

AAKASH PARMAR

DevOps Engineer | DevSecOps & Cloud-Native Security

aakashparmar788@gmail.com • +91 9904498695

DevOps Engineer with 3 years of experience building secure, production-grade Kubernetes and cloud infrastructure, embedding security controls, image hardening, policy-as-code, secrets management, and CIS-benchmarked cluster hardening directly into CI/CD pipelines. Skilled in reducing attack surface through hardened container images, RBAC/IAM least-privilege design, and eBPF-based network security and observability (Cilium), while sustaining 99.9% SLA across 30+ production applications. Experienced in auditing live Kubernetes clusters and bringing them to a production-ready, security-compliant state.

PROFESSIONAL EXPERIENCE

Orscope Technologies LLP

Sep '24 – Present

DevOps Engineer

- **Secure CI/CD Pipeline Implementation:** Architected CI/CD pipelines for 25+ projects (GitHub Actions, ArgoCD) with integrated SAST/SCA and container image vulnerability scanning, built around a centralized, security-gated configuration repository cutting deployment time to seconds while enforcing enterprise security standards.
- **Kubernetes Cluster Hardening & Audits:** Audited running Kubernetes clusters end-to-end and brought them to a production-ready state by applying CIS Kubernetes Benchmark controls, hardened RBAC policies, and audit logging supporting 30+ production applications at 99.9% SLA on constrained hardware (256GB RAM).
- **Container Image Hardening:** Designed minimal, hardened container images with no shell utilities, package managers, or sudo access, blocking privilege escalation and lateral movement so that even an application RCE or container compromise cannot be used to install tools, exfiltrate data, or pivot further.
- **Secrets & Policy-as-Code Guardrails:** Implemented centralized secrets management (HashiCorp Vault, Sealed Secrets/SOPS) and policy-as-code enforcement (OPA, Kyverno, Gatekeeper) across GitOps workflows to block non-compliant or insecure deployments before they reach production.
- **eBPF-Based Network Security & Observability:** Used Cilium/eBPF for zero-trust network policies, deep traffic visibility, and runtime security monitoring across microservices migrated from a monolith via Istio service mesh, paired with Prometheus/Grafana observability and Karpenter/KEDA/VPA/HPA autoscaling.
- **AI Workload Isolation:** Engineered NVIDIA GPU efficiency (fractional GPU, MIG, vGPU, timeslicing) for a 140% increase in workload capacity while maintaining tenant isolation boundaries for large-scale LLMs (671B & 405B parameters) on enterprise-grade and RTX 4090 GPU clusters, with KubeVirt/SR-IOV passthrough for VM workloads.

Freelancer, Remote

Jul '23 – Aug '24

Software Developer

- **AWS Cloud Infrastructure & IAM Hardening:** Designed AWS infrastructure (EC2, Fargate, ECR) with CloudFormation, hardening security groups, IAM roles, and load balancer configurations under least-privilege principles for secure, scalable service delivery.
- **Terraform Infrastructure-as-Code:** Built highly available AWS environments via Terraform (EC2, VPC, subnets, security groups) with disaster recovery built in and security-reviewed provisioning, reducing maintenance cost and deployment time.
- **Monitoring, Alerting & Audit Visibility:** Established monitoring and alerting (Prometheus, Grafana, AlertManager) with audit-log-driven visibility into infrastructure activity, cutting incident response time by 25%.

OPEN SOURCE CONTRIBUTIONS & PROJECTS

- **Container Runtime Hardening:** Added a script to install CRI-O with Flatcar, hardening the container runtime for low-resource platforms and cutting overhead by up to 30% versus typical Docker setups shrinking the runtime's attack surface in the process.
- **Reliability Fix:** Fixed retry logic in docker-entrypoint.sh for Nextcloud installation (#2256), improving installation reliability and success rates.
- **Stability Fix:** Fixed compilation and execution issues in lapack/dpttrf (#4503), restoring proper functionality and stability.
- **Minimal-Footprint OS:** Built a custom Linux-based OS requiring only 12MB of RAM and a 13MB ISO, designed around a reduced attack surface and minimal installed components, while supporting SSH, FTP, Telnet, Wget, and Curl.

SKILLS

Security & DevSecOps: SAST/SCA Scanning, Container Image Scanning & Hardening, Secrets Management (Vault, Sealed Secrets, SOPS), Policy-as-Code (OPA, Kyverno, Gatekeeper), RBAC/IAM Hardening, CIS Kubernetes Benchmarking, Audit Logging, eBPF-Based Network Security (Cilium)

Programming Languages: Python, JavaScript, Golang, Bash

DevOps & CI/CD Tools: Kubernetes, Docker, GitHub Actions, Postman, Ansible, Jenkins, Terraform, Git, GitLab CI, ArgoCD, Flux

Cloud-Native & Other Tools: Cert-manager, Karpenter, Envoy, Istio, Jaeger, Kong, KEDA, KubeVirt, Prometheus, Grafana, Helm, CRDs, Gin, Node.js, Express.js, React.js, Next.js