



Supported by:



on the basis of a decision  
by the German Bundestag



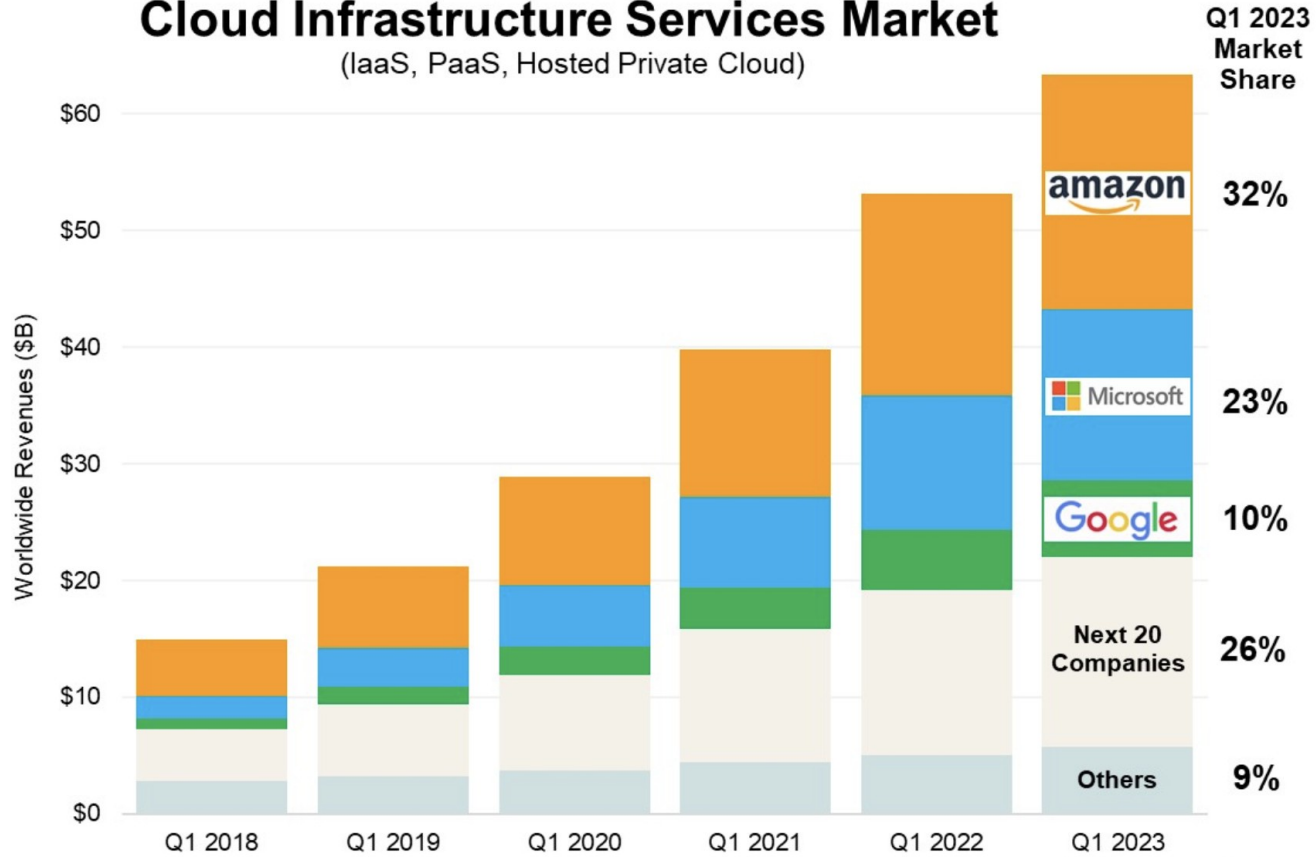
C4DT Conference on Trustworthy and Sovereign Cloud Computing  
September 13th, 2023

Dr. Manuela Urban

# Sovereign Cloud Stack: Open Source and Open Operations Solutions

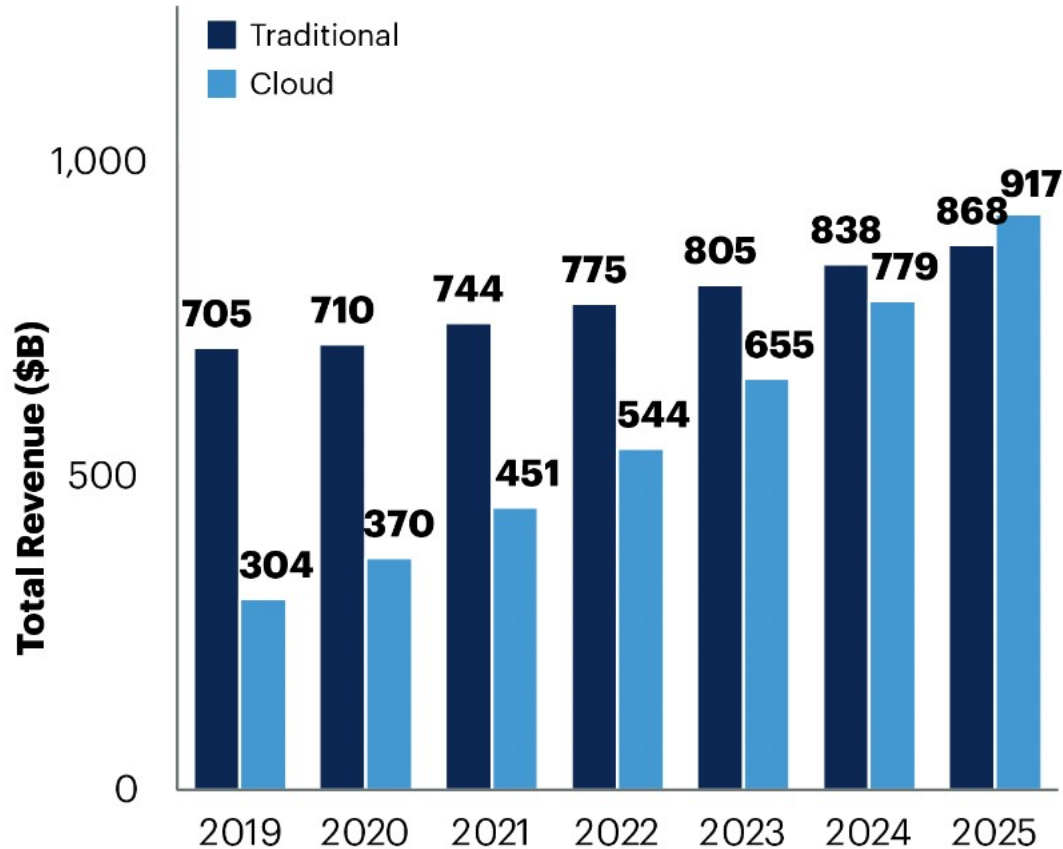
# Cloud Infrastructure Services Market

(IaaS, PaaS, Hosted Private Cloud)



Source: Synergy Research Group

# "Cloud-Shift": Enterprise IT Spending Worldwide



Source: Gartner 2022

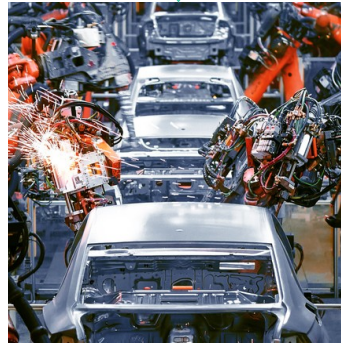
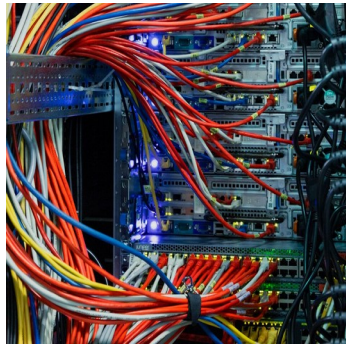


# Sovereign Cloud Stack

...is an open community that builds standardised Open Source cloud technology and shares operational knowledge.



# Sovereign Cloud Stack Mission: Open Source Cloud Technology Toolbox and a Community of Practice for all Sectors



# SCS Supporting Organisations

23|Technologies



SPRIN-D



cleura



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.



OVHcloud

plusseryer

Stackable

StackHPC

Syself

univention  
be open

WAVECON



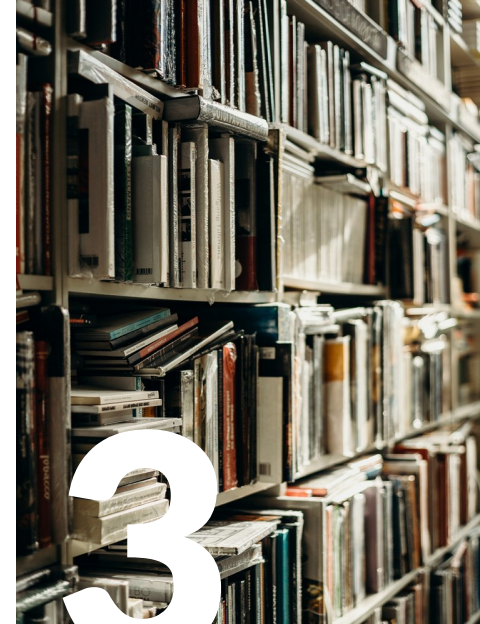
# Sovereign Cloud Stack Deliverables



Certifiable Standards

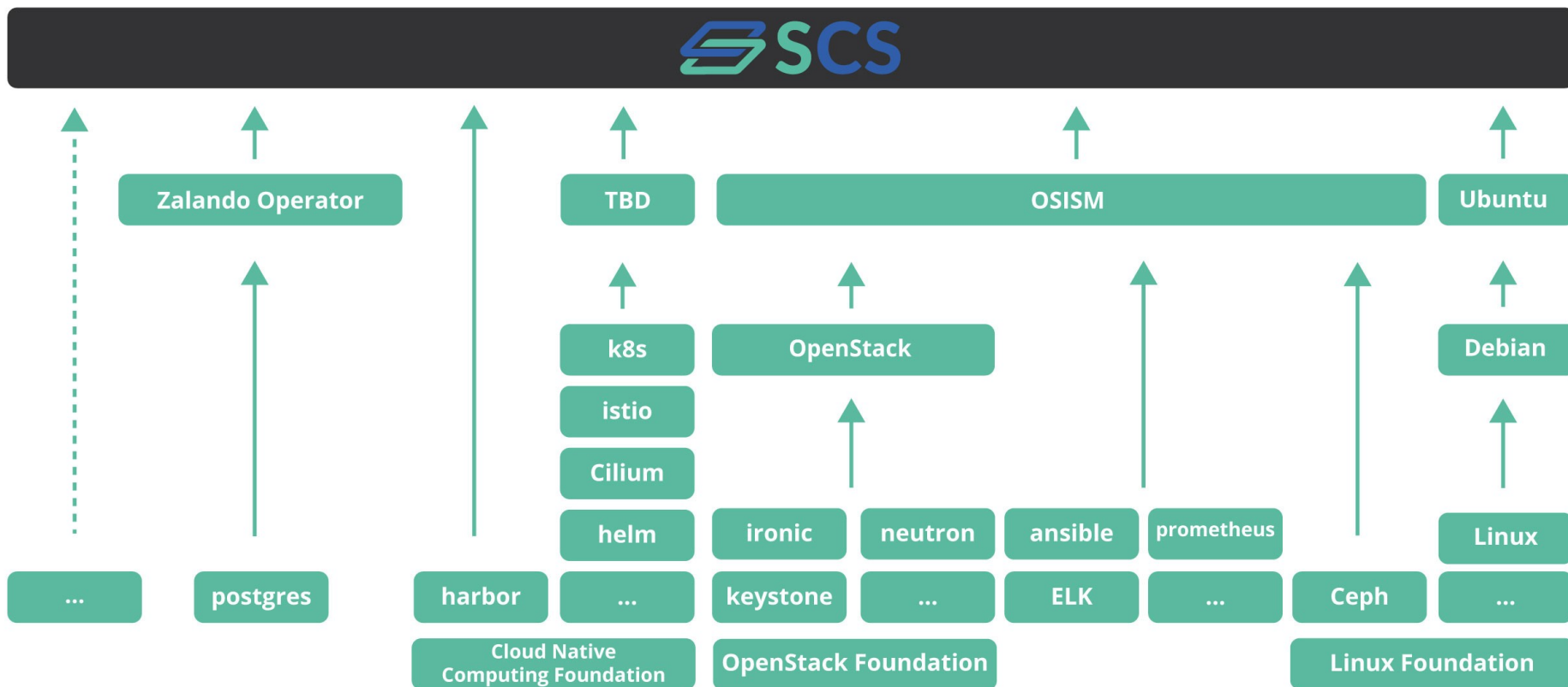


Modular Open Source  
Reference Implementation



Operational Knowledge

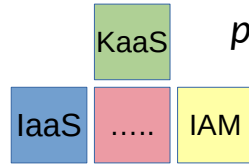
# SCS integrates, standardizes and complements proven building blocks





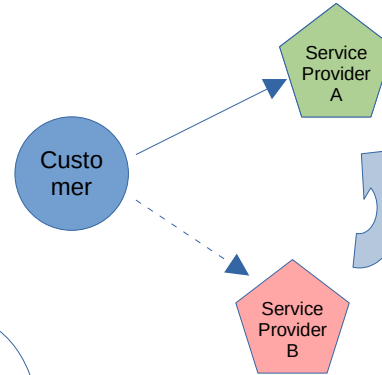
# SCS Certified Standards provide...

Modularity



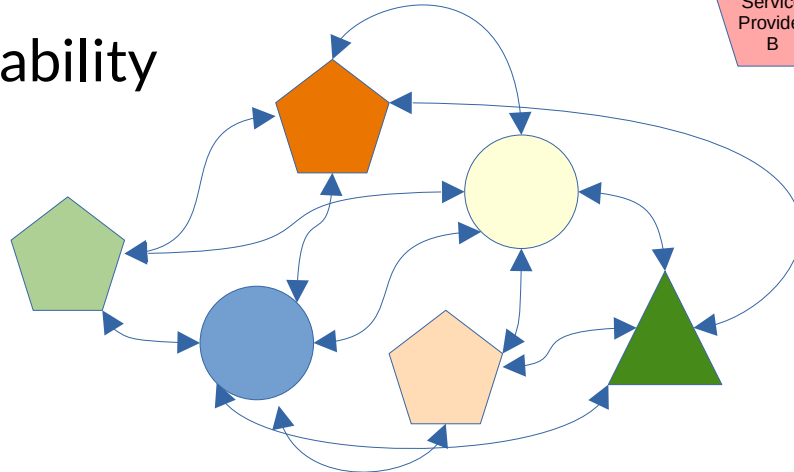
All pieces can be used independently or put together to build a complete stack.

Interoperability, Portability



Choose your service provider freely, transfer your data & applications easily and safely.

Federability, Scalability



Build a virtual hyperscaler.



tagesschau

Sendung verpasst?



Cloud-Anwendungen

## Hacker-Angriff auf Microsoft war gravierend

Stand: 08.09.2023 12:03 Uhr

# Open Operations

## 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

RCA templates

Link collection



# OPEN OPERATIONS MANIFESTO

Building a community of practice and transparency for operations

<https://openoperations.org>

## **We build a community of practice**

Open Operations builds a community of practice to keep the barrier to entry low and create a thriving environment for comfortable exchange.

## **We share knowledge**

The availability of knowledge and skilled engineers is the limiting factor for many organizations to adopt, leverage, and successfully operate complex technology.

## **We're transparent about our incidents**

We firmly believe that failures make us experts. The way we handle mistakes is how we become better.

## **We're transparent about our operational processes**

We share our internal processes for the sake of transparency. We firmly believe that transparency leads to better and more reliable processes.



# Cloud Services based on SCS

## pluscloud open



by

plusseryer



Bundesamt  
für Sicherheit in der  
Informationstechnik



wavestack

by

**noris network**



BETACLOUD

by

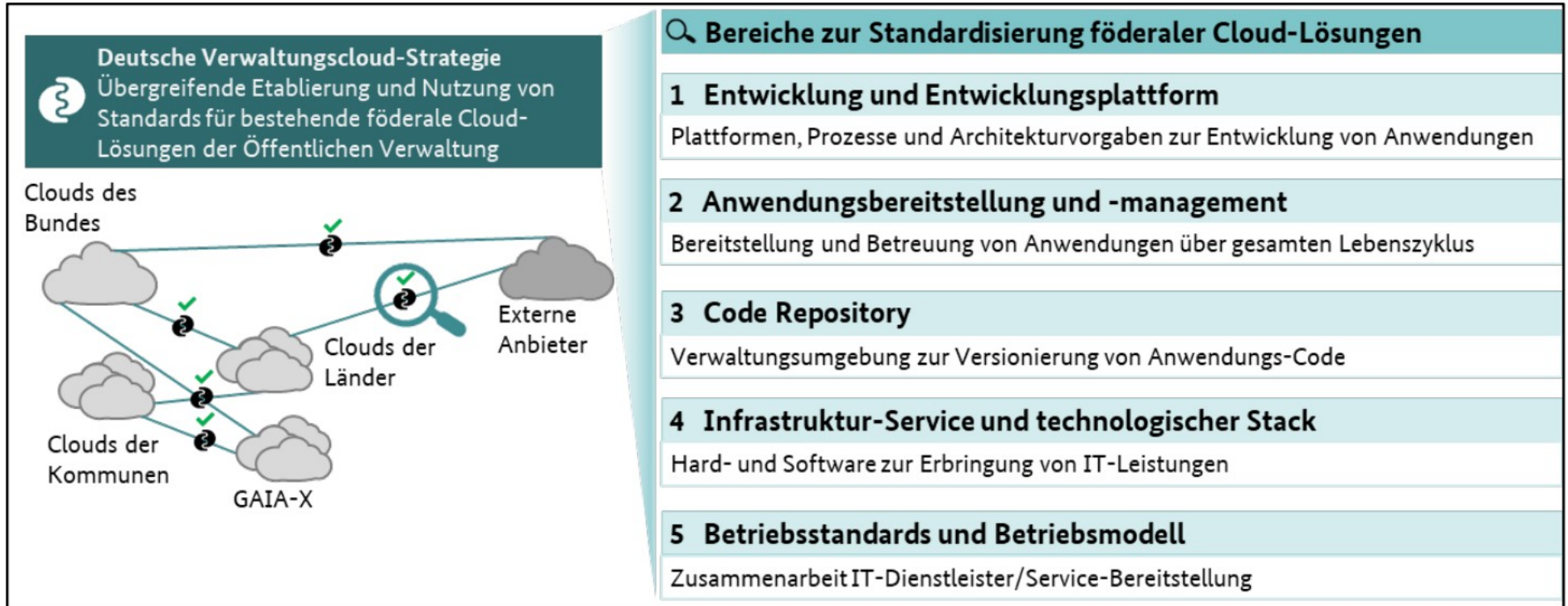


OSISM



*...more are under development.*

# SCS is involved in the German Federal Public Admin Cloud (Deutsche VerwaltungscLOUD DVC)



## 🔍 Bereiche zur Standardisierung föderaler Cloud-Lösungen

### 1 Entwicklung und Entwicklungsplattform

Plattformen, Prozesse und Architekturvorgaben zur Entwicklung von Anwendungen

### 2 Anwendungsbereitstellung und -management

Bereitstellung und Betreuung von Anwendungen über gesamten Lebenszyklus

### 3 Code Repository

Verwaltungsumgebung zur Versionierung von Anwendungs-Code

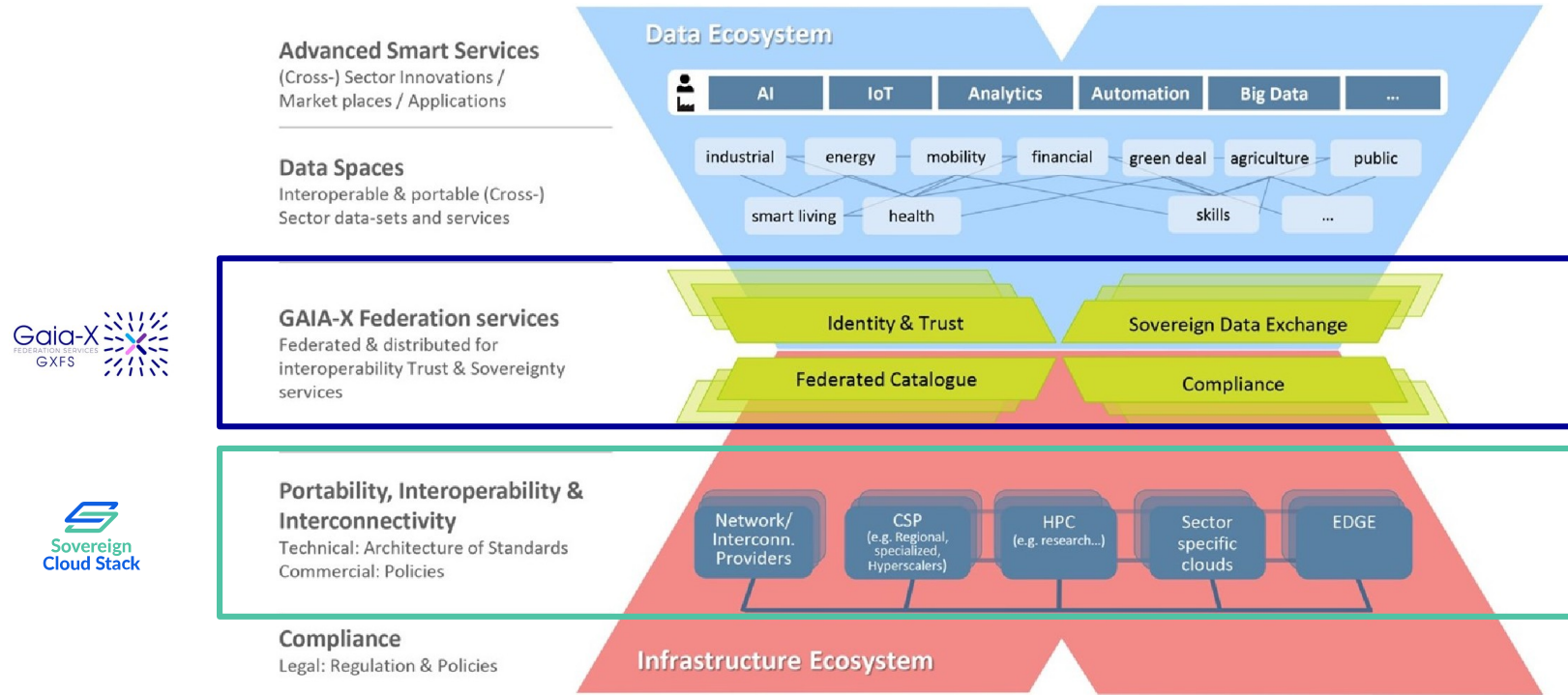
### 4 Infrastruktur-Service und technologischer Stack

Hard- und Software zur Erbringung von IT-Leistungen

### 5 Betriebsstandards und Betriebsmodell

Zusammenarbeit IT-Dienstleister/Service-Bereitstellung

# SCS provides a Technical Underpinning for Gaia-X



# SCS contributes to GovStack

GovStack harnesses the power of a global network and is led by:



About ▾

Our Offerings ▾

Global Showcase

News & Events

Participate ▾



## GovSpecs

We work with governments to identify real-life scenarios for digital...

[Learn more](#)



## GovTest

We provide an open demonstration environment for...

[Learn more](#)



## GovLearn

We collaborate to provide capacity building, trainings, and support designing...

[Learn more](#)



## GovExchange

We offer a platform to research the market of digital services and find...

[Learn more](#)

digital  
impact  
alliance





— An OSB ALLIANCE project —



<https://scs.community>

Supported by:



Federal Ministry  
for Economic Affairs  
and Climate Action

on the basis of a decision  
by the German Bundestag

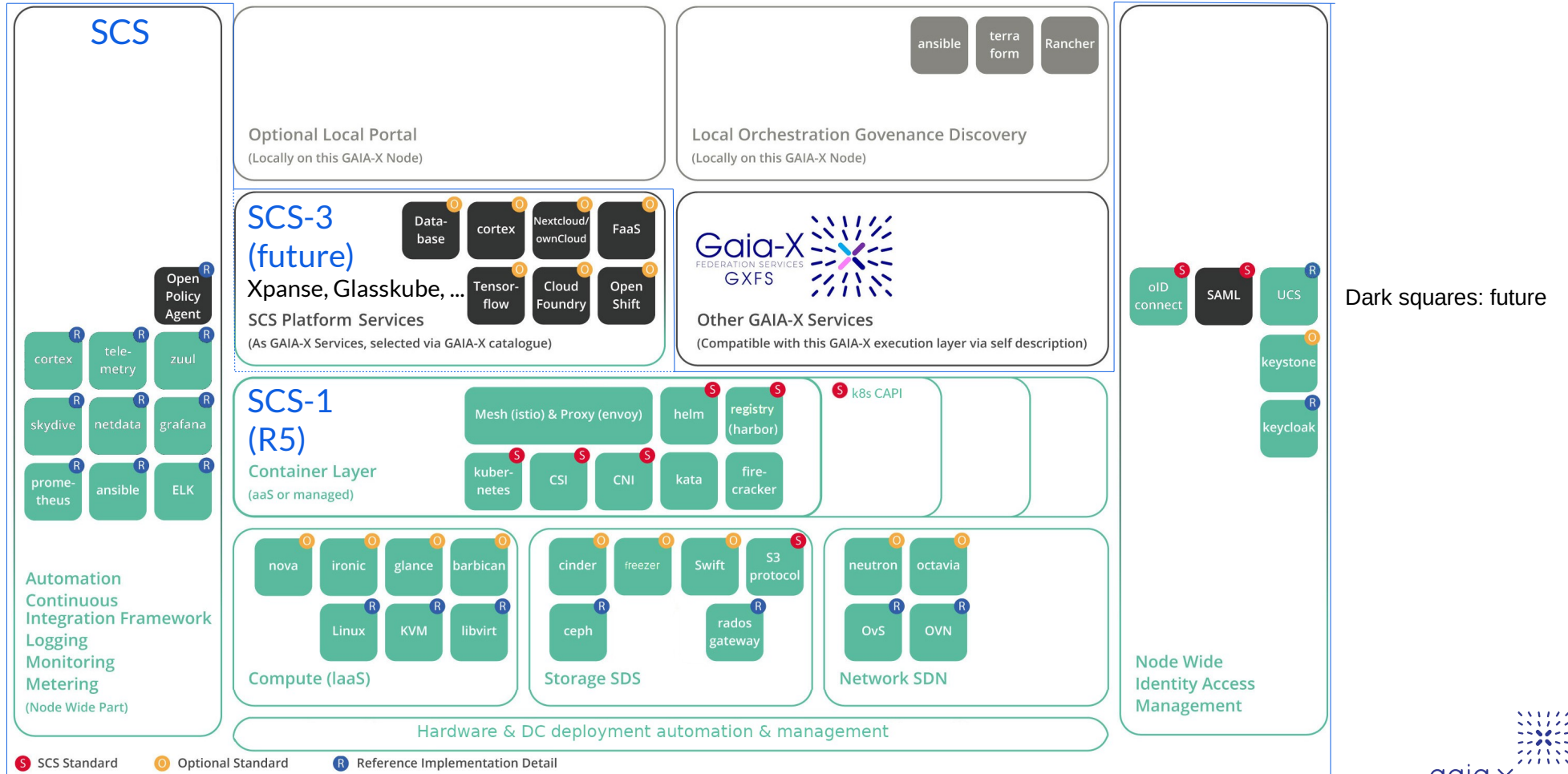


<https://scs.community>

**One platform – standardised, built and operated by many.**

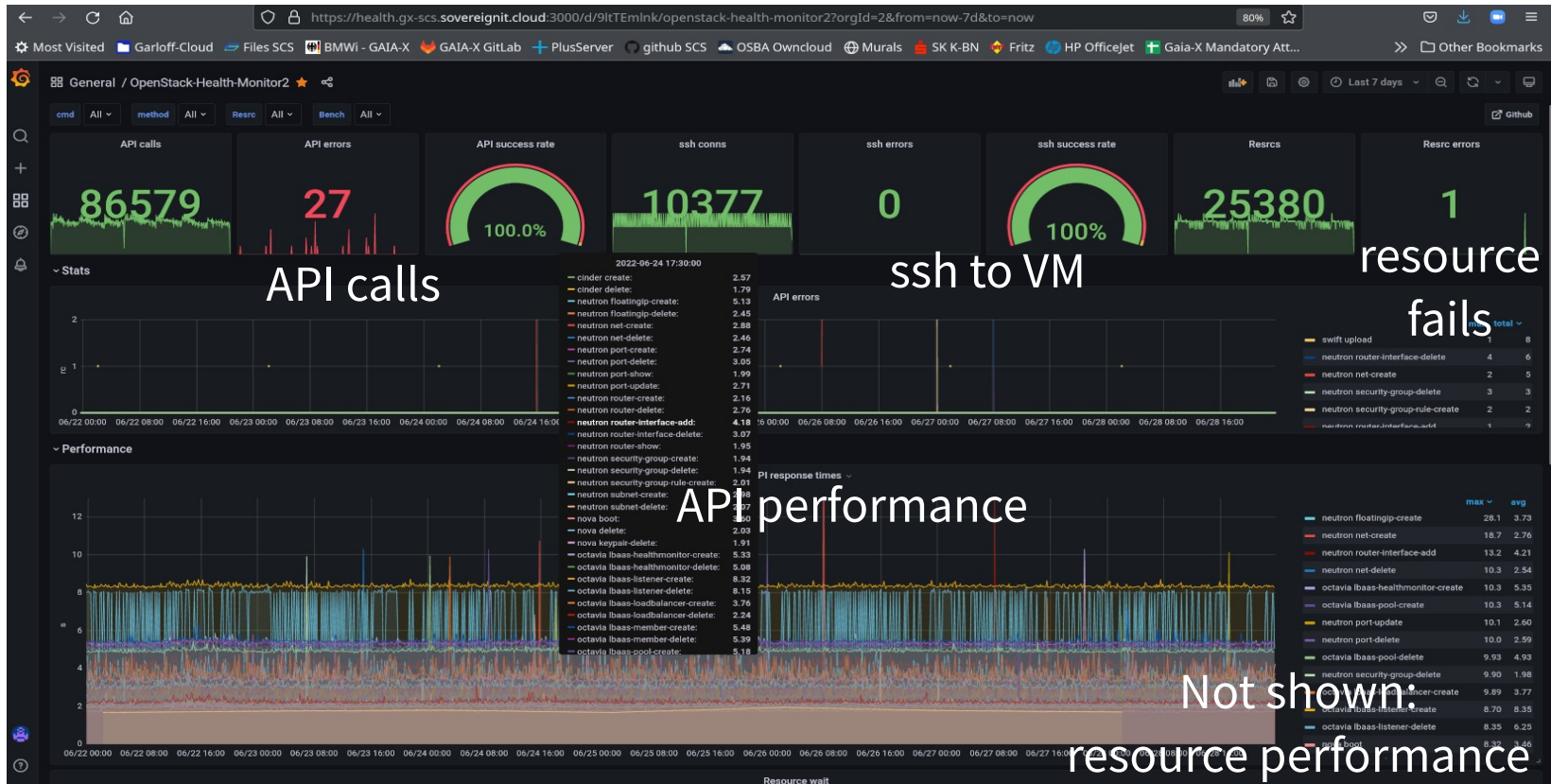
# Supplement

# SCS Reference Architecture (current status)





# SCS Operations: Measure what you want to manage.





# Operations: SCS Tooling



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]

**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

## 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 >

### Device Roles

Name	Devices	VMs	Color	VM Role	Description
<input type="checkbox"/> Ceph control node	0	0	Orange	✓	—
<input type="checkbox"/> Ceph resource node	0	0	Orange	✓	—
<input type="checkbox"/> Compute node	0	0	Blue	✓	—
<input type="checkbox"/> Control node	0	0	Blue	✓	—
<input type="checkbox"/> Generic node	0	0	Black	✓	—
<input type="checkbox"/> Manager node	0	0	Green	✓	—
<input type="checkbox"/> Monitoring node	0	0	Green	✓	—
<input type="checkbox"/> Network node	0	0	Blue	✓	—

50 per page  
Showing 1-8 of 8

Kibana

Netbox

# SCS Open Development in Practice

< >
today edit
18 – 22 Sep 2023

day week month

	Mon 18/09	Tue 19/09	Wed 20/09	Thu 21/09	Fri 22/09
all-day					
09				09:05 - 9:55 GMT+2 Team OPS Sprint Review/Planning and Refinement	
9:30					
10			10:05 - 10:55 GMT+2 Team IaaS Sprint Review/Planning and Refinement		10:05 - 10:55 GMT+2 IAM Hacking session
10:30				10:35 - 11:25 GMT+2 Team Container Sprint Review/Planning and Refinement	
11	11:05 - 11:55 GMT+2 SIG Documentation				
11:30			11:35 - 12:25 GMT+2 Team IAM Sprint Review/Planning and Refinement		
12					
12:30					
13					
13:30					
14	14:05 - 14:55 GMT+2 SCS Product Board			14:05 - 14:55 GMT+2 SIG Standardization/Certification	
14:30					
15	15:05 - 15:55 GMT+2 Blocker: SCS Team Overflow/Replacement	15:05 - 15:55 GMT+2 Lean SCS Operator Coffee		15:05 - 15:45 GMT+2 Weekly SCS Community Meeting	
15:30					

# SCS: Realize Digital Sovereignty



Competence (esp. Operations)

Ability to shape technology

Choice / Switching / Interoperability

Legal Compliance (GDPR ...)



<https://rdcu.be/cWdBJ>

# SCS Certification

## Levels of digital sovereignty

4: Operational transparency and knowledge and skills available

3: Transparent technology and capability to contribute & shape

2: Freedom of choice (many providers as well as on-prem) , Interoperability, Portability

1: Legal compliance



## SCS certification levels



3: “**SCS-Sovereign**” – Ops/IAM Stacks “open” as well, transparency on monitoring, incidents, contributing to “Open Operations”  
(5x Open)

2: “**SCS-Open**” – SBOM for functional stack available, fully “open”  
(4x Open according OpenInfra Foundation)

1: “**SCS-Compatible**” – Technical compatibility, interoperabel (Conformance tests pass: CNCF, OIF, SCS)

0: ENISA / Gaia-X labels / GDPR (no SCS certificate)

# 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 community on further improving supply chain security (reproducible builds, scanning, ...)

## Confidential computing

- Work with intel (and AMD) on TDX / SVE enablement for additional protection





# SCS Open Source Health Check

<https://github.com/SovereignCloudStack/Docs/blob/main/Design-Docs/OSS-Health.md>

1. Really Open: Four Opens (Code, Development, Design, Community)
2. Maturity: Quality, Reviews, CI, Maintenance, Standards
3. Security: Supply Chain, Sec Response, SecTesting / PenTest
4. Activity: Adoption, Community, Ecosystem
5. Risk Assessment: Likelihood to fail? Replace? Fork?

# SCS: How to start

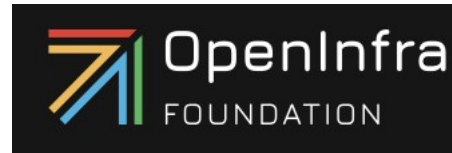
1. Use existing SCS public cloud IaaS offerings:
  - OSISM's betacloud, PlusServer's pluscloudopen, Wavecon/Noris' wavestack, regio.digital
  - a) Running SCS ref.impl. for k8s aaS (KaaS) on top of it
  - b) Using managed SCS ref.impl. for KaaS (using e.g. sysself, see GXFS)
  - c) Using Gardener based managed k8s (PSKE, ...)
2. Use Cloud-in-a-Box (128GB RAM box for 3.5k€)
3. Deploy SCS testbed on top of pre-existing OpenStack IaaS.  
*(Deploy SCS on a notebook in a camper van as Robert Holling @ HS Osnabrück did.)*
4. Build small PoC env (min. 5 hardware nodes: 4\*HCI+1\*Manager)
5. Production env. ~12 -- 300 nodes

# The Four Opens

1. Open Source
2. Open Design
3. Open Development
4. Open Community

*A fifth Open?*

5. Open Operations



# Zur Bedeutung von Open Source

## EU-Studie: Open Source stärkt die Wirtschaft und die technologische Unabhängigkeit

FEATURED | VERBANDS-NEWS | 13. DEZEMBER 2021



<https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and>

<https://www.acatech.de/publikation/open-source-i40-innovationstreiber/>



# SCS: Why thoroughly Open?

- Highly innovative
- Best possible quality
- Efficiency and reduced complexity.
- Trust through transparency
- Digital sovereignty
- We believe that basic cloud technology and know-how should be common property.

