Rewat Singh

Contact

+91 8290671201
rewatsingh271@gmail.com
B-96 Heerawala, Jaipur
www.rewatsingh.site

Objective

DevOps Engineer with 5+ years of IT experience, including 3+ years in cloud-native infrastructure, CI/CD automation, and workflow orchestration. Strong background in networking, system administration, and technical support, with a proven track record of building secure, scalable, and observable systems. Seeking to contribute to a high-impact DevOps/SRE/Cloud team by driving automation, reliability, and innovation that directly supports organizational growth and success.

Education

Bachelor of Technology in ECE | JNIT, Jaipur | 2013 - 2017

Experience

Technical Support Engineer, *Q3 Technologies, Jaipur*
NOV 2022 – PRESENT

- Assisted development teams and client teams by supporting SDLC processes and ensuring efficient project delivery.

- Coordinated with stakeholders, project managers, and L2 teams to resolve technical issues and conduct RCA for production incidents, and achieve project goals within SLA.

- Administered and optimized Atlassian tools — Jira (workflow automation), Confluence (documentation), OpsGenie, and StatusPage (incident management) — improving cross-team collaboration and project visibility.

- Monitored AWS, Azure, and on-prem critical infrastructure, web, and mobile applications using CloudWatch, Zoho, and custom analytics dashboards; delivered incident, health check, and quarterly performance reports.

- Managed CMS platforms (Sitecore, WordPress), handling live content updates,

publishing, troubleshooting, and out-of-hours maintenance to ensure accuracy and uptime.

- Performed API testing and monitoring using Postman and FastAPI; contributed to automated testing pipelines with Selenium and Pytest integrated into CI/CD workflows to ensure continuous quality assurance.

- Supported identity and access management by provisioning roles via AD/LDAP, managing RBAC through OIDC-based platforms, and automating secrets delivery with HashiCorp Vault.

- Delivered timely email and voice support while actively participating in agile ceremonies (sprint planning, standups, retrospectives) to maintain clear communication and progress tracking.

- Mentored junior team members, led on-site network engineering activities, and ensured efficient collaboration across cross-functional teams.

- Supported internal access requests and incident resolution through ticketing workflows.

DevOps Engineer Intern, *Ecuzen Softwares, Jaipur*
AUG 2020 - SEPT 2022

- Proficient in Git: advanced Git commands, branching strategies, and merge conflict resolution to ensure seamless version control and collaboration.

- Set up and assisted in CI/CD pipelines using Jenkins for both monolith and containerized apps, and built multi-stage GitHub Actions workflows for microservices deployment along with GitLab CI/CD.

- Built and deployed serverless apps with AWS Lambda, API Gateway, and SAM CLI; used AWS Secrets Manager for credentials, CloudWatch for monitoring, and automated delivery with AWS CodePipeline.

- Provisioned and managed AWS infrastructure using Terraform, Ansible, and CloudFormation covering VPC, EC2, RDS, EKS, S3, and IAM.

- Built GitOps pipelines combining GitHub Actions, Helm, and Argo CD; managed multi-chart apps and Argo CD sync policies for version control in Kubernetes environments.

- Configured Prometheus and Grafana with custom dashboards and Slack alerts via Alertmanager; used ELK and Splunk for log aggregation, querying, and incident handling.

- Worked on scripting tasks using Bash and Python to automate routine system administration tasks.

- Designed and maintained production-grade Docker images using multi-stage builds; enforced security best practices with Trivy scans, labels, and health checks; streamlined local development with Docker Compose; managed image versioning and distribution via JFrog Artifactory.

- Managed web servers, mail, FTP, DNS, DHCP, NFT, SAN, and storage systems across Linux and Windows environments, including MS365 administration and support.

- Architected secure, cost-efficient AWS infrastructure with VPC, ALB, IAM, and KMS using Terraform; enforced auditing via CloudTrail and Config; optimized EC2, S3, and Lambda usage; tracked spend with Budgets and Cost Explorer.

- Deployed and maintained EKS clusters with Calico and eBPF for network policy enforcement, observability, and high-performance service mesh.

- Implemented hybrid connectivity with Site-to-Site VPN, Transit Gateway, and Client VPN, integrating AWS with on-prem infrastructure securely.

- Set up Disaster Recovery solutions using S3 versioning, RDS snapshots, and cross-region replication for failover and data protection.

- Implemented Single Sign-On (SSO) and authentication methods, including OIDC and token-based authentication (HashiCorp Vault, OneLogin, JWT).

- Supported IAM by provisioning roles via AD/LDAP, managing RBAC through OIDC-based platforms, and automating secrets delivery with HashiCorp Vault.

- Handled Linux/Windows system administration, patching, tuning, and backups; managed virtualization using VMware and Hyper-V.

- Strong understanding of IP, subnetting, firewalls, BGP, and the OSI model, applied to design and troubleshoot secure, high-performance hybrid networks.

Network Engineer, *Edge Telecom, Gurugram*
Dec 2017 – Jul 2018

- Deployed and commissioned telecom and enterprise networks, including fiber connectivity, edge devices, and service testing.

- Managed WAN networks on OTNM2000 software for the BSNL CPAN project, with proactive monitoring and fault resolution.

- Configured and troubleshot MPLS L3 switches/routers (VRF, OSPF, BGP, QoS) for backbone integration.

- Implemented redundancy (HSRP/VRRP) to ensure high availability of customer services.

- Integrated MPLS-TP with optical layers (OTN/DWDM) for seamless Ethernet/MPLS transport across 40G/100G links.

- Monitored optical parameters (dB loss, OSNR, dispersion) and resolved fiber-related issues.

- Led a team of 4 engineers, managing daily operations and technical support.

Personal Hands-on

Web Development and Security

- Developed web applications using Django, Flask, Laravel and SpringBoot utilizing Python, Java and PHP for backend logic.

- Designed and maintained MySQL, Postgrasql and MongoDB databases, ensuring data integrity and performance.

- Created RESTful APIs and performed testing and monitoring using Postman, FastAPI, and AWS API Gateway.

- Conducted penetration testing, cryptography, and reverse engineering through CTF challenges.

- Strengthened application security with SSO, OIDC, RBAC, token-based authentication, and vulnerability scans.

- Configured firewalls, IDS, and performed security audits to identify and mitigate vulnerabilities.

- Used security tools like Metasploit Framework, Burpsuite, OWASP ZAP, and various security distros for testing.

Data Analysis and Machine Learning / Data Science

- Managed Python environments with Conda/Anaconda and automated end-to-end ML pipelines using Jupyter Notebook, JupyterLab, and Spyder IDE.

- Skilled in data preprocessing, feature engineering, and handling missing values with

Pandas and NumPy.

- Designed, deployed, and automated ML models with Scikit-learn, including supervised (Regression, Decision Trees, SVM, Random Forest, XGBoost, KNN) and unsupervised methods (K-Means, PCA, Autoencoders) for classification, regression, clustering, and anomaly detection.

- Developed static and interactive visualizations using Matplotlib and Seaborn for actionable insights.

- Built ETL pipelines, integrated databases with Power BI and Tableau for real-time BI dashboards, and containerized applications with Docker for scalable deployments.

DevSecOps

- Performed static and dynamic application security testing with SonarQube, SonarCloud, Burp Suite, Nessus, and Kali Linux.

- Conducted dependency and container security scanning using Snyk, Trivy, Kube-bench, and Docker Trusted Registry.

- Managed AWS security tools including GuardDuty, Security Hub, WAF, Inspector, Config Rules, Macie, IAM policies, KMS, and Secrets Manager.

- Implemented secrets management using HashiCorp Vault, Identity, and AWS Secrets Manager.

- Applied Policy as Code (PaC) with HashiCorp Sentinel and Gatekeeper (OPA).

- Managed authentication and authorization with SSO, OIDC, SAML, MFA, RBAC, ABAC, and tools like Auth0, OneLogin, AWS IAM, and JWT tokens.

- Threat detection and incident management using CrowdStrike, Palo Alto Cortex XDR, and PagerDuty.

- Ensured network security using Nmap, Wireshark, AWS Security Groups, NACLs, and Palo Alto Firewalls.

- Configured traffic filtering and encryption with IPsec, TLS/SSL, VPNs, and Zero Trust Architecture.

- Maintained compliance with ISO 27001, NIST, GDPR, HIPAA, PCI-DSS, and CIS Benchmarks.

- Conducted post-exploitation techniques such as credential harvesting, lateral

movement, and exploit frameworks.

- Performed reverse engineering using Ghidra and Radare2.

- Applied cryptographic practices including PKI, HMAC, AES, RSA, and SHA algorithms.

- Practiced secure coding with code linters and remediation of OWASP Top 10 vulnerabilities, CVEs, and zero-day exploits.

- Administered and hardened Linux (Ubuntu, RHEL) and Windows systems (Active Directory, patching, group policy).

- Implemented shift-left security practices and chaos engineering for resilience testing.

Certifications

- AWS Certified DevOps Engineer Professional

- Certified Kubernetes Administrator

- CompTIA Network+

Additional Information

- Current CTC: 5.5 LPA

- Expected CTC: 8 - 12 LPA

- Notice Period: 1 month