

Open source observability in private cloud: mission impossible or not?

Diana Todea - Senior SRE @ EQS Group

20th of November 2024



OPEN SOURCE
MONITORING
CONFERENCE

SRE focused on o11y
ML, AI, OSS enthusiast 😊
support women in tech



Contact me:
[LINKEDIN](#) | [GITHUB](#)

01

Who are we?

02

Hybrid
architecture

03

Private cloud

04

OSS
observability

05

Challenges

06

Future plans





An international cloud software provider in the areas of corporate compliance, investor relations and sustainability reporting, headquartered in Munich, Germany. Founded in 2000, present in DACH (DE, AUT, CH) and internationally in US, UK, France, Spain, Denmark, Hong Kong, Italy.

- Whistleblowing
- Data protection
- GDPR

Private cloud

Focused on the EU

Challenges in terms of monitoring and scaling

Sensitive to upgrades

Public cloud

Not bound to very strict business regulations

Easier to handle and maintain

More costly



Developers

Plethora of frontend and backend applications connected to our databases. Lots of SDKs.



SREs

Support developers and align their infrastructure needs to the company's requirements. Provide and maintain reliable systems, manage the implementation of solutions and avoid downtime. Team of 5 SREs and limited time.



What?

- Type of cloud computing environment that is dedicated to a single organization.
- Designed to provide exclusive access and control
- It can be hosted on-prem or by a third-party service provider.



Who?

- T-systems: Germany
- Swisscom: Switzerland
- OVH: France



Why?

- Used for business reasons and state regulations
- Data stays local to that region or country



APM solution

Primarily focused off the shelf solutions where we ingested some logs and monitored data centers and applications.



OSS

Prometheus metrics, Grafana dashboards, ELK for logging become our observability pillars.



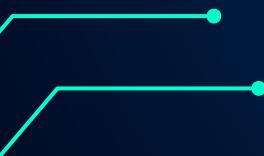
DevOps morphs into SRE

DevOps transitioned to SRE best practices. The crucial need for consistent and stable observability gets priority.



Logs, traces, metrics

Fragmentation of o11y leads to confusion amongst the developers and creates instability. Aiming for a unified o11y.





If it's trendy doesn't mean it's good



Think twice about the cost

What private cloud taught us?



Are developers using it?



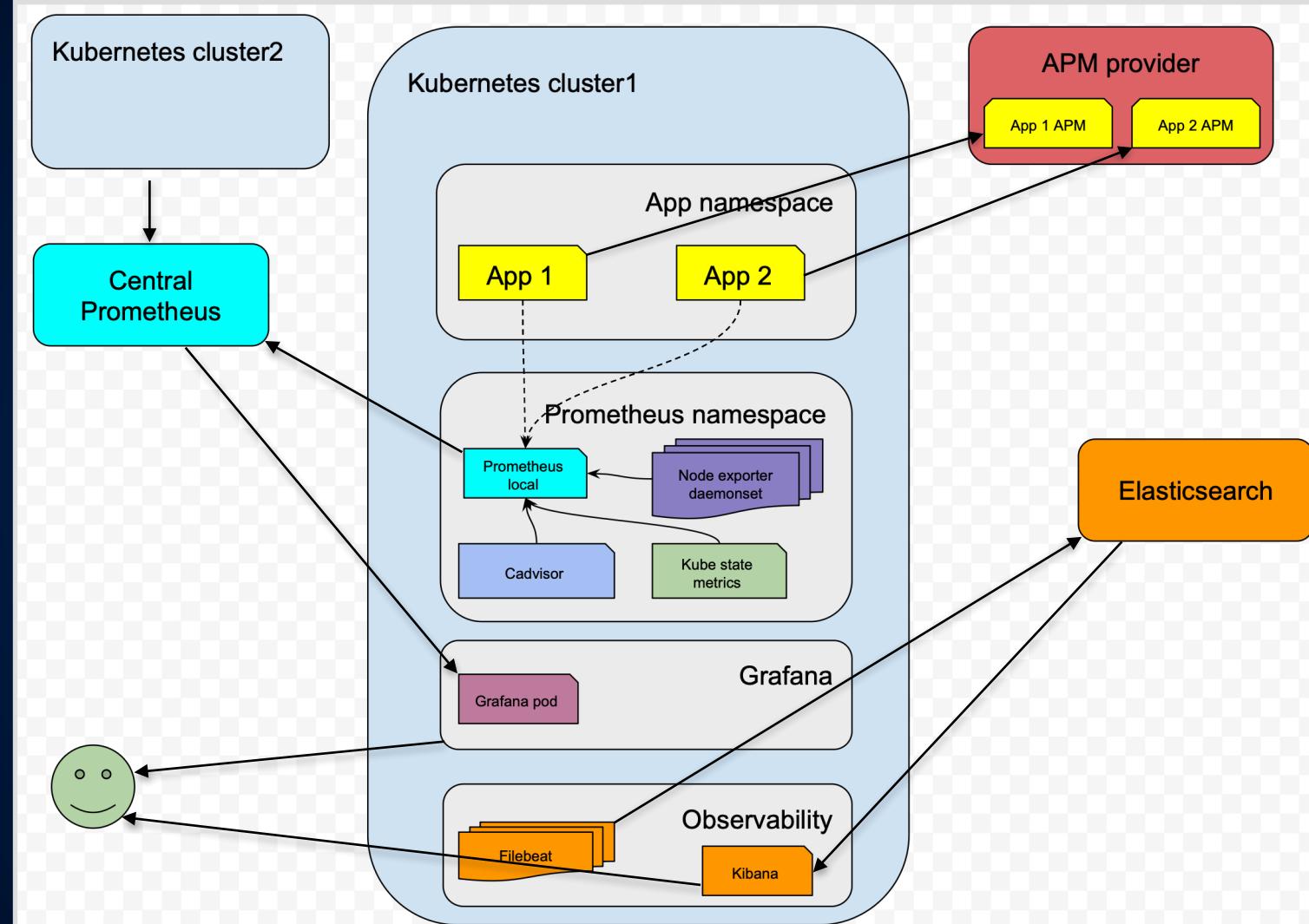
Security



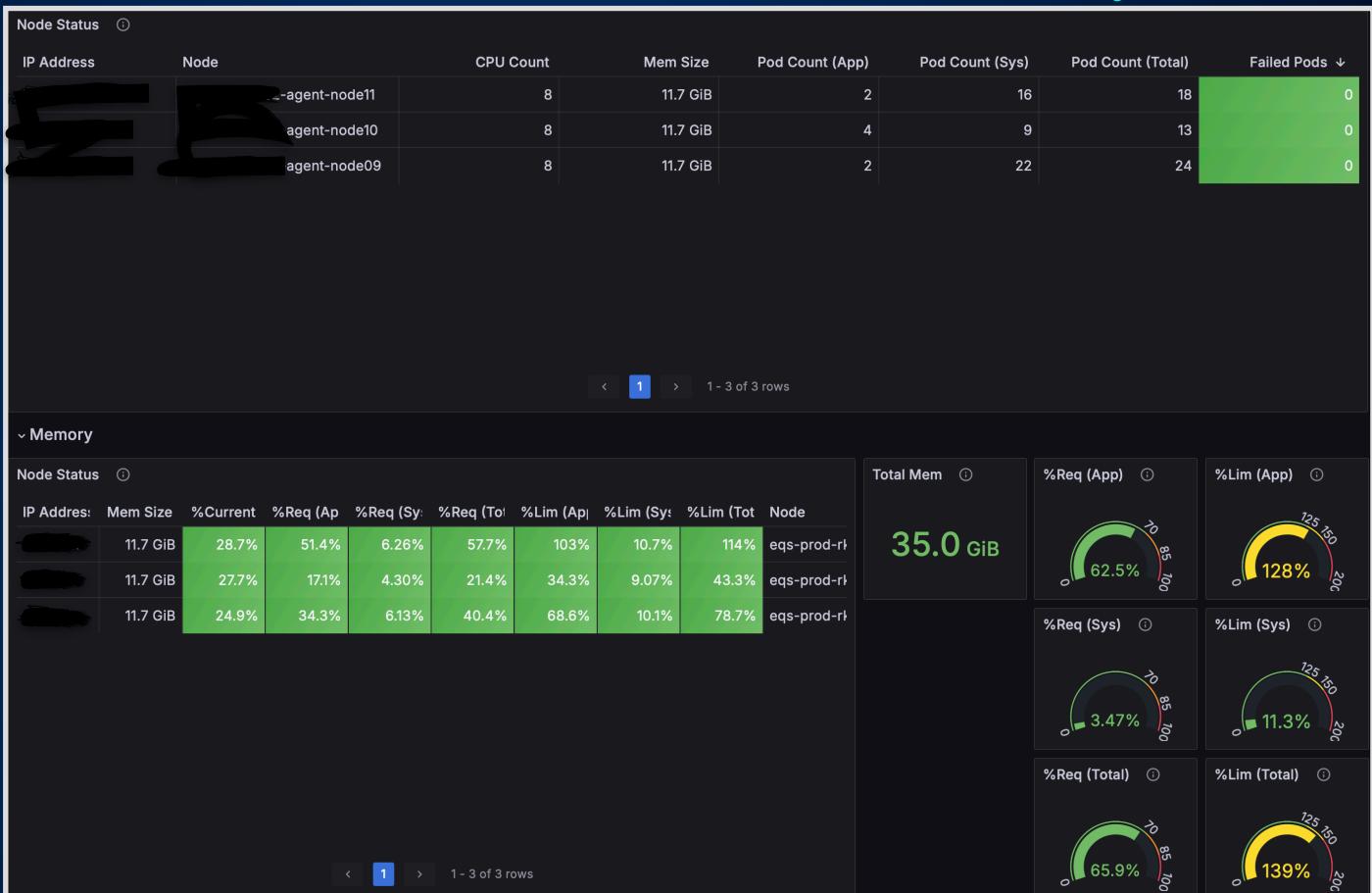
Priority



Less is more



OSS Grafana
for our
production K8s
clusters



Private cloud monitoring

Cluster: upstream-t-systems-prod | Namespace: kube-system | General K8s Object Status

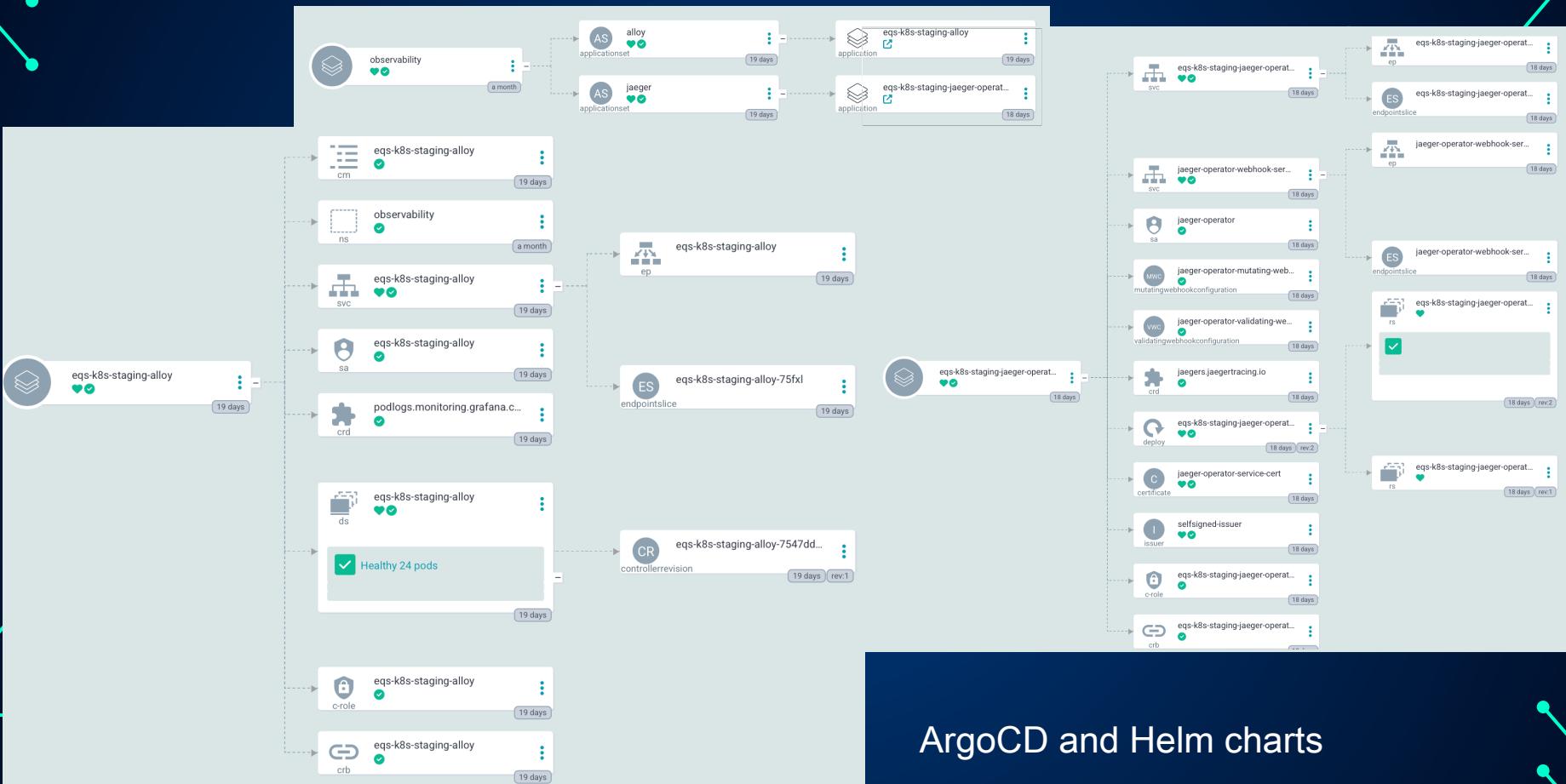
Pods Totals

Pod Container Status

Pod	Container	Owner	Node	Restarts	Req(CPU)	Lim
etcd-[REDACTED]-master-node01	etcd	Node	eqs-prod-rke2-maste	0	0.200	
etcd-[REDACTED]-master-node02	etcd	Node	eqs-prod-rke2-maste	0	0.200	
etcd-[REDACTED]-master-node03	etcd	Node	eqs-prod-rke2-maste	2	0.200	
hubble-relay-[REDACTED]	hubble-relay	ReplicaSet	eqs-prod-rke2-agent	0	No Req	
kube-apiserver-[REDACTED]-master-node01	kube-apiserver	Node	eqs-prod-rke2-maste	0	0.250	
kube-apiserver-[REDACTED]-master-node02	kube-apiserver	Node	eqs-prod-rke2-maste	0	0.250	
kube-apiserver-[REDACTED]-master-node03	kube-apiserver	Node	eqs-prod-rke2-maste	3	0.250	
kube-controller-manager-[REDACTED]-master-node01	kube-controller-manag	Node	eqs-prod-rke2-maste	3	0.200	
kube-controller-manager-[REDACTED]-master-node02	kube-controller-manag	Node	eqs-prod-rke2-maste	3	0.200	
kube-controller-manager-[REDACTED]-master-node03	kube-controller-manag	Node	eqs-prod-rke2-maste	8	0.200	
kube-proxy-[REDACTED]-master-node01	kube-proxy	Node	eqs-prod-rke2-maste	0	0.250	
kube-proxy-[REDACTED]-master-node02	kube-proxy	Node	eqs-prod-rke2-maste	0	0.250	

Grafana alerting

Prod > Application						1 firing	3 normal	0 1m	edit	refresh	more
State	Name	Health	Summary	Next evaluation	Actions						
> Normal	[K8s] Unschedulable pods	ok	Pod is pending scheduling	in a few seconds	edit More						
> Firing for 1d 18h 56m	[K8s] Pods in invalid status	ok	The pod is in invalid status (any status other than running/completed etc.).	in a few seconds	edit More						
> Normal	[K8s] [Private Cloud] Container throttling > 50%	ok	Pod has at least one container being throttled.	in a few seconds	edit More						
> Normal	[K8s] [AWS] Container throttling > 50%	ok	Pod has at least one container being throttled.	in a few seconds	edit More						
Prod > OS						3 normal	0 1m	edit	refresh	more	
State	Name	Health	Summary	Next evaluation	Actions						
> Normal	[OS K8s] Memory > 85%	ok	Used kubernetes node memory over 85%.	in a few seconds	edit More						
> Normal	[OS K8s] CPU > 85%	ok	Used kubernetes node cpu over 85%.	in a few seconds	edit More						
> Normal	[OS Gitlab] Service status	ok	One of the systemd gitlab services is down.	in a few seconds	edit More						



ArgoCD and Helm charts

Challenges: can we migrate our APM solution?

Really useful for
developers



Only hosted by
external vendor at
the moment



Synthetic monitoring
only in Grafana
Cloud



Can ELK be an
alternative?



Private cloud
limitations



Distributed
tracing: OSS



Open Telemetry

Further OTEL integration and customization within our apps is needed for Jaeger operator to work properly and for traces to be sent and seen from and within the applications.

Jaeger

Easy to setup and test, Jaeger operator with K8s clusters was our choice for distributed tracing.

Many programming languages

The necessity to follow the behavior of the apps and account for their traces will play a huge role in our observability.

Lessons learned

OTEL insufficient docs

Testing OTEL with simple apps lead us in the first instance to drop it due to insufficient explanation of official/non-official docs.

Dashboards

Great, but we want to have lots of visualizations. Can we try Grafana Alloy?

Jaeger POC with 3 SDKs

Successful integration of Jaeger Operator with K8s.

Standby

Documentation and all integrations to become more mature and stable. Still work in progress. Keeping an eye on the OTEL community and further developments.

Not going to prod

Why? Profiling signals in OTEL

Stay open

Open to further OSS projects and POCs. Each SRE should POC their own favorite project.





Roadmap

- ⌚ Further develop our OSS strategy
- ⌚ Maintain our OSS tools with Grafana, Prometheus
- ⌚ Integrating apps with OpenTelemetry
- ⌚ Move away from o11y fragmentation
- ⌚ Achieve consistency on all platforms
- ⌚ Stay open to further OSS POCs and tools

To improve

- ⌚ Alerts, dashboards, customization
- ⌚ Substitute public cloud APM solutions with OSS
- ⌚ Plan and solve any capacity, scaling or data ingestion questions (where to centralize the data, how many metrics to pull and ingest, which data to choose from)
- ⌚ Incident management: provide uptime status of internal tools
- ⌚ Culture: accountability and ownership
- ⌚ Communication between developers and SREs



Catalog | Resources | Corporate Solutions | Explore

[Certification](#) > [Cloud & Containers](#) > OpenTelemetry Certified Associate (OTCA)

CERTIFICATION

OpenTelemetry Certified Associate (OTCA)

As cloud native systems grow more complex, the demand for professionals who can leverage telemetry data is growing rapidly. Open new career paths – prove your expertise in OpenTelemetry – the industry standard for tracing, metrics & logs.

OTCA includes:

- ✓ 12-months to schedule & take the exam
- ✓ Two exam attempts

IMPORTANT: The OTCA certification exam is now available for purchase, but the ability to schedule the OTCA exam will not be available until January 2025.



OPEN SOURCE
MONITORING
CONFERENCE



VIELEN DANK!
THANK YOU!

ANY QUESTIONS?

<https://www.linkedin.com/in/diana-todea-b2a79968>
https://github.com/didiViking/Conferences_Talks