



RAPPORT DE SOUTENANCE

VINCENT MONNOT

**Alternance dans l'équipe Service Offering DevOps au
sein de BNP Paribas**

- Zakia DIFALLAH -

Alternant apprenti Ingénieur ESIEE Paris

**Filière Informatique et Application, spécialité Ingénierie 3D et technologie des
médias.**

- Benjamin PERRET -

Table des matières

<i>I. Remerciements</i>	3
<i>II. Introduction</i>	4
1. Annonce de l'alternance.....	4
2. Déroulement de l'alternance	4
3. Problématique et objectifs du rapport.....	5
4. Annonce de plan	5
<i>III. Contexte entreprise</i>	6
5. Présentation générale	6
6. Mon groupe : ITG	8
7. Mon entité : ITG DevOps – ODM09.....	8
8. Mon produit : ITNorms	9
9. La méthode Agile.....	11
<i>IV. Mes missions sur ITNorms</i>	12
10. Refonte du portail ITNorms	12
11. Refonte des APIs ITNorms.....	14
<i>V. Problématique Ansible Tower et utilisation de l'authentification SAML</i>	17
12. Présentation de Ansible et Ansible Tower.....	17
13. Modes d'authentification offerts par Ansible Tower :	17
14. Exclusion mutuelle des méthodes d'authentification	18
15. La problématique de l'API Ansible Tower.....	19
16. Les problèmes s'enchaînent.....	19
17. La solution que nous avons envisagée	20
18. Briques utilisées	20
19. Le détail des 3 étapes de génération de token	21
<i>VI. Bilan et recul sur la mission</i>	24
20. L'organisation de l'entreprise	24
21. Mon apport à l'entreprise.....	24
22. Les apports personnels de l'alternance	25
23. Conclusion	25

I. Remerciements

Avant tout développement sur cette expérience professionnelle, il apparaît opportun de commencer ce rapport de stage par des remerciements, à ceux qui m'ont beaucoup appris au cours de ce stage, et même à ceux qui ont eu la gentillesse de faire de cette alternance un moment très profitable.

Aussi, je remercie Zakia DIFALLAH, ma tutrice qui m'a accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie. Je remercie tous les membres des équipes DIM et ITNorms pour les conseils qu'ils ont pu me donner au cours de cette année.

Je remercie tout particulièrement Patrice Riou pour avoir pris le temps de m'expliquer clairement les enjeux d'Ansible Tower ainsi que pour m'avoir aider à la rédaction de ce rapport.

Je remercie également Benjamin PERRET mon tuteur école qui est resté disponible durant mon année et qui a été mon contact durant mes différentes périodes.

II. Introduction

1. Annonce de l'alternance

J'effectue depuis le 01/09/2020 une alternance au sein de l'entreprise BNP Paribas, située au 93 Rue Marceau, Montreuil. Au cours de cette alternance dans le groupuscule ODM09 et plus précisément au sein de l'équipe ITNorms, j'ai eu l'occasion d'approfondir mes compétences de développement Java.

Plus largement, ce stage a été l'opportunité pour moi d'appréhender la réalisation d'un projet en mode Agile SCRUM.

2. Déroulement de l'alternance

Au cours de mon alternance, ma mission principale a été de participer au développement d'une application trois tiers et notamment à l'évolutions d'APIs Java pour l'application ITNorms. L'objectif de cette dernière est de contrôler les normes établies par ITRules, une entité en charge de fournir une bibliothèque de règles de normes pour les différents middlewares présents sur un serveur.

J'ai également l'opportunité d'approfondir mes connaissances sur les notions de CI/CD (Continuous Integration / Continuous Developpement). Ainsi j'apprends à fournir une chaîne de déploiement automatique grâce à des outils tels que Jenkins, Ansible, Kubernetes et bien d'autres.

Enfin j'ai eu l'opportunité de mettre à disposition mes ressources à l'étude d'une solution alternative de connexion pour Ansible Tower de la suite RedHat.

Redhat, à travers Ansible Tower ne propose pas de solution permettant de générer un token d'accès applicatif de manière automatisé dans une chaîne de déploiement. Afin de générer des tokens d'authentification à partir d'organisations tout en identifiant l'utilisateur nous avons dû faire une étude et réaliser un POC (Proof of Concept) afin de dresser une architecture permettant de répondre à nos besoins. De plus, étant donné que ce procédé permet, entre autres, de générer des accès automatiquement (c'est un outil d'automatisation qui s'identifie à la place de l'utilisateur), il faut aussi s'assurer que personne ne puisse voler l'identité d'autrui. Notre architecture a donc été présenté à un jury en charge de valider la sécurité de notre procédé. Une fois validé nous avons donc commencer à la mettre en place.

3. Problématique et objectifs du rapport

Cette alternance a donc été une opportunité pour moi de mettre en pratique les connaissances et compétences acquises au cours de ma formation. En particulier, il m'a permis d'avoir une première approche de la méthodologie Agile SCRUM.

L'élaboration de ce rapport a pour principale source les différents enseignements tirés de la pratique journalière des tâches auxquelles j'ai été affectées. Enfin, les nombreux entretiens que j'ai pu avoir avec les employés des différents services de la société m'ont permis de donner une cohérence à ce rapport.

4. Annonce de plan

En vue de rendre compte de manière fidèle et analytique de l'année passée au sein de la société BNP Paribas, il apparaît logique de présenter à titre préalable l'entreprise, à savoir une introduction de celle-ci et son fonctionnement, puis d'envisager le service dans lequel j'ai été placée.

Enfin, il sera précisé les différentes missions et tâches que j'ai pu effectuer au sein de l'équipe ITNorms, et les nombreux apports que j'ai pu en tirer.

III. Contexte entreprise

5. Présentation générale

Le groupe BNP Paribas est un leader financier puissant et performant avec un solide ancrage en Europe et actif en Asie et aux Etats-Unis. La BNP a été créée en 1966 de l'union de deux banques françaises, la BNCI (Banque Nationale pour le Commerce et l'Industrie) et le CNEP (Comptoir National d'Escompte de Paris). En 1993, sa privatisation en 1993 a marqué un nouveau temps fort. Enfin, la fusion de BNP et Paribas en 2000 a donné naissance à un acteur incontournable du paysage bancaire mondial. Ce rapprochement a permis de dynamiser le développement des créneaux stratégiques en pleine expansion comme la banque privée et la gestion d'actifs.

Le groupe comporte aujourd'hui 193 000 collaborateurs et est implanté dans 68 pays avec un chiffre d'affaires de 44,3Md €.

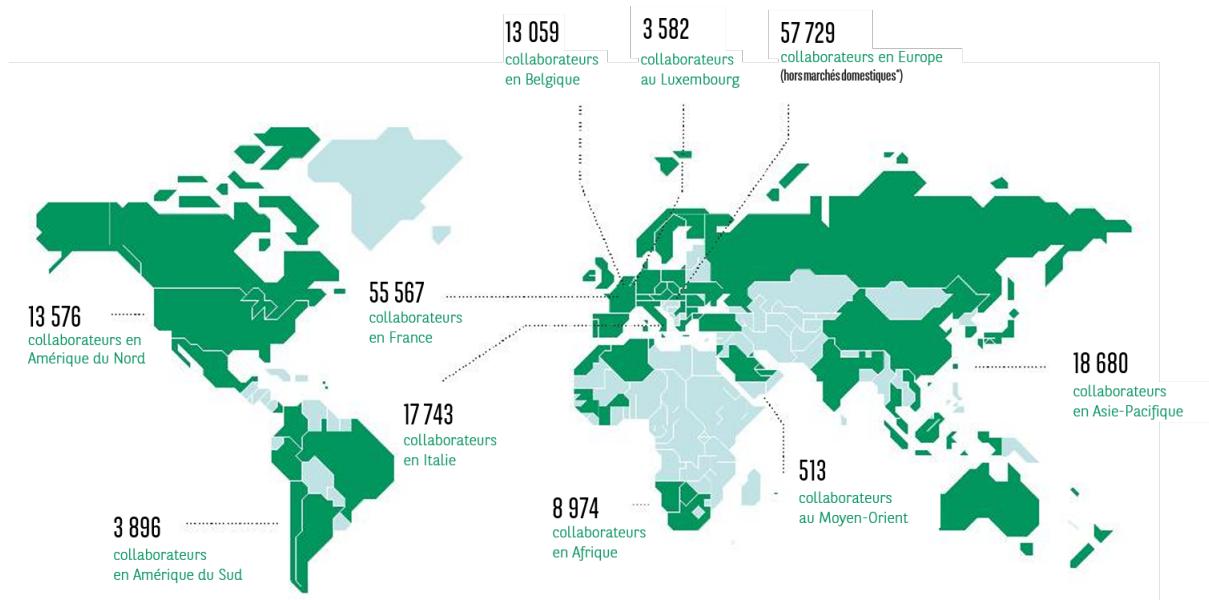


Figure 1: Implantations mondiales de BNP Paribas

BNP Paribas occupe des positions clés dans ses trois pôles opérationnels :

- **Retail Banking** fédère les réseaux des banques de détail du Groupe et plusieurs métiers spécialisés.
- **Investment & Protection Services** regroupe des métiers spécialisés offrant un large éventail de solutions d'épargne, d'investissement et de protection
- **Corporate & Institutional Banking** propose des solutions financières sur mesure pour les clientèles entreprises et institutionnels

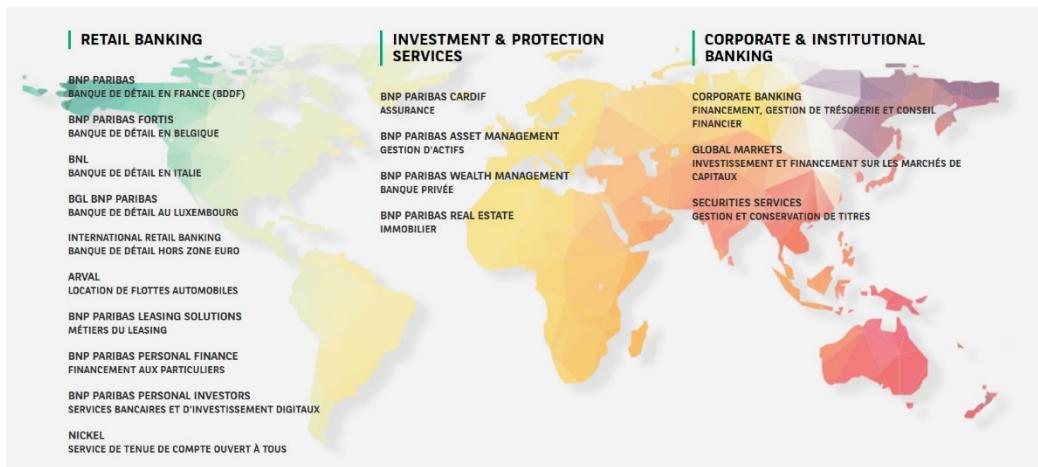


Figure 2 : Les 3 pôles opérationnels



6. Mon groupe : ITG

IT GROUP est l'informatique du Groupe BNP Paribas.

La direction d'IT GROUP définit et déploie la stratégie informatique du Groupe BNP Paribas à l'échelle mondiale, assure la cohérence globale du Système d'Information du Groupe et œuvre à la mutualisation de ses choix technologiques et méthodologiques.

Elle coordonne les directions informatiques des Fonctions et des Métiers de la Banque, les aide à mettre en œuvre la stratégie IT définie pour le Groupe et à adopter les outils et technologies innovants, sécurisés et à valeur ajoutée pour ses clients (cloud, intelligence artificielle & robotique, management de la data, blockchain, etc.).



Figure 3 : L'implémentation de ITG au sein de la BNP

7. Mon entité : ITG DevOps – ODM09



Le domaine "DevOps Platform" d'IT Group Production a la charge de la définition et la mise en place d'un socle commun pour le Groupe, des pratiques et des outils DevOps.

Il contribue au déploiement DevOps en mettant la plateforme DevOps ITG à disposition des équipes IT pour le "Continuous Delivery" de leurs applications.



8. Mon produit : ITNorms

L'application **IT Norms** est un package SHA, actuellement dédié à Linux Redhat, qui permet de connaître l'état de compliance de votre parc vis-à-vis des règles [ITRules](#) (une autre entité qui regroupe l'ensemble des règles textuels de normes au sein de la BNP).

★ Pourquoi ?

- Parce que le développeur veut déployer son application sur les environnements de non-production **en respectant les règles de production** sans avoir à accéder à aucune documentation,
- Parce que l'OPS (l'Opérateur Serveur) veut savoir **rapidement et facilement** si ses serveurs applicatifs sont sécurisés vis-à-vis des règles IT Rules, ODM fournit l'outil "ITNorms", une application qui vérifie pour la compliance des serveurs Linux vis-à-vis des règles de production BNPP, automatiquement, via des appels API, pendant toutes les étapes du cycle de vie de l'application.

★ Comment ?

Grâce aux fonctionnalités suivantes :

- **Possibilité de pluguer des orchestrateurs à ITNorms pour automatiser** le contrôle qualité des environnements techniques dès la livraison des serveurs
- **Contrôle** de la compliance des environnements applicatifs vis-à-vis des règles de production
- **Homogénéisation** du parc applicatif
- **Facilitation** du traitement de l'obsolescence des assets applicatifs

★ Grâce à quoi ?

IT Norms met à disposition différents outils :

- Le script Python lance le scan sur vos serveurs.
- Les rôles Ansible sont disponibles pour industrialiser le scan sur des ensembles de serveurs (avec restriction au périmètre UPM).
- Le portail web vous permet de créer des demandes et d'afficher le résultat des scans.
- Les APIs REST peuvent être appelées par des partners externes (exemple : CI/CD , Toolchain, etc..).

IT Norms est une solution **intégrée** dans le CLOUD privé ITG.

★ Pourquoi respecter les règles d'ingénierie de production ?

1. Le respect des règles d'ingénierie ITGP (IT Groupe Production) permet bien entendu de **profiter des processus standardisés et idéalement automatisés de production**, actuels ou à venir.
2. Ces règles d'ingénierie intègrent l'expertise des équipes de production et sont notre **outil commun de capitalisation**. Une règle d'ingénierie évolue en fonction des retours de chacun des acteurs, prod ou IT métiers
3. Une règle d'ingénierie peut être **contrôlée à la demande**, ceci sur la base des règles unitaires définies.

9. La méthode Agile

Présentation de la méthodologie :

L'agilité est une méthodologie de gestion de projet. Elle permet de travailler en collaboration avec le client afin d'éviter un effet tunnel souvent remarqué en cycle en V. Elle offre une expression des besoins adaptables au cours du projet et une meilleure visibilité sur l'avancement de celui-ci grâce à des présentations régulières.

Planification

Chaque sprint commence par cette réunion. Comme son nom l'indique, l'équipe technique se réunit avec le Product Owner (Le responsable du produit) et le Scrum Master (Le responsable de la méthodologie) pour planifier le sprint à venir. Le PO (Product Owner) décide des User Stories à réaliser. Puis, l'équipe quantifie la difficulté de celle-ci à l'aide d'un planning poker.

Daily meeting

Chaque matin, l'équipe se réunit. Chaque collaborateur cite les tâches qu'il a réalisées la veille, explique s'il a rencontré des difficultés et les tâches qu'il prévoit d'effectuer. Afin de consulter ces informations au cours d'un sprint, l'équipe utilise JIRA, un outil informatique, en tant que KANBAN.

Répétition

Deux jours avant la démonstration terminant le sprint, chaque membre de l'équipe technique présente les US terminées dans le sprint à l'équipe. Cette répétition permet de valider les US à présenter aux clients et à souligner les points importants à montrer.

Démonstration

Pour clôturer un sprint, l'équipe présente les US (User Stories) terminées devant les clients. Cette démonstration permet de récolter le feedback des clients et de corriger au plus vite les points à améliorer.

Rétrospective

Suite à la démonstration, chaque collaborateur explique ce qui s'est bien passé au cours du sprint et les points à améliorer. Cette réunion a pour but de cerner les problématiques à résoudre afin d'améliorer la performance de l'équipe dans les prochains sprints.

IV. Mes missions sur ITNorms

10. Refonte du portail ITNorms

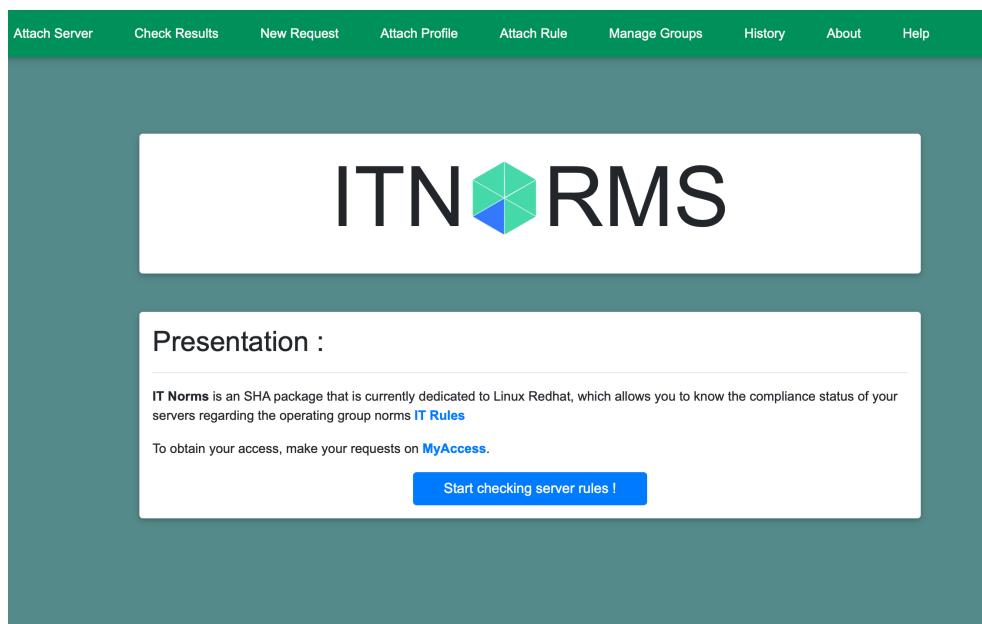
Dans le cadre de l'évolution d'ITNorms il paraît naturel de rendre le portail de l'application le plus intuitif et le plus ergonomique possible. Dans cette optique, j'ai réalisé durant mon premier semestre de nombreuses tâches de résolution de bug ainsi que des apports de nouvelles features sur le Dashboard. Le portail ITNorms est codé en Java avec le framework Angular, s'accompagne de portail un webservice 'IHMBACK' permettant d'interroger la base de données.

Afin de suivre un exemple concret d'une de mes tâches, en voici un exemple.

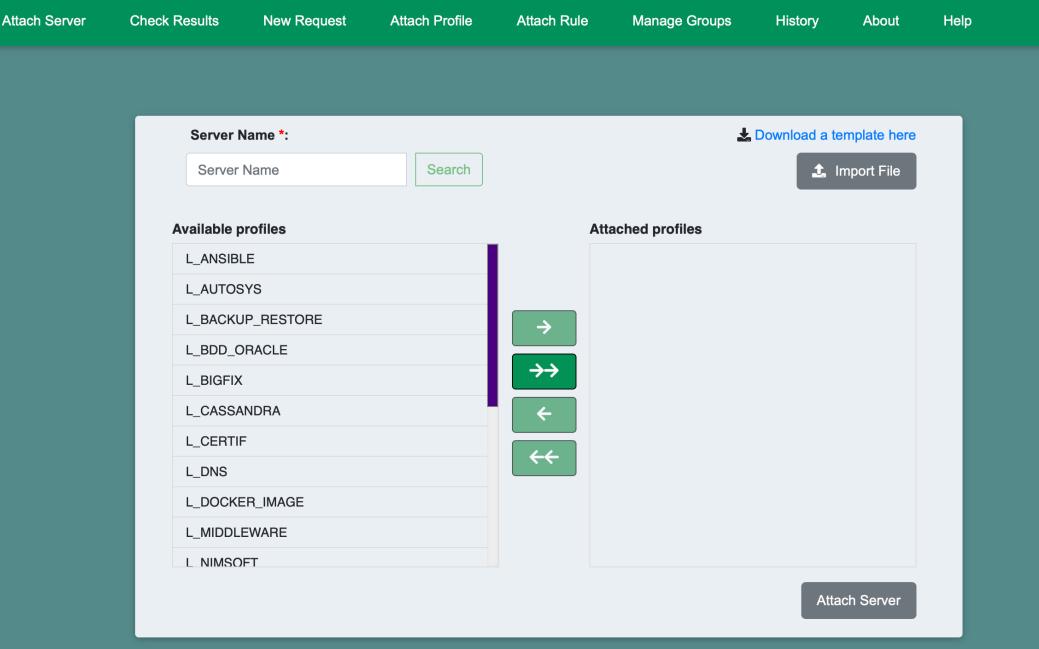
Lors de son utilisation classique le workflow d'ITNorms consiste à attacher un profile à son serveur, puis de générer un request Token, ensuite il faut se connecter à son serveur afin de lancer son analyse grâce au Token et enfin il faut consulter les résultats sur le portail. Ce processus peut sembler compliqué et il est peu intuitif de suivre ce workflow à travers une navbar tel que nous le proposons :



C'est pourquoi, afin de faciliter le processus pour l'utilisateur j'ai réalisé une page d'accueil proposant une pipeline « Start checking server rules ! » qui guide l'utilisateur au fur et à mesure des processus à l'aide d'un défilement ainsi que de courtes descriptions.

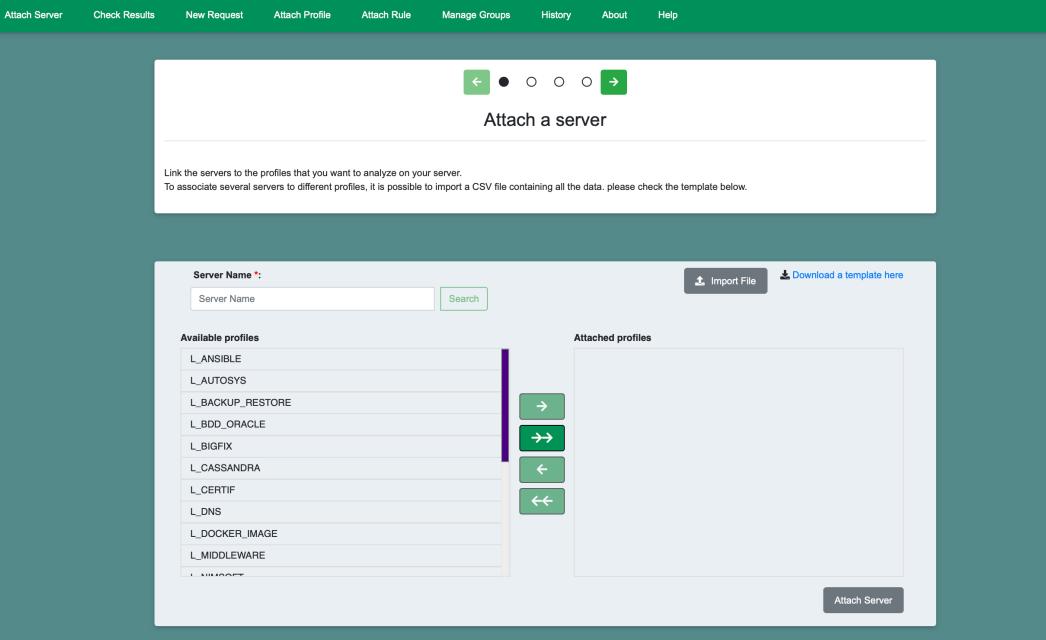


Ainsi une page qui ressemblait auparavant à ceci :



This screenshot shows a previous version of the server attachment interface. At the top, there is a navigation bar with links: Attach Server, Check Results, New Request, Attach Profile, Attach Rule, Manage Groups, History, About, and Help. Below the navigation bar is a search bar with a 'Search' button and a 'Download a template here' link. The main area is divided into two sections: 'Available profiles' on the left and 'Attached profiles' on the right. The 'Available profiles' list includes: L_ANSIBLE, L_AUTOSYS, L_BACKUP_RESTORE, L_BDD_ORACLE, L_BIGFIX, L_CASSANDRA, L_CERTIF, L_DNS, L_DOCKER_IMAGE, L_MIDDLEWARE, and L_NIMSOFT. Between these lists is a vertical toolbar with four buttons: a green arrow pointing right, a green double arrow, a green arrow pointing left, and a green double arrow. At the bottom right of the interface is a 'Attach Server' button.

Sera maintenant présenté de cette manière :



This screenshot shows the updated server attachment interface. At the top, there is a navigation bar with links: Attach Server, Check Results, New Request, Attach Profile, Attach Rule, Manage Groups, History, About, and Help. Below the navigation bar is a large 'Attach a server' button with a circular progress bar. The main area is divided into two sections: 'Available profiles' on the left and 'Attached profiles' on the right. The 'Available profiles' list is identical to the previous interface: L_ANSIBLE, L_AUTOSYS, L_BACKUP_RESTORE, L_BDD_ORACLE, L_BIGFIX, L_CASSANDRA, L_CERTIF, L_DNS, L_DOCKER_IMAGE, L_MIDDLEWARE, and L_NIMSOFT. Between these lists is a vertical toolbar with four buttons: a green arrow pointing left, a black dot, a green arrow pointing right, and a green double arrow. At the bottom right of the interface is a 'Attach Server' button.

11. Refonte des APIs ITNorms

ITNorms est un produit dont le développement s'étend depuis déjà 3 ans, il a vu passer plusieurs développeurs différents qui ont chacun apporté leur brique à cet édifice à travers sa soixantaine de Sprint (au sein de notre équipe un sprint représente 3 semaines). Comme tout architectures, que ce soit dans le domaine du Bâtiment ou en informatique, arrive un moment où la structure a besoin de travaux de de consolidation. Les APIs d'ITNorms (Crcollect, Partners et IHMBack) souffrent du passage de ces différentes équipes. Il en résulte que ces webservices qui proposent des routes en API REST ainsi que des réponses JSON qui se veulent universel et simples d'utilisation ne respectent plus les normes de ces technologies.

C'est pourquoi il m'a été donné la tache de mettre aux normes ces différentes APIs en revoyant le code, afin que les utilisateurs puissent utiliser simplement et efficacement nos services. Pour ce faire j'ai dû éplucher le code, faire des changements et de l'optimisation et à travers les différents environnements (Développement, Qualification et Production), travailler de manière transverse afin de proposer ces changements à mon équipe ainsi qu'à nos clients. De cette manière, je m'assure que le produit ITNorms soit toujours en RUN et que ces changements n'impactent pas directement la production.

Concrètement une route qui auparavant suivait cette logique :

<https://itnormspartners.group.echonet/partners/v2/profiles/{filename}>

Va désormais respecter les normes dictées par le langage REST :

<https://itnormspartners.group.echonet/partners/v2/profiles?filename={filename}>

Swagger des anciennes routes de l'API Partners

certificat-ctl Certificate management module

POST	<code>/v2/certificat</code> <small>createCertificat : Create a certificate from certis</small>
-------------	--

ref-it-rule-ctl ItRule rules management module

GET	<code>/v2/refItRule</code> <small>getAll : Get the ItRule reference</small>
GET	<code>/v2/refItRule/{idItNorms}/{idItNorms}</code> <small>getByRuleId : Get the ItNorms reference</small>

request-ctl Request management module

POST	<code>/v2/req</code> <small>createRequest : Create a request and attach profiles concerned by the request</small>
-------------	---

result-ctl Request results management module

GET	<code>/v2/req/{requestId}/results</code> <small>getProfileByRequestId : Get the list of the profiles by servers depending on the request id</small>
GET	<code>/v2/req/{requestId}/servers/results</code> <small>getServerResultByRequestId : Get the list of the results of the servers depending on the request id</small>

server-ctl Server management module

GET	<code>/v2/req/{requestId}/servers</code> <small>getServersByRequestId : Get the list of servers depending on the request id</small>
GET	<code>/v2/req/servers/{codeAP}/codeap/{env}/env</code> <small>getServersByCodeApAndEnv : Get the list of servers depending on the APcode and the environment</small>
GET	<code>/v2/req/servers/{upm}/upm</code> <small>getServersByUpm : Get the list of servers depending on the UPM</small>
GET	<code>/v2/req/servers/{upm}/upm/{env}/env</code> <small>getServersByUpmEnv : Get the list of servers depending on the UPM and the environment</small>
POST	<code>/v2/servers/{serverName}/profiles</code> <small>attachServerToProfiles : Attach a server to a list of profiles</small>

Swagger des nouvelles routes de l'API Partners

ItNorms API 1.0.0
[Base URL: itnormspartners.group.echonet/partners]
<https://itnormspartners.group.echonet/partners/v2/api-docs>

API pour le module Partners

[Contact MLIST PARIS ITG IPS ITNORMS](#)

ref-it-rule-ctl ItRule rules management module

request-ctl Request management module

result-ctl Request results management module

server-ctl Server management module

Models

V. Problématique Ansible Tower et utilisation de l'authentification SAML.

12. Présentation de Ansible et Ansible Tower

D'après le site de Redhat (l'éditeur de cette suite de logiciel) :

« Ansible est un moteur d'automatisation informatique Open Source qui automatise l'approvisionnement, la gestion des configurations, le déploiement des applications, l'orchestration et bien d'autres processus informatiques. »

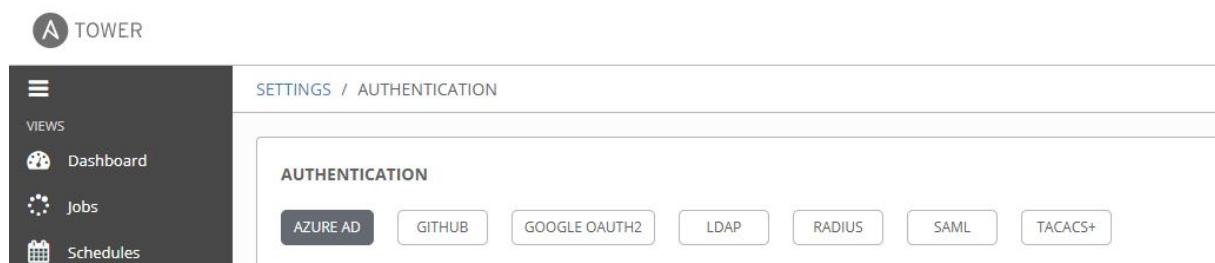
En d'autres termes Ansible est un **orchestrateur**. Son fonctionnement est simple le Master Ansible va se connecter sur des nœuds (les serveurs sous sa gouvernance) à l'aide du protocole SSH.

Ansible se configure à l'aide de Playbook et de Rôles. Ces playbooks se configurent, en leur fournissant une liste de serveurs (hosts) ainsi qu'une suite d'instructions fourni dans un langage très simple (YAML). Ces fichiers de configurations sont ensuite chargés grâce à des modules Ansible, qui interprètent le YAML pour le transformer en commande linux qu'il injecte par SSH.

Ansible Tower est un Dashboard qui vient se pluguer au Master Ansible qui permet de centraliser et contrôler une infrastructure informatique à l'aide d'une UI (User Interface), un contrôle d'accès basé sur les rôles, une planification des tâches, des notifications intégrées et une gestion graphique des stocks. Ansible Tower s'intègre facilement dans les outils et processus existants grâce à son API REST et à son CLI (Command Line Interface).

13. Modes d'authentification offerts par Ansible Tower :

Ansible Tower permet 7 modes de connexions pour authentifier les utilisateurs

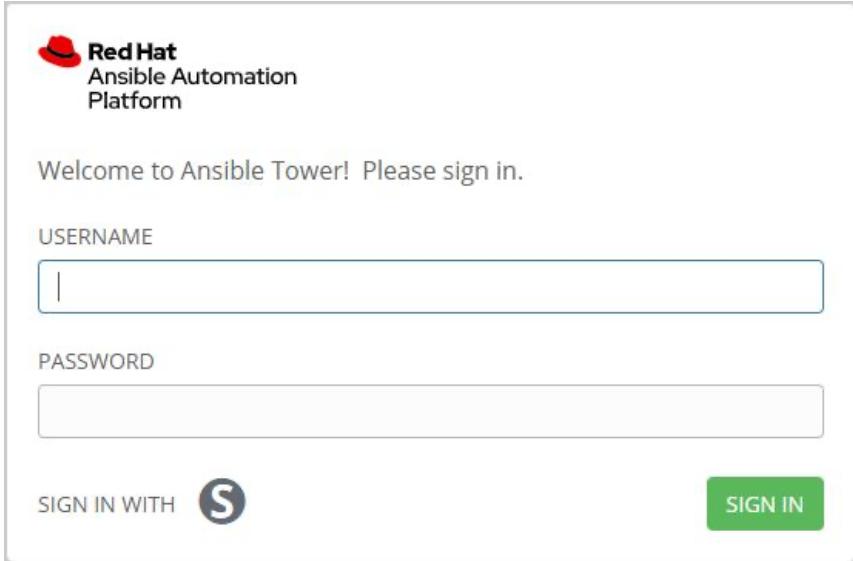


L'usage veut que nous utilisions le SAML pour nous authentifier sur les différents Services du groupe, la connexion LDAP (login / password) est tolérée pour les applications n'offrant pas un niveau de sécurité très élevé (ce qui est de plus en plus rare).

14. Exclusion mutuelle des méthodes d'authentification

Certaines applications supportent bien l'utilisation mixte, du LDAP et du SAML, le LDAP pouvant être utilisé dans le cas où SAML dysfonctionne, c'est le cas par exemple d'outils tels que Gitlab ou Artifactory.

Ansible Tower en revanche ne supporte pas la cohabitation du LDAP et du SAML. Si les deux modes de connexions sont proposés aux utilisateurs



The image shows the Ansible Tower login screen. At the top, there is a Red Hat logo and the text "Ansible Automation Platform". Below that, a message says "Welcome to Ansible Tower! Please sign in." There are two input fields: "USERNAME" and "PASSWORD". Below these fields is a "SIGN IN WITH" button with a "S" icon, indicating SAML authentication. To the right of the "SIGN IN" button is a "SIGN IN" button in a green box.

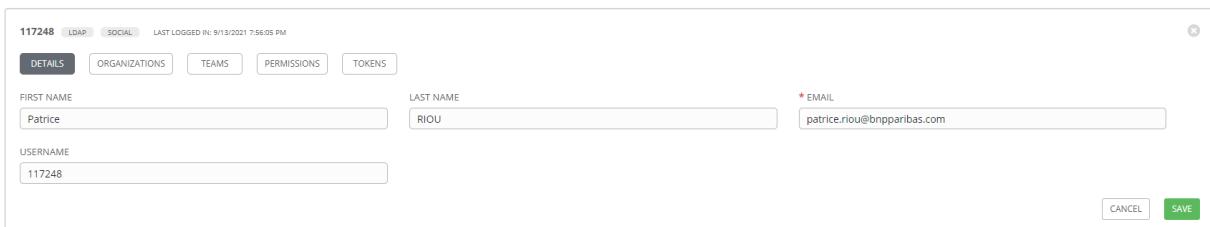
Comme dans cet exemple, on peut s'authentifier par LDAP (login/password) ou SAML (logo S).

Si un utilisateur se connecte uniquement par LDAP, tout se passe bien, et Ansible Tower le classe comme un utilisateur LDAP



The image shows a user profile for a user named "117248". The profile is marked as "LDAP" and "LAST LOGGED IN: 9/13/2021 7:51:02 PM". The "DETAILS" tab is selected. The user's first name is "Patrice", last name is "RIOU", and email is "patrice.riou@bpnparris.com". The "USERNAME" field contains "117248". There are "ORGANIZATIONS", "TEAMS", "PERMISSIONS", and "TOKENS" tabs at the top. At the bottom are "CANCEL" and "SAVE" buttons.

En revanche dès que ce dernier va utiliser l'authentification SAML, il va être reclassé SAML et il ne sera pas possible de revenir en arrière (sauf en supprimant le compte)



The image shows the same user profile for "117248". The "DETAILS" tab is selected. The user's first name is "Patrice", last name is "RIOU", and email is "patrice.riou@bpnparris.com". The "USERNAME" field contains "117248". The "S" icon in the "LAST LOGGED IN" status bar indicates SAML authentication. There are "ORGANIZATIONS", "TEAMS", "PERMISSIONS", and "TOKENS" tabs at the top. At the bottom are "CANCEL" and "SAVE" buttons.

Le mot de passe de l'utilisateur va être « dévalide » par Ansible Tower et ce dernier ne pourra plus se connecter qu'en SAML (même si le SAML dysfonctionne, cela pouvant empêcher la connexion).

15. La problématique de l'API Ansible Tower

Durant le deuxième semestre de mon alternance j'ai principalement œuvré à l'étude de cette problématique, ainsi toutes les explications que vont suivre ont été étudié par Patrice Riou ainsi que leur réalisation à travers un POC sous sa directive :

Même si l'interface graphique (UI) d'Ansible Tower est assez agréable, de nombreux utilisateurs trouvent plus commode de déclencher les jobs par API plutôt que par l'UI, c'est encore plus vrai en ce qui concerne les outils de CI/CD, tel que Gitlab-ci ou Jenkins.

Dans le cas de ces outils il est indispensable de passer par l'API pour déclencher les jobs Ansible Tower. Cette API peut être accédée via une « Basic Authent » via login@passwd ou le codage du login:password en base64 ou alors l'authentification via token avec la fonction « Bearer ».

Si un utilisateur est passé à l'authentification SAML, son mot de passe est invalidé, il n'est plus question pour lui d'utiliser une « basic authent », il est contraint à l'utilisation d'un token pour l'authentification à l'API.

16. Les problèmes s'enchaînent

Afin de sécuriser les connexions un token n'a pas pour vocation d'être éternel, et dans le cas où il doit être changé régulièrement. Se pose la question de son stockage.

Il y a des solutions de stockage de secret, mais il faut que ce secret soit disponible facilement et de préférence sans interaction avec l'utilisateur, nos utilisateurs ont bien noté que le « C » de CD signifie « Continuous » et le fait de s'interrompre pour devoir saisir ses credentials pour la connexion au Safe ou est stocké le secret (en l'occurrence ici le token), n'est pas acceptable puisque cela requiert une intervention humaine.

Il y a des systèmes d'authentifications qui peuvent aider à la création d'une connexion de confiance entre deux applicatifs, c'est le cas d'OIDC qui est déjà utilisé dans l'entreprise via Keycloak (token JWT). Hélas, là encore, Ansible Tower offre une solution de serveur JWT (via son système de gestion d'Applications) mais il n'est pas client JWT. C'est une fonctionnalité qui est envisagée par Redhat mais qui n'est pour l'instant pas disponible.

Avec plusieurs milliers d'utilisateurs et un temps de développement restreint, nous ne pouvons pas non plus nous lancer dans une solution de stockage de secret maison, dédiée, en haute disponibilité. Nous devons coller aux standards du marché, avec un minimum de développement maison.

Nous nous ajoutons une contrainte supplémentaire (qui satisfera nos utilisateurs et nous rendra la tâche plus commode en termes de gestion de la sécurité). Le token utilisé par l'API restera invisible de l'utilisateur.

Il faut enfin sécuriser la fourniture du token pour qu'un utilisateur ne puisse pas usurper une identité en demandant la génération d'un PAT (Private Acces Token) qui ne lui appartient pas.

17. La solution que nous avons envisagée

Cette solution tourne autour de trois axes :

- La simplicité pour l'utilisateur : il n'aura pas à mémoriser ou stocker son token
- La sécurité : on s'assurera que le PAT sera donné à la bonne personne (ou à défaut une personne ayant le même niveau de responsabilité)
- La traçabilité : en cas d'audit de sécurité ou de suspicion d'usurpation d'identité

Se base sur 3 étapes :

- Un enrôlement au service
- Une pre-authent pour limiter les accès frauduleux
- Une génération de PAT, à la volée et à la demande, avec une durée de vie courte (la durée de vie d'une pipeline CD) que nous avons estimé à 4h maximum

Une solution intégrée aux pipelines :

- Gitlab-ci
- Jenkins
- CDD

Pour les utilisateurs souhaitant utiliser l'API par leur propres moyens (via shell scripts, ou Python) nous n'offrons pas de solution, ils devront gérer eux même la génération du token, son stockage et son utilisation.

18. Briques utilisées

Nous allons utiliser :

- Hashicorp Vault, offre de service interne déjà à disposition pour le stockage du secret intermédiaire
- Ansible Tower pour :
 - Créer le PAT (via une API maison)
 - Créer les playbooks d'interface avec nos utilisateurs
- Un binaire en C (afin de cacher le fonctionnement de génération du PAT aux utilisateurs) intégré dans les outils de pipeline

19. Le détail des 3 étapes de génération de token

Enrôlement

Via un playbook lancé depuis tower, sous son identité, l'administrateur de l'espace Tower d'une entité (une organisation au sens Ansible Tower). Cela va avoir pour action de créer l'emplacement d'un nouveau secret sur Hashicorp, la création d'un profile donnant les droits en lecture sur ce secret et la création d'un credential (authentification AppRole) associé à ce profile.

Le Rôle ID (méthode d'authentification AppRole d'Hashicorp) sera fourni à l'administrateur pour valider son enrôlement et il aura la charge de stocker cet ID dans une variable privée sur son projet CD (gitlab/jenkins/CDD) : HASHI_KEY. Si cet ID venait à être perdu, le service ne serait plus utilisable, et il faudra alors à l'administrateur demander un nouveau refresh de son credential Hashicorp.

Le token d'orga

Chaque semaine, l'administrateur devra générer un nouveau token pour son entité, ce token aura une validité de 7 jours. Il fera cette opération via un second playbook (lancé depuis tower).

Cette action aura pour effet de stocker dans son secret Hashicorp, son token d'orga. Ce token sera requis pour la dernière étape : la génération du PAT.

Le PAT ou token de pipeline

Lors de l'exécution du pipeline, un appel au binaire en C sera faite. Le rôle du binaire :

- Collecter les informations nécessaires
- Fournir un PAT qui sera stocké dans une nouvelle variable privée : PIPE_TOKEN

Le binaire va :

- Récupérer l'identité de l'appelant via les variables système de l'outil CD (nom différent suivant les outils)
- Récupérer le HASHI_KEY et s'en servir pour récupérer le token d'orga dans Hashicorp. NB : une partie de l'authent est fournie par la variable HASHI_KEY (RoleID) et le binaire contient le SecretID (deuxième partie de l'authent). Il est donc impossible de récupérer le secret de Hashicorp par une autre méthode que le binaire.
- L'appartenance de l'utilisateur à l'organisation associée au token est nécessaire pour valider la restitution du PAT (traité au niveau de l'API maison)
- Appel de l'API maison installée sur le serveur tower avec les paramètres suivants :
 - o Nom de l'utilisateur
 - o Token d'orga
 - o Checksum du binaire lui-même

L'API va :

- Créer le PAT associé à l'utilisateur connecté sur l'outil CD.
- Tracer le demandeur, l'ORGANISATION, l'IP Source et le checksum du binaire appelant.
- Si les conditions sont réunies on aura en output un PAT Ansible Tower associé au demandeur valable 4h (que le binaire fournira en output)

Il ne reste plus qu'à stocker le token dans une variable privée de l'environnement CD (son contenu n'apparaît pas dans le log CD) et d'utiliser cette variable sur les différents appels API vers tower

Schéma fonctionnel de l'enrôlement

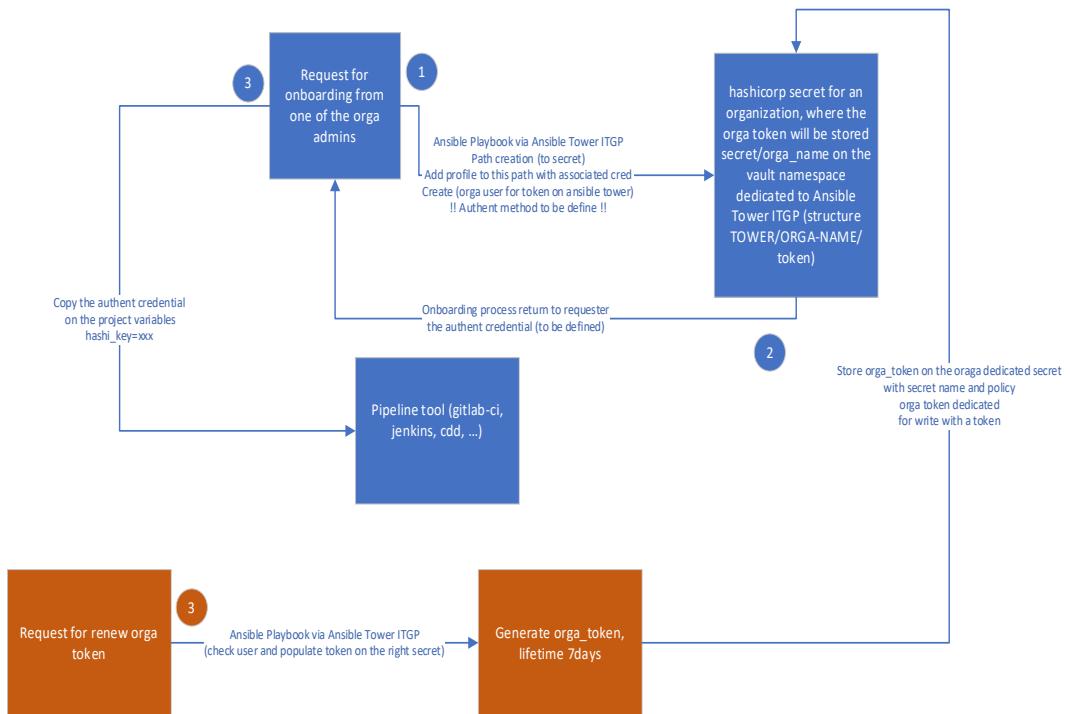
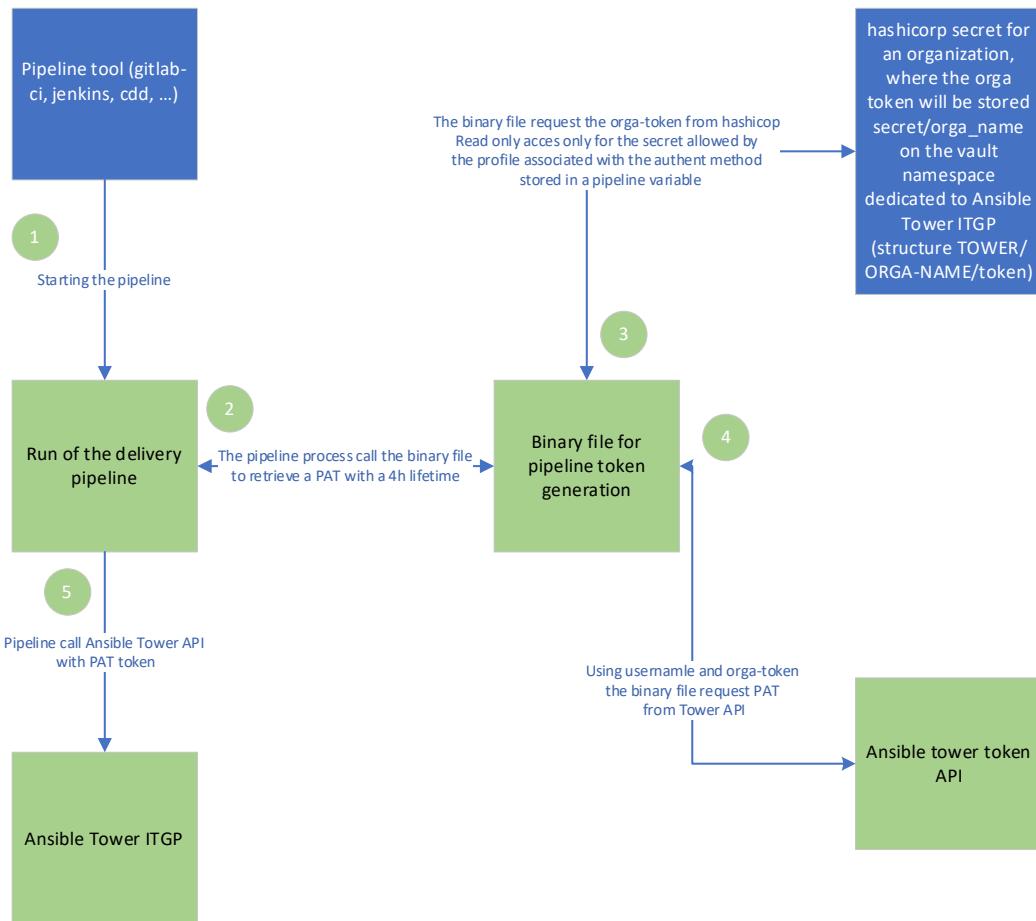


Schéma fonctionnel de l'utilisation d'un Private Access Token



VI. Bilan et recul sur la mission

20. L'organisation de l'entreprise

BNP Paribas malgré son statut de grande entreprise se structure autour de nombreuses petites équipes indépendantes les unes des autres. Chaque équipe joue un rôle et des missions bien précis conférant un dynamisme transverse pertinent. Néanmoins de petites équipes impliquent une hiérarchie plus horizontale qui réduit le processus de prise de décision et de transmission de l'information. Cette logique permet un détachement des tâches précis et peut augmenter les performances de production en revanche il ralenti considérablement les échanges transverses. Ainsi il m'est souvent arrivé d'être dans l'attente de réponses afin de pouvoir finir les tâches sur lesquels j'étais.

A la BNP Paribas, il n'y a pas de document résumant la totalité des projets ayant été mis en place ou en cours au sein du département informatique. Par conséquent, il arrive que des équipes travaillent sur un produit similaire au sein de deux équipes totalement différentes, de même il est quasi impossible chercher un produit existant au sein du groupe. Et même dans le cas où vous avez la connaissance de la portabilité du produit dans l'entreprise il est très dur de trouver les informations relatives au produit et à ses responsables.

21. Mon apport à l'entreprise

Tout au long de cette aventure professionnelle, j'ai pu contribuer à la réalisation du projet ITNorms tant à travers mes compétences informatiques que mes compétences relationnelles. Au sein de mon équipe, nous étions seulement deux apprentis à travailler sur les APIs. Cela nous a permis de mettre au service de l'entreprise nos talents de développement mais aussi et surtout notre talent relationnel et de prise de décision.

De plus, en tant que nouvel arrivant, j'ai pu apporter un regard neuf et non biaisé sur le projet. J'ai pu remarquer que les APIs méritait une sérieuse refonte étant donné que les informations fournies par l'application n'étaient pas optimisées pour l'utilisation des clients. Je pense qu'apporter ce regard neuf est une chose fondamentale dans une équipe, il permet de remettre certaines pratiques en question par des personnes qui ne parviennent plus à se rendre compte de certaines problématiques ayant pris l'habitude de travailler de la même manière sur une grande période.

22. Les apports personnels de l'alternance

Cette alternance m'apporte beaucoup sur l'aspect professionnel et technique tout comme sur mon développement personnel et sur la culture de l'entreprise de manière générale. Elle me permet de consolider mes connaissances en Java et apprendre de nouvelles astuces du langage qui me permettront à terme de produire un code optimisé et lisible.

Cette alternance a une note toute symbolique à mes yeux car c'est la première longue expérience professionnelle dans le domaine de l'informatique. J'ai ainsi découvert le monde du travail avec ses avantages comme ses contraintes et une réelle culture d'entreprise. Même si le monde de l'informatique peut paraître distant et technique pour certaines personnes il ne faut pas oublier que des hommes et des femmes collaborent au quotidien dans leurs missions. Par conséquent, il est fondamental de savoir communiquer et entretenir de bonnes relations au sein d'une équipe pour pouvoir à la fois apprécier ses journées et avoir une bonne synergie de travail.

23. Conclusion

Cette alternance est ma première longue expérience professionnelle en informatique. C'est une expérience très enrichissante pour moi car j'ai pu découvrir la méthode Agile et sa mise en pratique dans un contexte professionnel. J'ai pu consolider mes bases en Java et j'ai l'opportunité d'apprendre à utiliser des outils d'automatisation de déploiement opérationnel. Cette expérience m'a également permis de découvrir l'environnement et l'ambiance de travail dans une grande entreprise.