



SCS - GI INFORMATIK2024 2024-09-26

Sovereign Cloud Stack: Common standards, software and practices for a network of SCS clouds

Kurt Garloff, Dirk Loßack, **Manuela Urban**, Bianca Hollery-Pfister, Felix Kronlage-Dammers, Alexander Diab, Maximilian Wolfs, Jan Schoone, Friederike Zelke, Nadja Schieber, Marc Schöchlin, Regina Metz, **Dominik Pataky**, Artem Goncharov (SCS @ OSBA)
scs@osb-alliance.com

<https://scs.community/>
<https://docs.scs.community/>
<https://github.com/SovereignCloudStack/>



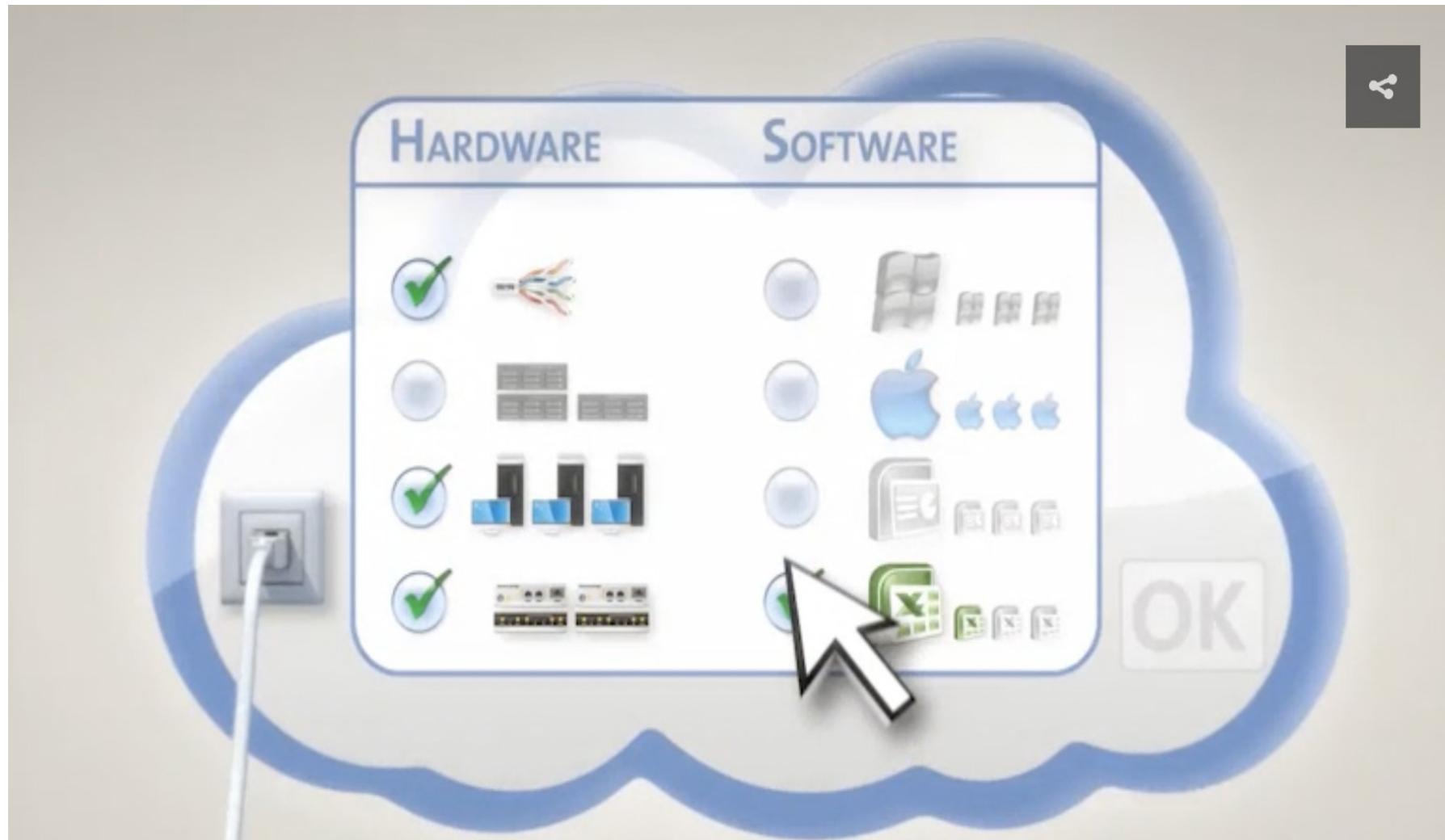
Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



Der Traum von der Wolke...



Quelle: Bundesministerium für Wirtschaft und Technologie 2010



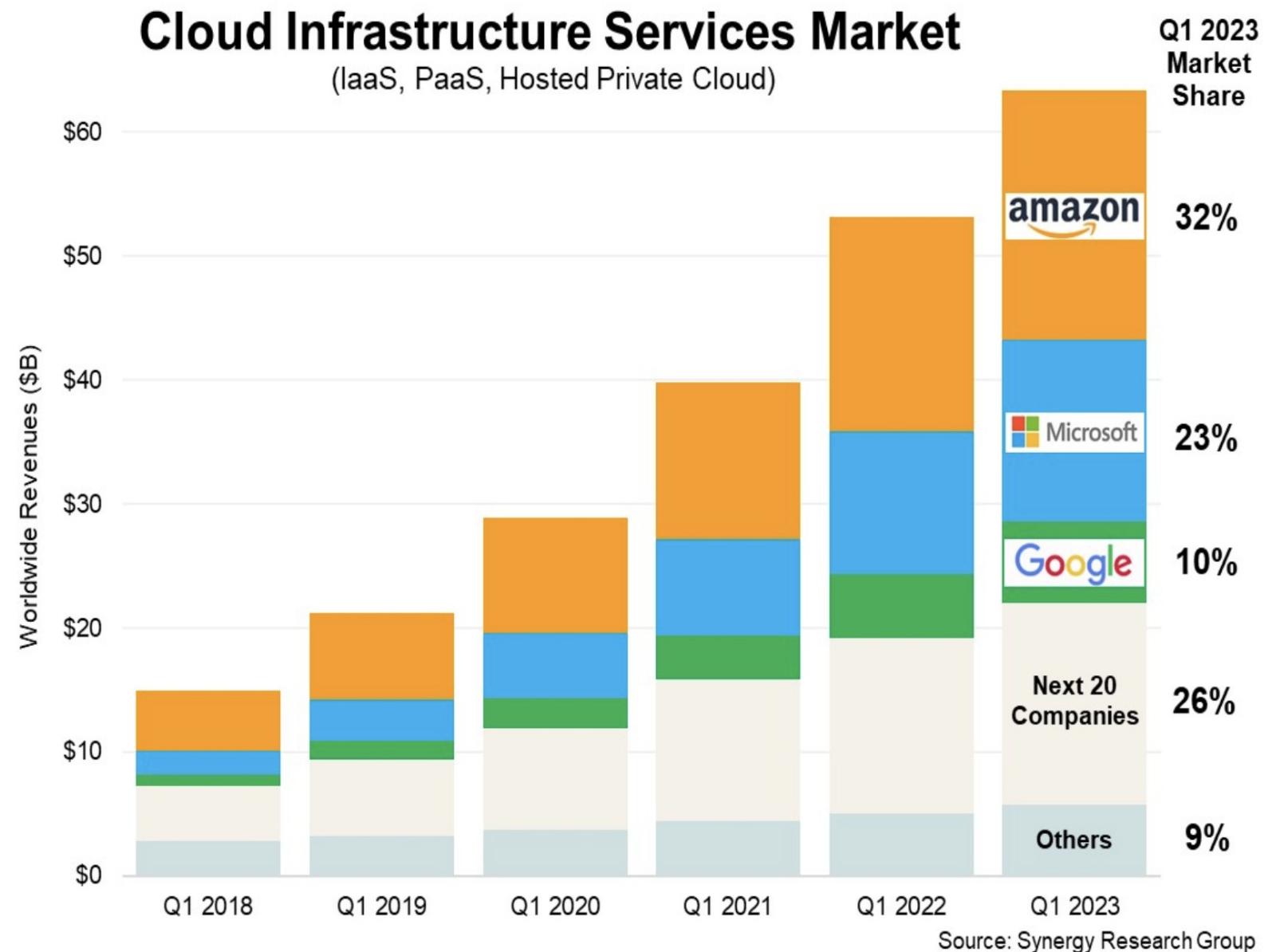
...und die Realität

- Über 80 % der Unternehmen in Europa fühlen sich technologisch abhängig.¹
- Amazon, Microsoft, Alphabet (Google) beherrschen den Markt.²
- Vendor lock-in³
- Inkompatibilität bei Infrastrukturen, Plattformen und Applikationen
- US Foreign Intelligence Surveillance Act (FISA) ↗ EU DSGVO
- hohe Komplexität dynamischer, verteilter Plattformen im Betrieb
- Fachkräftemangel

1 ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung; „Schwerpunktstudie Digitale Souveränität 2021“ Hrsg.: Bundesministerium für Wirtschaft und Energie (Oktober 2021)

2 <https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues>

3 https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/marktanalyse-reduzierung-abhaengigkeit-software-anbieter.pdf?__blob=publicationFile&v=1



Digitale Wertschöpfung & Marktmacht

Die Top100 größten börsennotierten Unternehmen der Welt

Nach Marktkapitalisierung

Zum Vergleich (Market Cap):

GER 2,2 Bio. EUR (2023)

	Name	Land	Umsatz (EUR)	Gewinn (EUR)	↓ Market Cap (EUR)
# 1	Microsoft Corp. Registered Shares DL-,00000625	🇺🇸	192,4 Mrd.	65,7 Mrd.	3,0 Bio.
# 2	Apple	🇺🇸	355,6 Mrd.	90,0 Mrd.	2,7 Bio.
# 3	Alphabet Inc. Reg. Shs Cl. A DL-,001	🇺🇸	282,5 Mrd.	67,9 Mrd.	1,9 Bio.
# 4	Amazon.com	🇺🇸	533,2 Mrd.	28,2 Mrd.	1,8 Bio.
# 5	Meta Platforms Inc. Reg.Shares Cl.A DL-,000006	🇺🇸	125,1 Mrd.	36,3 Mrd.	1,0 Bio.

Source: Finanzen 100, June 2024

Koalitionsvertrag Ampel

- "sichern digitale Souveränität"
- ...Recht auf Interoperabilität, Portabilität...

Open Washing - "souveräne Clouds"?

Der AWS Digital Sovereignty Pledge in der Praxis

Mit dem [AWS Digital Sovereignty Pledge](#) verpflichten wir uns, AWS-Kunden die fortschrittlichsten Souveränitätskontrollen und -funktionen zu bieten, die in der Cloud verfügbar sind. Wir verpflichten uns, unsere Funktionen zu erweitern, damit Sie Ihre Anforderungen an die digitale Souveränität erfüllen können, ohne die Leistung, Innovation, Sicherheit oder den Umfang der AWS-Cloud zu beeinträchtigen.

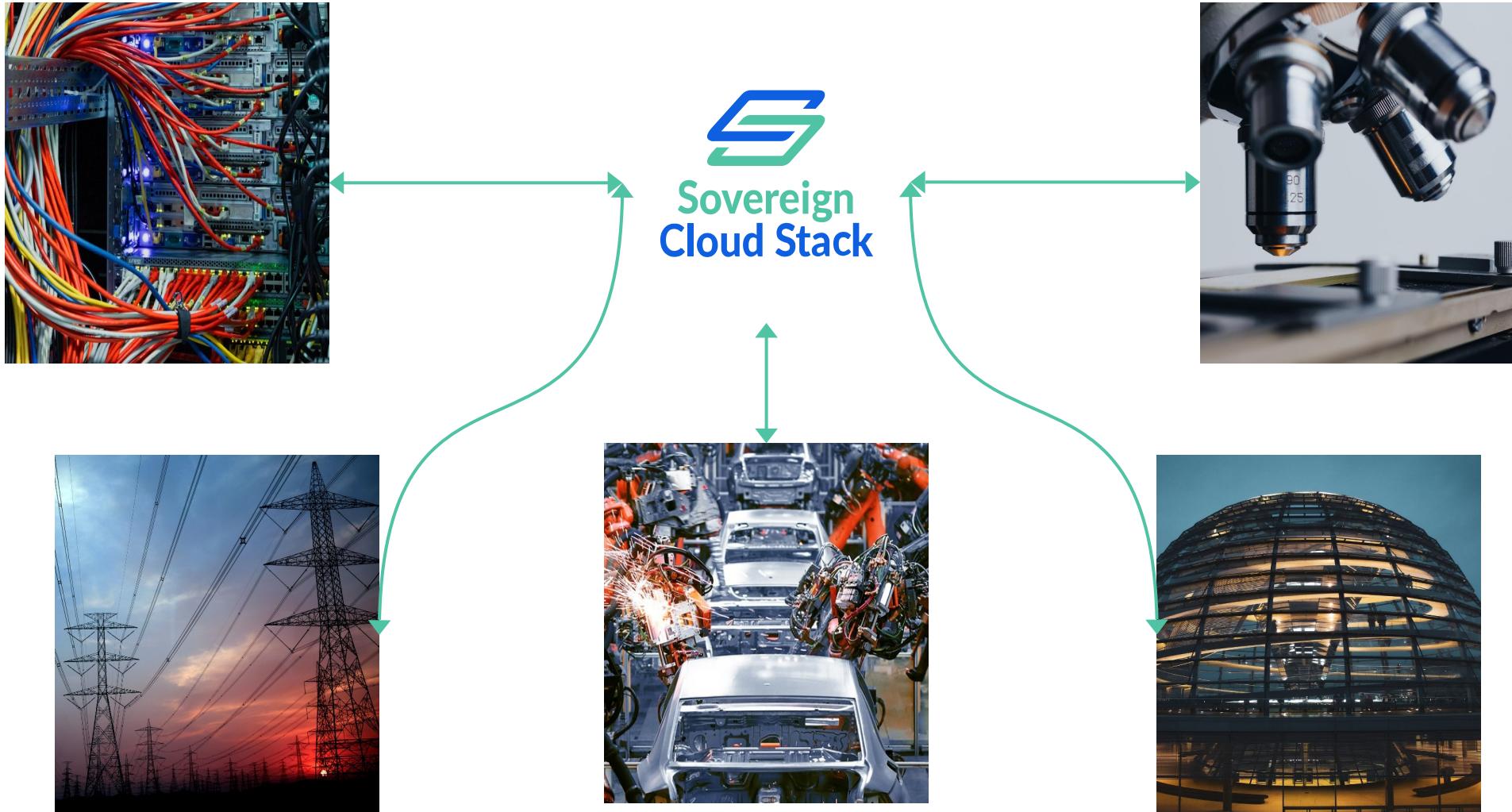
Google Sovereign Cloud

Die umfassendste und flexibelste Lösung für Kunden, um Anforderungen an Daten-, Betriebs- und Softwarehoheit zuversichtlich zu erfüllen.



Gemeinsam souverän
Die Cloud für den öffentlichen Dienst

Sovereign Cloud Stack bringt Entwickler und Anwender sektorübergreifend zusammen, um Cloud-Technologie gemeinsam zu standardisieren und zu entwickeln.



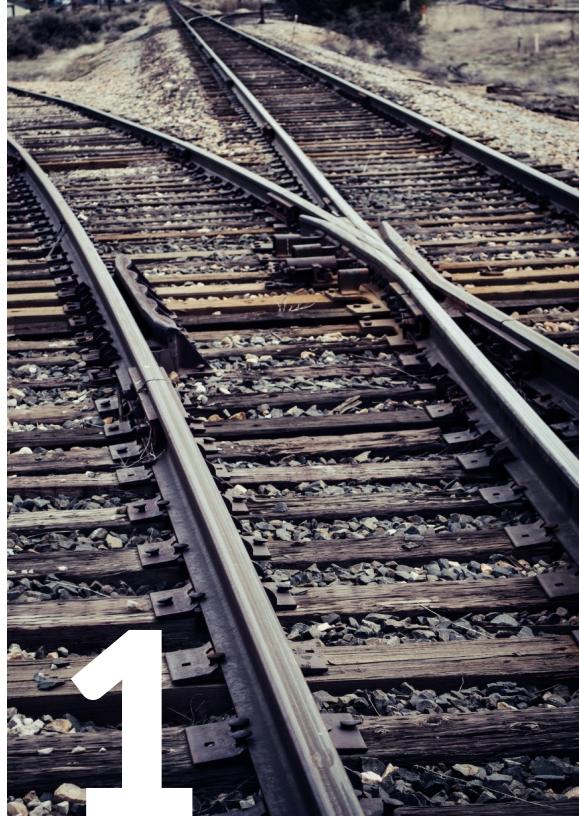
imagine a Cloud Platform...

**... where users can easily switch between
different cloud service providers without being
locked in.**

SCS Mehrwert

- für Kunden
 - Wechselfähigkeit, Wettbewerb, Wahlmöglichkeiten durch standardisierte Technologie
 - Transparenz durch Offenheit im Code, im Design, im Betrieb
 - Gestaltungsfähigkeit durch Kontaktmöglichkeiten zu Service Providern und Community
- für Cloud Service Provider (public or private)
 - „Turnkey Solution“: betriebsfähiger, produktionsreifer vollständiger Stack, modular, inkl. Betriebstools
 - Föderierung: Skalierbarkeit („Virtual Hyperscaler“)
 - „Open Knowledge“: frei zugängliches Knowhow durch umfassende Dokumentation und Community
- für Applikationsentwickler
 - Plattformunabhängigkeit durch Standardisierung

Sovereign Cloud Stack Deliverables



Certifiable Standards



Modular Open Source
Reference Implementation



Operational Knowledge

What is sovereignty?

Levels of Digital Sovereignty

4: Operational Transparency and - knowledge available

3: Technological Transparency and ability to influence and innovate

2: Free provider choice (also after initial choice, in-and-out-sourcing (on-prem/public)

1: Following legal requirements (GDPR)

0: None

SCS Levels of Certifications

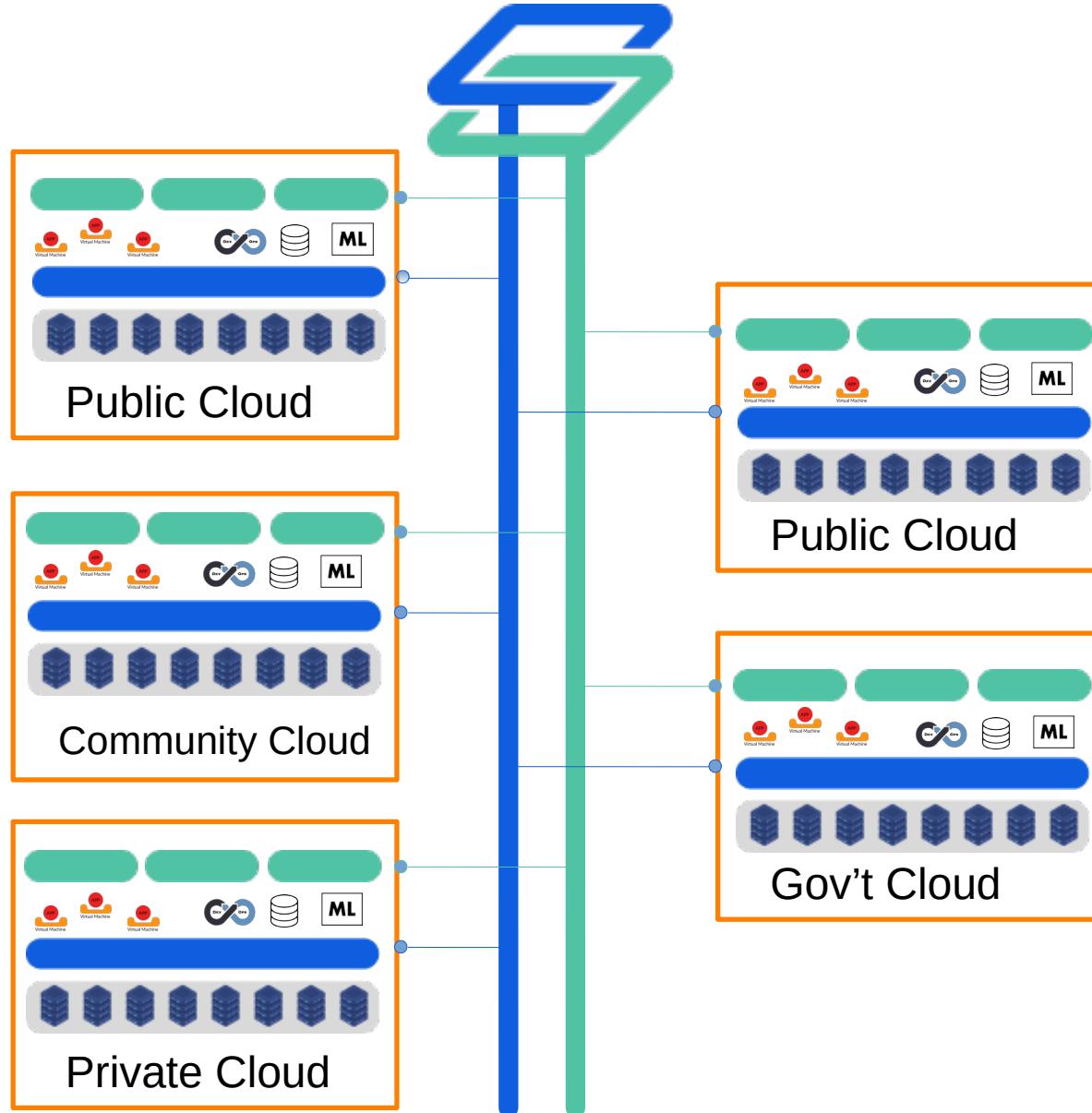
4: “SCS-sovereign” – Ops/IAM Module OSS too, Monitoring and Event Transparency, Contribution to Open Operations (5 x open)

3: “SCS-open” – SBOM of functional stack available and complete OSS (4 x open)

2: “SCS-compatible” – Technical compatibility (automated conformity tests: CNCF, OIF, SCS)

1: Defined and checked outside of SCS (rely on ENISA / Gaia-X labels / EU-CS)

Federated Infrastructure



Built on Common standards

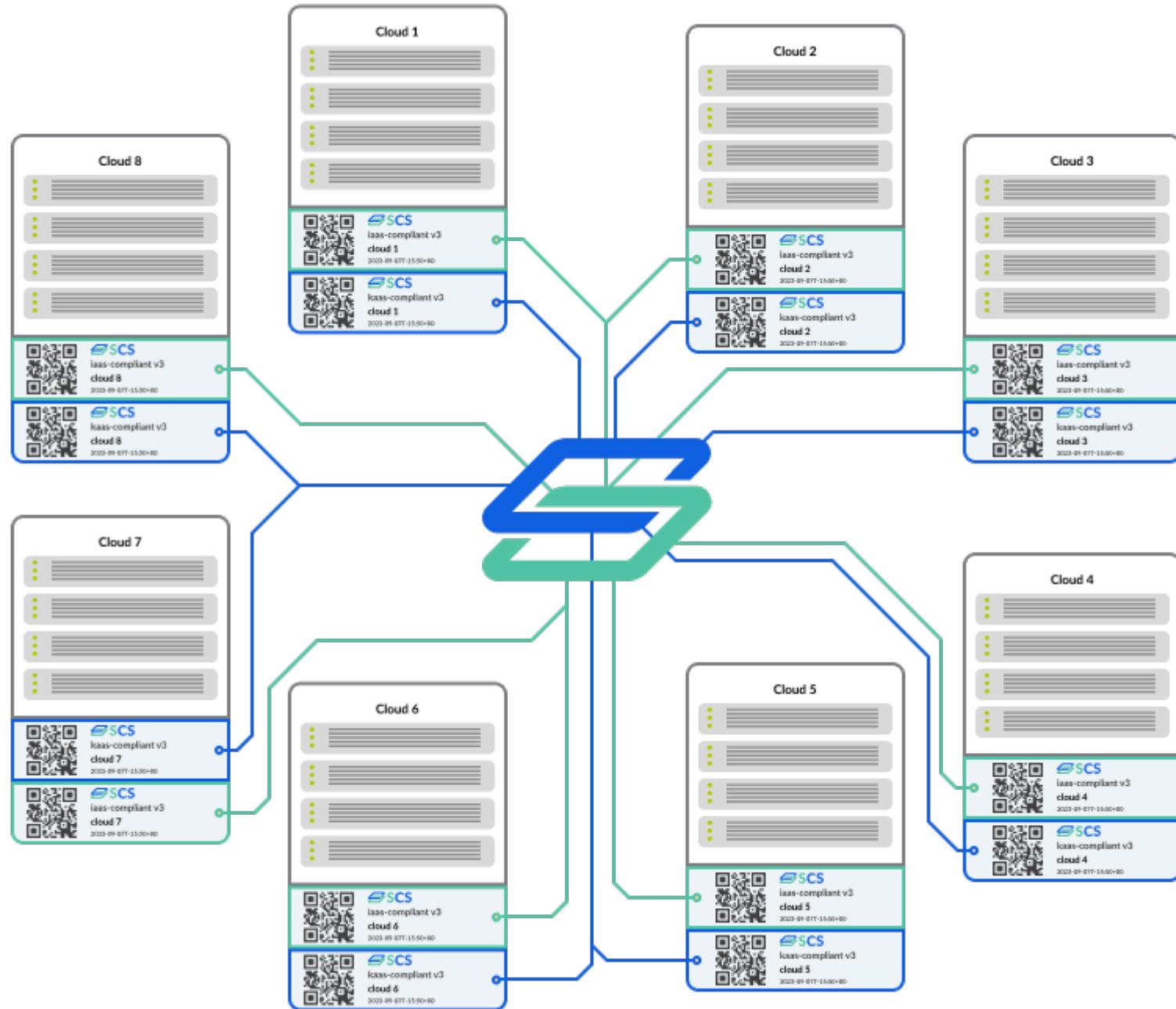
... for users of cloud services to enable mobility of workloads

... for cloud service providers to offer standardized lock-in-less services

... for the ecosystem to build knowledge and skills on a common technical and organizational foundation

... for solution providers that want to build on a common platform

SCS = an open, federated, virtual Hyperscaler



Existing public providers

← → ⌂ https://docs.scs.community/standards/certification/overview

 Standards For Operators For Contributors Community FAQ GitHub

Introduction

Certification

Scopes and Versions

Standards

Compliant cloud environments

This is a list of clouds that we test on a nightly basis against the certificate scope *SCS-compatible IaaS*.

Name	Description	Operator	SCS-compatible IaaS Compliance	HealthMon
gx-scs	Dev environment provided for SCS & GAIA-X context	plusserver GmbH	v4 passing	HM
pluscloud open - prod1 - prod2 - prod3 - prod4	Public cloud for customers (4 regions)	plusserver GmbH	- prod1 v4 failing - prod2 v4 failing - prod3 v4 failing - prod4 v4 failing	HM1 HM2 HM3 HM4
Wavestack	Public cloud for customers	noris network AG/ Wavecon GmbH	v4 passing	HM
REGIO.cloud	Public cloud for customers	OSISM GmbH	v4 passing	broken
CNDS	Public cloud for customers	artcodix GmbH	v4 passing	HM
aov.cloud	Community cloud for customers	aov IT.Services GmbH	(soon)	HM
PoC WG-Cloud OSBA	Cloud PoC for FITKO (yaook-based)	Cloud&Heat Technologies GmbH	v4 passing	HM
PoC KDO	Cloud PoC for FITKO	KDO Service GmbH / OSISM GmbH	v4 passing	(soon)
syseleven - dus2 - ham1	Public OpenStack Cloud (2 SCS regions)	SysEleven GmbH	- dus2 v4 failing - ham1 v4 failing	(soon) (soon)

Public quality assurance:
Continuous monitoring of
SCS clouds for security
(not shown here), SCS
standards conformance
and health.

Health Monitor dashboard:
Public realtime monitoring
of errors and performance

Daily updated standard conformity result
(here:
IaaS SCS-compatible)



SCS-based infrastructures and services

plusserver

secunet

CLOUD
& HEAT

Syself

REGIO
Digital für Deutschland



wavestack

aov
IT.Services GmbH



dNation
MAKING CLOUD EASY

ScaleUp
Technologies

stackXperts

SysEleven

dataport

B1
SYSTEMS

HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

Freistaat
Thüringen



Thüringer
Landesrechenzentrum

Govstack: SCS as the reference for sovereign cloud infrastructure

← → ⌂ https://govstack.gitbook.io/cloud-infrastructure/2-description ⌂ ⌂ Give Feedback GovStack Hom

GovStack

Cloud Infrastructure

1 Version History

2 Description

3 Terminology

4 Key Digital Functionalities

5 Cross-Cutting Requirements

6 Functional Requirements

7 Data Structures

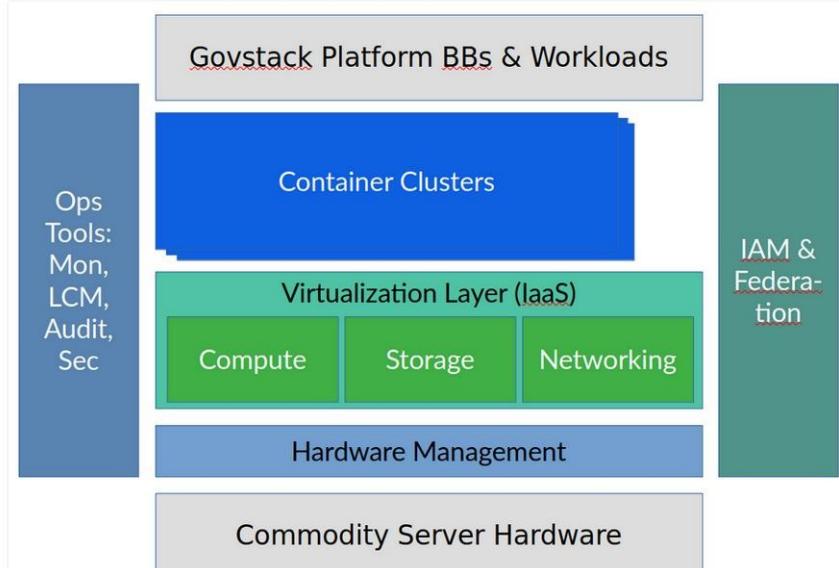
8 Service APIs

9 Internal Workflows

10 Other Resources

While many organizations have benefitted from gradually adapting their workloads to take advantage of the automation possibilities of cloud computing, the IT industry witnesses a new generation of workloads that has been designed from the ground up to take full advantage of the possibilities of cloud infrastructure; auto-scaling stateless services on-demand to the current level of load and automating a lot of the operational tasks that would otherwise be done manually by operations teams. These workloads are called cloud-native. While the first wave of these were based on virtual machines (VMs), we see a second, larger wave of these that leverage container technologies. In many cases, these containers run on top of virtual machines, thus allowing to balance good developer abstractions and fast scalability (where container technologies excel) with flexibility and isolation requirements (the strength of virtualization technology). In dedicated environments however, it can be beneficial to cut out the complexity of a virtualization layer and to run containers on bare-metal.

In all cases, users of the technology should consider the dependencies on providers of technology and infrastructure and take deliberate decisions on all components of the technology stack required to develop and run their workloads.



```

graph TD
    BBs[Govstack Platform BBs & Workloads] --- CC[Container Clusters]
    CC --- VL[Virtualization Layer IaaS]
    VL --- Compute[Compute]
    VL --- Storage[Storage]
    VL --- Networking[Networking]
    HL[Hardware Management] --- CH[Commodity Server Hardware]
    OT[Ops Tools: Mon, LCM, Audit, Sec] --- BBs
    OT --- HL
    IAM[IAM & Federation] --- BBs
  
```

The diagram illustrates the Govstack Platform architecture. At the top is a grey box labeled "Govstack Platform BBs & Workloads". Below it is a blue box labeled "Container Clusters". Underneath the Container Clusters is a green box labeled "Virtualization Layer (IaaS)" containing three sub-components: "Compute", "Storage", and "Networking". Below the Virtualization Layer is a blue box labeled "Hardware Management". At the bottom is a grey box labeled "Commodity Server Hardware". To the left of the central stack is a blue vertical bar labeled "Ops Tools: Mon, LCM, Audit, Sec". To the right is a teal vertical bar labeled "IAM & Federation". Arrows point from both the "Ops Tools" and "Hardware Management" boxes towards the central stack.

Powered by GitBook

<https://govstack.gitbook.io/cloud-infrastructure>



Open CoDE



Below you will find all the groups that are public.

You can easily contribute to them by requesting to join these groups.

> ⚙ S [Smarte.Land.Regionen](#)

⚙ S [SopraSteria](#)

⚙ Sovereign Cloud Stack Owner

Eine Plattform — standardisiert, entwickelt und betrieben von Vielen.
Sovereign Cloud Stack (SCS) ist ein vom BMWK gefördertes Projekt der OSB Alliance e.V.
SCS stellt Standards, Software und Wissen für Cloudfra bereit. <https://scs.community/>

⚙ S [Stadt Detmold](#)

> ⚙ [Stadt Soest](#)

⚙ [Stadt Wolfsburg](#)

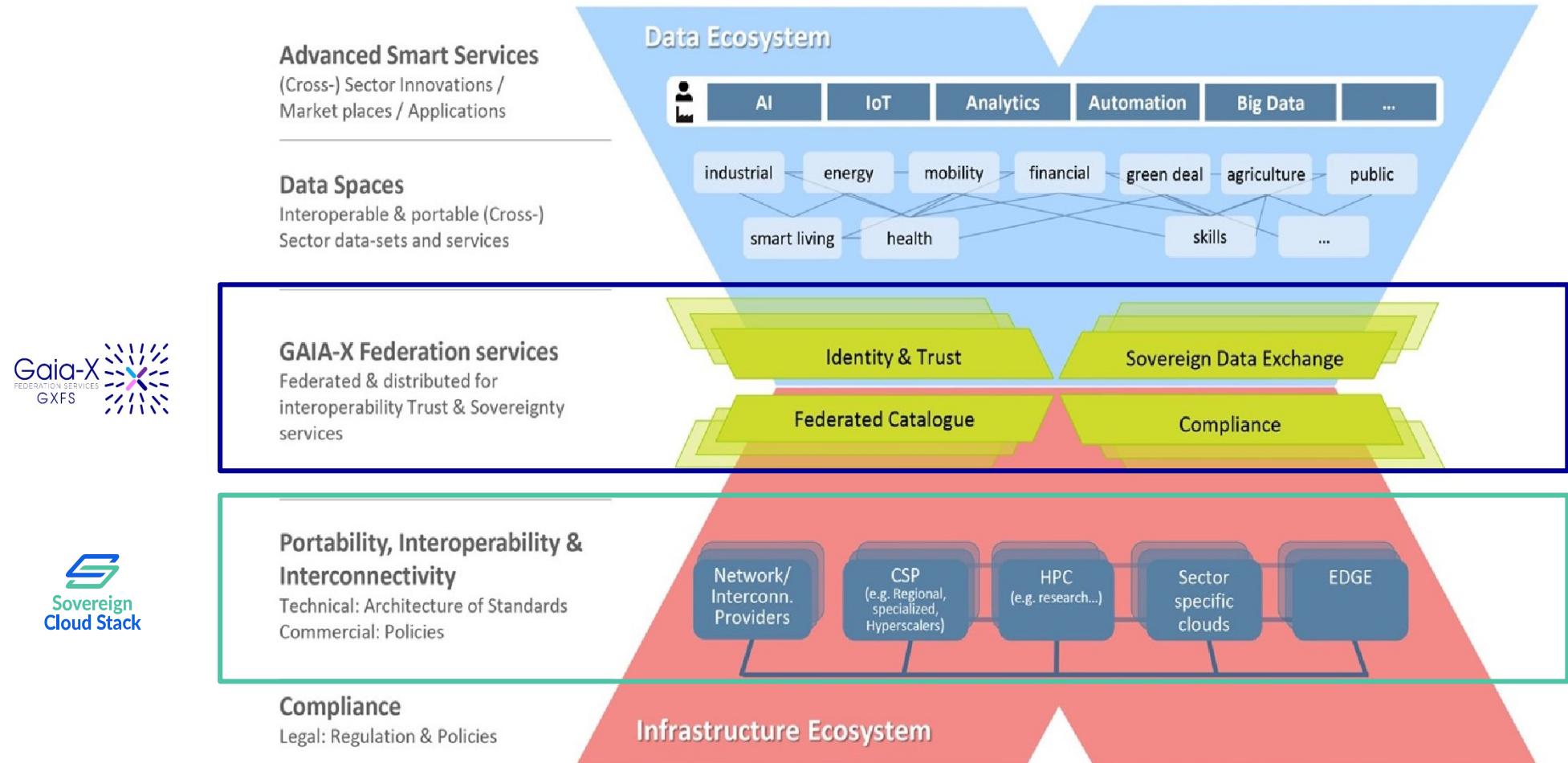
This is the official group of the city of Wolfsburg, Germany. Here you can find the open source projects that the city is working on or supporting.

⚙ T [Testgruppe](#)

⚙ T [Thüringer Landesverwaltung](#)



SCS liefert Infrastrukturschicht für Gaia-X Federation Services



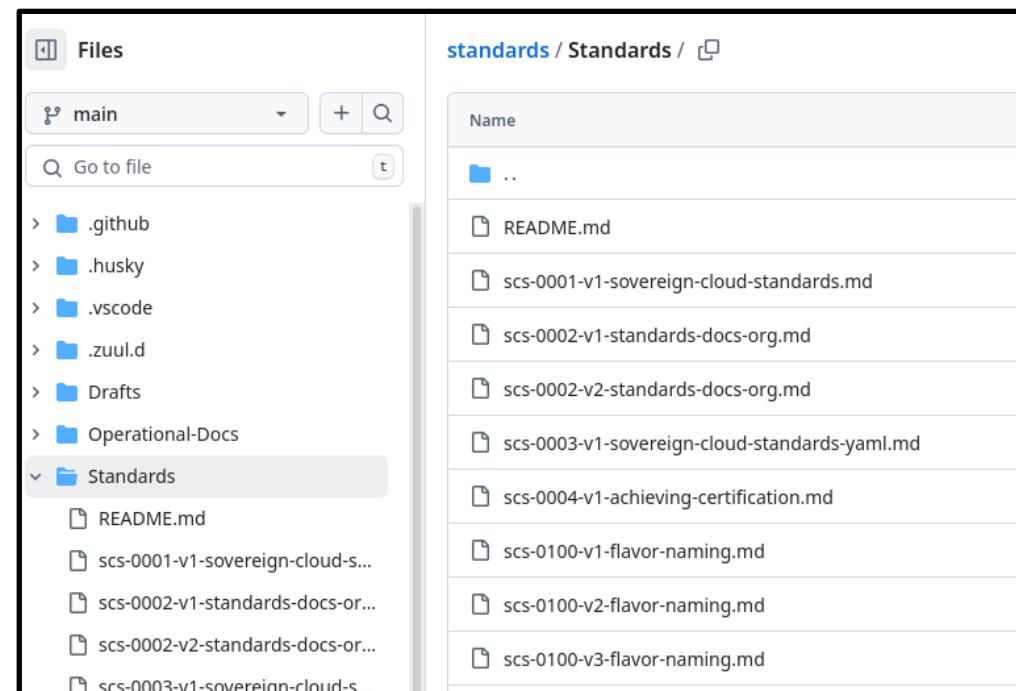
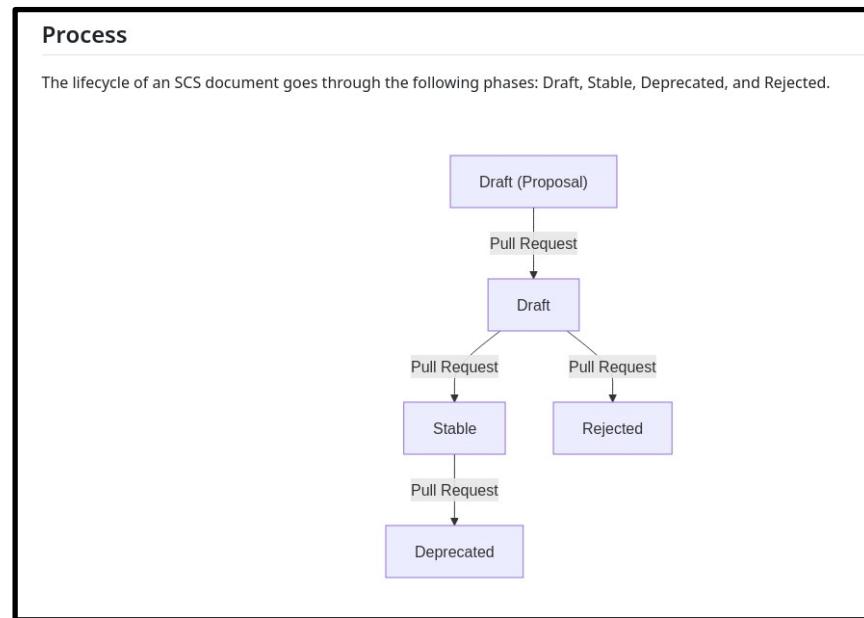
SCS Standards

Intro to SCS Standards

- **Standards of cloud platforms enforce interoperability**
- **We look at IaaS, KaaS and tooling as well as operational procedures**
- **Types of standards in SCS:**
 - 1) Procedural: describes a process, a policy or a guideline to which the SCS community adheres.
 - 2) Standard: describes a technical standard for SCS compliant clouds
 - 3) Decision Record: documentation of complex technical decisions during development
 - 4) Supplement: extends a Standard with additional information, such as implementation and testing notes

Collaboration via Github

- Repo <https://github.com/SovereignCloudStack/standards>
 - Standard documents as Markdown files
 - Compliance test suite in Python, with YAML as data/variable storage
 - Additional tooling, drafts etc.



Standards on docs.scs.community

Standards	▼
Global	➤
IaaS	➤
KaaS	➤
IAM	➤
Ops	➤

Global Standards

This track encompasses the foundational standards that guide the overall structure, documentation, and general topics related to the Cloud Stack. It serves as the core framework, ensuring consistency, clarity, and comprehensibility across all aspects of the cloud stack in an environment where information is easily accessible and understood.

*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Description	Draft	Effective	Deprecated*
scs-0001	Sovereign Cloud Standards	-	v1	-
scs-0002	Standards, Docs and Organisation	v2	v1	-
scs-0003	Sovereign Cloud Standards YAML	v1	-	-
scs-0004	Regulations for achieving SCS-compatible certification	v1	-	-

Home > Standards > IaaS

IaaS Standards

The IaaS Layer Standards track focuses on the protocols, guidelines, and specifications that govern the infrastructure as a service layer. This encompasses standards for virtual machines, storage, networking, and other foundational resources, ensuring seamless, efficient, and secure operation, interoperability, and management of the underlying cloud infrastructure.

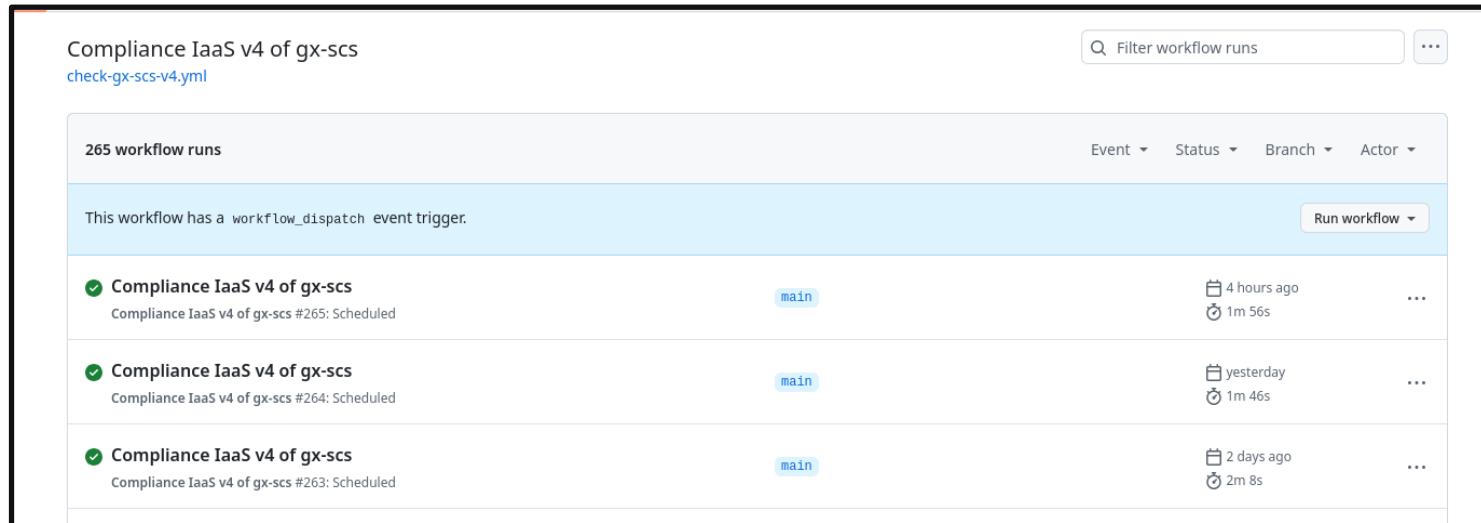
*Legend to the column headings and entries:

- Document states: Draft, Effective, Deprecated (and no longer effective)
- Entries in the effective column marked with an * are stable right now but turn to effective documents in the near future
- Entries in the effective column marked with a † will turn deprecated in the near future

Standard	Description	Draft	Effective	Deprecated*
scs-0100	SCS Flavor Naming Standard	-	v3	v1, v2
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0101	SCS Entropy	-	v1	-
	Supplement: Implementation and Testing Notes	w1	-	-
scs-0102	SCS Image Metadata Standard	-	v1	-
	Supplement: SCS Image Metadata: Implementation and Testing Notes	w1	-	-
scs-0103	SCS Standard Flavors and Properties	-	v1	-
scs-0104	SCS Standard Images	-	v1	-
	Supplement: Implementation Notes	w1	-	-
scs-0110	SSD Flavors	-	v1	-
scs-0111	Decisions for the Volume Type Standard	v1	-	-
scs-0112	SONiC Support in SCS	v1	-	-
scs-0113	Security Groups Decision Record	v1	-	-

SCS compliance monitor

- **Compliance Monitor is a Python-based test suite for cloud environments**
- **Takes Standard's parameters and checks CSP instance**
 - Example: allowed versions, mandatory OpenStack flavors
- **Recurring job to check compliance as Github Action**



The screenshot shows a GitHub interface for a workflow named "check-gx-scs-v4.yml". The page displays 265 workflow runs. A message indicates that the workflow has a `workflow_dispatch` event trigger. Three recent runs are listed:

- Compliance IaaS v4 of gx-scs (Scheduled) - Run #265, main branch, 4 hours ago (1m 56s)
- Compliance IaaS v4 of gx-scs (Scheduled) - Run #264, main branch, yesterday (1m 46s)
- Compliance IaaS v4 of gx-scs (Scheduled) - Run #263, main branch, 2 days ago (2m 8s)

Dashboard of „Compliant cloud environments“

https://docs.scs.community/standards/certification/overview

SCS Standards For Operators For Contributors Community FAQ GitHub

Introduction

Certification

Scopes and Versions

Standards

Compliant cloud environments

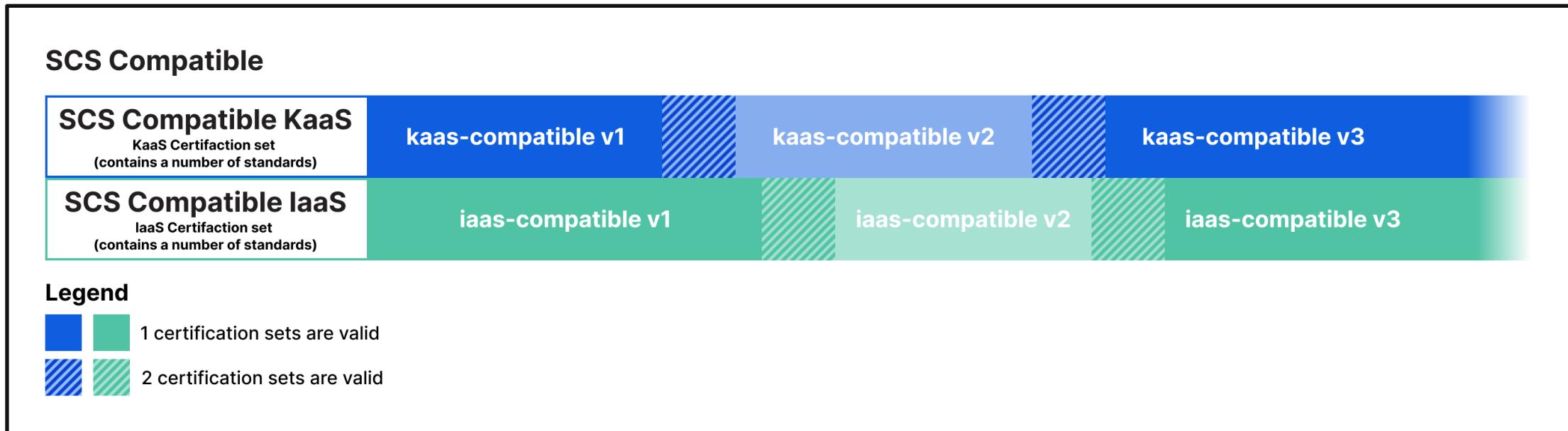
This is a list of clouds that we test on a nightly basis against the certificate scope *SCS-compatible IaaS*.

Name	Description	Operator	SCS-compatible IaaS Compliance	HealthMon
gx-scs	Dev environment provided for SCS & GAIA-X context	plusserver GmbH	v4 passing	HM
pluscloud open - prod1 - prod2 - prod3 - prod4	Public cloud for customers (4 regions)	plusserver GmbH	- prod1 v4 failing - prod2 v4 failing - prod3 v4 failing - prod4 v4 failing	HM1 HM2 HM3 HM4
Wavestack	Public cloud for customers	noris network AG/ Wavecon GmbH	v4 passing	HM
REGIO.cloud	Public cloud for customers	OSISM GmbH	v4 passing	broken
CNDS	Public cloud for customers	artcodix GmbH	v4 passing	HM
aov.cloud	Community cloud for customers	aov IT.Services GmbH	(soon)	HM
PoC WG-Cloud OSBA	Cloud PoC for FITKO (yaook-based)	Cloud&Heat Technologies GmbH	v4 passing	HM
PoC KDO	Cloud PoC for FITKO	KDO Service GmbH / OSISM GmbH	v4 passing	(soon)
syseleven - dus2 - ham1	Public OpenStack Cloud (2 SCS regions)	SysEleven GmbH	- dus2 v4 failing - ham1 v4 failing	(soon) (soon)



Scopes and versions

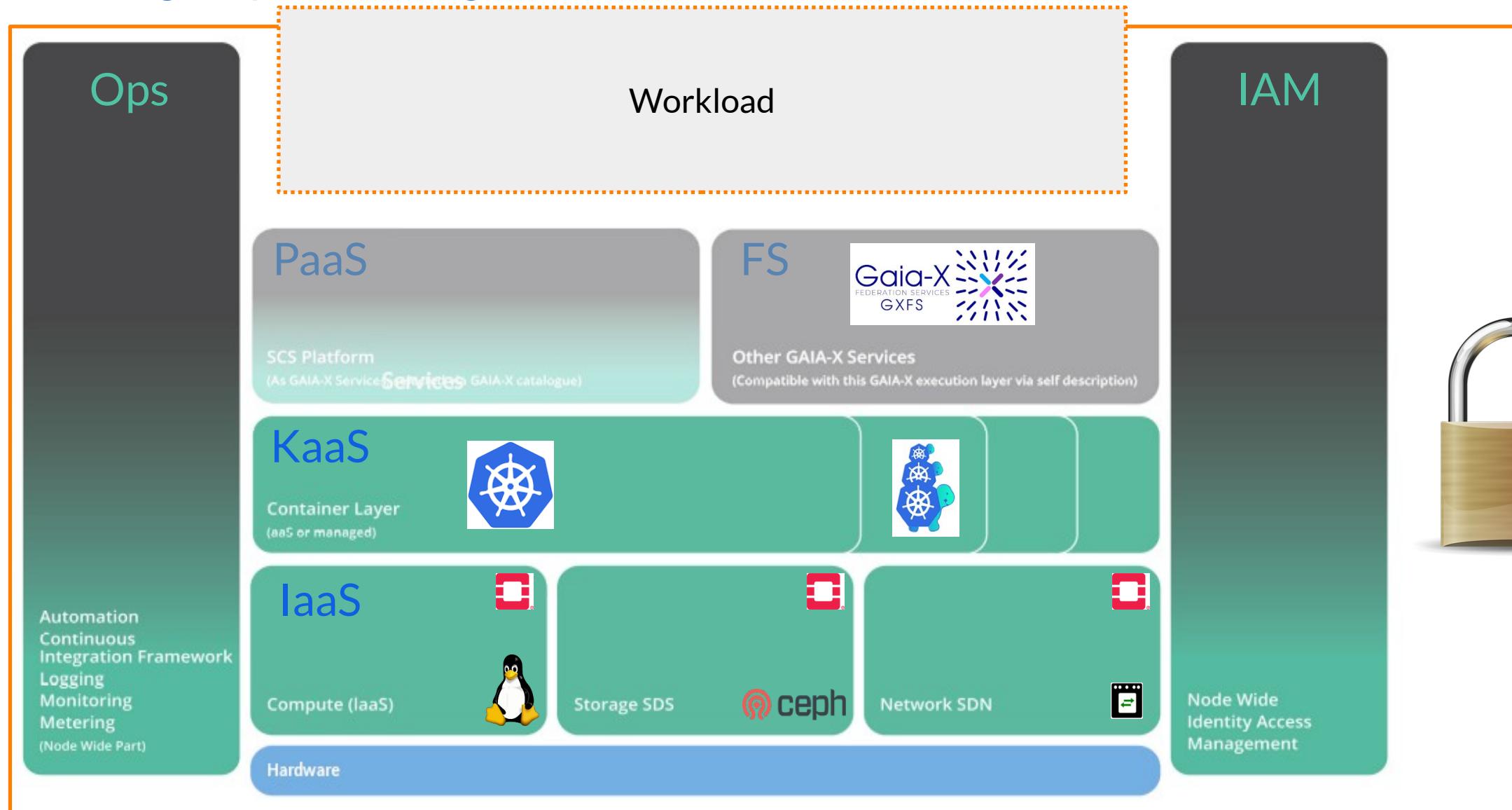
- Each Standard is versioned, so updates can be differentiated
 - v3 can be deprecated, while v4 must be adopted etc.
- Scopes: IaaS and KaaS



Technology: What's inside SCS?

SCS Architecture (Software/Ref.Impl.)

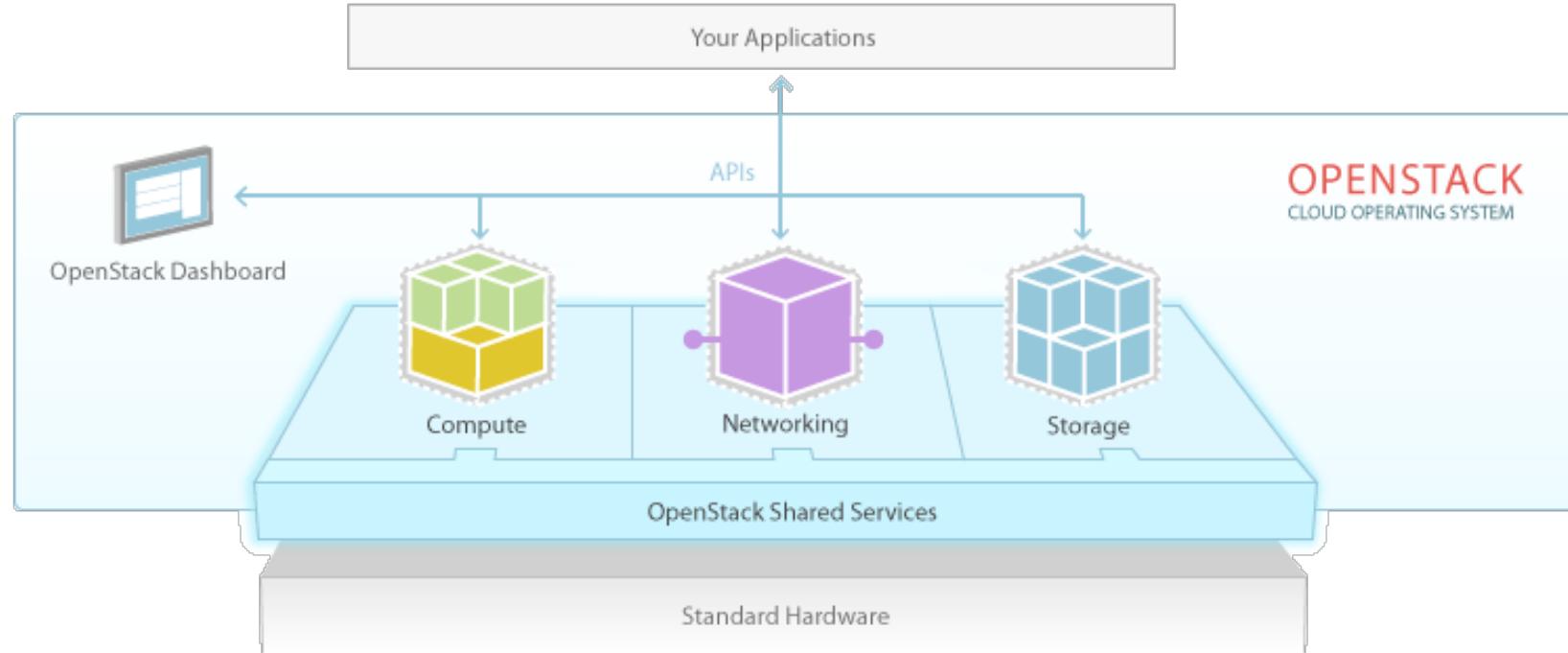
building it up from the ground



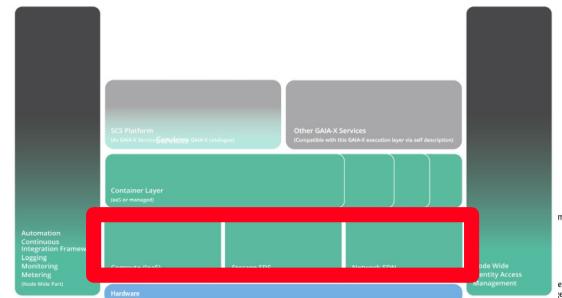
SCS Platform Services (PaaS) are planned
 Hardware and Federation Services not part of SCS software
 KaaS = Kubernetes as a Service



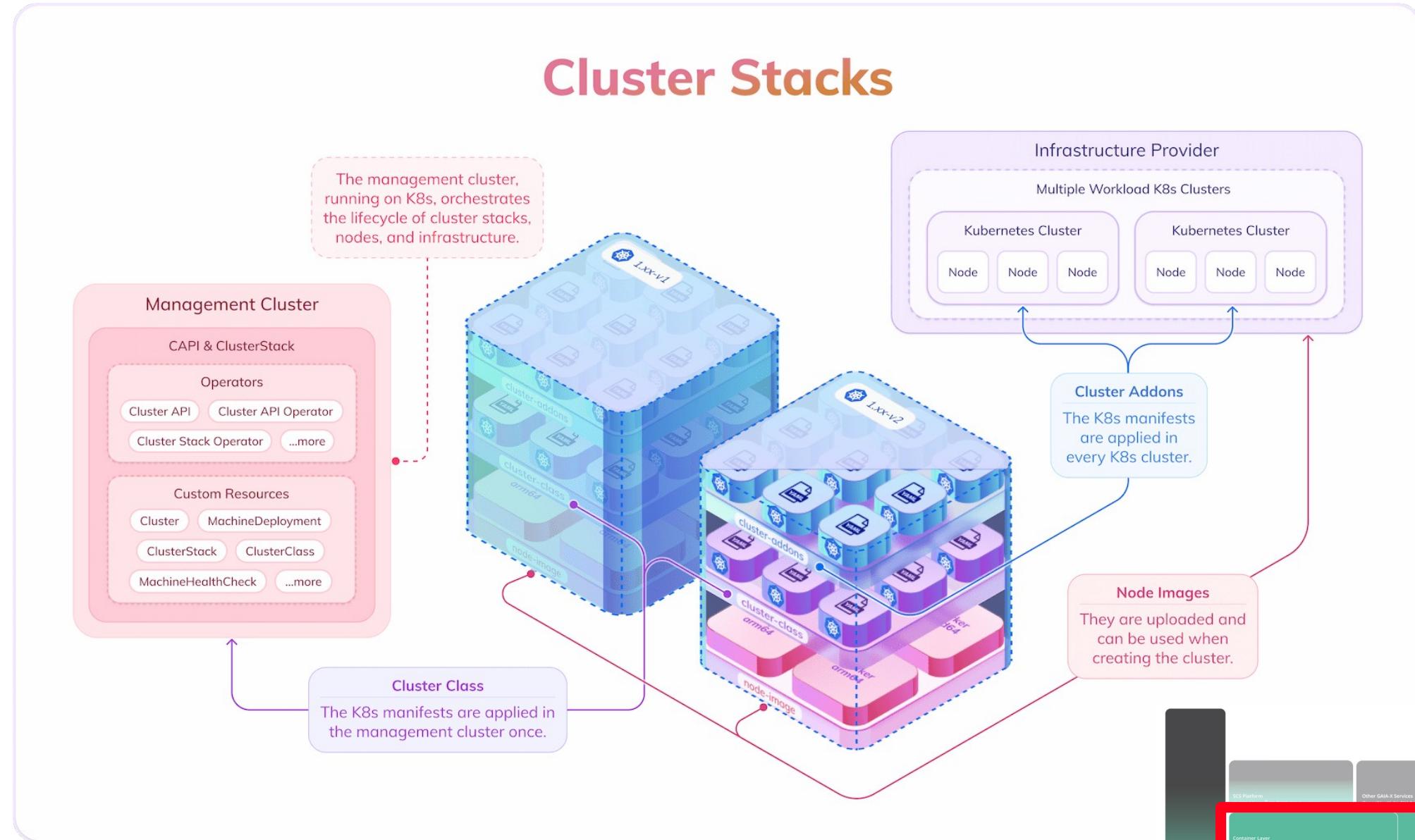
Virtualization & IaaS



- Compute Virtualization: KVM (Linux)
- Storage SDS: ceph (incl. rados GW) – ceph-ansible / ceph-rook
- Network SDN: OvS + OVN
- ... orchestrated via OpenStack core services & APIs
(deployed containerized with OSISM / kolla-ansible)



Container layer



Platform Monitoring

https://monitoring.scs.community/d/e1b111ecbb5185e637d5a7eef26e850f/kubernetes-monitoring-harbor?ref=...

ctrl+k

Search or jump to... Sign in

Home > Dashboards > dNation > Kubernetes Monitoring Harbor

2024-05-13 15:11:58 to 2024-05-13 15:16:58 10s

Alerts

Critical: 0

Warning: 0

Control Plane

- API Server: 100%
- Controller Manager: 100%
- Etcd: 100%
- Kubelet: 100%
- Proxy: 100%
- Scheduler: 100%

Overview

- Nodes Health: 100%
- Running StatefulSets: 100%
- Running Pods: 100%
- Succeeded Jobs: 100%
- Deployments Health: 100%
- DaemonSets Health: 100%
- Running Containers: 100%
- PVC Bound: 100%
- Most Utilized Pod: 59.7%

Master Nodes Metrics

Category	Value
CPU	Overall Utilization: 23.3% Most Utilized Node: 26.3%
RAM	Overall Utilization: 44.1% Most Utilized Node: 46.6%
Disk	Overall Utilization: 24.3% Most Utilized Node: 53%
Network	Overall Errors: 0 p/s Most Affected Node: 0 p/s
Used Cores	1.40
Total Cores	6
Used RAM	5.04 GiB
Total RAM	11.5 GiB
Used Disk	26.4 GiB
Total Disk	62.5 GiB

Worker Nodes Metrics

Category	Value
CPU	Overall Utilization: 0% Most Utilized Node: 0%
RAM	Overall Utilization: 0% Most Utilized Node: 0%
Disk	Overall Utilization: 0% Most Utilized Node: 0%
Network	Overall Errors: 0 p/s Most Affected Node: 0 p/s

Automation

SCS Platform: A service layer for managing the SCS stack.

Other GAIA-X Services: Compatible with this GAIA-X execution layer via self-description.

Container Layer: Used for management.

Compute (IaaS): Provides cloud computing services.

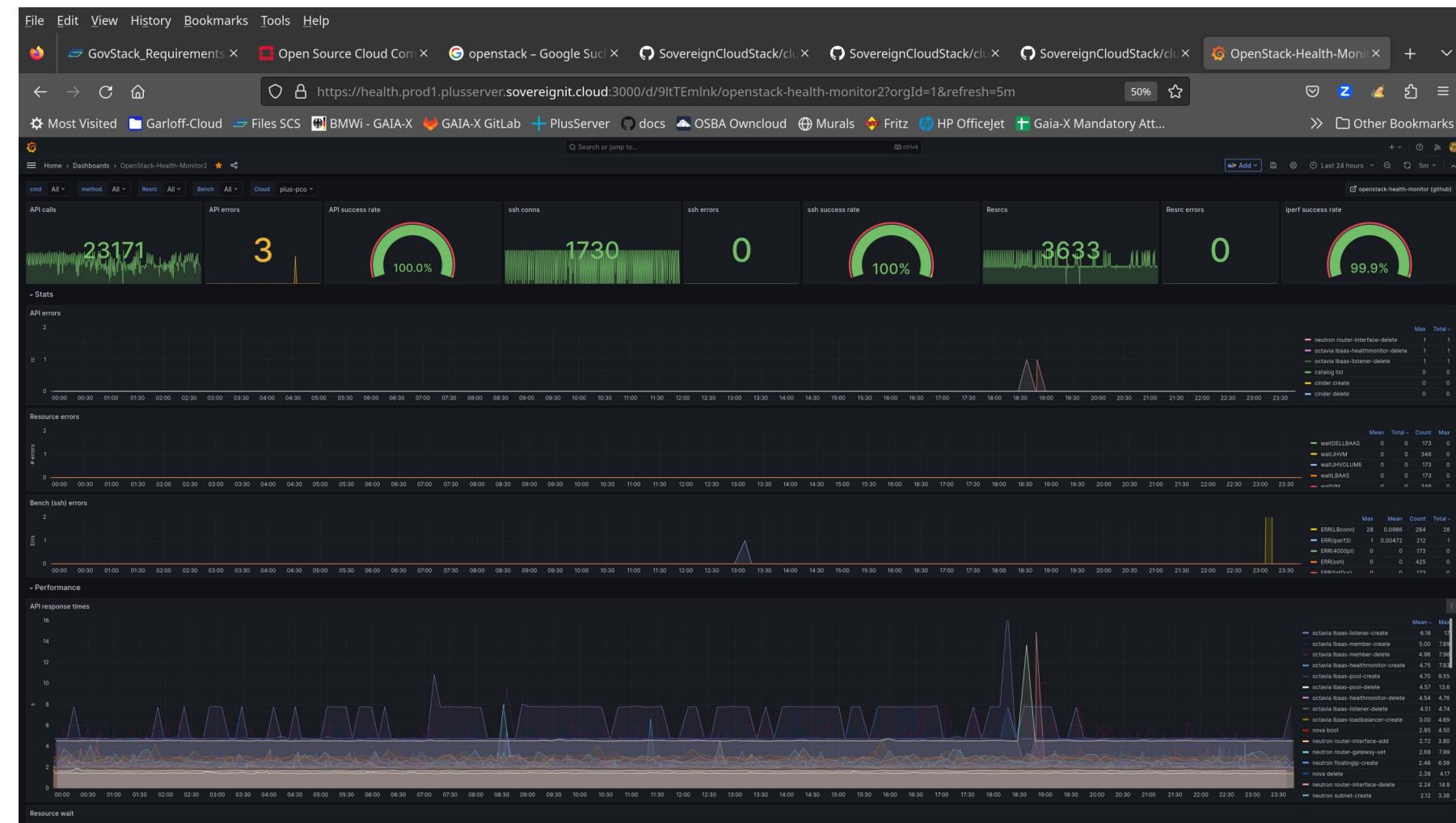
Storage SDS: Provides storage services.

Network SDN: Provides network services.

Node Wide Identity Access Management: Manages identities across nodes.

Infra Monitoring

- Health monitoring (→ scenario tests)
- Compliance monitoring (public for SCS-certified)
- Metrics collection for metering and operations (prometheus)
- Alert-Manager

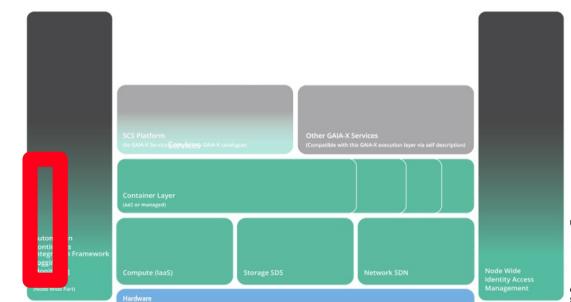
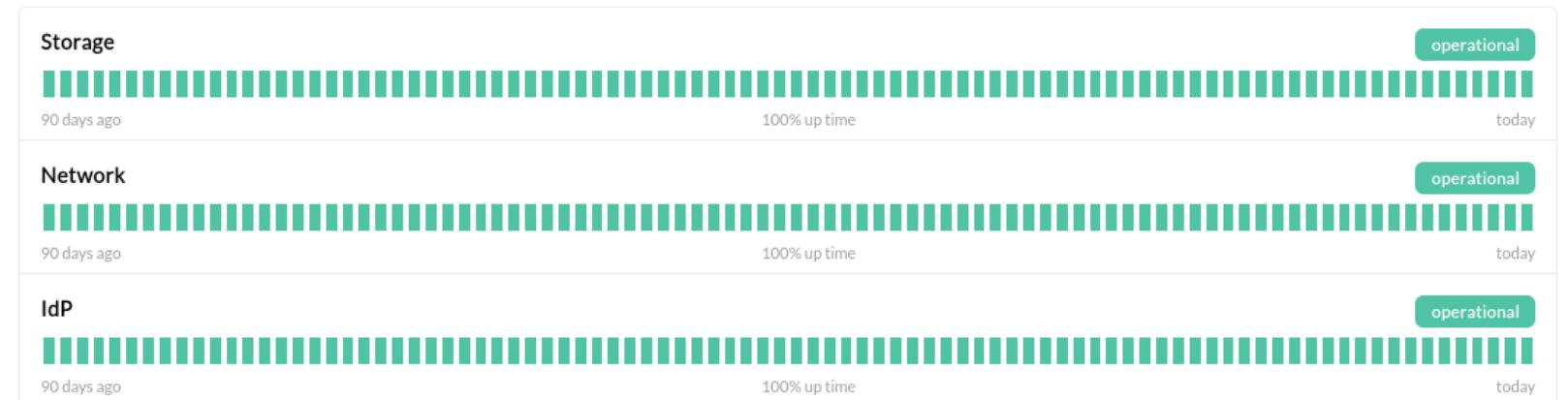


Status Page (with own API)

- Manage incident status, current or planned
- Clear design with simple colors, historic events

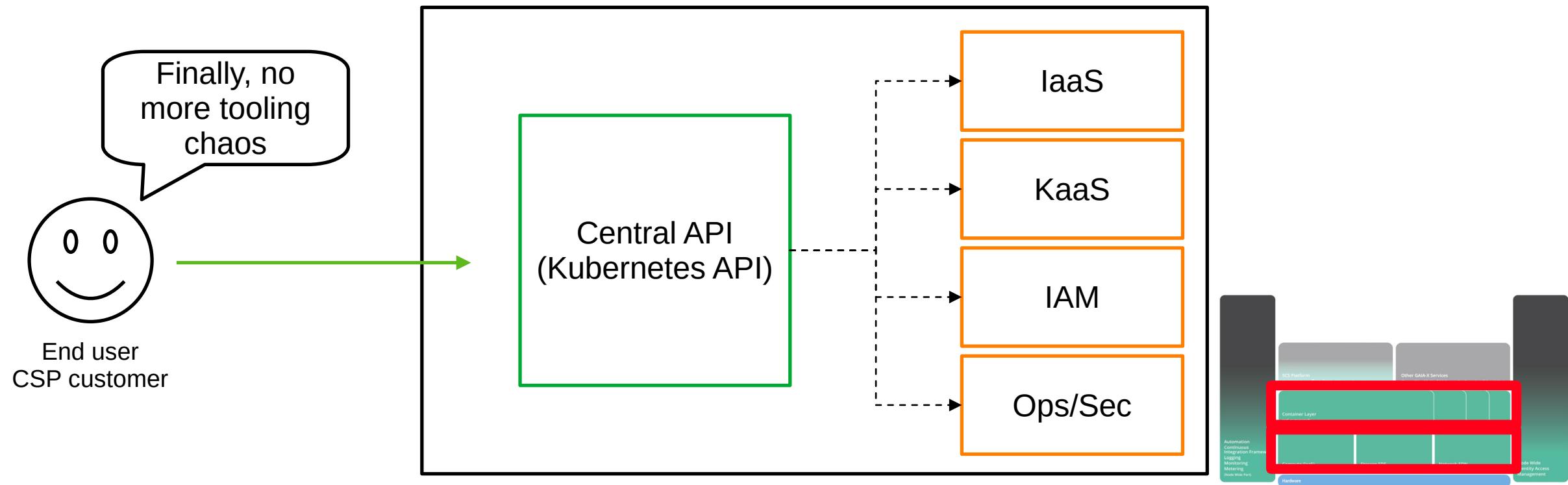


End user
CSP customer

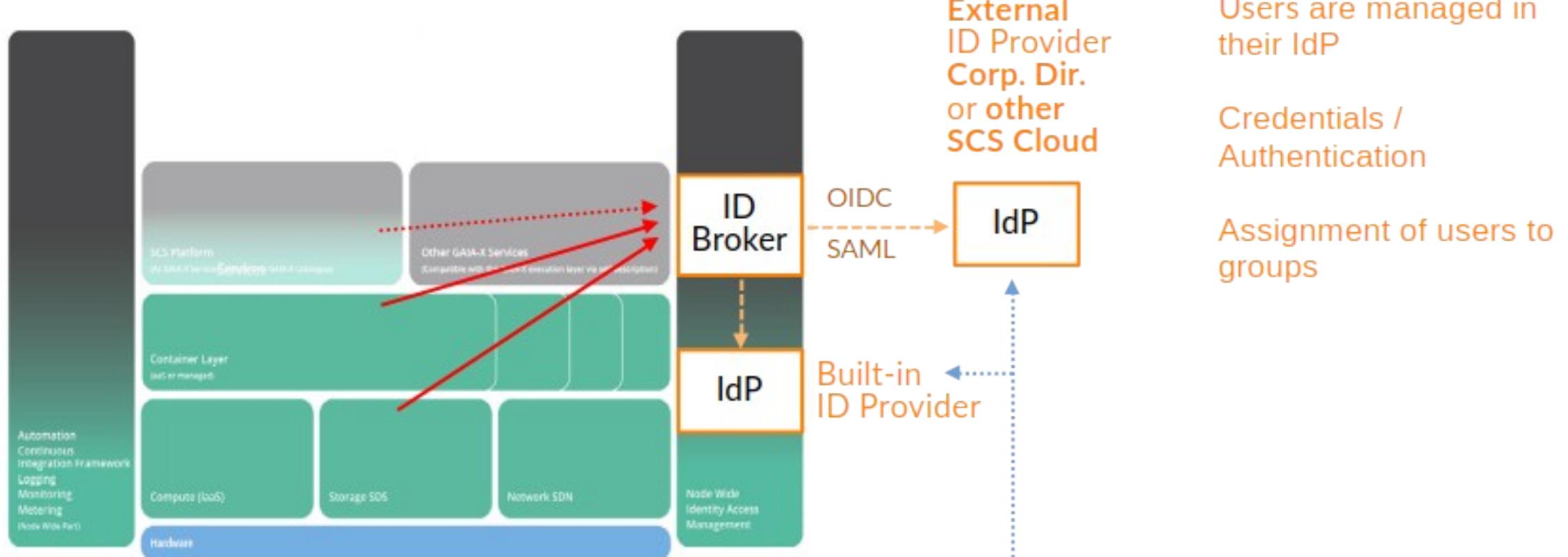


Central API – one endpoint for daily business

- Standardized API endpoint for majority of use cases
- Combines IaaS, KaaS, IAM and Ops into 1
- Powered by Kubernetes and Crossplane



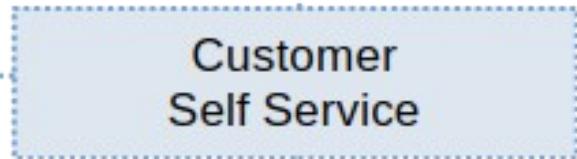
Self-Service Identity Federation: Cross-Service and Cross-Cloud identities



All functional layers use Identities from built-in Identity Broker (keycloak) for customers

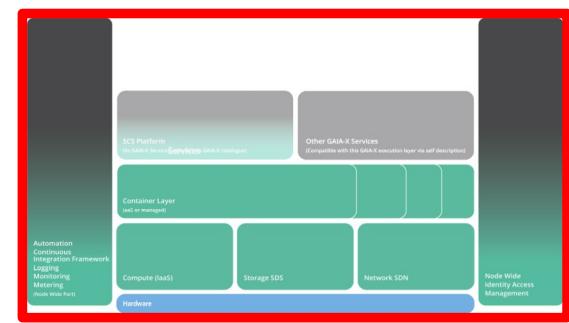
ID Broker maps groups to role assignments (authorizations) on resources in this specific cloud

Customer manages his own domain / realm



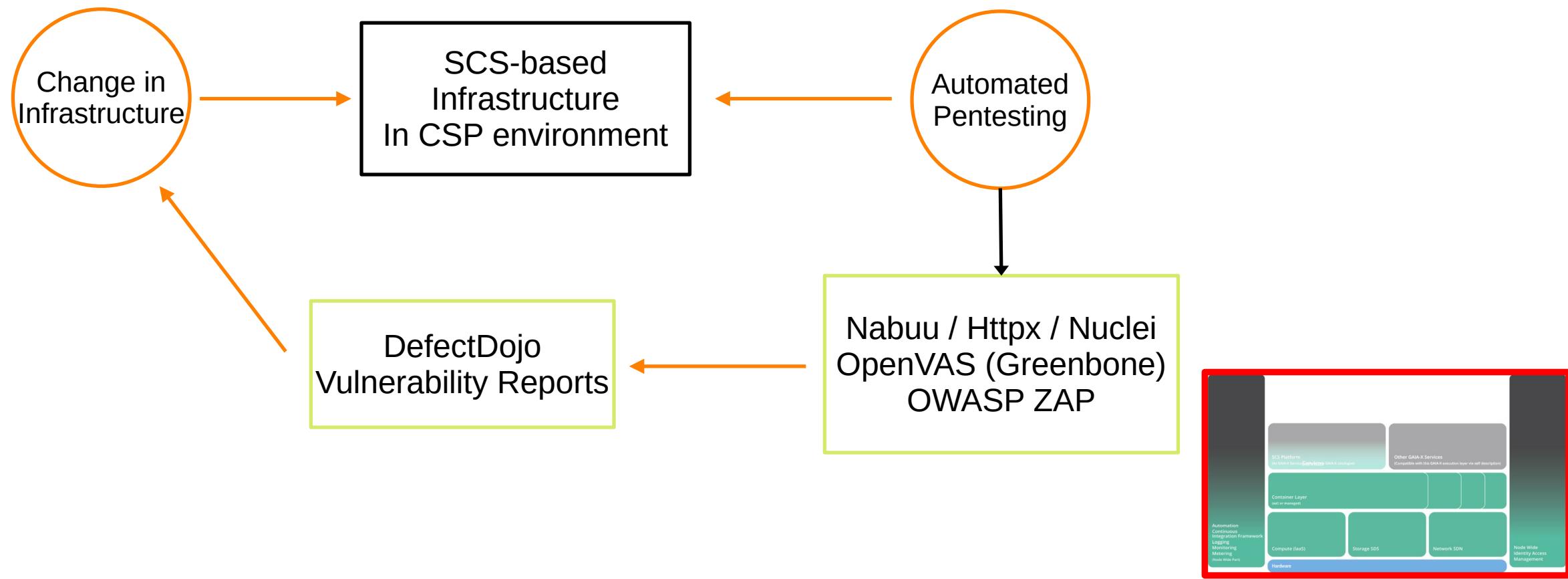
Security by design

- Standardized best practices
- Deployment uses strong secure defaults
- Hardware isolation features, confidential computing
- Sharing knowledge through blog posts
- Supply chain security



Automated Security Penetration Testing

- Dynamic Security Analysis of deployed infrastructure
- Scheduled job creates daily reports



Summary

The **SCS software** is a secure, complete and open turnkey solution:
HW deployment, Virtualization layer (IaaS), Container Layer,
Federated Identity Management, Operational tooling, Security

The **SCS software** fulfills all **SCS standards** (and is thus the **SCS** reference implementation)

In productive use in parts or as a whole at various Operators,
public and private Cloud

Operations supported by knowledge sharing (**Open Operations**)



— An **OSB ALLIANCE** project —

Supported by:



Federal Ministry
for Economic Affairs
and Climate Action



<https://scs.community>

on the basis of a decision
by the German Bundestag



Save the date:
SCS Summit #3
8. Mai 2025
Berlin

One platform – standardised, built and operated by many.

<https://scs.community>