INTERNSHIP REPORT

Téo Franoux

Epitech, Third Year

Societe Generale Luxembourg
Epitech Nancy

–

April to July 2025

Implementation and Securing of Rundeck with Vault Plugin

Internship Supervisor : Bertrand Docquois

Table of Contents

Section 1: New Employee Report

Introduction

During my four-month internship at Société Générale Luxembourg, I worked on Rundeck, a transaction automation tool. My main mission was to test and implement the community version of the Vault plugin for Rundeck, as well as work on its SCM.

Company Description

Société Générale Luxembourg is a subsidiary of the Société Générale Group, one of Europe's leading financial institutions. It offers a wide range of banking and financial services, including wealth management, private banking, and corporate financing solutions. Security and effective access management are crucial in this sector to protect sensitive client data.

The company operates in several countries and employs thousands of professionals who work together to deliver high-quality services. It is recognized for its innovation and commitment to its customers, making it a key player in the European banking sector.

The Department I Worked In: GTS (Global Technology Services)

GTS, or Global Technology Services, is a key department within Société Générale that focuses on managing and maintaining the company's technology infrastructure. But what does this mean exactly?

Imagine that Société Générale is a large city. Within this city, there are buildings, roads, utilities, and communications systems. All of this must function smoothly and in a coordinated manner so that its residents (in this case, the bank's employees and customers) can live and work efficiently.

GTS is like this city's Department of Public Works and Essential Services. It ensures everything runs smoothly, from buildings (servers and data centers) to roads (networks and internet connectivity) to utilities (applications and workstations).

What is IT Infrastructure?

IT infrastructure is the set of elements needed for a company's technology systems to function. This includes:

- ➔ Workstations :These are the computers, laptops and tablets that employees use daily.
- ➔ Servers and Virtual Machines:Servers are powerful computers that store and manage data and applications. Virtual machines are like multiple virtual computers running on a single physical server, allowing for better resource utilization.

- ➔ Collaborative Applications and Services:These are the software and tools that employees use to collaborate and get their work done, such as email and messaging systems.
- ➔ Networks and Telephony:This includes everything that connects different equipment together, as well as telephone systems that allow employees to communicate effectively.

Simply put, IT infrastructure is the technological backbone that enables a company like Société Générale to operate smoothly and efficiently.

Some Figures on GTS

To give you an idea of the scale of GTS's operations, here are some key figures

- Global Staff:GTS has nearly 4,000 employees and service providers worldwide.
- Workstations:GTS manages over 103,000 workstations, which include laptops, desktops and tablets.
- Emails :Every day, more than 50 million emails are managed by GTS systems.
- Servers and Virtual Machines:GTS maintains 15,000 physical servers and 100,000 virtual machines to ensure the smooth running of applications and services.

To give an idea of the geographical distribution of GTS staff:

- ➔ In Paris, the main center has 2,070 employees.
- ➔ In Luxembourg, the team is smaller, but just as essential, with approximately 30 employees.

These figures demonstrate the scale and importance of GTS's role in maintaining Société Générale's technology operations. Working in this department has allowed me to see firsthand how a well-managed IT infrastructure can support a large organization and its clients around the world.

Team Description

Our IT infrastructure team consisted of four members, each with specific responsibilities:

- Bertrand - Project Manager (My Manager):

  Bertrand ensures our work is running smoothly and that we achieve our goals. He tells us what we need to do and takes care of discovering his own manager's needs. For example, if the company decides to move part of its infrastructure to Paris, Bertrand will discuss it with us and assign tasks based on each person's skills.

- Boris - Expert Kubernetes :

  Boris manages groups of servers that work together to run applications. He uses a tool called Ansible, which helps him configure and manage these servers

efficiently. His job is to ensure that the services are always accessible, running smoothly, and easy for other teams to use.

- Marie-France - Automic Automation Expert:

  Marie-France works with a tool called Automic Automation, which is used to automate and manage various IT processes within the company. Her role is to ensure these processes run smoothly and without interruption. She monitors the system to quickly identify and resolve any issues, ensuring that Automic Automation always functions properly and that all services that depend on it remain available and efficient.

- Myself - Infrastructure Intern:

  My role was to test and implement the Vault plugin for Rundeck, review and restructure ACLs to improve security, and work on Rundeck's SCM to ensure stability of the changes.

Detailed Explanations of the Tools

Rundeck

Rundeck is like an assistant that takes care of repetitive tasks for you. Imagine you have a list of daily tasks to do at home, like watering the plants or washing the dishes. Rundeck does these tasks for you, but in the IT world, like backing up files or restarting a computer.

Vault

Vault is a digital safe. You store your valuables in it, but instead of jewelry or important documents, it keeps secret information, like passwords, safe. Only someone you trust can access it when needed.

SCM (Source Control Management)

In the context of Rundeck, SCM acts as a logbook that records every change made to the scripts and configurations used to automate tasks. Imagine having a recipe book to manage your daily tasks, where you record every change you make. If you modify a recipe (or a script in Rundeck) and it doesn't work as expected, you can simply revert to the previous version that worked well.

This ensures that you can always go back if something goes wrong. Additionally, this log facilitates team collaboration, as everyone can see who did what and when, and work together more efficiently.

The Vault Plugin for Rundeck

The Vault plugin for Rundeck allows Rundeck to use Vault to manage sensitive information needed to run automated tasks. This means that when Rundeck needs to run a task that requires sensitive information, such as a password or secret key, it can temporarily retrieve it from Vault.

The process works as follows: When Rundeck begins a task that requires sensitive information, it requests that information from Vault. Vault then securely provides that information to Rundeck. Once the task is complete, the information is secured back into Vault, ensuring it is never exposed insecurely.

Thus, the Vault plugin allows Rundeck to perform tasks that require sensitive information without that information ever being stored or exposed insecurely. The plugin therefore acts as a secure intermediary between Rundeck and the sensitive information stored in Vault.

Different environments

- Development (dev): Used by developers to write and test code. Usually locally or on a dedicated server.
- Integration (int): Used to test interactions between different modules or systems. Ensures that the code works correctly with other components.
- Production (prod): Environment where the final code is deployed and used by end users. Configured to be stable and reliable.

Project Description

My project involved testing and implementing a plugin called Vault for Rundeck. Vault is a tool for securely storing and managing sensitive information, such as passwords or sensitive data.

The community version of Rundeck means it's free and open-source, but it requires more manual configuration than the paid version. This means I had to do more work to get everything set up correctly.

One of the key aspects of my work was reviewing and restructuring the ACLs (Access Control Lists) in Rundeck. ACLs are like checklists that determine who is allowed to do what. In Rundeck, ACLs determine which teams can access which features. By reviewing and restructuring these lists, we were able to improve the overall security of the system.

I also worked on Rundeck's SCM to improve collaboration, track changes, enable error rollback, and ensure automation while maintaining security.

Context and Objectives of the Project

Data security is a top priority for Société Générale Luxembourg. Amid a significant increase in cyberattacks and data breaches, protecting sensitive client and corporate information has become more crucial than ever. Rundeck, an essential tool used to automate and orchestrate various operational tasks, plays a key role in ensuring efficient and reliable operations.

However, to meet the high security standards required by the banking industry, it was imperative to strengthen the security associated with its use. Despite its usefulness and effectiveness, like any powerful system, Rundeck requires rigorous security precautions to minimize any risk and ensure optimal data protection.

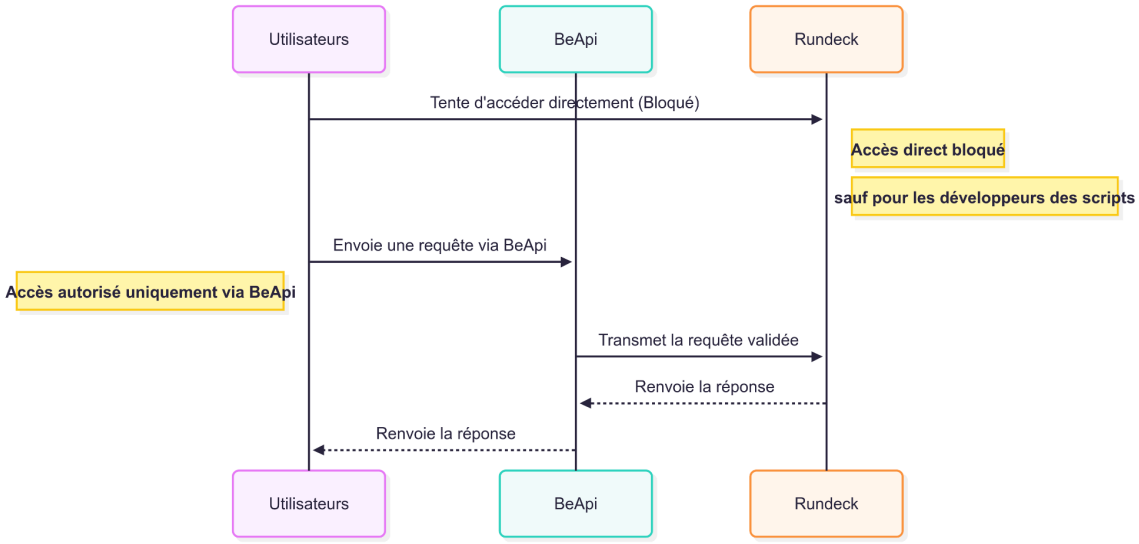
Description of BeApi

BeApi is a tool developed internally by Société Générale to enable different teams to launch various tasks via Rundeck. To understand what an API is, imagine it like a server in a restaurant: you place your order (you make a request) and the server brings you your dish (the response to your request). In the same way, BeApi acts as a secure and controlled intermediary that allows different software programs to communicate and access Rundeck's features.

To make it easier to use, BeApi uses a Swagger interface, which can be compared to a restaurant menu. This menu lists all available features (dishes) and explains how to use them (how to order). This allows various teams to easily understand and use the features offered by BeApi without the need for in-depth technical knowledge.

Identified Problems

- ➔ BeApi Bypass:
  - ◆ Some teams were using Rundeck directly in their development environment, thus bypassing the security controls implemented by BeApi.



- ➔ Security Risks:
  - ◆ By using Rundeck directly, teams bypassed security checks, which was like entering a private party without an invitation.

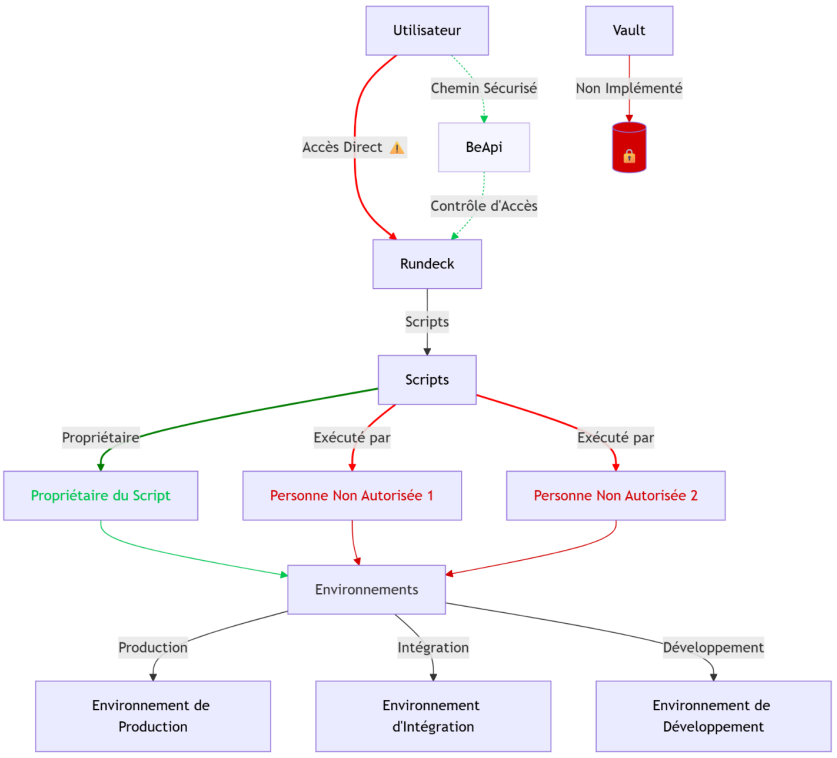
- ➔ Impact on Production:
  - ◆ Some scripts running in the development environment could affect production environments, posing a significant risk.

- ➔ Incomplete Processes:
  - ◆ When a procedure failed, manual corrections via Rundeck left unnecessary elements that cluttered and could cause problems.

- ➔ Using Unknown Scripts:
  - ◆ Some users were running scripts they didn't fully understand, which was dangerous because they could misuse them or skip crucial steps.

- ➔ Need to Secure Access:
  - ◆ It was essential to secure access to Rundeck and ensure that all script executions go through BeApi, where access controls are appropriate.

- ➔ Migrating Sensitive (Secret) Information to Vault:
  - ◆ It was important to migrate secrets management to Vault for enhanced security, as Rundeck's default storage was not secure enough.



Incidents et Motivations

There have been incidents where critical scripts, supposed to be executed only via BeApi with appropriate access controls, were launched directly from Rundeck during development. This posed not only an operational risk in terms of the stability and performance of production systems, but also a risk of non-compliance with Société Générale's internal security policies.

Imagine a scenario where a critical command, such as changing a user password or deleting a server, is executed without proper checks. This could cause major problems and financial losses.

These incidents highlighted the need to secure access to Rundeck and ensure that all script executions go through BeApi, where appropriate access controls are in place. Additionally, it was crucial to migrate secrets management away from Rundeck's default storage, which was not sufficiently secure. This storage potentially allowed all teams to access everyone's secrets. By migrating to Vault, a more robust and secure solution, we were able to implement stricter access controls and limit access to secrets to authorized teams only.

Project Objectives

The main objective of the project was to test and implement the Vault plugin for Rundeck, which allows for the secure storage and management of secrets. By using Vault, we can centralize the storage of secrets, reduce the risk of data leaks, and

improve access management. Additionally, using a version control system (VCS) for Rundeck configurations and scripts allows for change tracking, facilitates collaboration between teams, and ensures better version control.

Solution Implementation

To address these issues, several measures have been taken:

Securing access to Rundeck

I restructured the Access Control Lists (ACLs) in Rundeck to define granular permissions for each user and each project. ACLs function like a guest list for a private party: only the names on the list can enter. This approach ensured that only authorized users could run scripts, and only in environments for which they had the appropriate rights. Additionally, this restructuring helped mitigate the risk of unauthorized manipulation and improve the traceability of actions performed.

Vault Integration

I implemented and configured the Vault plugin for Rundeck, which allowed me to remove secrets from Rundeck's less secure internal storage. By centralizing these secrets in Vault, I benefited from more fine-grained access control and improved auditing capabilities. Vault offers advanced secrets management features, such as encryption, automatic key (password) rotation, and detailed access logging. These improvements significantly reduced the risk of sensitive data leakage and strengthened compliance with internal security policies.

Improved collaboration and backup

To improve collaboration and ensure change traceability, I integrated a version control system (VCS) for Rundeck configurations and scripts. This not only allowed me to save changes, but also facilitated teamwork by enabling accurate change tracking and efficient version management. This approach also allowed me to quickly restore previous configurations when needed, while ensuring better coordination between different team members.

Development and Testing Process

The development and testing process for this project was divided into several stages:

Needs Analysis:

- ➔ Understand enterprise security requirements and the features offered by the Vault plugin.
- ➔ Identify gaps in current secrets management and potential improvements.

Initial Configuration:

- ➔ Install the Vault plugin in Rundeck.

- ➔ Configure the Vault plugin in Rundeck's configuration files.

Initial Tests:

- ➔ Test the Vault plugin in an isolated environment to ensure it works as expected.
- ➔ Identify and resolve configuration and compatibility issues.

ACL Review:

- ➔ Analyze existing ACLs and identify unnecessary or excessive permissions.
- ➔ Review and restructure ACLs to minimize security risks and improve access management.

Integration with SCM:

- ➔ Integrate Rundeck with version control system to track changes to configurations.
- ➔ Automate testing and deployments to ensure stability of changes.

Presentation to the Team:

- ➔ Present test results, the benefits of the Vault plugin, and SCM integration for configuration and script management.
- ➔ Explain the implementation process, including restructuring ACLs to improve security and access management.
- ➔ Describe the next steps for deployment to production, with emphasis on:
  - ◆ Implementing and configuring the Vault plugin in Rundeck
  - ◆ Using SCM for collaboration, traceability and backup of changes.
  - ◆ Continuous management of ACLs to limit access to sensitive resources and improve traceability of actions.
- ➔ Discuss expected benefits, such as reduced data leakage risks, improved collaboration, and better compliance with security policies.

Deployment in Integration Environment:

- ➔ Deploy the Vault plugin and ACL changes to an integration environment for further testing.
- ➔ Monitor system stability and performance to identify potential issues.

Production Deployment:

- ➔ Deploy the Vault plugin, ACL changes, and integrate the SCM for configuration management and scripts into an integration environment for further testing.
- ➔ Monitor system stability and performance, including the interaction between Vault, ACLs, and SCM, to identify potential issues.
- ➔ Conduct additional testing to verify that all features work as expected and that collaboration via the SCM runs smoothly.

Challenges Encountered and Solutions

During my project, I encountered several challenges that required creative solutions and close collaboration with my team:

Managing Complex Permission Lists

- Problem: I found the existing permission lists (which determine who can do what) to be complex and difficult to understand. This made reorganizing them difficult.
- Solution: I documented each permission list and created a diagram to visualize who had access to what. This helped me identify unnecessary or redundant permissions and create simpler, more secure permission lists.

Configuring Access for a Digital Safe (Vault Plugin)

- Problem: One of my complex tasks was configuring our automation tool (Rundeck) to securely use our digital vault (Vault). Even though there was only one vault, each team needed their own secure access method (AppRole) to maximize security. Additionally, the instructions available for this version were limited, making the initial setup difficult.
- Solution: I spent a lot of time testing different configurations to successfully connect our vault to our tool. Ultimately, I managed to configure multiple access methods (AppRoles) for secure key storage in our tool, allowing each team to have their own access method. This improved security and allowed for more detailed access management.

Resistance to Change

- Problem: Some team members were reluctant to adopt new tools and methods, preferring the old ways of doing things.
- Solution: I held training sessions and demonstrations to demonstrate the benefits of the new tools and updated permission lists. I also gathered feedback from the team and made adjustments to address their concerns.

Limited Instructions

- Problem: The free version of our automation tool and digital vault plugin wasn't well documented, making setup and integration difficult. It took a lot of trial and error to figure out how to set everything up correctly.
- Solution: I documented each step of my setup process and created an internal guide to facilitate future integrations and setups. This also served as a resource for other teams who might encounter similar challenges.

Integration with Existing Systems

- Problem: Integrating the new secure information management system with existing systems (development, integration, and production) without disrupting ongoing operations was a major challenge. I had to ensure that the changes did not affect critical processes.
- Solution: I planned the integration in stages, starting with testing in an isolated environment and then gradually deploying to environments closer and closer to production. This allowed me to detect and correct potential issues without impacting ongoing operations.

Results and Impact

Thanks to our efforts, we managed to implement the Vault plugin for Rundeck and restructure the ACLs, which had several positive impacts on the business:

Improved Security

- ➔ Centralizing secrets in Vault has reduced the risk of data leaks and improved access management.
- ➔ The new ACLs limited access to sensitive resources to only those teams that needed it, minimizing security risks.
- ➔ SCM integration enabled better traceability of configuration and script changes, facilitating collaboration between teams and ensuring rapid backup and restoration of configurations when needed.

Operational Efficiency

- ➔ Automating operational tasks with Rundeck and Vault has reduced the time and effort required to manage secrets and configurations.
- ➔ Automated testing and deployment processes enabled changes to be delivered faster and with fewer errors.
- ➔ SCM integration enabled rapid restoration of configurations when needed, reducing downtime and improving overall operational efficiency.

Improved Collaboration

- ➔ Integration with the SCM facilitated collaboration within the team by enabling clear tracking of changes and better coordination.

Positive Feedback from the Team

- ➔ Team members expressed satisfaction with the new features and processes, noting an improvement in their efficiency and ability to manage operational tasks.
- ➔ The positive feedback confirmed that our contributions had a significant impact on the functioning of the team.

Lessons Learned

This project allowed me to acquire many skills and knowledge, as well as to learn several important lessons for my professional development:

Importance of Safety

- I learned that security is a top priority in the banking industry, and every decision must be made with risk in mind.
- Managing secrets and access is a crucial part of IT security, and tools like Vault can greatly improve the protection of sensitive data.
- SCM integration enabled configurations and scripts to be backed up and tracked, ensuring rapid recovery in the event of a problem and maintaining a complete history for compliance. This demonstrated that SCM is a key component of the security strategy.

Collaboration et Communication

- Working in a diverse team has taught me the importance of collaboration and effective communication.
- Presenting my results and explaining the benefits of new technologies improved my communication and presentation skills.

Problem Solving

- I developed my problem-solving skills by identifying and resolving challenges encountered during the project.
- The ability to analyze problems, propose creative solutions, and work as a team to implement them is essential for success in a professional environment.

Adaptability

- I learned to adapt to changes and new technologies, which is crucial in a constantly evolving field like IT.
- Being open to feedback and willing to adjust my approaches based on the needs of the team and the business is a valuable skill.

Conclusion

My internship at Société Générale Luxembourg was a rewarding experience that allowed me to develop my technical and professional skills. Working on the project to implement the Vault plugin for Rundeck, restructure ACLs, and integrate SCM for configuration and script management provided me with a unique opportunity to apply my knowledge of IT security, operations automation, and version control.

I am grateful for the opportunity to work with a talented and dedicated team, and for the valuable feedback I received throughout my internship. This experience has strengthened my interest in IT security and operations automation, and I look forward to continuing to develop my skills in these areas.

I am confident that the skills and experience I gained during my internship will be valuable for my future career, and I am excited to contribute to new projects and initiatives within Société Générale Luxembourg or other organizations.

Section 2: Letter to the Manager

Introduction

My internship at Société Générale Luxembourg was a deeply enriching and formative experience, significantly contributing to my technical and professional development. Working on the project to implement the Vault plugin for Rundeck and restructure permission lists provided me with a unique opportunity to apply and enhance my skills in IT security and operations automation.

Qualities and Assets

During my internship, I developed several qualities and skills that were essential to the success of my projects. My organizational skills and rigor allowed me to successfully complete complex tasks, such as the detailed documentation of processes for the Vault plugin implementation. Furthermore, my ability to work in a team and communicate effectively was crucial for collaborating with my colleagues and presenting my results clearly.
My ability to work independently and take initiative was evident when I documented each step of my configuration process and created an internal guide to facilitate future integrations and configurations. I also demonstrated strong perseverance in the face of challenges, particularly when solving complex problems related to configuring and securing Rundeck. My technical curiosity and desire to continually learn new technologies, such as Kubernetes and Ansible, demonstrate my commitment to staying at the forefront of IT infrastructure.

Concrete Results

My work during the internship had a significant impact on the team and operations. Thanks to my research, testing, and documentation on the implementation of the Vault plugin for Rundeck, we saved the team several weeks of work. This not only improved our productivity but also strengthened the security of our operations, which is essential in the banking sector.
Another notable achievement was the development of a web application during my first internship, which allowed us to visualize the physical equipment in our data centers. This application saved our teams valuable time by making it easier to find information about equipment.
Thanks to my efforts, the security of our automation tool has been significantly improved. Rigorous testing and permission list revisions have minimized security risks. Additionally, positive feedback from my team indicates that my contributions have helped optimize their workflows. I've also created detailed documentation that will serve as a valuable resource for future integrations and configurations. This will help not only my current team, but also other teams who may be facing similar challenges.

Discovering an Interest in IT Infrastructure

These internships allowed me to discover and develop a genuine interest in IT infrastructure. Working on projects related to server management, data security, and task automation showed me the importance and impact of these systems on business efficiency and security.
I am particularly fascinated by how infrastructure can be optimized to support an organization's strategic objectives. My enthusiasm for this field motivates me to continue learning and developing, and I look forward to contributing to projects that improve and secure IT infrastructures.

Proposal for a New Project

I am convinced that my skills and experience can add significant value to other projects within Société Générale Luxembourg. I am particularly interested in contributing to initiatives aimed at improving the security and automation of operational processes.
My experience with Rundeck and Vault, combined with my ability to work in a team and communicate effectively, makes me an ideal candidate for such projects. I am enthusiastic about continuing to contribute to the company and am open to discussing any opportunities that could benefit from my skills.
Outside of work, I'm considering purchasing a minicomputer, specifically the Miniforum MS-02, to create a home server, a "homelab," which will allow me to continue learning and experimenting with different infrastructure technologies. This personal initiative could also benefit our company by bringing new ideas and innovative solutions.
I look forward to continuing to collaborate with you and contributing to the continued success of our team.