

Kubernetes Saved My Grandma: High-Reliability IoT for Elderly Care

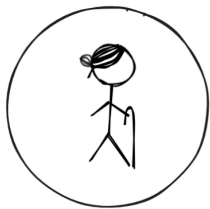


Fabrizio Lazzaretti



Linus Basig





Why Now?

GDPR/nDPA

US cloud providers cannot fully guarantee data protection under current legal acts.

heise online

heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissenschaft

Not sovereign: Microsoft cannot guarantee the security of EU data

In a hearing, the Chief Legal Officer of Microsoft France had to admit: There is no guarantee that EU data is safe from being transferred to the USA.

heise.de

Digital Switzerland Strategy

Switzerland sets digital sovereignty as a top priority.

Press release | Published on 12 December 2025

Federal Council adopts Digital Switzerland Strategy 2026

Bern, 12.12.2025 — On 12 December, the Federal Council adopted the updated Digital Switzerland Strategy for 2026 and selected the new focus themes. The focus themes for next year are: [digital sovereignty](#), digital host state and the introduction of the e-ID. This reflects the current priorities.

admin.ch

Sanctions

US sanctions on the ICC and its staff also block its IT contracts with US companies.

Reuters

Subscribe 🔍 ☰

US imposes sanctions on ICC hours after former judge wins Nobel Peace Prize

By Humeyra Pamuk, Steve Holland and Anthony Deutsch

October 9, 2026 4:02 PM GMT+2 · Updated October 10, 2026

[Reuters, via usnews.com](#)

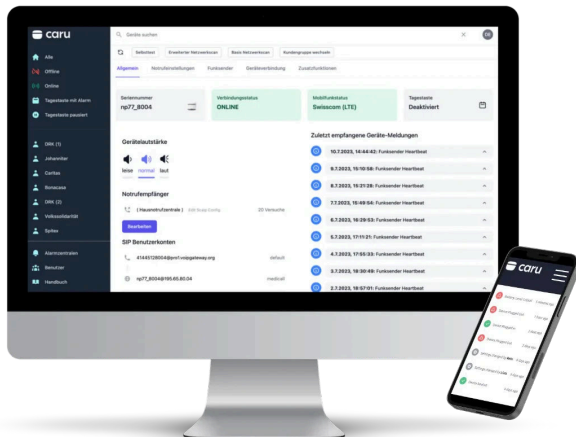
GDPR: EU General Data Protection Regulation nDPA: revised Swiss Federal Act on Data Protection (2023)

Disclaimer: We are software architects planning for the future, not legal experts.

The CARU care Device



The CARU cloud Platform



Shaping the Future of Care



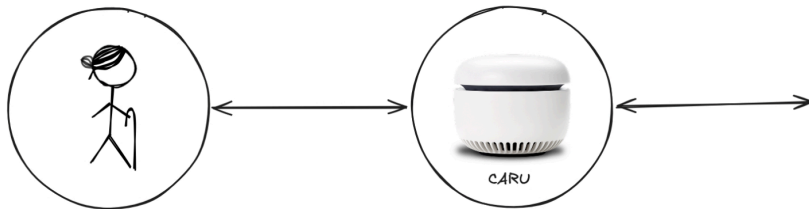
Home Emergency System



Virtual Care Home OS

Goal of the Talk

What would a truly sovereign architecture look like?



**Thought
Experiment**

Open Source to the Rescue



Open Today, Closed Tomorrow

2021 Elasticsearch

Change
Apache 2.0 →
SSPL / Elastic
License

Impact / Fork
OpenSearch fork
under Linux
Foundation

Reversion
Added AGPL
back in Aug 2024

2023 HashiCorp Vault

Change
MPL → BSL

Impact / Fork
OpenBao fork
under Linux
Foundation

2023 Terraform

Change
MPL → BSL

Impact / Fork
OpenTofu fork
now a CNCF
project

2024 Redis

Change
BSD → RSAL /
SSPL

Impact / Fork
Valkey fork under
Linux Foundation

Reversion
Back to AGPLv3
with v8 in 2025

2025 MinIO

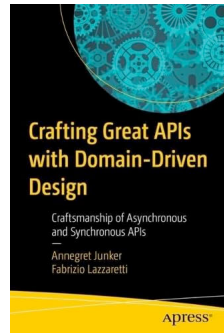
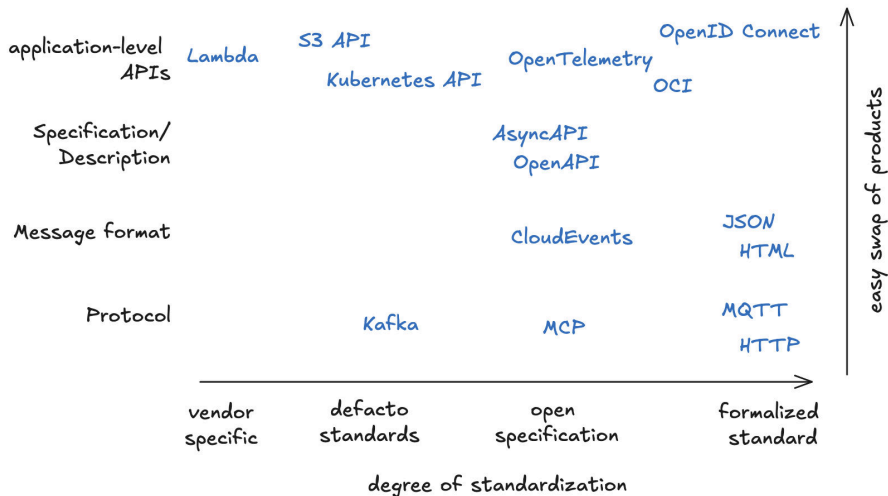
Change
Admin UI
removed,
binaries/images
stopped,
maintenance
mode

Impact / Fork
Community forks
& alternatives
emerging

The Way Out: Foundation-Governed Open Source



The Foundation to Switch Fast: Open Standards, APIs and Protocols



Migration Strategy

1 Backup of everything off-cloud

Your safety net



Off-cloud backup of

- Data
- Source code
- Documentation
- Passwords (with proper encryption)
- Certificates
- ...

2 Get the abstractions right

Slow but steady towards sovereignty



Abstractions, APIs and open standards

- Step by step: be able to interchange when needed
- Do tests and move slowly
- Split components and use standard APIs in between

3 Prepare the escape

Be ready to leave when you have to



Classical disaster recovery preparations

- An honest plan including communication
- Rehearsals to find gaps
- Reassess the situation regularly

Two Views on the Same System

Platform view

Focus today

- Compute
- Event Subsystem
- Fleet Management
- Storage
- Monitoring & Observability
- ...

⇒ **Solve it once, with standards, for all capabilities**

Capability view

- Emergency Call
- Daily Check-In
- CO₂
- Care Partner Portal
- Hydration Reminder
- ...

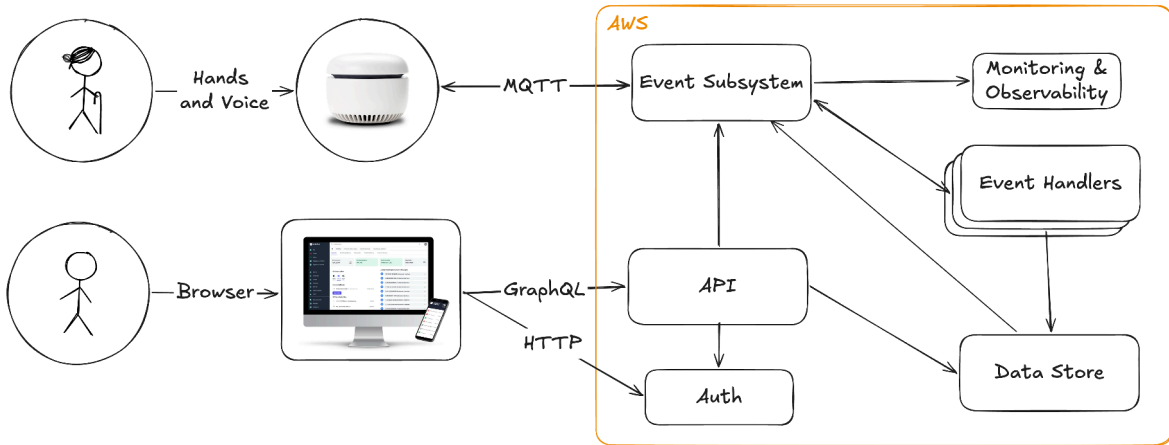
⇒ **Prioritize:**

- What must work first, or only, after a switch?
- What can we drop before changing anything?
- Where do we start?

Methods: Business model canvas, Wardley mapping, ...

See talk: [Spring I/O 2026: Crafting Great APIs with Domain-Driven Design](#)

Current Architecture on AWS

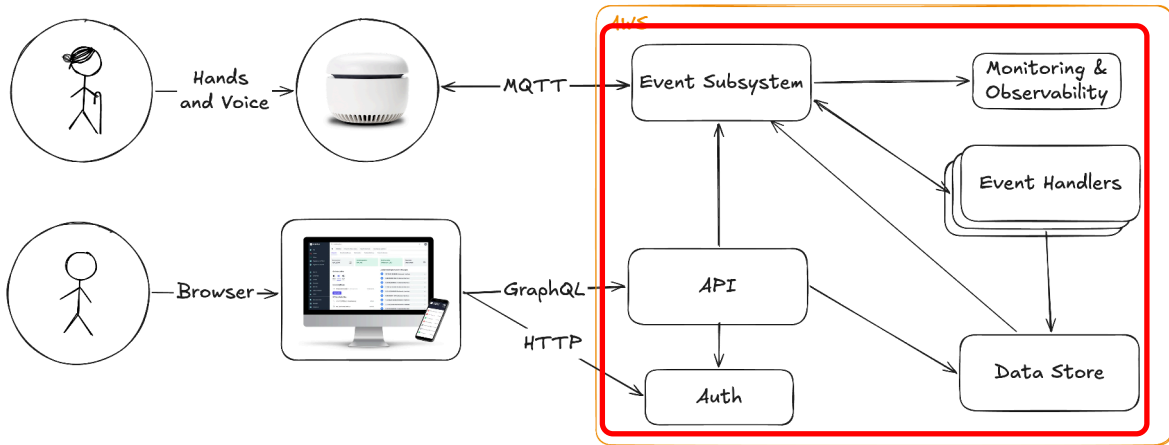


Where We Stand

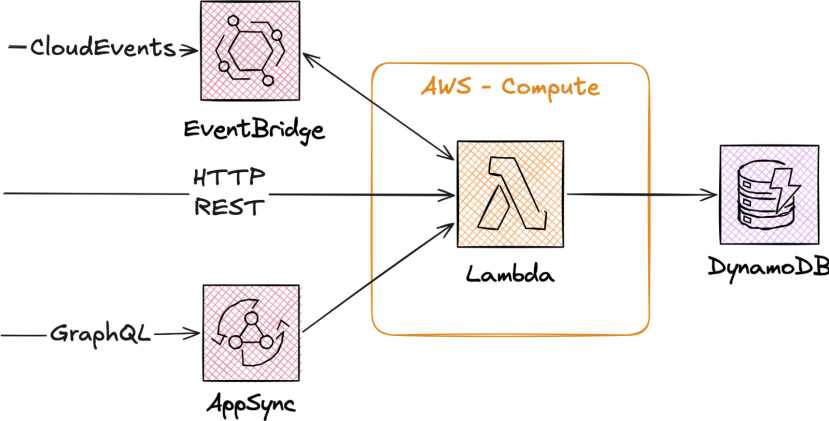
Area	API	Ideas	Candidate	Evaluated	Decided	Ready
Compute	Known (OCI, Kubernetes)	●	●	●	●	○
Event Subsystem	Exploring	●	●	○	○	○
Fleet Management	Exploring	●	●	●	●	○
Storage	Unchanged / Known (S3, ...)	●	●	○	○	○
Monitoring & Observability	Known (OpenTelemetry)	●	●	●	○	○
Authentication & Authorization	Known (OpenID Connect, ...)	●	○	○	○	○
Infrastructure & Hardware	Exploring	●	○	○	○	○
People & Processes	n/a	●	○	○	○	○

API: Exploring = no target standard yet · **Known** = target standard chosen, code changes once · **Unchanged** = already on the open standard, only the backend moves

The Compute Question

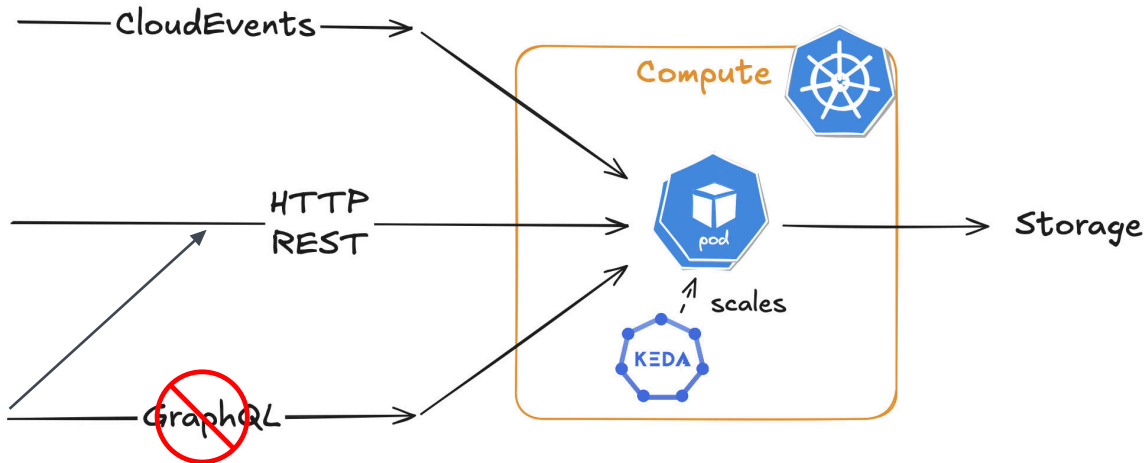


Compute on AWS



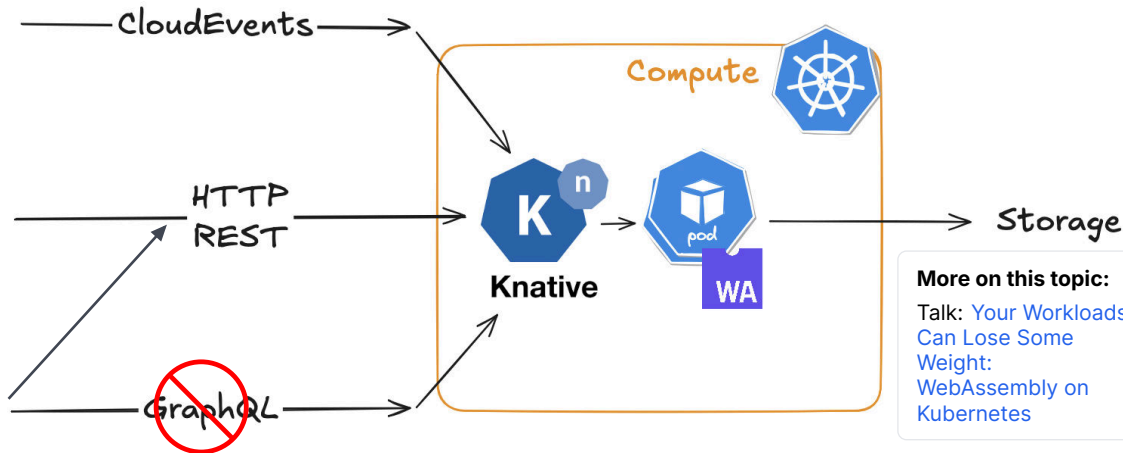
The Compute Answer: Kubernetes

1. Start with Kubernetes (EKS)
2. Move first services
3. Do scaling

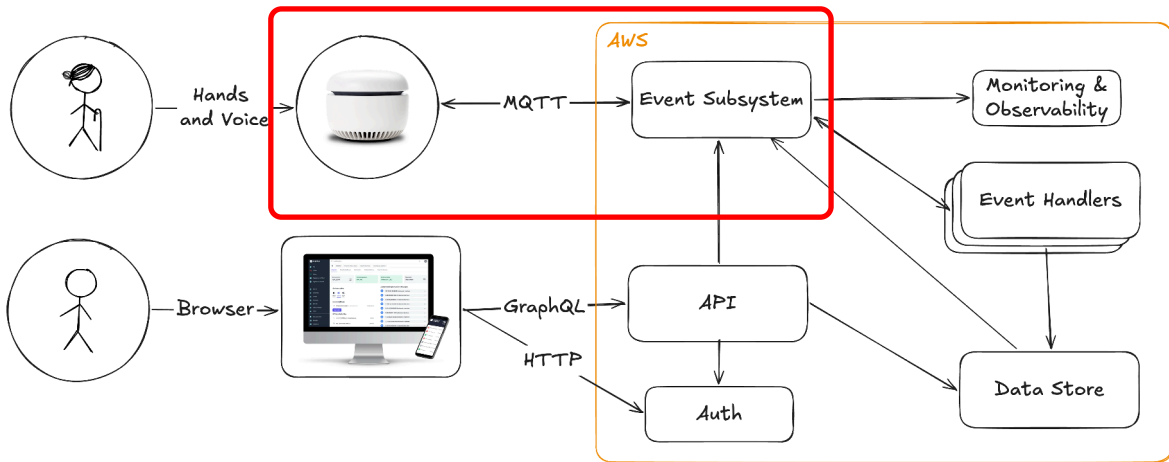


The Compute Answer: Kubernetes

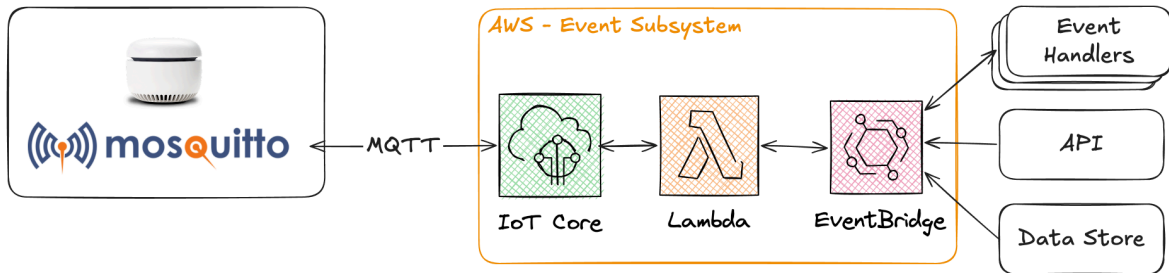
1. Start with Kubernetes (EKS)
2. Move first services
3. Do scaling
4. Do more



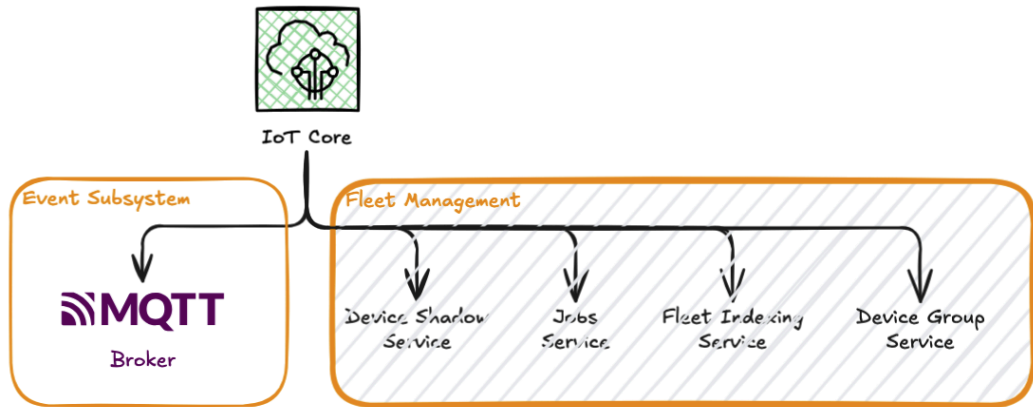
The Event Subsystem Question



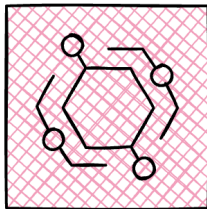
Event Subsystem on AWS



Device-to-Cloud on AWS



Intra-Cloud on AWS



EventBridge

The Candidates: Criteria and Tests

In
Progress

Criteria

- 1 OSI open-source license
- 2 Free for commercial use
- 3 Vendor-neutral foundation (tiebreaker)
- 4 Real clustering: active/active
- 5 Retained messages correct across the cluster
- 6 Small footprint

Target: RPO = 0 when a single node dies

Brokers

RMQTT

Single vendor (MIT)

comqtt

Single maintainer (MIT)

BifroMQ

Apache (Apache 2.0)

ActiveMQ Artemis

Apache (Apache 2.0)

NATS + JetStream

CNCF (Apache 2.0)

TBMQ

ThingsBoard (Apache 2.0)

Zilla + Kafka

Aklivity (source-available)

Kafka + Hono

Apache + Eclipse (Apache 2.0, EPL 2.0)

... and more

Test Cases

Standard Suites

Conformance (Eclipse Paho) · Load (emqtt-bench) · Fault (Toxiproxy, Pumba)

Retained

Cluster-wide · Burst + wildcard · Clear/overwrite

Session Handling

Resume same node · Resume cross-node · Client-ID takeover · Offline queue

Failover

QoS 0 outage · QoS 1/2 kill subscriber node · QoS 1/2 kill publisher node · Crash before ack

Last Will

Client death · Node death

Restart & Partition

Rolling restart · Full stop/start · Partition · Partition heal

Resources

Footprint · Backing store kill · Shared subscriptions

The Event Subsystem Answer: Three Approaches

In
Progress

1

One Broker to Rule them All

e.g.



2

Kafka + Protocol Adapter

e.g.



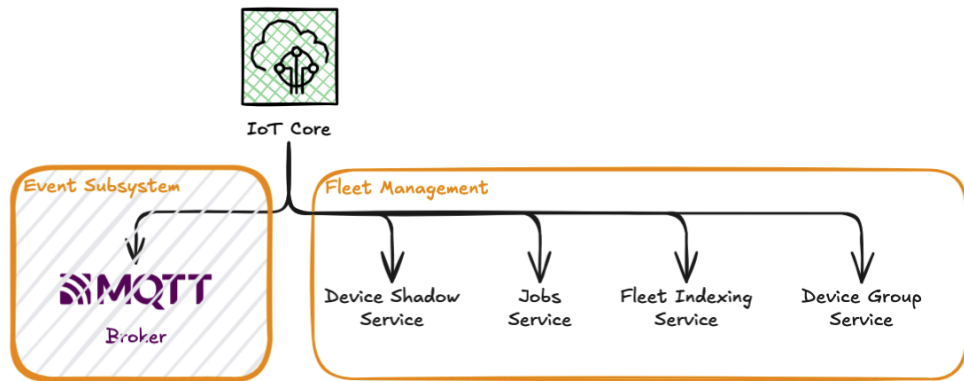
3

Keep It Simple

e.g.

HTTP + SSE
+ Event Store

Fleet Management on AWS



The Candidates: Fleet Management

IoT Management Platform	Maintainer	Device Shadow	Jobs	Fleet Index	Device Groups	Operational Overhead
Eclipse Ditto	Eclipse (EPL 2.0)	✓	⚠	⚠	⚠	Low
Eclipse Kapua	Eclipse (EPL 2.0)	⚠	✓	⚠	⚠	High
Eclipse hawkBit	Eclipse (EPL 2.0)	✗	✓	⚠	✓	Low
KubeEdge	CNCF (Apache 2.0)	✓	⚠	⚠	⚠	High
ThingsBoard	ThingsBoard (Apache 2.0)	✓	⚠	✓	⚠	High
Mender	Northern.tech (Apache 2.0)	✓	✓	⚠	⚠	High
OpenRemote	OpenRemote (AGPL 3.0)	⚠	⚠	✓	✓	Medium
Edgehog	SECO Mind (Apache 2.0)	⚠	✓	⚠	✓	High

✓ meets the requirement

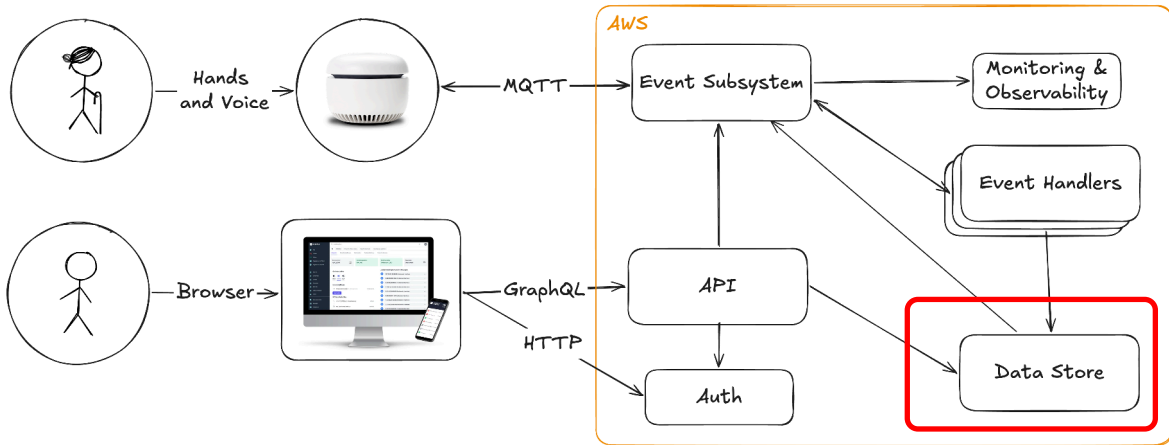
⚠ partial coverage

✗ not covered

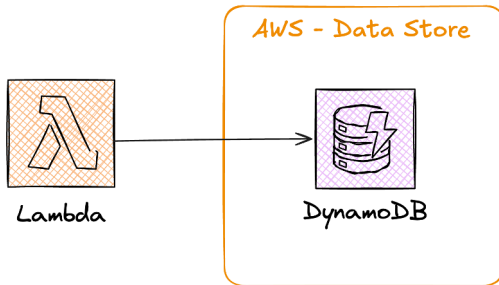
The Fleet Management Answer: DIY



The Storage Question



Storage on AWS



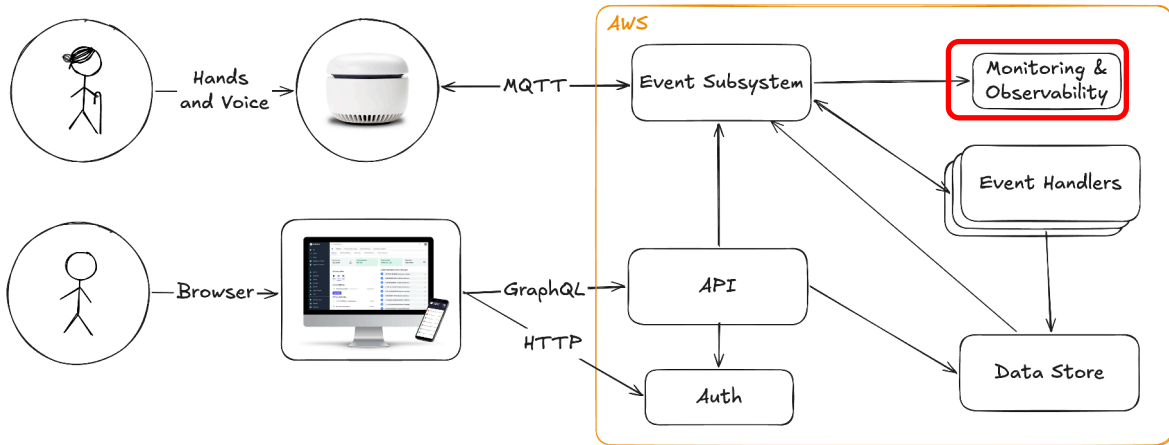
The Storage Answer: Abstraction

Or just take
what the sovereign
provider offers

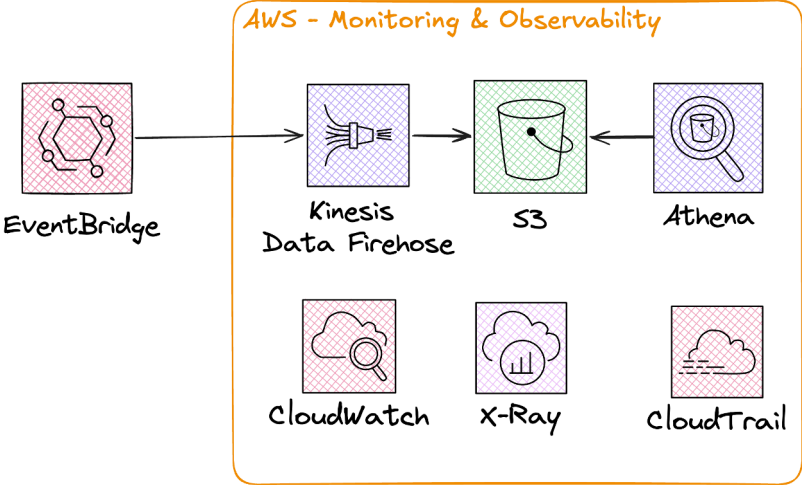
What	AWS (today)	Target Abstraction	Self-Hosted
Document Store	DynamoDB	CRUD + simple filters (avoid heavy ORMs)	Any DB that can store documents (e.g., Postgres, Cassandra, Valkey, NATS KV, ...)
Volumes	EBS	Files	Any Kubernetes Persistent Volume Provider (e.g., Rook + Ceph)
Blob Storage	S3	Basic S3 API	Any S3-compatible blob store (e.g., Ceph RGW, Garage, ...)

The API stays, the product is a deployment choice.

The Monitoring & Observability Question



Monitoring & Observability on AWS



The Monitoring & Observability Answer: OpenTelemetry

OpenTelemetry: one open standard for traces, metrics and logs, supported by all major tools

⇒ We just use what we know and what supports the standard.

What	API	Product	Owner	License
Collection	OTLP	OpenTelemetry Collector	CNCF	Apache 2.0
Traces, Logs	OTLP (via Collector)	OpenSearch	Linux Foundation	Apache 2.0
Metrics	OTLP, PromQL	Prometheus	CNCF	Apache 2.0
	PromQL	Grafana (UI)	Grafana Labs (only a UI, simple change)	AGPLv3
	PromQL (alert rules)	Alertmanager (alerting)	CNCF	Apache 2.0

And Don't Forget the Hard Stuff

- Authentication & Authorization
 - Authentication: great standards like OpenID Connect, OAuth2, SAML
 - Key management (PKI)
- Infrastructure & Hardware
 - Networking, physical redundancy, DNS, cellular connections
- People & Processes
 - Operations, backups & recovery
 - Certifications (e.g., C5 of the German BSI), audits
 - DevOps know-how
 - New vendor relations

Five Steps to Sovereignty

Decide

1 Do you need to be sovereign?

Start from your goals and constraints.

arc42 1 Goals · 2 Constraints · 10 Quality

2 How sovereign are you?

Measure the gap, start with the BSI C3A criteria.

arc42 10 Quality

3 Is the gap worth closing?

Cheap: clear components, APIs, open standards.

Harder: training, DevOps, 24/7 ops.

arc42 11 Risks

Act

4 Close the gap where needed

- Backups first (code, docs, pipelines, data).
- Then open standards and well-sliced components.
- Go fully sovereign only if required, and don't forget the people.

5 Validate and test it, regularly

- Restore your backups.
- Run a disconnect test (C3A SOV-4-09).

arc42 10 Quality: scenarios as tests



Conclusion: The Journey of CARU



BaselOne 2026

Kubernetes Saved My Grandma: High-Reliability IoT for Elderly Care



PRESENTER

Fabrizio Lazzaretti
Senior Managing Consultant
CNCF Ambassador

WAVESTONE



PRESENTER

Linus Basig
Head of Engineering

caru

<https://lazzaretti.me/baselone26>

Sources

Icons:

- Stick Figures by @Youri Tjang, [Excalidraw libraries](#)
- AWS Architecture Icons by @Anna Pastushko, [Excalidraw libraries](#)
- Kubernetes icons by @Nikola Markovic, [Excalidraw libraries](#)
- Database by @Stefan Oehrli, [Excalidraw libraries](#)
- Phosphor Icons, phosphoricons.com