

AMAL ZACHARIA C.R.

contact@crza.dev ♦ amalzacharia.com ♦ [GitHub](#) ♦ [LinkedIn](#) ♦ India (IST)

PROFESSIONAL SUMMARY

Platform and infrastructure engineer with 6+ years of production ownership across bare metal and multi-cloud environments. Built and operated distributed systems handling 200,000+ concurrent connections, wrote an eBPF firewall and networking stack for microVM hosts, and evolved production Kubernetes infrastructure through five major iterations driven by cost, scale, and security constraints.

SKILLS

Languages	Go, TypeScript, Kotlin, Python, Bash
Linux	Debian, Ubuntu
Orchestration	Kubernetes (k3s, rke2, AKS), Docker, Helm, Gateway API
Networking & CNI	Cilium (eBPF firewall, L2 announce), Calico (BGP), WireGuard mesh, nftables
Cloud & Bare Metal	AWS, Azure, Hetzner, OVH, Oracle Cloud, Contabo, DigitalOcean
IaC & GitOps	Terraform, Ansible, ArgoCD, CI/CD (GitHub Actions), GoReleaser
Observability	Prometheus, Grafana, Alertmanager, Loki
Databases	PostgreSQL, MongoDB, Redis, MySQL
Security	eBPF host firewalls, Cilium NetworkPolicies, mTLS, Cloudflare WAF
DNS & TLS	cert-manager (HTTP-01, DNS-01 via Cloudflare), wildcard certs
Architecture	Distributed systems, multi-tenant isolation, WebSockets at scale

EXPERIENCE

FYNOVA LABS LLP

Apr 2025 - Present

Platform & Infrastructure Engineer

Remote

- Built an eBPF firewall and networking stack for microVM hosts, modeled on Cilium's host firewall. It delivered about 6x the throughput of an nftables rule chain at 4,000 rules.
- Root-caused intermittent 30-second TCP stalls (every 90 seconds) to one IP address held by two devices, after disproving the provider packet-loss theory.
- Operate the production rke2 + Cilium cluster on OVH bare metal: eBPF host firewall, Cloudflare-only ingress with mTLS, and tenant isolation via Cilium NetworkPolicies.
- Mentoring two fresh graduates (since July 2026) on bare-metal server provisioning and cluster setup.

INDEPENDENT CONSULTANT

Apr 2020 - Apr 2025

Senior Platform & Infrastructure Engineer

Remote

- Designed, built, and rebuilt five production Kubernetes clusters across Hetzner, Contabo, Oracle Cloud, and OVH, each iteration driven by cost, scale, or security constraints.
- Kept 200,000+ concurrent WebSocket connections live for two years as the sole operator, holding the client's 75% connection floor outside planned maintenance and above 90% most of the time, on a 5-node bare metal k3s cluster on Hetzner using StatefulSets and protocol-level efficiencies.
- Built and operated cross-cloud WireGuard mesh connecting Contabo amd64 nodes and Oracle Cloud ARM64 workers, with multi-arch builds via GoReleaser triggered through GitHub Actions.
- Migrated production workloads from managed and VPS-based hosting to self-hosted Kubernetes on bare metal, cutting infrastructure costs by roughly 85%.
- Rewrote Node.js services to Go using only the standard library, with zero external dependencies, reducing per-task RAM from 1024MB to 32MB.
- Provisioned bare metal infrastructure from scratch: Ventoy boot, gparted live, dd to disk, Debian installation, SSH and networking configuration.

- Operated solo on-call across all client systems for five years, owning incident response, postmortems, and run-books end to end.
- Maintained 3-4 long-term international client contracts continuously, all inbound.

TECHNICAL PROJECTS

Multi-Cloud Bare Metal Kubernetes Infrastructure (2020-Present): Five-generation production cluster evolution.

- Stage 5 (current): rke2 + Cilium on OVH bare metal. L2 LB announcement, CiliumClusterwideNetworkPolicy host firewall with egress-only public interface enforced at eBPF layer. Traefik ingress restricted to Cloudflare IPs, with Cloudflare Authenticated Origin Pulls (mTLS) requiring a Cloudflare client certificate at the origin. Strong tenant isolation between namespaces via incoming-decides NetworkPolicy model.
- Stage 4: 5-node Hetzner cluster. Calico BGP internode mesh, private VLAN for internode communications, Keepalived floating IP with Hetzner API hooks. Evaluated MetalLB + BGP for LB announcement, reverted after one month due to HTTP latency through cloud network routing.
- Stage 3: Multi-cloud cluster with Contabo amd64 masters and Oracle Cloud ARM64 workers connected via WireGuard mesh. Multi-arch Go builds via GoReleaser, node affinity for arch-specific scheduling.
- Full architectural evolution with reasoning at each stage documented at amalzacharia.com.

Distributed WebSocket Infrastructure (2022-2024): System managing 200,000+ concurrent persistent connections.

- Deployed across a 5-node bare metal k3s cluster on Hetzner using StatefulSets for stable pod identity and shard-based connection ownership.
- Rewrote from Node.js to Go with custom no-cache architecture, reducing RAM by 90% per instance.
- Multi-node egress to distribute outbound traffic across cluster IPs, preventing rate limit triggers.
- Estimated managed-cloud cost: ~\$320/month at 80k connections. Actual bare-metal cost: ~\$190/month at 200k connections.

Task Automation Engine (2021-2024): Event-driven execution system for bursty workloads.

- Processed 50,000+ events per day at peak across multiple long-term clients.
- Prototyped on single VPS, migrated to AWS Lambda for parallel execution, then to Go services on Kubernetes.
- Rewrote critical paths from Node.js to Go, reducing per-task RAM from 1024MB to 32MB.
- Deployed on idle cluster capacity, reducing that portion of infrastructure cost to near zero.

eBPF NAT and Firewall for Firecracker microVMs (In Progress): Firewall policy and networking stack for microVM hosts that are not Kubernetes nodes, modeled on Cilium's host firewall.

- Benchmarked against an nftables rule chain in network namespaces: nftables was about 5% faster at 1 and 10 rules, while at 4,000 rules eBPF delivered about 6x the packets per second (154,114 vs 25,562) with 4.3x fewer CPU cycles per packet.
- Policy compiles into longest-prefix-match map entries with constant-cost lookups, capped at 4,096 entries. Swapping a full policy at the cap takes about 26 ms.
- Write-up: amalzacharia.com/blog/ebpf-vs-nftables-rule-count.

CERTIFICATIONS

- AWS Certified Solutions Architect
- AWS Certified Cloud Practitioner
- Kubernetes and Cloud Native Associate (KCNA), The Linux Foundation

ADDITIONAL CONTEXT

Full technical write-ups at amalzacharia.com.