

YAZN ZAMEL

Software Infrastructure Engineer

Dual Citizenship (Canadian & Jordanian) | Mobile: +974 77 215 085 | Email: zamelyazn@gmail.com

PROFESSIONAL PROFILE

Software infrastructure engineer who designs and builds technical solutions on AWS and Azure, delivered both inside engineering organizations and directly for external clients in a professional services setting. Ships secure, highly available systems for production workloads, writes the automation and services behind them in code with Terraform, AWS CDK, and Python, and builds the release pipelines that carry them to production. Strong in observability and monitoring with Prometheus, OpenSearch, and ELK, with a consistent record of improving reliability, reducing operational cost, and shortening incident response times. Works comfortably across engineering teams, client stakeholders, and third party vendors to turn requirements into working solutions.

CORE SKILLS

Cloud Platforms: AWS, Azure (multi cloud)

CI/CD Pipelines: GitLab CI, Jenkins, AWS CodePipeline, Azure DevOps

Observability and Monitoring: Prometheus, Grafana, OpenSearch (ELK), Loki, Datadog

AI/ML Infrastructure: Model deployment and lifecycle management (GPU, AKS)

Security: IAM, zero trust access, OIDC, mTLS, SAST and DAST integration

Infrastructure as Code: Terraform, AWS CDK, Ansible

Containers and Orchestration: Kubernetes (CKAD), Docker, Helm

Reliability and RCA: Root cause analysis, post mortems (CoE), on call support

Data Systems: Queuing (SQS), streaming (Filebeat), SQL, NoSQL, vector databases

Client Facing: Stakeholder management, vendor collaboration, solution documentation

PROFESSIONAL EXPERIENCE

Amazon

Sep 2024 to Present

Software Infrastructure Engineer , L5

- **Deployment architecture:** Architected and led the implementation of a one box canary deployment strategy using AWS CDK and CodePipeline, replacing a high risk monolithic all at once release model.
- **Risk and impact reduction:** Reduced the potential incident impact radius from 100% of users to 1% on initial rollout, eliminated customer impacting deployment incidents, and brought deployment MTTR down to 5 minutes.
- **Security architecture (identity):** Designed a zero trust access model for a 30TB production OpenSearch cluster, resolving a critical vulnerability that allowed anonymous corporate access.
- **Security solutioning (OIDC):** Designed and integrated an OIDC based authentication solution using AWS Cognito and ALB to restore secure, auditable log access for 30 plus engineers, reducing troubleshooting time by roughly 40%.
- **Security architecture (application):** Architected a secure Lambda proxy solution to close a critical vulnerability that exposed 28,000 sensitive user accounts through an unauthenticated internal testing framework.
- **Business enablement:** Removed the security risk by enforcing IAM based authentication, unblocking 120 plus test cases for critical Spay and Gpay programmes and saving 290 plus manual QA hours per regression cycle.
- **Observability solution:** Designed and implemented a centralised multi account hub and spoke logging architecture on AWS OpenSearch, SQS, and Filebeat to ingest and normalise ALB, CloudTrail, and EC2 logs.
- **Cost and performance optimisation:** Reduced incident MTTR through a unified observability platform and achieved a 50% reduction in logging operational cost through optimised capacity planning.
- **Monitoring strategy:** Defined a data informed observability framework for Tier 1 services following a critical SSL related outage, replacing noisy machine learning alarms with calibrated static CloudWatch alarms.
- **Operational excellence:** Cut critical issue detection time from hours to 5 minutes and reduced false positive alert tickets by 74%, from 38 to 10, in a single cycle.

- **Vendor and stakeholder management:** Led a complex security implementation to design and validate a mutual TLS authentication model, working directly with Cloudflare solution architects to establish a new reusable security pattern for internal teams.
- **Application modernisation:** Led the migration of legacy EC2 based applications to containerised workloads on AWS ECS, delivering material cost reduction and improved resource utilisation.
- **Hybrid cloud:** Architected and managed hybrid cloud deployments on AWS Outposts, enabling low latency processing for on premises applications while integrating with AWS cloud services.

PwC (PricewaterhouseCoopers)

Aug 2022 to Sep 2024

Software Infrastructure Engineer , Associate

- **Client delivery:** Delivered cloud engineering work for internal firm platforms and external client engagements, gathering requirements from client stakeholders, presenting architecture options, and handing over documented, supportable environments.
- **AI platform engineering:** Built and managed scalable infrastructure for AI model deployment and lifecycle management, including GPU optimised Azure Kubernetes Service clusters (NVadsA10 v5) for high traffic production environments.
- **Infrastructure as code:** Developed and standardised reusable Terraform modules for automated provisioning on Azure, giving delivery teams consistency and a faster path to scale.
- **CI/CD and security integration:** Owned the full CI/CD lifecycle on Azure DevOps Server with automated pipelines across dev, staging, and production. Managed custom build runners for Windows and Linux containerised applications, integrated Azure Key Vault for secret and configuration management, and embedded SAST (SonarQube) and DAST (OWASP ZAP) scanning into pipelines.
- **Cost optimisation:** Optimised cloud resources for scalability and efficiency, driving a \$700K annual reduction in Azure spend, a 23% saving.
- **Observability platform:** Deployed a full observability stack on Prometheus, Loki, and Grafana to centralise monitoring and production logs across multiple applications and environments. Used PromQL and Node Exporter for system metrics, built custom JSON log parsers for Loki to enable rich querying, and produced dashboards correlating system health, logs, and model performance.
- **GenAI platform architecture:** Architected a secure multi tenant GenAI platform on Azure, integrating a full stack of services for production applications.

CERTIFICATIONS

AWS Solutions Architect Professional (SAP)

AWS Developer Associate (DVA)

AWS Solutions Architect Associate (SAA)

Kubernetes and Cloud Native Associate (KCNA)

CompTIA Linux+

Linux Foundation Certified System Administrator (LFCS)

Certified Kubernetes Application Developer (CKAD)

EDUCATION

Princess Sumaya University for Technology, Bachelor of Software Engineering