

RAFAEL MADOLELL

DEVOPS & CLOUD ENGINEER

rmadolell@gmail.com

+34 694 473 103

Spain

SKILLS

Cloud & Infrastructure

- AWS (EC2, S3, RDS, R53, AS)
- GCP
- vSphere / On-Premises
- Terraform
- Ansible
- CloudFormation

Containers & Orchestration

- Docker / Docker Compose
- Kubernetes (K8s)
- Helm Charts

CI/CD & DevOps

- GitLab CI/CD
- Jenkins
- GitHub Actions
- Sonarqube

Observability

- Grafana
- Prometheus
- Alertmanager
- Loki / Promtail
- Elastic / Kibana

Networking & Security

- Nginx / Traefik
- API Gateway
- Wireguard VPN
- Pentesting
- DevSecOps

Other

- Bash Scripting
- Nagios
- MongoDB
- PostgreSQL
- Portainer
- Agile / CTI

EDUCATION

Advanced Vocational Training

Computer Science,
Communications & Support
Services

TnexT — Spain | 2022

LANGUAGES

Spanish — Native

English — Intermediate

COURSES

- AWS Certified Cloud Practitioner
- AWS DevOps Navigate – Technical

PROFILE

DevOps & Cloud Engineer with 4+ years of experience building and operating infrastructure across diverse and demanding environments — from multi-cloud architectures on AWS and GCP to hardened, air-gapped on-premises deployments in high-security contexts. I work across the full stack: infrastructure provisioning with Terraform and Ansible, container orchestration with Kubernetes, end-to-end CI/CD pipelines, and full observability stacks. Beyond the tooling, I bring a strong security-first mindset shaped by working in the cybersecurity industry, where resilience and compliance are non-negotiable. I'm equally comfortable designing a scalable cloud environment and locking down a bastionized private infrastructure — and I take ownership of both.

EXPERIENCE

DevOps & AI Engineer | S2 Grupo

S2 Grupo is the leading European company in cybersecurity, cyber intelligence, and critical system operations, operating in 35+ countries with a team of 700+ experts and technology trusted by IBEX-35 corporations, government ministries, and the CCN-CERT.

- Part of the DevOps & AI team, responsible for automation and deployment of environments for specific cybersecurity products.
- Infrastructure provisioning on VMware vSphere using Terraform and Ansible, targeting hardened, air-gapped on-premises environments with strict security baselines.
- Deployment and management of services on Kubernetes (primary platform) with Helm Charts, ensuring high availability and policy compliance.
- Full observability stack implementation: Grafana, Prometheus, Alertmanager, Promtail, and Loki for metrics, logs, and alerting.
- Configuration and management of reverse proxies and API Gateways using Traefik and Nginx for secure internal service routing.
- Development of custom Docker images and internal policies aligned with company branding and security standards.
- CI/CD pipeline management with Jenkins and GitLab CI/CD for automated testing and delivery of internal products.
- Participated in AI automation initiatives to enhance operational efficiency across DevOps workflows.
- Maintained exceptional security posture across all environments — all infrastructure local, hardened, and bastionized; cloud services used only in exceptional cases.

Tech-Stack: vSphere, Terraform, Ansible, Kubernetes, Helm, Docker, Docker Compose, Jenkins, GitLab CI/CD, Grafana, Prometheus, Alertmanager, Promtail, Loki, Traefik, Nginx, API Gateway.

DevOps Engineer | Blue Trail Software

Designed, implemented, and maintained scalable and secure cloud infrastructure across multiple client projects, covering AWS and GCP environments.

Centex

- Full AWS infrastructure deployment (EC2, RDS, S3, R53) across Test, Staging, and Production.
- Backup & Restore and Disaster Recovery plans developed in Terraform.

- Automated deployments with GitHub Actions and security best practices applied to all services.

Tech-Stack: *AWS, GitHub Actions, Terraform, Bash Scripting, Linux.*

CCC

- Maintenance of full AWS stack (EC2, RDS, S3, R53, Lambda, ECS, CloudFront, ECR).
- Disaster Recovery in CloudFormation; automated CI/CD with GitHub Actions (deployments, builds, backups, lambdas).
- Jbase and PostgreSQL database migrations; Datadog and Err0 metrics integration.

Tech-Stack: *AWS, GitHub Actions, CloudFormation, Bash Scripting, Linux.*

Cartier (ALG / MegaComputers)

- Migrated Elastic & Kibana to a new GCP instance with SSL and DNS management.
- Deployed Ansible playbooks for automated ALG installation on MegaComputers; set up Portainer for container management.
- Implemented WireGuard VPN on each MC for secure remote administration; created custom Linux distribution for automated ALG deployment.
- Containerization monitoring via Metricbeats; new CI/CD pipelines for ALG image generation.

Tech-Stack: *GCP, Elastic, Kibana, Docker, Docker Compose, GitLab CI/CD, Wireguard, Ansible, Traefik, Portainer, Bash Scripting, Linux.*

Internal Projects (MyBTS, BTS Office, MyLuna)

- MyBTS: Automated deployments, CI/CD pipelines, and service security on AWS + GitLab. Redesigned office network infrastructure with security filters.
- MyLuna: Full migration of repositories to GitHub; new AWS environment with Docker, MongoDB, and SSL. Multi-environment migration (Production, Pre-Production, QA).
- Abbott environment: EC2 Autoscaling Groups, Load Balancers, SSL, CloudWatch, AMI, Mongo Atlas, KMS, Nagios, UpTimeRobot.

Tech-Stack: *AWS (EC2, S3, RDS), GitLab, GitLab CI/CD, Docker, Docker Compose, Sonarqube, PostgreSQL, MongoDB, Nginx.*

KEY ACHIEVEMENTS

- Improved security guidelines at BTS, reducing incidents by 30%.
- Integrated cutting-edge security tools, enhancing threat detection by 40%.
- Automated internal processes with scripts, saving 20 hours/week and reducing errors by 90%.
- Created real-time availability dashboards, reducing downtime by 25%.
- Conducted penetration testing on web APIs and mobile apps, identifying critical vulnerabilities.
- Developed an internal AI chatbot PoC to enhance operational efficiency.
- Integrated advanced AI tools for cybersecurity automation and improved threat response.