

Deepak Kumar

+91-9120088883 Bengaluru, Karnataka

apsdeepakkumar270501@gmail.com linkedin.com/in/apsdeepak/

EDUCATION

Bachelor of Technology (Computer Science), Lovely Professional University
CGPA - 7.89

2019 - 2023

Jalandhar, Punjab

Senior Secondary School (Mathematics), Army Public School Nehru road
Score - 81.2%

2018 - 2019

Lucknow, Uttar-Pradesh

EXPERIENCE

Software Engineer I - DevOps

Sigtuple Technologies Pvt. Ltd.

Oct 2022 - Ongoing

Bengaluru, Karnataka

- Created a full-fledged, production-ready infrastructure for the “Anemia Mukht Bharat” & “Cyber-security audits” project on **GCP**, leveraging **Docker**, **Kubernetes (GKE)**, **Ansible playbooks**, **Docker Compose**, **Nginx**, **VM and node pool configuration**, while managing **multiple microservices**, configuring **DNS for each service**, integrating **Cloud Storage**, and administering **MongoDB and MySQL databases** to enable efficient deployment, scalability, and reliable application management.
- Designed and implemented a **CI/CD pipeline** using **Jenkins for continuous integration**, **Docker for building application images**, and **GCP Artifact Registry** for secure image storage, enabling automated build, versioning, and deployment of containerized applications.
- Owned the **release management process** for both **production and non-production environments**, successfully delivering multiple releases with controlled rollouts, validation checks, and zero-downtime deployment strategies.
- Achieved 40% cost reduction on GCP through strategic resource scheduling and utilization limits.
- Successfully managed Kubernetes clusters, achieving an average resource utilization rate of 80%. Ensured 99.99% uptime for critical workloads, minimizing downtime and maintaining uninterrupted availability for end-users.
- Successfully managed services on product/devices through Docker Compose, optimizing resource allocation by 30%, simplifying deployment by 40%, and achieving a 25% decrease in service-related incidents.
- Effectively scheduled cluster node size and VM instances to automatically downscale after 10 pm and start them at 9 am on weekdays for non-production projects, leading to a 50% reduction in cloud infrastructure costs during off-peak hours.
- Proactively resolved **production-level DevOps issues** across **networking**, **IAM permissions**, **Kubernetes pods**, **services**, **nodes**, **CI/CD pipelines**, and **database connectivity**, ensuring high system reliability, faster incident resolution, and minimal downtime.
- Successfully designed and implemented a robust continuous integration (CI) pipeline using CircleCI, resulting in a 50% reduction in build and deployment time.
- Technologies used - **Docker**, **Google Kubernetes Engine**, **Google Cloud Platform (GCP)**, **Jenkins**, **Ansible**, **Docker-Compose**, **containerization**, **GitOps**, **Continuous Integration and Continuous Deployment (CI/CD)**, **Configuration-management**, **Yaml**, **Git**, **Linux**, **Python**, **Cloud Cost-optimisation**, **Infrastructure as code (IaC)**, **BASH**, **Cloud Storage & Databases**, **Secrets Management**, **Monitoring**, **Google-analytics (GA-4)**

Certifications

- DevOps MasterClass - GIT Docker Jenkins Kubernetes Terraform - Udemy - Ongoing
- Modern big Data Analysis with SQL specialization
- Programming Using c++ (CipherSchools)
- Python for Everyday Specialization

TECHNICAL SKILLS

Languages: C, C++, Python, HTML/CSS, Javascript, bash scripting

Tools : Docker, Docker-Compose, Google Kubernetes Engine (GKE), Google Cloud Platform(GCP), Jenkins, Ansible, Helm, GitHub Actions, Playbooks, Containerization, Service Mesh: Istio

Cloud Networking: VPC DNS, Subnet, firewall rules, Cloud-Security Interconnect, VPN

Database Management: MySQL, MongoDB

Development Methodology : Agile, Waterfall, DevOps, Event Driven Architecture, CI/CD, DDD, TDD,

Networking : Nginx

Security: SSL/TLS Certificate Management

Miscellaneous: Linux, Unix, Git, Tableau, Microsoft Excel, Jira, Confluence, Slack

ACHIEVEMENTS

- Remediated cloud infrastructure vulnerabilities flagged in an external security audit, strengthening product security and compliance