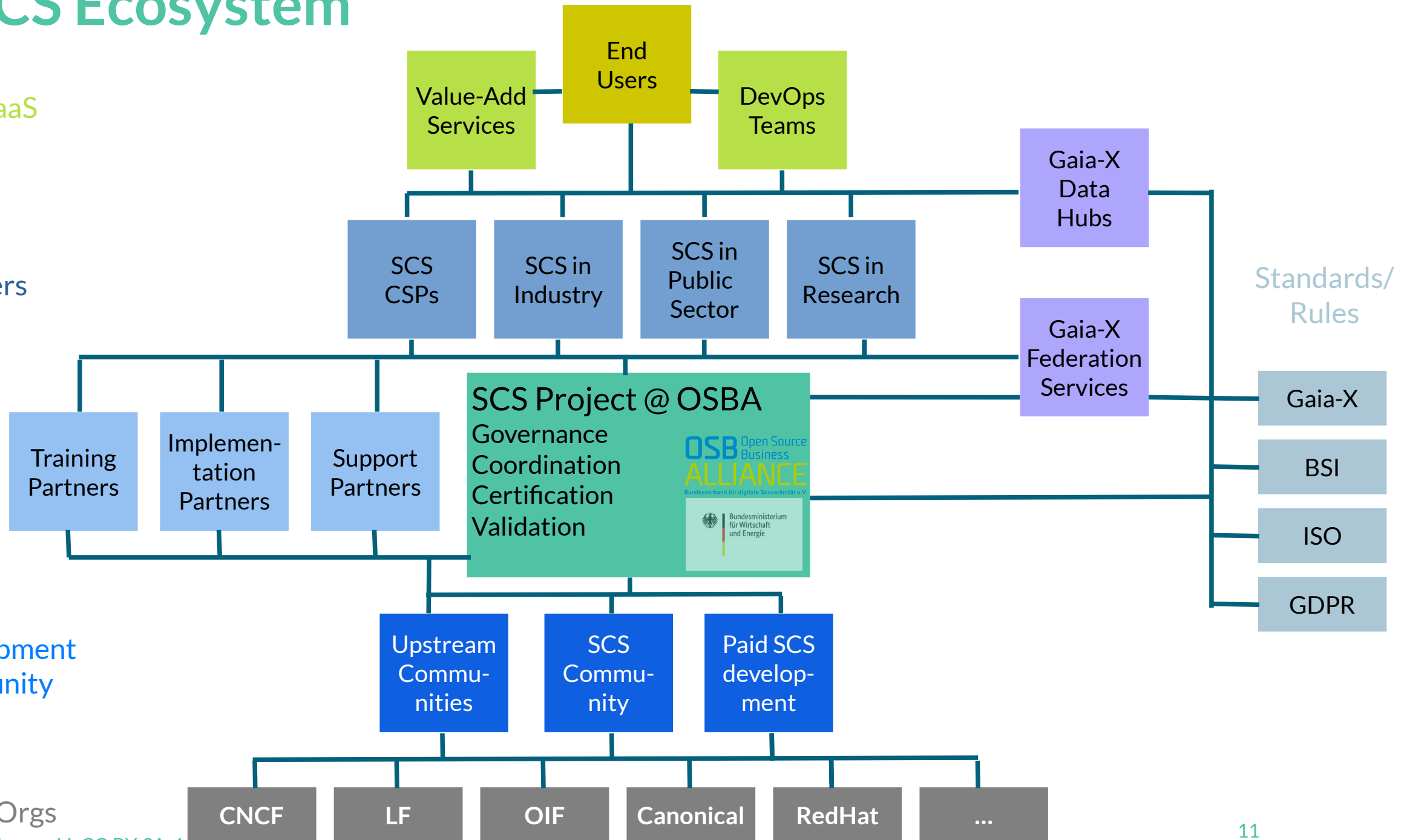
SaaS/PaaS

(Infra) Providers

Services

Development Community

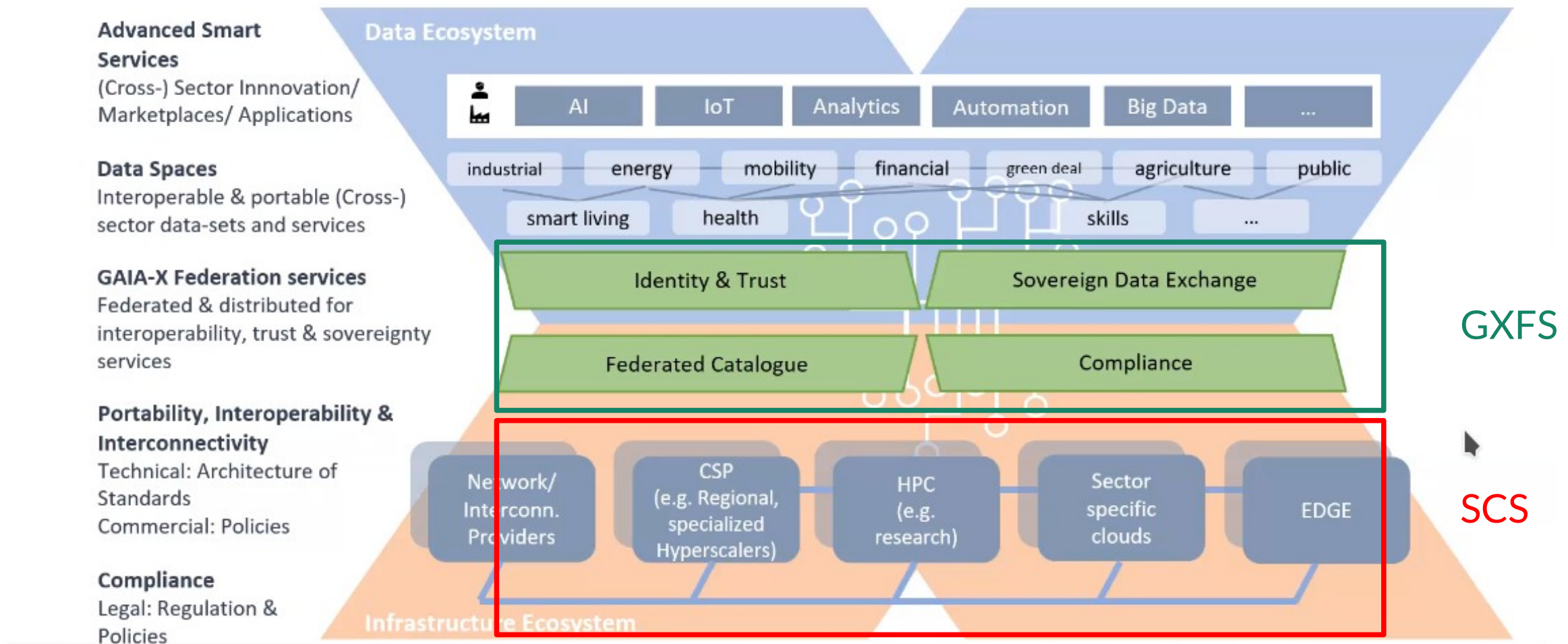
Found/Orgs



Sovereign Cloud Stack and Gaia-X

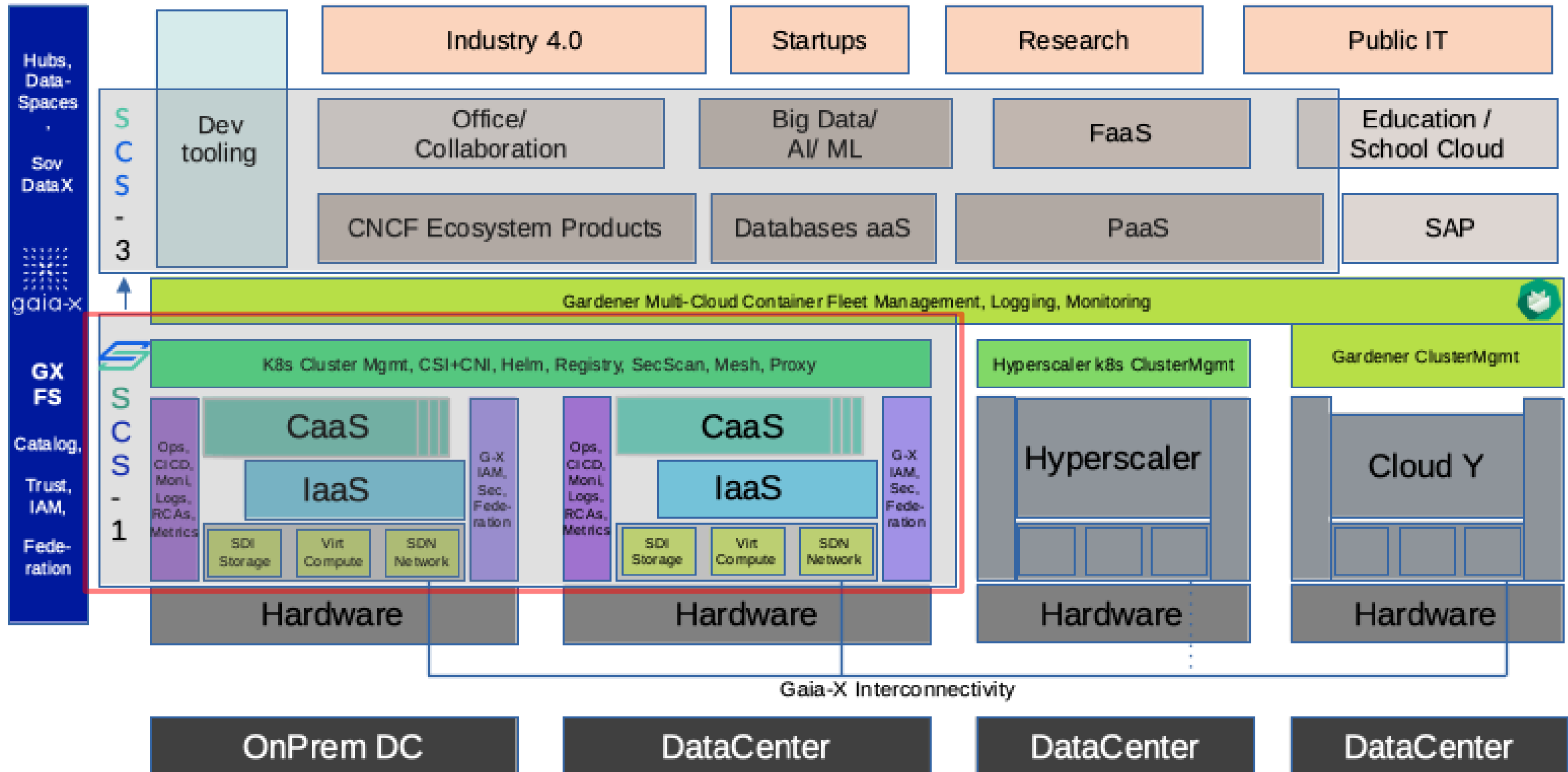
SCS im Gaia-X Magazin
Juni 2022
<https://gaia-x.eu/mediatech/the-gaia-x-magazine/>

Gaia-X in One (Big) Figure

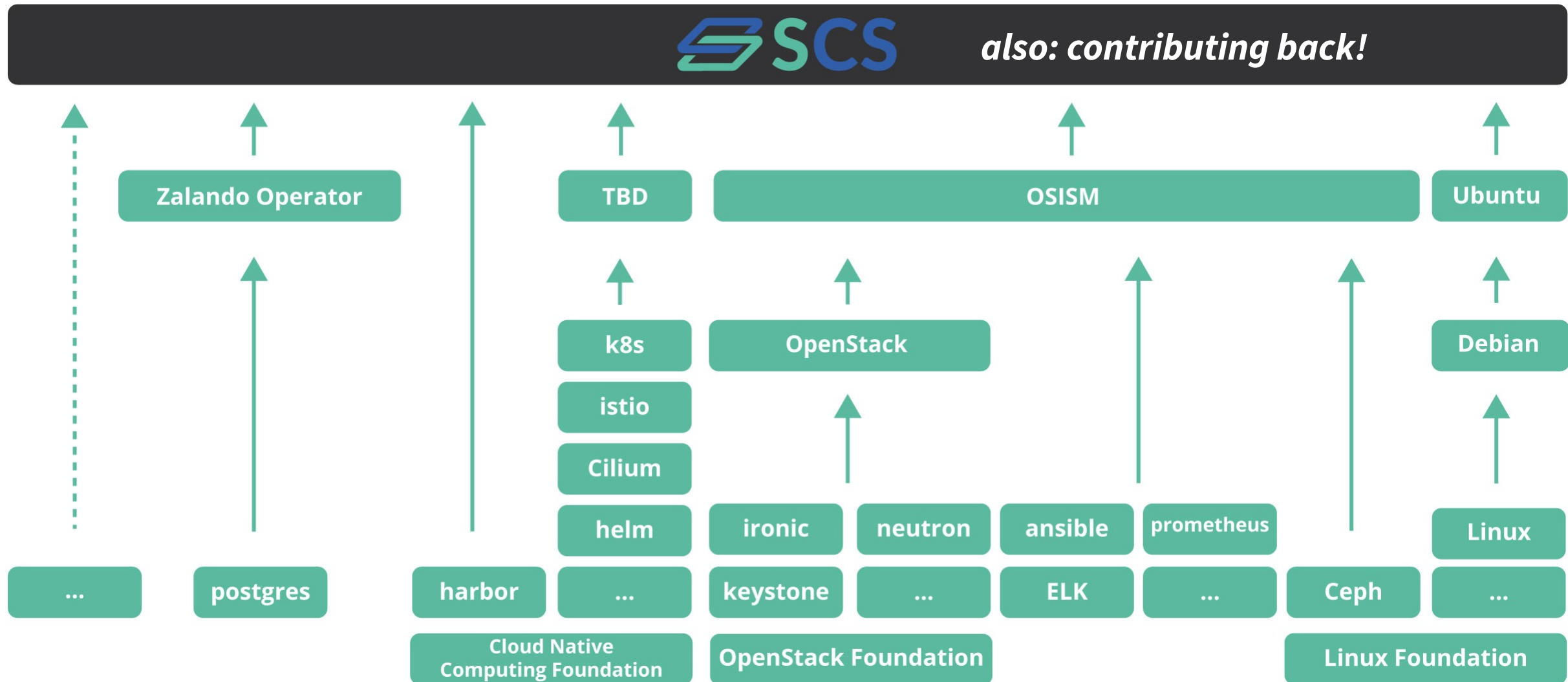


IT Ecosystem with GAIA-X

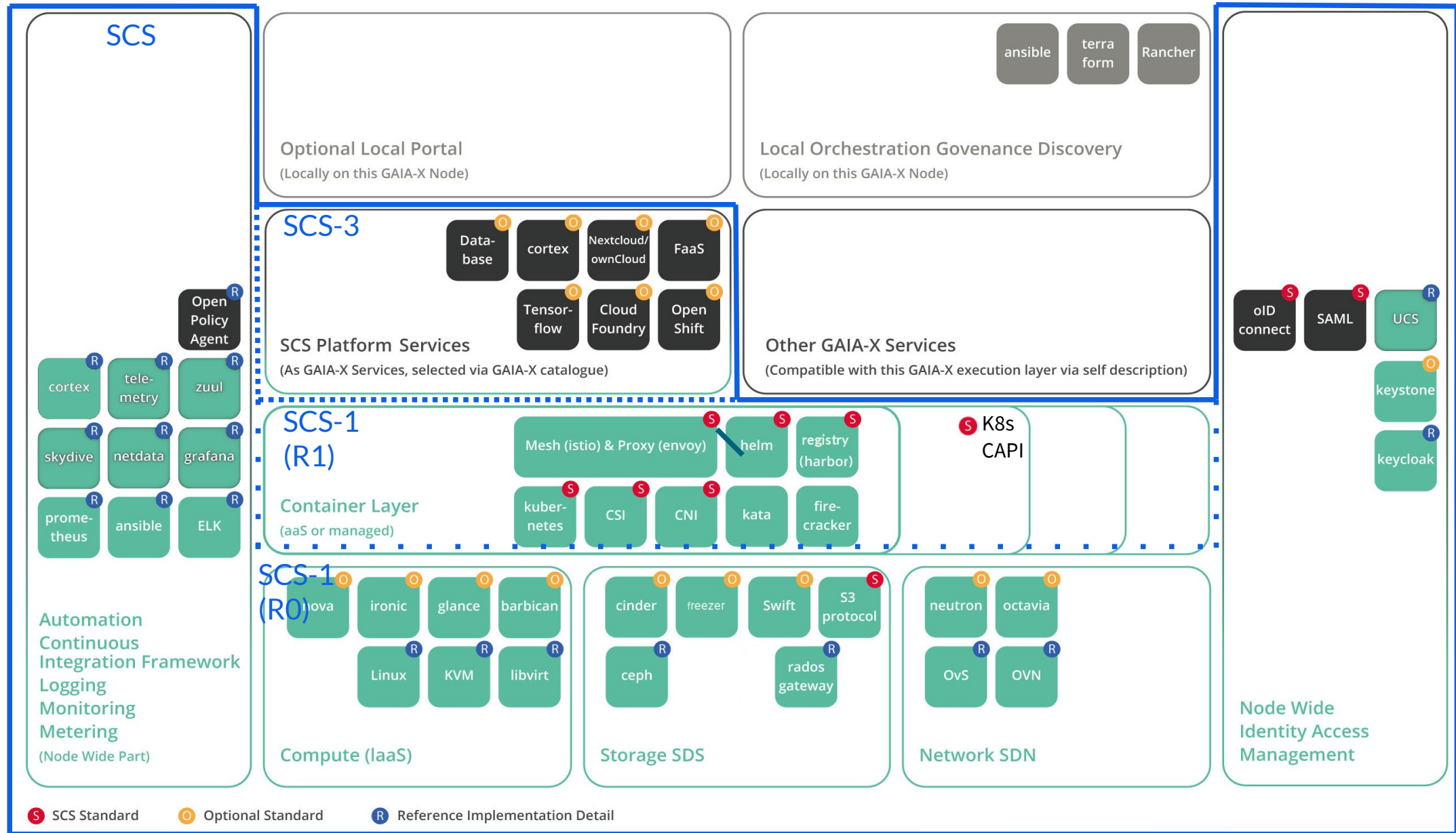
adapted from Acatech whitepaper



Wie wird SCS gebaut? (Entwicklerperspektive)



SCS Architektur Referenzimplementierung Sovereign Cloud Stack



Security by Design

Strikte Isolierung von Container-Clustern

- Jeder Mandant erhält standardmäßig seinen eigenen Kubernetes Cluster; kein Cluster-Sharing.
- Zugrundeliegende VMs, Netzwerke, Speicher sind durch strenge Virtualisierungsbarrieren getrennt.

Private Registry für Nutzer

- DevOps Teams sollen auf einfache Weise ihre eigenen Sicherheitsüberprüfungsprozesse etablieren und ihre Lieferketten kontrollieren können.
- Vulnerability Scanning in der Registry-Lösung enthalten.

Daily Patching

- Architektur erlaubt Daily Patching (oder Redeployment), ohne Beeinträchtigung beim Kunden.
- Stets aktuelle Security Patches.

Sicherheitsorientierte betriebliche Praktiken

- Alle Verfahren, Patches, Updates werden lückenlos und transparent dokumentiert.
- systematische, kontinuierliche Qualitätsverbesserung in der betrieblichen Praxis

Air-Gap-Modus wird unterstützt

- Deployment und Aktualisierung ohne Internetverbindung möglich
- Nutzung eines internen Registry und Patch-Distributions-Mechanismus (einschließlich Vulnerability-Scan)

Sicherheits-Zertifizierungen

- Sicherheitszertifizierungen bei Partnern können im Rahmen des Projekts unterstützt werden
- Pen Testing

Lieferkettenabsicherung

- SBOM Tool, reproduzierbare Builds, Scanning...



SCS Referenzimplementierung Status

OSI-konforme Upstream-Komponenten (OSS Health check)

- Mitwirkung bei den relevanten Upstream Communities

Jegliche Entwicklungsarbeit vollständig offen (github.com/SovereignCloudStack)

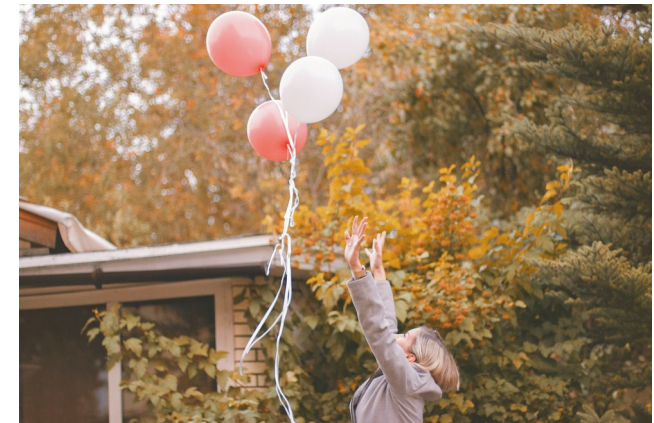
- modularer Code, agile Entwicklungsarbeit, offene Community

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

- sicherer, stabiler, nachhaltiger Base Layer mit Bare-Metal-Automation (OSISM)
- vollständiger IaaS Stack (inkl. OpenStack Xena)
- **föderationsfähig (OpenID Connect) & Gaia-X Federation Services**
- Operational Stack (Lifecycle Management, Monitoring, Alerting, ...) integriert
- K8s Cluster-API-basiertes Container-Cluster-Management (KaaS) (nur API/CLI)

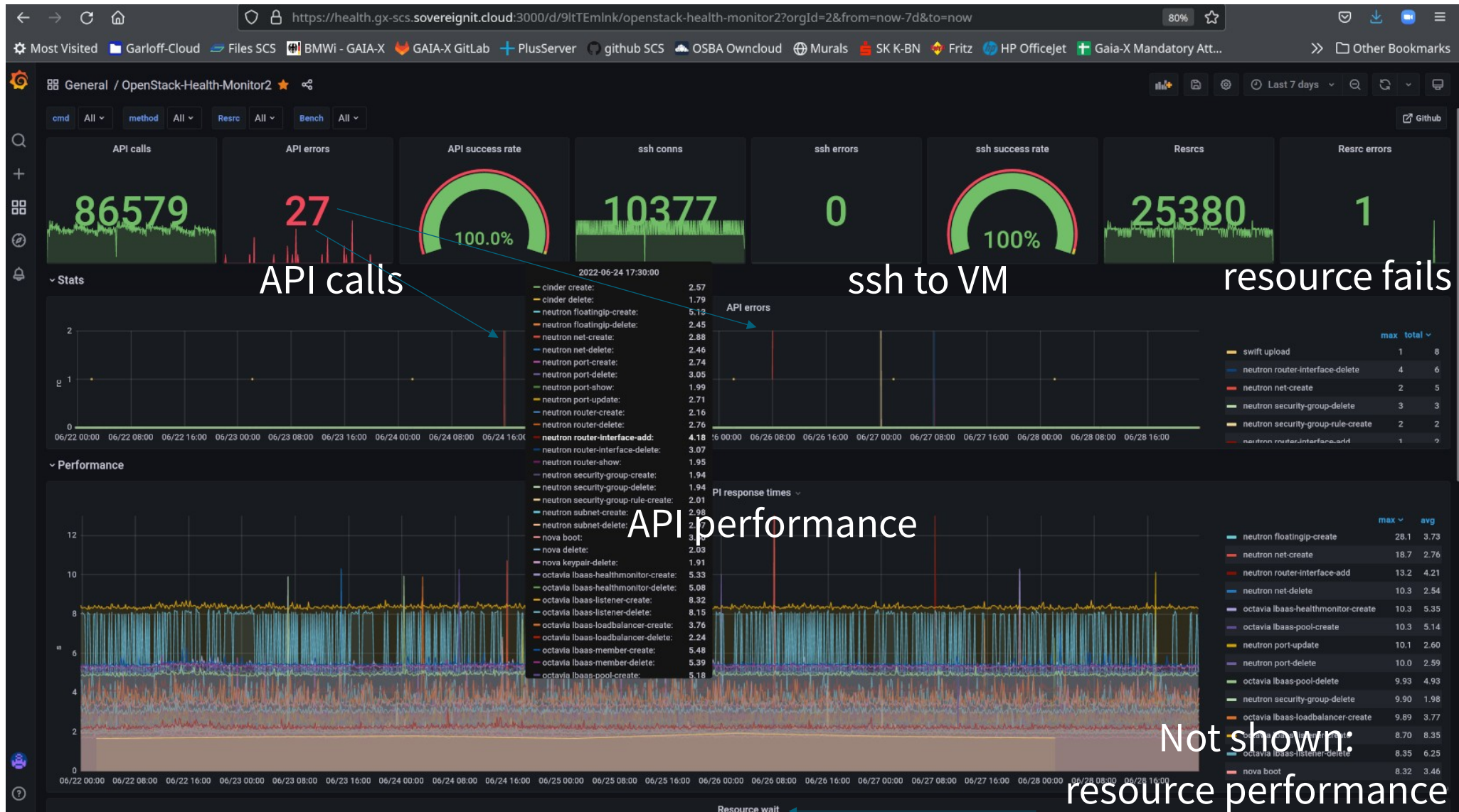
Roadmap für R3 (Sept 2022)

- Verschlüsselung aller Daten im Ruhezustand (Opt-out möglich)
- Standardisierung des k8s Cluster Management Provider-übergreifend (auch für nicht-SCS IaaS)
- Stärkung CI Framework und Abdeckung
- Conformance Tests für IaaS
- Dokumentieren und Validieren von IAM-Föderation-Anwendungsfällen
- Später: PaaS, Edge Setups, Netzwerkverschlüsselung, ...

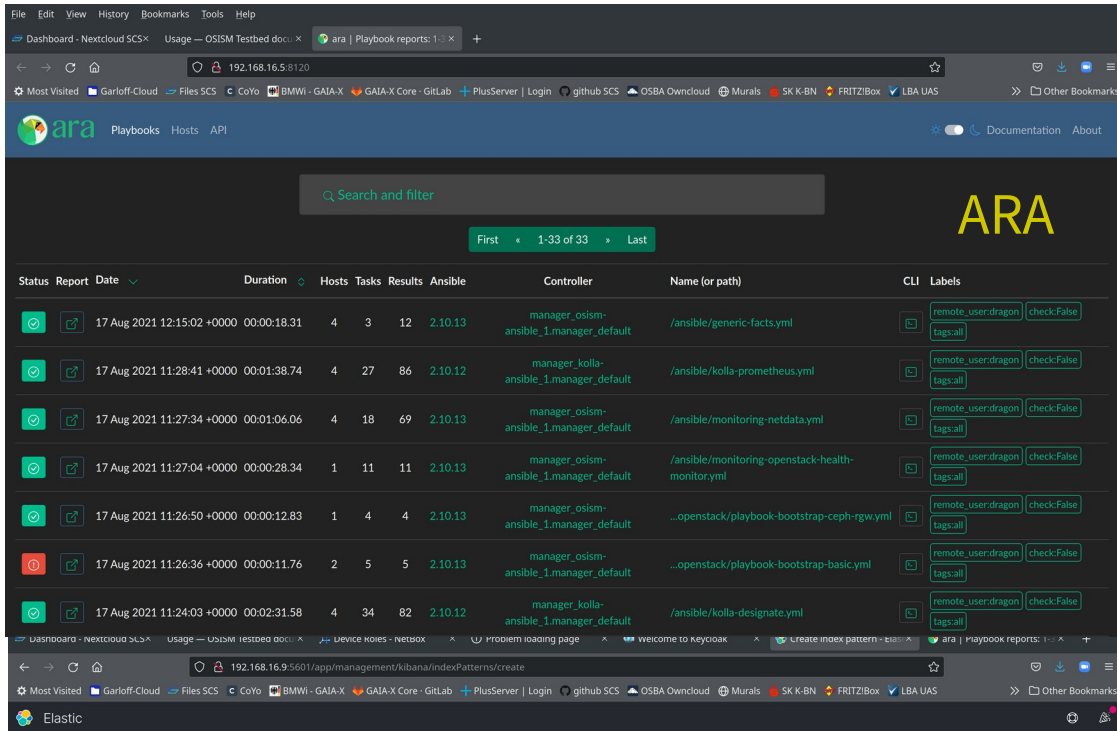


Operations:

Messbar machen, was gemanagt werden soll

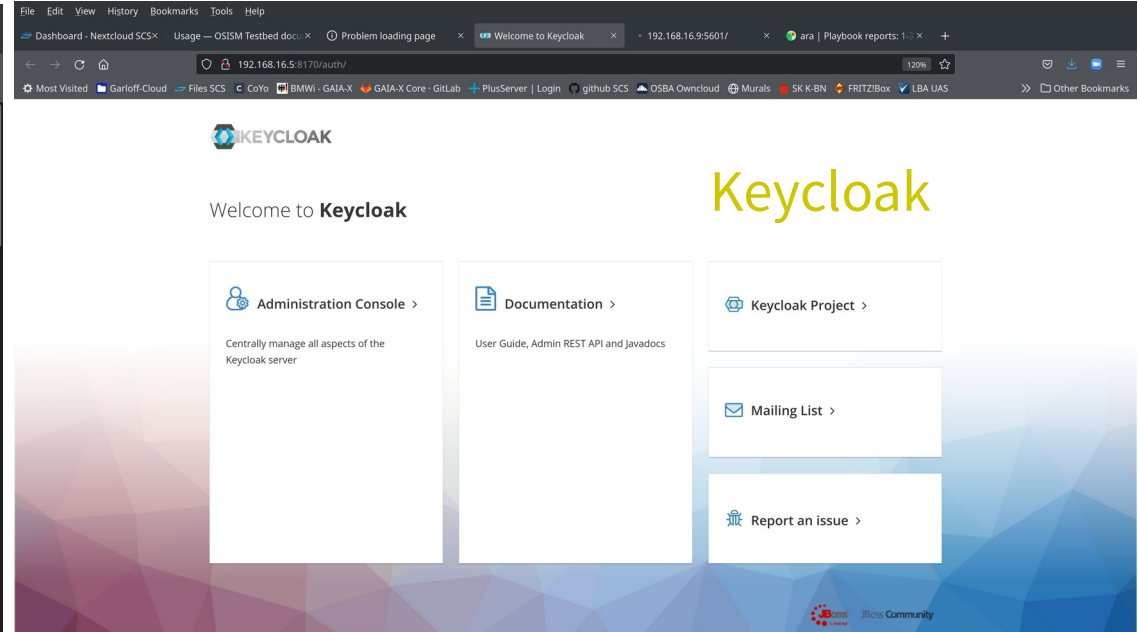


Operations: Betriebswerkzeuge

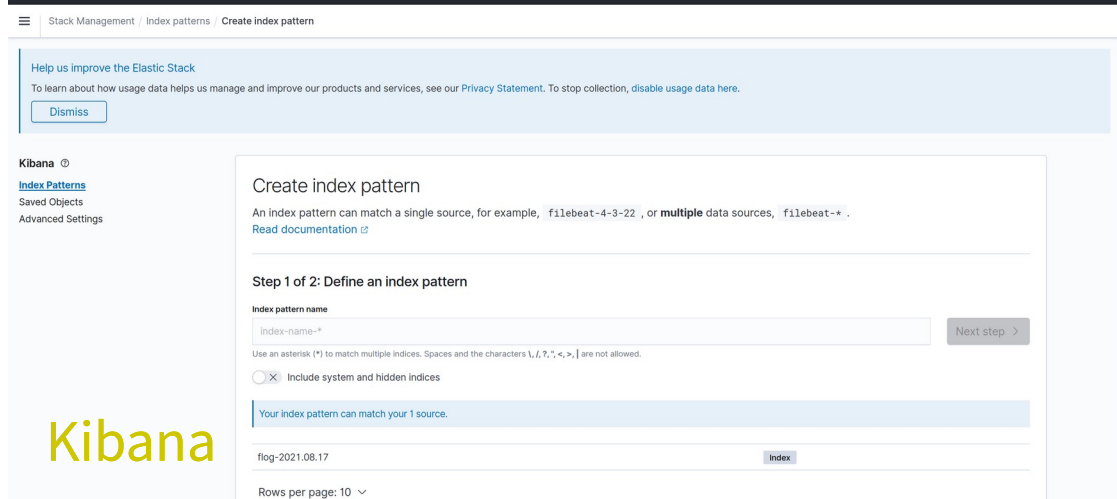


The screenshot shows the ARA web interface with a table of reports. The table has columns for Status, Report Date, Duration, Hosts, Tasks, Results, Ansible version, Controller, Name (or path), and CLI. The reports are sorted by date, showing various playbook runs from August 17, 2021.

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 tags:all	check:False
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 tags:all	check:False
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 tags:all	check:False
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 tags:all	check:False
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 tags:all	check:False
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 tags:all	check:False
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 tags:all	check:False



The screenshot shows the Keycloak Administration Console. It features a 'Welcome to Keycloak' message and several navigation links: Administration Console, Documentation, Keycloak Project, Mailing List, and Report an issue. The interface is clean and modern with a blue and white color scheme.



The screenshot shows the Kibana 'Create index pattern' form. It includes a title 'Create index pattern', a description, and a form field for the index pattern name. The form is currently empty, and the 'Next step' button is visible.

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

index-name-*

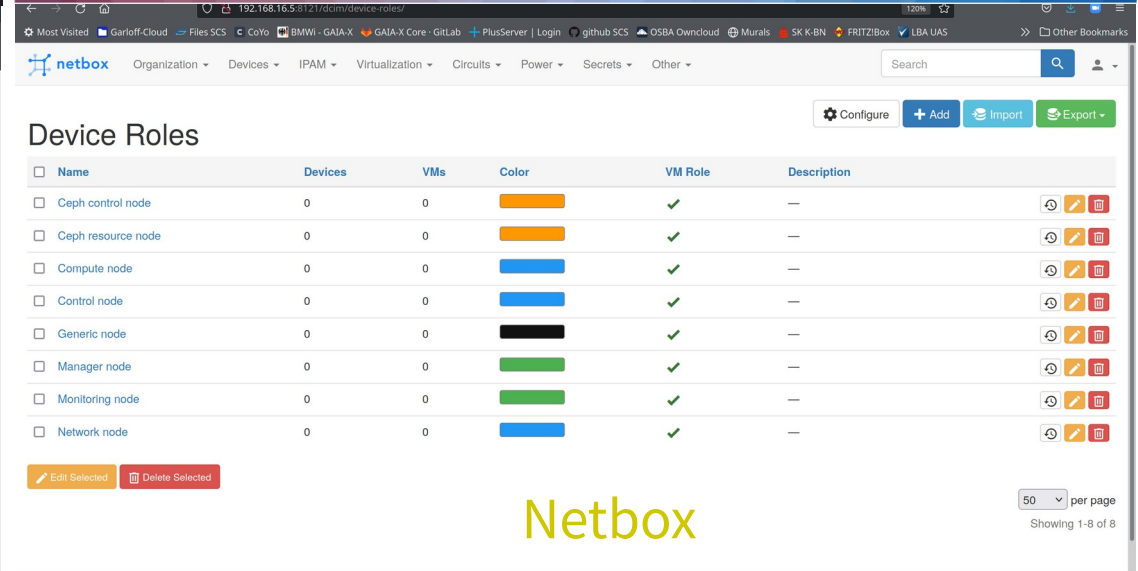
Use an asterisk (*) to match multiple indices. Spaces and the characters `\, /, *, <, >` are not allowed.

Include system and hidden indices

Your index pattern can match your 1 source.

filebeat-2021.08.17

Rows per page: 10



The screenshot shows the Netbox 'Device Roles' table. It lists various roles such as Ceph control node, Ceph resource node, Compute node, Control node, Generic node, Manager node, Monitoring node, and Network node. Each row includes columns for Name, Devices, VMs, Color, VM Role, and Description.

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

Open Operations: Weitere Pläne

weitere Werkzeuge (gut konfiguriert und dokumentiert)

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

Best Practices dokumentieren und teilen

- Knowledge Management offen verfügbar

Transparente Issue Resolution

- Public Root Cause Analyses

Public Dashboard / Status Page

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

=> **Entwicklung einer Open Operations Community**



Open Operations Culture

Share knowledge

e.g. monitoring setup and config

Share status

e.g. health & performance monitoring

Share challenges

e.g. fraud detection

Public Root Cause Analyses

e.g. outages

SCS resources:

Operational Docs

Operator Lean Coffee

Blog

Tools:

e.g. Health-mon dashboard

Next: RCA templates

Link collection

Open Operations Manifesto

SCS Zertifizierung



Stufen digitaler Souveränität

4: Transparente operative Praktiken und Austausch von Wissen

3: Transparente Technologie und die Gestaltungsmöglichkeit

2: Wahlfreiheit, Interoperabilität

1: Rechtskonformität (GDPR)

0: Keine

VMware vCloud
& Tanzu
AzureStack

OTC, OVH
IONOS cloud
Arvato/MSFT cloud
TSI/GCP cloud

AWS/Azure/GCP
AliBaba

StackHPC
C&H
StackIT
CityNetworks

Betacloud
PlusCloudOpen
Noris
...

SCS Zertifizierungsstufen



4: **“SCS-Sovereign”** – Ops/IAM Stacks sind ebenfalls durchgängig OSS, Transparenz bei Monitoring, Incidents, Contributions zu “Open Operation” (5x Open)

3: **“SCS-Open”** – SBOM für den funktionalen Stack vorhanden, durchgängig “open” (4x Open gemäß OpenInfra Foundation)

2: **“SCS-Compatible”** – Technische Kompatibilität, interoperabel (Conformance tests pass: CNCF, OIF, SCS)

1: ENISA / Gaia-X labels / GDPR – kein SCS-Zertifikat

SCS im Einsatz

Zwei Public Clouds mit vollständigen SCS IaaS/Ops/IAM Stacks seit Ende 2020 produktiv:



pluscloud open seit Nov. '21 BSI-C5-zertifiziert



Weitere Implementierungen

- vorauss 8/2022: dritte Public Cloud (vollst. SCS Stack); Thüringer Landesrechenzentrum (TLRZ) in 2023
- PoCs in Industrie und staatl. Verwaltung (dataport, Deutsche Verwaltungscloud Strategie)
- Gaia-X Lighthouse Projects
- Module bei den weiteren beteiligten Partner (s. SCS Homepage)
- Ökosystem an Servicepartner in Entwicklung (Training, Consulting, Implementierung, Support, ...)
- SCS Gitops Container Management Definition auch mit nicht-SCS-IaaS-Providern (WIP)

Validierung in Gaia-X Hackathons sowie durch Betacloud- und pluscloud open-Kunden

- Gaia-X Self-Descriptions: Gaia-X Working Group "Service Characteristics", Bachelor Thesis @ Cloud&Heat GmbH

Gaia-X Federation Services

- SCS ist Dev- und Validierungsplattform für Gaia-X Federation Services

Engagierte Unternehmen



23|Technologies



SPRIN-D



citynetwork



C CLOUDICAL

dataport

dilossacon

GONICUS
PIONEERS OF OPEN SOURCE

gridscale

LEITWERK
Die Zukunft Ihrer IT

noris network

Open
Infrastructure
FOUNDATION

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



OX Stay Open.

OSISM

OVHcloud

plusseryer

Stackable

Stackable GmbH

StackHPC

Syself

univention
be open

WAVECON

Join the SCS community!

Als Cloud-Service-Provider oder organisationsinterner IT-Service

- Mitwirkung (Diskussion, Use cases, Contributions...) in der offenen SCS Community
- Verwendung von Standards und/oder Technologie

Als OSS-Infrastruktur-SW-Entwickler

- Mitwirkung in der offenen SCS Community
- Als festangestelltes Mitglied im OSB Alliance Team

Als interessiertes Unternehmen

- Auftragnehmer für SCS oder eigenständige Mitwirkung
- Business Cases rund um SCS entwickeln

Als PaaS/SaaS Entwickler

- Gegen SCS-Standards entwickeln und testen.

Als Nutzer

- echte Souveränität von den genutzten Plattformen verlangen
- Transparenz und Standards verlangen

Weiter Informationen:

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, Service Characteristics

Email: project@scs.sovereignit.de

Matrix: SCS rooms

Backup

SCS platform features IaaS (as of R1) (optional standard)

OpenStack APIs (Victoria or newer – passing OpenStack powered Compute 2021.11)

- Core: User Management (keystone) with federation support (OIDC)
- Core: Block storage (cinder), Compute (nova), Networking (neutron), Image Mgmt (glance)
- Loadbalancer as a Service (octavia)
- Optional: DNS (designate), Orchestration (heat), Secrets (barbican)
- SCS Standardized flavor naming and standard flavors
- SCS Standardized image metadata (and image handling)

Optional standard, what does this mean?

- Some CSPs might decide to not expose the VM management layer or diverge in how they implement it, as their users might not need access on that layer (or don't need SCS compatibility there). If Operators decide to offer it, there is an SCS standard that ensures interoperability at that layer.

SCS features Object Storage and General

(mandatory for all SCS)

S3 compatible object storage (mandatory)

- Ceph backed (in reference implementation, CSPs can diverge)
- Optionally also exposed via OpenStack swift (in addition to S3 API)

Stay up-to-date with SCS releases (2x per year, Mar and Sep).

Fully open source stack, openly developed, openly operated, following GDPR and Gaia-X rules

Security principles (DC, isolation, updateability, sec response, supply chain transparency, private registry, ...)

Gaia-X self descriptions (WIP)

SCS platform features Container R2

(mandatory for all SCS)

Flexible k8s container management that allows on-demand scaling of clusters (adding and removing nodes, upgrading, etc.) using k8s-cluster-API

- Can be used by customer (or intermediary) via self-service (providing own cluster-API node with full access) or by provider to create a managed offering
- One or many k8s clusters per customer (tenant), no sharing by default

SCS k8s capi standards

- Kubernetes 1.19.x – latest (curr. 1.23.x) supported, can be chosen per cluster
- Clusters with 1/3/5 ... controller nodes, N worker nodes (with any SCS machine flavor), can be adjusted on the fly(!)
- OpenStack Cloud Controller Mgr (OCCM), CSI cinder persistent volumes, CNI (calico or cilium)
- Passes CNCF conformance tests (sonobuoy)
- Metrics Service included (opt-out possible)
- Cluster-admin credentials handed to user, full control over cluster, k8s API access via internet
- Optional pre-install: nginx ingress controller (uses OpenStack Loadbalancer via OCCM)
- Optional pre-install: cert-manager
- Optional pre-install: flux2 gitops tooling
- Optional pre-install: private container image registry (harbor)

K8s cluster management vision: gitops

Keep description of desired clusters as YAMLs in git

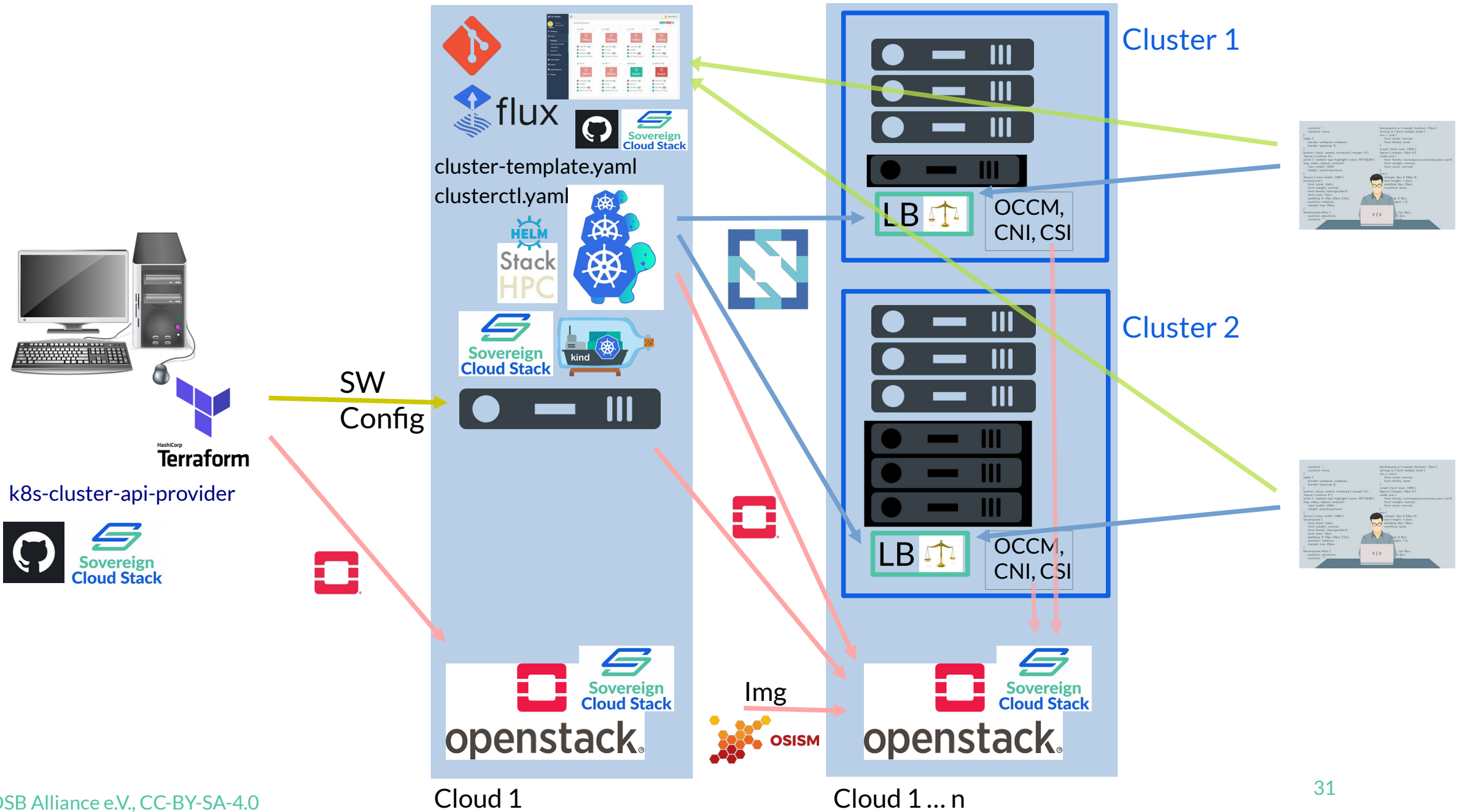
- Declarative description of desired state ...
- Avoid dependence on SCS IaaS / OpenStack (abstract description with neutral CAPI provider & CCM)

Gitops reconciliation (using flux or Argo):

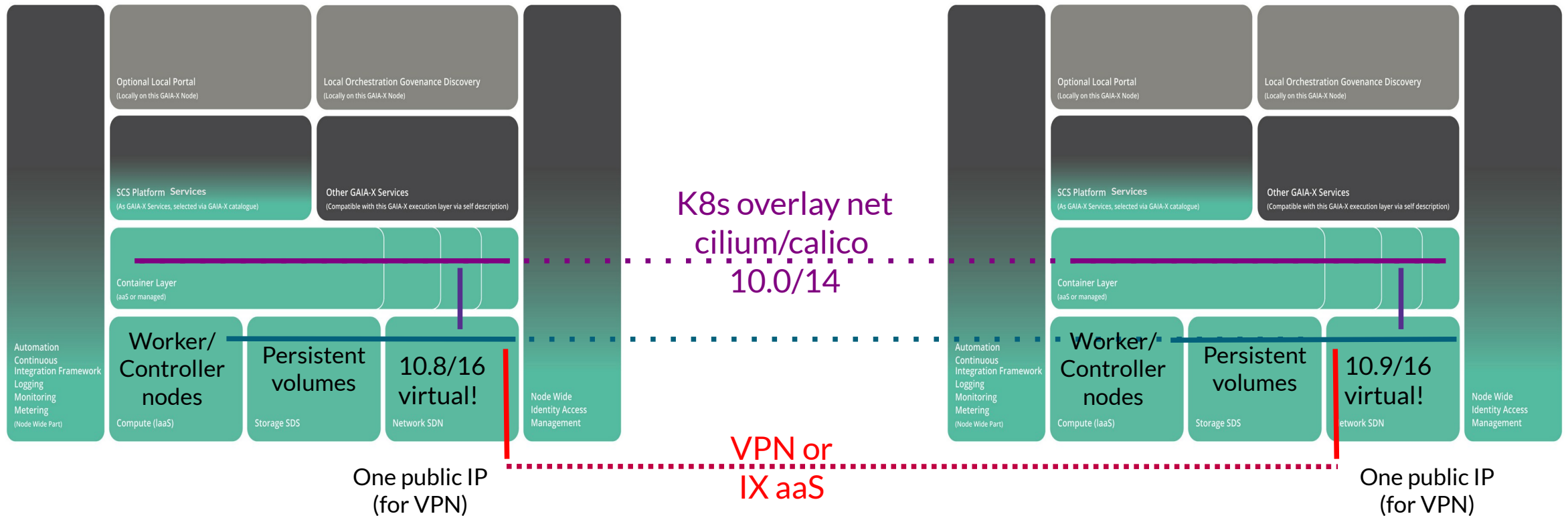
Lifecycle management for the desired clusters from git repos/branches:

- Create projects (optional) and application credentials
- Ensure images are available
- More pre-flight health checks (quota etc. - TBD)
- Ensure we have anti-affinity rules configured (optional)
- Ensure we have the security groups set up (for cilium/hubble – optional)
- Create/change clusters (via cluster API)
 - Scaling
 - Includes support for rolling upgrades by automatically cycling machine descriptions (helm)
 - Includes optional deployment of standardized services (OCCM, CNI – calico or cilium, CSI, optional: metrics, cert-manager, flux, nginx-ingress, harbor registry, ...)
 - Optionally running tests (CNCF conformance, connectivity, storage, ...)

K8s Cluster deployment structure - gitops



Cross-provider cluster networking



How is it developed?

Upstream communities

- OIF: OpenStack, kolla-ansible, kayobe, zuul, ...
- CNCF: kubernetes, helm, harbor, openstack-capi-provider
- LF: Linux, KVM, ceph, ...
- OSISM: Integration, Ops tooling (<https://github.com/OSISM/>)

SCS community

- <https://github.com/SovereignCloudStack/Docs>
<https://scs.community/docs/contributor/>
- Contributions from providers, users, volunteers
- IP policy (Various FOSS licenses, Four Opens, DCO, SPDX)
- Paid development via public tenders (BMW funded): <https://scs.community/Tender/>
- Development performed in agile teams coordinated by POs (@OSBA)
- Align with upstream and contribute back

Collaboration

- Weekly sprints: Sprint reviews, backlog refinement, sprint planning via weekly VC (Jitsi)
- Weekly team call (Thu afternoon, SCS Jitsi)
- Taskboard (nextcloud deck, trello-like)
- Github: Reviews, PRs, Issues
- Mailing list

How to get started? How to join?

Test testbed ...

- Virtual deployment of SCS for testing, exploring, demos, CI,
 - You need access to a reasonably vanilla OpenStack
 - OR: You can help us port the terraform recipes to VMware, AWS, ...
- Ask questions, raise issues, submit PRs (with DCO)

Contribute upstream

Join the SCS community

- Become a regular contributor ...
- Onboarding call to understand interests, needs, skills, contribution areas ...
- Participate in team calls (Thu 15:00 CEST) and sprint reviews (Mon, Wed, Thu 10:00 CEST)
- Onboarding to nextcloud and mailing lists
- Participate in tenders

Use SCS

- Create production setups for internal usage or as public clouds
 - Support available via partners (e.g. osism.tech)
 - Certification conformance tests in development
- Develop apps/services for SCS container/cloud platform (preferably with k8s operators)
- Become skilled to offer services around SCS (partner certification program in preparation)