

Federico Nicolas Cabrera

Cloud Solutions Architect | DevSecOps | AI Engineer | AWS & Azure

✉ fcabrera.all@gmail.com

in linkedin.com/in/federicocabreraf

github github.com/19fn

Summary

I'm a Cloud Solutions Architect with a DevSecOps and AI engineering background. I design, automate, and deliver secure, scalable cloud platforms on AWS and Azure, building security and compliance into every stage, from infrastructure and CI/CD pipelines to production.

I like to own problems end to end. I work closely with product and engineering teams to turn ideas into production-ready software, taking them from concept and architecture through implementation, troubleshooting, and delivery. I've also provided technical leadership, setting technical direction and making key architecture decisions.

Experience

Cloud Solutions Architect

Ewents

Sep 2025 - Present

- Architected a FedRAMP 20x continuous-compliance platform from the ground up: a distributed, read-only scanner deployed in each customer's AWS landing zone that pushes SigV4-authenticated evidence to a central multi-tenant control plane, documented through architecture decision records and diagrams.
- Led the design of the multi-account AWS landing zone and platform infrastructure (Terraform), implemented by the engineering team: management, audit, and log-archive accounts with organization-wide CloudTrail, AWS Config conformance packs, SCPs, IAM Identity Center, GuardDuty, Inspector, Security Hub-to-Jira integration, and SIEM, plus the ECS Fargate, RDS, and CloudFront product stack with an OIDC-based plan/apply pipeline and production approval gates.
- Led the design of the Federated Identity Service, implemented by the engineering team: federating human identity through each tenant's OIDC provider (Okta, Entra ID), issuing short-lived internal JWTs, and providing zero-trust service-to-service authentication via AWS STS identity attestation.
- Founded and led development of the core compliance engine, evolving it into an event-driven platform of services on ECS Fargate (S3, EventBridge, SQS with dead-letter queues and redrive, PostgreSQL), with FedRAMP 20x Key Security Indicator (KSI) validators for 46+ KSIs across 10+ families that automatically assess AWS (IAM, Organizations, CloudTrail, Config, Security Hub, GuardDuty, KMS, WAF), Okta, Jira, GitHub, and third-party services against NIST SP 800-53 controls.
- Built a framework-agnostic compliance runtime with provider execution contexts and a validator registry, and aligned all validators to the final FedRAMP 20x rules.
- Implemented zero-trust service-to-service authentication: RS256 JWT validation with JWKS caching, caller allow-lists, and fail-closed behavior, plus SigV4-signed scanner calls with IAM role-to-agent verification.
- Delivered multi-tenant data isolation, evolving from per-tenant databases resolved via Secrets Manager to a shared PostgreSQL model with Row-Level Security, including a rebuilt migration pipeline.

- Designed the DevSecOps CI/CD foundation on GitHub Actions: reusable service and migration pipelines, ECR/ECS deployments, releases, and security gates with Trivy, Bandit, pip-audit, gitleaks, mypy, and Ruff; added test-coverage gates to backend and frontend CI.
- Automated FedRAMP drift detection with scheduled workflows that compare vendored FedRAMP schemas and KSI definitions against the official upstream sources.
- Integrated a Go vulnerability management service into the Trust Center: added tenant sync from JWT claims, replaced its standalone Okta authentication with upstream token validation, built its ECR/ECS deployment pipeline, moved reports to S3, and added Corrective Action Plans.
- Shipped full-stack features across the NestJS/TypeScript backend and React frontend, including compliance history and control-family trend dashboards, compliance artifact discovery and indexing, and automated availability reports (closing an SSRF vulnerability in the process).
- Mapped FedRAMP 20x KSIs to NIST SP 800-53 controls, AWS implementation patterns, and machine-readable evidence sources, and authored a compliance-as-code repository (branch protection, change-management PR templates, Checkov/tfsec scanning, BC/DR plan, tagging policy, SIEM monitoring plan).
- Acted as technical lead alongside the client's VP of Engineering, defining integration scope and coordinating a mixed client and contractor team; set up AI-assisted development workflows with custom agents and Jira/GitHub/AWS MCP integrations.

G> Senior Cloud Engineer

Globant

Sep 2023 - Present

- Designed and built an AI usage and cost analytics platform (Python, FastAPI, SQL Server): a multi-tenant ingestion service that pulls per-user cost, credit, token usage, and engagement data from multiple AI vendor APIs into the enterprise data warehouse, feeding the data team's medallion (lakehouse) pipeline; migrated storage from PostgreSQL to SQL Server.
- Designed a pluggable provider architecture with a tenant registry (per-tenant vendor and live or deterministic mock mode), so new AI vendors plug in without changing the core pipeline; integrated a second vendor's cost and token-usage feeds end to end, from API integration to warehouse tables and per-user analytics endpoints.
- Built incremental watermark-based sync with overlap windows for late-arriving data, a reconciler job, per-feed health tracking, exponential-backoff retries, an in-process scheduler with distributed locking, and vendor-partitioned raw storage for replay and audit; defined an append-only bronze data contract and optimized warehouse queries with resumable index creation and zero-downtime schema migrations.
- Provisioned and secured the platform's Azure infrastructure with Terraform (App Service, Container Registry, Key Vault, networking, monitoring): scoped per-workspace API keys, Key Vault with managed identity, IP restrictions, a NAT Gateway for static-IP vendor allowlisting, and Azure Monitor and Application Insights alerts for failed ingestion, stalled feeds, API errors, and resource pressure.
- Built GitHub Actions CI/CD with linting, unit and live SQL Server integration tests, container image security scanning, dependency auditing, and versioned image deployment, plus a replayable mock-data framework and Docker Compose environments for local development, CI, and smoke testing.
- Configured and administered the organization-wide ChatGPT Enterprise and Claude Enterprise plans: SSO and user provisioning, workspace and seat management, credit allocation, usage quotas, and consumption metrics and reporting for cost control.
- Led several major releases of a production RAG API service (Python, FastAPI) that lets users bring their own documents: grounded answers with citations, retrieval tuning, timeouts, and per-request cost guardrails, backed by a retrieval-quality evaluation framework and post-deployment smoke tests.
- Improved the async RAG service's reliability with non-blocking I/O, idempotent operations, retry logic, automatic index rebuilds when the embedding model changes, and scheduled resource cleanup; added

privacy and security controls (hashed user identifiers, health and readiness probes, dependency vulnerability fixes), removed legacy components, and built reusable CI/CD pipelines with lint and test gates.

- Built and maintained multi-region, multi-environment Terraform for an enterprise GenAI platform: API Management, Azure Functions, App Service, Azure OpenAI, AI Search, Cosmos DB, Key Vault, Container Registry, and private networking (VNet Peerings, Private DNS Zones, Private Endpoints); designed a private-only network architecture for production AI services, and resolved production incidents including TLS failures, private DNS conflicts, and Azure Policy misconfigurations.
- Deployed and configured Azure API Management with multiple Azure OpenAI backends, implementing advanced load-balancing strategies through XML policies.
- Automated end-to-end API endpoint provisioning with Ansible (credential issuance, request validation, renewal, decommissioning, and templated user notifications), with failure classification, audit traceability, secure credential delivery that keeps secrets out of logs, and containerized regression test harnesses.
- Consolidated two legacy pipelines into one automated cloud subscription lifecycle system (Python, GitHub Actions) covering capacity monitoring, on-demand creation through a third-party provisioning API, configuration, and regulatory compliance submissions, orchestrated with dry-run and live modes, concurrency locking, idempotent reruns, and automatic recovery.
- Built a REST API gateway with 30+ operations for the subscription platform, replacing key-based access with identity-based OAuth/Entra ID authentication; automated compliance evidence capture with browser automation (screenshots and PDF reports) and batch submission, and added telemetry and capacity reporting.
- Administered over 1,000 Azure subscriptions, managing access with Entra ID groups, custom roles, and policies, and automated role creation, role assignments, and resource tagging with PowerShell 7 and the Az module.
- Built scheduled monitors (Python, GitHub Actions) with automated alerting and ticketing for multi-region endpoint health including WAF checks, AI model deprecations, cloud cost reporting, and request tracking, using vault-managed secrets and least-privilege CI/CD permissions, and complemented them with Application Insights availability tests and Azure alerts.
- Wrote 80+ architecture, security, and reliability documents, and delivered presentations and demos on real-world AI use cases to engineering teams.



Senior DevOps Engineer

Parallel Staff · Contract

Jun 2024 - Sep 2025

- Migrated a .NET SaaS application from VM-based servers to self-hosted Windows containers, running 100+ containers.
- Orchestrated containers on self-managed Azure Windows VMs using DuploCloud.
- Built fully custom, per-customer deployments with Terraform, script blocks, and a JSON customer list: adding a new entry automatically deploys that customer's application.
- Managed infrastructure capacity and cost, tracking VM CPU time, memory, and disk usage to handle the container workload.
- Configured a NAT Gateway to provide outbound internet access for the VM servers.
- Created Grafana reporting dashboards with custom queries and metrics.
- Managed domains and TLS certificates using ACME and GoDaddy.
- Supported and debugged the .NET SaaS application, including its ORM data layer.



DevOps Engineer (Senior Technician)

Endava

Jul 2023 - Sep 2023

- Automated infrastructure deployment and configuration using pipelines in Azure DevOps, Jenkins, and GitHub Actions (Environments, Reusable Workflows, Repository and Organization Secrets, Inputs).
- Deployed multiple environments (Dev/QA/PreProd/Prod) using Infrastructure as Code (IaC) with Terraform and custom ARM templates.
- Developed a multi-tenant Azure Active Directory solution with service principals, groups, and RBAC.
- Deployed and maintained 25+ microservices on Azure Kubernetes Service (AKS).
- Worked with Azure services: SQL Server, App Services, Cosmos DB, Data Factory, Data Lake, Virtual Machines, Logic Apps, Databricks, Machine Learning Workspace, Key Vault, AKS, and Cloud Shell.
- Worked with AWS services: EC2, Fargate, RDS, DynamoDB, VPC, S3, CloudWatch, and Route 53.
- Automated maintenance and configuration tasks, including SQL users and roles, using PowerShell, Bash, and SQL queries.
- Implemented TestOps with the Allure Framework.
- Backend development with Python and Flask (Jinja2 template engine).
- Built development environments with Docker and Docker Compose on Windows and Linux.
- Documented solutions in Confluence and Azure Wikis.
- Worked in Agile, multidisciplinary, and diverse teams across multiple locations and cultures.



DevOps Engineer (Technician)

Endava

Oct 2022 - Jun 2023



Junior DevOps Engineer (Junior Technician)

Endava

Apr 2022 - Sep 2022



Intern

Endava

Jan 2022 - Mar 2022

Education



Universidad Tecnológica Nacional

Engineer's degree, Software Engineering

Feb 2018 - Jul 2025

Licenses & Certifications



AWS Certified DevOps Engineer – Professional - Amazon Web Services (AWS)

Issued Feb 2026 · 078131344fa440108c685e67cc8ac5b1



HashiCorp Certified: Terraform Associate (003) - HashiCorp

Issued Dec 2024 · fc9d14f9-63cc-420a-a580-15137783c2d2



Microsoft Learn Cloud Skills Challenge at Build 2024 - Microsoft

Issued Jun 2024



Microsoft Certified: Azure Solutions Architect Expert - Microsoft

Issued Apr 2024 · E580630AC17DBA4E



Microsoft Certified: Azure Data Fundamentals - Microsoft

Issued Oct 2023 · 3B9A550FF75DE6AD



CKAD: Certified Kubernetes Application Developer - The Linux Foundation

Issued Jul 2023 · LF-lshxp2kcyi



AWS Partner: Accreditation (Technical) - Amazon Web Services (AWS)

Issued Jul 2023 · dd090c1d-c607-405f-8d12-597ba7298c5e



AWS Partner: Cloud Economics Accreditation - Amazon Web Services (AWS)

Issued Jul 2023 · 50ee21f9-d298-4bb2-9f6e-03333f636ac1



AWS Partner: Sales Accreditation (Business) - Amazon Web Services (AWS)

Issued Jul 2023 · de442de4-24ae-490d-b574-453209aa1629



OpenHack: Containers - Microsoft OpenHack

Issued May 2023



Microsoft Certified: DevOps Engineer Expert - Microsoft

Issued Apr 2023 · B401166B10857606



HashiCorp Certified: Terraform Associate (002) - HashiCorp

Issued Dec 2022



Microsoft Certified: Azure Administrator Associate - Microsoft

Issued Oct 2022 · 99E4C0EA208471CF



AWS Certified Cloud Practitioner - Amazon Web Services (AWS)

Issued May 2022 · 89032aba-d8a2-4922-8a2f-27f70f1328ff



Microsoft Certified: Azure Fundamentals - Microsoft

Issued Mar 2022 · 42359D6861AB2B3A