

Ahmad Babaei

📍 Hamburg, Germany | ✉ babaeiamd@gmail.com | 🌐 ahmadbabaei.dev

🐙 github.com/ahmadbbi | 🔗 linkedin.com/in/AhmadBabaei | 📝 medium.com/@AhmadBabaei

Cloud Platform Tech Lead

Summary

Platform engineer and tech lead with **13 years in infrastructure**, the last 7 building cloud-native Kubernetes platforms on AWS and GCP with Terraform and Go/Python. Founding engineer of Graylog's multi-tenant SaaS platform: **100+ tenants, 2+ PB of customer data**, 4 regions on two clouds, run 24/7 at **99.99% availability**. Cut tenant onboarding from **3 days to 1 hour**, halved infrastructure cost, and reduced per-tenant cost **by up to 80%**. CKA and CKS certified.

Experience

Technical Leader

GRAYLOG · PROMOTED FROM SENIOR CLOUD ENGINEER IN 2024

04/2022 – Present

Hamburg, Germany

Founding engineer of Graylog's multi-tenant SaaS platform (**100+ tenants, 2+ PB**, AWS and GCP across 4 regions, **99.99% availability** target met and verified). Tech lead of the 6-engineer Cloud team: I set the platform's technical direction and stay hands-on from design through delivery.

- **Delivered strategic enterprise onboarding** — technical lead for a **10 TB/month** customer that required GCP: authored the deployment plan and delivered the multi-cloud stack and Cloud Infra API it depended on; recognized with the **Graylog Award for Ownership (2025)**.
- **Designed the Cloud Infra API** — Python async FastAPI control plane for the full multi-cloud tenant lifecycle; replaced direct Git reads by the autoscaler, CLI, and Jenkins with one centralized tenant state; unit and API behaviour tests (pytest, httpx) gate every merge alongside ruff and basedpyright checks.
- **Built self-service web console** — Litestar/HTMX front end for the Cloud Infra API with Okta SSO (OIDC + PKCE) and RBAC, used by Cloud, SRE, and Support teams for tenant onboarding and workflow tracking.
- **Re-architected AWS EKS** — Karpenter spot autoscaling and workload-placement strategy, with Terraform and Argo Workflows automation, cut tenant onboarding from **3 working days to 1 hour** and infrastructure cost **by half**.
- **Built tenant-lifecycle engine** — Argo Workflows orchestrating provisioning, parallel batch upgrades, and day-2 operations, delivered through Flux CD GitOps to every cluster on AWS and GCP; wrote the Go Kubernetes operator managing the GraylogApplication custom resource.
- **Engineered custom autoscaler** — prioritized horizontal and vertical scaling of Graylog and OpenSearch from journal, CPU, and heap signals, with asymmetric cooldowns to stop flapping; cut manual scaling work on call **by up to 85%**.
- **Owned infrastructure as code and network** — Terraform/Terraform across AWS and GCP (accounts, VPC, EKS/GKE, IAM, KMS); designed a multi-region AWS Transit Gateway hub giving one Client VPN entry point to every cluster.
- **Hardened platform security** — SOPS GitOps secrets with pre-commit guards, Kyverno admission policy protecting tenant cloud resources from accidental deletion, and quarterly AWS security reviews.
- **Cut per-tenant cost by up to 80%** — led the zero-downtime migration from AWS-managed to self-hosted OpenSearch, moved warm-tier storage from EBS to S3 with searchable snapshots, and tuned Graylog and OpenSearch JVM configurations.
- **Drove FinOps** — built the per-tenant cost model and OpenCost reporting with waste alerting; scoped self-service Trials with Product and shipped them on spot EKS at ~\$150/month (**60% cheaper**) per tenant (non-HA).
- **Ran reliability and on-call** — **24/7** incident response; designed multi-tier PagerDuty/OpsGenie alert routing, Thanos multi-cluster metrics, Filebeat/Auditbeat security telemetry, and quarterly backup-restore tests.
- **Set team standards and mentored** — authored **140+ technical documents** (design docs, runbooks, DR tests, policies), mentored the team, and advised product teams on deploying and scaling services on the platform.

AWS GCP Kubernetes Terraform Python Go Flux CD Argo Workflows

Skills

Languages Python, Go, Bash, Ruby

Kubernetes EKS, GKE, kOps, Karpenter, Docker, CRDs, Operators (Go)

GitOps Flux CD, Argo CD, Helm, Kustomize, tofu-controller

IaC Terraform, Terragrunt, Ansible, Packer

AWS EKS, EC2, VPC, Transit Gateway, IAM, S3, RDS, Lambda, ECS Fargate, ECR, MSK, KMS, Secrets Manager, Route 53, CloudTrail, GuardDuty, Inspector, Security Hub

GCP GKE, Compute Engine, Cloud DNS, IAM, Artifact Registry, KMS, Secret Manager, Workload Identity Federation

Testing pytest, pytest-asyncio, RSpec, SimpleCov, InSpec, ruff, basedpyright, RuboCop

CI/CD Argo Workflows, GitHub Actions, Jenkins, GitLab CI, Scaffold

Data PostgreSQL, MongoDB/Percona, OpenSearch, CockroachDB, Redis

Observability Prometheus, Thanos, Grafana, Alertmanager, Graylog, Loki, OpenTelemetry/Jaeger, PagerDuty, OpsGenie

Security SOPS, External Secrets, Sealed Secrets, cert-manager, Dex, Trivy, Kyverno, OIDC/RBAC

FinOps OpenCost, Kubecost, AWS Cost Explorer

AI/LLM OpenAI, Gemini, Llama, Claude, MCP, RAG

Awards & Certifications

Graylog Award for Ownership

Graylog · 2025

CKA - Certified Kubernetes Administrator
CNCF / Linux Foundation

CKS - Certified Kubernetes Security Specialist

CNCF / Linux Foundation

Education

M.Sc. Computer Engineering

Sharif University of Technology 2012 – 2014

B.Sc. Computer Engineering

Islamic Azad University 2008 – 2012

Senior Cloud Engineer

X-ION GMBH · PROMOTED FROM CLOUD ENGINEER

07/2019 – 03/2022

Hamburg, Germany

Founding member of the PaaS team: built managed Kubernetes and CockroachDB-as-a-Service from inception on self-managed OpenStack across 3 regions, for internal and external customers.

- **Co-built managed Kubernetes service** — kOps cluster lifecycle (Ruby cluster manager, Terraform, Argo Workflows), hardened Packer images with InSpec compliance, per-branch ephemeral dev clusters, and RSpec unit, e2e, and stress suites with on-cluster functional tests gating every cluster create and update; drove rolling upgrades from Kubernetes 1.14 to 1.21.
- **Authored Go Kubernetes operator** — kubebuilder controller giving each customer a self-service observability stack (Thanos, Loki, Grafana with alerting), reconciling 9 resource types with cert-manager TLS and per-component NetworkPolicies; led its v1alpha1 to v1alpha2 API migration.
- **Built CockroachDB-as-a-Service** — HA clusters spanning 3 OpenStack sites over a WireGuard mesh (Terraform/Ansible); zero-downtime node-by-node version and image upgrades, GPG-encrypted nightly S3 backups with restore runbooks, across 7 environments for 3 customers.
- **Owned platform GitOps for 30+ clusters** — Argo CD ApplicationSets and Kustomize overlays; introduced Dex OIDC SSO, Sealed Secrets, and cert-manager.
- **Built multi-tenant monitoring** — federated Prometheus with Thanos on S3, contributed to the Ansible MonitoringSet operator, wrote Ruby Prometheus exporters for cluster health, and extended Trivy image scanning across GitLab CI.
- **Authored platform design docs** — monitoring architecture, managed Kubernetes network topology (private nodes, bastion, L3 gateway), CockroachDB multi-region design with TPC-C capacity benchmarking, and an options analysis for self-hosted Jira Service Desk.

OpenStack Kubernetes Go GitLab CI Ansible Argo CD CockroachDB
Argo Workflows

System Engineer

MOBARAKEH STEEL COMPANY (MSC)

05/2013 – 06/2019

Isfahan, Iran

Largest steel producer in the Middle East, with **60,000+ users** across employees and contractors.

- **Containerized the web platform** — designed new infrastructure on Docker Swarm behind NGINX for internal web applications and microservices, with Jenkins and GitLab CI pipelines for development teams.
- **Automated WebLogic deployments** — built semi-continuous delivery for WebLogic 11g/12c applications with Bash, Python, and WLST.
- **Built logging and metrics** — ELK with Beats for centralized logs and TIG (Telegraf, InfluxDB, Grafana) for metrics and alerting.
- **Maintained core infrastructure** — RedHat and Ubuntu servers, Oracle WebLogic, Database, and Oracle Service Bus integration layer; ran internal YUM and Nexus repositories.
- **Automated operations** — built Ansible automation and on-call schedules.

Linux RedHat Docker Swarm Jenkins ELK Ansible Oracle