Sovereign Cloud Stack

An OSB ALLIANCE project

https://scs.community

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

gaia-x

SCS Summit 2024
2024-05-14

Sovereign Cloud Stack as integrated turnkey solution

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 @ OSB Alliance e.V.)

Sovereign Cloud Stack

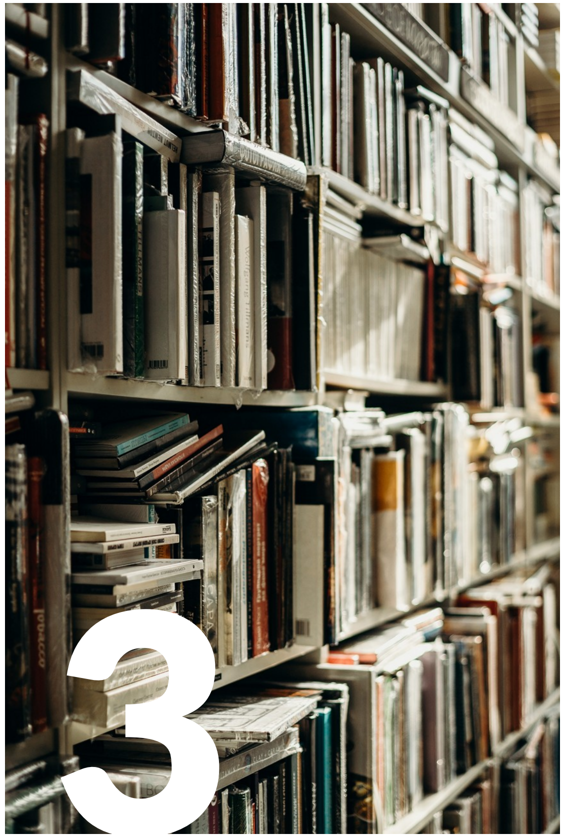
One platform - standardized, built and operated by many.

gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Sovereign Cloud Stack Deliverables

Certifiable Standards

Modular Open Source
Reference Implementation

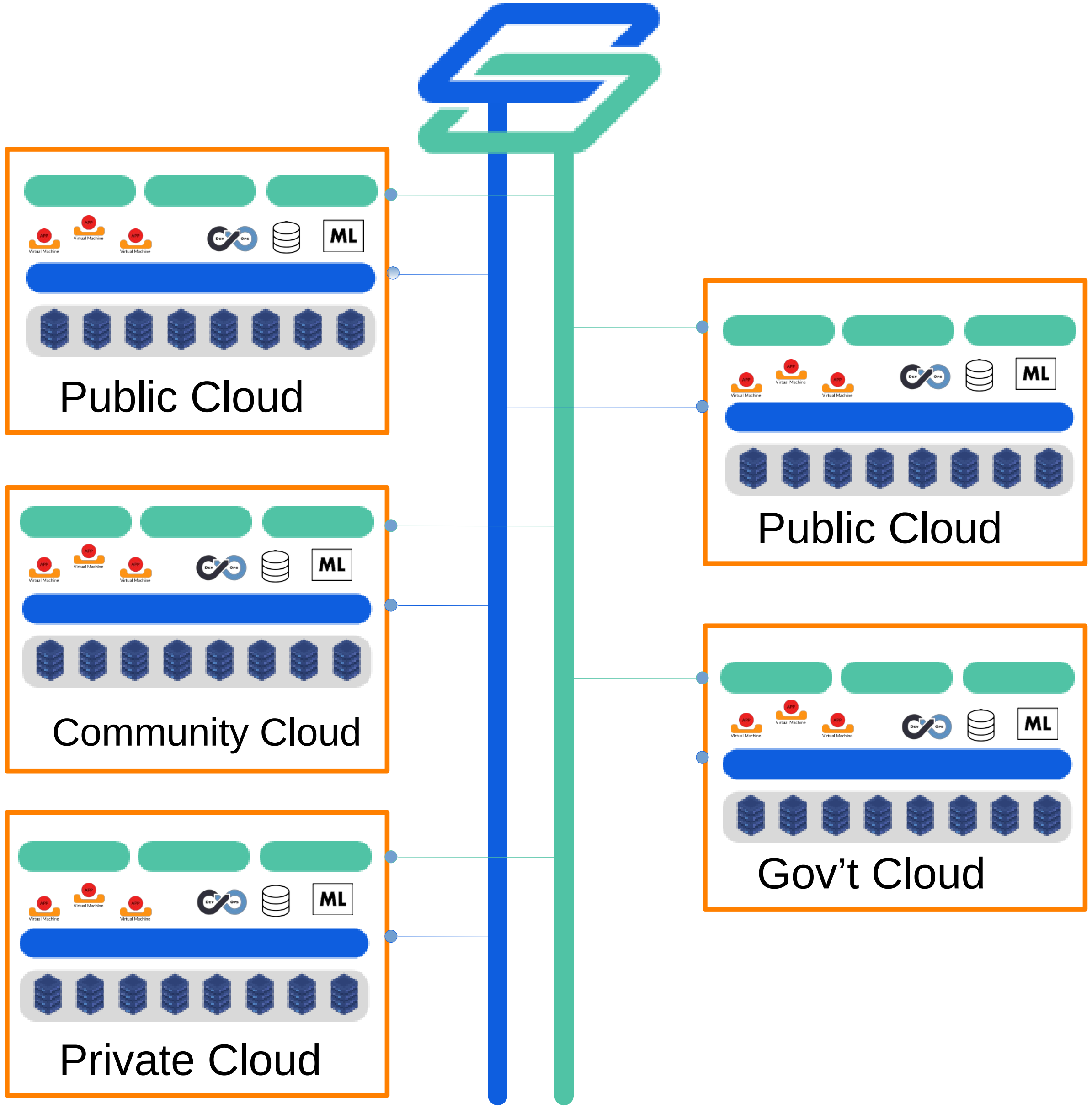


Operational Knowledge

gaia-x

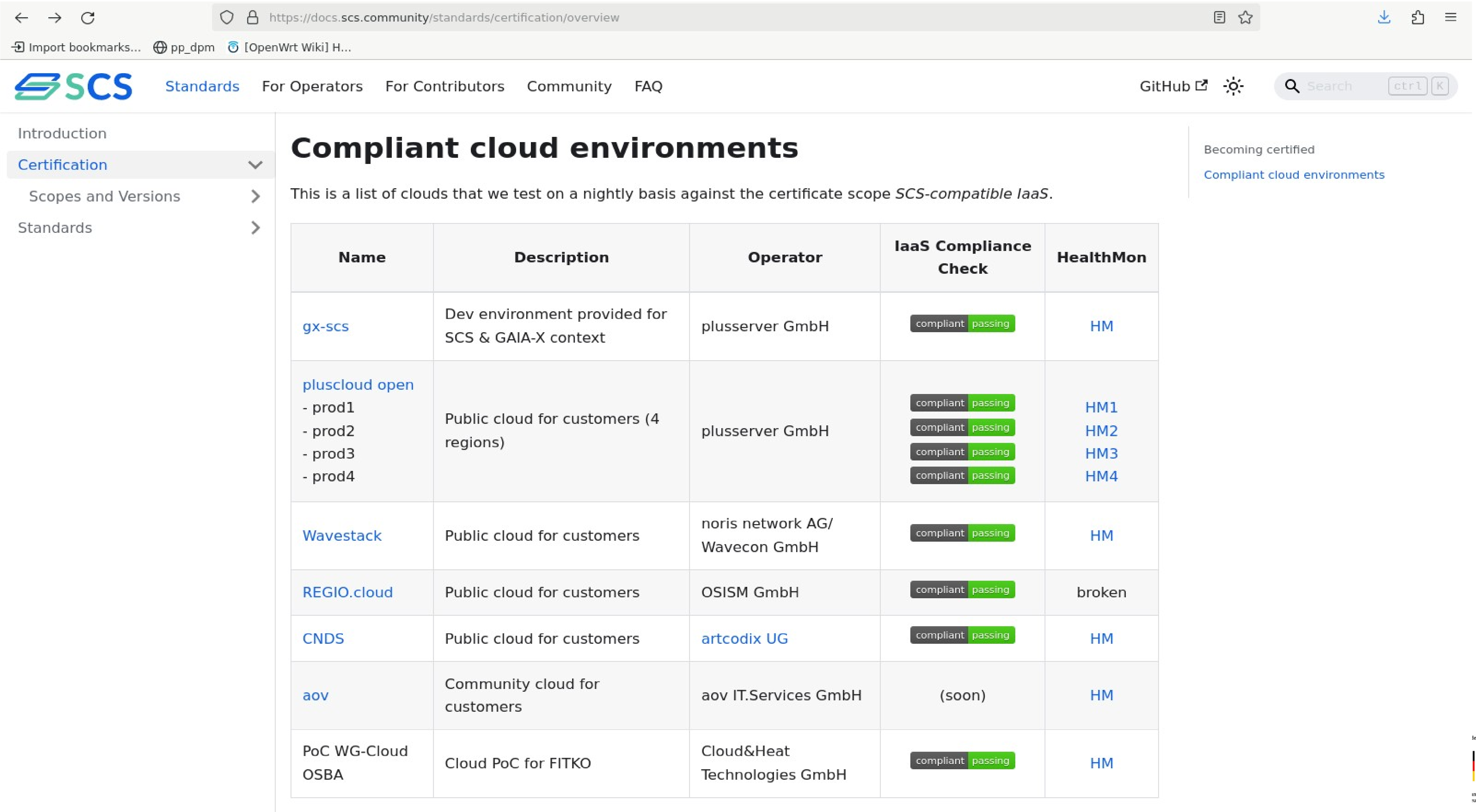
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

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

Existing public providers



Compliant cloud environments

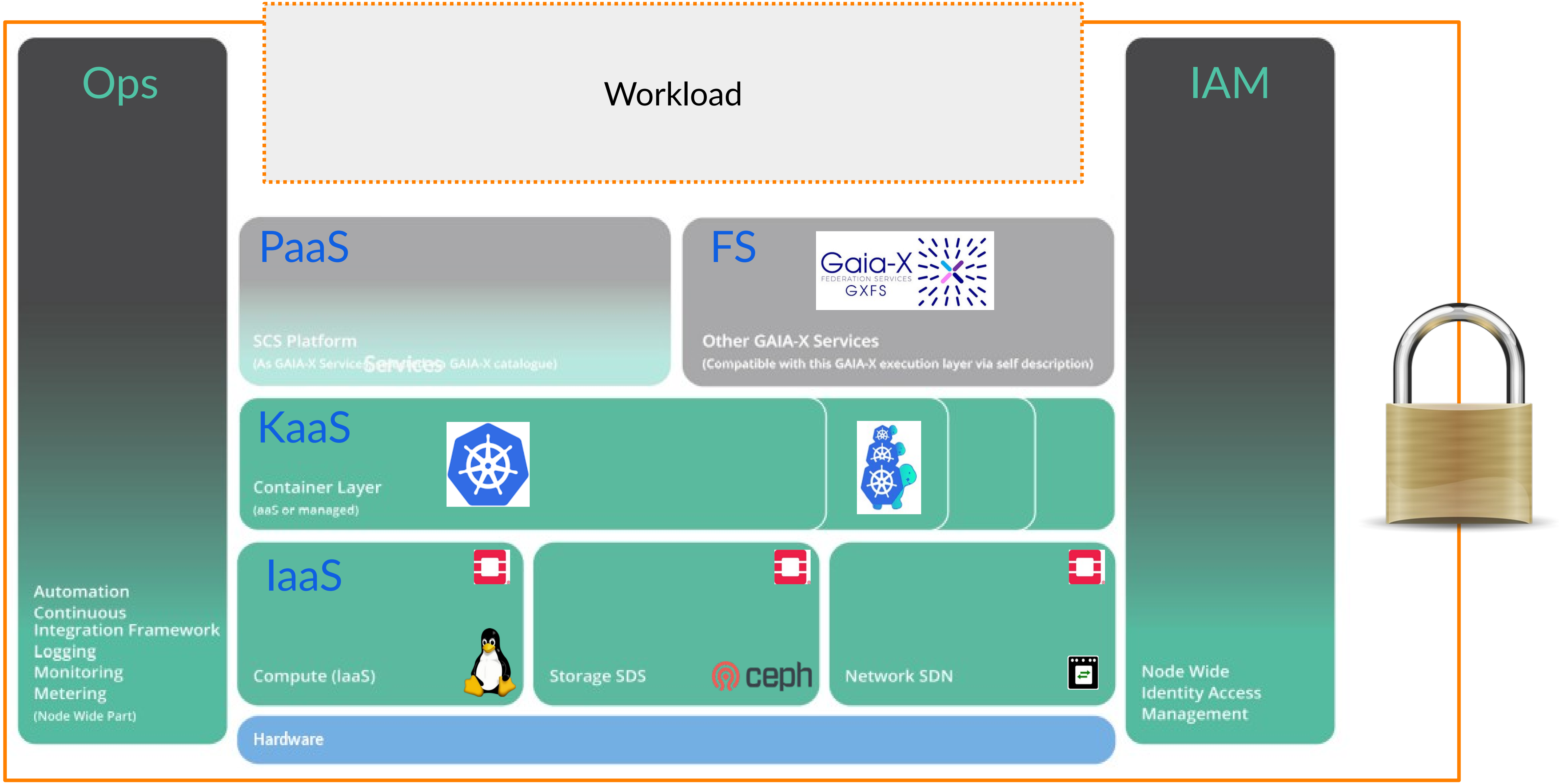
This is a list of clouds that we test on a nightly basis against the certificate scope *SCS-compatible IaaS*.

Name	Description	Operator	IaaS Compliance Check	HealthMon
gx-scs	Dev environment provided for SCS & GAIA-X context	plusserver GmbH	compliant passing	HM
pluscloud open - prod1 - prod2 - prod3 - prod4	Public cloud for customers (4 regions)	plusserver GmbH	compliant passing compliant passing compliant passing compliant passing	HM1 HM2 HM3 HM4
Wavestack	Public cloud for customers	noris network AG/ Wavecon GmbH	compliant passing	HM
REGIO.cloud	Public cloud for customers	OSISM GmbH	compliant passing	broken
CNDS	Public cloud for customers	artcodix UG	compliant passing	HM
aov	Community cloud for customers	aov IT.Services GmbH	(soon)	HM
PoC WG-Cloud OSBA	Cloud PoC for FITKO	Cloud&Heat Technologies GmbH	compliant passing	HM

dert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
und eines Beschlusses
eutschen Bundestages

SCS Architecture (Software/Ref.Impl.)

building it up from the ground



Workload

Ops

Automation
Continuous
Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

PaaS

SCS Platform
(As GAIA-X Service Services GAIA-X catalogue)

FS

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

KaaS

Container Layer
(aaS or managed)

IaaS

Compute (IaaS)

Storage SDS

Network SDN

Hardware

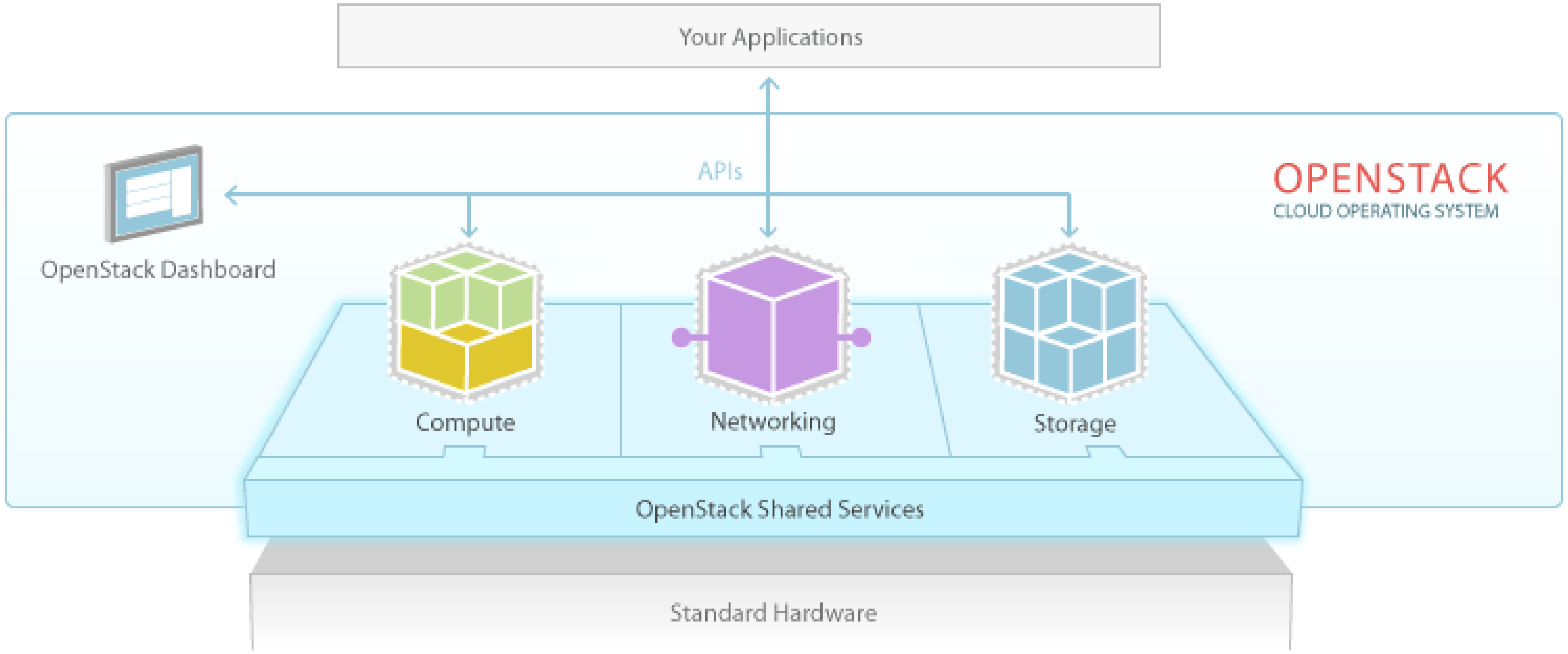
IAM

Node Wide
Identity Access
Management

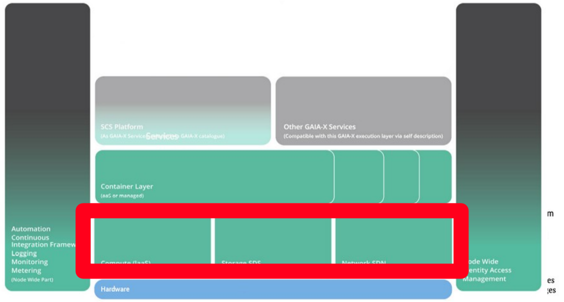
SCS Platform Services (PaaS) are planned
Hardware and Federation Services not part of SCS software
KaaS = Kubernetes as a Service

gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Virtualization & IaaS



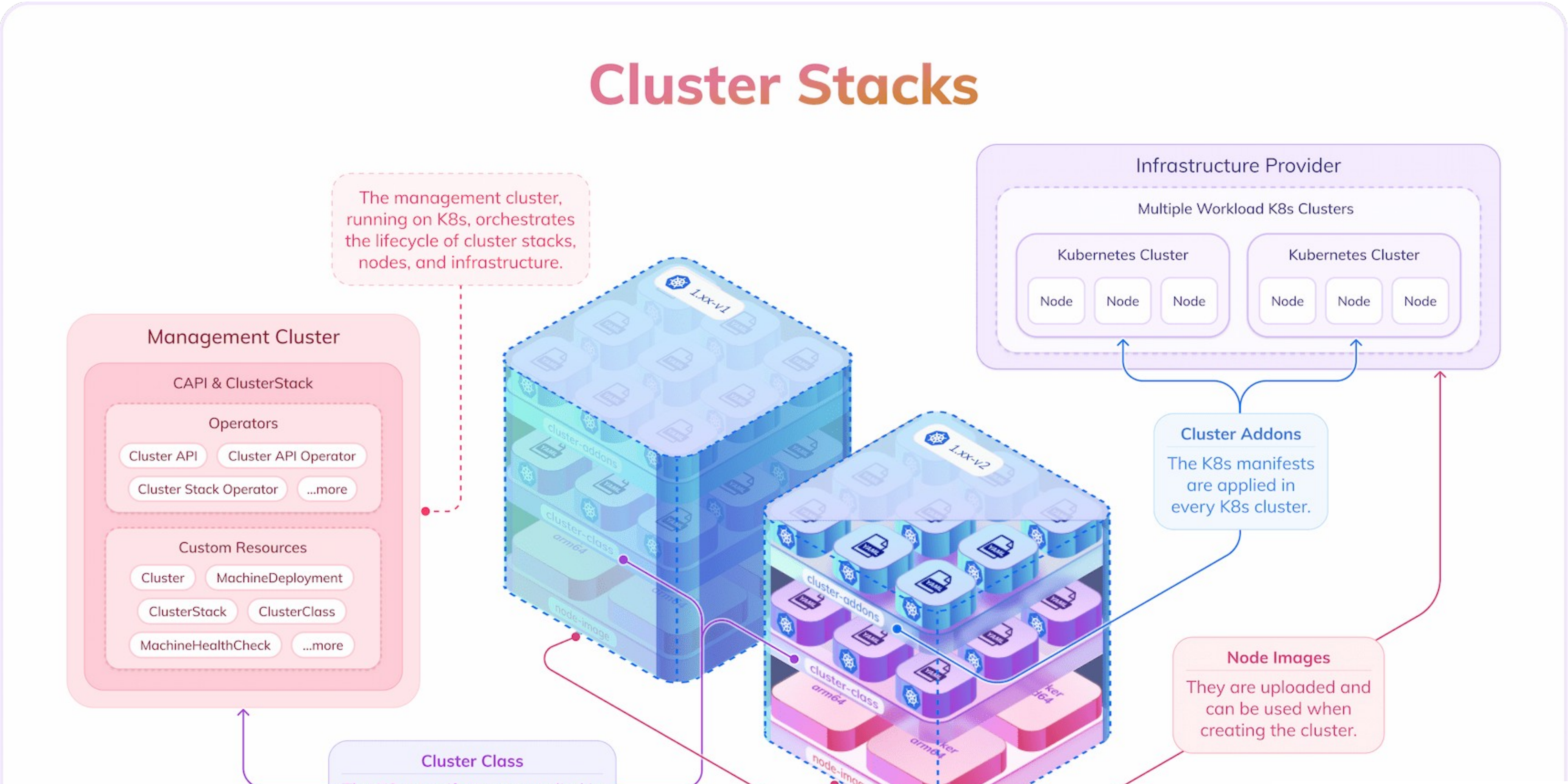
- Compute Virtualization: KVM (Linux)
- Storage SDS: ceph (incl. rados GW) – ceph-ansible / ceph-rook
- Network SDN: OvS + OVN
- … orchestrated via OpenStack core services & APIs (deployed containerized with OSISM / kolla-ansible)



Sovereign Cloud Stack

An OSB ALLIANCE project

Container layer



Cluster Stacks

The management cluster, running on K8s, orchestrates the lifecycle of cluster stacks, nodes, and infrastructure.

Management Cluster

CAPI & ClusterStack

Operators

Cluster API | Cluster API Operator | Cluster Stack Operator | ...more

Custom Resources

Cluster | MachineDeployment | ClusterStack | ClusterClass | MachineHealthCheck | ...more

Infrastructure Provider

Multiple Workload K8s Clusters

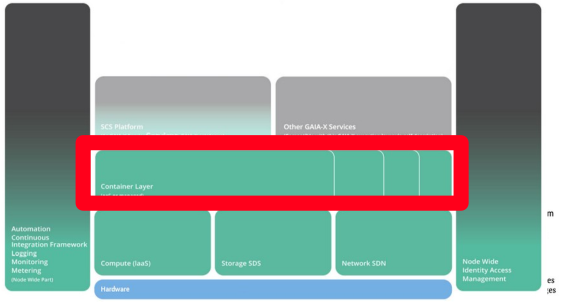
Kubernetes Cluster: Node | Node | Node

Kubernetes Cluster: Node | Node | Node

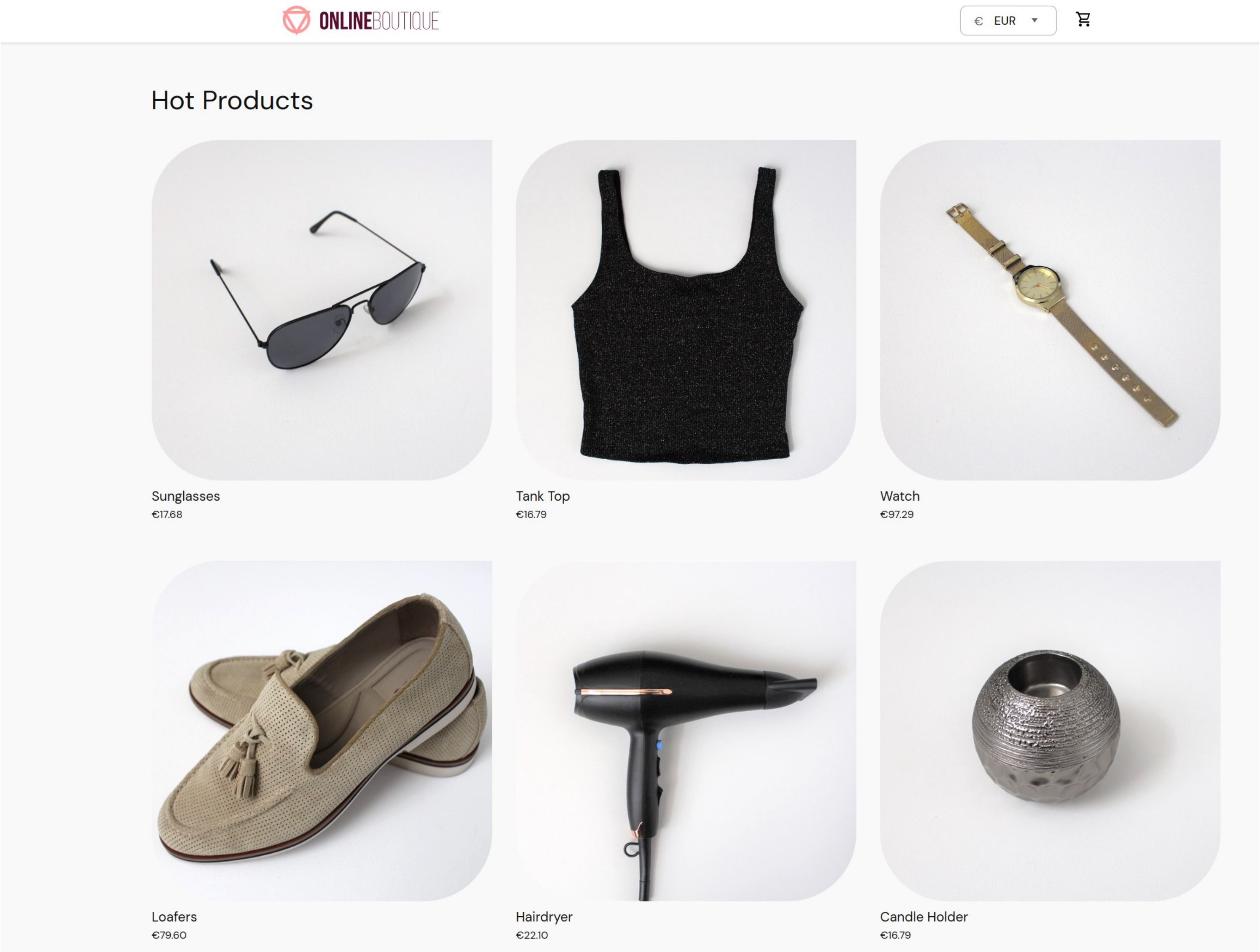
Cluster Addons
The K8s manifests are applied in every K8s cluster.

Node Images
They are uploaded and can be used when creating the cluster.

Cluster Class
The K8s manifests are applied in the management cluster once.



Example application: An e-commerce application



Hot Products

Sunglasses
€17.68

Tank Top
€16.79

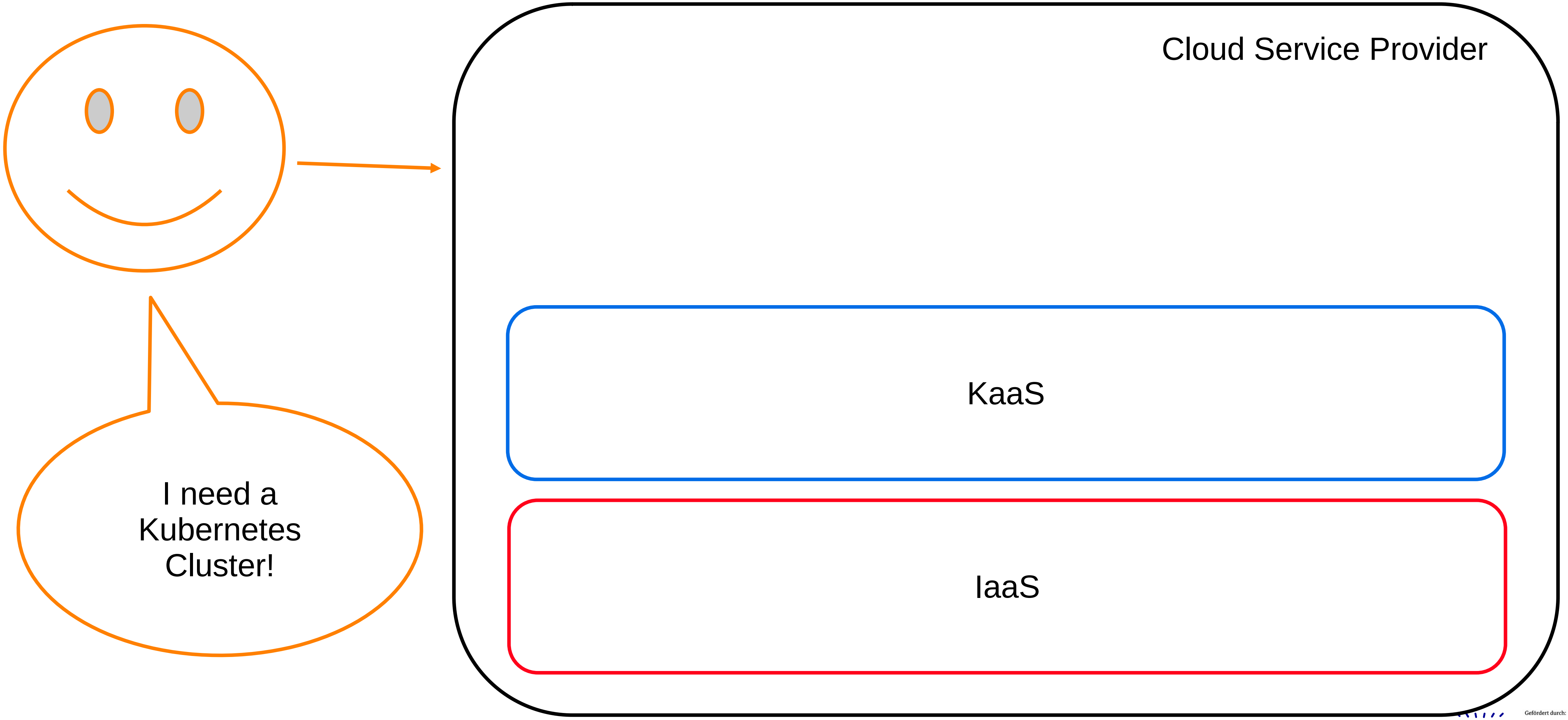
Watch
€97.29

Loafers
€79.60

Hairdryer
€22.10

Candle Holder
€16.79

gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages



I need a Kubernetes Cluster!

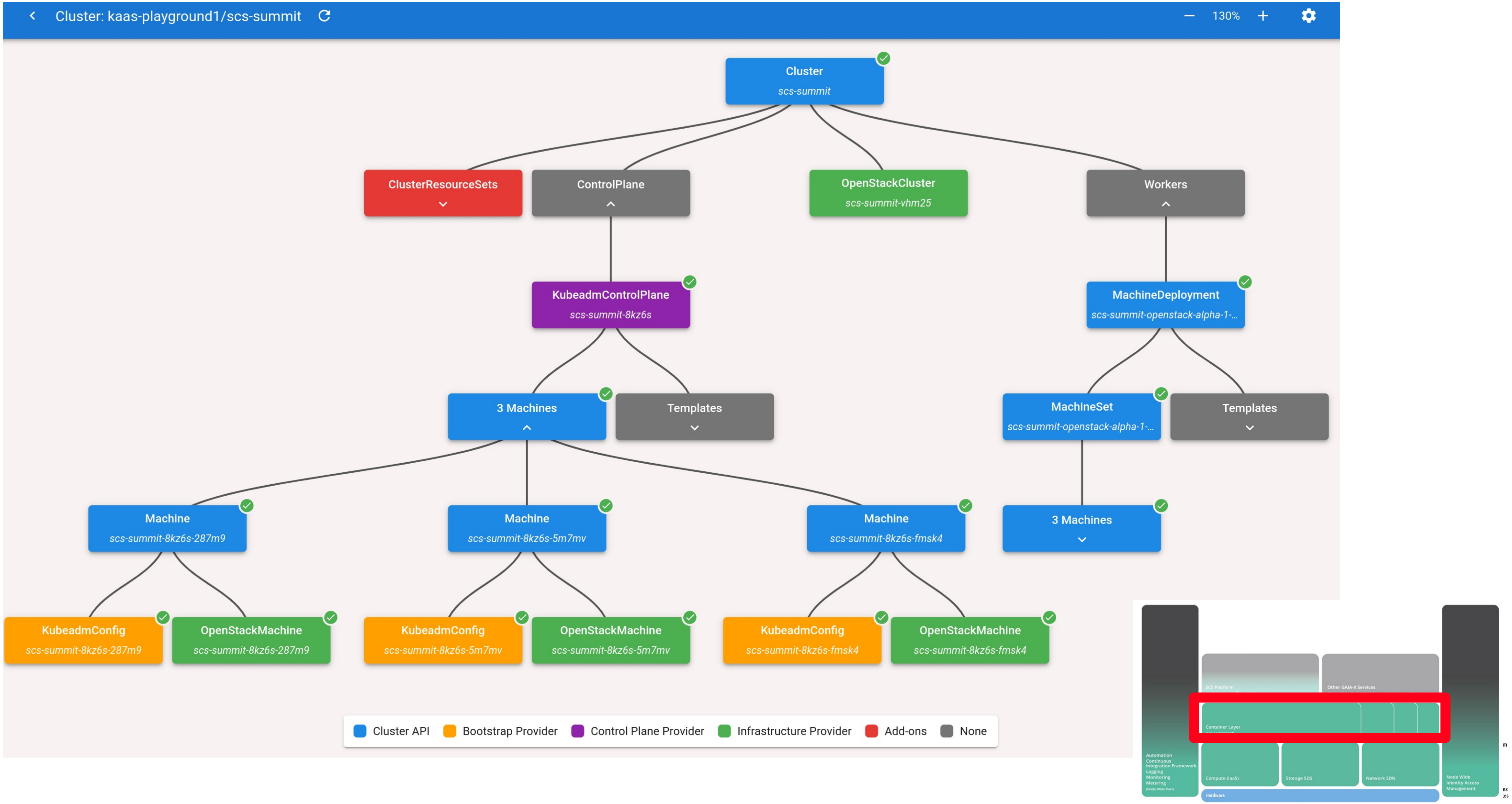
Cloud Service Provider

KaaS

IaaS

gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Cluster in detail



Cluster: kaas-playground1/scs-summit

130%

Cluster
scs-summit

ClusterResourceSets

ControlPlane

OpenStackCluster
scs-summit-vhm25

Workers

KubeadmControlPlane
scs-summit-8kz6s

MachineDeployment
scs-summit-openstack-alpha-1-...

3 Machines

Templates

MachineSet
scs-summit-openstack-alpha-1-...

Templates

Machine
scs-summit-8kz6s-287m9

Machine
scs-summit-8kz6s-5m7mv

Machine
scs-summit-8kz6s-fmsk4

3 Machines

KubeadmConfig
scs-summit-8kz6s-287m9

OpenStackMachine
scs-summit-8kz6s-287m9

KubeadmConfig
scs-summit-8kz6s-5m7mv

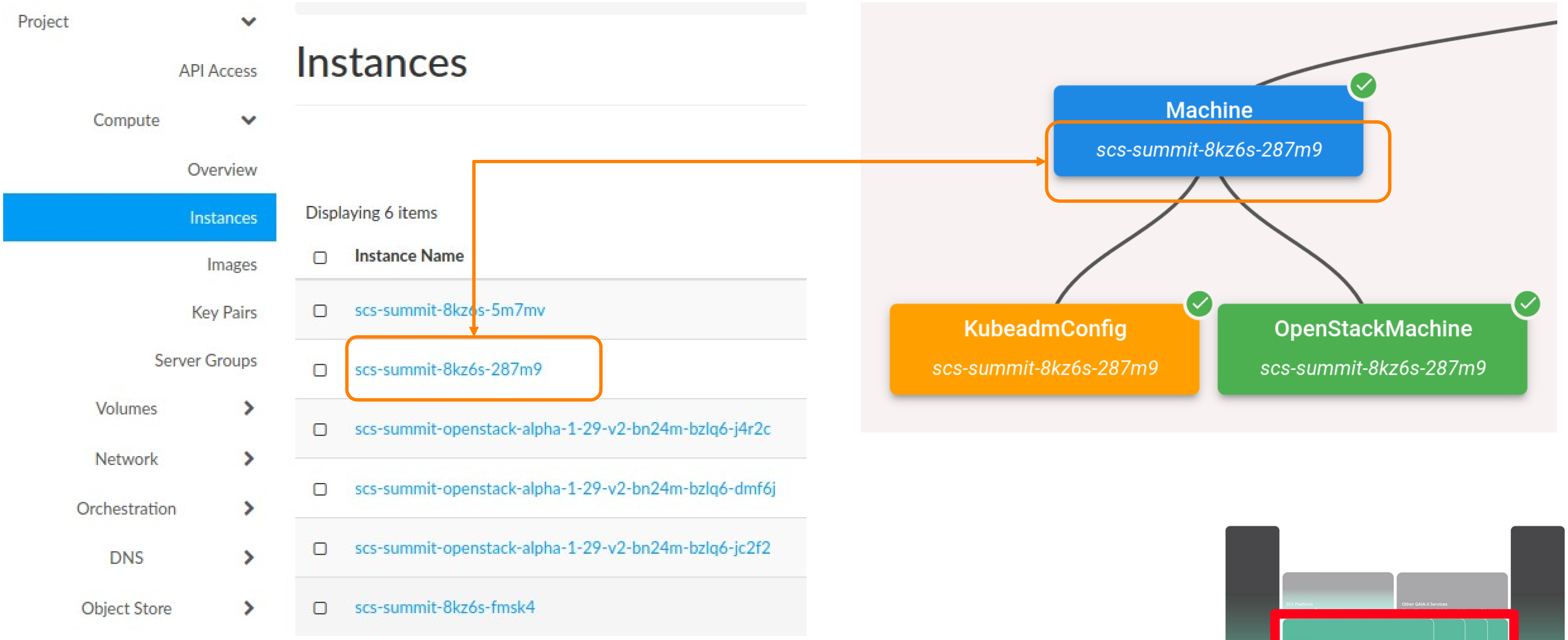
OpenStackMachine
scs-summit-8kz6s-5m7mv

KubeadmConfig
scs-summit-8kz6s-fmsk4

OpenStackMachine
scs-summit-8kz6s-fmsk4

🟦 Cluster API 🟧 Bootstrap Provider 🟪 Control Plane Provider 🟩 Infrastructure Provider 🟥 Add-ons ⬛ None

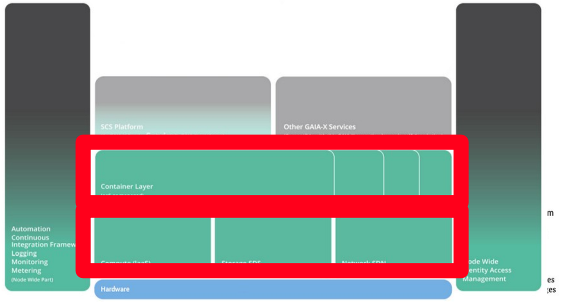
Kubernetes Node as Openstack Instance



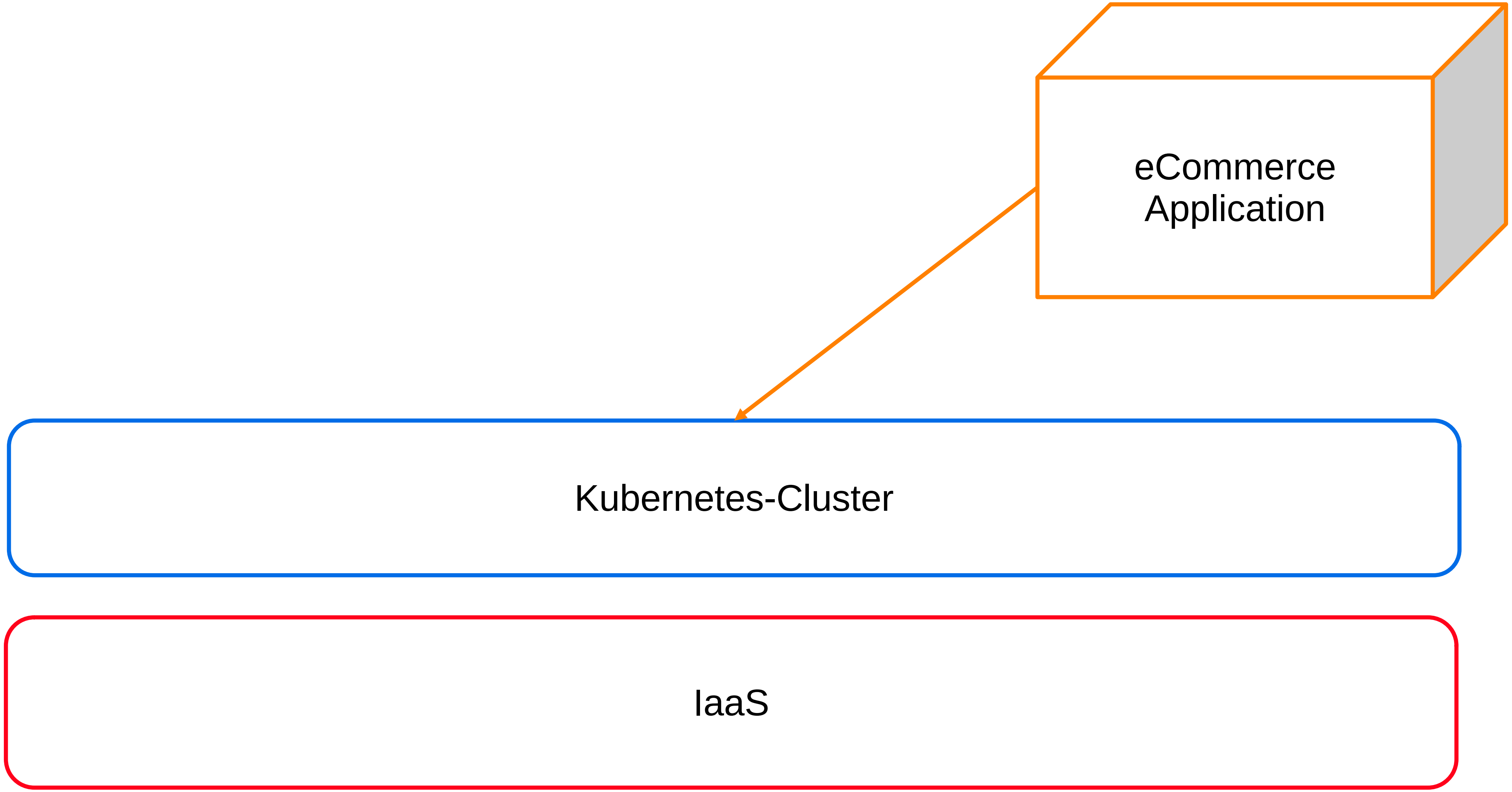
Instances

Displaying 6 items

□	Instance Name
□	scs-summit-8kz6s-5m7mv
□	scs-summit-8kz6s-287m9
□	scs-summit-openstack-alpha-1-29-v2-bn24m-bzlq6-j4r2c
□	scs-summit-openstack-alpha-1-29-v2-bn24m-bzlq6-dmf6j
□	scs-summit-openstack-alpha-1-29-v2-bn24m-bzlq6-jc2f2
□	scs-summit-8kz6s-fmsk4

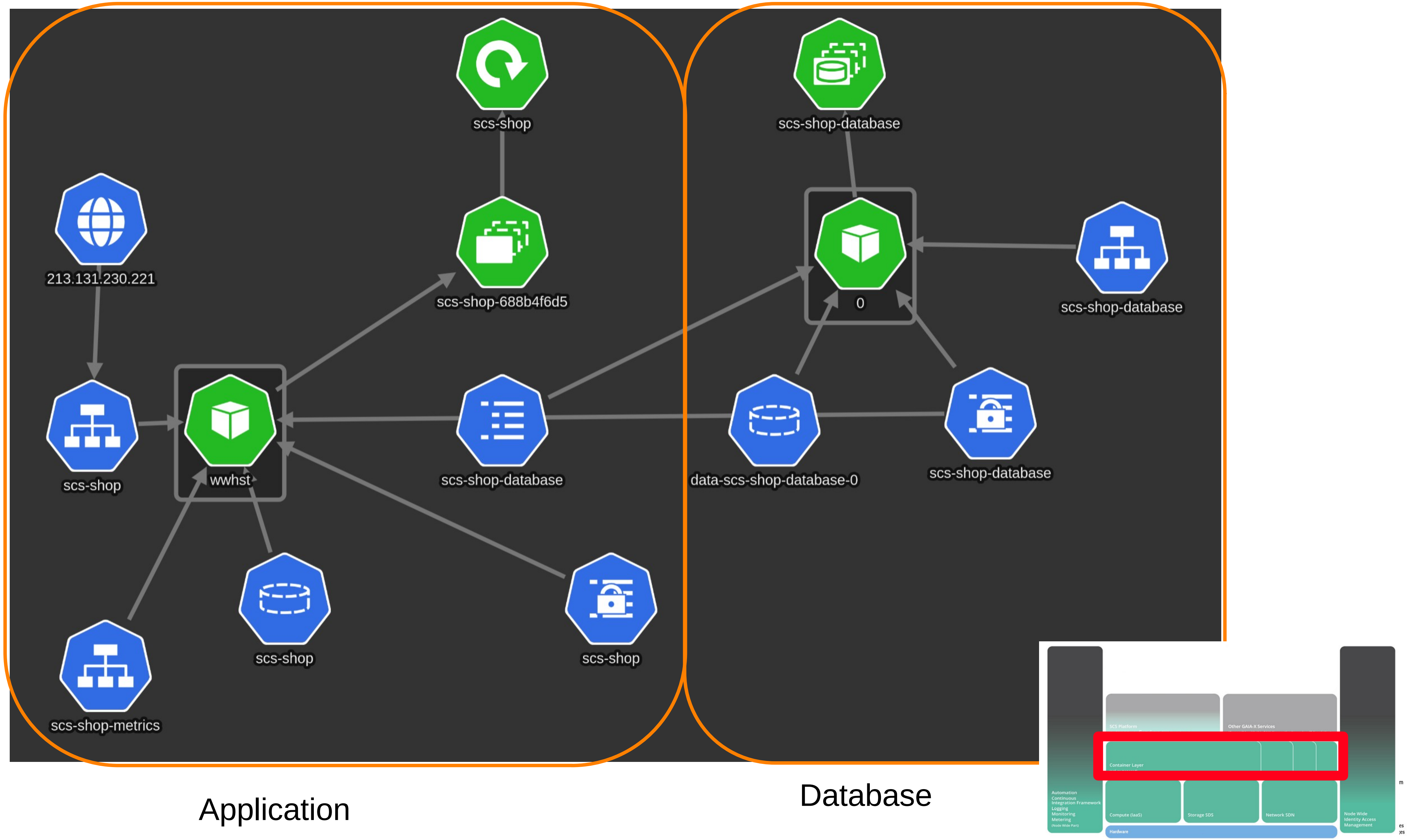


Install eCommerce Application

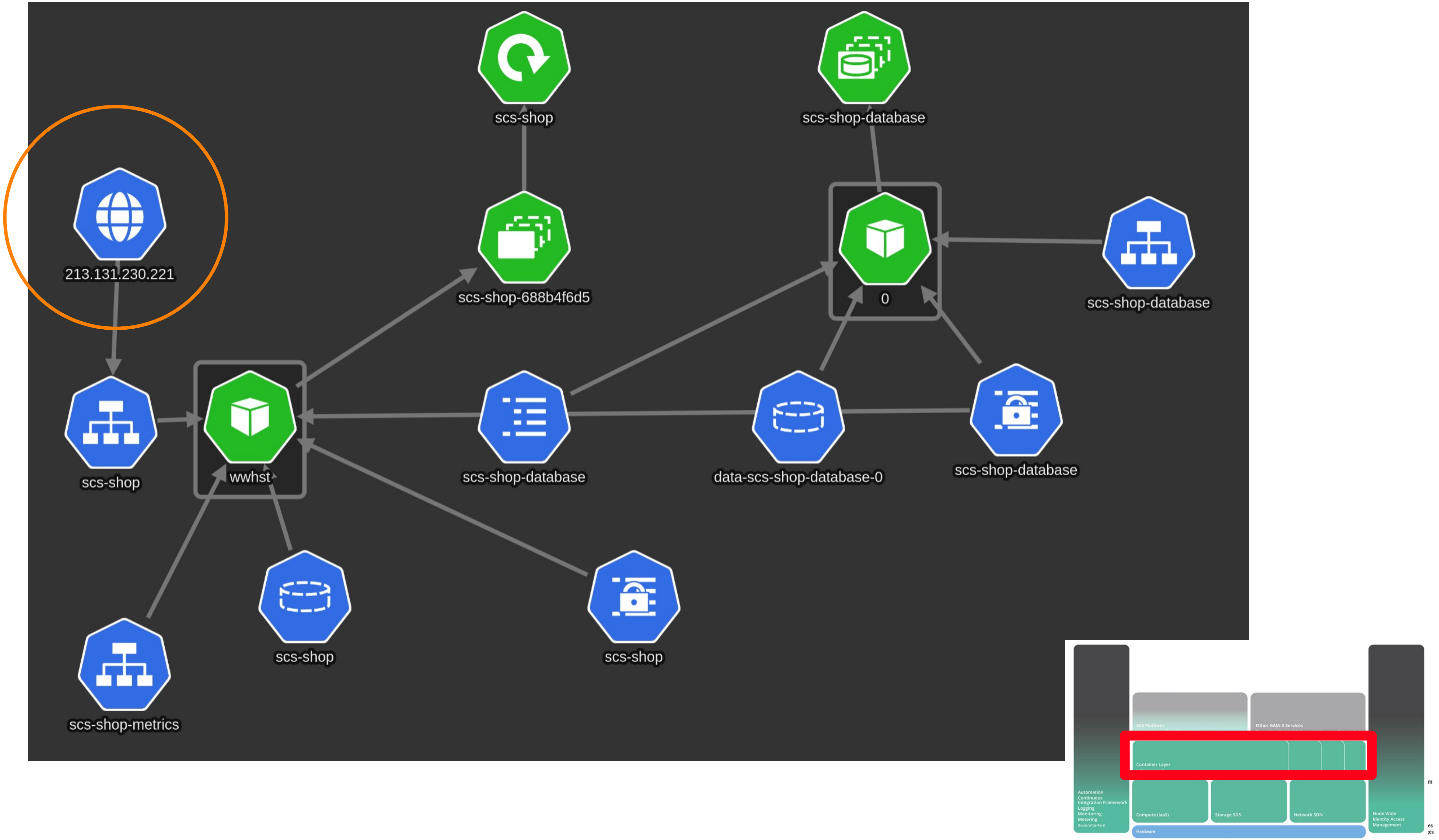


gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

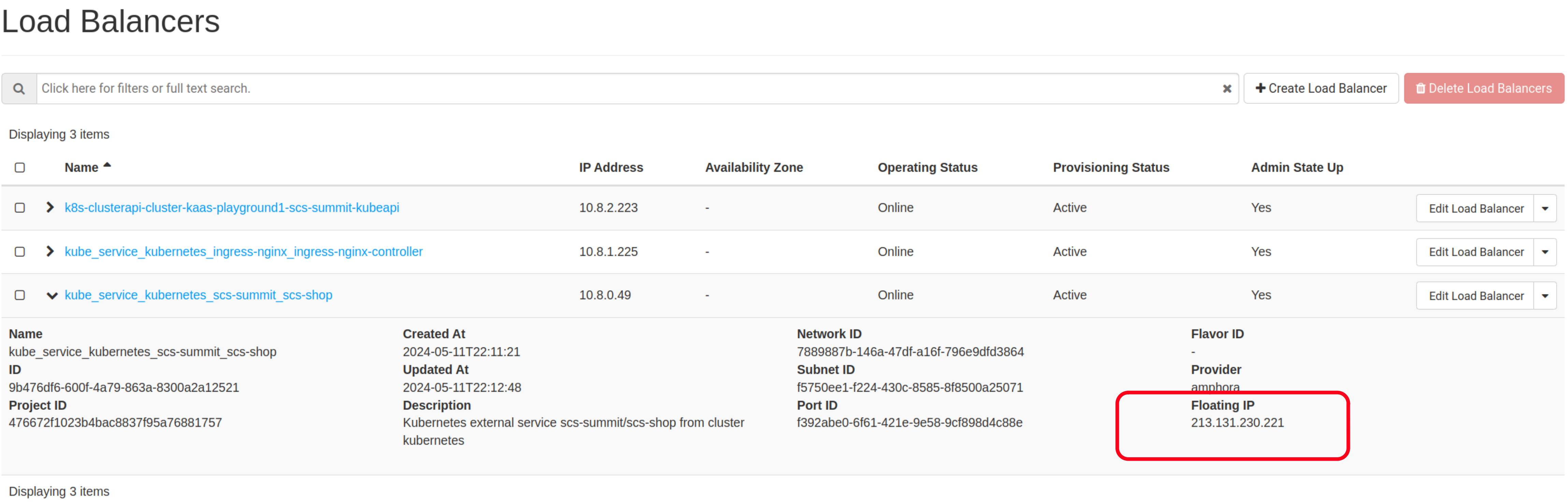
eCommerce application in Kubernetes



Example application in Kubernetes



How the application is exposed



Load Balancers

Click here for filters or full text search. ✖ + Create Load Balancer | Delete Load Balancers

Displaying 3 items

□	Name ▲	IP Address	Availability Zone	Operating Status	Provisioning Status	Admin State Up	
□	k8s-clusterapi-cluster-kaas-playground1-scs-summit-kubeapi	10.8.2.223	-	Online	Active	Yes	Edit Load Balancer ▾
□	kube_service_kubernetes_ingress-nginx_ingress-nginx-controller	10.8.1.225	-	Online	Active	Yes	Edit Load Balancer ▾
□	kube_service_kubernetes_scs-summit_scs-shop	10.8.0.49	-	Online	Active	Yes	Edit Load Balancer ▾

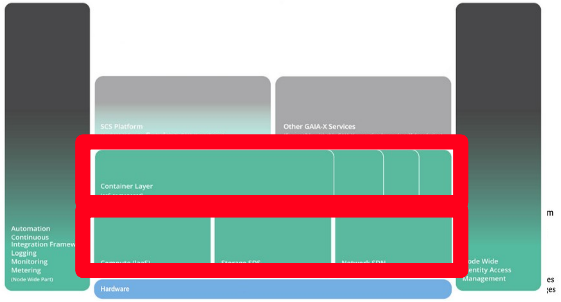
Name
kube_service_kubernetes_scs-summit_scs-shop
ID
9b476df6-600f-4a79-863a-8300a2a12521
Project ID
476672f1023b4bac8837f95a76881757

Created At
2024-05-11T22:11:21
Updated At
2024-05-11T22:12:48
Description
Kubernetes external service scs-summit/scs-shop from cluster kubernetes

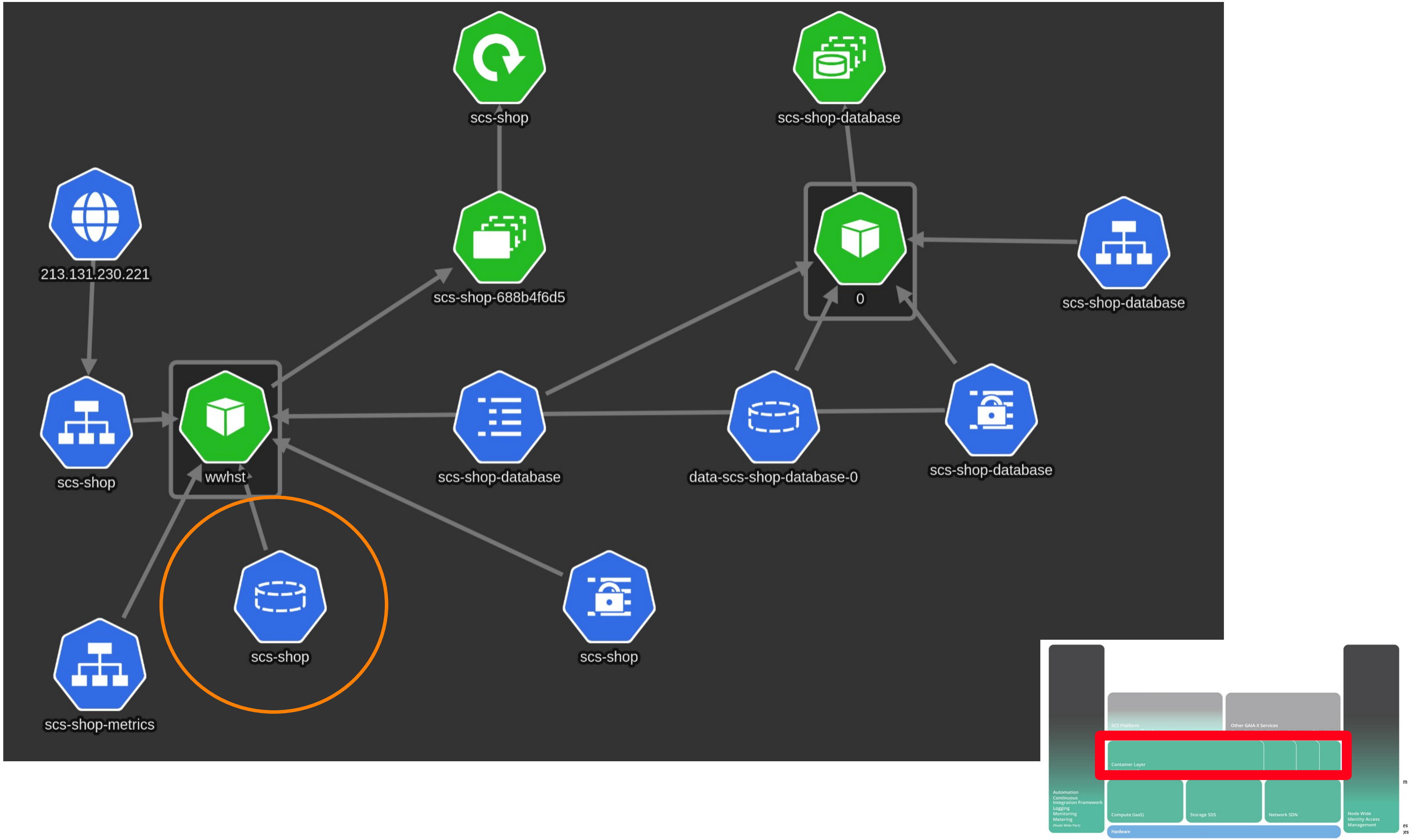
Network ID
7889887b-146a-47df-a16f-796e9dfd3864
Subnet ID
f5750ee1-f224-430c-8585-8f8500a25071
Port ID
f392abe0-6f61-421e-9e58-9cf898d4c88e

Flavor ID
-
Provider
amphora
Floating IP
213.131.230.221

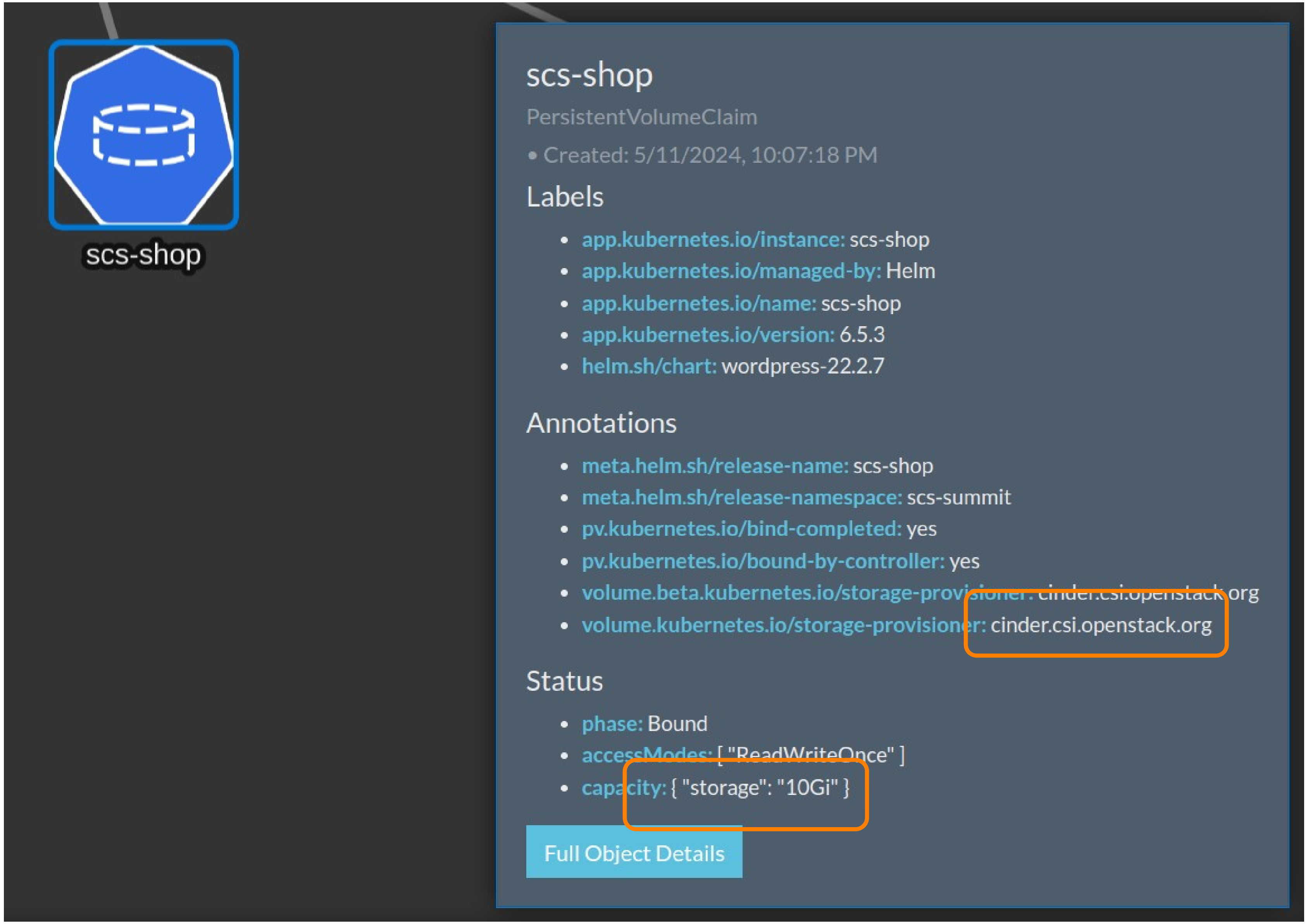
Displaying 3 items



Example application in Kubernetes



Storage Details



scs-shop

PersistentVolumeClaim

• Created: 5/11/2024, 10:07:18 PM

Labels

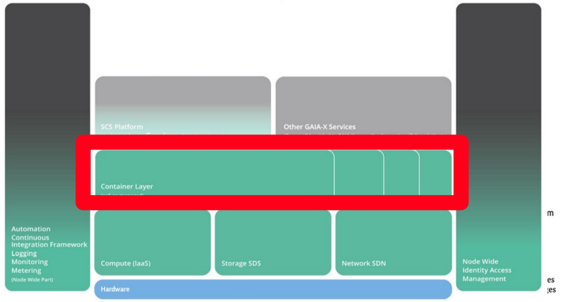
- app.kubernetes.io/instance: scs-shop
- app.kubernetes.io/managed-by: Helm
- app.kubernetes.io/name: scs-shop
- app.kubernetes.io/version: 6.5.3
- helm.sh/chart: wordpress-22.2.7

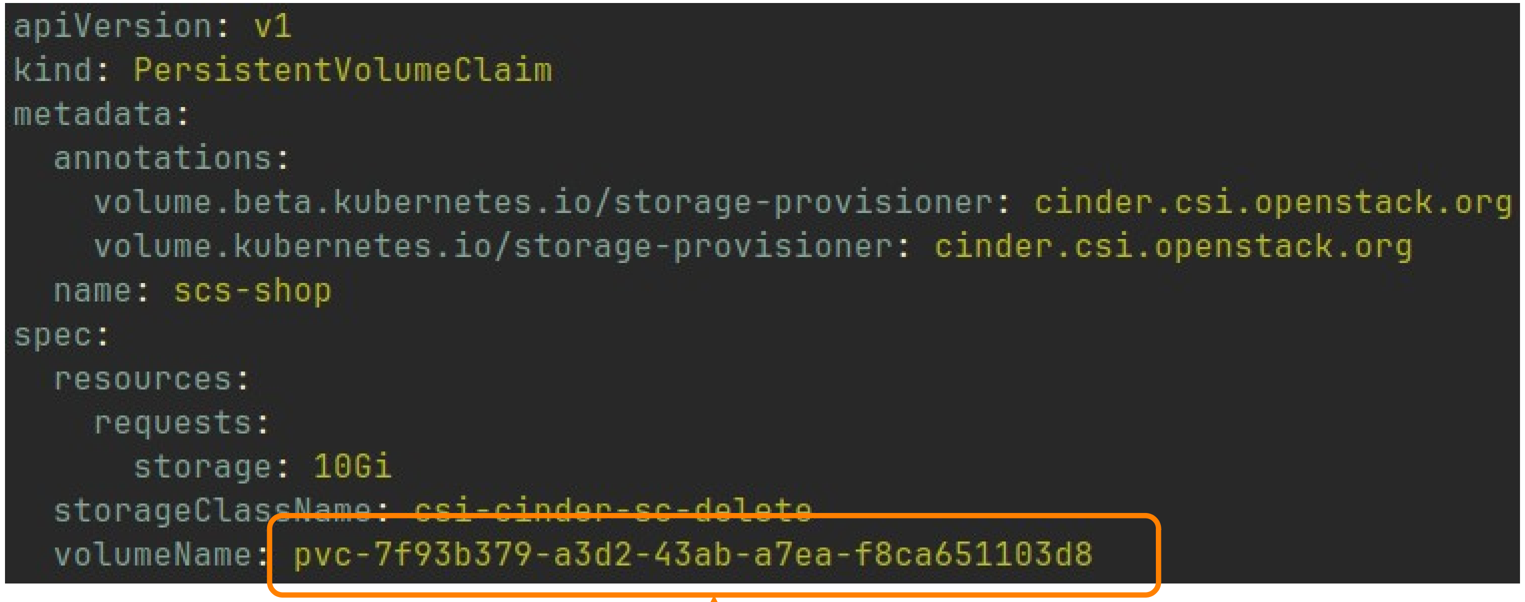
Annotations

- meta.helm.sh/release-name: scs-shop
- meta.helm.sh/release-namespace: scs-summit
- pv.kubernetes.io/bind-completed: yes
- pv.kubernetes.io/bound-by-controller: yes
- volume.beta.kubernetes.io/storage-provisioner: cinder.csi.openstack.org
- volume.kubernetes.io/storage-provisioner: cinder.csi.openstack.org

Status

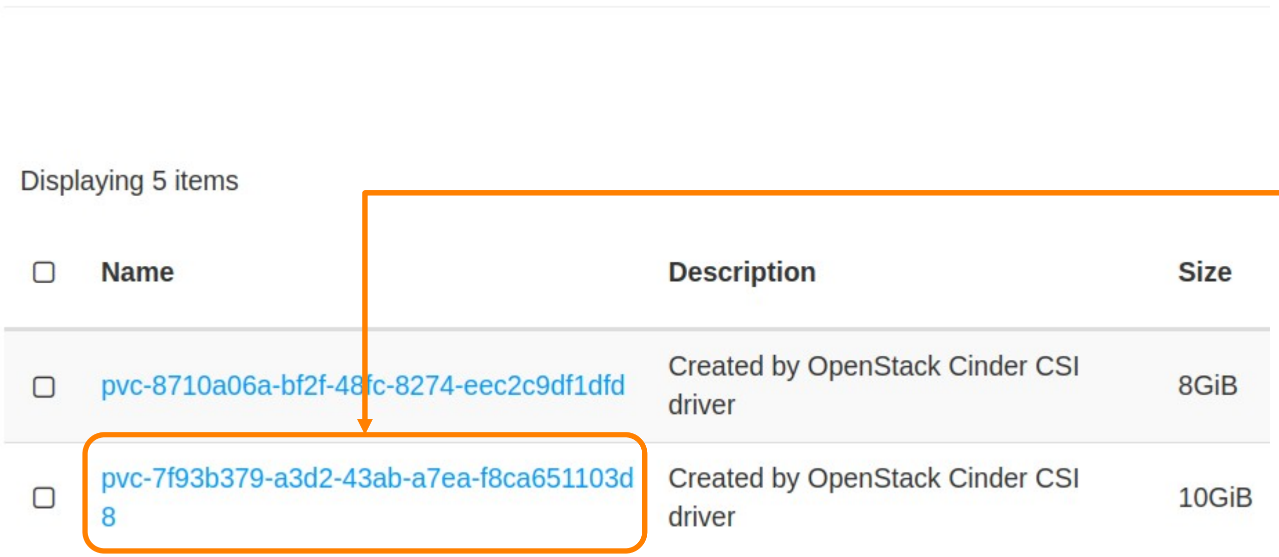
- phase: Bound
- accessModes: ["ReadWriteOnce"]
- capacity: { "storage": "10Gi" }





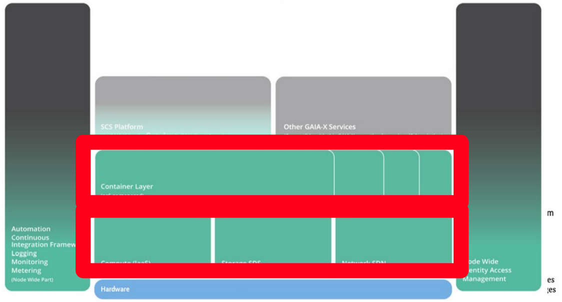
```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    volume.beta.kubernetes.io/storage-provisioner: cinder.csi.openstack.org
    volume.kubernetes.io/storage-provisioner: cinder.csi.openstack.org
  name: scs-shop
spec:
  resources:
    requests:
      storage: 10Gi
  storageClassName: csi-cinder-sc-delete
  volumeName: pvc-7f93b379-a3d2-43ab-a7ea-f8ca651103d8
```

Volumes

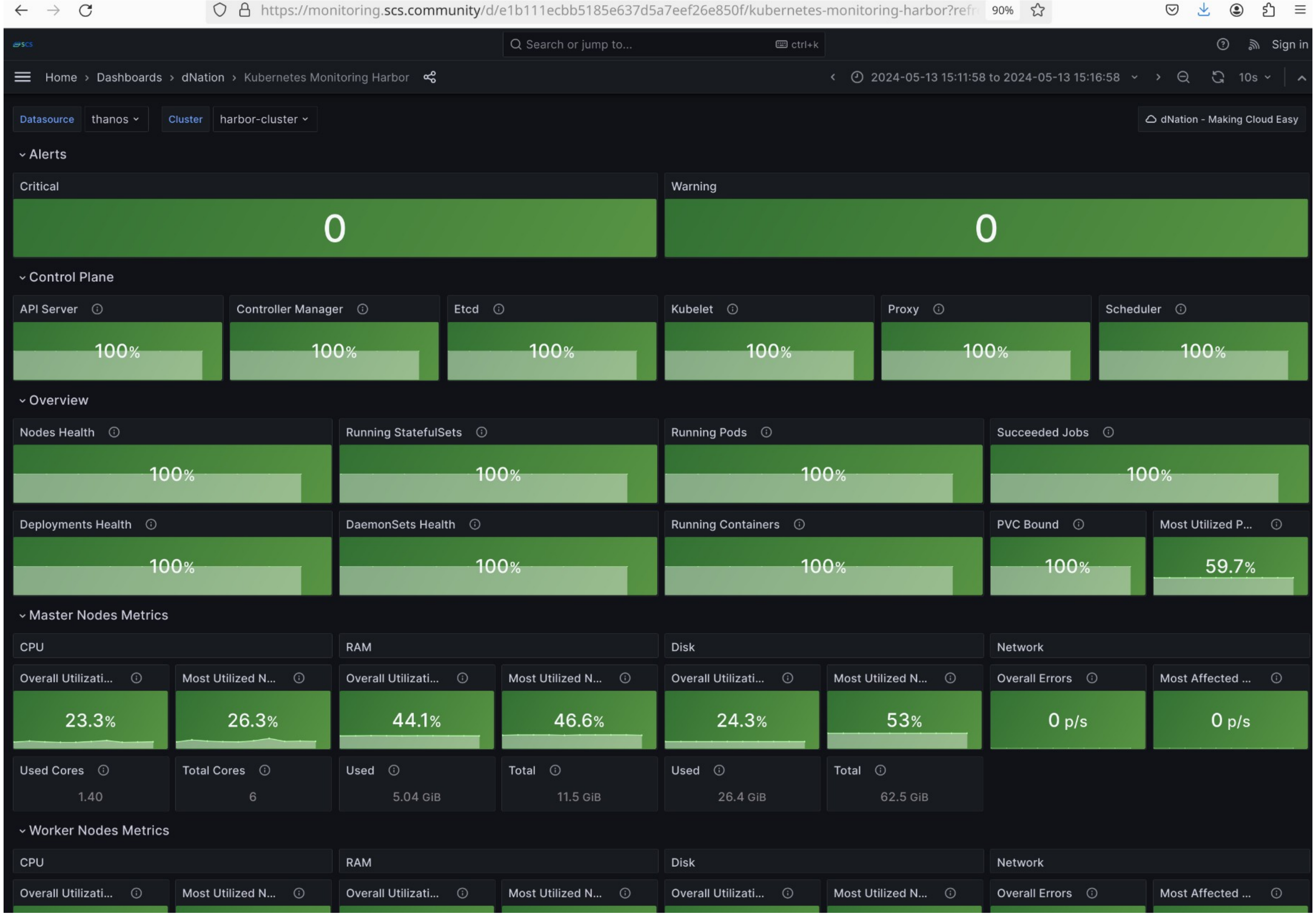


Displaying 5 items

□	Name	Description	Size
□	pvc-8710a06a-bf2f-48fc-8274-eec2c9df1dfd	Created by OpenStack Cinder CSI driver	8GiB
□	pvc-7f93b379-a3d2-43ab-a7ea-f8ca651103d8	Created by OpenStack Cinder CSI driver	10GiB



Platform Monitoring


https://monitoring.scs.community/d/e1b111ecbb5185e637d5a7eef26e850f/kubernetes-monitoring-harbor?refr 90%

Search or jump to... ctrl+k Sign in

Home › Dashboards › dNation › Kubernetes Monitoring Harbor

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

Datasource thanos Cluster harbor-cluster dNation - Making Cloud Easy

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 P... 59.7%

Master Nodes Metrics

CPU

Overall Utilizati... 23.3%

Most Utilized N... 26.3%

Used Cores 1.40

Total Cores 6

RAM

Overall Utilizati... 44.1%

Most Utilized N... 46.6%

Used 5.04 GiB

Total 11.5 GiB

Disk

Overall Utilizati... 24.3%

Most Utilized N... 53%

Used 26.4 GiB

Total 62.5 GiB

Network

Overall Errors 0 p/s

Most Affected ... 0 p/s

Worker Nodes Metrics

CPU

Overall Utilizati...

Most Utilized N...

RAM

Overall Utilizati...

Most Utilized N...

Disk

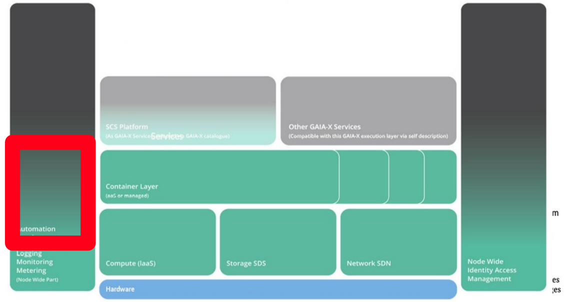
Overall Utilizati...

Most Utilized N...

Network

Overall Errors

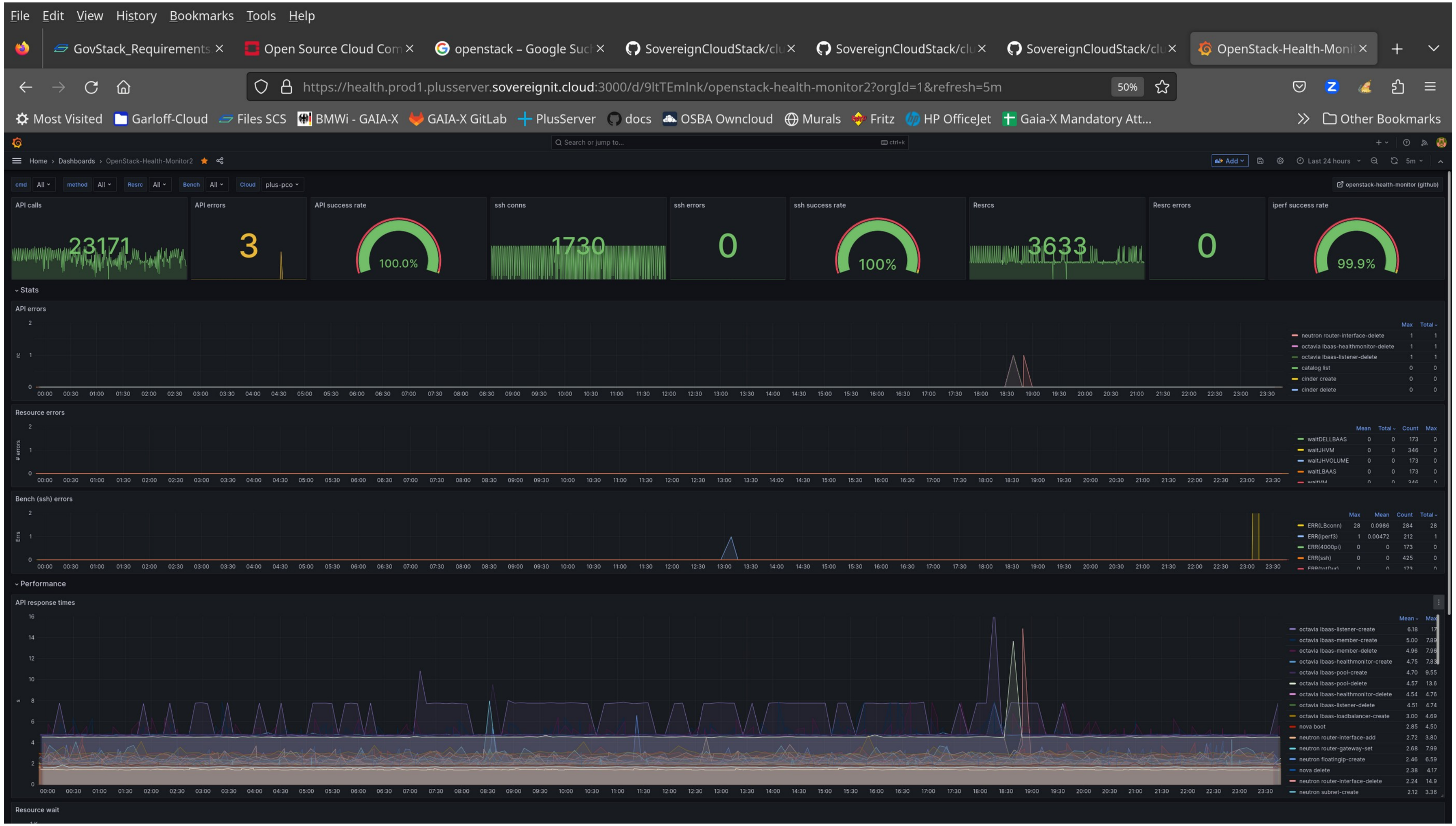
Most Affected ...



Sovereign Cloud Stack
An OSB ALLIANCE project

Infra Monitoring

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



https://health.prod1.plusserver.sovereignit.cloud:3000/d/9ltTEmlnk/openstack-health-monitor2?orgId=1&refresh=5m

API errors

	Max	Total
neutron router-interface-delete	1	1
octavia lbaas-healthmonitor-delete	1	1
octavia lbaas-listener-delete	1	1
catalog list	0	0
cinder create	0	0
cinder delete	0	0

Resource errors

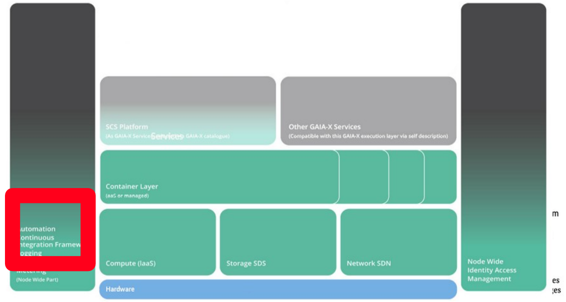
	Mean	Total	Count	Max
waitDELLBAAS	0	0	173	0
waitJHVM	0	0	346	0
waitJHVOLUME	0	0	173	0
waitLBAAS	0	0	173	0
waitVM	0	0	346	0

Bench (ssh) errors

	Max	Mean	Count	Total
ERR(LBconn)	28	0.0986	284	28
ERR(iperf3)	1	0.00472	212	1
ERR(4000pi)	0	0	173	0
ERR(ssh)	0	0	425	0
ERR(totDur)	0	0	173	0

API response times

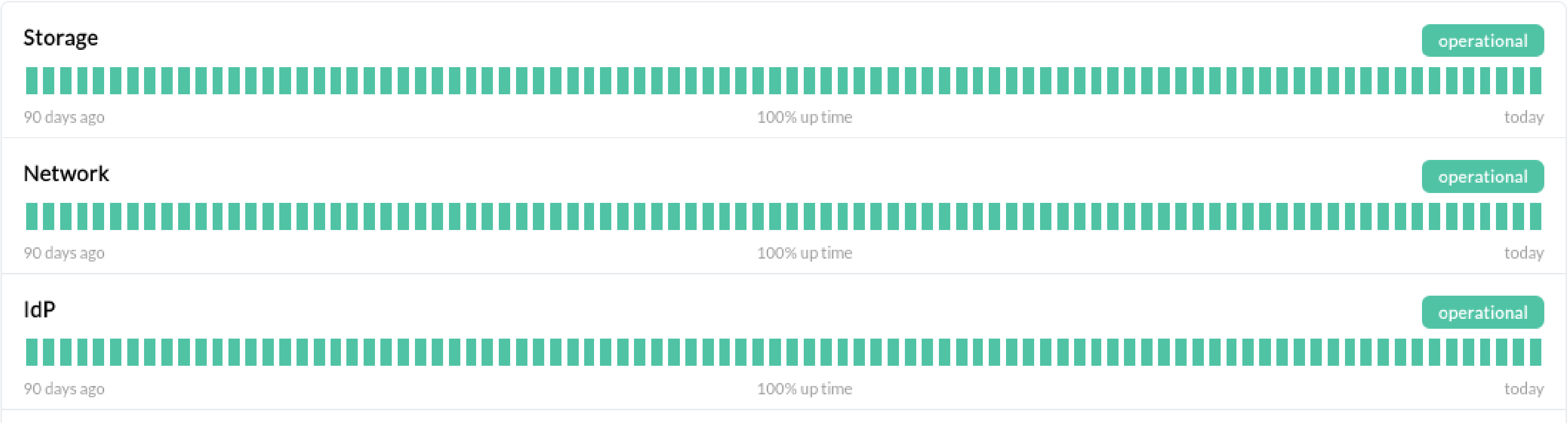
	Mean	Max
octavia lbaas-listener-create	6.18	17
octavia lbaas-member-create	5.00	7.89
octavia lbaas-member-delete	4.96	7.96
octavia lbaas-healthmonitor-create	4.75	7.83
octavia lbaas-pool-create	4.70	9.55
octavia lbaas-pool-delete	4.57	13.6
octavia lbaas-healthmonitor-delete	4.54	4.76
octavia lbaas-listener-delete	4.51	4.74
octavia lbaas-loadbalancer-create	3.00	4.69
nova boot	2.85	4.50
neutron router-interface-add	2.72	3.80
neutron router-gateway-set	2.68	7.99
neutron floatingip-create	2.46	6.59
nova delete	2.38	4.17
neutron router-interface-delete	2.24	14.9
neutron subnet-create	2.12	3.36



Status Page (with own API)

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

End user
CSP customer



Storage operational
90 days ago 100% up time today

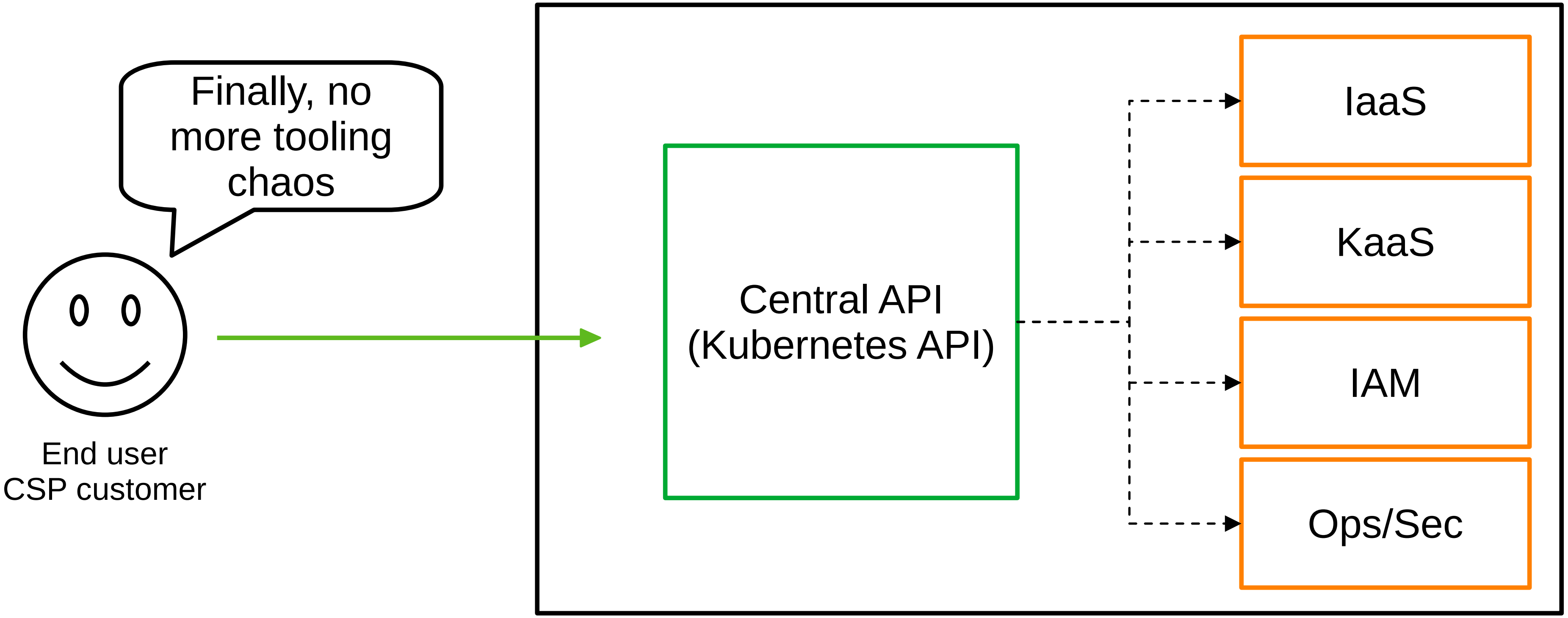
Network operational
90 days ago 100% up time today

IdP operational
90 days ago 100% up time today

gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

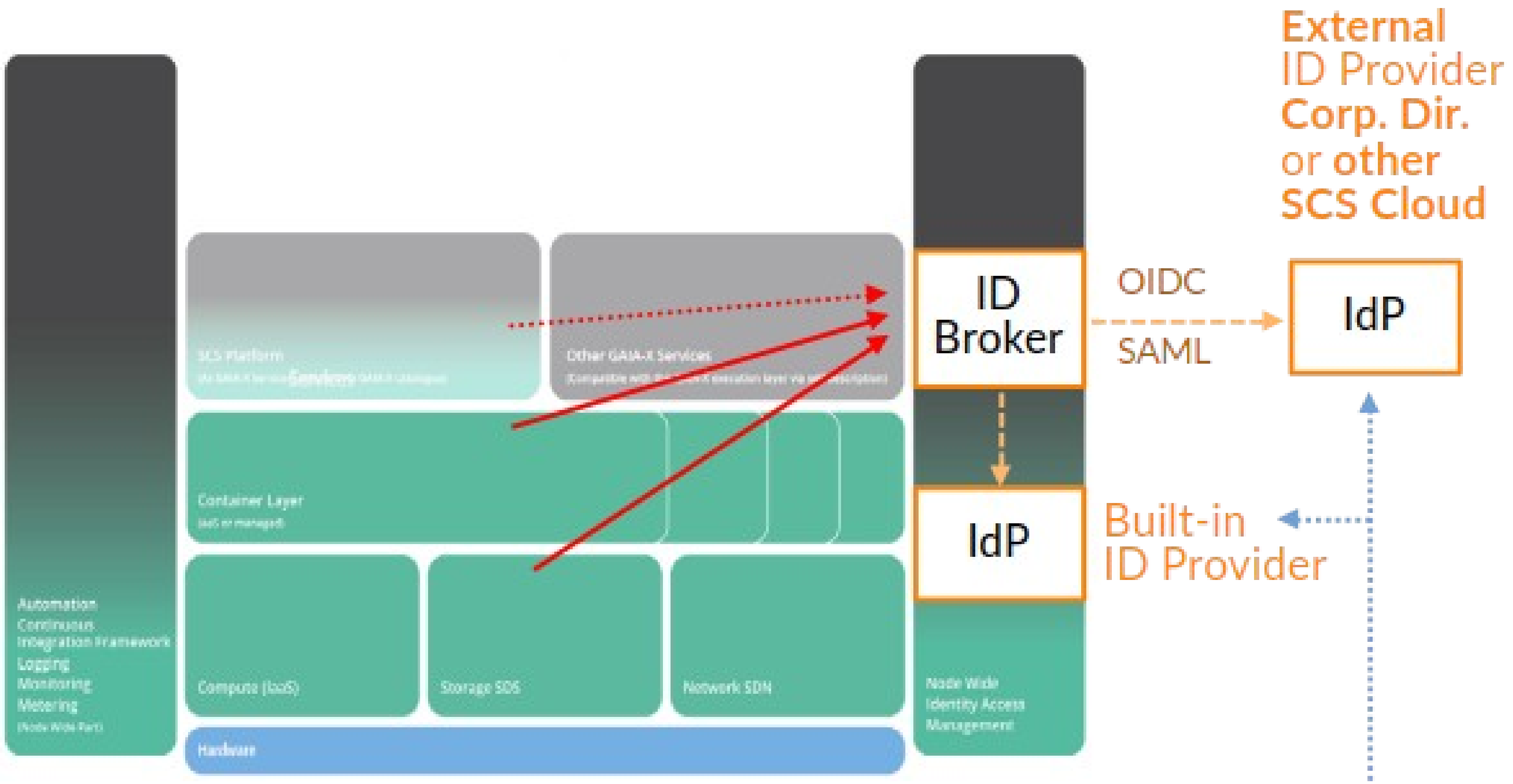
Central API – one endpoint for daily business

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



gaia-x
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

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



Users are managed in their IdP

Credentials / Authentication

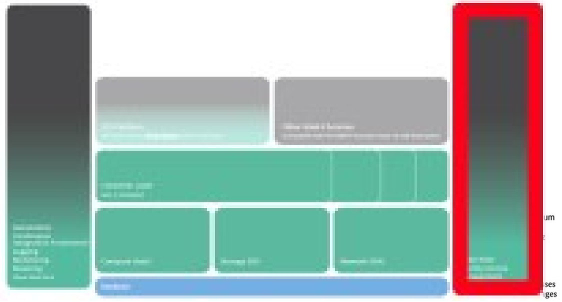
Assignment of users to groups

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

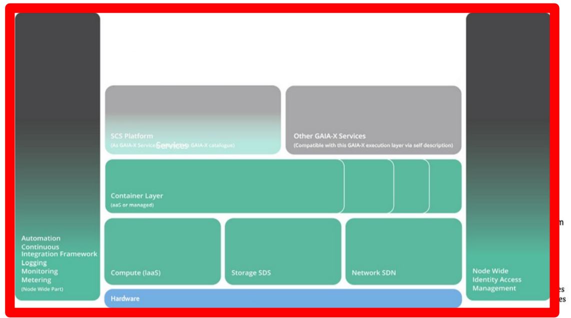
Customer manages his own domain / realm

Customer Self Service



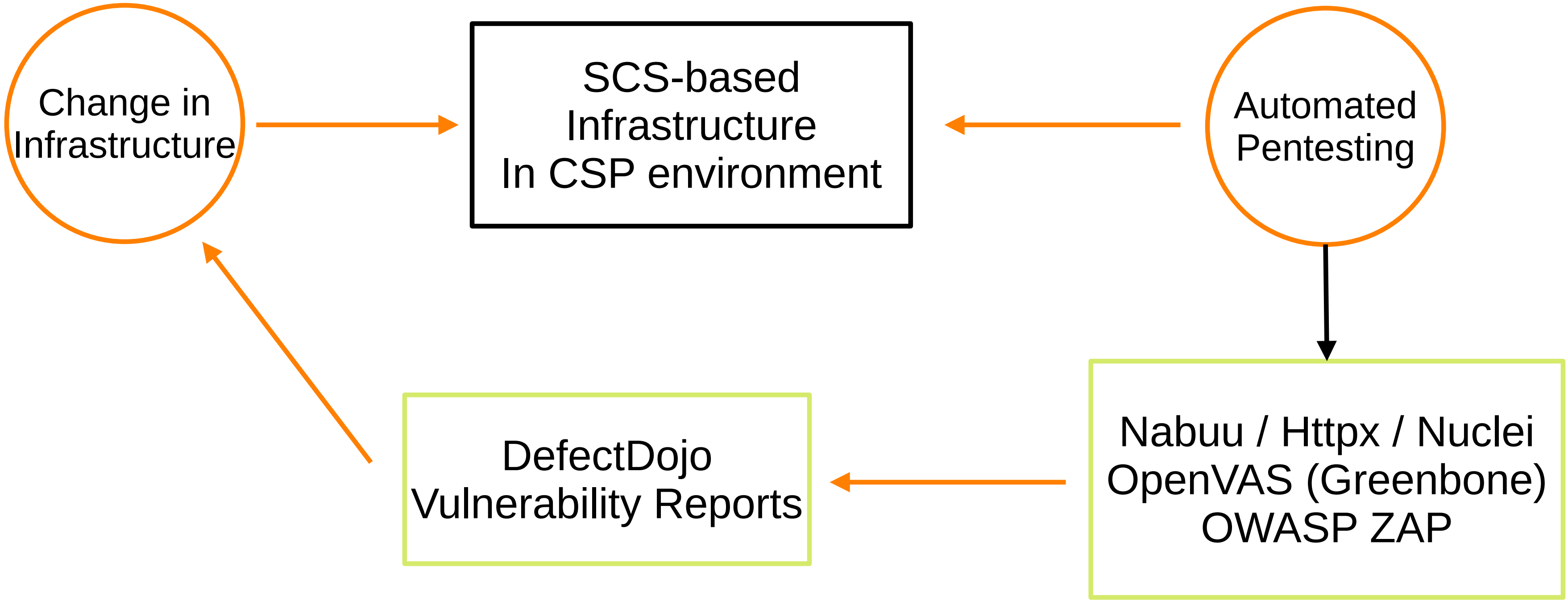
Security by design

- Standardized best practices
- Deployment uses strong secure defaults
- Hardware 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**


Change in Infrastructure
SCS-based Infrastructure In CSP environment
Automated Pentesting
Nabuu / Httpx / Nuclei OpenVAS (Greenbone) OWASP ZAP
DefectDojo Vulnerability Reports

Summary

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**)