



Franck TOUNGA

Architecte Plateforme & Cloud AWS • Gouvernance & FinOps

13 ans d'expérience • 4x AWS • 3x Kubernetes • 1x Terraform • 1x Prometheus

+33 7 55 49 28 81 | tounga.franck@ng-itconsulting.com

<https://toungafranck.com> | Achères, Île-de-France • Freelance

PROFIL PROFESSIONNEL

Architecte plateforme et Cloud AWS avec 13 ans d'expérience, dont plus de 6 ans sur la conception, la gouvernance et l'exploitation d'environnements AWS multi-comptes. Aujourd'hui chez CAGIP, opérateur IT industriel du groupe Crédit Agricole, je porte les standards de la plateforme conteneurs et cloud à l'échelle du groupe et j'encadre une cellule CloudOps de 5 personnes sur une plateforme data AWS critique. J'interviens sur tout le cycle de vie d'une plateforme : Landing Zone et guardrails (AWS Organizations, SCP, IAM Identity Center), réseau hybride, industrialisation (Terraform, Atlantis, GitLab CI, Argo CD), sécurité et conformité DORA, observabilité et FinOps. Habitué aux environnements bancaires régulés et transverses (Crédit Agricole, BPCE, Banque du Luxembourg, Banque de France), je conjugue direction d'architecture et capacité à reprendre en main des chaînes techniques très pointues. Pédagogue confirmé (formateur Udemy, auteur), je place le partage de connaissances et les revues d'architecture au cœur de mon rôle.

COMPÉTENCES TECHNIQUES

Gouvernance & Plateforme Cloud

AWS Organizations, Control Tower / AFT, Service Control Policies (SCP), Landing Zone multi-comptes, IAM Identity Center (SSO), AWS Well-Architected Framework, standards d'architecture, conformité DORA

Réseau AWS

VPC, Transit Gateway, PrivateLink et endpoints VPC, VPN Site-to-Site, Direct Connect, Route 53, ALB/NLB, CloudFront, WAF, réseaux sans sortie Internet

Sécurité & DevSecOps

IAM, KMS, Secrets Manager, Security Hub, GuardDuty, AWS Config, Inspector, CloudTrail ; posture CSPM/KSPM, policy as code, Prisma Cloud, Cosign, CyberArk Conjur, Supply Chain Security

Services AWS

EKS, EC2, RDS, S3, Lambda, API Gateway, SQS, SNS, EventBridge, ECR, MWAA

FinOps & Optimisation des coûts

AWS Cost Explorer, AWS Budgets (alertes), Cost Allocation Tags, politique de tagging, Savings Plans, réservé / Spot, rightsizing, showback par entité

Infrastructure as Code & CI/CD

Terraform (modules, registre privé, remote state), Atlantis, Argo CD, GitOps, GitLab CI, Jenkins, Ansible, Git, industrialisation des déploiements

Observabilité & Exploitation

Amazon CloudWatch (métriques, logs, alarmes, dashboards), CloudTrail, Prometheus, Grafana, ELK, MCO, diagnostic et résolution d'incidents

Conteneurisation & Orchestration

Kubernetes, Amazon EKS, OpenShift 4.x, Docker, Helm, Harbor, IRSA, admission controllers

Développement & Architecture applicative

Java / Spring Boot, Angular, REST/Swagger, OAuth2/OIDC, Keycloak, PostgreSQL, ActiveMQ

Leadership & Accompagnement

Encadrement d'équipe, revues d'architecture, ateliers techniques, rédaction de DAT, mentorat, coaching, Scrum, Kanban

EXPÉRIENCE PROFESSIONNELLE

CAGIP (Groupe Crédit Agricole) | Septembre 2026 – à ce jour | Paris, France

Architecte Plateforme Groupe • Lead CloudOps AWS (Corporate Center)

Opérateur IT industriel du groupe Crédit Agricole, qui opère l'essentiel de la production informatique du groupe pour ses filiales et caisses régionales. Double mandat : standards de la plateforme conteneurs et cloud à l'échelle du groupe, et responsabilité opérationnelle de la plateforme data AWS du Corporate Center. Encadrement hiérarchique d'une cellule CloudOps de 5 personnes.

Architecture plateforme • périmètre Groupe :

- ▶ Définition des standards d'architecture conteneurs et cloud du groupe, déclinés en golden paths réutilisables (socle durci, pipeline, observabilité, secrets et policy embarqués) : 6 entités équipées, délai de mise à disposition d'un environnement projet ramené de 6 semaines à 5 jours.
- ▶ Pilotage de la trajectoire de convergence des distributions Kubernetes du groupe vers le socle OpenShift standardisé : cartographie des clusters, plan de migration par vagues et critères de sortie.
- ▶ Cadrage de la gouvernance multi-comptes AWS et des garde-rails associés : structure d'organisation, Service Control Policies, processus de dérogation instruit et tracé.
- ▶ Déclinaison des exigences DORA et des standards de sécurisation de la chaîne logicielle : signature d'images, SBOM, admission controllers, posture CSPM/KSPM avec findings rattachés aux équipes propriétaires ; écarts critiques réduits de 40 % sur le premier trimestre.
- ▶ Standard d'observabilité unifiée (métriques, journaux, traces), showback par entité et diffusion des pratiques FinOps de la plateforme mutualisée.
- ▶ Méthode de benchmark et de qualification des nouvelles solutions avant généralisation ; animation des revues d'architecture et des ateliers techniques auprès des équipes internes.

Lead CloudOps AWS • plateforme data du Corporate Center :

- ▶ Reprise en urgence d'une chaîne critique en relais du référent historique : organisation AWS multi-comptes (18 comptes, Control Tower / AFT, IAM Identity Center, eu-west-3), réseau sans sortie Internet, adressage mixte routable et CG-NAT, landing zone opérée par une équipe tierce.
- ▶ Livraison du socle d'un nouvel environnement AWS de bout en bout (conception, Terraform, revue, déploiement par la chaîne Atlantis) : VPC, Transit Gateway, ALB, cluster EKS, RDS PostgreSQL, buckets S3, endpoints VPC, IAM et fournisseur OIDC ; une cinquantaine de ressources livrées en 3 semaines.
- ▶ Déblocage de la chaîne sur preuve : échec d'adhésion de nœuds Kubernetes élucidé par l'analyse des journaux de flux VPC (absence de route retour sur la plage CG-NAT), et portée réelle des Service Control Policies établie par comparaison inter-comptes ; contournements déployés et dérogation argumentée.
- ▶ Industrialisation Terraform et GitOps : autoplan Atlantis étendu à l'ensemble des dépôts, socles alignés sur le registre de modules interne, environnements de préproduction et de production propagés, chaîne Argo CD et services de plateforme du cluster repris et étendus ; délai de livraison d'un environnement divisé par 4.
- ▶ Construction de l'alerting et de l'observabilité d'un périmètre qui n'en portait aucun, y compris en production : une trentaine d'alarmes CloudWatch, dashboards d'exploitation, procédures d'exploitation et de reprise documentées ; délai de remise en service divisé par 3.
- ▶ Sécurisation de la chaîne : secrets sortis des dépôts vers Secrets Manager, accès inter-comptes durcis, politiques IAM trop larges revues, écarts du scanner de sécurité des merge requests résorbés.
- ▶ Encadrement de la cellule CloudOps : priorisation des tickets par impact, revues de merge requests, montée en compétence de deux arrivants, cartographie de l'architecture produite à partir du code d'infrastructure.

Environnement technique : AWS (Control Tower, AFT, IAM Identity Center, EKS 1.34, ECR, S3, RDS PostgreSQL, KMS, IAM, Secrets Manager, Transit Gateway, PrivateLink, Route 53, ALB, MWAA, Lambda, SQS, SNS, EventBridge, ACM, CloudWatch, journaux de flux VPC), Terraform, Atlantis, GitLab CI, Argo CD, Kubernetes, OpenShift, GitOps, Snowflake, dbt, Airflow.

BPCE-IT | Août 2024 – Août 2026 | Paris, France

Lead DevSecOps / Architecte Sécurité Cloud AWS & Containers • Projet SCC

Mise en œuvre d'une stratégie complète de sécurisation du Cloud AWS et des plateformes containers

OpenShift/Kubernetes : standards et garde-rails de sécurité, gestion des secrets, durcissement d'images, sécurisation de la Supply Chain, maîtrise des coûts de la plateforme et accompagnement des équipes.

Réalisations clés :

- ▶ Provisionnement d'un cluster Amazon EKS sécurisé via Terraform et GitLab CI : réseau VPC (subnets privés, VPC endpoints, ALB/NLB), rôles IAM à moindre privilège (IRSA), chiffrement KMS.
- ▶ Optimisation des coûts de la plateforme EKS : rightsizing des node groups, instances Spot pour les workloads CI/CD non critiques, Savings Plans pour les charges stables.

- ▶ Tagging FinOps industrialisé dans les modules Terraform (Cost Allocation Tags par application et environnement), budgets et alertes AWS Budgets, suivi des consommations dans Cost Explorer.
- ▶ Mise en œuvre de standards de sécurité et de guardrails sur les comptes AWS : suivi des findings Security Hub, GuardDuty et AWS Config, priorisation et remédiation des non-conformités avec les équipes projets.
- ▶ Gestion des secrets avec CyberArk Conjur (SecretProviderClass, rotation), en cohérence avec AWS Secrets Manager et KMS pour les workloads AWS.
- ▶ Industrialisation de pipelines CI/CD sécurisés pour patcher, durcir et publier les images Red Hat (UBI8/UBI9) dans un catalogue interne standardisé (BuildConfig, ImageStream, registre Harbor).
- ▶ Supply Chain Security : Twistlock (Prisma Cloud) sur plusieurs clusters et signature des images avec Cosign.
- ▶ Accompagnement des équipes projets : revues d'architecture sécurité, ateliers IAM, RBAC, NetworkPolicy.

Environnement technique : AWS (EKS, IAM, VPC, KMS, Secrets Manager, Security Hub, GuardDuty, AWS Config, Cost Explorer, Budgets), Terraform, GitLab CI, Jenkins, OpenShift 4.x, Helm, Harbor, Prisma Cloud, Cosign, CyberArk Conjur, UBI8/9, SCC.

EDF | Juillet 2022 – Août 2024 | Paris, France

Architecte Cloud AWS / OpenShift · Projets SENARIO, SYNEMA, CAMERA

Migration et modernisation du back office vers une architecture hybride AWS / OpenShift : conception de l'infrastructure Cloud et du réseau hybride, pilotage FinOps et accompagnement des équipes applicatives.

Réalisations clés :

- ▶ Conception de l'architecture réseau hybride : AWS Direct Connect avec VPN Site-to-Site en secours, interconnexion des VPC (Transit Gateway, VPC Peering), résolution DNS hybride Route 53, exposition via ALB/NLB.
- ▶ Définition de l'architecture cible selon le AWS Well-Architected Framework (sécurité, fiabilité, performance, coûts) : EC2, S3, CloudFront, EKS, SQS, SNS, Lambda, API Gateway, dans la Landing Zone AWS Organizations du groupe.
- ▶ Prise en compte du pilier Optimisation des coûts dès la conception : estimation et dimensionnement des architectures cibles, arbitrages serverless (Lambda) / EC2, politiques de cycle de vie S3.
- ▶ Pilotage FinOps des trois projets : tagging par projet et environnement pour l'imputation des coûts, budgets et alertes AWS Budgets, suivi mensuel dans Cost Explorer et restitution aux chefs de projet.
- ▶ Réduction des coûts hors production : arrêt automatique des environnements en dehors des heures ouvrées, rightsizing EC2/RDS, instances réservées pour les charges stables.
- ▶ Contrôles de sécurité : CloudTrail, GuardDuty, Security Hub, WAF, KMS, IAM à moindre privilège.
- ▶ Accompagnement des équipes applicatives dans la migration et la modernisation : conteneurisation, découplage (SQS/SNS, ActiveMQ), API REST documentées (Swagger), authentification OAuth2.
- ▶ Supervision : CloudWatch (métriques, alarmes, dashboards d'exploitation) et Prometheus ; résolution d'incidents.
- ▶ Rédaction des DAT et des manifestes OpenShift ; animation des revues d'architecture.

Environnement technique : AWS (Direct Connect, VPN, Transit Gateway, VPC, Route 53, EKS, Lambda, SQS, SNS, WAF, KMS, CloudWatch, Cost Explorer, Budgets), Terraform, Ansible, GitLab, Kubernetes, OpenShift, Prometheus, PostgreSQL, HAProxy, Keycloak.

Ministère de la Justice | Mai 2021 – Septembre 2022 | Paris, France

Tech Lead / Expert DevOps Kubernetes-OpenShift · Projet PPN

Programme de numérisation des procédures pénales. Encadrement d'une équipe de 7 développeurs sur la centralisation des dossiers DPN et la mise en place d'une console de gestion des droits.

Réalisations clés :

- ▶ Encadrement d'une équipe de 7 développeurs : revues de code, montée en compétences, animation de sessions de coaching et de formation.
- ▶ Conception de pipelines CI/CD Jenkins pour les clusters Kubernetes, packaging Helm et monitoring Prometheus.
- ▶ Diffusion des bonnes pratiques Kubernetes : scan d'images Docker, validation des versions déployées, NetworkPolicy dans les Admission Controllers, volumes persistants, rôles et ServiceAccounts.
- ▶ Conception de la couche d'authentification (Spring Security) et d'une architecture MOM avec ActiveMQ.
- ▶ Bonnes pratiques craftsmanship et pilotage de la qualimétrie via SonarQube.

Environnement technique : Kubernetes, OpenShift, Jenkins, Helm, Java 11, Spring Boot 2, Angular 11, Elasticsearch, PostgreSQL, Docker, ActiveMQ, Nginx.

Banque du Luxembourg (BDL) | Septembre 2020 – Mai 2021 | Luxembourg

Architecte Cloud AWS · Projet AWS Landing Zone & EKS

Conception et mise en œuvre d'une plateforme Cloud AWS multi-comptes sécurisée, gouvernée et maîtrisée en coûts : Landing Zone, guardrails de sécurité, démarche FinOps et cluster EKS.

- ▶ Conception et déploiement de la Landing Zone AWS via Terraform : structure AWS Organizations (OU, comptes par environnement, comptes socle sécurité et journalisation), baseline IAM, VPCs et groupes de sécurité.
- ▶ Définition des guardrails de gouvernance : Service Control Policies (SCP), règles AWS Config, CloudTrail centralisé et GuardDuty activé sur l'ensemble des comptes.
- ▶ Centralisation des accès via IAM Identity Center (SSO) : permission sets par profil, principe du moindre privilège.
- ▶ Mise en place d'un cluster EKS via Terraform : rôles IAM, politiques de sécurité et intégration réseau.
- ▶ Provisionnement automatisé des ressources AWS (EC2, RDS, ALB/NLB, S3), configuration de CloudFront, Route 53 et CloudWatch (métriques, alarmes).
- ▶ Démarche FinOps : tagging (Cost Allocation Tags), suivi via Cost Explorer et AWS Budgets, rightsizing et instances réservées/Spot.
- ▶ Encadrement DevOps et formation de l'équipe sur Terraform, AWS et Well-Architected.

Environnement technique : AWS (Organizations, SCP, IAM Identity Center, AWS Config, CloudTrail, GuardDuty, VPC, EKS, RDS, Route 53, CloudWatch, Cost Explorer, Budgets), Terraform, Git, Docker, Kubernetes.

Renault Digital | Septembre 2019 – Octobre 2020 | Paris, France

Analyste & Développeur Fullstack · Projet Golden Eye

- ▶ Conception de la couche d'authentification OAuth2 via Keycloak (stack OpenIDConnect).
- ▶ Optimisation des requêtes SQL, tests d'intégration Quickperf et tuning JVM via VisualVM.
- ▶ Déploiement et dimensionnement d'instances EC2 sur AWS, optimisation des images Docker (multi-stage build), orchestration Docker Swarm.

Environnement technique : Java 11, Spring 5, Spring Boot 2, PostgreSQL, Nginx, Docker, GitLab, Git, VisualVM, AWS.

Buyway Services | Juin 2018 – Août 2019 | Bruxelles, Belgique

Analyste Big Data & Développeur Fullstack · Projet PSD2

- ▶ Conception du middleware de gestion des sessions SCA, pilotage de l'API d'envoi SMS et couche d'authentification JWT (Spring Security).
- ▶ Installation et administration d'un cluster Elasticsearch 6 sous Docker, monitoring des logs via la stack ELK et création de dashboards.
- ▶ Animation de 2 sessions hebdomadaires de formation Elasticsearch pour l'équipe.

Environnement technique : Elasticsearch, Kibana, Logstash, Java 8, Spring 4, Spring Boot, MySQL, PHP, Apache, Docker, Jenkins, Git.

AXA Groupe Solutions | Mars 2017 – Juin 2018 | Paris, France

Fullstack Engineer · Projet COMRM

- ▶ Définition de l'architecture du projet et des bonnes pratiques (versioning, gestion des erreurs, code review) ; conception du middleware communiquant avec une base MarkLogic.
- ▶ Couche de sécurité Spring Security, batch de processing XML Spring Boot et IHM Angular 5 de pilotage des services back office.
- ▶ Installation et configuration de Jenkins et d'Apache (proxy, load balancer, virtual hosts) ; montée en compétences des nouveaux collaborateurs.

Environnement technique : Java/JEE, Angular 5, Spring MVC, Spring Security, Spring Batch, MarkLogic, Unix, Tomcat, Jenkins, Spring Boot, Maven.

Banque de France | Juin 2015 – Août 2016 | Paris, France

Concepteur / Développeur · Programmes FIBRE & Portail Surendettement

- ▶ Couche d'accès aux données et de persistance, rédaction de spécifications techniques, chiffrement et développement de web services REST.
- ▶ PoC Spring Batch et implémentation JBeret de batchs d'insertion CSV ; fonctionnalités métier (réponses créanciers, notifications).

Environnement technique : Java 8, JavaEE, JAX-RS, Hibernate, AngularJS, JUnit, Oracle, JBoss, CDI, Maven, Git.

BforBank | Août 2013 – Juin 2015 | Paris, France

Concepteur / Développeur · *Projet LEMON*

- ▶ Développement de fonctions métier du site web (oppositions chèques et prélèvements) et de services REST pour les applications mobiles Android et iOS.
- ▶ Mise en place de correctifs dans le cadre de l'assistance technique.

Environnement technique : Spring MVC, Spring REST, Thymeleaf, Java 8, Mockito.

FORMATIONS & CERTIFICATIONS

Master en Architecture Logicielle et Design Patterns · University of New Brunswick (Canada), 2013

Diplôme d'Ingénieur en Électronique des Systèmes Embarqués · CPE Lyon, 2013

Formation Elasticsearch 6.0 · Zenika Training Center (Rennes), Mars 2018

Formation Spring Core 4.3 · Zenika Training Center (Rennes), Mai 2017

ACTIVITÉS COMPLÉMENTAIRES & ENGAGEMENT PÉDAGOGIQUE

- ▶ Formateur sur la plateforme Udemy : <https://www.udemy.com/user/tounga-franck/>
- ▶ Auteur du livre technique « Les nouveautés de Java 8 et la programmation fonctionnelle ».
- ▶ Conception et administration du blog technique <https://toungafranck.com> (articles bimensuels sur les SI et la transformation digitale).
- ▶ Animation d'une chaîne YouTube avec formations vidéo : Apache, Jenkins, Elasticsearch.
- ▶ Conception, administration et déploiement du site <https://www.ngconsulting.io> sur AWS.

LANGUES

Français · Langue maternelle

Anglais · Niveau professionnel