

Fabio Sussarellu

DevOps / Platform Engineer

sussarellu.fabio@gmail.com · linkedin.com/in/fabio-sussarellu · gitlab.com/eathtespagheti · github.com/eathtespagheti

ABOUT ME

DevOps / Platform Engineer owning CI/CD and build infrastructure for a microservice estate on AWS (~30 services across ~20 engineering repositories). Hands-on with Bitbucket Pipelines, Docker/ECR image supply chains (BuildKit, registry cache, pull-through cache, multi-arch), a self-hosted EC2 runner fleet, and a reusable shared release step adopted across the product's repositories. Also Kubernetes/EKS cluster operations and upgrade runbooks, Terraform IaC and secrets management (Infisical, SOPS, OIDC), Flux CD GitOps delivery, observability, security remediation, and internal developer-platform tooling. Interfaces with ~20 codebases and provides on-call developer support.

SKILLS

Programming & Scripting: Bash, POSIX Shell, Python, JavaScript / Node.js, Java, PHP, C, MIPS Assembly

CI/CD & Build Engineering: Bitbucket Pipelines, Custom Bitbucket Pipes, Reusable pipeline steps, Back-merge pipelines, Canary deployments, SonarQube quality gates, GitLab CI/CD, Jenkins, Dagger (evaluated), Playwright

Containers & Registries: Docker, BuildKit (RUN --mount=type=cache), Multi-stage Dockerfiles, ECR registry cache, ECR pull-through cache, Multi-architecture (ARM64) builds, ECR lifecycle policies, Image provenance & attestations, Podman

Kubernetes & Cloud: Kubernetes (AWS EKS), Helm, Flux CD (GitOps), Argo Workflows (platform environment), Karpenter (platform environment), Kubeadm (self-managed), Cilium eBPF, Gateway API, AWS — ECR, EKS, EC2, ECS, S3, IAM, Lambda, SQS/SNS, Parameter Store, Secrets Manager, CloudFront

Infrastructure as Code & Secrets: Terraform, Ansible, Infisical, SOPS + age, External Secrets Operator, OIDC (pipeline to AWS), OAuth2-proxy, SSM Parameter Store SecureString

Self-hosted Runners & Systems: AWS EC2 runner fleet, systemd services, inotifywait, POSIX shell / awk, shfmt, yq, AMI lifecycle & instance sizing

Observability & Reliability: Elasticsearch, Logstash / Beats, Kibana, Grafana, APM, Slack alerting, Incident triage & rollback

Security Engineering: OWASP API2 remediation, Committed-credential remediation, Root-RCE remediation, Secret hygiene (SOPS / OIDC), IAM / RBAC, Backup & disaster recovery, GDPR Art. 32 measures

Data Stores & Messaging: MongoDB, Redis, PostgreSQL, MariaDB, SQLite, Apache Kafka

Networking: Tailscale, Headscale, OpenWrt, Split-horizon DNS, Cloudflare CDN / anti-DDoS, Firewalls

Development Tools: Git, Make, Subversion, SQL, HTML, SCSS / CSS, YAML, Markdown

Operating Systems: Linux (Arch, Alpine, openSUSE), BSD, macOS

AI & Productivity: Cursor IDE, LLM-assisted engineering, Model Context Protocol (MCP) services, OmniRoute AI-provider proxy (evaluated)

KEY ACHIEVEMENTS

- Designed, implemented and rolled out a reusable shared release step now adopted across ~20 services in a ~30-microservice AWS estate, with canary deployments and back-merge support
- Rebuilt the container build pipeline around BuildKit and ECR caching, mitigating the Docker Hub pull-rate limit and cutting build times across the estate
- Authored the official EKS Cluster Upgrade Runbook for a critical, irreversible control-plane procedure (Upgrade Insights, kubent/Pluto scanning, add-on compatibility validation)
- Designed and operated a self-hosted EC2 runner fleet with per-runner systemd services, an inotify-based cleanup service and a usage-based storage reclamation strategy
- Acted on 170 Jira tickets (130 created, 109 released) and authored 20+ internal runbooks, procedures and technical proposals
- Appointed company System Administrator with 11 formal security duties (authentication/authorization, GDPR Art. 32, backup & restore, periodic controls)
- Remediated penetration-test findings (OWASP API2), a committed AWS IAM access key and a root-RCE in an internal CI service; replaced long-lived AWS credentials with OIDC-based pipeline authorization
- Built internal self-service QA environments (devops-manager) used by non-technical teams to spin up isolated environments on demand
- Led a team of 3 Junior DevOps engineers at Abika, owning project intake, task breakdown and technical escalation
- Architected a single-node kubeadm Kubernetes homelab with Cilium eBPF (full kube-proxy replacement), Gateway API, Flux GitOps, SOPS-encrypted secrets, Keycloak OIDC/RBAC and a Headscale control plane

EXPERIENCE

BizAway — DevOps Engineer, 2024/07 - Present

- CI/CD & build engineering: developed and maintained Bitbucket Pipelines; designed, implemented and rolled out the reusable shared release step now adopted across ~20 services; added canary deployments, back-merge pipelines and a custom merge check; adopted custom Bitbucket Pipes for build flexibility; introduced a SonarQube quality gate served through the ECR pull-through cache.
- Containers & image supply chain: engineered the Docker build pipeline with BuildKit (RUN --mount=type=cache, provenance/attestation control), multi-stage Dockerfiles, ECR registry cache and ECR pull-through cache (mitigating the Docker Hub pull-rate limit), multi-architecture (ARM64) publishing, and custom docker:dind / Node / multitool base images; managed image versioning and ECR lifecycle policies.
- Kubernetes / EKS operations: manage and upgrade the AWS EKS clusters, and authored the official EKS Cluster Upgrade Runbook (2026-06-01) for the critical, irreversible control-plane procedure - including AWS Upgrade Insights, deprecated-API scanning with kubent and Pluto, managed add-on compatibility validation and a POSIX-shell add-on compatibility checker. Also worked on Helm charts, autoscaling on custom metrics and terminationGracePeriod tuning.
- Infrastructure as Code & secrets: manage infrastructure with Terraform; migrated Terraform secrets to Infisical; introduced a SOPS pre-commit hook and encryption at rest; adopted the External Secrets Operator with AWS Parameter Store / Secrets Manager as a single source of truth for

Kubernetes secrets; deployed an OAuth2-proxy; introduced OIDC-based pipeline-to-AWS authorization to replace long-lived keys.

- GitOps with Flux CD: implement and drive the transition to a GitOps delivery model with Flux, migrating deploy steps and stage deployments, and recovering a Flux staging incident after an accidental cluster wipe.
- Self-hosted runner fleet (AWS EC2): designed and operated Bitbucket shell / hybrid runners - a configurable per-runner systemd service, an inotifywait-based cleanup service, and a smart usage-based cleanup strategy for images and storage; runner upgrades, AMI lifecycle, instance sizing and autoscaler plans; coordinated a fleet-wide runner-label rename across ~24 repositories.
- Testing infrastructure (E2E): built E2E environments for four services - Bitbucket services, docker-compose, seeded DB images, Playwright and Mongo/Redis/Elasticsearch/Kafka service bring-up.
- Observability: operate the logging and monitoring stack (Elasticsearch, Kibana, Grafana, APM, Slack alerting) for production troubleshooting, incident diagnosis and proactive anomaly detection; proposed StatsD-to-Elasticsearch ingestion of runner metrics.
- Security engineering: appointed company System Administrator (2025-04-09) with 11 security duties (authentication/authorization, backup & restore, anti-intrusion tooling, periodic controls, GDPR Art. 32). Remediated penetration-test findings (OWASP API2 - session tokens exposed in document URLs) across two backends, a committed AWS IAM access key and a root-RCE in an internal CI cleanup service.
- Internal developer tooling: developed and maintained the internal platform tools behind self-service QA environments (devops-manager) - real-time per-pipeline tracking, foreground and background deploy operations, a navigation guard, a one-click Slack support flow and an inactive-tab notification.
- Operations, documentation & support: actor on 170 Jira tickets (130 created, 109 released); authored 20+ internal technical documents (runbooks, procedures, troubleshooting guides, technical proposals); provided on-call developer support through the internal support channel (triage, diagnosis, resolution, rollback of failed releases).

AWS EKS, Terraform, Bitbucket Pipelines, Docker, BuildKit, ECR, Flux CD, Helm, Infisical, SOPS, OIDC, Elasticsearch, Grafana, systemd, Node.js

Abika — Lead DevOps Engineer, 2023/01 - 2024/06

- Owned delivery infrastructure for the engineering team while leading 3 Junior DevOps engineers: triaged incoming requests, assessed solutions by cost, reliability and performance, and chose the approach to proceed with.
- Broke project work into micro-tasks and assigned them across the team, matching each task to the engineer best suited to it, and provided technical support to keep the team unblocked.
- Introduced new tooling and practices into the team's arsenal, and led the migration of workloads to AWS.
- Deployed microservices on ECS (EC2 and Fargate) with autoscaling and blue/green deployments, and on AWS Lambda.
- Built hybrid multi-cloud infrastructure across AWS, Contabo, Cloudflare and DigitalOcean, managed entirely through Terraform IaC.
- Implemented CI/CD with GitLab Pipelines and Jenkins, machine configuration with Ansible, CDN and DDoS protection with CloudFront and Cloudflare, and multi-zone DNS.
- Automated dynamic service activation on AWS through scheduling.

AWS ECS, AWS Lambda, Terraform, GitLab CI, Jenkins, Ansible, Cloudflare, CloudFront, DigitalOcean

Of Course Me — Software Developer / DevOps, 2021/09 - 2022/12

- Developed backend microservices for search, cataloguing and distribution of over a million online courses.
- Dismantled a monolithic scraping and data-cataloguing system into multiple independent, faster microservices.
- Managed CI/CD for those services with Terraform IaC on AWS.

Python, Scrapy, Django, Terraform, AWS

Abinsula — DevOps, 2019/01 - 2021/08

- Development of microservices infrastructure based on Docker.
- CI/CD on microservices with GitLab Pipelines and Jenkins.
- CDN services, DDoS protection and network optimisation on Cloudflare.

Docker, GitLab CI, Jenkins, Cloudflare

Abinsula — Full Stack Developer (Internship), 2017/07 - 2018/11

- Converted a semester internship into a permanent role by demonstrating rapid acquisition of containerisation and full-stack development skills.
- Worked across the stack on containerisation and Bootstrap-based frontends.

Docker, Bootstrap, HTML, CSS

EDUCATION

Politecnico di Torino, Computer Engineering (BSc, not completed), 2017 - 2023

Cambridge Assessment English, FCE B2 (First Certificate in English, grade 163)

Istituto Tecnico Industriale G.M. Angioy, Sassari, Diploma in Informatica (EQF 4), 2012 - 2017

LANGUAGES

Italian — Native, English — Professional working proficiency (B2/C1), Sardinian — Native