

PAVANI KODURU

+91 6302046783 | Gudur, Tirupati | pavanikoduru06@gmail.com | <https://www.linkedin.com/in/pavani-koduru-869997325/>

PROFILE SUMMARY

DevOps Engineer with 2+ years of hands-on experience in designing, deploying, and managing scalable applications on AWS Cloud and DevOps toolchains. Skilled in CI/CD pipeline automation, Infrastructure as Code (Terraform, CloudFormation), containerization (Docker, Kubernetes EKS), and configuration management (Ansible, Chef). Strong experience in monitoring, performance optimization, and troubleshooting using Prometheus, Grafana, and AWS CloudWatch. Basic knowledge of Azure Cloud services including Virtual Networks, IAM, and DevOps pipelines. Demonstrates strong communication and problem-solving skills with a commitment to DevOps best practices, security compliance, and agile teamwork.

KEY SKILLS

- Cloud Platforms: AWS (EC2, S3, IAM, VPC, RDS, Route53, Lambda, CloudFormation, CloudWatch, CloudTrail), Azure (VMs, VNet, IAM, DevOps, Key Vault, RBAC, Serverless)
- CI/CD & DevOps Tools: Jenkins, Git, GitHub, GitHub Actions, Azure DevOps (Basics)
- Infrastructure as Code (IaC): Terraform, AWS CloudFormation, ARM Templates (Basics)
- Configuration Management: Ansible, Chef
- Containerization & Orchestration: Docker, Kubernetes (EKS), Helm
- Monitoring & Logging: Prometheus, Grafana, AWS CloudWatch
- Web/App Servers: Nginx, Apache, PM2
- Programming & Scripting: Python, Shell Script, YAML
- Databases: MySQL, PostgreSQL
- Networking: TCP/IP, DNS, Load Balancers, Firewalls, VPC, Subnets, Route Tables
- Operating Systems: RedHat 7, CentOS 7, Ubuntu (20/22/24), Windows
- Security & Compliance: IAM roles, MFA, Security Groups, NACLs, WAF, DevSecOps practices, SonarQube, OWASP Dependency Check, SAST

PROFESSIONAL EXPERIENCE

DevOps Engineer | Codetez Technologies

Chennai Feb 2025 – April 2025 | Project: Canny Minds

Environment: AWS, Node.js, PNPM, PM2, Nginx, mkcert, Ubuntu, Docker, Ansible, Prometheus, Grafana

- Deployed and managed Node.js applications using PNPM and PM2 for service management.
- Configured SSL certificates (mkcert) and secured reverse proxy with Nginx.
- Automated environment provisioning with Ansible playbooks for consistent and repeatable infrastructure setup.
- Containerized applications using Docker and integrated with AWS EC2 instances for scalable deployments.
- Implemented monitoring dashboards using Prometheus and Grafana to track application and infrastructure health metrics.
- Resolved DNS misconfigurations, SSL/TLS handshake errors, and optimized Nginx for high traffic workloads.
- Implemented Infrastructure as Code using Terraform and Ansible for automated environment provisioning. Enhanced container orchestration by managing Kubernetes/EKS clusters, Helm charts, and service discovery.
- Designed and enabled centralized logging using ELK stack for efficient troubleshooting and observability.
- Enforced best security practices by managing IAM roles, policies, and secrets with AWS Secrets Manager.

- Automated CI/CD pipelines with GitOps principles using GitHub Actions integrating Kubernetes deployments.
- Collaborated closely with development and QA teams to facilitate high-quality automated testing and artifact management.
- Automated backup and disaster recovery processes using AWS native tools.
- Ensured patch management and vulnerability scanning compliance aligned with corporate security policies.

Associate DevOps Engineer | Capgemini Technology Services, Chennai

Sept 2022 – Aug 2024 | Project: 5G OAM NETCONF

Environment: AWS (EC2, VPC, IAM, CloudFormation), Terraform, Jenkins, GitHub, Python, CloudWatch, Docker

- Provisioned secure and compliant AWS infrastructure using Terraform and CloudFormation templates with multi-tier VPC designs.
- Designed robust IAM policies, Security Groups, and Network ACLs to harden cloud infrastructure security.
- Built and optimized CI/CD pipelines using Jenkins and GitHub for automated building, testing, and deployment cycles.
- Containerized 5G network services using Docker for consistent and repeatable deployments across environments.
- Integrated NETCONF protocol with Python scripts for automated device configuration and real-time monitoring.
- Developed monitoring solutions leveraging AWS CloudWatch, Prometheus, and Grafana to ensure high system availability and responsiveness.
- Automated routine health checks and incident response actions using Python and Shell scripting.
- Collaborated with security teams to integrate security scanning tools such as SonarQube and OWASP Dependency Check in pipelines, promoting DevSecOps culture.
- Developed reusable Terraform modules standardizing provisioning of networks, compute, and storage resources.
- Monitored system health via Prometheus Alertmanager and CloudWatch alarms, ensuring prompt incident detection and resolution.
- Authored comprehensive deployment documentation, infrastructure runbooks, and knowledge base articles to support operations and audits.
- Designed VPC architectures with private/public subnets, NAT gateways, route tables, and load balancers to support high availability and scalability.
- Conducted root cause analysis and troubleshooting of production issues using centralized logging and monitoring tools.
- Hardened container security by managing Kubernetes RBAC, network policies, and image vulnerability scans.
- Improved container image builds using multistage Dockerfiles and implemented automated image versioning pipelines.

EDUCATION

Bachelor of Technology (B.Tech) – Computer Science & Engineering

JNTUA University | Graduated: July 2022 | Aggregate: 77.35%