

Amin Amini

DevOps & Platform Engineer

Netherlands | [+31 6 47467979](tel:+31647467979) | m.a.amini2011@gmail.com | [LinkedIn](#) | [GitHub](#) | [Website](#)

Professional Summary

I spent five years on the NOC floor of a national payment network, watching what breaks at 3 a.m., then four years as a DevOps engineer making sure it would not break again. That path shapes how I build platforms: I design for the engineer who gets paged, not only the one who deploys. I do my best work where reliability, security and compliance are non-negotiable (payments, fintech, regulated SaaS), turning audit requirements and incident history into guardrails developers actually want to use.

Technical Skills

- **Cloud:** AWS (EKS, EC2, Lambda, API Gateway, SQS, DynamoDB, Route 53), Azure (AKS, Azure SQL), GCP (GKE Autopilot)
- **Containers & Orchestration:** Kubernetes, Docker, Docker Swarm, OpenShift, Helm, Karpenter, KEDA
- **IaC & CI/CD:** Terraform, Bicep, Ansible Tower, Argo CD (GitOps), GitHub Actions, GitLab CI/CD, Jenkins, AWS CodeDeploy
- **Observability:** Prometheus, Grafana, Loki, OpenTelemetry, Jaeger, ELK Stack, Zabbix, Manageengine, CloudWatch, X-Ray
- **Security & Compliance:** PCI DSS 4.0, Utimaco HSM, Least-Privilege IAM, Workload Identity, Kyverno, Azure Policy / Gatekeeper, SAST/SCA (Semgrep, Checkov, gitleaks), AWS WAF
- **Networking:** F5 Big-IP, AWS ALB, TLS termination, Load Balancing, Multi-site DR / Failover
- **AIOps:** LangGraph, LLM-based incident agents, AI observability
- **Languages & Scripting:** Bash, Python, SQL

Professional Experience

DevOps Engineer | SADAD PSP | Aug 2021 – Nov 2025

A leading Payment Service Provider in national banking infrastructure

- Maintained national payment services (internet gateways and mobile platforms) processing 20M+ daily transactions at >99.99% uptime, with PCI DSS 4.0 compliance through Utimaco HSM integration.
- Managed Docker Swarm and OpenShift workloads, reducing deployment times by 40%; automated provisioning with Terraform and Ansible Tower, cutting manual effort by 70%.
- Built a proprietary incident portal that reduced root cause analysis time for transaction failures from 2–3 days to under 30 minutes.
- Managed traffic routing, load balancing and TLS termination with F5 Big-IP, and maintained DR/BC strategies across multiple data centers.

- Partnered with government and enterprise clients to deliver billing-status and real-time transaction notification APIs (Nanino, BNPL).

NOC Engineer | SADAD PSP | Aug 2016 – Aug 2021

- Designed and ran 24/7 monitoring for national payment infrastructure (Zabbix, Grafana, ELK Stack, ManageEngine), reducing false alerts by 35% through tuned thresholds and alert correlation rules.
- Cut Mean Time To Recovery (MTTR) by 45% through streamlined log analysis (SQL, API traces) and automated RCA documentation.
- Reduced post-deployment rollback incidents by 25% by integrating live health-check dashboards into CI/CD pipelines.
- Automated monitoring tasks and incident escalations with Bash and Python, laying the groundwork for standardised incident response playbooks.
- Authored SOPs, DR monitoring plans and failover scenarios for switch and settlement services.
- Acted as the bridge between NOC and DevOps teams, and trained NOC engineers in metrics interpretation, log analysis and first-line automation.

Freelance Cloud & Platform Projects | Nov 2025 – Present

Payment Transaction Simulator (AWS, Serverless)

A card-payment authorization engine that reproduces how a real issuer approves or declines card transactions. ([Details](#))

- Implemented real ISO 8583 messaging, deterministic issuer decision logic and database-enforced idempotency, so a retried payment is never processed twice. Runs serverless on Lambda, API Gateway and SQS.
- Defense-in-depth security: AWS WAFv2, JWT authentication and Secrets Manager for all credentials.
- Safe releases through CodeDeploy canary deployments that roll back automatically when alarms fire; full observability with X-Ray tracing, dashboards and alarms; covered by 60+ automated tests.

Enterprise EKS Platform (AWS)

A multi-environment Kubernetes platform where every change ships through Git and must pass security checks before it reaches the cluster. ([Details](#))

- Provisioned multi-environment EKS with Terraform, delivered workloads with Argo CD GitOps, and enforced cluster standards with Kyverno policies.
- Built a blocking DevSecOps CI gate (gitleaks for secrets, Semgrep for code, Checkov for IaC): insecure changes cannot be merged.
- Combined Karpenter node autoscaling with a KEDA predictive autoscaler that scales on forecast traffic before the load arrives, instead of reacting after it.
- Designed and tested a multi-region disaster recovery proof-of-concept with DynamoDB Global Tables and Route 53 failover.

BidFlow — Self-Service Internal Developer Platform (GCP)

A platform that lets developers deploy Go and Ruby services to production on their own, with compliance built in by default. ([Details](#))

- One reusable Helm chart deploys services in either language on GKE Autopilot, with security and compliance guardrails baked in, enabling compliant deployments in under 3 minutes.
- Keyless push-based GitOps: GitHub Actions authenticates to GCP through Workload Identity Federation, so no long-lived service-account keys exist.
- End-to-end distributed tracing across Go and Ruby services with OpenTelemetry and Jaeger; Prometheus metrics drive HPA autoscaling under simulated high traffic.

Zero-Trust AKS Platform (Azure)

A private Kubernetes platform with nothing exposed to the internet and no stored passwords or keys, designed for payment-grade compliance. ([Details](#))

- Private AKS cluster with no public API server; workloads authenticate through Azure AD Workload Identity instead of static credentials.
- Azure Policy and Gatekeeper enforce security guardrails at deployment time.
- Tamper-evident audit trail with Azure SQL Ledger, mapped to PCI DSS 4.0 Requirement 10 (audit logging).
- Identical infrastructure defined in both Bicep and Terraform (IaC parity).

AIOps Incident-Investigation Agent (Kubernetes)

An AI agent that starts investigating a production incident as soon as an alert fires, so on-call engineers begin with findings instead of a blank screen. ([Details](#))

- LangGraph-based agent triggered by Prometheus / Alertmanager alerts, with strictly read-only access to the cluster.
- Paired with a Kubernetes security-audit pipeline (Grafana Alloy + Loki) that tracks RBAC changes and `kubectl exec` sessions.
- The agent's own runs are instrumented for AI observability, so every investigation can be traced and reviewed.

Certifications & Training

- Kubernetes Administration (CKA Preparation) – Anisa Academy (2024)
- PCI DSS 4.0 – IT-House (Jan 2024)
- AWS Training: Security Fundamentals (May 2025), Amazon EKS (Dec 2023), Cloud Essentials (Aug 2023)
- Full Stack Software Developer – IBM (Mar 2025)
- Linux (LPIC-1) – Laitec (Jun 2021)

Education & Languages

- **Bachelor of Software Engineering** (2014) — ACM/ICPC participant
- **Languages:** English (Fluent, C1) · Dutch (Elementary, A2, actively learning)