Sovereign Cloud Stack

SCS: Sovereign Cloud Infrastructure Software & Ecosystem

Kurt Garloff, Peter Ganten
Christian Berendt, Dirk Loßack, Oliver Mauss

Prepared for Open Source Day 2020-11-19

Quo vadis, Europe?
Digitalization Dilemma

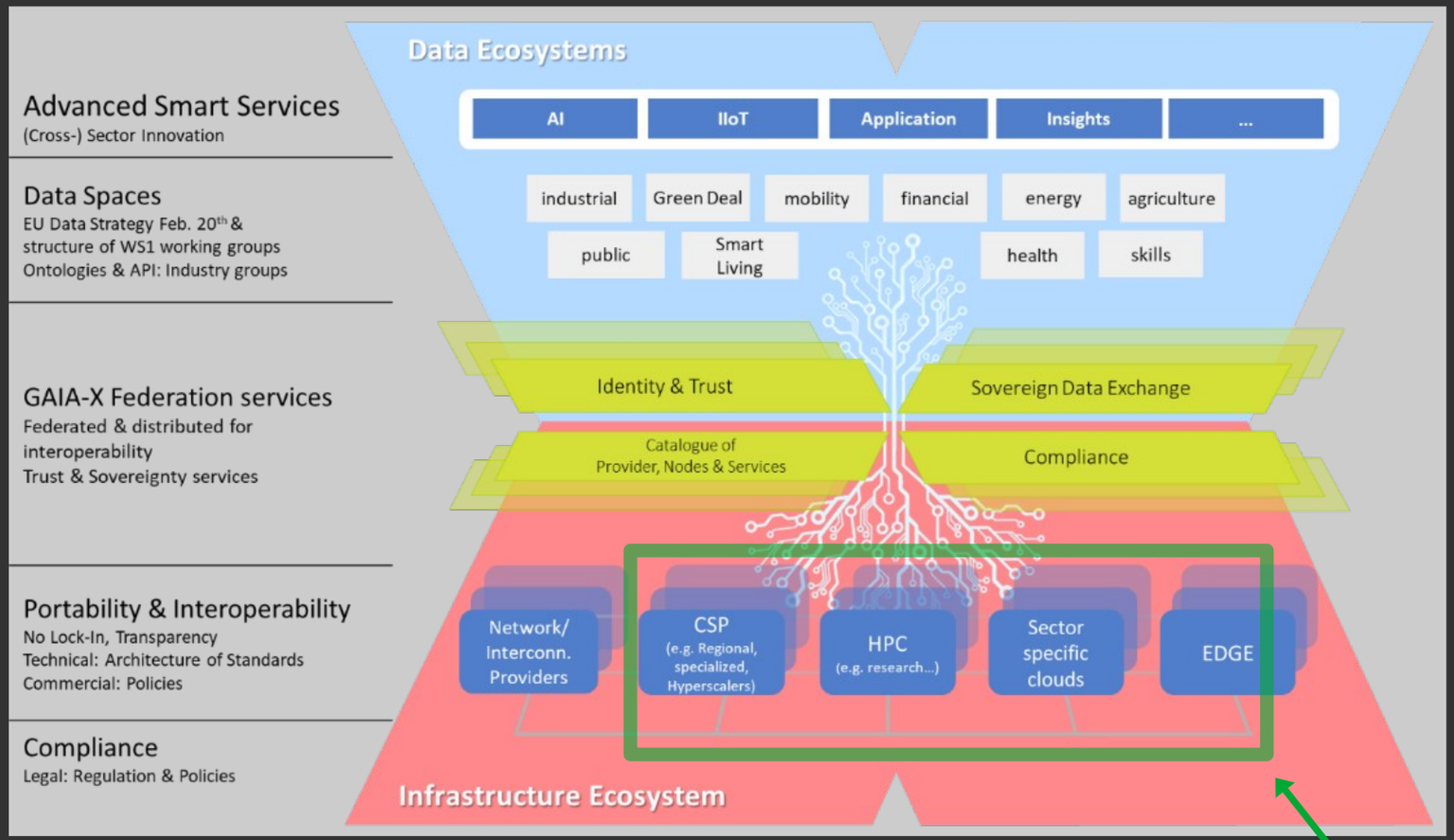
?

Classical development & production:
+ Well-protected in-house
+ Close to developer / in-house support
o Bare-Metal, Enterprise Virtualization
o Proprietary tooling, niche solutions
- Slow, manual deployment processes
- Even slower approval processes (CapEx)

Own Infra-as-Code platform:
+ API driven automation
+ Flexible, optimized
- Non-standardized, niche solutions
- Not enhancable by federation with others
- Expensive/scarce skills needed to operate

Infra-as-Code on Hyperscalers:
+ Full automation of infrastructure (API driven) allowing efficient Dev(Sec)Ops
+ Ready to use building blocks
+o A lot of Open Source tooling but sometimes not really (Open Core)
- Dependencies and lock-in
- Data protection challenges, no sovereignty
- Cloud Act; Privacy Shield & SCC dead

Enter GAIA-X



GAIA-X's mission is to strengthen digital sovereignty for business, science, government and society by empowering the development of innovation ecosystems. Digital sovereignty means that these individuals, organizations and communities stay in complete control over stored and processed data and are enabled to decide independently who is permitted to have access to it.

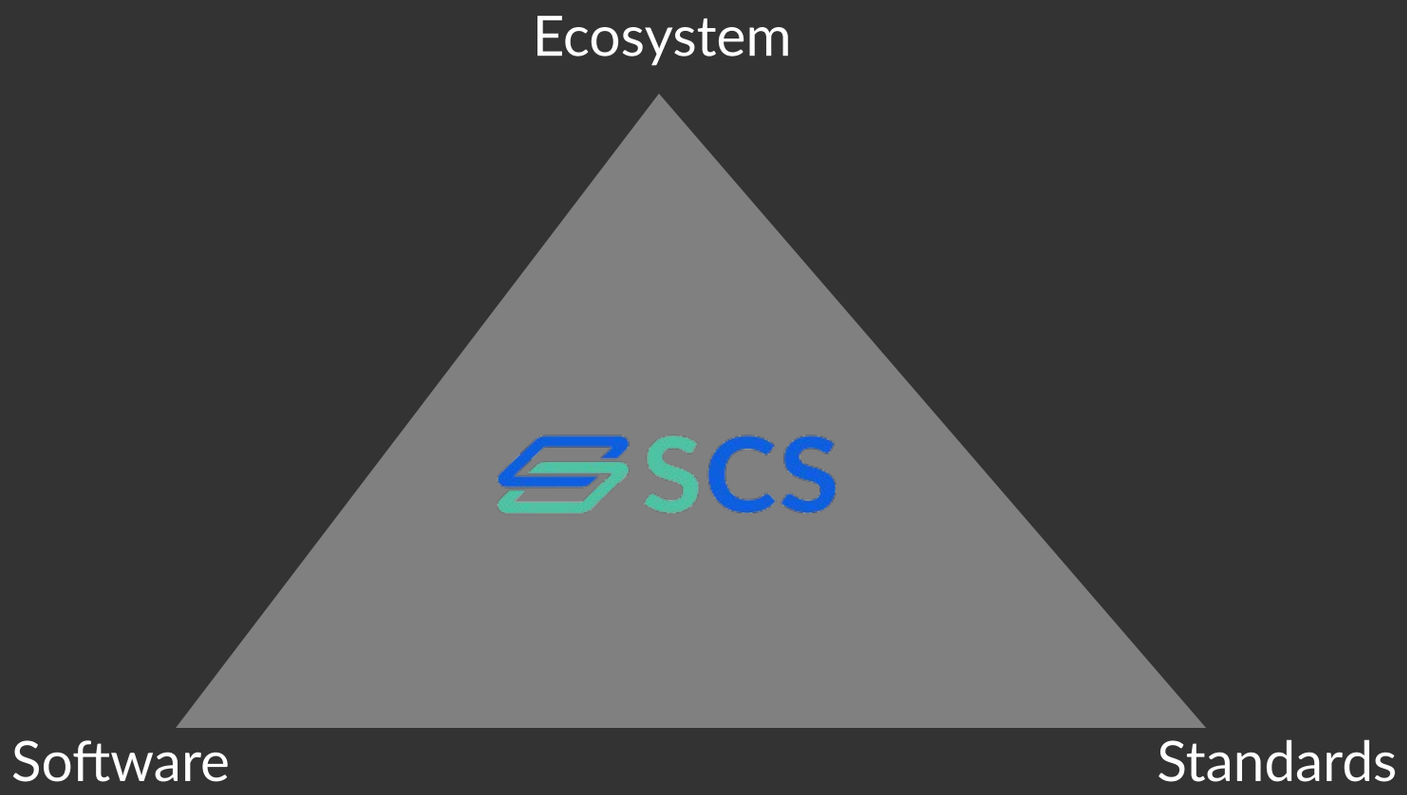
Source: (w/o SCS frame)
https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7

Sovereign Cloud Stack vision & mission

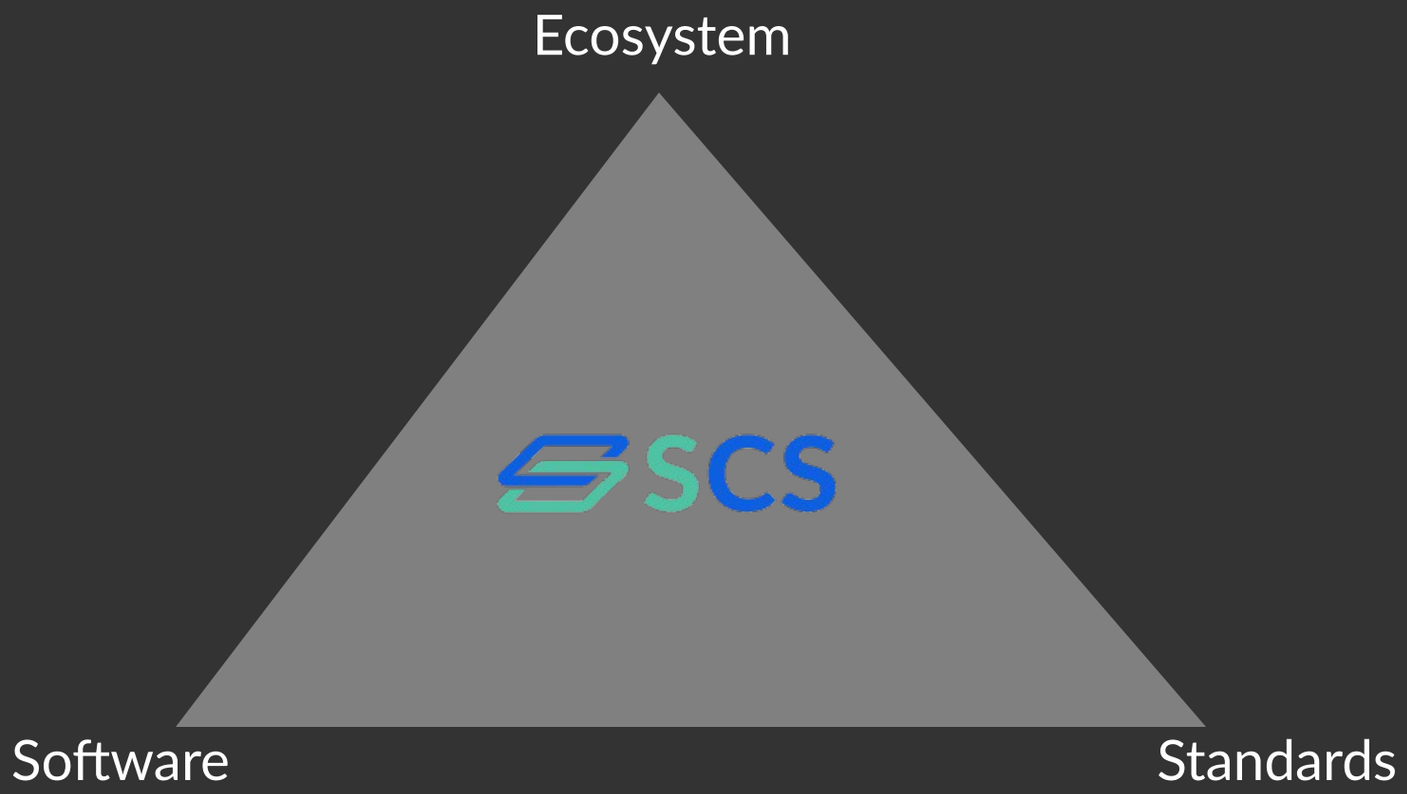
We imagine the desired IT landscape to be under the control of the developers and users, supported by a broad set of providers that deliver modern agile IT infrastructure and data services in certifiable interoperable and federated ways respecting their users' rights, data protection and security requirements. The easy availability of such compliant services enables digital innovation across the industry, research and public sector.

Sovereign Cloud Stack empowers IT developers and users to innovate on modern, self-service automated IT infrastructure that is sovereign, i.e. under their own control or under control of federatable providers that they can chose according to their technical, strategic and regulatory needs from a broad set of choices.

SCS Deliverables

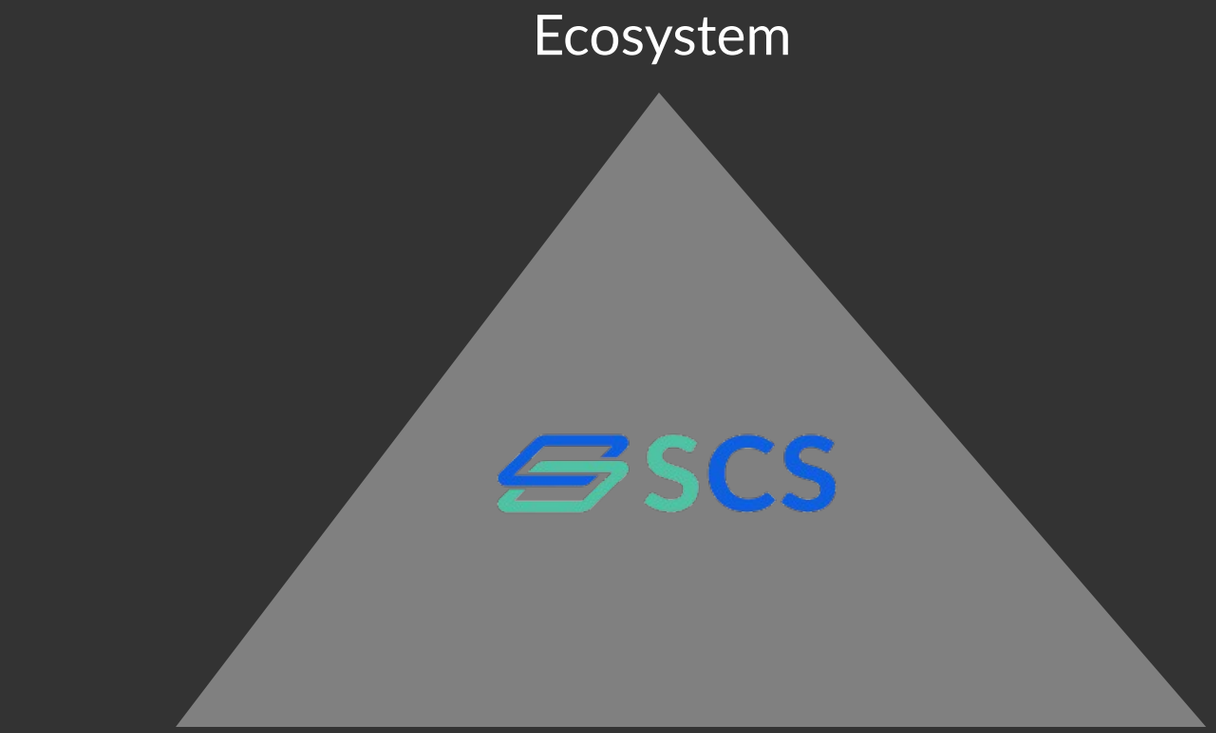


SCS Deliverables



- Complete Stack: IaaS, KaaS, (PaaS)
- Including Ops: Lifecycle Mgmt, Infra, CI, Moni
- Including Federatable IAM
- Modular
- Open (4x)

SCS Deliverables

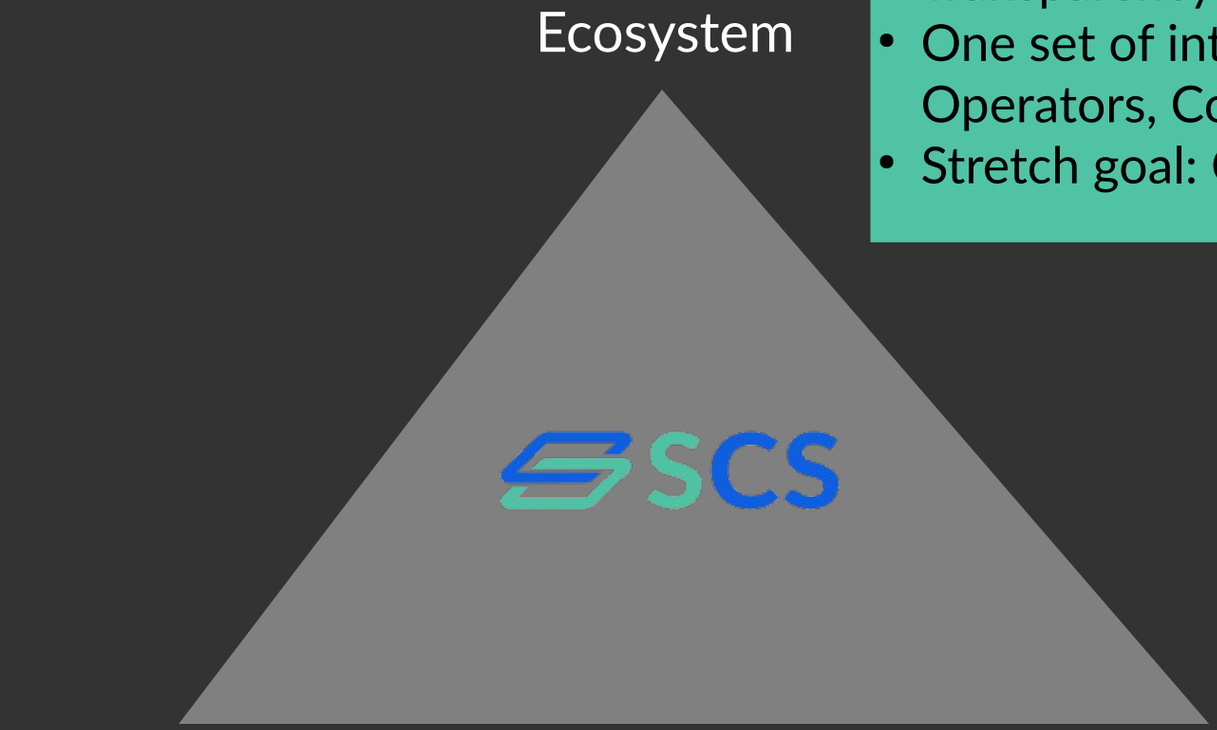


- Complete Stack: IaaS, KaaS, (PaaS)
- Including Ops: Lifecycle Mgmt, Infra, CI, Moni
- Including Feder-atable IAM
- Modular
- Open (4x)

- Strict standards: IaaS, k8s, k8s cluster mgmt Behavior (e.g. AZ definition), roles
- Ops standards (e.g. updating!)
- SLAs
- GAIA-X Self-Desc

SCS Deliverables

- CSPs: Share Ops Best Practices
- Transparency on Quality, RCAs
- One set of interfaces for ISVs, Operators, Consultants, ...
- Stretch goal: Cross-reselling



- Complete Stack: IaaS, KaaS, (PaaS)
- Including Ops: Lifecycle Mgmt, Infra, CI, Moni
- Including Federatable IAM
- Modular
- Open (4x)

- Strict standards: IaaS, k8s, k8s cluster mgmt Behavior (e.g. AZ definition), roles
- Ops standards (e.g. updating!)
- SLAs
- GAIA-X Self-Desc

Design Criteria (Vision)

Standardization

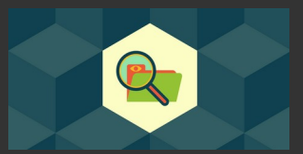
- Of the offered interfaces (compatibility for users) – combining existing standards w/ precision
- Operator – Focus: Configuration, Operations Tooling, Continuous Ops Processes
- Create scale advantages for all

Certification

- Verifiable Compatibility/Interoperability, Quality, Security

Transparency

- Completely Open Source Software, Open Community, Open Design and Development
- But also Configuration, Operational Processes and Operation Knowledge (new!)



Sustainability

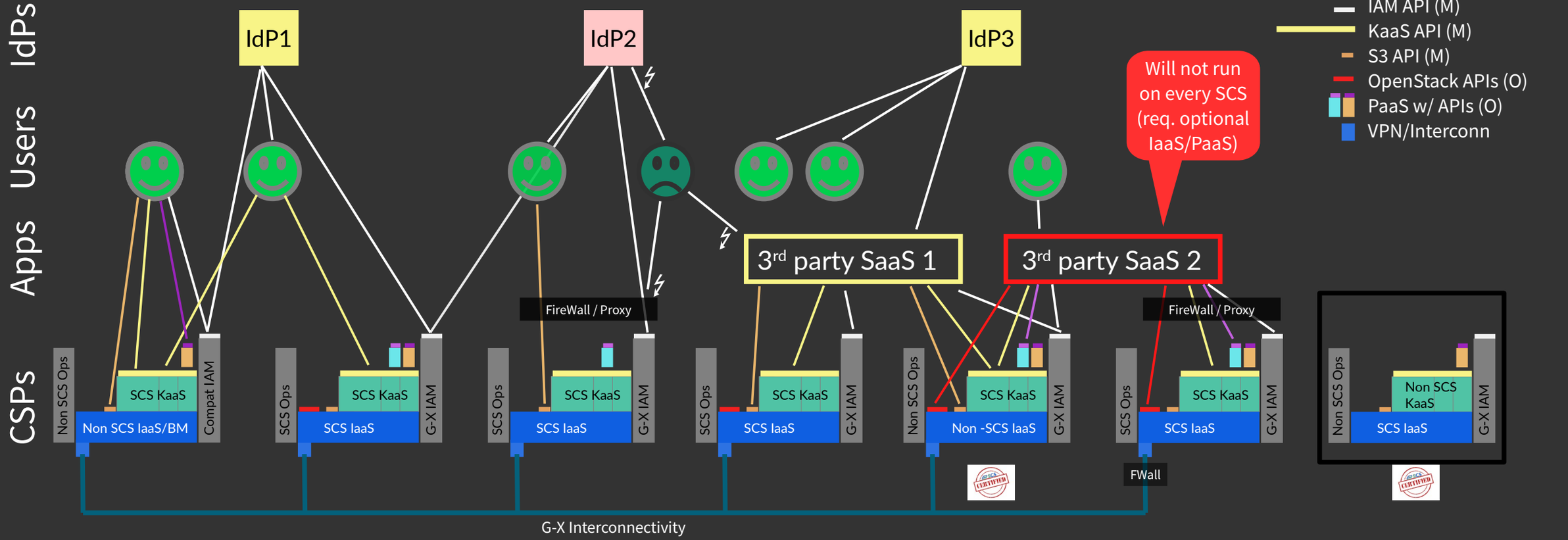
- Long-term existence of SCS
- Contribute back to existing upstream projects
- Efficient usage of resources

Federation

- Network of federated, compatible providers is better than monolithic structure
- Allows for specialization and differentiation

=> Relevance as <u>one</u> federated platform consisting of many providers

CSP ecosystem target (examples)



Prov1: (public)	Prov2: (public)	Prov3: (priv/comm)	Prov4: (public)	Prov5: (public)	Prov6: (priv/corp)	Prov7: (gov/mil)
Using preex IaaS or BM, not exposing IaaS, Non-Std Ops, Compat IAM Standard SCS KaaS, S3, PaaS 2	Standard SCS Ops, IaaS (exposed), IAM, KaaS, S3, PaaS 1+2	Extra protection (limit users/IdPs) Standard SCS Ops, IaaS (not exposed), IAM, KaaS, S3, PaaS 1	Standard SCS Ops, IaaS (exposed), IAM, KaaS, S3	Non-Standard Ops, IaaS (but certified & exposed as std) Standard SCS IAM, KaaS, S3, PaaS 1+2	Extra protection for Interconnect, limited federation Standard SCS Ops, IaaS (exp), IAM, KaaS, S3, PaaS 1+2	Air-Gap protected Own KaaS, but compatible (cert) Still using std SCS Ops, IaaS (not exp), IAM, S3, PaaS 2

SCS project status

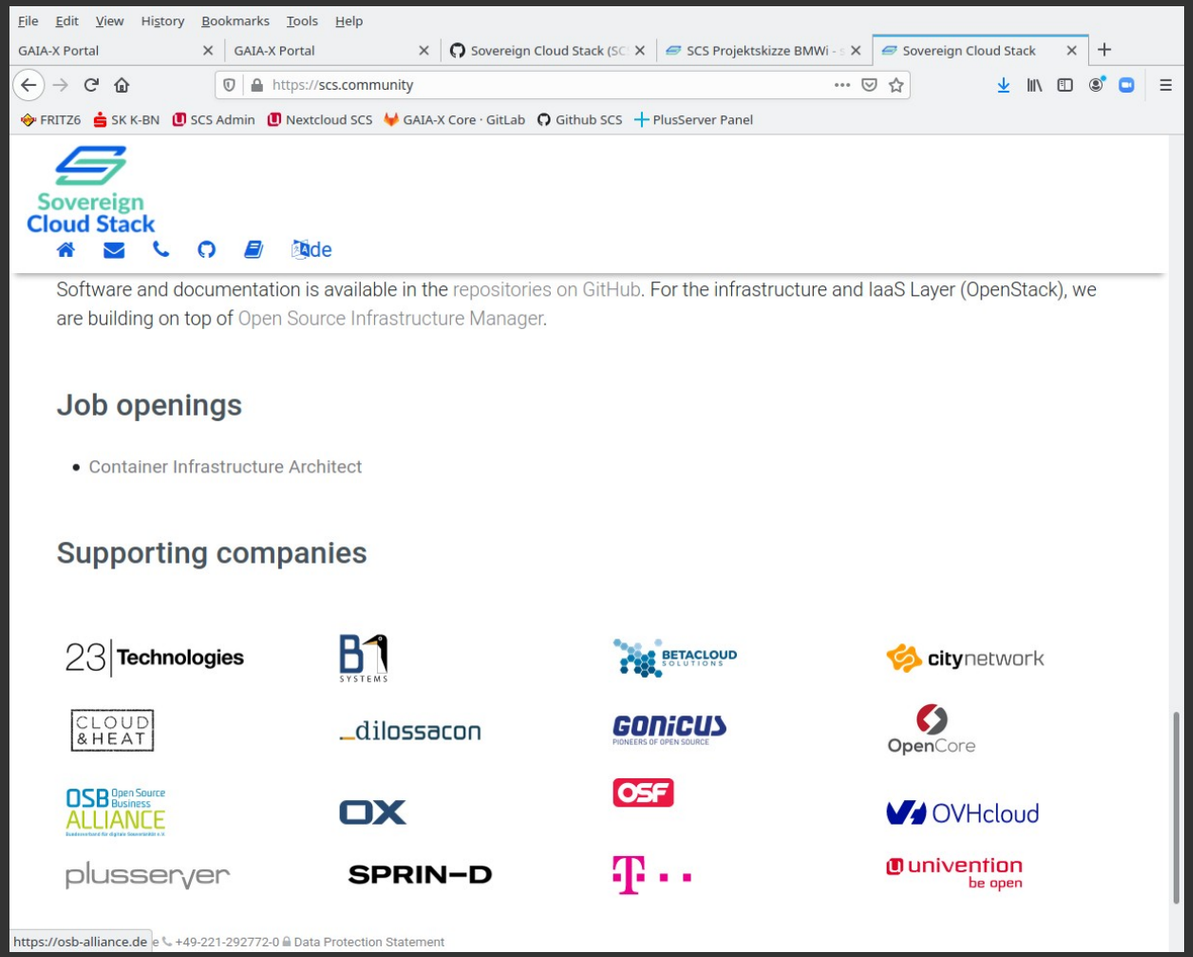
Small Project team operational

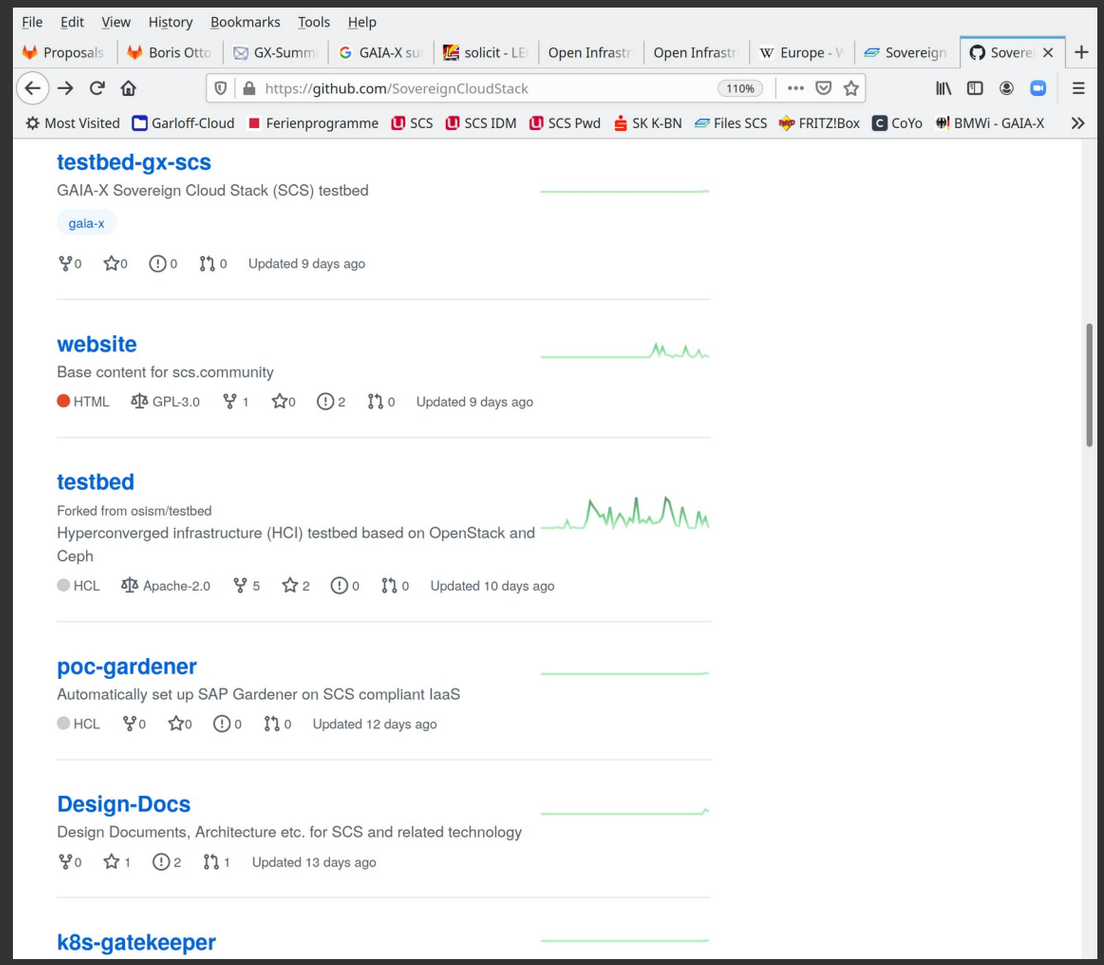
- Young project, current group came together first in Nov 2019
- Coordinating & orchestrating larger community, bringing IT departments and existing and new providers together
- Funded by SPRIN-D for 2020; funding proposal from OSBA for BMWi in finalization to fund central coordination work; allows contributing companies to build up business models; transfer central work to association/foundation later

Ecosystem

- Growing number of supporting & contributing partners (OSBA members plus companies from Sweden and France); Continuous SCS installations at 2 (physical) + 7 (virtual) providers
- Trademark, Logo, Web page, github SovereignCloudStack and OSISM
- Part of GAIA-X – SCS is Work Package of GAIA-X. Intense collaboration e.g. w/ IAM
  → Join the GAIA-X summit, Nov 19/20 (virtual event)
- Amazing feedback from many discussions, both industry and public sector
- Public coverage (SPRIN-D, c't, WDR, … see web page)
- Open for more contributions!

Webpage https://scs.community/ & github github/SovereignCloudStack





Growing community (2020-10)

Central team

- 3 people
- Will grow next year (OSBA project)
- Long-term vision: Association/Foundation

Main contributors:

- OSBA members: Univention, B1-Systems, Gonicus
- CSPs: PlusServer, CityNetwork, OVH, T-Systems, teuto.net
- GAIA-X: Cloud&Heat, GEC
- OSS projects: Stackable, Gardener, Kubermatic

Discussions:

- Industry: Daimler, Schwarz/StackIT, Trumpf, ...
- Public Sector: BMI, BWI, dataport, HiSolutions, ...
- Research Clouds: GWDG, CERN, StackHPC
- Vendors: RedHat, Ubuntu, Mirantis, Scality
- Organizations: Open Infrastructure Foundation, Dutch Cloud Infrastructure Coalition

SCS technical status (2020-10)

Infra + IaaS + Ops reference implementation pieces operational

- Includes Bare Metal install (MaaS), inventory (Netbox), zabbix, automated containerized install (using ansible) of Manager with Management tooling (ELK, Netdata, ARI, prometheus, skydive, patchman, DB, MsgQ, ...) and Hyperconverged Nodes (with KVM, encrypted ceph, OvS/OVN, core OpenStack plus octavia, barbican – vanilla kolla-ansible)
- Virtual deployment ("testbed") can be done on top of another IaaS using terraform – self-hosting (SCS testbed on SCS physical) works of course – ~60 – 90min deployment time.
- Virtual deployment useful for demos, CI testing (smoke-tests, refstack, API monitoring, more TBD ...), validating upgrades, exploration, ...
- Physical deployments on Bare Metal at two providers (Betacloud (prod), PlusServer)
- Virtual deployment tested on half a dozen providers (Betacloud, PlusServer, CityNetwork, OVH, teuto, OTC – with patches)
- Testbed for GAIA-X ID-Federation using keycloak as ID-Proxy
- Strong SCS standard definitions at IaaS layer (images, flavors, AZ meaning etc.) is WIP

Container layer in development:

- Working with SAP Gardener, kubermatic, Giantswarm, rancher (rke) – challenge is missing standardization for k8s cluster management – MVP planned for Q1/21,
  OpenStack k8s cluster API provider?

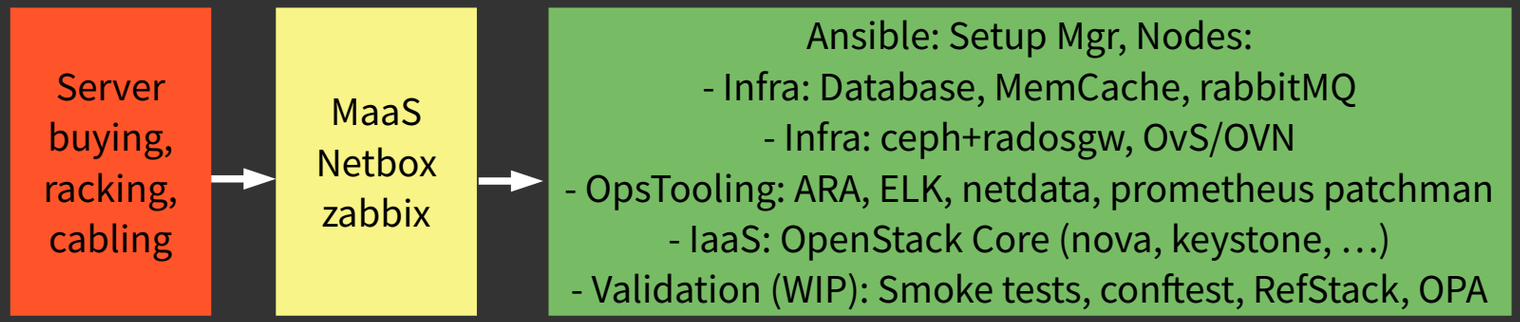
Using testbed framework also for automating other GAIA-X infra, e.g. IAM

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

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

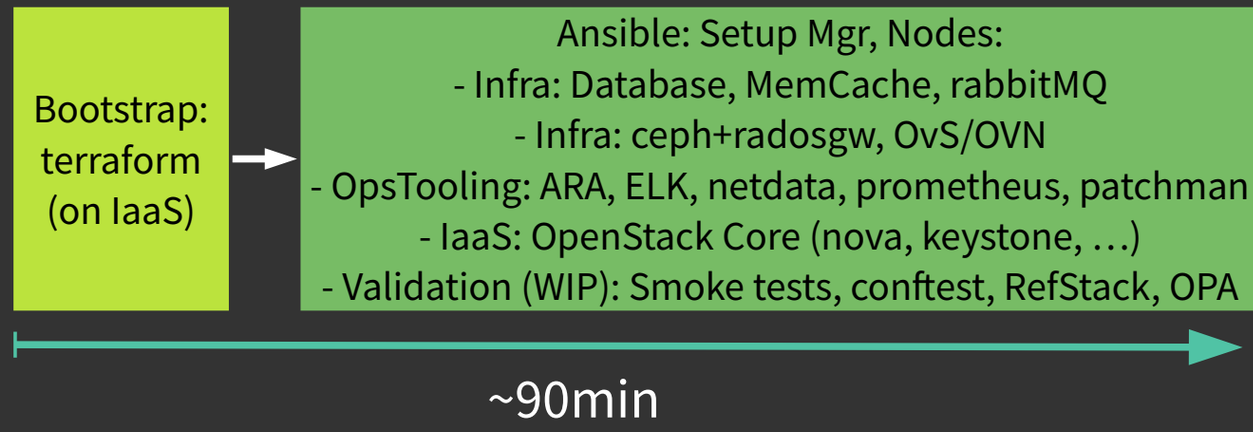
Physical deployment

Production („Live“)



Virtual (testbed) deployment

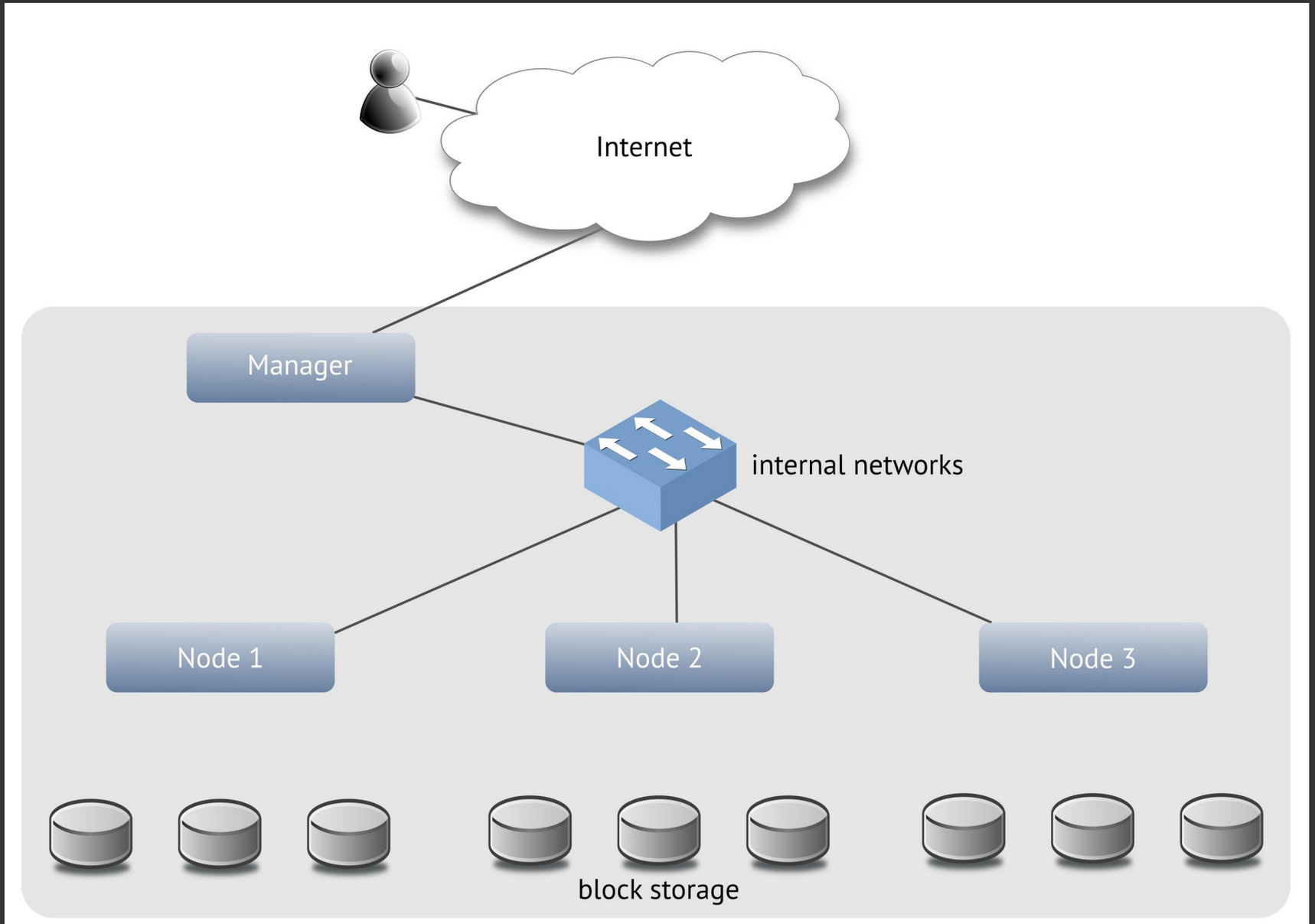
Dev, Testing / CI („Ref/Test“)
Demo, Explore, Debug, ...



https://github.com/OSISM https://docs.osism.de/ https://docs.osism.de/testbed/

https://github.com/OSISM/testbed https://github.com/SovereignCloudStack/testbed

Minimal testbed setup



Porting testbed to new cloud

Ensure command line access (openstack client tools) work, install sshuttle, terraform

Ensure sufficient quota (`openstack quota show`): min = 104GiB RAM, 28Cores, 90GiB Storage (+root volumes) on 9 vols, router, 6nets+subnets, 6SGs (50rules), 1FIP, 4 instances

Fill in configuration (`environment-xxx.tfvars`)

- Availability zone
- Flavors (manager, HCI nodes)
- Name of public net
- Image name (Ubuntu 18.04)

```
cloud_provider              = "ovh"
availability_zone           = "nova"
volume_availability_zone    = "nova"
network_availability_zone   = "nova"
flavor_node                 = "c2-15"
flavor_manager              = "s1-8"
image                       = "Ubuntu 18.04"
public                      = "Ext-Net"
volume_size_storage         = "10"
port_security_enabled       = null
~
```

Special work (OVH, OTC) as needed

```
make deploy-openstack watch \
  ENVIRONMENT=xxx
make sshuttle
```

Webinterfaces:

https://docs.osism.de/testbed/usage.html#webinterfaces

Port to terraform libvirt provider WIP

Testbed demo

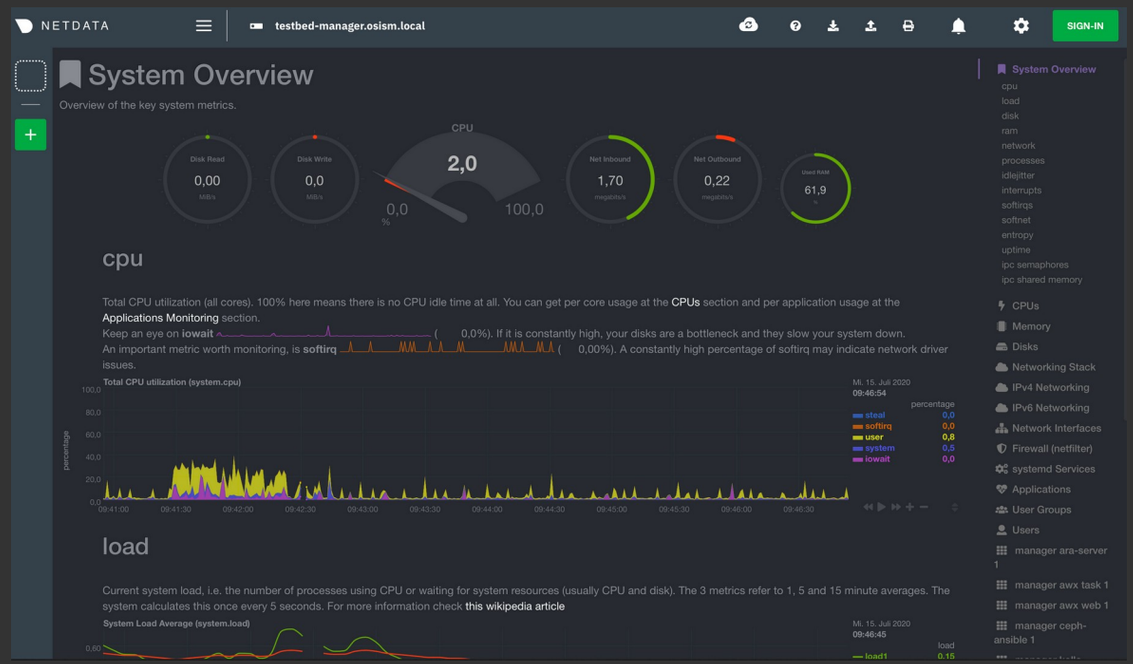
SCS base (OSISM) testbed running on Betacloud, PlusServer, CityCloud, OVH, OTC, C&H

Videos (testbed deployment)

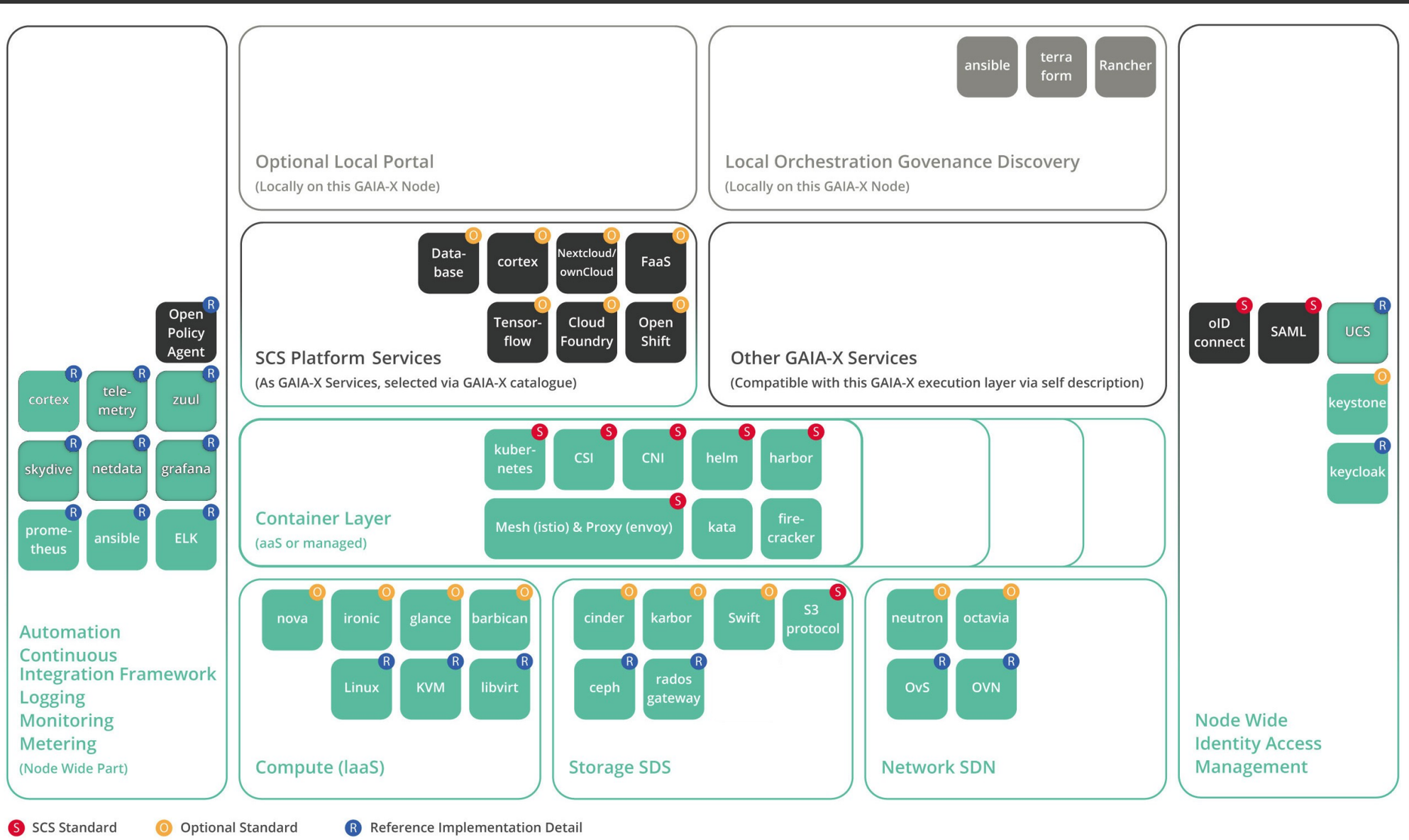
- Start Deployment (terraform, make deploy-openstack watch)
  https://asciinema.org/a/fCxgxV8a5bJMtubw8mBPdtozI
- Ceph & OpenStack deployment
  https://asciinema.org/a/E0dUtNlftLOLZRu6ajawi9lbo
  https://asciinema.org/a/FD90KLmSGp9IWT1jTF6S9yBJj

Web interfaces

- Ceph dashboard
- Cockpit
- netdata
- Skydive
- Patchman
- Kibana
- Horizon
- ...



Architecture (current status)



Roadmap

- Automate deployment for Infra, IaaS, OpsTools √
- Resolve k8s aaS automation std challenge (v1 until end of 2020)
- Strengthen CI (ongoing)
- Implement daily updates for production (v1 in 2020)
- Implement OPA policies (v1 in 2020)
- Document SCS certification requirements (1H 2021)
- Create plan for Security Certifications (BSI, TC, ISO, ...)
- Start implementing first PaaS services (DB, Big Data, ...) (1H2021)
- Cloud federation use cases (1H2021)
- Automation for SCS certification (2H2022)
- Monitoring driven mitigation – remediation workflows (v1 in 2H2021)
- Access to acceleration technologies (2H2021)
- SDN scalability work (1H2022)
- Cross-cloud orchestration & monitoring (1H2022)
- Utilization optimizations (2022)
- Developer toolchain (starting in 2021)
- Simplified stacks for special use cases (2022)
- AI supported operations (2023)

- WG/WorkPkg in GAIA-X √
- Code on github √
- Press / WebPage √
- GAIA-X AISBL incorp
- More virtual SCS deployments
- Leverage GAIA-X IAM and Network
- Funding

- Developer onboarding (ongoing)
- Productive use (IaaS)
- Sec Certification
- SCS foundation/association
- Productive use (KaaS)
- Partner ecosystem (support, training, ...)

- Ecosystem growth

- EPI collaboration?

SCS Summary

For data sovereignty, infrastructure and control over infrastructure matters.

Our response in GAIA-X and SCS is to build a network of providers of interoperable, federated services (not: one European hyperscaler).

SCS helps GAIA-X node providers to easily deliver modern interoperable, federated infrastructure.

SCS believes in certifiable standards, in (4x) openness and transparency, sustainability and federation.

It does so by defining certifiable standards, delivering a modular open source implementation and building a provider ecosystem in which we share the tools and best practices for operating it.

SCS status: Automated deployment for Infra, Ops Tools, IaaS in daily use (CI) and in production (Betacloud). K8s aaS not yet standardizable, automation available for Gardener, Kubermatic, Rancher.

Sovereign Cloud Stack

Join us!

Questions?

https://scs.community/
Contact: project@scs.sovereignit.de
scs@garloff.de

Sovereign Cloud Stack

Legal Remark:

SCS, Sovereign Cloud Stack are protected trademarks of OSB Alliance e.V.
The logo is protected as well.
Other trademarks are registered trademarks of their respective owners.
No warranty for the correctness of information provided in these slides can be taken. Use at your own risk.