

FNA

Ingénieur DevSecOps

FORMATIONS & CERTIFICATIONS

- 2023** Diplôme National d'Ingénieur en Informatique, École supérieure privée d'ingénierie et de technologie
- 2019** Licence Fondamentale en informatique de gestion, Faculté des sciences économiques et de gestion

Certifications :

- | | |
|--|--------------------|
| ▪ K8S - Certified Kubernetes Administrator | Réf: LF1nqm7hn33q |
| ▪ HashiCorp - Terraform | Réf: HCP00204831 |
| ▪ Developing Secure Software | Réf: LF-rf4qjainkx |
| ▪ Linux Kernel Development | Réf: LF-fhqcjhx5ii |
| ▪ Intro GitOps | Réf: LF8jswysj84d |

COMPETENCES FONCTIONNELLES & TECHNIQUES

- Pilotage de l'automatisation des chaînes CI/CD (Jenkins, GitLab CI)
- Management de plateformes Kubernetes / Openshift
- Sécurité et conformité
- Supervision et automatisation
- Formation et transfert de compétences

COMPÉTENCES TECHNIQUES

- OS : Linux (CentOS, SELinux, Ubuntu, Debian), Windows
- Containerisation : Docker, Containerd
- Orchestration : Kubernetes, Openshift
- CI/CD : Jenkins, GitLab CI
- IaC : Ansible, Terraform, Vagrant.
- Scripting : Bash, Groovy, PowerShell.
- Serveur : Tomcat, JBoss, WildFly, NGINX.
- Cloud : AWS, Microsoft Azure DevOps, GCP
- Versioning : Git, SVN
- Build : Nexus, Maven, NPM
- Base de données : Oracle, PostgreSQL
- Test : OPA conftest, CIS Benchmark

- Scanner (SAST & DAST) : Sonar, NexusIQ, Fortify, Sysdig, OWASPZAP, Trivy
- Collaboration : Jira, Confluence, Wiki, Microsoft 365

Anglais : Professionnel.

EXPERIENCES PROFESSIONNELLES

SOCIETE GENERALE

Juin 2023 à février 2026

Ingénieur DevSecOps

Contexte :

Une plateforme Middle Office est généralement conçue pour améliorer la gestion des opérations intermédiaires entre le front office (activités de trading, gestion de portefeuille, leasing et collatéral) et le back office (gestion des règlements, conformité, etc.). Elle vise à optimiser les processus, réduire les risques opérationnels et améliorer l'efficacité. Au sein d'une équipe Agile de 22 personnes (1 Scrum master, 1 Product Owner et 1 ingénieurs DevOps, 4 TechLeads, 16 Développeurs)

Responsabilités principales :

- Direction d'une équipe DevOps transverse en charge de la migration complète du cloud interne hybride (DIN) vers le cloud public Azure, tout en gérant des services multi-cloud (AWS, GCP).
- Stratégie et gouvernance : Conception et supervision des environnements (intégration, recette, pré production, production) via une approche Infrastructure as Code (Terraform), en garantissant la cohérence et la sécurité sur tous les environnements.
- Pilotage de l'automatisation : Mise en place et optimisation des chaînes CI/CD (Jenkins, GitHub Actions) avec développement de bibliothèques partagées pour standardiser les processus et améliorer la qualité des déploiements.
- Management de plateformes Kubernetes : Supervision du provisionnement et de la gestion des clusters Kubernetes (AKS) via Helm Charts, avec mise en place de politiques de sécurité et de coûts.
- Migration des bases de données : Pilotage de la migration des bases PostgreSQL on-premise vers des services managés Azure Database for PostgreSQL, en assurant la continuité et la performance.
- Sécurité et conformité : Responsable de la sécurisation des accès et des secrets via HashiCorp Vault et Ansible, et application des bonnes pratiques Red Hat (à hauteur de 60%).
- Supervision et optimisation : Implémentation d'outils de monitoring (Prometheus/Grafana) et de sécurité Sysdig Secure pour une supervision proactive des performances et des coûts.
- Gestion des applications et registres : Maintenance des serveurs d'application (Tomcat, JBoss) et migration du registre Docker vers Harbor pour une gestion centralisée des images.
- Formation et accompagnement : Animation de transferts de connaissances (knowledge transfer) pour les équipes métier sur les outils DevOps et les bonnes pratiques cloud.

Synthèse : La Middle Office Platform est un projet qui est autonome en termes d'opérations maintenant et ne nécessite pas une intervention humaine.

Environnement : Ansible, Jenkins, GitLab CI, GitHub Action, Linux, Docker, Groovy, Terraform, Helm Chart, Bash, K8S, Openshift, Grafana, PSQL, Fortify, Sysdig Secure, Cloud hybrid (AWS, Azure, GCP, Internal Provider), S3, Vault, File Storage, RabbitMQ, Snowflake, Sysdig, Sonar, SAST, DAST, Load Balancing, Dataviz, Advisory.

GENERALI

Juillet 2022 à Mai 2023

Ingénieur DevSecOps

Contexte :

Chrysalide est une application de gestion d'assurances santé et prévoyance. Une application développée avec Spring boot pour le backend et Angular pour le frontend et des micro-services RESTFUL. Au sein d'une équipe Agile de 7 personnes (1 Scrum master, 1 Product Owner et 4 ingénieurs DevOps).

Responsabilités principales :

- La conception et la configuration des environnements d'intégration, de recette, de préproduction et de production.
- L'automatisation des déploiements et la mise en production sur les environnements IBM gérer par Kyndryl.
- L'automatisation des chaînes CI/CD à l'aide de l'outil d'Infrastructure as Code (IaC) Ansible.
- La mise en œuvre de Vault Ansible pour sécuriser les variables sensibles telles que les mots de passe des nœuds cibles, les clés SSH, etc.
- Le développement de bibliothèques partagées (shared library) au niveau de Jenkins afin d'assurer l'aspect générique du processus.
- L'optimisation des scripts d'installation en Bash et l'externalisation des variables.
- La mise en place et la maintenance des serveurs d'application (Tomcat, JBoss, WildFly).
- La conteneurisation de la totalité des applications.
- L'automatisation de la gestion des bases de données PSQl à l'aide de scripts déclenchés par des pipelines Jenkins paramétrables pour l'importation, l'exportation, le clonage et la suppression. Cela a réduit les coûts en termes de temps de 40% et le risque d'erreurs humaines de 90%.
- Application des bonnes pratiques recommandées par Red Hat du côté d'Ansible.
- La mise en place de cron jobs pour les pipelines Jenkins qui analysent le code avec l'outil Sonar chaque jour à 18h30 (30 18 * * * *).
- Migration vers le cloud AWS en mode SaaS.
- Participation aux ateliers de définition de l'architecture cloud.
- Gestion de la configuration et de l'administration des clusters Kubernetes pour structurer les applications conteneurisées.
- Encadrement d'une équipe de 5 personnes (DevSecOps) chargée de scanner, signaler et assister l'équipe projet dans la correction des vulnérabilités au niveau du code et des dépendances.
- Gestion des vulnérabilités et évaluation des vulnérabilités.

Synthèse : La création d'une chaîne d'intégration robuste et complète, alliant technologie, synergie d'outils, autonomie et sécurité, a entraîné une réduction de 60% du temps nécessaire pour les versions et le déploiement en production.

Environnement : Ansible, Jenkins, Linux, Docker, Groovy, YAML, Bash, K8S, PSQl, Sonar, NexusIQ, Fortify, Git, GitLab CI, Sysdig Secure, Burp Suite, OWASP ZAP, Talisman.

MALAKOFF HUMANIS

Juillet 2020 à Juin 2022

Ingénieur DevOps

Contexte :

Octave est une application d'assurance qui permet de gérer les polices, simuler les coûts des assurances vie et non-vie et gérer les sinistres. Une application développée avec Java et Angular et des micro-services RESTFUL à travers les architectures MVC et MVVM.

Au sein d'une équipe avec la méthode Scrum qui se compose d'un Product owner, un scrum master, 3 ingénieurs DevOp avec la méthodologie Agile.

Responsabilités principales :

- Dockerisation de la solution
- Mise à jour des outils de travail Jenkins, Maven.
- Mise en place des pipelines CI/CD pour (INT, UAT, PréProd et Prod)
- Externalisation des variables pour assurer une mise à jour fluide, fiable et générique.
- Migration de Artifactory à Nexus
- Mise en place de la configuration LDAP dans Jenkins, Nexus, GitLab.
- Optimiser les projets Ansible en termes de bonnes pratiques et généricité.
- Implémenter des outils de monitoring pour suivre l'état des environnements.
- Mise en place de Vault coté Ansible pour sécuriser les données sensibles au niveau des playbooks, rôles et services.
- Gérer les bases de données PSQl.
- Migration vers AWS.
- Utilisation de l'architecture à trois niveaux dans AWS (VPC, EC2, Application Load Balancer, ASG, RDS).
- Création de l'environnement à l'aide de Terraform.
- Mise en place de la chaîne CI/CD avec Jenkins, S3, et AWS Launch Template.
- Optimisation des coûts par la création d'une fonction Lambda pour le démarrage/arrêt des environnements (réduisant le nombre d'instances EC2 dans les Auto Scaling Groups à zéro et arrêtant le RDS).
- Création d'un job pour arrêter les environnements chaque jour après les heures de travail.

Synthèse : Le projet a été caractérisé par la dockerisation de la solution, la mise à jour des outils tels que Jenkins et Maven, la migration vers Nexus, et la configuration LDAP. Une migration réussie vers AWS a été réalisée avec une architecture à trois niveaux, et des optimisations significatives ont été apportées à la chaîne CI/CD, incluant la création d'une fonction Lambda pour le contrôle des coûts et l'automatisation de l'arrêt des environnements.

Environnement : Ansible, Jenkins, Docker, Maven, Nexus, Artifactory, GitLab, Git, Prometheus, Grafana, PSQl, AWS (VPC, EC2, LB, RDS, ASG, S3, Lambda), Terraform.

LLOYDS

Juin 2019 à Juin 2020

Ingénieur DevOps

Contexte :

Money For Life (M4L) est une application assurance bancaire qui permet aux clients d'investir et de penser à leurs retraites. Développer par un backend Java et frontend Angular.

Au sein d'une équipe adopte la méthodologie Agile avec la méthode Scrum qui se compose de 10 personnes. Un Product owner, un scrum master, 2 ingénieurs DevOps, 4 ingénieurs de développement et 2 testeurs..

Responsabilités principales :

- Migration de SVN vers Git.
- Conception et intégration de la chaîne CI/CD en utilisant Jenkins comme serveur d'automatisation.
- Migration vers Nexus.
- Duplication des environnements à l'aide d'Ansible.
- Élaboration des scripts d'automatisation pour toutes les opérations sur les bases de données.
- Intégration des outils de scan et de test du code (Sonar, NexusIQ,).
- Création des Dockerfiles et optimisation de la taille minimale des images.
- Analyse des vulnérabilités des images Docker.
- Publication des images dans un référentiel privé (Nexus).

Synthèse : Le projet a connu une transition significative, passant de technologies obsolètes à des solutions innovantes et récentes.

Environnement : SVN, Git, Jenkins, Nexus, Ansible, Sonar, NexusIQ, Docker, Bash.