

Sovereign Cloud Stack

Open Source Cloud & Container Stack for Gaia-X

Planning SCS for 2022

Dr. Manuela Urban, Dirk Loßack, Eduard Itrich, Kurt Garloff (OSB Alliance e.V.)
Christian Berendt, Felix Kronlage-Dammers, John Garbutt,
Mathias Fechner, Tim Beermann, Arvid Requate, Jonas Schäfer

project@scs.sovereignit.de

2021-12-15

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Topics for 2022

Gaining traction & visibility / reach

– growing the # partners (adoption) and community

- Public admin clouds (DE)
- Industry partners (EU - IPCEI)
- Public cloud partners (EU – IPCEI)
- Other allies

Scaling the development model

- Growing the community 2x-3x: What now?

Gaia-X

IPCEI-CIS

- Neutral ground for EU players (together with Eclipse)

Topics for 2022 – technical: R2+R3

Open Ops – start delivering on vision

- Really sharing best practices, RCAs, solved issues
- Metering
- Logging/Monitoring
- More Automation (where exactly?)

IaaS / Infra

- Disk encryption, overcome networking trouble
- Bare Metal provisioning

Container Platform

- Seek collaboration with container platform managers (Gardener, Rancher, ...) with SCS common ground

IAM

- Demo federating two/three SCS clouds (operator perspective / user perspective)
- Logout

Other

- Own infrastructure (Lab)
- CI
- Security work: Pentesting, Security Response, Network encryption, “Confidential Computing“
- SBOM / SPDX
- Standardization / certification

SCS roadmap

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

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



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
- Possibly Release 1.1? (2021-11): Release 1 with k8s-capi v1beta1
- Release 2: (2022-03-1x)
 - More Container work (cluster API, k8s, registry, multi-AZ/multi-cloud, rolling upgrades in prod)
 - Ops Stack: More preconfigured Metering, Monitoring, Logging, Alerting
 - Federation: Cross-Layer (IaaS / KaaS) user management (optional!),
 - More Bare Metal automation
 - Extend CI coverage
 - Disk Encryption
- Half-yearly releases (3/22, 9/22, 3/23, 9/23, 3/24, 9/24):
 - Multi-region setups, Security scanning, Security Certifications, CI coverage (for daily updates!), Compliance test coverage (automated certification), SSI/DID federation, X-Cloud Orchestration, Service Mesh, ...



SCS Roadmap (non-technical)

Growing the team & community

- Public funding (BMWi) since 7/'21
- 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

Ecosystem

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

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



SCS R1 retro – Dirk driving the process

Good and open discussion, great input

KALM methodology: Keep, Add, Less, More (on wekan)

- Dirk working through the doc ...

Preliminary Results 1: Short term improvements

- Use wekan
- Status update in Kanban board AHEAD of sprint review
- Spend more energy on breaking down Epics into digestable User Stories (typically fitting into one sprint)
- Workshop on Container use cases and strategy needed
- Set up tech leadership („PO“) meeting to prepare sprint planning

Preliminary Results 2: More investigation and discussion needed

- Two week – sprints with one intermediate whole-team touchpoint („Daily“) ?
- Increase clarity on people availability
- Split Thu team call into unidirectional (could be skipped / read / recorded) and bidirectional piece ?
- Define meaning and expectations on SIGs
- CoC
- Review dashboard
- More testing (CI) and documentation and release note writing



SCS Roadmap: R2 goals (tentative)

Release 2: 2022-03-1x

- **IaaS (→ team 1) Christian / Mathias / (John)**
 - Continue Bare Metal automation & documentation
 - e.g. vBMC in testbed
 - Image Manager: Split code&config
 - Discussion: Define / Build own SCS images? (Upstream from distro, Upstream with post-config, Self-built: Full automation req. (d-i-b/kiwi) and transparency required)
 - Disk encryption (User data, root disks, images, ... optionally with user-managed keys - HSM?)
 - Networking: Troubleshooting, prepare optional encryption
 - Deployment automation: Compare with yaook and find common building blocks (kolla images, ...) and standards
- **Containers aaS: kubernetes cluster API (→ team 2) John / (Kurt) / (GiantSwarm)**
 - Update to k8s-capi beta1 (v1.0.0) once the capi-provider-openstack is out (→ SCS R1.1 ?), adjust helm charts (Matt?)
 - Update to k8s-1.22 (→ R1.1 ?), k8s-latest, latest kind
 - K8s SCS integration strategy → (see box)
 - Optionally connect k8s user management to IaaS IAM (keycloak) – team 2+3
 - Harbor: update, install with SCS, expose scanning capabilities
 - Cilium as (preferred?) CNI option
 - Alternative ingress controllers? (alternatives to NGINX)
 - Envoy (with Contour ingress?)
 - Istio
 - Integrate building blocks from Joshua ...

Workshop on k8s strategy needed: (2021-11-15, 16:00 – 18:00 CET)

as self-service (multi-tenant provider?), as CaaS, as managed KaaS:

Not multi-tenant, weak on day 2 management, not good enough (Lacks HA/backup, update plan, ...)

CAPI is a good standard, but alone not very useful, need tooling around (→ talk to GiantSwarm, kubermatic, gardener, rancher?, ...) => TO DO: Build dialogue, exchange, and community

Scaling to smaller environments (R1: Match minimal reasonable full-SCS deployment – but with vision to have compatible APIs, ideally sharing most technology, in even smaller environments)

Internal use (monitoring for Ops)

SCS Roadmap: R2 goals (tentative)

Release 2: 2022-03-1x

- **IAM: (→ team 3) ARVID**
 - Federation (status: preparing: openldap merged, keycloak integrated, laaS federation is proceeding nicely, ...)
 - HA, test with several providers
 - Logout also needs to work :-) (=> noris)
 - Continue keycloak vs zitadel vs ... discussion
 - Continue SSI/DID investigation
 - SAML?
 - Continue: Management Web interfaces from OSISM should be linked to user/role management (→ reverse proxy?)
- **Monitoring/Logging: (→ team 3) FELIX**
 - Finish integration of preconfigured monitoring & logging blueprints
 - Roles (SIG)
 - OS-health-monitor => redevelop in tempest/rally/... (=> with OTC?)
 - Metrics collection framework (with demoable rating but APIs for real billing integration), user metrics dashboard? **JONAS**
- **CI: (→ team 3/1) TIM?**
 - Use Zuul CI everywhere in SCS
 - Provide for providers
- **Standards: (→ all teams) MATHIAS ?**
 - Ensure we implement what we standardize!
 - Definition of regions and availability zones
 - What's shared? (Identities, images, object storage, networks, block storage)
 - Require AZs to have significant failure independence ... (Meaningful subset of separate switches, power, fire protection zone, internet, ...?)
 - Require Regions to have low latency connections (<2ms?)
 - K8s standards
 - Standards compliance tests (as part of CI)

Hackathon #2 (Dec 2/3)

Support use case streams again with container clusters

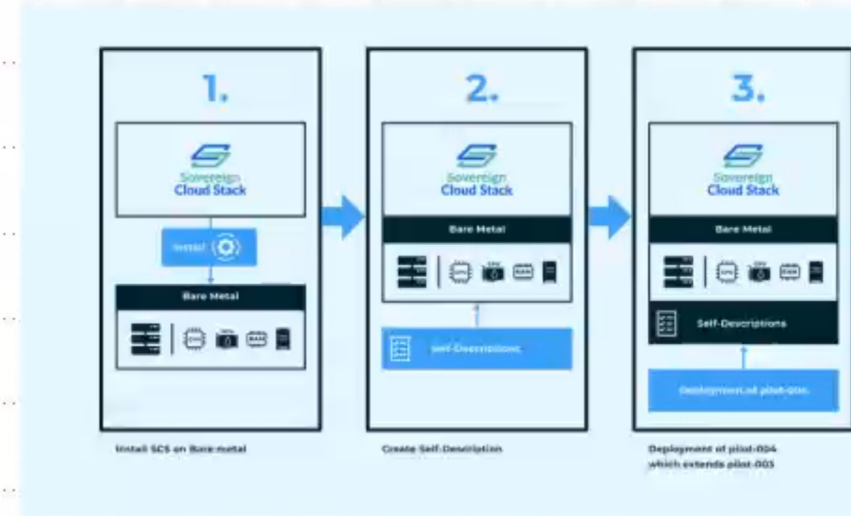
- Pluscloud supporting with gx-scs again
- Others?

Own Workstream: SCS install demo and bare metal install with partners

- Request for participants running ... (thanks for HW specs, Tim!)
- Position as THE platform for hackathon participants by Marius :-)
- DNation (stream#1) playing with capi ...

=> Learnings?

02 SCS session



Scenario: ACME would like to set up a Gaia-X compliant Cloud infrastructure and host applications

- Proposal for Hackathon #3:
- Publishing the Self-description to the Catalogue and querying for it
 - Onboarding of ACME as a Gaia-X provider

MVG/Piloting call

21/10/21