Ravindra Kumar GS, Principal SRE

229/1, Sri Nivasa, Puranik Road, Ward 4, Near Bharat Petrol Bunk, Thekkatte, Kundapura, Udupi District, Karnataka State, 576231, India, +916366666445, ravindrags24@gmail.com

PROFILE

Dynamic Principal SRE with 18 years of comprehensive experience in streamlining cloud operations and enhancing system reliability. Expertise in CI/CD pipeline optimization, Infrastructure as Code using Terraform, and advanced AWS architecture management drives significant improvements in resource utilization and operational efficiency. Proficient in diagnosing and resolving production issues rapidly, ensuring minimal service interruptions while fostering a culture of knowledge sharing through meticulous documentation. Committed to implementing robust backup and disaster recovery protocols, safeguarding data integrity and supporting organizational objectives. Eager to leverage extensive technical knowledge and leadership capabilities to further elevate cloud infrastructure performance.

EMPLOYMENT HISTORY

May 2019—Present — Principal SRE, Prognos India Health Private Limited — Bangaluru, Karnataka

- Streamlined CI/CD pipelines leveraging Git.
- Terraform for Infrastructure as Code (IaC) facilitating efficient cloud resource management. (AWS)
- Enhanced cloud architecture on AWS, achieving improved resources utilization.
- Efficiency diagnosed deployment failures and production issues, ensuring minimal service interruptions with rapid resolutions.
- Created detailed documentation for processes and systems to foster knowledge sharing and align with best practice.
- Executed automated backup and disaster recovery plans, guaranteeing data integrity.
- Working on documentation for SOC2 preparation to company.
- Preparing SOP and tracking as per requirements.

Dec 2014—Apr 2019 — Senior System Admin, Impelsys India Pvt Ltd — Bengaluru, Karnataka

- Oversaw AWS server management to assure peak performance and scalability for uninterrupted application operation.
- Configured and managed on-premise Linux servers to facilitate application deployment and data storage requirements.
- Administered Rackspace remote servers, managing the installation of applications and timely upgrades for improved functionality.
- Utilized monitoring tools to enhance server performance and address operational challenges swiftly.
- Analyzed server logs and performance metrics to proactively identify and mitigate potential issues.
- Tweaked server configurations to boost system efficiency while minimizing downtime.

Jan 2014—Dec 2014 — SRE, Jool Technologies — Bengaluru, Karnataka

- Assessed network performance and availability, executing proactive strategies to reduce downtime and optimize user experience.
- Configured AWS servers to maximize resource allocation and maintain high efficiency within a dynamic cloud setting.
- Introduced automated monitoring solutions to enhance incident response and boost overall system reliability.
- Followed configuration management best practices to ensure system compliance and consistency with organizational standards.
- Enhanced server security through the implementation of best practices and systematic audits, lowering potential vulnerabilities.

Feb 2008 __Dec 2014 System Admin, Impelsys India Pvt Ltd Bengaluru, Karnataka

- Oversaw server environments to guarantee peak performance, availability, and adherence to security standards.
- Configured networking devices and systems to enable seamless communication and effective data transfer across teams.
- Managed user accounts and permissions, ensuring adherence to company policies and security measures.
- Implemented backup and recovery protocols to protect essential data from loss due to system failures or Cyber threats.
- Conducted system performance monitoring and analyzed network traffic to identify issues before affecting operations.
- Utilized effective troubleshooting techniques to resolve user-reported technical issues promptly.

Present work achievements: TechOps Manager Portal (Vue 3, Python, AWS Serverless, Terraform, GitHub CI/CD)

- Architected a serverless internal ops platform (API Gateway + Lambda + DynamoDB) consolidating TechOps workflows across 5 AWS accounts, eliminating ad-hoc console access.
- Designed zero-trust auth layer with Cognito JWT/JWKS verification, DynamoDB feature-flag whitelist, and 90-day audit logging — enforcing least-privilege across all integrations.
- Built cross-account IAM inventory pipeline via STS AssumeRole with EventBridge-scheduled Lambda caching results as Parquet to S3, decoupling portal read latency from live IAM APIs
- Delivered CIS benchmark query service over Steampipe (PostgreSQL wire protocol) with role-scoped access control for on-demand security posture visibility
- Implemented cross-account CloudWatch log scanning with structured Slack alerting via EventBridge cron, reducing Lambda failure MTTD.
- Standardized auth across 6 SaaS proxy Lambdas (Google Workspace, Atlassian, Slack, Databricks, GitHub, Cognito) with centralized JWT enforcement.
- Provisioned full AWS stack (API Gateway, Lambda, DynamoDB, IAM, EventBridge, S3) via Terraform; authored CI packaging scripts and Nginx config for repeatable, auditable SPA deployments.

DevSecOps security auditing platform (FastAPI + Vue 3, GitHub CI/CD)

- Built a full-stack DevSecOps security auditing platform (FastAPI + Vue 3) with 15 scanning modules covering web, SFTP/SSH, FTP, AWS, Azure, and GCP infrastructure — deployed on AWS EC2 (Docker/Nginx) and AWS Lambda (serverless)
- Designed zero-trust auth layer with Cognito JWT/JWKS verification, DynamoDB feature-flag whitelist, and 90-day audit logging — enforcing least-privilege across all integrations.
- Engineered an async penetration testing suite including DNS recon, subdomain takeover detection, SSL/TLS vulnerability auditing, HTTP header grading, directory brute-forcing, and JWT analysis.
- Implemented role-based access control (admin/analyst/viewer) using AWS Cognito with MFA (SMS/TOTP) and automatic JWT token refresh.
- Integrated AI-powered remediation engine leveraging an offline knowledge base and OpenAI GPT-4o-mini to generate contextual fix advice per scan finding.
- Automated multi-format report generation (PDF via WeasyPrint, CSV, JSON, HTML) with scan-specific and multi-cloud combined templates.
- Applied OWASP security controls including SSRF protection (blocking private/loopback IP ranges), audit logging with user identity per scan, and input validation across all scanner endpoints.