Kiran Garud

DevOps Engineer

• Pune, India • +91-8446484854 • kgarud30@gmail.com

• LinkedIn: linkedin.com/in/kiran-garud-ab4674205 • GitHub: github.com/kirangarudofficial

PROFESSIONAL SUMMARY:

Early-career **DevOps Engineer** with strong hands-on experience designing and operating **production-style cloud-native platforms as learning initiatives**, using **AWS, Kubernetes, CI/CD, Infrastructure as Code, and observability tools**. Demonstrates a solid foundation in **system reliability, deployment automation, monitoring, security controls, and performance optimisation**, with an understanding of **risk, change management, and operational discipline** expected in regulated enterprise environments. Motivated to grow within a structured DevOps or Site Reliability Engineering team under experienced guidance

CORE TECHNICAL SKILLS:

- **DevOps & CI/CD**: CI/CD Pipelines, Jenkins (Shared Libraries), GitHub Actions, GitOps (ArgoCD), Build & Release Automation, Configuration Management
- **Containerization & Orchestration**: Docker, Kubernetes (EKS), Helm, Kustomize, Rolling & Blue-Green Deployments, HPA, StatefulSets, Namespace Isolation
- **Cloud & Infrastructure**: AWS (EKS, EC2, VPC, IAM, S3, RDS, Lambda, DynamoDB, CloudFront, ECR), Azure (AKS – foundational), GCP (foundational)
  Infrastructure as Code: Terraform, CloudFormation, Ansible
- **Observability & Monitoring**: Prometheus, Grafana, Alertmanager, Fluent Bit, ELK Stack, AWS CloudWatch, Log & Metric Analysis
- **Security & Controls**: IAM Least Privilege, Secrets Management, Container Vulnerability Scanning (Trivy), Network Policies, TLS/SSL, Pod Security Standards
- **Scripting & Automation**: Python, Bash, YAML, JSON
- **Operational Focus (ATS Keywords)**: System Reliability, Availability, Performance Monitoring, Incident Prevention, Root Cause Analysis (learning-based), Capacity Planning, Cost Optimisation

PROJECT EXPERIENCE

Cloud-Native Learning Hub Platform

Independent, Production-Style DevOps Project

AWS | Kubernetes | CI/CD | GitOps | Observability | Security

Designed and implemented a cloud-native learning platform as an independent engineering initiative, with the objective of understanding DevOps practices, distributed systems, automation, observability, and secure cloud operations. The project was intentionally built using production-style architecture and tooling, while remaining a non-commercial, non-regulated environment to safely explore complexity and operational trade-offs.

- **DevOps & Platform Engineering:**
  Designed a Kubernetes-based platform (Amazon EKS) to deploy and manage backend services and supporting components, focusing on workload isolation, deployment consistency, and resource governance using namespaces, resource limits, and network policies.
- **CI/CD & Automation:**
  Implemented CI/CD pipelines using Jenkins and GitHub Actions to standardise build, test, containerisation, security scanning, and image publishing workflows, reducing manual effort and improving deployment reliability.
- **GitOps & Change Management:**
  Practiced GitOps-based continuous deployment using ArgoCD to manage application state declaratively, enabling controlled rollouts, rollback capability, and configuration drift detection.
- **Infrastructure as Code:**
  Automated cloud infrastructure provisioning using Terraform and Ansible, enabling repeatable, auditable, and cost-aware environment creation aligned with Infrastructure-as-Code principles.
- **Reliability & Monitoring:**
  Established centralised observability using Prometheus, Grafana, Alertmanager, and structured logging to monitor

application health, infrastructure performance, and service behaviour, supporting early detection of failures and performance bottlenecks.

- **Operational Readiness:**
  Implemented health checks, readiness probes, and monitoring dashboards to understand service availability, dependency behaviour, and recovery patterns in a distributed environment.
- **Performance & Capacity Awareness:**
  Performed performance-tuning exercises using resource requests/limits and autoscaling configurations to study capacity planning and system stability under varying load.
- **Data & Stateful Workloads:**
  Deployed and managed containerised databases and stateful services using Kubernetes StatefulSets with persistent storage, backups, and controlled service access to understand data reliability, recovery, and isolation patterns.
- **Security & Risk Awareness:**
  Applied security-first DevOps practices, including IAM least-privilege access, secrets management, container vulnerability scanning, secure ingress configuration, and network segmentation to reduce blast radius and improve platform safety.
- **Collaboration Readiness:**
  Maintained documentation, self-review practices, and operational notes to simulate handover readiness, maintainability, and team-based operational clarity.

Scope Note:

This project was intentionally scoped as a production-style learning environment built independently to gain hands-on experience with enterprise DevOps patterns. It was not a commercial system, did not serve real customers, and did not operate under regulatory or business SLAs.

CERTIFICATIONS & EDUCATION

- AWS Certified Solutions Architect – Associate (Aug 2023 – Aug 2026)
- Diploma in AWS with Python – 3RI Technologies Pvt Ltd. (2024)