Elmoge Abukar

| 619-218-9567 | abukar5150@gmail.com | linkedin.com/in/eabukar | github.com/elnana93

Cloud Infrastructure / DevOps Engineer (Serverless • Kubernetes • Terraform • CI/CD)

SUMMARY

Cloud Infrastructure Engineer with 8+ years of experience building and operating secure, scalable platforms across AWS and GCP. Strong background in Terraform, Kubernetes (EKS/GKE), CI/CD automation, observability, and production operations, including on-call support, incident response, root cause analysis, and runbook development. Proven ability to improve reliability, standardize infrastructure, and support secure, repeatable delivery in regulated and high-availability environments.

Technical Skills

Cloud Platforms:

AWS (EKS, EC2, VPC, IAM, Route 53, ACM, ALB/NLB, RDS, S3, Lambda, CloudWatch, Secrets Manager, SSM, SNS, KMS),

GCP (GKE, VPC, IAM, Cloud SQL, BigQuery, Pub/Sub, Cloud Storage, Cloud Run, Cloud Functions, Cloud Monitoring, Cloud Logging, Cloud Build, Secret Manager, KMS)

Infrastructure as Code - Terraform (modules, workspaces, remote state, state locking, reusable patterns, drift remediation, environment isolation), CloudFormation (familiar)

CI/CD & Version Control - GitHub Actions, Jenkins, GitLab CI, Cloud Build, pipeline automation, Git workflows, branch-based delivery

Containers & Kubernetes - Kubernetes (EKS/GKE), Helm, Docker, Ingress, load balancing, cluster upgrades, node pools, workload deployments

Networking & Security - VPCs, subnets, route tables, security groups, NACLs, DNS, Route 53, TLS/SSL, IAM, RBAC, Secrets Manager, SSM Parameter Store, KMS, network segmentation

Observability & Operations - CloudWatch, Cloud Monitoring, Cloud Logging, Prometheus, Grafana, alerting, dashboards, health checks, incident response, root cause analysis, runbooks, production support

Systems & Scripting - Linux, Windows, Bash, PowerShell, basic Python

---

PROFESSIONAL EXPERIENCE

Independent Cloud & Web Infrastructure Consultant | Jan 2025 – Present
Part-time / Project-Based

- Partner with consultants and small business owners to design and launch web platforms aligned to their service model, customer workflow, and business goals.
- Build static websites for service-based businesses to improve branding, credibility, and lead generation.
- Develop portal-style solutions for staffing and operations-focused businesses to support intake, scheduling, document collection, and communication workflows.
- Tailor web solutions across industries including staffing, retail, and professional services based on client-specific operational needs.
- Manage hosting, DNS, SSL, domain configuration, and deployment setup to deliver secure, reliable, and production-ready web environments.
- Translate business requirements into practical technical solutions, balancing usability, maintainability, cost, and speed of delivery.

Cloud Infrastructure / CloudOps Engineer | Solio | Clean Energy / ClimateTech | Sep 2025 – Apr 2026
Remote

- Built and maintained multi-cloud infrastructure across AWS and GCP using Terraform, improving deployment consistency and reducing manual provisioning for engineering and application workloads.
- Designed reusable Terraform modules, remote state configurations, and environment-isolated infrastructure patterns to improve consistency and reduce deployment risk.
- Provisioned and managed core cloud services including networking, IAM, compute, storage, managed databases, DNS, secrets management, and monitoring.
- Configured cloud networking components such as VPCs, subnets, route tables, security groups, firewall rules, and service connectivity to support secure internal communication and application access.
- Implemented least-privilege IAM controls, role-based access patterns, and secure secrets handling practices to strengthen overall cloud security.
- Automated infrastructure delivery through GitHub Actions, Jenkins, and cloud-native CI/CD tooling, reducing manual deployment steps and improving release consistency across environments.
- Supported containerized and Kubernetes-based workloads, including infrastructure and operational patterns related to EKS and GKE.
- Improved monitoring, alerting, logging, and health-check workflows, increasing operational visibility and reducing time spent troubleshooting infrastructure and deployment issues.
- Investigated and resolved infrastructure, deployment, and platform issues, improving reliability and reducing operational friction.

Access2Care — NEMT
Cloud Engineer (AWS / IaC / Security) | Mar 2022– Jan 2025

- Co-owned Terraform infrastructure for production AWS environments, maintaining remote state, state locking, drift prevention, and controlled production changes.
- Secured RDS by deploying databases in private subnets with tightly scoped security groups, eliminating public exposure.
- Enforced least-privilege IAM access for workloads, restricting runtime permissions to required Secrets Manager retrieval and specific SSM Parameter Store paths.
- Implemented automated RDS credential rotation using AWS Secrets Manager and a rotation Lambda, reducing reliance on long-lived static credentials.
- Updated application configuration to retrieve credentials dynamically and validated service stability through CloudWatch logs, alarms, and health checks.
- Built reliability guardrails by alarming on ALB 5xx spikes with CloudWatch and SNS and linking alerts to runbooks for faster incident response.
- Standardized reusable Terraform patterns for core AWS resources to improve consistency, repeatability, and change safety across environments.
- Monitored infrastructure and application health using CloudWatch metrics, logs, and alarms to improve visibility and accelerate troubleshooting.

Cloud Engineer (Contract, Part-Time) / AWS Consultant — Managed Web Operations
2018-2021

- Managed AWS-hosted static/lightweight websites for multiple SMB clients on monthly retainers (S3, CloudFront, Route 53, ACM), delivering secure, fast, reliable public-facing sites.
- Owned DNS + HTTPS end-to-end (registrar/Route 53 cutovers, ACM lifecycle, redirects, cache behaviors), minimizing downtime and preventing certificate-expiry incidents.
- Hardened environments with secure-by-default controls (S3 Block Public Access, OAC/bucket policies, least-privilege IAM) and standardized release playbooks (deploy steps, invalidations, rollback).
- Delivered ongoing ops as the accountable owner: monitoring/alerts, incident response, maintenance, and cost guardrails (S3 lifecycle/retention, budget alerts).

CERTIFICATIONS
AWS Certified Solutions Architect – Associate *(In Progress)*