

Francisco De la Cruz

DevOps / Cloud Engineer · Computer Engineer

Córdoba, Argentina (remote-friendly) · franciscoo.delacruz@gmail.com · linkedin.com/in/francisco-delacruz · github.com/FranciscoCross

SUMMARY

DevOps / Cloud Engineer with ~4 years building, migrating and operating production **Kubernetes** platforms on **AWS** and **Azure** for fintech, insurtech, utilities and regulated/**PCI** workloads. Comfortable across the whole stack — greenfield IaC, GitOps, on-prem HA Kubernetes, observability, cloud security/SIEM and FinOps — and across clouds and bare metal. **AWS Certified Solutions Architect – Professional**. Internal technical referent and university professor: conference speaker, mentor and IaC module maintainer.

I take production Kubernetes platforms from fragile and expensive to boring and cheap — across clouds, on-prem, and the network underneath.

CORE SKILLS

- **Orchestration:** Kubernetes (EKS, EKS Auto Mode, on-prem kubeadm HA + etcd + kube-vip on vSphere), Helm, ArgoCD (GitOps/ApplicationSets), Karpenter, Cilium (CNI + Egress Gateway), Traefik, NGINX Ingress, KEDA, HPA, Longhorn (distributed storage), Harbor (registry / ECR pull-through cache)
- **AWS:** EKS, EC2, Lambda, API Gateway, RDS/Aurora, RDS Proxy, DynamoDB, ElastiCache, S3, EFS, ECR, SQS/SNS/EventBridge, Kinesis Firehose, MSK, CloudFront, Route 53, ACM, ALB/NLB, WAF, Cognito, OpenSearch, Control Tower, IAM Identity Center, IAM Roles Anywhere, GuardDuty/Security Hub/Inspector, Cost Explorer
- **Azure:** AKS, Azure PostgreSQL, ACR, Key Vault + Workload Identity, VNet, Application Gateway/AGIC + WAF, Front Door
- **IaC & CI/CD:** Terraform + Terragrunt (reusable module catalog), Atlantis (Terraform PR automation), CloudFormation; GitHub Actions (self-hosted ARC), GitLab CI, Bitbucket Pipelines (self-hosted runners)
- **Observability:** Prometheus / kube-prometheus-stack, Grafana, Loki (+ MinIO), Mimir, Tempo, Thanos, Alloy, Datadog, New Relic, Honeycomb, OpenTelemetry
- **Data & messaging:** PostgreSQL, MySQL, MongoDB → DocumentDB, Kafka/MSK, RabbitMQ/Amazon MQ, OpenSearch/ElasticSearch, CDC (Debezium / Red Panda / Rising Wave / Iceberg), DMS
- **Security & FinOps:** PCI environments, SIEM on OpenSearch (assessed vs Wazuh / Elastic / Datadog Cloud SIEM), IAM Roles Anywhere (X.509), Vault / External Secrets / Doppler, Kubecost, Savings Plans, Spot, log-ingestion reduction
- **Networking:** VPC/VNet, multi-region peering & failover, IPsec / WireGuard / Pritunl VPN, Cloudflare (Tunnel / Zero Trust Access), Private Link, egress HA, MikroTik/RouterOS, BGP fundamentals
- **Languages/tooling:** Python (boto3), Bash, PHP (legacy modernization), Locust; LLM-ops (MCP, Claude API, Claude Code)

EXPERIENCE

DevOps / Cloud Engineer — Cloud consultancy (AWS Partner)

2022 – present · Córdoba, Argentina (remote)

Delivered infrastructure across 15+ client engagements as part of dedicated DevOps squads and end-to-end cloud projects. Selected work (clients anonymized by domain):

Fiscal-traceability & digital-certification platform — hybrid AWS + on-prem · Lead infra (2024–present)

- Operate a mission-critical platform (PHP monolith + microservices) replicated across AWS (5 environments) and an on-

prem datacenter running self-managed HA Kubernetes (kubeadm, etcd, kube-vip).

- Built the on-prem platform end to end on **vSphere**: kubeadm HA + Cilium, **Longhorn** distributed block storage, and a **Harbor** registry as an ECR pull-through cache; modernized a legacy **CentOS 6 / PHP 5.4** component with containerized CI/CD and centralized logging (Grafana Loki via Alloy).
- Engineered **egress-gateway HA on Cilium OSS** (no Enterprise license): kube-vip floating VIP + a custom label-sync controller holding exactly one egress node via lease leader-election — ~4–5s failover; diagnosed and fixed a >30-min cold-start with IP pre-warming.
- Debugged a CSI-SMB DaemonSet **CrashLoop with ~21,000 restarts** to a duplicate Helm release colliding on a host port under hostNetwork.
- Slimmed observability: Loki → MinIO, retired Thanos (freed ~54 GiB orphan PVCs); migrated nginx → Traefik, ElastiCache → in-cluster Redis, DockerHub → ECR; replaced static keys with **IAM Roles Anywhere**.
- **FinOps**: hit an explicit ~US\$500/mo dev target via night shutdown, NAT-GW consolidation, Spot/On-Demand NodePools, EKS Auto Mode and Savings Plans.

Regulated consumer-credit & digital-wallet fintech — PCI (2024–2025)

- Ran **5 in-place EKS upgrades (1.28 → 1.32)** + Karpenter v0.34 → v1.32 with a repeatable, breaking-change-checked procedure and zero downtime.
- Unified **~15 microservices across 6 environments onto a single Helm chart** and moved deployments to GitOps (ArgoCD ApplicationSets), eliminating config drift.
- Built resilient multi-tunnel IPsec connectivity to financial regulators; ran SIEM (OpenSearch) + GuardDuty auto-remediation; configured 1-year audit log retention.

Card-issuing & loyalty fintech — PCI, Azure → AWS (2025–2026)

- After benchmarking managed vs open-source SIEM (Datadog Cloud SIEM, Wazuh, Elastic), built a **PCI SIEM on Amazon OpenSearch** (EventBridge → Firehose → S3 → Lambda → OpenSearch, OKTA SSO) ingesting CloudTrail, GuardDuty, VPC Flow Logs, EKS audit logs and more.
- Replaced Datadog with a self-hosted Prometheus/Grafana/Mimir/Loki/Tempo stack across ~6 clusters; cut **VPC Flow Log ingestion ~40–60%**.
- Migrated Azure SQL → RDS (DMS) and built a streaming CDC pipeline (Debezium → Red Panda → Rising Wave → Iceberg).

Tax-tech fintech (2022–2023) — ~25 microservices on EKS + Lambda/API Gateway; **RDS → Aurora + RDS Proxy** migration in prod; unified **OpenTelemetry** tracing (manual + auto-instrumentation → Honeycomb); FinOps right-sizing.

Utilities/energy SaaS — multi-cloud (2025) — extended an AWS/EKS+ArgoCD platform to **Azure** by building the Azure Terraform module catalog from scratch (AKS, App Gateway, Key Vault + Workload Identity); reused the same ArgoCD/Helm GitOps; cut ingress cost (AGIC → NGINX).

Other: ~20-microservice quote/insurtech platform (Karpenter migration, CI outage recovery); customer-flow SaaS with **Jitsi/Jibri video on EKS** (Azure → AWS); multi-region wellness apps (EKS 1.24 → 1.27, IAM Identity Center); insurtech observability (New Relic, EKS Auto Mode + Spot); banking-API GitOps; govtech e-auctions; data/BI migrations (DMS, MongoDB → DocumentDB).

Internal & leadership

- Maintainer of the company **Terraform Service Catalog** (reusable modules incl. EKS Auto Mode) published to the Terraform Registry.
- Platform work on an internal infra-automation SaaS: self-hosted **GitHub Actions ARC** on EKS with a dedicated Karpenter pool; led a production-outage post-mortem.
- Authored AWS **Well-Architected / Service Delivery** partner evidence (Graviton, API Gateway, RDS).
- Designed and mentored the **Trainee Program**; reviewer of technical hiring tests.
- **Client enablement** — delivered hands-on training (e.g., Grafana) to client engineering teams.
- Speaker at **Nerdearla 2025** — "Scaling apps on Kubernetes by HTTP request rate"; regular internal tech talks.

University Professor (part-time) — DevOps Diploma

2024 – present · Córdoba, Argentina

- Teach **Operating Systems, Databases and Microservices** within a professional DevOps Diploma — OS fundamentals (processes, concurrency, virtualization), containers and microservice design, networking and security, and Bash/Python

automation.

SELECTED SELF-DIRECTED PROJECTS

Two-node self-hosted homelab — Designed and run a production-grade lab mirroring my professional stack: **Traefik** ingress with automatic Let's Encrypt TLS (Cloudflare DNS-01) + **Authelia** SSO/2FA, **AdGuard** network DNS, a full **Grafana + Loki + Alloy + Prometheus** observability stack (plus PCP and Scrutiny), an x86 NAS with **RAID1 + btrfs** storage over SMB/NFS, **Kubernetes** tooling, GitOps via GitHub Actions and a **Tailscale** mesh — all declared as IaC in Docker Compose. Exposed publicly through a **Cloudflare Tunnel** (zero-trust ingress, zero inbound ports) fronted by **Cloudflare Access** (SSO), with a hardened edge (HSTS/CSP security headers, read-only docker-socket-proxy).

24/7 office-network observability & security — Built a full monitoring stack (Grafana + VictoriaMetrics/Logs, 10 containers, 17 alerts → Slack) for a MikroTik + UniFi network on a Raspberry Pi, all as IaC. **Mitigated a live DNS amplification attack** (~37× amplification, router abused as reflector), hardened the firewall (anti-brute-force, WAN default-drop, management off the internet), and tuned WiFi (2.4 GHz utilization 57% → 29%).

CERTIFICATIONS & TRAINING

- **AWS Certified Solutions Architect – Professional** — verifiable via Credly
 - **AWS Academy Educator**
 - Kubernetes & AWS networking (Black Belt)
 - GenAI / LLM-ops (Anthropic): MCP, Claude API, Agent Skills, Claude Code — 2026
-

EDUCATION

Computer Engineering — Universidad Nacional de Córdoba (UNC-FCEyN), 2017–2023

Final project: *DevSecOps in IoT environments* (grade 10/10).

LANGUAGES

Spanish (native) · English (professional working proficiency)