

# INTERNSHIP REPORT

Téo Franoux

Epitech, Third Year

Société Générale Luxembourg  
Epitech Nancy

–

April to July 2025

**Implementation and Securing of Rundeck with Vault Plugin**

*Internship Supervisor : Bertrand Docquois*

# Table des matières

<i>Table des matières.....</i>	<i>1</i>
Section 1 : Rapport pour un Nouvel Employé.....	3
Introduction.....	3
Description de l'Entreprise.....	3
Le Service où J'ai Travaillé : GTS (Global Technology Services).....	3
Qu'est-ce que l'Infrastructure Informatique ?.....	3
Quelques Chiffres sur GTS.....	4
Description de l'Équipe.....	4
Explications Détaillées des Outils.....	5
Rundeck.....	5
Vault.....	5
SCM (Source Control Management).....	5
Le Plugin Vault pour Rundeck.....	6
Différents environnements.....	6
Description du Projet.....	6
Contexte et Objectifs du Projet.....	7
Description de BeApi.....	7
Problèmes Identifiés.....	8
Incidents et Motivations.....	9
Objectifs du Projet.....	10
Solution Mise en Œuvre.....	10
Sécurisation de l'accès à Rundeck.....	10
Intégration de Vault.....	10
Amélioration de la collaboration et de la sauvegarde.....	10
Processus de Développement et de Test.....	11
Défis Rencontrés et Solutions.....	12
Gestion des Listes de Permissions Complexes.....	12
Configuration des Accès pour un Coffre-fort Numérique (Plugin Vault).....	12
Résistance au Changement.....	13
Instructions Limitées.....	13
Intégration avec les Systèmes Existants.....	13
Résultats et Impact.....	13
Amélioration de la Sécurité.....	13
Efficacité Opérationnelle.....	14
Collaboration Améliorée.....	14
Feedback Positif de l'Équipe.....	14

Leçons Apprises.....	14
Importance de la Sécurité.....	14
Collaboration et Communication.....	14
Résolution de Problèmes.....	14
Adaptabilité.....	15
Conclusion.....	15
Section 2 : Lettre au Manager.....	15
Introduction.....	15
Qualités et Atouts.....	16
Résultats Concrets.....	16
Découverte d'un Intérêt pour l'Infrastructure Informatique.....	16
Proposition pour un Nouveau Projet.....	17

# Section 1 : Rapport pour un Nouvel Employé

## Introduction

Pendant mon stage de quatre mois à la Société Générale Luxembourg, j'ai travaillé sur Rundeck, un outil d'automatisation des opérations. Ma mission principale était de tester et implémenter le plugin Vault pour Rundeck en version community, ainsi que de travailler sur son SCM.

## Description de l'Entreprise

La Société Générale Luxembourg est une filiale du groupe Société Générale, l'une des principales institutions financières en Europe. Elle offre une large gamme de services bancaires et financiers, incluant la gestion de patrimoine, les services de banque privée, et les solutions de financement pour les entreprises. La sécurité et la gestion efficace des accès sont cruciales dans ce secteur pour protéger les données sensibles des clients.

La société est présente dans plusieurs pays et emploie des milliers de professionnels qui travaillent ensemble pour offrir des services de haute qualité. Elle est reconnue pour son innovation et son engagement envers ses clients, ce qui en fait un acteur clé dans le secteur bancaire européen.

## Le Service où J'ai Travaillé : GTS (Global Technology Services)

Le GTS, ou Global Technology Services, est un département clé au sein de la Société Générale qui se concentre sur la gestion et la maintenance de l'infrastructure technologique de l'entreprise. Mais qu'est-ce que cela signifie exactement ?

Imaginez que la Société Générale est une grande ville. Dans cette ville, il y a des bâtiments, des routes, des services publics et des systèmes de communication. Tout cela doit fonctionner de manière fluide et coordonnée pour que les habitants (dans ce cas, les employés et les clients de la banque) puissent vivre et travailler efficacement.

GTS est comme le service des travaux publics et des services essentiels de cette ville. Il s'assure que tout fonctionne correctement, des bâtiments (serveurs et centres de données) aux routes (réseaux et connexion internet) en passant par les services publics (applications et postes de travail).

## Qu'est-ce que l'Infrastructure Informatique ?

L'infrastructure informatique est l'ensemble des éléments nécessaires pour que les systèmes technologiques d'une entreprise fonctionnent. Cela comprend :

- Les Postes de Travail : Ce sont les ordinateurs, portables et tablettes que les employés utilisent quotidiennement.
- Les Serveurs et Machines Virtuelles : Les serveurs sont des ordinateurs puissants qui stockent et gèrent les données et les applications. Les machines

virtuelles sont comme plusieurs ordinateurs virtuels fonctionnant sur un seul serveur physique, permettant une meilleure utilisation des ressources.

- Les Applications et Services Collaboratifs : Ce sont les logiciels et outils que les employés utilisent pour collaborer et effectuer leur travail, comme les emails et les systèmes de messagerie.
- Les Réseaux et la Téléphonie : Cela inclut tout ce qui permet de connecter les différents équipements entre eux, ainsi que les systèmes de téléphonie qui permettent aux employés de communiquer efficacement.

En termes simples, l'infrastructure informatique est la colonne vertébrale technologique qui permet à une entreprise comme la Société Générale de fonctionner de manière fluide et efficace.

## Quelques Chiffres sur GTS

Pour vous donner une idée de l'ampleur des opérations de GTS, voici quelques chiffres clés

- Effectifs Mondiaux : GTS compte près de 4000 employés et prestataires de services à travers le monde.
- Postes de Travail : GTS gère plus de 103 000 postes de travail, qui incluent des ordinateurs portables, des ordinateurs de bureau et des tablettes.
- Emails : Chaque jour, plus de 50 millions d'emails sont gérés par les systèmes de GTS.
- Serveurs et Machines Virtuelles : GTS maintient 15 000 serveurs physiques et 100 000 machines virtuelles pour assurer le bon fonctionnement des applications et services.

Pour donner une idée de la répartition géographique des effectifs de GTS :

- À Paris, le centre principal compte 2070 employés.
- Au Luxembourg, l'équipe est plus petite, mais tout aussi essentielle, avec approximativement 30 employés.

Ces chiffres montrent l'ampleur et l'importance du rôle de GTS dans le maintien des opérations technologiques de la Société Générale. Travailler dans ce département m'a permis de voir directement comment une infrastructure informatique bien gérée peut soutenir une grande organisation et ses clients à travers le monde.

## Description de l'Équipe

Notre équipe d'infrastructure informatique était composée de quatre membres, chacun ayant des responsabilités spécifiques :

- Bertrand - Chef de Projet (Mon Manager) :  
Bertrand s'assure que notre travail se déroule bien et que nous atteignons nos objectifs. Il nous dit ce que nous devons faire et s'occupe de découvrir les besoins de son propre manager. Par exemple, si l'entreprise décide de déplacer

une partie de son infrastructure à Paris, Bertrand nous en parlera et nous attribuera des tâches en fonction des compétences de chacun.

- Boris - Expert Kubernetes :

Boris s'occupe de groupes de serveurs qui fonctionnent ensemble pour faire tourner des applications. Il utilise un outil appelé Ansible, qui l'aide à configurer et gérer ces serveurs efficacement. Son travail consiste à s'assurer que les services sont toujours accessibles, fonctionnent correctement et sont faciles à utiliser pour les autres équipes.

- Marie-France - Experte Automatic Automation :

Marie-France travaille avec un outil appelé Automatic Automation, qui est utilisé pour automatiser et gérer divers processus informatiques au sein de l'entreprise. Son rôle est de s'assurer que ces processus s'exécutent de manière fluide et sans interruption. Elle surveille le système pour identifier et résoudre rapidement tout problème, garantissant ainsi que Automatic Automation fonctionne toujours correctement et que tous les services qui en dépendent restent disponibles et efficaces.

- Moi-même - Stagiaire en Infrastructure :

Mon rôle était de tester et d'implémenter le plugin Vault pour Rundeck, de réviser et de restructurer les ACL pour améliorer la sécurité, et de travailler sur le SCM de Rundeck pour garantir la stabilité des modifications.

## Explications Détaillées des Outils

### Rundeck

Rundeck est comme un assistant qui s'occupe des tâches répétitives pour vous. Imaginez que vous avez une liste de tâches quotidiennes à faire à la maison, comme arroser les plantes ou faire la vaisselle. Rundeck fait ces tâches pour vous, mais dans le monde informatique, comme sauvegarder des fichiers ou redémarrer un ordinateur.

### Vault

Vault est une boîte forte numérique. Vous y rangez vos objets de valeur, mais au lieu de bijoux ou de documents importants, elle garde des informations secrètes, comme des mots de passe, en sécurité. Seul quelqu'un de confiance peut y accéder quand c'est nécessaire.

### SCM (Source Control Management)

Dans le contexte de Rundeck, le SCM agit comme un journal de bord qui enregistre chaque modification apportée aux scripts et configurations utilisés pour automatiser les tâches. Imaginez que vous avez un livre de recettes pour gérer vos tâches

quotidiennes, où vous notez chaque changement que vous faites. Si vous modifiez une recette (ou un script dans Rundeck) et que cela ne fonctionne pas comme prévu, vous pouvez simplement revenir à la version précédente qui fonctionnait bien.

Cela garantit que vous pouvez toujours revenir en arrière si quelque chose ne va pas. De plus, ce journal facilite la collaboration au sein de l'équipe, car chacun peut voir qui a fait quoi et quand, et travailler ensemble plus efficacement.

## Le Plugin Vault pour Rundeck

Le plugin Vault pour Rundeck permet à Rundeck d'utiliser Vault pour gérer les informations sensibles nécessaires à l'exécution des tâches automatisées. Cela signifie que lorsque Rundeck doit exécuter une tâche qui nécessite des informations sensibles, comme un mot de passe ou une clé secrète, il peut les récupérer temporairement auprès de Vault.

Le processus fonctionne comme suit : lorsque Rundeck commence une tâche qui nécessite une information sensible, il demande cette information à Vault. Vault fournit alors cette information à Rundeck de manière sécurisée. Une fois la tâche terminée, l'information est à nouveau sécurisée dans Vault, assurant qu'elle n'est jamais exposée de manière non sécurisée.

Ainsi, le plugin Vault permet à Rundeck d'exécuter des tâches qui nécessitent des informations sensibles sans que ces informations ne soient jamais stockées ou exposées de manière non sécurisée. Le plugin agit donc comme un intermédiaire sécurisé entre Rundeck et les informations sensibles stockées dans Vault.

## Différents environnements

- Développement (dev) : Utilisé par les développeurs pour écrire et tester du code. Généralement local ou sur un serveur dédié.
- Intégration (int) : Employé pour tester les interactions entre différents modules ou systèmes. Assure que le code fonctionne correctement avec d'autres composants.
- Production (prod) : Environnement où le code final est déployé et utilisé par les utilisateurs finaux. Configuré pour être stable et fiable.

## Description du Projet

Mon projet consistait à tester et à implémenter un plugin appelé Vault pour Rundeck. Vault est un outil qui permet de stocker et de gérer des informations sensibles, comme des mots de passe ou des informations sensibles, de manière sécurisée.

La version community de Rundeck signifie que c'est une version gratuite et open-source, mais elle nécessite plus de configurations manuelles que la version payante. Cela signifie que j'ai dû faire plus de travail pour tout configurer correctement.

L'un des aspects clés de mon travail a été de réviser et de restructurer les ACL (Access Control Lists) dans Rundeck. Les ACL sont comme des listes de contrôle qui déterminent qui a le droit de faire quoi. Dans Rundeck, les ACL déterminent quelles équipes peuvent accéder à quelles fonctionnalités. En révisant et en restructurant ces listes, nous avons pu améliorer la sécurité globale du système.

J'ai également travaillé sur le SCM de Rundeck pour améliorer la collaboration, tracer les changements, permettre un retour en arrière en cas d'erreur, et garantir l'automatisation tout en maintenant la sécurité.

## Contexte et Objectifs du Projet

La sécurité des données constitue une priorité absolue pour la Société Générale Luxembourg. Dans un contexte marqué par une hausse significative des cyberattaques et des violations de données, la protection des informations sensibles des clients et de l'entreprise est devenue plus cruciale que jamais. Rundeck, un outil essentiel utilisé pour automatiser et orchestrer diverses tâches opérationnelles, joue un rôle clé dans l'efficacité et la fiabilité des opérations.

Cependant, pour répondre aux normes élevées de sécurité exigées par l'industrie bancaire, il était impératif de renforcer la sécurité associée à son utilisation. Malgré son utilité et son efficacité, comme tout système puissant, Rundeck nécessite des précautions de sécurité rigoureuses pour minimiser tout risque et garantir une protection optimale des données.

## Description de BeApi

BeApi est un outil développé en interne par la Société Générale pour permettre à différentes équipes de lancer divers tâches via Rundeck. Pour comprendre ce qu'est une API, imaginez-la comme un serveur dans un restaurant : vous passez votre commande (vous faites une demande) et le serveur vous apporte votre plat (la réponse à votre demande). De la même manière, BeApi agit comme un intermédiaire sécurisé et contrôlé qui permet à différents logiciels de communiquer et d'accéder aux fonctionnalités de Rundeck.

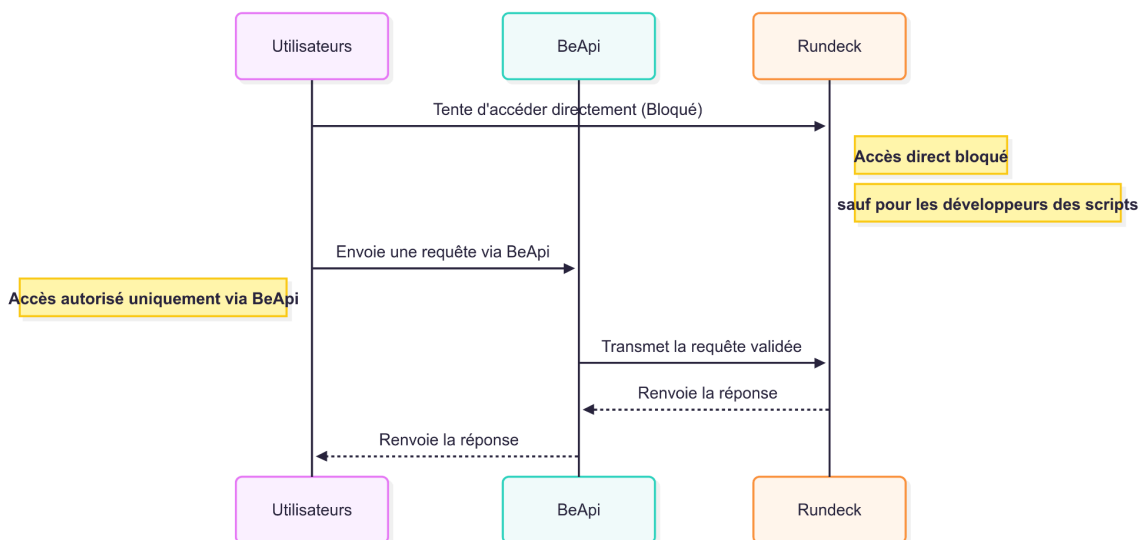
Pour faciliter son utilisation, BeApi utilise une interface Swagger, qui peut être comparée à un menu dans un restaurant. Ce menu liste toutes les fonctionnalités disponibles (les plats) et explique comment les utiliser (comment commander). Ainsi, diverses équipes peuvent facilement comprendre et utiliser les fonctionnalités offertes par BeApi sans avoir besoin de connaissances techniques approfondies.



## Problèmes Identifiés

### → Contournement de BeApi:

- ◆ Certaines équipes utilisaient directement Rundeck en environnement de développement, contournant ainsi les contrôles de sécurité mis en place par BeApi.



### → Risques de Sécurité:

- ◆ En utilisant directement Rundeck, les équipes ignoraient les contrôles de sécurité, ce qui équivaut à accéder à une fête privée sans invitation.

### → Impact sur la Production:

- ◆ Certains scripts exécutés dans l'environnement de développement pouvaient affecter les environnements de production, posant un risque significatif.

### → Processus Incomplets:

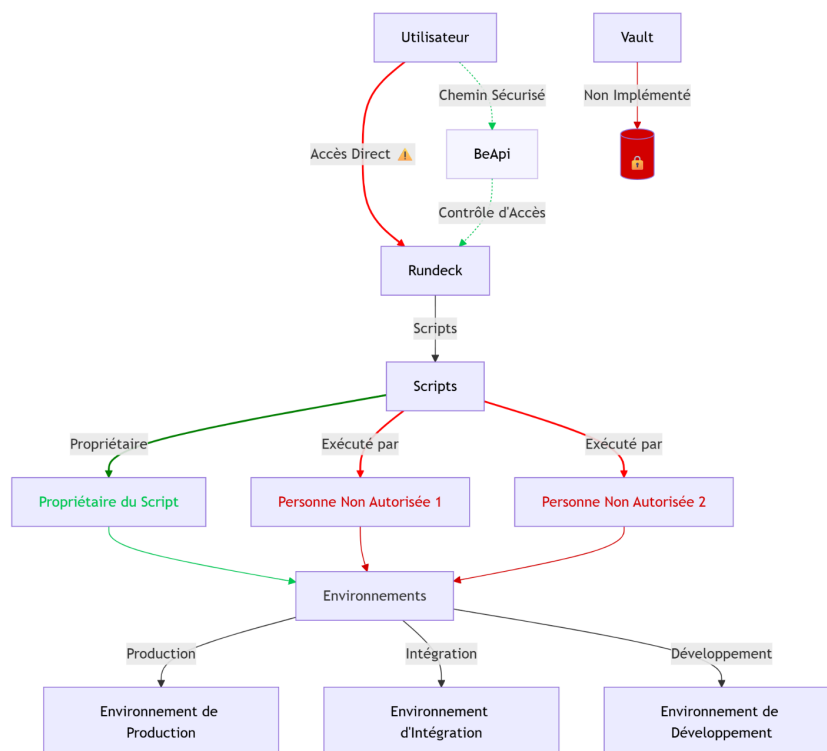
- ◆ Lorsqu'une procédure échouait, des corrections manuelles via Rundeck laissaient des éléments inutiles qui encombraient et pouvaient causer des problèmes.

### → Utilisation de Scripts Inconnus:

- ◆ Certains utilisateurs exécutaient des scripts qu'ils ne comprenaient pas pleinement, ce qui était dangereux car ils pouvaient mal les utiliser ou ignorer des étapes cruciales.

### → Nécessité de Sécuriser l'Accès:

- ◆ Il était essentiel de sécuriser l'accès à Rundeck et de s'assurer que toutes les exécutions de scripts passent par BeApi, où les contrôles d'accès sont appropriés.
- Migration des Informations sensibles (secrets) vers Vault:
  - ◆ Il était important de migrer la gestion des secrets vers Vault pour une sécurité renforcée, car le stockage par défaut de Rundeck n'était pas suffisamment sécurisé.



## Incidents et Motivations

Il y a eu des incidents où des scripts critiques, censés être exécutés uniquement via BeApi avec les contrôles d'accès appropriés, étaient lancés directement depuis Rundeck en développement. Cela posait non seulement un risque opérationnel en termes de stabilité et de performance des systèmes de production, mais aussi un risque de non-conformité avec les politiques de sécurité internes de la Société Générale.

Imaginez un scénario où une commande critique, comme la modification d'un mot de passe d'utilisateur ou suppression d'un serveur, est exécutée sans les vérifications nécessaires. Cela pourrait causer des problèmes majeurs et des pertes financières.

Ces incidents ont souligné la nécessité de sécuriser l'accès à Rundeck et de s'assurer que toutes les exécutions de scripts passent par BeApi, où les contrôles d'accès

appropriés sont en place. De plus, il était crucial de migrer la gestion des secrets hors du stockage par défaut de Rundeck, qui n'était pas suffisamment sécurisé. En effet, ce stockage permettait à toutes les équipes d'avoir potentiellement accès aux secrets de tout le monde. En migrant vers Vault, une solution plus robuste et sécurisée, nous avons pu mettre en place des contrôles d'accès plus stricts et limiter l'accès aux secrets uniquement aux équipes autorisées.

## Objectifs du Projet

L'objectif principal du projet était de tester et d'implémenter le plugin Vault pour Rundeck, qui permet de stocker et de gérer les secrets de manière sécurisée. En utilisant Vault, nous pouvons centraliser le stockage des secrets, réduire le risque de fuites de données, et améliorer la gestion des accès. Complémentairement, l'utilisation d'un système de gestion de version (SCM) pour les configurations et les scripts Rundeck permet de suivre les modifications, de faciliter la collaboration entre les équipes, et d'assurer une meilleure gestion des versions.

## Solution Mise en Œuvre

Pour résoudre ces problèmes, plusieurs mesures ont été prises :

### Sécurisation de l'accès à Rundeck

J'ai restructuré les listes de contrôle d'accès (ACL) dans Rundeck pour définir des permissions granulaires pour chaque utilisateur et chaque projet. Les ACL fonctionnent comme une liste d'invités pour une fête privée : seuls les noms sur la liste peuvent entrer. Cette approche a permis de s'assurer que seuls les utilisateurs autorisés pouvaient exécuter des scripts, et uniquement dans les environnements pour lesquels ils avaient les droits appropriés. De plus, cette restructuration a permis de limiter les risques de manipulation non autorisée et d'améliorer la traçabilité des actions effectuées.

### Intégration de Vault

J'ai implémenté et configuré le plugin Vault pour Rundeck, ce qui m'a permis de retirer les secrets du stockage interne de Rundeck, qui était moins sécurisé. En centralisant ces secrets dans Vault, j'ai bénéficié d'un contrôle d'accès plus fin et d'une capacité d'audit améliorée. Vault offre des fonctionnalités avancées de gestion des secrets, telles que le chiffrement, la rotation automatique des clés (mot de passe), et la journalisation détaillée des accès. Ces améliorations ont significativement réduit les risques de fuite de données sensibles et ont renforcé la conformité avec les politiques de sécurité internes.

## Amélioration de la collaboration et de la sauvegarde

Pour améliorer la collaboration et assurer la traçabilité des modifications, j'ai intégré un système de gestion de version (SCM) pour les configurations et les scripts Rundeck. Cela m'a permis non seulement de sauvegarder les modifications, mais aussi de faciliter le travail d'équipe en permettant un suivi précis des changements et une gestion efficace des versions. Cette approche m'a également permis de restaurer rapidement des configurations précédentes en cas de besoin, tout en assurant une meilleure coordination entre les différents membres de l'équipe.

## Processus de Développement et de Test

Le processus de développement et de test pour ce projet a été divisé en plusieurs étapes :

### Analyse des Besoins :

- Comprendre les exigences de sécurité de l'entreprise et les fonctionnalités offertes par le plugin Vault.
- Identifier les lacunes dans la gestion actuelle des secrets et les améliorations potentielles.

### Configuration Initiale :

- Installer le plugin Vault dans Rundeck.
- Configurer le plugin Vault dans les fichiers de configuration de Rundeck.

### Tests Initiaux :

- Tester le plugin Vault dans un environnement isolé pour s'assurer qu'il fonctionne comme prévu.
- Identifier et résoudre les problèmes de configuration et de compatibilité.

### Révision des ACL :

- Analyser les ACL existantes et identifier les permissions inutiles ou excessives.
- Réviser et restructurer les ACL pour minimiser les risques de sécurité et améliorer la gestion des accès.

### Intégration avec SCM :

- Intégrer Rundeck avec le système de gestion de versions pour suivre les modifications apportées aux configurations.
- Automatiser les tests et les déploiements pour garantir la stabilité des modifications.

### Présentation à l'Équipe :

- Présenter les résultats des tests, les avantages du plugin Vault, et l'intégration du SCM pour la gestion des configurations et des scripts.
- Expliquer le processus d'implémentation, incluant la restructuration des ACL pour améliorer la sécurité et la gestion des accès.
- Décrire les étapes suivantes pour le déploiement en production, en mettant l'accent sur :

- ◆ L'implémentation et la configuration du plugin Vault dans Rundeck
  - ◆ L'utilisation du SCM pour la collaboration, la traçabilité et la sauvegarde des modifications.
  - ◆ La gestion continue des ACL pour limiter l'accès aux ressources sensibles et améliorer la traçabilité des actions.
- Discuter des bénéfices attendus, tels que la réduction des risques de fuite de données, l'amélioration de la collaboration, et une meilleure conformité avec les politiques de sécurité.

#### Déploiement en Environnement d'Intégration :

- Déployer le plugin Vault et les modifications des ACL dans un environnement d'intégration pour des tests supplémentaires.
- Surveiller la stabilité et la performance du système pour identifier les problèmes potentiels.

#### Déploiement en Production :

- Déployer le plugin Vault, les modifications des ACL, et intégrer le SCM pour la gestion des configurations et des scripts dans un environnement d'intégration pour des tests supplémentaires.
- Surveiller la stabilité et la performance du système, y compris l'interaction entre Vault, les ACL et le SCM, pour identifier les problèmes potentiels.
- Effectuer des tests supplémentaires pour vérifier que toutes les fonctionnalités fonctionnent comme prévu et que la collaboration via le SCM se déroule sans problème.

## Défis Rencontrés et Solutions

Pendant mon projet, j'ai rencontré plusieurs défis qui ont nécessité des solutions créatives et une collaboration étroite avec mon équipe :

### Gestion des Listes de Permissions Complexes

- Problème : J'ai trouvé que les listes de permissions existantes (qui déterminent qui peut faire quoi) étaient complexes et difficiles à comprendre. Cela rendait leur réorganisation compliquée.
- Solution : J'ai documenté chaque liste de permissions et créé un diagramme pour visualiser qui avait accès à quoi. Cela m'a aidé à identifier les permissions inutiles ou redondantes, et à créer des listes de permissions plus simples et plus sécurisées.

### Configuration des Accès pour un Coffre-fort Numérique (Plugin Vault)

- Problème : Une de mes tâches complexes consistait à configurer notre outil d'automatisation (Rundeck) pour qu'il puisse utiliser notre coffre-fort numérique (Vault) de manière sécurisée. Même s'il n'y avait qu'un seul coffre-fort, chaque équipe devait avoir sa propre méthode d'accès sécurisée (AppRole) pour

maximiser la sécurité. De plus, les instructions disponibles pour cette version étaient limitées, ce qui a rendu la configuration initiale difficile.

- Solution : J'ai passé beaucoup de temps à tester différentes configurations pour réussir à connecter correctement notre coffre-fort à notre outil. Finalement, j'ai réussi à configurer plusieurs méthodes d'accès (AppRoles) pour le stockage sécurisé des clés dans notre outil, permettant à chaque équipe d'avoir sa propre méthode d'accès. Cela a amélioré la sécurité et permis une gestion plus détaillée des accès.

## Résistance au Changement

- Problème : Certains membres de l'équipe étaient réticents à adopter de nouveaux outils et méthodes, préférant les anciennes façons de faire.
- Solution : J'ai organisé des sessions de formation et des démonstrations pour montrer les avantages des nouveaux outils et des listes de permissions mises à jour. J'ai également recueilli les retours de l'équipe et apporté des ajustements pour répondre à leurs préoccupations.

## Instructions Limitées

- Problème : La version gratuite de notre outil d'automatisation et du plugin de coffre-fort numérique n'était pas bien documentée, ce qui a compliqué leur mise en place et leur intégration. J'ai dû faire beaucoup d'essais et d'erreurs pour comprendre comment tout configurer correctement.
- Solution : J'ai documenté chaque étape de mon processus de configuration et créé un guide interne pour faciliter les futures intégrations et configurations. Cela a par ailleurs servi de ressource pour d'autres équipes qui pourraient rencontrer des défis similaires.

## Intégration avec les Systèmes Existants

- Problème : Intégrer le nouveau système de gestion sécurisée des informations avec les systèmes existants (développement, intégration et production) sans perturber les opérations en cours était un défi majeur. Je devais m'assurer que les changements n'affectaient pas les processus critiques.
- Solution : J'ai planifié l'intégration en plusieurs étapes, en commençant par des tests dans un environnement isolé, puis en déployant progressivement dans des environnements de plus en plus proches de la production. Cela m'a permis de détecter et de corriger les problèmes potentiels sans impact sur les opérations en cours.

## Résultats et Impact

Grâce à nos efforts, nous avons réussi à implémenter le plugin Vault pour Rundeck et à restructurer les ACL, ce qui a eu plusieurs impacts positifs sur l'entreprise :

### Amélioration de la Sécurité

- La centralisation des secrets dans Vault a réduit le risque de fuites de données et amélioré la gestion des accès.

- Les nouvelles ACL ont limité l'accès aux ressources sensibles aux seules équipes qui en avaient besoin, minimisant ainsi les risques de sécurité.
- L'intégration du SCM a permis une meilleure traçabilité des modifications des configurations et des scripts, facilitant ainsi la collaboration entre les équipes et assurant une sauvegarde et une restauration rapides des configurations en cas de besoin.

## Efficacité Opérationnelle

- L'automatisation des tâches opérationnelles avec Rundeck et Vault a réduit le temps et les efforts nécessaires pour gérer les secrets et les configurations.
- Les processus de test et de déploiement automatisés ont permis de livrer les modifications plus rapidement et avec moins d'erreurs.
- L'intégration du SCM a permis une restauration rapide des configurations en cas de besoin, réduisant ainsi les temps d'arrêt et améliorant l'efficacité globale des opérations.

## Collaboration Améliorée

- L'intégration avec le SCM a facilité la collaboration au sein de l'équipe en permettant un suivi clair des modifications et une meilleure coordination.

## Feedback Positif de l'Équipe

- Les membres de l'équipe ont exprimé leur satisfaction avec les nouvelles fonctionnalités et processus, notant une amélioration de leur efficacité et de leur capacité à gérer les tâches opérationnelles.
- Le feedback positif a confirmé que nos contributions avaient un impact significatif sur le fonctionnement de l'équipe.

## Leçons Apprises

Ce projet m'a permis d'acquérir de nombreuses compétences et connaissances, ainsi que de tirer plusieurs leçons importantes pour mon développement professionnel :

### Importance de la Sécurité

- J'ai appris que la sécurité est une priorité absolue dans le secteur bancaire, et que chaque décision doit être prise en tenant compte des risques.
- La gestion des secrets et des accès est une partie cruciale de la sécurité informatique et des outils comme Vault peuvent grandement améliorer la protection des données sensibles.
- L'intégration du SCM a permis de sauvegarder et de tracer les configurations et les scripts, assurant une récupération rapide en cas de problème et maintenant un historique complet pour la conformité. Cela a montré que le SCM est un élément clé de la stratégie de sécurité.

### Collaboration et Communication

- Travailler au sein d'une équipe diversifiée m'a appris l'importance de la collaboration et de la communication efficace.

- Présenter mes résultats et expliquer les avantages des nouvelles technologies a amélioré mes compétences en communication et en présentation.

## Résolution de Problèmes

- J'ai développé mes compétences en résolution de problèmes en identifiant et en résolvant les défis rencontrés pendant le projet.
- La capacité à analyser les problèmes, à proposer des solutions créatives, et à travailler en équipe pour les mettre en œuvre est essentielle pour réussir dans un environnement professionnel.

## Adaptabilité

- J'ai appris à m'adapter aux changements et aux nouvelles technologies, ce qui est crucial dans un domaine en constante évolution comme l'informatique.
- Être ouvert aux retours d'information et prêt à ajuster mes approches en fonction des besoins de l'équipe et de l'entreprise est une compétence précieuse.

## Conclusion

Mon stage à la Société Générale Luxembourg a été une expérience enrichissante qui m'a permis de développer mes compétences techniques et professionnelles. Travailler sur le projet d'implémentation du plugin Vault pour Rundeck, de restructuration des ACL, et d'intégration du SCM pour la gestion des configurations et des scripts m'a offert une opportunité unique d'appliquer mes connaissances en sécurité informatique, en automatisation des opérations, et en gestion de versions.

Je suis reconnaissant pour l'opportunité de travailler avec une équipe talentueuse et dédiée, et pour les précieux retours d'information que j'ai reçus tout au long de mon stage. Cette expérience a renforcé mon intérêt pour la sécurité informatique et l'automatisation des opérations, et je suis impatient de continuer à développer mes compétences dans ces domaines.

Je suis convaincu que les compétences et l'expérience que j'ai acquises pendant mon stage seront précieuses pour ma future carrière, et je suis enthousiaste à l'idée de contribuer à de nouveaux projets et initiatives au sein de la Société Générale Luxembourg ou dans d'autres organisations.



## Section 2 : Lettre au Manager

### Introduction

Mon stage à la Société Générale Luxembourg a été une expérience profondément enrichissante et formatrice, qui a significativement contribué à mon développement technique et professionnel. Travailler sur le projet d'implémentation du plugin Vault pour Rundeck et de restructuration des listes de permissions m'a offert une opportunité unique d'appliquer et d'améliorer mes compétences en sécurité informatique et en automatisation des opérations.

### Qualités et Atouts

Durant mon stage, j'ai développé plusieurs qualités et compétences qui ont été essentielles pour le succès de mes projets. Mon sens de l'organisation et ma rigueur m'ont permis de mener à bien des tâches complexes, comme la documentation détaillée des processus pour l'implémentation du plugin Vault. De plus, ma capacité à travailler en équipe et à communiquer efficacement a été cruciale pour collaborer avec mes collègues et présenter mes résultats de manière claire.

Ma capacité à travailler de manière autonome et à prendre des initiatives a été mise en évidence lorsque j'ai documenté chaque étape de mon processus de configuration et créé un guide interne pour faciliter les futures intégrations et configurations. J'ai également démontré une forte persévérance face aux défis, en particulier lors de la résolution de problèmes complexes liés à la configuration et à la sécurisation de Rundeck. Ma curiosité technique et mon désir d'apprendre continuellement de nouvelles technologies, comme Kubernetes et Ansible, montrent mon engagement à rester à la pointe dans le domaine de l'infrastructure informatique.

### Résultats Concrets

Mon travail pendant le stage a eu un impact significatif sur l'équipe et les opérations. Grâce à mes recherches, tests et documentation sur l'implémentation du plugin Vault pour Rundeck, nous avons économisé plusieurs semaines de travail pour l'équipe. Cela a non seulement amélioré notre productivité, mais a aussi renforcé la sécurité de nos opérations, ce qui est primordial dans le secteur bancaire.

Un autre résultat notable est le développement d'une application web lors de mon premier stage, qui a permis de visualiser les équipements physiques dans nos datacentres. Cette application a fait gagner un temps précieux aux équipes en facilitant la recherche d'informations sur les équipements.

Grâce à mes efforts, la sécurité de notre outil d'automatisation a été significativement améliorée. Les tests rigoureux et la révision des listes de permissions ont permis de minimiser les risques de sécurité. De plus, le feedback positif de mon équipe indique que mes contributions ont aidé à optimiser leurs processus de travail. J'ai aussi créé une documentation détaillée qui servira de ressource précieuse pour les futures

intégrations et configurations. Cela aidera non seulement mon équipe actuelle, mais aussi d'autres équipes qui pourraient rencontrer des défis similaires.

## Découverte d'un Intérêt pour l'Infrastructure Informatique

Ces stages m'ont permis de découvrir et de développer un véritable intérêt pour l'infrastructure informatique. Travailler sur des projets qui touchent à la gestion des serveurs, à la sécurisation des données et à l'automatisation des tâches m'a montré l'importance et l'impact de ces systèmes sur l'efficacité et la sécurité des entreprises. Je suis particulièrement fasciné par la manière dont l'infrastructure peut être optimisée pour soutenir les objectifs stratégiques d'une organisation. Mon enthousiasme pour ce domaine me motive à continuer à apprendre et à me perfectionner, et je suis impatient de contribuer à des projets qui améliorent et sécurisent les infrastructures informatiques.

## Proposition pour un Nouveau Projet

Je suis convaincu que mes compétences et mon expérience peuvent apporter une valeur ajoutée significative à d'autres projets au sein de la Société Générale Luxembourg. Je suis particulièrement intéressé à contribuer à des initiatives visant à améliorer la sécurité et l'automatisation des processus opérationnels. Mon expérience avec Rundeck et Vault, combinée à ma capacité à travailler en équipe et à communiquer efficacement, fait de moi un candidat idéal pour de tels projets. Je suis enthousiaste à l'idée de continuer à contribuer à l'entreprise et je suis ouvert à discuter de toute opportunité qui pourrait bénéficier de mes compétences. En dehors du travail, j'envisage de me procurer un mini-ordinateur, spécifiquement le MS-02 de Miniforum, pour créer un serveur à domicile, un "homelab", qui me permettra de continuer à apprendre et à expérimenter avec différentes technologies d'infrastructure. Cette initiative personnelle pourrait également profiter à notre entreprise en apportant de nouvelles idées et solutions innovantes. Je suis impatient de continuer à collaborer avec vous et de contribuer à la réussite continue de notre équipe.