Sovereign Cloud Stack

gaia-x

Berner Fachhochschule – IT-Beschaffungskonferenz 2022

Agile Open-Source-Entwicklung und öffentliche Beschaffung – wie geht das zusammen?

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

project@scs.sovereignit.de

2022-08-24

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

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Was ist der Sovereign Cloud Stack?

Sovereign Cloud Stack

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

Ein Beitrag zu digitaler Souveränität bei Cloud-Services.

- Projekt, 2021 – 2024
- Community von Entwicklern, Betreibern, Nutzern und Bedarfsträgern von Cloud-Technologien und -Services

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

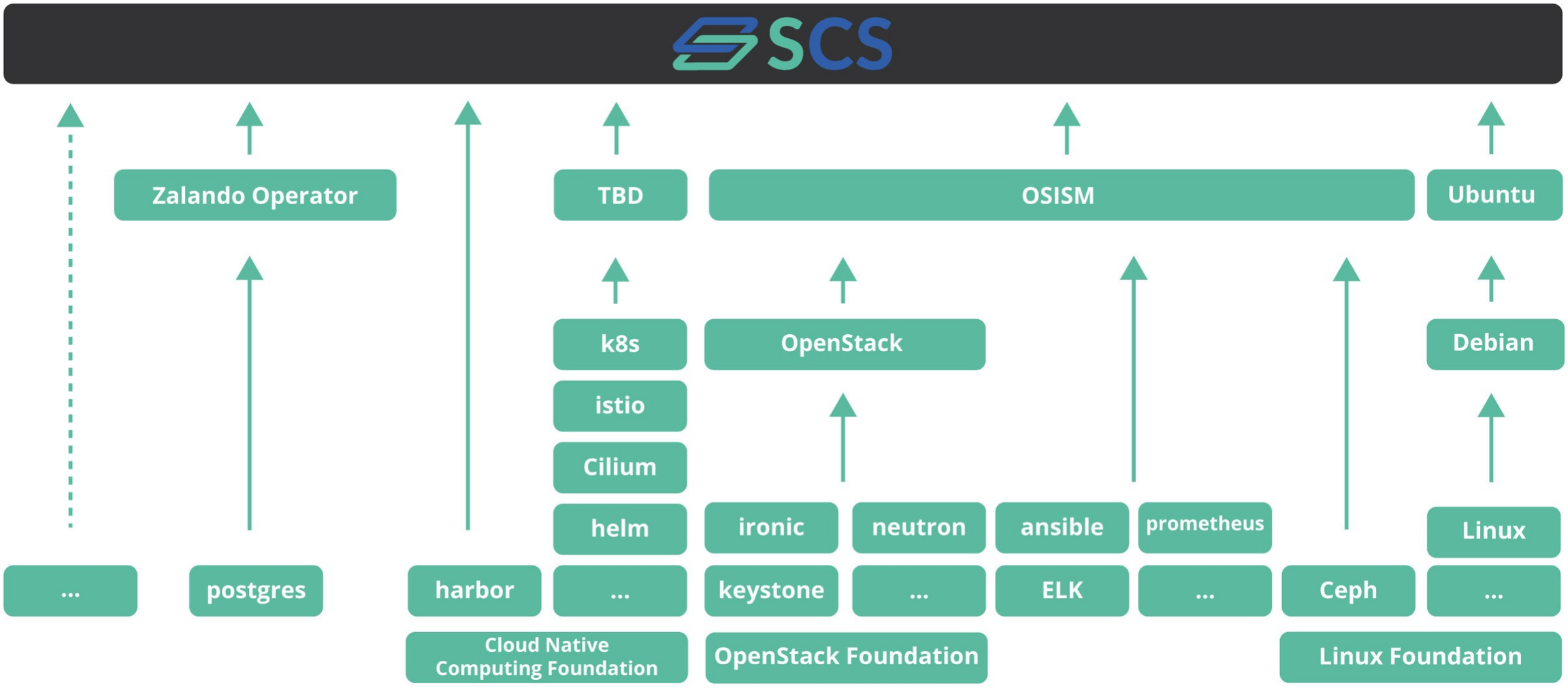
Engagierte Unternehmen

StackHPC Ltd

SCS Vision und Ziele

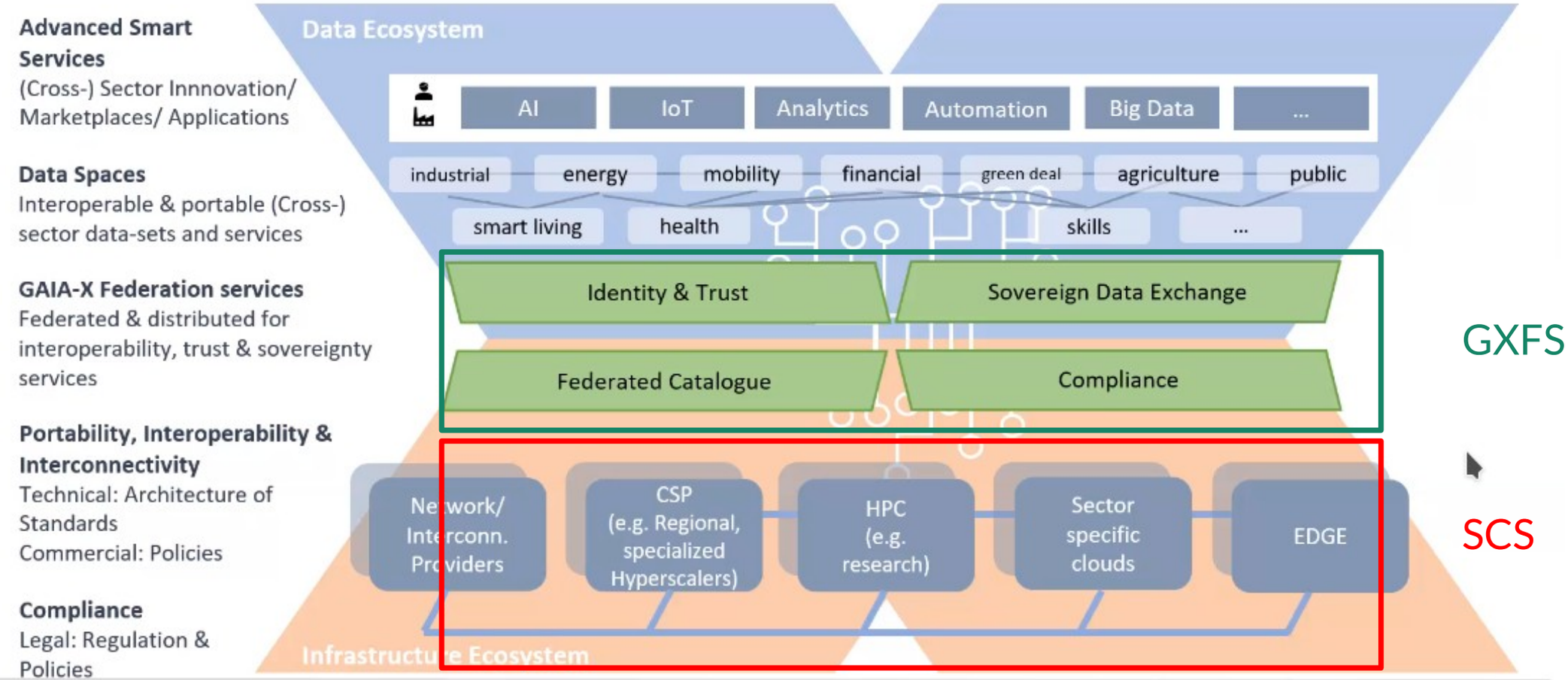
- Open Source Toolbox für Cloud- und Container-Infrastruktur
- Standardisierung von Schnittstellen und Komponenten
- Föderierung möglich machen
- Zertifizierung: digitale Souveränität nachweisbar machen
- Transparenz: Offenheit und Partizipation
- Nachhaltigkeit

How is it built? (SCS developer perspective)



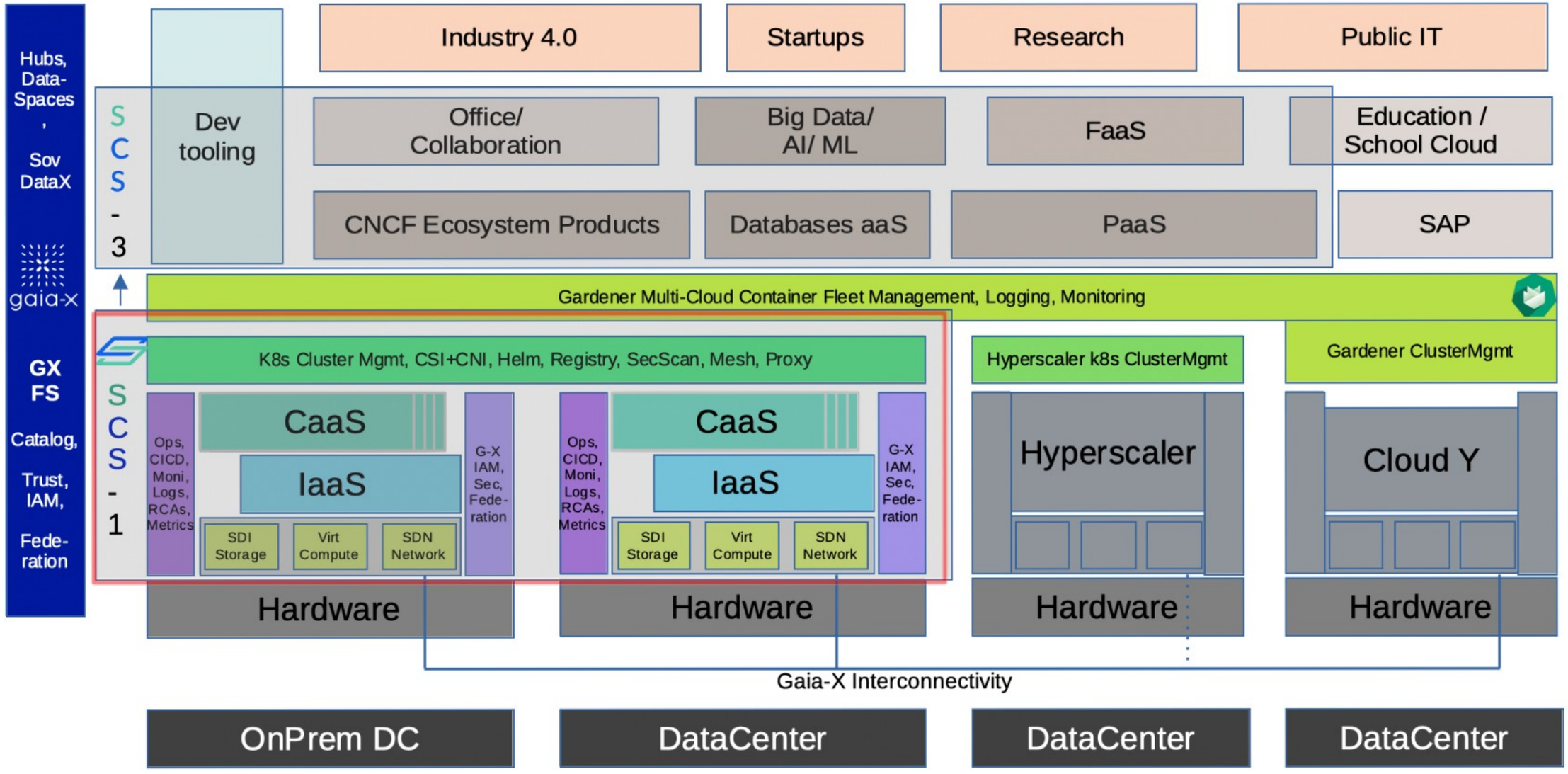
Sovereign Cloud Stack and Gaia-X

Gaia-X in One (Big) Figure



IT Ecosystem with Gaia-X

adapted from Acatech whitepaper



Vergabe von SCS-Aufgaben-paketen:

(Stand 28.07.2022)

https://scs.community/de/tenders/

#	Name	Beschreibung	Start	Abgabefrist	Link zum Vergabeportal
1	Betriebswerkzeuge, Testabdeckung durch CI/CD für Infrastruktur und IaaS, BareMetal als Dienst, Lifecycle Management	Paket 1	2021-07-30	2021-08-20	~~SCS-VP01~~
2	Wissensmanagement für Betriebsprozesse, Herstellung von Transparenz bei den Cloudanbietern	Paket 2	*tba*	*tba*	*tba*
3	Speichertechnologie	Paket 3	*tba*	*tba*	*tba*
4	Netzwerktechnologie	Paket 4	*tba*	*tba*	*tba*
5	Integration von Kubernetes als Dienst (KaaS)	Paket 5	*tba*	*tba*	*tba*
6	Container Netzwerk und Container Speicher Integration	Paket 6a	*tba*	*tba*	*tba*
7	Container Meshing und Proxy	Paket 6b	*tba*	*tba*	*tba*
8	Container Registry / Scanning	Paket 6c	2022-06-29	2022-07-21 T12:00+01:00	~~SCS-VP6c~~
9	Container Monitoring / IaC / CI / Installationsautomatisierung	Paket 6d	2021-12-22	2022-01-19	~~SCS-VP6d~~
10	Container Tracing & Audit	Paket 6e	*tba*	*tba*	*tba*
11	Nutzermanagement und Föderierung	Paket 8	2022-02-28	2022-03-22	~~SCS-VP08~~
12	Infra Scanning / Isolierung / Policymanagement	Paket 9a	*tba*	*tba*	*tba*
13	Lieferkettenabsicherung	Paket 9b	*tba*	*tba*	*tba*
14	Penetration Testing	Paket 9c	*tba*	*tba*	*tba*
15	SCS Zertifizierung	Paket 10	2021-11-12	2021-12-07	~~SCS-VP10~~
—	SCS Zertifizierung	Paket 10	2022-01-12	2022-01-27	~~SCS-VP10-2~~
—	**SCS Zertifizierung**	Paket 10	2022-06-24	2022-08-02 T12:00+01:00	SCS-VP10-3
16	Aufbau Serverhardware	Paket 11	*tba*	*tba*	*tba*

Charakteristika der Aufgabenpakete

- Rahmenvereinbarungen über Programmier- oder sonstige Dienstleistungen oder Forschungs- & Entwicklungsaufträge
- Volumina: 100 – 2.300 k€ (inges. ca. 10 Mio. €)
- Laufzeit i.d.R. bis zu 3 Jahren (bis Projektende Sept. 2024)
- agiles Projektmanagement (Scrum),
  Steuerung durch Product Owner der OSB Alliance
- volle Einbindung in die Entwicklungsarbeit der offenen
  SCS Community
- Kenntnis der eingesetzten Open-Source-Technologien erforderlich

Ausschreibungsverfahren

1. in der Regel öffentliche Ausschreibung über „DTVP“(Deutsches Vergabeportal)
2. Rechtsgrundlage: UVgO (Unterschwellenvergabeordnung)
3. Leistungsbeschreibung
4. Bewerbungsbedingungen:
    1. Anforderungen an das Unternehmen
    2. Anforderungen an das Personal
5. vorgegebener Tagessatz von ca. 600 € p.d. => Qualitätswettbewerb
6. Zuschlagskriterien

Bewerbungsbedingungen

am Beispiel „IaC- und Kubernetes-Werkzeuge“

Auftragsgegenstand:

Rahmenvereinbarung über Programmier- und sonstige Dienstleistungen zur Entwicklung von *Infrastructure-as-Code-(IaC)-Werkzeugen zu automatisierter Bereitstellung und Betrieb von Anwendungen auf virtueller/containerisierter Infrastruktur sowie von Werkzeugen rund um Kubernetes zur Installationsautomatisierung, CI-Testautomatisierung von Containertools und zum Monitoring*

- Begründung für Rahmenvertrag: agile Arbeitsweise; konkrete Einzelabrufe ergeben sich aus monatlicher Arbeitsplanung
- keine Mindestabnahmeverpflichtung; Höchstabnahmegrenze entspr. Auftragswert
- 2-3 Berater:innen mit Erfahrungen in den relevanten OS-Technologien; müssen insgesamt das geforderte Qualifikationsspektrum abdecken
- Austausch von Beratern nur mit Einwilligung des Auftraggebers
- fachliches Konzept
- geschätzter Leistungsumfang von x Personenmonaten à 16 Arbeitstage
- festgelegter Tagessatz von EUR 575 netto
- => Zuschlagskriterien ausschließlich qualitativer Natur

Leistungsbeschreibung

- ***keine*** Beschreibung genau definierter Endprodukte, sondern:
  planerische und konzeptionelle Arbeit, Entwicklung von Software und Automatisierung, Testentwicklung, Fehleranalyse, Dokumentation

A) Funktionale Anforderungen, Beschreibung der Aufgabenpakete:

1. Werkzeuge rund um Kubernetes:
   Installationsautomatisierung, CI-Testautomatisierung (Containertools), Monitoring,
   z.B.: Bereistellung von *helm*, Pflege & Update, Rahmenwerk für CI-Tests, gitops-Schablonen, gitops-Tooling für Entwickler *(gitops*, *flux2*, *GitHub actions*, *policies…)*, Bereitstellung von Monitoring für den Kunden, Bereitstellung von Daten aus der zugrundeliegenden Infrastruktur (*cortex*) geschätzter Aufwand: 38 Personenmonate

2. IaC-Werkzeuge:
   … *(ansible*, *terraform...)*… geschätzter Aufwand: 28 Personenmonate

Leistungsbeschreibung

B) Nicht-funktionale Anforderungen, Qualität der Arbeit:

- **Codequalität**: Einhaltung von Standards; Refaktorierung von Code in sauber abgegrenzte Daten- und Codestrukturen mit definierten Schnittstellen; Dokumentation von Code.
- **Testabdeckung**: Code wird immer mit Tests entwickelt, die parallel in die Testrahmenwerke eingepflegt werden. Die Testergebnisse werden sorgfältig und täglich beachtet; sollten Tests fehlschlagen, so werden der Code oder die Tests kurzfristig korrigiert.
- In Architektur und Implementierung werden Fehler und bösartige Angriffe mit bedacht und angemessen behandelt; sicherheitsrelevante Risiken werden so an der Wurzel erkannt, adressiert und durch Testfälle abgesichert. Relevante **Sicherheitsstandards** werden umgesetzt und eingehalten.
- Der Auftragnehmer sorgt für **Datenschutz und IT-Sicherheit** nach den geltenden rechtlichen Bestimmungen sowie den allgemein anerkannten Standards hinsichtlich Sicherheit und Sorgfalt nach dem **Stand von Wissenschaft und Technik**.
- **Entwicklerdokumentation** wird parallel mit dem Code entwickelt.
- Entwicklungsfortschritte werden mehrmals täglich in die **öffentliche Codeverwaltung** eingepflegt und somit den Teamkolleg:innen zur Verfügung gestellt.
- **Fortbildung**: Die Mitarbeitenden bilden sich entsprechend der Arbeitsfortschritte fort. Insbesondere nehmen sie auch das weitergegebene Wissen im Team an und bieten ihrerseits an, ihre Arbeit und das dazu notwendige Wissen vorzustellen.
- Die Vorstellung von Erkenntnissen und Arbeitsergebnissen auf den SCS-Konferenzen und auch auf externen **Konferenzen** ist ausdrücklich erwünscht. Ebenso sind Berichte ins Team von auf externen Konferenzen erlangtem Wissen ausdrücklich erwünscht.
- Die Arbeit der Kolleg:innen im **Team** wird verfolgt und durch Kommentare, Reviews, Hinweise unterstützt. Ebenso werden die Kommentare und Reviews der Kolleg:innen angenommen und berücksichtigt.

Anforderungen an das Unternehmen

- (Eintragung ins Berufs- und Handelsregister)
- **wirtschaftliche und finanzielle Leistungsfähigkeit:**
  Umsatz in den letzten drei Jahren im auftragsgegenständlichen Tätigkeitsbereich
- **technische und berufliche Leistungsfähigkeit:**
  mind. drei geeignete Referenzen über Aufträge aus den letzten drei Jahren im auftragsgegenständlichen Tätigkeitsbereich;
  qualitative Mindestanforderungen:
  - Erfahrung bei der Entwicklung von Automatisierung bei der Verwaltung von virtueller/containerisierter Infrastruktur
  - Entwicklung von Automatisierung und bewährten Vorgehensweisen zur Verwaltung von Diensten und Anwendungen auf solch automatisierter Infrastruktur
  - Erstellung von Dokumentation und Testverfahren für diese Automatisierung
  - Erfahrung mit Werkzeugen zur Überwachung und Analyse, Kontrolle und Sammlung von Metriken aus der Containerinfrastruktur und den dort installierten Diensten
  - Kenntnis der eingesetzten Technologien:
    - ansible, terraform
    - kubernetes
    - helm
    - flux, gitops
    - github actions
    - prometheus, cortex/thanos
  - öffentlich sichtbare Beiträge oder wichtige Rollen bei relevanten Upstream-Open-Source-Projekten

Anforderungen an die Entwickler

- fachliche Erfahrung in den relevanten **Open-Source-Technologien** wie in Leistungsbeschreibung genannt
- Erfahrung in der **agilen Projektarbeit** (Scrum)
- **Share early, share often**: Beiträge zu Upstream- (und anderen relevanten) Communities erwartet
- **Fehlerkultur**: gründliche und reproduzierbare Analyse und Dokumentation von Fehlern; nicht nur Code, sondern auch automatisierte Testfälle für CI-Rahmenwerk
- gute Strukturierung und **Dokumentation** zu Code, Testfällen, Rahmenwerk etc.
- Teilnahme an **Konferenzen** (SCS und andere)
- kontinuierliche **Fortbildung**
- Berater/Entwickler werden *nicht* in Arbeitsorganisation der OSB Alliance eingebunden; fachliches (und disziplinarisches) Weisungsrecht verbleibt beim Auftragnehmer
- Auftragnehmer berät den Auftraggeber bei **konzeptionellen Fragen**, **methodischer Umsetzung** und Feinsteuerung

Zuschlagskriterien

- **Wertung:**
  - festgelegter Tagessatz EUR 575 netto
  - Qualität des fachlichen Konzepts 40 %
  - Qualität der Berater:innen 60 %

Zuschlagskriterien - Qualität des fachlichen Konzepts

- fachlich-inhaltliche Beschreibung
- methodische Entscheidungen
- Auswahl von Technologien und Werkzeugen
- Überprüfung der Ergebnisse
- Dokumentation

Wertungspunkte:

- 0 (nicht erfüllt)
- 2,5 (unterdurchschnittlich erfüllt)
- 5,0 (durchschnittlich erfüllt)
- 7,5 (überdurchschnittlich
- 10,0 (weit überdurchschnittlich)

Zuschlagskriterien – Qualität der Berater:innen

CV für jede:n Berater:in

- Welche Kompetenzen und **Erfahrungen in Open-Source-Projekten** liegen vor?
- Welche davon sind auf Grundlage **allgemein zugänglicher Informationen** nachvollziehbar?
- Welche Erfahrungen bezüglich **agiler Arbeitsmethoden** (z.B. Scrum) sowie Zusammenarbeit in agilen Teams etc. liegen vor?
- Welche **technologischen Kompetenze**n bei Entwicklung und Automatisierung von virtueller/ containerisierter Infrastruktur und der Verwaltung von Anwendungen darauf liegen vor?
- Welche technologischen Kompetenzen und Erfahrungen bezüglich der Analyse und Überwachung von containerisierten Anwendungen und der Infrastruktur liegen vor?
- Welche Kompetenzen und Erfahrungen aus dem **gesamten Spektrum** der zu erwartenden Arbeit (Konzeption/Architektur, Planung, Entwicklung, Tests, Fehleranalyse, Dokumentation) liegen vor?

Zuschlagskriterien – Qualität der Berater:innen

Wertung der CVs:

- 10,00 Wertungspunkte Die Angaben belegen eine **weit überdurchschnittliche** Qualifikation und Erfahrung des angebotenen Beraters für den ausgeschriebenen Auftrag. Der Berater verfügt über herausragende Erfahrungen in einer Vielzahl o.g. Bereiche (Open Source, agile Arbeitsmethoden, zu validierende Technologien und Prozesse etc.).
- 07,50 Wertungspunkte Die Angaben belegen eine **überdurchschnittliche** Qualifikation und Erfahrung des angebotenen Beraters für den ausgeschriebenen Auftrag. Der Berater verfügt über überdurchschnittliche Erfahrungen in einer Vielzahl o.g. Bereiche (Open Source, agile Arbeitsmethoden, zu validierende Technologien, Prozesse etc.).
- 05,00 Wertungspunkte Die Angaben belegen eine **durchschnittliche** Qualifikation und Erfahrung des angebotenen Beraters für den ausgeschriebenen Auftrag. Der Berater verfügt über durchschnittliche Erfahrungen in den o.g. Bereichen (Open Source, agile Arbeitsmethoden, zu validierende Technologien, Prozesse etc.).
- 02,50 Wertungspunkte Die Angaben belegen eine zwar **unterdurchschnittliche, aber noch gegebene** Qualifikation und Erfahrung des angebotenen Beraters für den ausgeschriebenen Auftrag. Der Berater verfügt über durchschnittliche Erfahrungen in wenigen der o.g. Bereiche (Open Source, agile Arbeitsmethoden, zu validierende Technologien, Prozesse etc.).
- 00,00 Wertungspunkte Die Angaben belegen nicht die Qualifikation und Erfahrung des zum Einsatz kommenden Beraters für den ausgeschriebenen Auftrag. Der Berater verfügt über **keine Erfahrungen** in den o.g. Bereichen (Open Source, agile Arbeitsmethoden, zu validierende Technologien, Prozesse etc.).

Einbindung in die Entwicklungsarbeit

- **SCS Teamarbeit**:
  - agiles Projektmanagement (Scrum)
  - 14tägige Sprint-Planung unter Leitung und Priorisierung durch SCS Product Owner (Team Infra & IaaS, Team Container, Team Operations & IAM)
  - Mitarbeit in „Special Interest Groups“ (SIG Monitoring, SIG Standardisation/Certification, …) und Open Hacking Sessions
- „**Monthly**“ mit Projektleitung
- **SCS-Konferenzen** viertel- bis halbjährlich
- kontinuierliche Entwicklung und Integration, dennoch halbjährliche **Releases**: konsolidierte Dokumentation, Kommunikation, Retrospektive, Fortschrittsbericht
- Planung und **Ergebnisse** auf offenen Code-Hosting-Plattformen https://github.com/SovereignCloudStack
- **Leistungsnachweise** müssen in GitHub-Planung und Team-Kalender nachvollziehbar sein
- jährlicher **Review** (und Kündigungsmöglichkeit)

Herausforderungen

- insbesondere kleinere Unternehmen oft nicht vertraut mit öffentlichen Vergabeverfahren
- Verfahrenssprache Deutsch
  (Angebote können jedoch auch in Englisch eingereicht werden)
- Markterkundung: entsprechend erfahrene Unternehmen finden
- Fachkräftemangel
- niedriger Tagessatz
- Compliance (Interessenkonflikte ausschließen)
- Management mit sehr kleinem SCS-Team

Sovereign Cloud Stack

gaia-x

Vielen Dank für Ihre Aufmerksamkeit! Fragen, Anregungen, Kommentare...?

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

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Backup

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 (BMWi 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 helps 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)

SCS Roadmap (non-technical)

Growing the team & community

- Initial funding via SPRIND, public funding (BMWi) since 7/’21 – 14.9M€
- Growing project team @ OSB Alliance
- Growing contributions (volunteers)
- Paid development work via public tenders

Adoption

- Public Clouds: Betacloud Solutions (2020), PlusCloud Open (12/2020), ….
- Industry Partners: (Automotive, Commerce, …)
- Public Sector: DVS – looking for pilot / PoC partners
- Gaia-X Hackathon #2: TEF, C&H, intel?, IONOS?

Ecosystem

- Building skilled support, implementation, training partners
- Platform services on top of well-defined SCS standards

Add-ons:

SCS-2: Edge (project proposal in IPCEI-CIS, WIP)

- Even smaller simplified stacks (limited multitenancy), but w/ special acceleration / realtime requirements, bare metal

SCS-3: PaaS&Dev (project proposal in IPCEI-CIS, WIP)

- Integrate set of Platform services and Dev Tooling as SCS-standardized modules

Sovereignty & SCS certification

Levels of digital sovereignty

4: Operational transparency and knowledge available (skills building)

3: Technological transparency and capability to contribute & shape

2: Choice b/w many providers, insourcing (on-prem) option

1: Legal compliance (GDPR)

0: None

SCS certification levels

4: "SCS-sovereign" – Ops/IAM stacks OSS as well, transparency on monitoring, incidents, contributing to OpenOperations (5 x open)

3: "SCS-open" – SBOM for functional stack available and fully OSS (4 x open)

2: "SCS-compatible" – technical compatibility (conformance tests pass: CNCF, OIF, SCS)

1: None (rely on ENISA / Gaia-X labels / Law)

Betacloud
PlusCloudOpen
Noris
…

StackHPC
C&H
StackIT
CityNetworks

VMware vCloud
& Tanzu
AzureStack

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

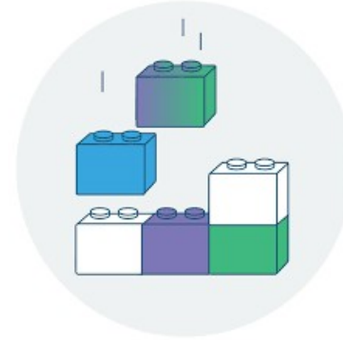
AWS/Azure/GCP
AliBaba

Notes: Levels build on top of each other
SCS reference implementation not required anywhere (but makes passing a lot easier)

Status Quo

Hyperscaler dominieren den Markt

- Abhängigkeiten (ökonomischer, strategischer oder juristischer Natur) → Digitalisierungshemmnis
- Zentrale Kontrolle über die Plattform und den verarbeiteten Daten
- Kontrolle und Wertschöpfung findet außerhalb Europas statt



Es gibt Open Source Alternativen, aber...

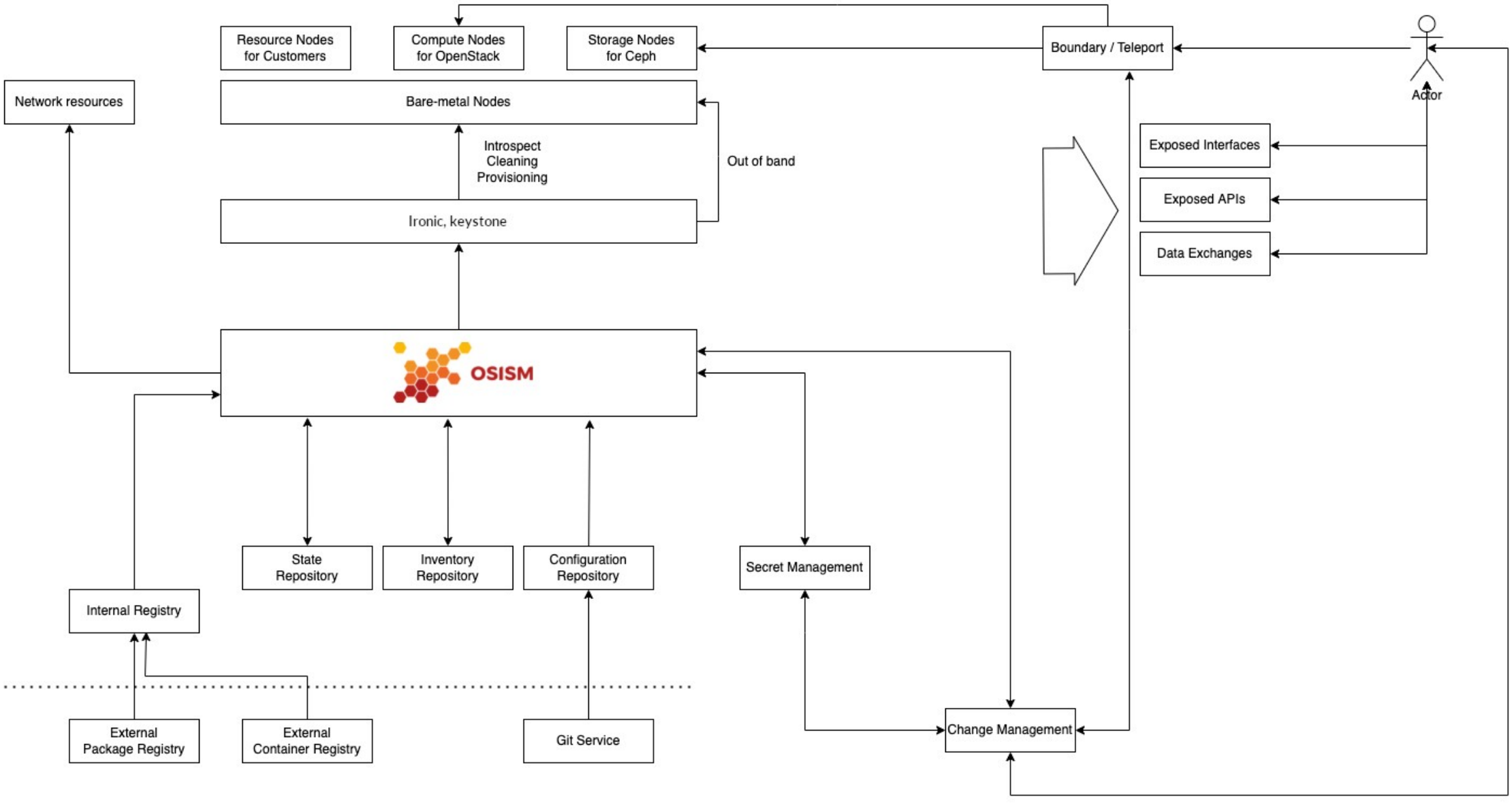
- die meisten Unternehmen, Institute und CSP, die offene Alternativen anbieten/betreiben, arbeiten lose für sich,
- der Betrieb einer solchen Plattform ist hochkomplex,
- erfahrene IT-Fachkräfte fehlen auf dem Arbeitsmarkt,
- erfindet jedes Team das Rad neu (beispielsweise im Bereich Integration, Testing, Zertifizierung, Betriebsautomatisierung, etc.),
- viele zueinander inkompatible Lösungen bilden in der Summe keine Alternative.

Sovereign Cloud Stack...

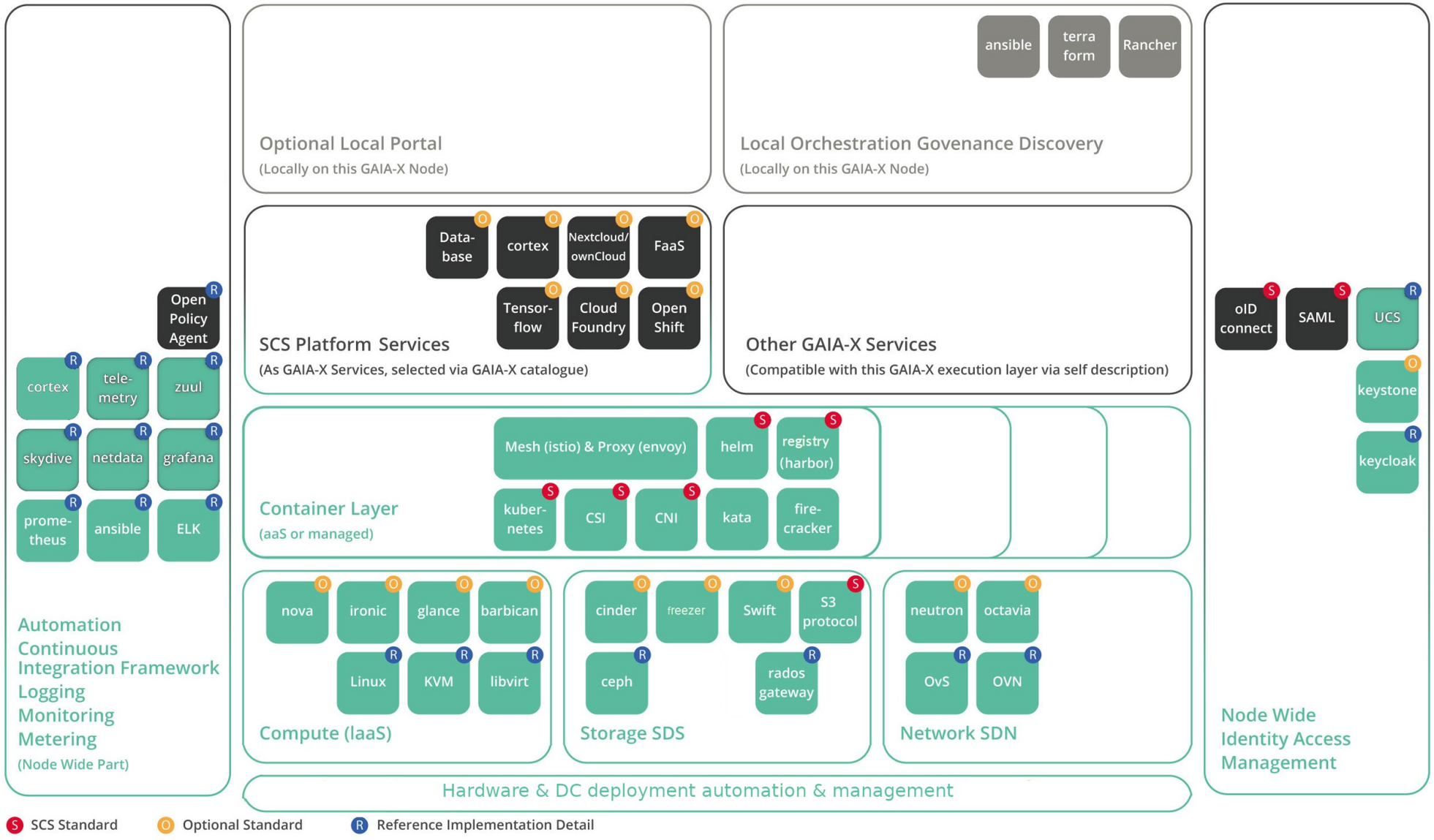
- bringt diese hochqualifizierten Teams zusammen, um gemeinsam zueinander kompatible Lösungen zu entwickeln und Standards zu etablieren,
- stellt Marktbedingungen wieder her und ermöglicht lokale Wertschöpfung,
- stärkt somit den Fortschritt bei der Digitalisierung in Europa, ohne dabei größere Risiken von Kontrollverlust über Technologie und Daten mit sich zu bringen.

Architektur von SCS

SCS DC Hardware Management (OSISM)



SCS Architektur



SCS Roadmap (technical)

Releases

- Release 0: (2021-07-14)
  - Fully automated Infra, IaaS, Ops automation (CI/CD, Monitoring, Patching), local IAM
  - Technical Preview for Container Stack (k8s cluster API, incl. CNI/CSI, helm)
- Release 1: (2021-09-29)
  - Container Stack in production quality
  - Federation (OIDC, ~~SAML~~)
  - More preconfigured monitoring and logging
- Release 2: (2022-03-23)
  - More Container work (cluster API, k8s, registry, multi-AZ/multi-cloud, rolling upgrades in prod)
  - Ops Stack: More preconfigured Metering, Monitoring, Logging, Alerting
  - Federation: Cmd line tool support OpenStack
  - More Bare Metal automation
  - Extend CI coverage
- Half-yearly releases (9/22, 3/23, 9/23, 3/24, 9/24):
  - Multi-region setups, Security scanning, Security Certifications, CI coverage (for daily updates!), Encryption (disk, network), Compliance test coverage (automated certification), SSI/DID federation, X-Cloud Orchestration, Service Mesh, ...

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

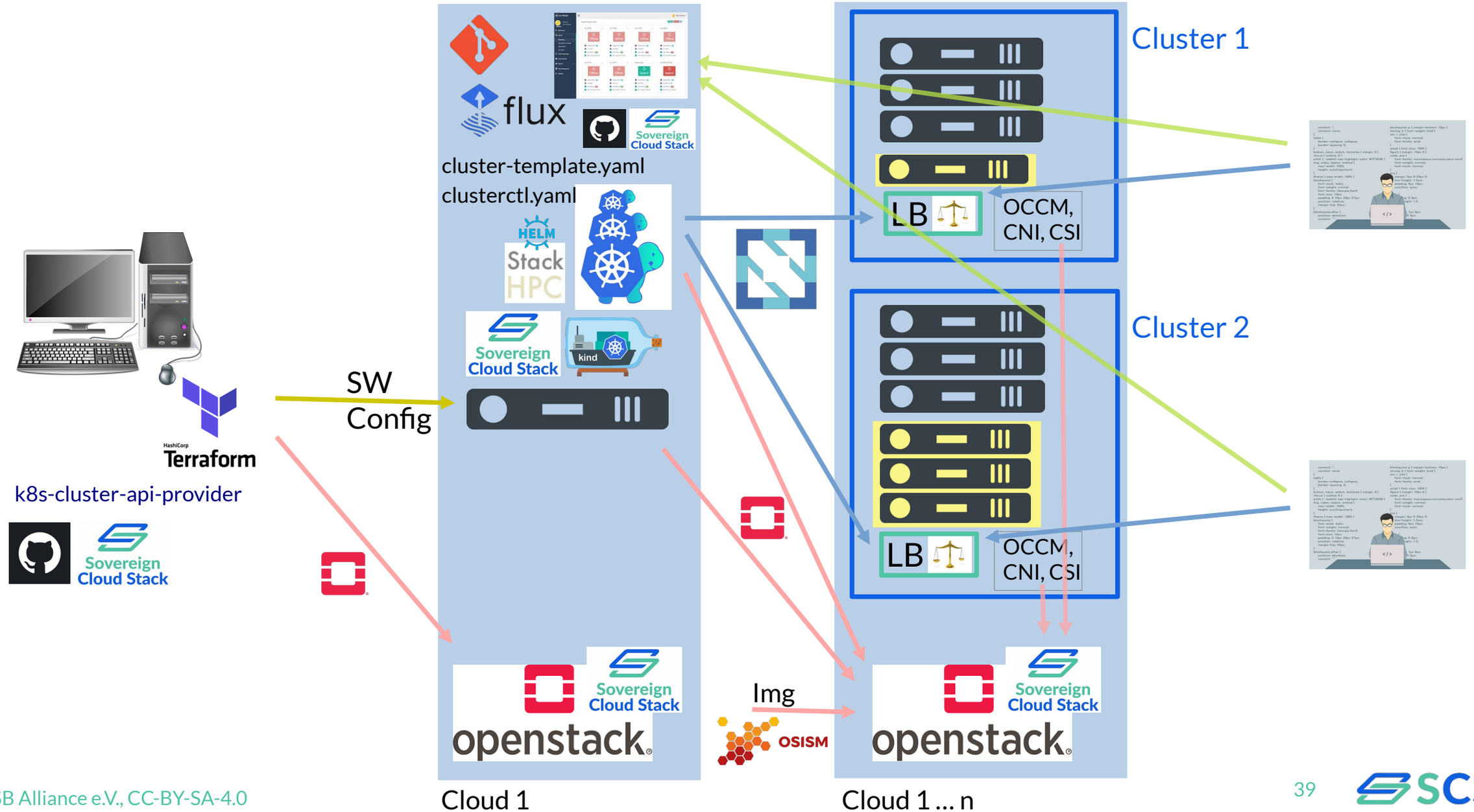
- Declarative description of desired state …
- Avoid dependence on SCS IaaS / OpenStack (abstract description with neutral CAPI provider & CCM)

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



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)

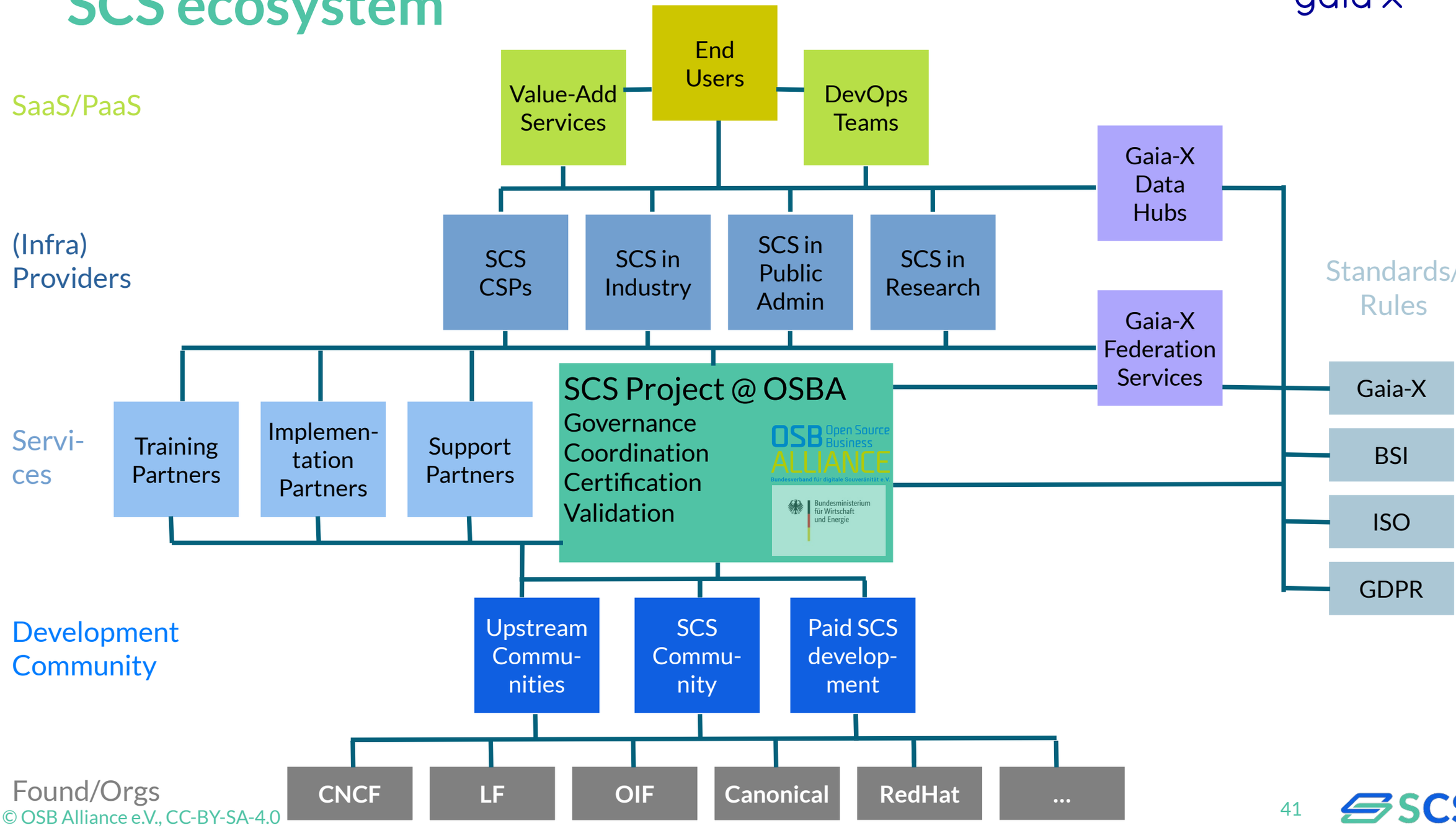
Certification

- 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 ecosystem



Beitrag von SCS zur deutschen Verwaltungscloud-Strategie

- Aufbau einer vollständig offenen, modularen, föderierten Cloud und Containerplattform auf Basis von SCS
- Standardbausteine erlauben und unterstützen Zertifizierungen
  - Mit Plusserver setzt ein BSI C5 zertifizierter CSP bereits SCS ein
  - Absicherung der Software-Lieferkette
  - Einfacher Zugriff auf Ursprung und Version der Softwarekomponenten
  - Verringerter Aufwand bei Auditierungen

Beitrag von SCS zur deutschen Verwaltungscloud-Strategie

gaia-x

- Aufbau eines offenen Lösungsportfolios mit Bausteinen für die Verwaltung (Phoenix usw.)
- PoC und Aufbau zunächst einer Plattform durch Infrastruktur-Betreiber (Rechenzentren, SCS Betrieb) und Middleware/Applikationspartner (Bereitstellung der Lösungsbausteine und Applikationsbetrieb)
- Partner für Beratung und Implementierung vorbereitet: dataport, B1, Gonicus, HiSolutions, PD
- Kleine kompatible Clouds auch möglich – Effizienz durch gemeinsamen Betrieb

SCS

Flow of automated deployment (currently covering: Infra, IaaS, Ops, KaaS is WIP)

gaia-x

Physical SCS can of course host virtual SCS
Nested virtualization support recommended

BETACLOUD plusserver

Physical deployment

Production („Live“)

Server buying, racking, cabling

Kayobe/ Ironic Netbox

Ansible: Setup Mgr, Nodes:
- Infra: Database, MemCache, rabbitMQ
- Infra: ceph+radosgw, OvS/OVN
- OpsTooling: ARA, ELK, netdata, prometheus, patchman
- IaaS: OpenStack Core (nova, keystone, …) - kolla
- KaaS (WIP): k8s cluster API, CNI, CSI, registry, helm
- Validation (WIP): Smoke tests, conftest, RefStack, OPA

Virtual (testbed) deployment

Dev, Testing / CI („Ref/Test“)
Demo, Explore, Debug, ...

citynetwork T . . OVHcloud

Bootstrap: terraform (on IaaS)

Ansible: Setup Mgr, Nodes:
- Infra: Database, MemCache, rabbitMQ
- Infra: ceph+radosgw, OvS/OVN
- OpsTooling: ARA, ELK, netdata, prometheus, patchman
- IaaS: OpenStack Core (nova, keystone, …) - kolla
- KaaS (WIP): k8s cluster API, CNI, CSI, registry, helm
- Validation (WIP): Smoke tests, conftest, RefStack, OPA

~90min

https://github.com/OSISM

https://docs.osism.de/

https://docs.osism.de/testbed/

https://github.com/OSISM/testbed

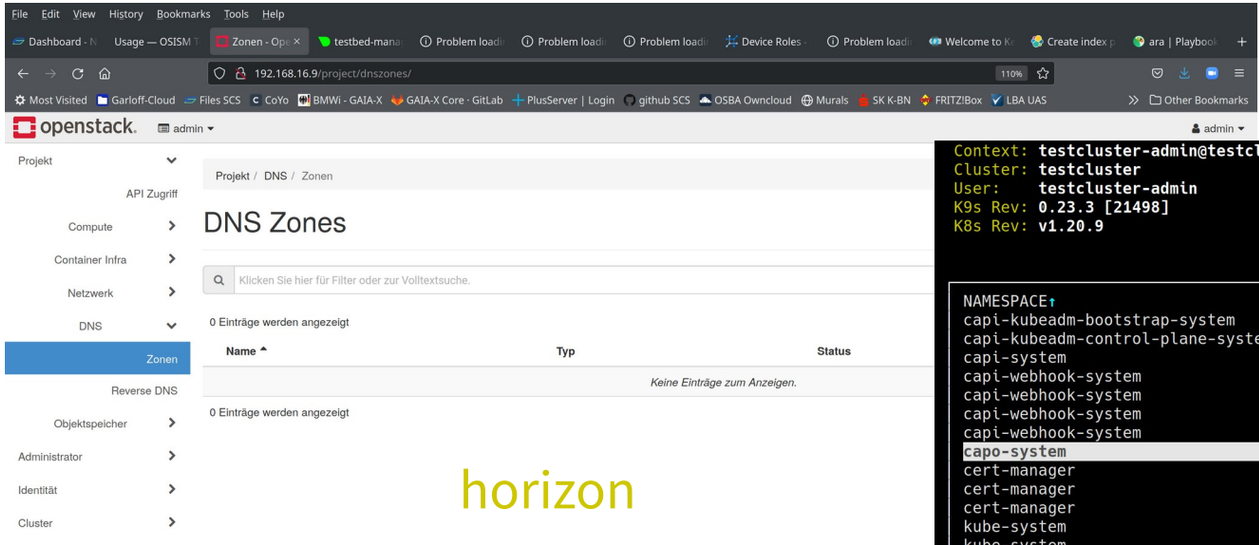
https://github.com/SovereignCloudStack/Docs

SCS

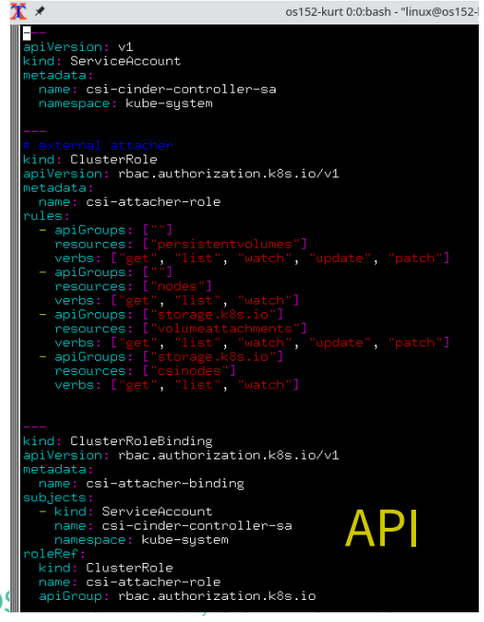
SCS screenshots

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

How does it look? (Customer perspective)

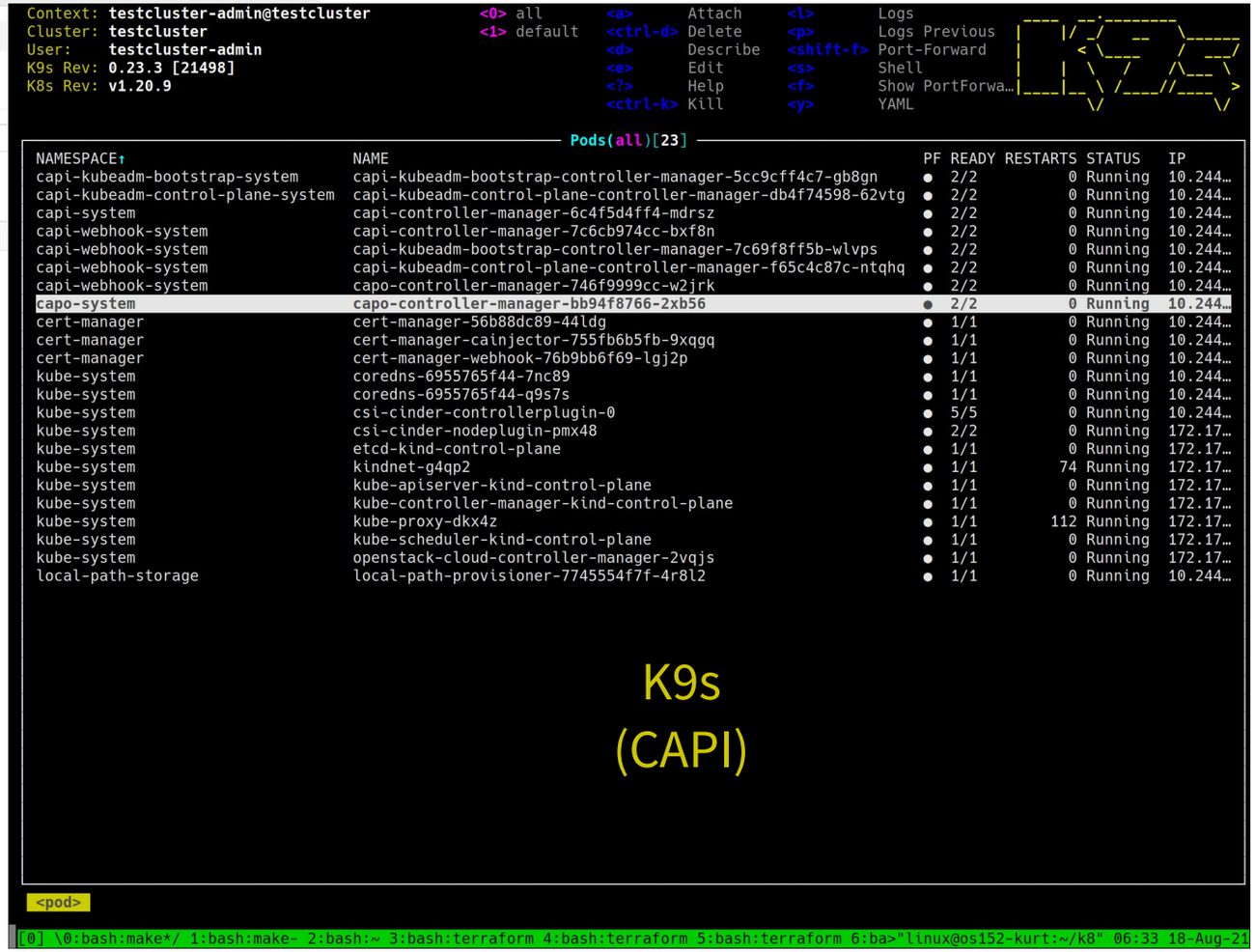


horizon



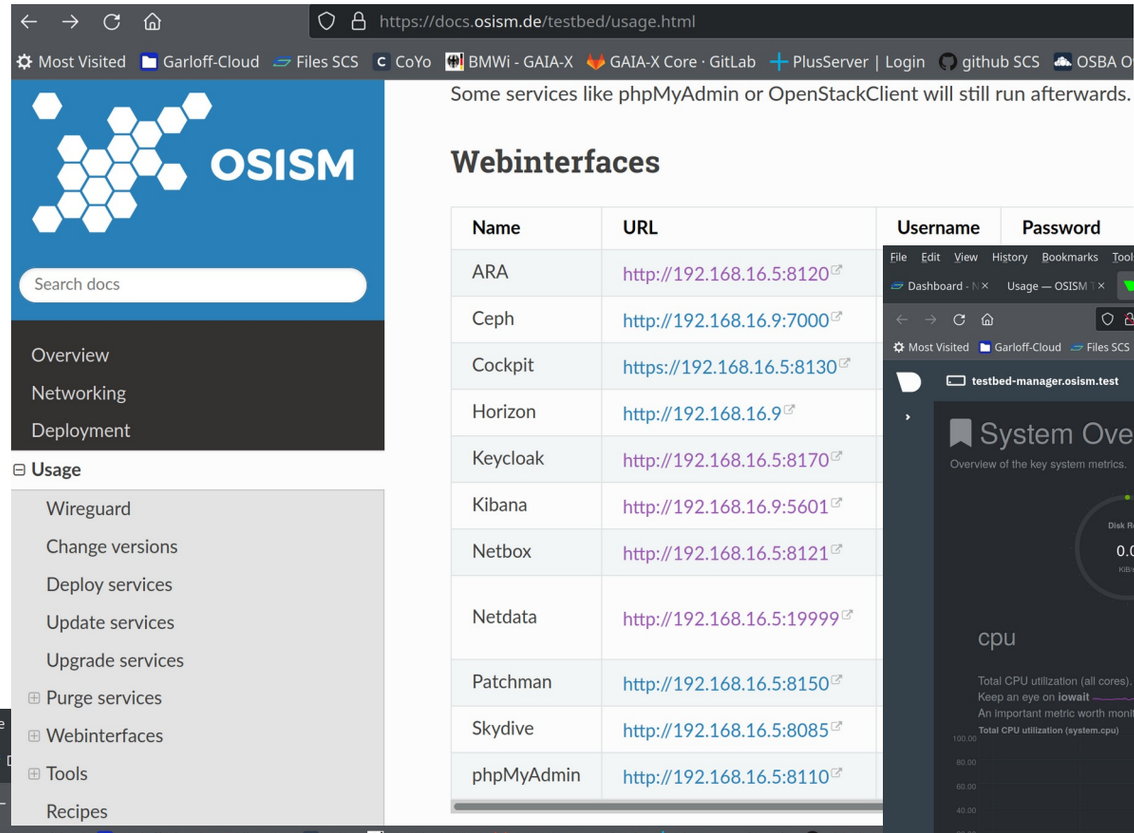
API

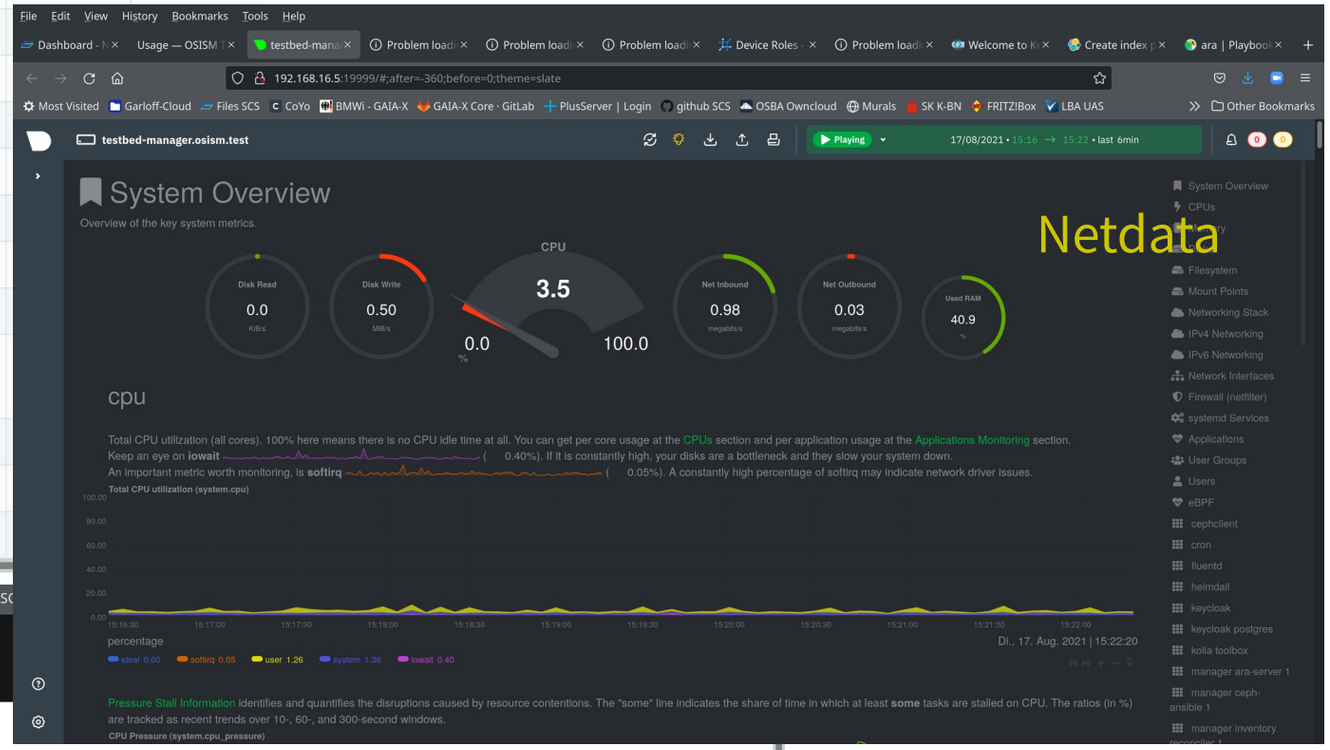
REST APIs for DevOps teams (Infra-as-Code)



K9s (CAPI)

How does it look? (Operator perspective)

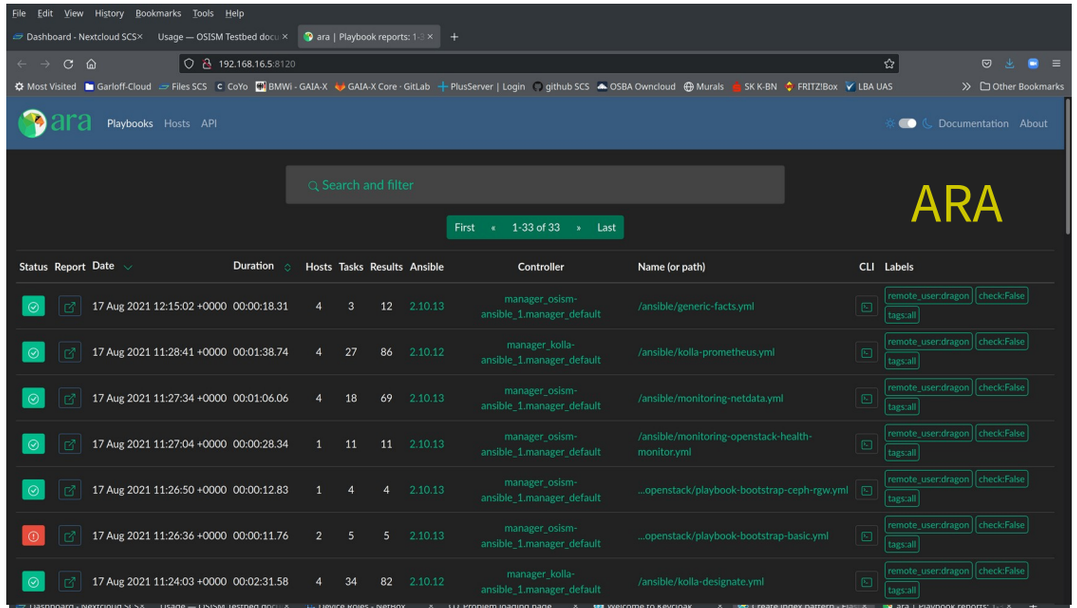


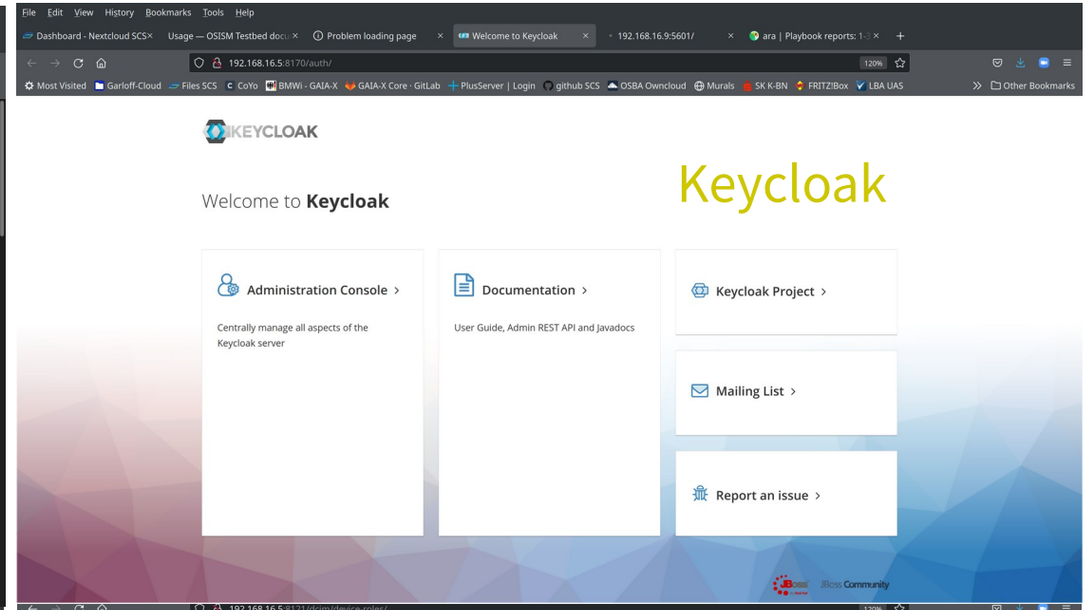


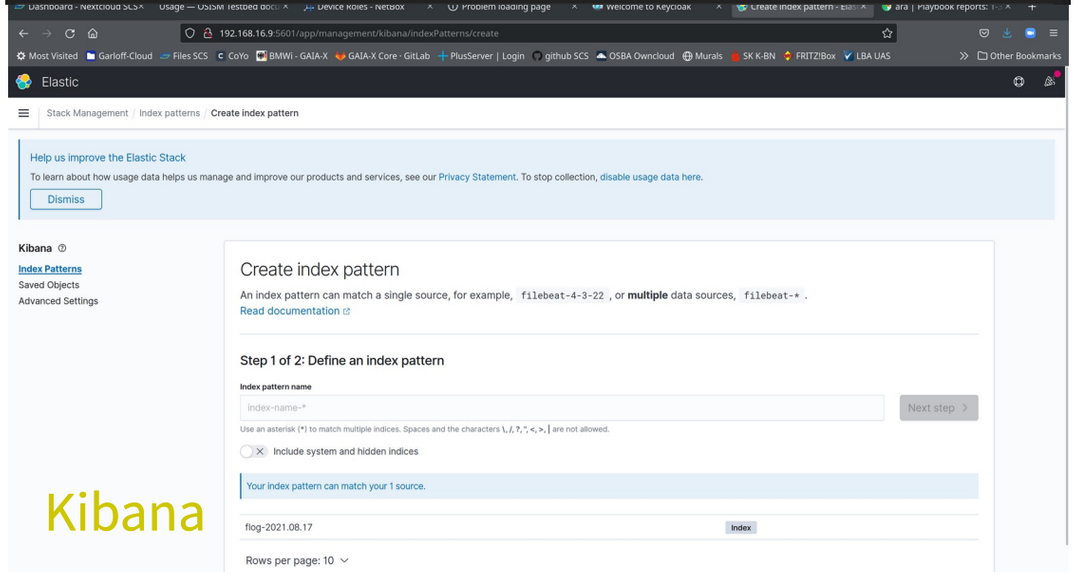
Job | Filter by Job...

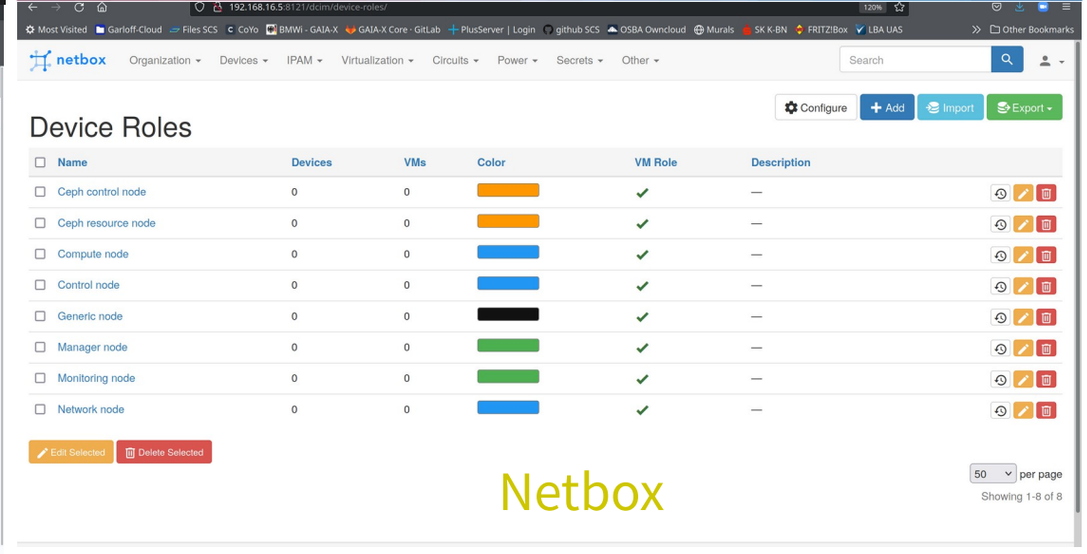
Job	Project	Branch	Pipeli...	Change	Dur...	Start time	Result
markdownlint	SovereignCloudStack/zuul-sandbox	main	gh_post	a6fe9d6	20 secs	2021-08-17 12:45:29	RETRY_LIMIT
markdownlint	SovereignCloudStack/zuul-sandbox	main	gh_post	a6fe9d6	19 secs	2021-08-17 12:45:09	RETRY
markdownlint	SovereignCloudStack/zuul-sandbox	main	gh_post	a6fe9d6	20 secs	2021-08-17 12:44:39	RETRY
demo-job	SovereignCloudStack/zuul-sandbox	main	gh_post	a6fe9d6	15 secs	2021-08-17 12:44:39	SUCCESS

How does it look? (Operator perspective)









You can only manage what you measure ...

openstack-health-monitor: Black-box monitoring

Developing SCS

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

Discussion

QUESTIONS?

Test it!

Pilot project / Proof-of-Concept

Join us!

Team meeting on Thu, 15:00 CE(S)T

GAIA-X: https://gaia-x.eu/

SCS Project: https://scs.community/

EMail: project@scs.sovereignit.de, garloff@osb-alliance.com