



Rapport de stage S10

Paul LEFAY

2021/2022

TYPE : ☒ Stage de fin d'études (Stage ingénieur - S10)
ENTREPRISE : Empreinte digitale
DATES : Du 31 janvier 2022 au 11 septembre 2022
SUJET MISSION : Analyse et réalisation d'audits automatisés de l'infrastructure
TUTEUR ENTREPRISE : Valentin Baraise et Yves-Gaël Cheny



**empreinte
digitale**

Créateur de vos **SOLUTIONS**
NUMÉRIQUES RESPONSABLES

OPTION : ☒ CSS
CONFIDENTIALITÉ : Mon rapport est confidentiel niveau : ☒ 0
DOMAINE ENTREPRISE : ☒ Autres (précisez) : Développement d'applications, hébergement web, conformité RGPD, audit d'accessibilité.
AUTRES POINTS : ☐ Stage à dominante **management**
☐ Stage à dominante **recherche**
☒ E5e effectuée sous Contrat Pro
☒ Mon tuteur sera présent à ma soutenance
☒ Mon tuteur participera au déjeuner le jour de ma soutenance

1 Engagement de non plagiat

Je soussigné(e), Paul LEFAY, étudiant à l'ESEO, atteste avoir pris connaissance du contenu du Règlement intérieur de l'École et de l'engagement de « non-plagiat ». Je déclare m'y conformer dans le cadre de la rédaction de ce document. Je déclare sur l'honneur que le contenu du présent mémoire est original et reflète mon travail personnel. J'atteste que les citations sont correctement signalées par des guillemets et que les sources de tous les emprunts ponctuels à d'autres auteur(e)s, textuels ou non textuels, sont indiquées. Le non-respect de cet engagement m'exposerait à des sanctions dont j'ai bien pris connaissance.

Fait à Angers le 11 février 2021.

2 Remerciements

Je tiens à remercier Yves-Gaël Cheny, Nicolas Gourichon et Valentin Baraise pour l'opportunité qu'ils m'ont donné en m'acceptant en contrat de professionnalisation. L'expérience acquise lors de la période de Projet de Fin d'Etude (PFE) est inestimable comparée à celle que j'aurai eu si j'avais travaillé sur un PFE scolaire.

Je remercie particulièrement Valentin Baraise, mon tuteur, pour son accompagnement durant toute cette année. Bien que très occupé, il a toujours pris le temps de m'accompagner lorsque j'étais bloqué. Il a également (malgré lui), pris la peine de réparer les quelques erreurs que j'ai pu commettre.

Je remercie également Inès Audouin et Nicolas Gourichon, qui m'ont accompagné sur mes premières installations et utilisations d'Ansible. Ils m'ont apportés de nombreuses connaissances sur le sujet, ce qui fait qu'à ce jour, je suis autonome sur l'utilisation des outils Ansible et AWX.

Enfin, merci à Yves-Gaël Cheny et Raphaël Poitevin pour l'aide qu'ils m'ont apportée, notamment sur les aspects réseaux et mail.

Table des matières

1	Engagement de non plagiat	2
2	Remerciements	3
3	Introduction	7
4	Abstract	8
5	L'environnement et le contexte du stage	9
5.1	Contrat de professionnalisation	9
5.2	Empreinte Digitale	9
5.2.1	Activités	9
5.2.2	Structure	10
5.2.3	Responsabilité sociétale et environnemental	10
5.3	Le pôle datacenter	13
5.4	Comité sécurité	14
5.5	Sujet	14
5.5.1	Contexte	14
5.5.2	Problématique	14
5.5.3	Objectifs	14
5.5.4	Outils et ressources	15
6	Préambule technique	16
6.1	Proxmox	16
6.2	Terraform	18
6.3	Ansible	19
7	Travaux de sécurité	21
7.1	Période d'alternance	21
7.2	16 thématiques de sécurité	22
7.3	Inventaire des machines	24
7.3.1	Description	24
7.3.2	Architecture	24
7.3.3	Principe de fonctionnement	25
7.3.4	Ajout d'un plugin	25
7.3.5	Installation avec Ansible	26
7.3.6	Bilan	28

7.4	Durcissement Linux	29
7.4.1	Objectif	29
7.4.2	Openscap	29
7.4.3	Création de machines virtuelles de test	29
7.4.4	Création d'une archive Debian	29
7.4.5	Mise en oeuvre	30
7.4.6	Bilan	31
7.5	Documentation	32
7.5.1	Objectif	32
7.5.2	Documents	32
7.5.3	Outils	32
7.5.4	Bilan	32
7.6	Autres pistes d'étude	33
7.7	Bilan	34
8	Travaux d'administrateur système	35
8.1	Nextcloud et Collabora	35
8.1.1	Objectif	35
8.1.2	Schéma applicatif	35
8.1.3	Description	35
8.1.4	Utilisation des variables	36
8.1.5	Inventaire Ansible	37
8.1.6	Utilisation d'AWX	37
8.1.7	Rôle Ansible	38
8.1.8	Conclusion	38
8.2	Proxmox	40
8.2.1	Rappel	40
8.2.2	Objectif	40
8.2.3	Matériel	40
8.2.4	Logiciel	40
8.3	Projet Dehon	42
8.3.1	Objectif	42
8.3.2	Installation matériel	42
8.3.3	Création des cluster de machines physiques avec proxmox et terraform	43
8.3.4	Installation du clusters Kubernetes via Kubespray	44
8.3.5	Configuration de proxy avec vip	44
8.3.6	IngressController, Certmanager, namespace, rancher rke	44
8.3.7	Stockage	44

8.3.8	Mongo Arbiter	44
8.4	Actualisation et mise en oeuvre de la procédure d'arrivée	45
8.4.1	Objectif	45
8.4.2	Description	45
8.4.3	Documentation	45
8.4.4	Groupe de Travail Embarquement	45
8.5	Bilan	46
9	Bilan personnel	47
10	Annexes	48
10.1	CV	48
10.2	Planning détaillé de la période d'alternance	49
10.3	Planning détaillé de la période de stage	50
10.4	Bibliographie	51
10.5	Liste des figures	52
10.6	Liste des tables	53
10.7	Acronymes et définition	54

3 Introduction

Mon sujet de stage S10 orienté autour de la sécurité informatique porte sur la mise en place de divers outils pour améliorer l'infrastructure. J'ai principalement travaillé sur des outils d'inventaire des machines du système d'information et sur le durcissement des systèmes Linux. En parallèle de ces travaux de sécurité, j'ai mis en place de nouvelles infrastructures ou logiciels pour des clients, amélioré le processus pour les nouveaux arrivants et rédigé de la documentation technique propre aux administrateurs système.

Ce stage à eu lieu dans le cadre d'un contrat de professionnalisation chez Empreinte Digitale, située au 10 rue des Noyers à Angers. J'y ai effectué mon stage de 7 mois du 30 janvier 2022 au 8 septembre 2022. Ce rapport à donc été rendu 2 semaines avant la fin du stage.

Ce stage fait suite à un besoin grandissant d'Empreinte Digitale d'améliorer en continu l'infrastructure sur divers aspects de sécurité. Étant une entreprise développant des applications web et hébergeant des applications open-source, elle se trouve impacté par la menace grandissante des attaques informatiques.

Mon rapport s'organise en 4 parties. Dans la première, j'exposerai l'environnement et le contexte du stage. La seconde partie sera consacrée à la présentation de 3 outils techniques régulièrement utilisées et cités dans ce document. Dans une troisième partie, j'évoquerai les travaux de sécurité avec les thématiques de sécurité, l'inventaire des machines, le durcissement des systèmes Linux et la documentation. Viendra en 4ème parties les divers travaux d'administrateur système. Enfin, je conclurai par un bilan personnel.

Ce rapport a été rédigé en \LaTeX à partir du template de M Woodward.

4 Abstract

5 L'environnement et le contexte du stage

5.1 Contrat de professionnalisation

Pour rappel, j'ai effectué mon stage en contrat de professionnalisation. J'étais donc présent en entreprise la plupart des jeudis et vendredis du 8 Septembre 2021 au 30 janvier 2022. J'ai par la suite enchaîné avec la période de stage du 31 Janvier 2022 au 7 Septembre 2022.

Dès le début de mon contrat de professionnalisation, le sujet portait sur la sécurité. Les travaux effectués durant l'alternance sont donc les prémices des travaux effectués lors du stage.

5.2 Empreinte Digitale

Empreinte Digitale est une SCOP d'une cinquantaine de collaborateurs basée sur Angers depuis 27 ans. Elle travaille dans la réalisation de solutions numériques responsables et sur mesures.



5.2.1 Activités

L'activité de l'entreprise se découpe en 5 axes :

Développement sur-mesure : réalisation de logiciels répondant à un besoin métier.

Hébergement en cloud privé : hébergement Web responsable en Cloud privé indépendant dans des Datacenter en France. Les serveurs sont exclusivement gérés avec des technologies libres et open source, garantissant une indépendance d'entreprises tierces.

Accessibilité numérique : audit de services numériques, formations et accompagnement dans la mise en place de démarche de mise en accessibilité des sites et services.

Système d'information archivistique : suite logicielle Ligeo Archives, un système d'information archivistique. Il répond aux besoins de gestion et de valorisation du patrimoine archivistique, tout en garantissant une souplesse d'utilisation, de paramétrage et une ergonomie moderne.

Mise en conformité RGPD : évaluation du niveau de conformité RGPD avec pilotage de la mise en oeuvre des préconisations essentielles à la mise en conformité au RGPD.



5.2.2 Structure

Juridiquement, une SCOP (Société coopérative et participative) est une société coopérative de forme SA, SARL ou SAS dont les salariés sont les associés majoritaires et le pouvoir y est exercé démocratiquement. Les salariés détiennent au moins 51 % du capital social et 65 % des droits de vote. Si tous les salariés ne sont pas associés, tous ont vocation à le devenir. Chaque salarié associé dispose d'une voix, quel que soit son statut, son ancienneté et le montant du capital investi. Les informations liées à la vie de l'entreprise circulent en toute transparence et les décisions stratégiques sont l'expression du plus grand nombre.



Financièrement, cela signifie qu'Empreinte Digitale fonctionne sur un principe de réserve, avec une répartition d'au moins 25 % du résultat reversé sous forme de participation pour tous les salariés en fonction de leur ancienneté.

La SCOP apporte un avantage dans la pérennisation de l'entreprise et ses emplois avec un modèle attirant pour les futur collaborateurs. La transparence et la collaboration est un facteur clé dans l'entretien de l'implication et la motivations des salariés.

La gouvernance se découpe de la manière suivante :

La gouvernance coopérative est similaire au fonctionnement d'une association loi 1901 avec les membres de l'association et le conseil d'administration. Le conseil d'administration a pour rôle de déterminer les orientations de l'activité de la société. Actuellement, l'assemblée générale est consisté de 32 salariés. Un salarié ne peut pas rester dans l'entreprise si au bout de 3 ans d'ancienneté celui-ci ne veut pas adhérer à la SCOP. Cette assemblée générale mandate le conseil d'administration constitué des membres élus et en "échange", les membres de conseil anime, représente et rend compte aux associés.

De l'autre côté on trouve la gouvernance de l'entreprise, avec un directeur général, responsable légale qui travail avec un comité opérationnel ou COMOP. Ils travaillent avec les différents pôles dans la mise en oeuvre de la stratégie d'entreprise.

La partie décisionnel est aux salariés car c'est bien la gouvernance coopérative qui mandate et pilote la gouvernance d'entreprise, qui elle propose et rend compte de l'activité.

Une assemblée générale ordinaire à lieu une fois par an pour voter les grandes orientations de l'entreprise, valider les comptes, voter la répartition des bénéfices et également voter pour les nouveaux associées.

5.2.3 Responsabilité sociétale et environnemental

L'axe principal de la démarche RSE chez Empreinte Digitale porte sur le numérique responsable, qui intègre à la fois des problématiques environnementales et sociétales.

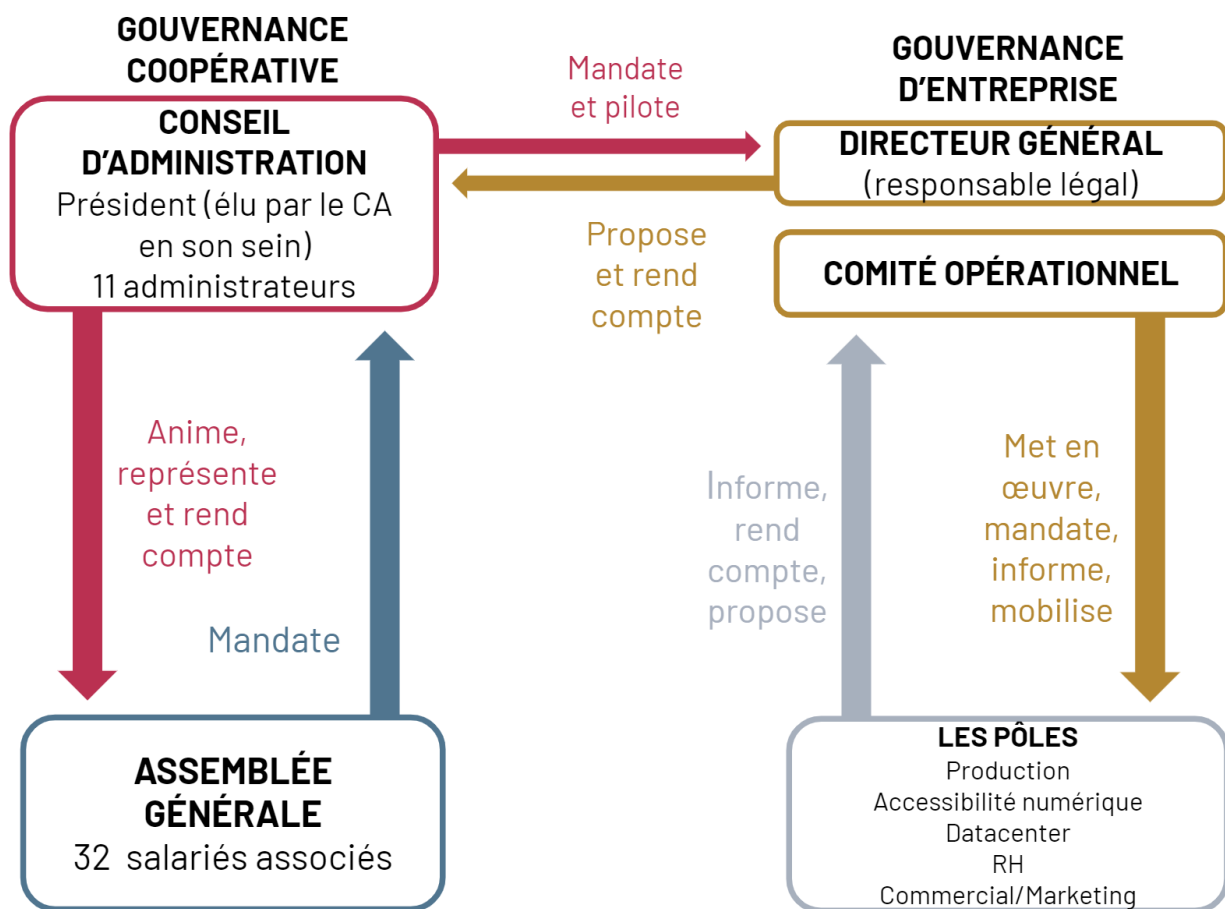


Figure 5.1: Schéma de la gouvernance chez Empreinte Digitale

Empreinte digitale est officiellement engagés dans une démarche Responsabilité Sociétales des Entreprises (RSE) depuis 2018, année de sa labellisation Lucie ISO 26000. LUCIE est une certification qui prouve qu'une entreprise, un produit ou un service à une démarche réussie en matières de RSE.



Voici quelques projets RSE d'Empreinte digitale :

Design4Green Le Design4Green est un challenge organisé tous les ans de depuis 5 par l'ESAIP, une école d'ingénieur Angevine basée sur Angers. C'est un hackathon en équipe de 48h durant lequel il faut répondre à un sujet autour de l'éco-conception.

Chaque année, l'objectif du concours était de développer un projet web en limitant son empreinte environnementale. En 2021, il fallait développer une interface pour les professionnel de suivi de l'éco-conception d'un projet web intégrant 491 critères.

Empreinte à participé à cette édition 2021 et l'a remporté avec une application statique. Cela permet de réduire au maximum la consommation de ressources au niveau du serveur. Le site à

été conçu sous forme de "Progressive Web App" (PWA). L'application est alors téléchargée une seule fois et mise en cache dans le navigateur, ainsi il n'y a pas d'aller-retour avec le serveur. Avec son application, Empreinte Digitale a remporté le concours et gagné un chèque de 1000€. Cette argent fut par la suite placé dans le budget participatif.

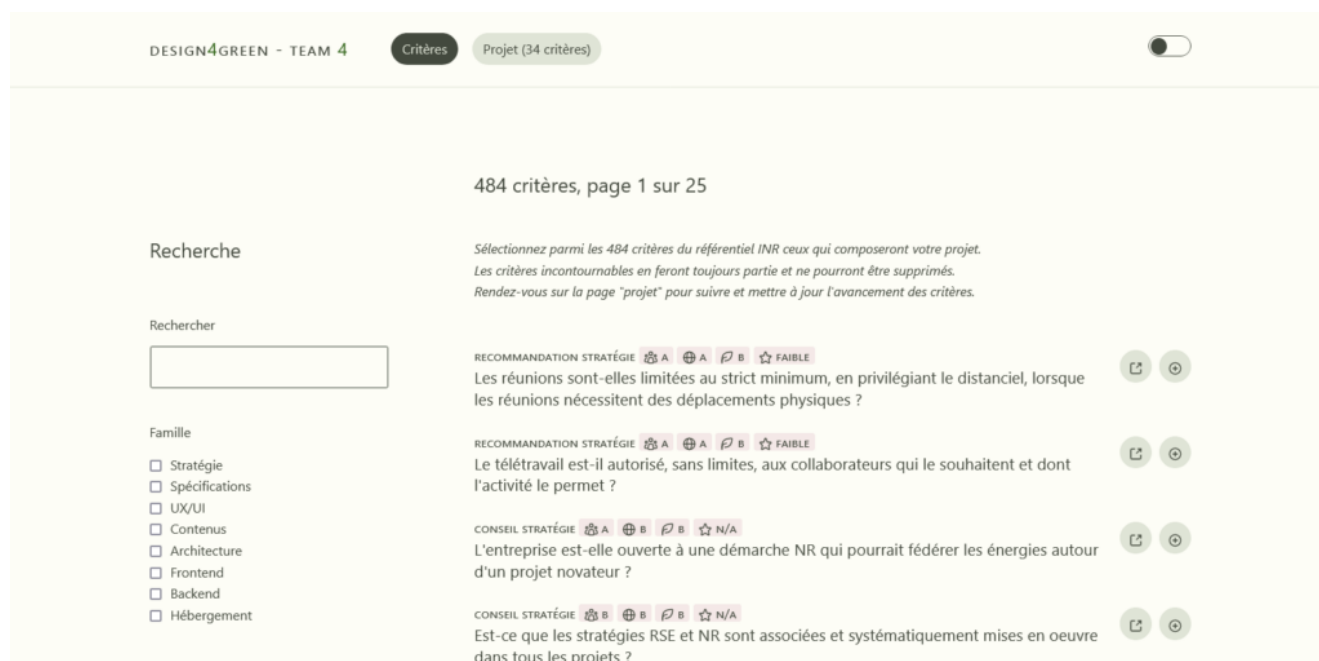


Figure 5.2: Application web réalisée par Empreinte Digitale pour le Design4Green

Budget participatif En 2022, Empreinte Digitale a lancé un appel à projet nommé Budget Participatif. Chaque employé pouvait présenter un ou plusieurs projets qui ont été ensuite soumis à vote. Pour financer les divers projets, l'argent gagné au Design4Green a été mis en jeu et une participation supplémentaire de 1000€ a été attribuée par l'entreprise. Ainsi, c'est 2000€ de projets, proposés par les salariés, qui ont vu le jour. Parmi eux, console de jeu, abri pour oiseaux, salle de sport, jeu de fléchette etc.

Stratosfair En 2022, Empreinte Digitale a lancé un partenariat avec Stratosfair. L'objectif, créer un datacenter responsable. Ce nouveau datacenter a vu le jour deux ans à Lanester, une ville voisine de Lorient. L'idée est d'utiliser des énergies renouvelables produites sur place, d'utiliser à bon escient la perte d'énergie (chaleur) engendrée par les serveurs et de se "fondre" dans le milieu naturel.

- Le datacenter n'est pas posé à même le sol, ne bloquant pas la circulation des organismes vivant dans le sol.
- Une partie de l'énergie qui alimente les divers serveurs est une énergie renouvelable générée par des panneaux solaires.
- La chaleur des serveurs est redirigée dans une serre permettant la culture de légumes bio.



Figure 5.3: Maquette 3D du datacenter de Stratosfair

Avec ce datacenter, stratosfair lance une offre similaire à celle OVH etc. avec la mise à disposition de machines virtuelles. Empreinte Digitale a donc travaillé avec Stratosfair sur l'installation de 3 serveurs physiques ainsi qu'au développement d'une application et d'une API pour la génération de machine virtuelle via API dans un cluster Proxmox.

5.3 Le pôle datacenter

Empreinte digitale est constitué de 5 pôles : production, accessibilité numérique, datacenter, RH et commercial/marketing.

J'étais intégré dans le pôle Sysadmin composé de 7 personnes. Les activités sont découpables de la manière suivante :

- **Ligeo** : deux personnes travaillent principalement sur les produits Ligeo. Cela comprend les installations, les mises à jours et la maintenance.
- **Cloud** : une personne travaille sur la conception, les installations et la maintenance des produits cloud. Cela va de l'installation de produits tels que Nextcloud, Zammad, Bitwarden jusqu'à la conception et l'installation d'architecture spécifique à un besoin. C'est le cas par exemple pour le projet Dehon, décrit en partie.
- **Travaux interne** : deux personnes, moi y compris, pour travailler sur divers travaux interne. Cela concerne notamment les besoins salariés : PC, mail, compte, accès etc.
- **Commercial** : une personne pour la partie commercial.
- **Chef de projet** : une personne sur la gestion de projet, en lien avec le commercial.

Mise à part la partie commercial et chef de projet, les activités ne sont pas à ce point-là segmentées. Dû au astreinte et à l'entre-aide collective, tout le monde "touche à tout". Par exemple, bien qu'ayant travaillé majoritairement sur des travaux interne, j'ai également travaillé sur des offres cloud.

Les astreintes vont également couper cette segmentation. Les astreintes, toujours pas deux avec une personne principales et une personne de support si nécessaire obligent chacun à être capable d'intervenir sur n'importe quel service.

5.4 Comité sécurité

Mon stage ayant une dominante sur la sécurité, j'ai été intégré au comité sécurité de l'entreprise. Celui-ci est composé d'une dizaine de personnes aux profils variés. On y trouve des développeurs, Sysadmin, testeurs et chefs de projet.

Le pôle sécurité étant assez récent, ça mission est pour le moment de maintenir une veille sur la sécurité afin d'apporter des axes d'améliorations. Cela tiens compte du développement, de l'hébergement, la documentation et les bonnes pratiques générales à l'attention de tous.

5.5 Sujet

5.5.1 Contexte

Empreinte digitale développe son offre DATACENTER. Cela engendre une évolution rapidement de l'infrastructure qui demande de nouveaux besoins notamment en matière de sécurité. En effet, l'entreprise ne possède pas pour le moment d'outils de conformité, d'outils de contrôle de sécurité ni d'outils de CVE. De plus, il n'y a pas de documentations mis à disposition des salariés afin de spécifié le comportement à avoir lors de l'utilisation du SI ou en cas de faille de sécurité révélée.

5.5.2 Problématique

Les problématiques sont multiples :

- Comment réaliser un état des lieux du système d'information actuel ?
- Comment établir les besoins en hiérarchisant les priorités ?
- Comment faire un choix parmi l'ensemble des outils d'audits disponibles ?
- Comment pérenniser les solutions mises en oeuvre ?

5.5.3 Objectifs

Travailler en mode projet sur l'infrastructure de l'entreprise afin d'améliorer celle-ci en continu. Cela passe par la mise en oeuvre de nouveaux outils mais également de nouvelles procédures

afin de pérenniser les solutions. En parallèle, il y a divers tâches annexes d'administration système sur l'installation de nouveaux logiciels pour les clients, la configuration de matériels pour les nouveaux arrivants, etc.

5.5.4 Outils et ressources

Afin de réaliser les divers objectifs, il n'y a aucune limitation des ressources et matériels. Les accès administrateur sur les plate-formes nécessaires à la mise en oeuvre de l'objectif ont été donnés. L'objectif n'étant pas concentré sur un sujet en particulier, les divers documentations de l'ANSSI servent de conseil.

6 Préambule technique

Les travaux effectués on fait appels à des logiciels régulièrement cités dans ce document. Afin de rendre la compréhension de ce rapport plus aisée, cette section décrit brièvement Proxmox, Terraform et Ansible.

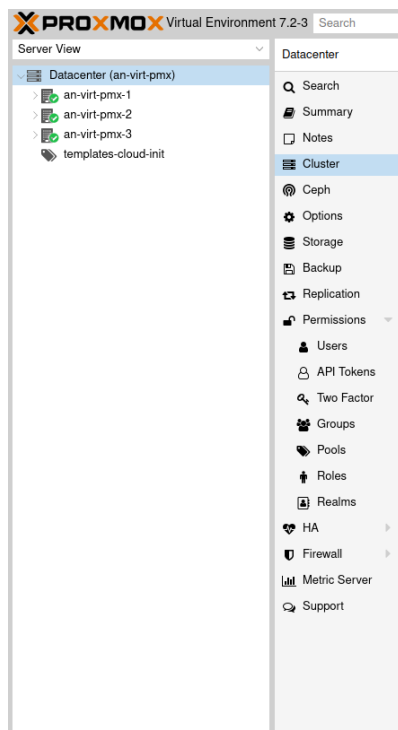
6.1 Proxmox

Proxmox est une plate-forme open-source complète pour la virtualisation d'entreprise. Grâce à l'interface Web intégrée, nous pouvons facilement gérer les machines virtuelles et les conteneurs, le stockage défini par logiciel, la mise en réseau, le clustering haute disponibilité et plusieurs outils prêts à l'emploi sur une seule solution.



Proxmox possède 3 outils pour manipuler l'ensemble des ressources :

- Un utilitaire en ligne de commande installé.
- Une API.
- Une interface web.



Depuis l'interface, on visualise l'élément Datacenter, correspondant au cluster. On visualise également chacun des noeuds du cluster avec leur nom et leur état. Depuis la section Datacenter, on peut modifier les noeuds, les différents stockages, la configuration de backup avec l'ajout de serveur de backup tel que Proxmox Backup Server, les permissions utilisateurs, la haute disponibilité du cluster (HA), les statistiques et le support.

Il est également possible d'agir sur les noeuds ou sur les machines virtuelles qui y sont installées. La vision sur un noeud représente un tableau de monitoring du noeud, avec des statistiques résumant les ressources occupées. La vision sur les machines virtuelles résume l'état d'une machine virtuelle, ses caractéristiques principales telles que l'usage du CPU, de la mémoire, de la taille du disque et les adresses IPs. Les parties hardware utilisateur peuvent être modifiées depuis l'interface.

Empreinte Digitale possède 3 clusters Proxmox :

- Un de 3 noeuds à Angers destiné aux tests.

- Un de 11 noeuds à Rennes pour la production.
- Un de 4 noeuds à Tours pour la production également.

Au niveau du stockage, chacun des noeuds est configuré avec 2 pools de stockages. Le premier `ssd` regroupe l'ensemble des disques `ssd`. Celui-ci est utilisé lorsqu'il y a un besoin de performance. Le second `hdd` regroupent les disques `hdd`. Il est utilisé lorsqu'il faut stocker des grands volumes de données mais qui sont rarement actualisés ou utilisés. Enfin, un stockage partagé entre les noeuds permet de déposer les images ISO de différents systèmes d'exploitation utilisés pendant les installations.

Lors du déploiement d'une nouvelle machine virtuelle, nous passons souvent par Terraform et l'API du cluster. En plus des backups, cela permet de garder le code source de la création de machines virtuelles et ainsi donner une autre possibilité de reconstruction de l'infrastructure.

6.2 Terraform

Terraform est un outil open source d'infrastructure as code développé par Hashicorp. Il permet de déclarer sous forme de code l'infrastructure que l'on souhaite obtenir. Dans des fichiers de configuration structurés, basé sur un système d'état, on va pouvoir manager l'infrastructure et mettre à jours son état.



Au travers de scripts dans un langage propre à Terraform, on va décrire l'état de l'infrastructure souhaité. Son workflow le rend facile à comprendre et à mettre en oeuvre :

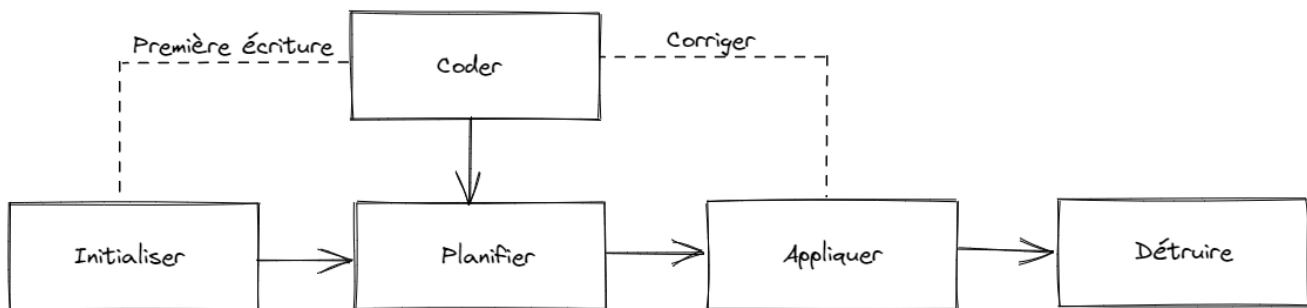


Figure 6.1: Workflow de Terraform

Après les quelques première écritures de configuration, on va :

- Initialiser le projet avec un nouvel état. Commande : `terraform init.`
- Planifier les configurations. Commande : `terraform plan.`
- Appliquer les configurations. Commande: `terraform apply.`
- Détruire les configurations si nécessaire. Commande : `terraform destroy`

L'étape d'initialisation permet la création d'un état de l'infrastructure qui sera stocké sous la forme d'un fichier `terraform.tfstate`. Cet état permet d'assurer la cohérence entre ce qui est écrit localement et ce qui a déjà été appliqué. Dans un travail collaboratif, cette état peut être configuré sur GitLab de façon à assurer la cohérence des états entre différents développeurs.

Terraform se base sur un fonctionnement autour de "Provider" ou fournisseurs. Un provider est là pour manager une ressource donnée. Ces provider sont nombreux : Amazon Web Services, Google Cloud Platform, Azure, VmWare Vsphere, Proxmox etc.

A ces providers on spécifie des ressources. Chaque bloc de ressources décrit un ou plusieurs objets d'un service. La construction d'une ressource est basé sur le provider qui la fournit.

Il est également possible de créer des modules afin de les réutiliser. Utile par exemple dans le cas de template de machines virtuelles, où les variables sont toujours les mêmes mais où seuls les valeurs changent.

Chez Empreinte Digitale, Terraform permet le déploiement dans un premier de temps de machines virtuelles qemu sur des cluster Proxmox. Par la suite, Terraform permet d'installer des composants sur ces machines telles que des ressources Kubernetes, MongoDB, Helm, etc.

6.3 Ansible

Nous avons vu précédemment l'intérêt de Terraform dans l'installation de machine de machines virtuelles ou logicielle à partir de différents fournisseurs. Une fois cette étapes effectuée, il peut être nécessaire d'effectuer des configuration supplémentaires. C'est à cette étapes qu'Ansible intervient.

Ansible est un logiciel libre de gestion des configurations qui automatise le déploiement de configurations sur un ensemble de machines. Celui-ci est basé sur l'utilisation du protocole SSH. Cela lui donne l'avantage considérable de ne pas avoir besoin d'installer d'agents sur les machines, parfois consommateur de ressources.



Au travers de scripts généralement en YAML, on décrit l'état souhaité d'une ou plusieurs ressources pour une ou plusieurs machines. Ces scripts vont alors exécuter des modules sur les cibles qui essaieront d'appliquer des correctifs afin d'atteindre cet état souhaité. On distingue trois principaux types de scripts :

- Les **rôles**. Ce sont un ensemble de playbooks qui s'assurent de la présence ou absence de fonctionnalité spécifique.
- Les **playbooks**. Ce sont un ensemble de tâches d'automatisations.
- Les **tâches**. Une tâche correspond à la description de l'état souhaité d'un composant d'un machine. Cela peut être exemple la présence ou non d'un paquet apt.

L'utilisation de rôle n'est pas toujours nécessaire. Un rôle à surtout pour vocation de créer une configuration qui sera réutilisée régulièrement. Il donc possible de se limiter à l'utilisation de playbook.

Comme indiqué précédemment, Ansible est dit "agentless". Cela signifie qu'il n'est pas nécessaire d'installer d'agents sur les cibles. Pour réaliser sa mission, Ansible n'a donc besoin que 3 de pré-requis :

- Une connexion SSH vers ces cibles.
- La bonne version de python d'installé sur ces cibles.
- Un inventaire de l'ensemble des cibles.

Lorsqu'un script Ansible est exécuté, la première étape consiste toujours à récupérer les "facts". Ces "facts" sont l'ensemble des informations de la machine cible. On aura le nom de la machine, sa version de système d'exploitation, son numéro de version, etc.

A partir de ces informations, nous allons être en mesure de paramétrer l'utilisation d'Ansible. Cela va notamment permettre de faire une distinction entre les différents systèmes d'exploitation, leurs versions, leurs logiciels installés etc.

Lorsqu'une task Ansible est jouée, il y a 4 états principaux :

OK : la configuration était déjà correcte, Ansible n'a rien changé.

SKIPPED : les conditions d'application de la tâche ne sont pas validées. La tâche est ignorée.

CHANGED : la configuration n'était pas correcte, Ansible a apporté les changements nécessaires.

ERROR : la configuration ne s'est pas bien passé, Ansible renvoie l'erreur associée.

Dans le cadre de l'exploitation du système d'information d'Empreinte Digitale, Ansible permet d'automatiser certaines tâches d'installation et de configuration sur plus de 700 machines virtuelles. Grâce à un bastion SSH ayant accès à l'ensemble des machines, il suffit d'exécuter les scripts Ansible en passant par celui-ci. Cela représente un gain de temps considérable pour l'ensemble de l'équipe sysadmin.

7 Travaux de sécurité

7.1 Période d'alternance

Comme dit précédemment, j'ai réalisé mon stage dans le cadre d'un contrat de professionnalisation. Globalement, mon sujet **Analyse et réalisation d'audits automatisés de l'infrastructure** s'est découpé en 4 phases pendant la période d'alternance :

1. **Analyse abstraite et bonnes pratiques.** Durant cette phases j'ai réalisé une veille technologique sur les logiciels et outils utilisés par les Sysadmins. De plus, j'ai pris le temps de me cultiver sur les sujets de sécurité avec les documentation et livre blanc de sécurité de l'ANSSI ainsi que les sites de conseils de sécurité sur Internet.
2. **Analyse.** Durant cette phase, j'ai débuté une analyse de l'infrastructure en me basant sur les critères du référentiel secNumCloud de l'ANSSI. L'analyse n'a pas portée que sur l'infrastructure, en effet, parmi les nombreux critères de certification, on va trouver des besoins en documentation, procédure, organisation etc.
3. **Préconisations.** Rédactions de documentations destinées au pôle Sysadmin et à l'ensemble des salariées : livre blanc de sécurité, PSSI (Plan de sécurité des systèmes d'information)
4. **Mise en oeuvre.** Bien qu'aucune solution n'ait été retenue à l'issue de la période d'alternance, j'ai effectué des tests avec Rudder et Ansible CMDB.

A l'issue de mes travaux, j'ai rédigé un PSSI et un tableau de suivi d'audit de l'infrastructure. Les deux documents sont composés de 16 thématiques présentés dans la section suivante.

Organisation de la sécurité de l'information							
PSSI	Titre	Avancement Initial (%)	Action à mener	Action menée	Avancement actuel (%)	Commentaire	État de l'audit
Organisation SSI							
ORG-SSI	Organiser la SSI	100,00 %	Aucune	Aucune	100,00 %		Terminé
ORG-SSI-DOC	Documenter l'organisation de la SSI	0,00 %	Rédaction du document	Aucune	0,00 %		Non débuté
ORG-SSI-ACT	Identifier les acteurs de la SSI	50,00 %	Faire apparaître dans la documentation de l'organisation de la SSI	Aucune	50,00 %		Non débuté
Responsabilité Internes							
ORG-RSSI	Désigner un responsable de la SSI	90,00 %	Faire apparaître dans la documentation de l'organisation de la SSI	Aucune	90,00 %		Non débuté
ORG-SECU-PHY	Désigner un responsable de la sécurité physique	90,00 %	Faire apparaître dans la documentation de l'organisation de la SSI	Aucune	90,00 %		Non débuté
ORG-RGPD	Désigner un responsable RGPD auprès de la CNIL	100,00 %	Aucune	Aucune	100,00 %		Terminé
ORG-RGPD-DATA	Réaliser une analyse d'impact relative à la protection des données	100,00 %	Aucune	Aucune	100,00 %		Terminé
ORG-RESP	Formaliser les responsabilités	50,00 %	Faire le point	Aucune	50,00 %		Non débuté
Responsabilité vis-à-vis des tiers							
ORG-TIERS	Intégrer les clauses SSI dans tout contrat ou convention	0,00 %			0,00 %		Non débuté
ORG-TIERS-LIST	Lister les tiers	50,00 %			50,00 %		Non débuté
ORG-TIERS-RISQ	Etudier les risques inhérents à chaque projet	0,00 %			0,00 %		Non débuté
Application des mesures de sécurité							
ORG-APP-INSTR	Appliquer le PSSI dans l'entité	30,00 %			50,00 %		En progression

Figure 7.1: Extrait du tableau de suivi de sécurité

J'ai ensuite complété ce tableau afin de mettre en avant les points déjà mis en oeuvre au sein d'Empreinte Digitale et ceux qui ne l'était pas.

7.2 16 thématiques de sécurité

Les 16 thématiques contiennent des aspects organisationnels, techniques et documentaires. Voici un résumé de chacune des parties :

1 - Politique de l'information et gestion du risque Il s'agit d'assurer l'utilisation de logiciels stables avec des suivi de correctifs. De la documentation approuvée par la direction doit être rédigée afin d'assurer l'évolution du SI en matière de sécurité.

2 - Organisation de la sécurité de l'information La sécurité de l'information doit être documentée en spécifiant les acteurs principaux sur chacun des domaines : développement applicatif, infrastructure, RGPD etc.

3 - Sécurité des ressources humaines L'exploitation d'un SI passant par ses utilisateurs, ils sont une sources indéniables de faille possible. Les employés doivent être formés à la sécurité du SI et avoir accès en permanence à des documentations rappelant les règles de sécurités à appliquer.

4 - Gestion des actifs Le matériel du personnel ainsi que toutes autres machines sur lesquelles reposent l'exploitation du SI doit être inventorié.

5 - Contrôle d'accès et gestion des identités L'utilisation du SI doit se faire de manière à pouvoir en tout temps identifier l'identité d'une personne l'exploitant. Même si cela peut être contraignant dans l'exploitation, il n'est pas question d'ouvrir les accès à une ressources si la personne n'en a pas besoin. L'ajout, la modification ou la suppression d'un accès quel-qu'il soit doit être documenté et archivé afin d'assurer un suivi.

6 - Cryptologie Des mécanismes cryptographique sécurisés doivent être employés lors de l'utilisation de protocoles tels que TLS, IPsec ou SSH.

7 - Sécurité physique et environnementale La sécurité des logicielles n'est pas suffisante. Un aspect réglementaire oblige le découpage de zone d'accès aux différentes bâtiments. Des mécanismes contre les sinistres tels que des inondations, coupures d'électricité ou incendie doivent permettre la continuité de l'activité.

8 - Sécurité liée à l'exploitation Il a de nombreuses règles lié à l'exploitation. Celles-ci sont généralement liées aux autres sections du PSSI avec une prise en compte par exemple de l'exploitation de données sensibles, l'accès aux ressources informatiques, le nomadisme etc.

9 - Sécurité des communications et réseau Les différents équipements réseaux nécessite des configurations supplémentaires. Cela concerne les différentes réseaux Wifi, Ethernet ainsi que les accès aux ressources distantes. Des mécanismes de surveillance sur le SI doivent permettre la mise en avant d'une activité non-autorisée.

10 - Acquisition, développement et maintenance des systèmes Une des tâches les plus importante et pour autant ardue concerne la maintenance du système existant. Il s'agit de garder les systèmes à des niveaux de sécurité satisfaisant sans impacter son exploitation. Cela nécessite une vision en temps réel de l'état de l'infrastructure.

11 - Relations avec les tiers L'ouverture d'accès aux tiers sur des ressources du SI nécessite des procédures et documentations engageant la responsabilité des tiers en cas de faille. Il est nécessaire de maintenir un listing des tiers et des ressources auxquels ils sont accès.

12 - Gestion des incidents liés à la sécurité de l'information De la documentation doit permettre l'évaluation rapide du niveau de criticité d'un incident. Cette même documentation doit ensuite établir les acteurs à contacter : RSSI, DG, client etc.

13 - Continuité d'activité Le Plan de Continuité d'Activité (PCA), et le Plan de Reprise d'Activité (PRA) doivent prendre en comptes différents cas de figures afin d'assurer un maintien de l'activité en cas de sinistre.

14 - Conformité L'aspect conformité impose d'être en mesure d'assurer l'harmonisation des systèmes entre ce qui est prévu et effectif.

15 - Poste de travail Le développement du télé-travail nécessite de porter une attention particulière aux personnes en distanciel. Leurs ordinateurs sont à configurer en conséquence.

16 - Exigences supplémentaires Les certifications imposent des aspects supplémentaire tels que la mise en oeuvre de convention de service avec les clients, l'obligation de stockage sur le territoire Européens etc.

7.3 Inventaire des machines

7.3.1 Description

Dans le cadre de la 4^{ème} thématique portant sur la gestion des actifs, il est nécessaire de tenir un inventaire des ressources informatiques. Cela comprend l'ensemble des ordinateurs du personnel, les machines physiques liées aux différents datacenters ainsi que les machines virtuelles qu'elles hébergent. La solution retenue pour répondre à ce besoin est d'utiliser 2 logiciels open-source :

1. **Open Computers and Software Inventory (OCSInventory)** une solution open-source de gestion technique de parc informatique. Ce logiciel libre permet l'inventaire hardware et software. On va ainsi inventorier des machines avec leurs caractéristiques matérielles et les logiciels qui y sont installés.
2. **Gestionnaire Libre de Parc Informatique (GLPI)** est une solution open-source de gestion de parc informatique qui permet la classification des différentes ressources.

Concrètement, OcsInventory va être en charge de récupérer l'ensemble des informations des machines tandis que GLPI lui va les classer. Par le biais d'un paramètre appelé TAG configuré dans OcsInventory, j'ai créé le classement suivant :

- **ANG-ORD** : les ordinateurs de l'ensemble du personnel à Angers.
- **ANG-DC** : les machines physiques et virtuelles qui se trouvent sur le site d'Angers.
- **REN** : les machines physiques et virtuelles qui se trouvent sur le site de Rennes.
- **TRS** : les machines physiques et virtuelles qui se trouvent sur le site de Tours.

7.3.2 Architecture

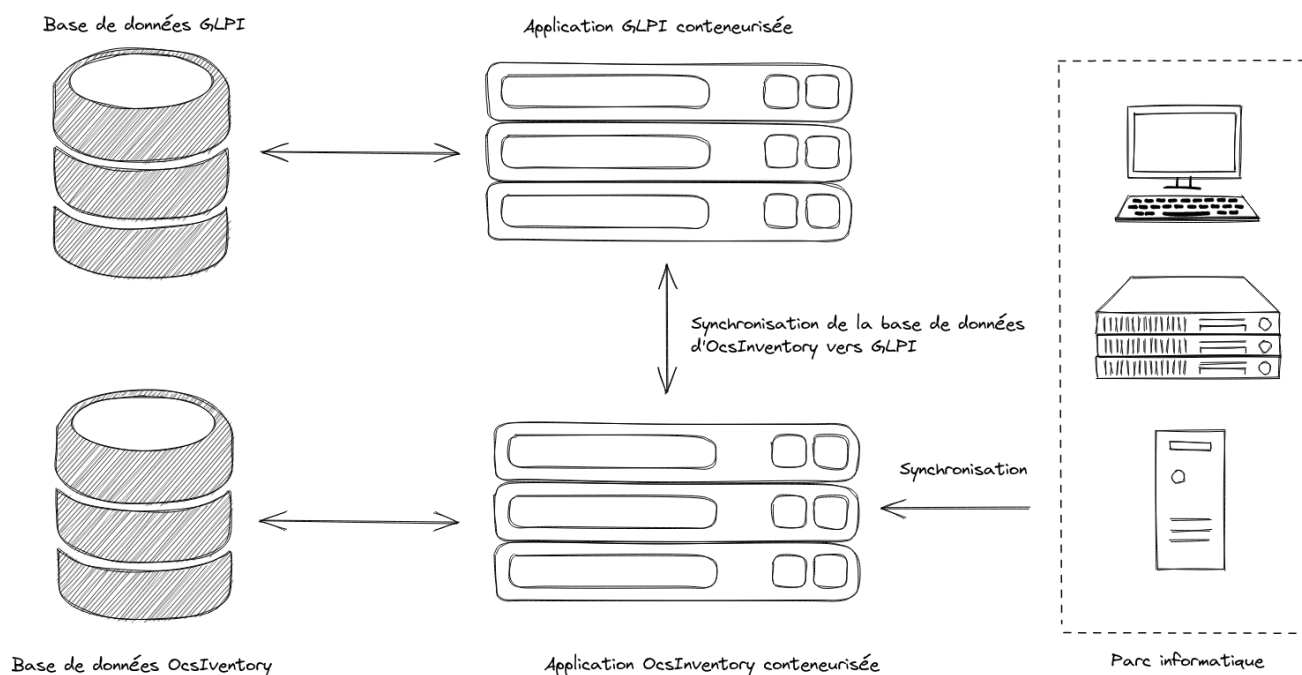


Figure 7.2: Architecture entre OcsInventory et GLPI

7.3.3 Principe de fonctionnement

L'application OCSInventory fonctionne sur un système d'agent. C'est-à-dire qu'un agent est installé sur l'ensemble des machines, et celui-ci va par la suite envoyer des rapports au format XML quotidiennement via le protocole HTTP au serveur maître.

Ensuite, l'application GLPI avec un plugin dédié à l'import des données d'OCSInventory va se connecter à l'application OCSInventory et lire les données dans un premier. Ensuite, par une action manuelle à réaliser dans GLPI, je valide les imports en vérifiant que les règles soient bien appliquées. Une fois l'import fait, je peux dans GLPI visualiser les machines avec les TAGs associés. Lorsqu'un import est validé, GLPI écrit dans une base de données qui lui ait propre les informations.

Une autre architecture aurait été possible en utilisant FusionInventory à la place d'OCSInventory. L'avantage de fusion est qu'il ne possède pas sa propre base de données. Une fois les données récupérées, il les inscrit directement dans la base de données de GLPI. Cette solution n'a pas été retenue car un serveur OCSInventory était déjà utilisé.

7.3.4 Ajout d'un plugin

Par défaut, OcsInventory ne possède pas de plugin permettant d'inventorier les vhosts. Les vhosts sont les noms des sites webs hébergés sur une machine. Afin de répondre à ce besoin interne, j'ai repris le travail d'un collègue avec l'écriture d'un script perl permettant d'inventorier les vhosts des serveurs web Nginx, les vhosts des conteneurs Docker et le nom des clients pour chacun des sites. Le nom des sites ayant une structure comprenant à la fois le service et le

nom du client, il est possible de faire du traitement afin de créer et d'écrire dans une nouvelles tables 2 colonnes, une pour le vhost et l'autre pour le client.

7.3.5 Installation avec Ansible

Bastion SSH L'une des problématiques du projet est d'installer les agents sur chacune des machines du SI. Cela représente environ 700 machines virtuelles. Heureusement, l'accès aux différentes machines passe par un Bastion SSH. Cela fonctionne par un contrôle d'accès basé sur les rôles (RBAC). Le rôle sysadmin dont je fais partie donne les droits sur toutes les machines. Les accès SSH étant fonctionnels, j'ai utilisé Ansible.

Inventaire Ansible se base sur des fichiers d'inventaire dans lequel on décrit le nom des machines dans différents niveaux de catégories. La première chose que j'ai fais est de mettre à jours l'inventaire. En effet, la différence de nombre de machines entre le Bastion SSH et l'inventaire Ansible mettait en avant qu'il en manquait au niveau d'Ansible. J'ai alors fais une comparaison entre le listing du Bastion et celui d'Ansible pour en ressortir les machines manquantes.

Ensuite j'ai repris la structure de l'inventaire. Parmi les différents groupes de l'inventaire, il y a 3 groupes permettant de distinguer les machines se trouvant sur Angers, Rennes et Tours. Cependant, après avoir visualisé l'inventaire sous forme d'arborescence avec la commande `ansible-inventory --graph`, j'ai remarqué qu'il y avait des petites erreurs. J'ai corrigé ces erreurs petit à petit en me basant sur la représentation de l'inventaire sous forme de graphique.

Rôle Ansible Un rôle est découpé de la manière suivante :

```
|-- ocsinventory-agent
|   |-- /default           # Variables par défaut
|   |-- /files             # Fichiers supplémentaires
|   |-- /meta              # Nécessaire à l'utilisation d'Ansible Galaxy
|   |-- /tasks             # Ensemble des playbooks
|   |-- /vars              # Fichier de variables supplémentaires
```

- Default : contient les variables pour le TAG, le nom des paquets, etc.
- Files : contient les scripts supplémentaire d'installation du plugin.
- Meta : enregistrement du créateur du rôle.
- Tasks : ensemble des tâches Ansibles.
- Vars : variables supplémentaires s'il est nécessaire de modifier les valeurs pas défaut.

Le diagramme de séquence ci-dessous met en lumière de façon simplifié les différentes tâches Ansible. On considère que l'ensemble des tâches se sont déroulés sans erreurs. On considère 3 acteurs :

- Utilisateur : personne qui exécute le script
- Ansible : machine exécutant les scripts de configuration Ansible.
- Cible : machine configuré par Ansible.

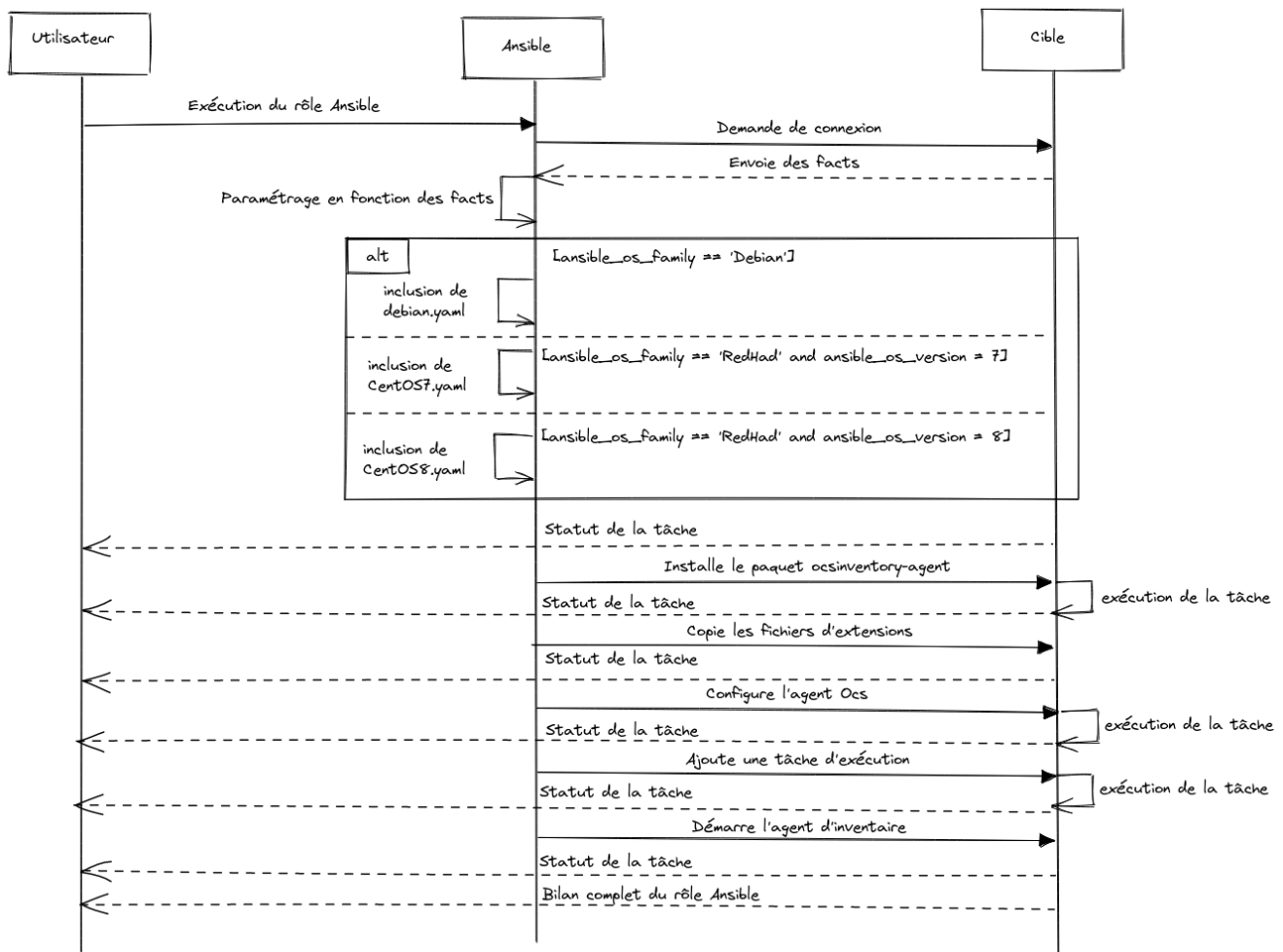


Figure 7.3: Diagramme de séquence de l'installation d'OCSInventory avec Ansible

Pour les ordinateurs des salariés, j'ai rédigé une documentation décrivant comment installer et configurer l'agent OCSInventory sur Windows, Linux et ArchLinux.

7.3.6 Bilan

L'installation sur les machines accessibles via le réseau d'Angers est terminée. L'ensemble des salariés ont également installé l'agent. L'agent est installé sur la majorité des machines du datacenter de Rennes. L'agent est installé sur les machines de Tours. Cependant, le réseau d'Angers et Tours n'étant pas encore relié à la date de ces installations, les agents ne peuvent pas joindre le serveur OCSInventory.

7.4 Durcissement Linux

7.4.1 Objectif

Dans le cadre de la 8^{ème} thématique portant sur la sécurité liée à l'exploitation, il est nécessaire d'effectuer un durcissement des systèmes Linux à l'installation d'une nouvelle machine. En effet, une nouvelle machine installée à partir de l'image d'origine de la distribution n'est pas suffisamment sécurisée.

7.4.2 Openscap

OpenSCAP représente à la fois une bibliothèque et un outil de ligne de commande qui peuvent être utilisés pour analyser et évaluer chaque composant de la norme SCAP. L'outil de ligne de commande, appelé oscap, offre un outil polyvalent conçu pour formater le contenu en documents ou analyser le système en fonction de ce contenu. L'outil en ligne de commande permet de :

1. Effectuer un scan d'une machine et de générer un rapport en HTML à la volé
2. De générer à partir d'un rapport, un ensemble de tâches Ansible pour effectuer des correctifs
3. D'appliquer les correctifs et générer un nouveau rapport en HTML

7.4.3 Création de machines virtuelles de test

Avant de procéder à l'installation et l'exécution d'Openscap sur l'ensemble des machines, il est nécessaire de le tester. En effet, l'outil effectuant de nombreuses modifications à la volé, il faut d'abord éprouver la solution afin de s'assurer qu'elle n'entraîne pas de modifications handicapant pour l'exploitation. Ainsi, afin d'avoir un panel assez large pour effectuer des tests, j'ai créé sur le Proxmox d'Angers 6 machines virtuelles :

- Debian 10, 32 Gb stockage, 2 Gb Ram
- Debian 11, 32 Gb stockage, 2 Gb Ram
- Ubuntu 20.04, 32 Gb stockage, 2 Gb Ram
- Fedora 36, 32 Gb stockage, 2 Gb Ram
- Centos 7, 32 Gb stockage, 2 Gb Ram
- Centos 8, 32 Gb stockage, 2 Gb Ram

7.4.4 Création d'une archive Debian

Le paquet openscap ne se trouve pas dans les listes des sources apt de Debian 11. Afin de résoudre ce problème, il fallu créer une archive Debian à partir des sources officiels de l'application.

7.4.5 Mise en oeuvre

A nouveau, c'est avec Ansible que la configuration d'Openscap est faite. Cette fois-ci, les scripts Ansible doivent prendre en compte la différence entre les distributions et leurs versions. Le diagramme de séquence suivant décrit le processus d'installation. Afin de le simplifier, la différenciation entre distribution et version n'est pas représentée.

On considère 3 acteurs :

- Utilisateur : personne qui exécute le script
- Ansible : machine exécutant les scripts de configuration Ansible.
- Cible : machine configuré par Ansible.

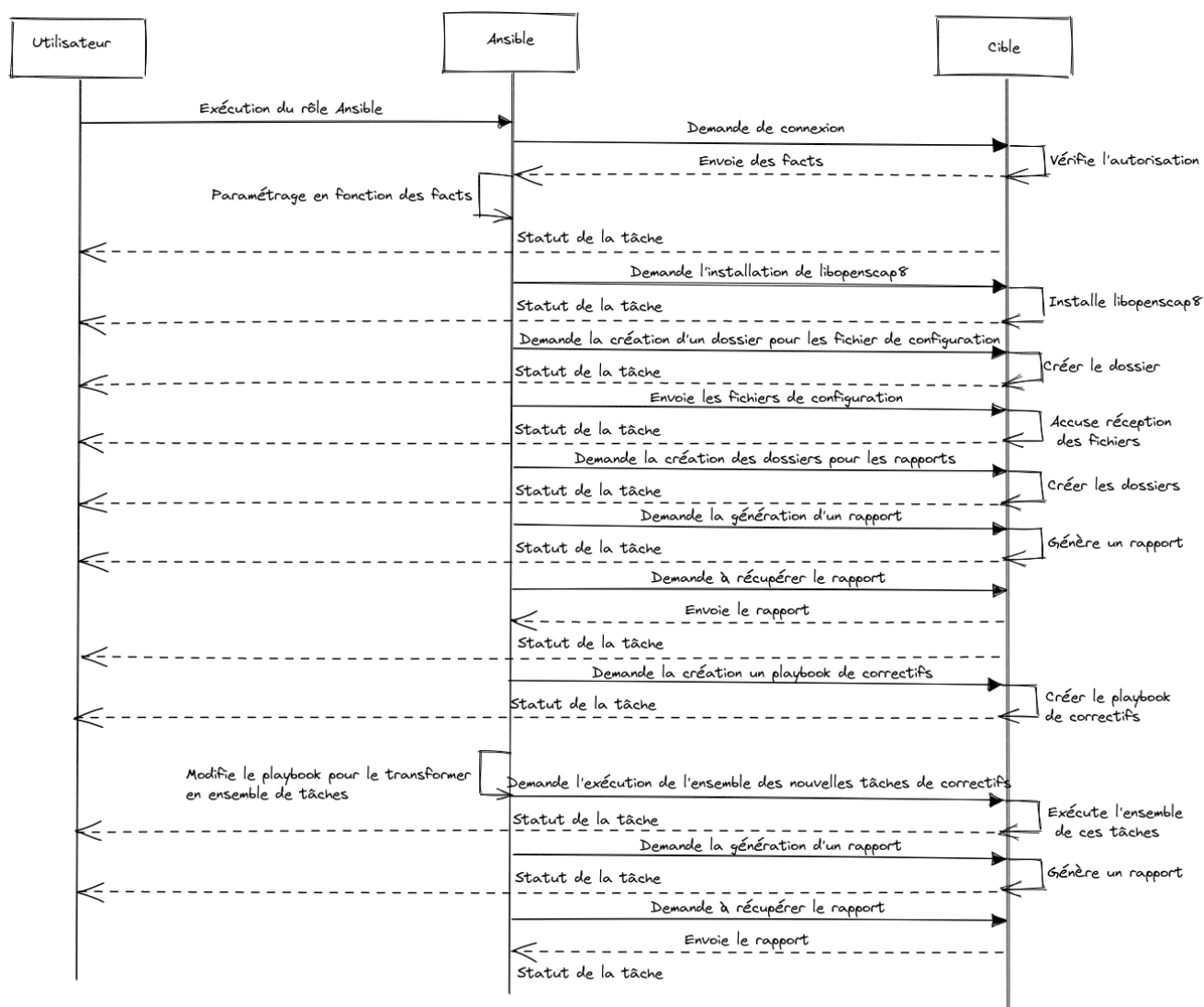


Figure 7.4: Diagramme de séquence du fonctionnement d'Ansible avec OpenSCAP

7.4.6 Bilan

Au moment de la rédaction de ce rapport, l'installation et l'exécution d'Openscap n'a pas été réalisée sur l'ensemble des machines. Cependant l'ensemble des tests en fonction des distributions est fonctionnel. La volumétrie en temps sur ce projet est :

7.5 Documentation

7.5.1 Objectif

Dans plusieurs des thématiques portant sur la sécurité, un aspect documentaire est mis en avant. Il s'agit d'avoir des documents descriptifs de l'infrastructure, de procédures et processus liés à l'exploitation ou de documents juridiques sur les engagements qui doivent être mis en oeuvre entre employeur et salariés, mais aussi clients et prestataire. L'objectif est d'avancer sur les documentations manquantes et d'établir un fonctionnement afin d'en assurer la pérennité.

7.5.2 Documents

Lors de l'alternance j'ai travaillé sur la Politique de Sécurité des Systèmes d'Information (PSSI) ainsi que sur la charte informatique. Durant la période de stage, j'ai travaillé sur la reprise de la documentation interne du datacenter afin de rédiger surtout les procédures, politiques et processus déjà mis en oeuvre mais dont il manquait l'aspect documentaire. De plus, suite à la demande d'un client, j'ai rédigé un Plan d'Assurance Sécurité (PSA) spécifiant les devoirs entre prestataires et clients au niveau de l'exploitation des services installés par Empreinte Digitale.

7.5.3 Outils

La documentation à destination des clients et prestataire est rédigée soit sur le Google Drive soit sur le Nextcloud de l'entreprise. Quant aux documentations internes au Sysadmin ou à l'ensemble des salariés, celles-ci sont rédigés sur un Wiki.js, une application open-source hébergée en interne. Cette application permet de rédiger des documents en markdown depuis une interface web.



7.5.4 Bilan

Il reste encore de nombreuses documentation à rédiger et notamment de la documentation qui nécessite la mise en place de révision annuelle. Bilan en temps :

7.6 Autres pistes d'étude

Les outils présentés précédemment ont été mis en application sur l'ensemble du système d'information. Cependant, d'autres essais ont été fait.

Durant la période de d'alternance, j'ai fais des essais avec Ansible CMDB. Cette solution bien que non retenue pourrait être reconsidérer. Son aspect ne nécessitant qu'une connexion SSH permet de gérer la totalité du parc, contrairement à d'autres comme OcsInventory qui posait des problèmes liés au réseau.

J'ai également testé Rudder durant l'alternance. Techniquement, la solution est intéressante mais possède un coût important.

Wazuh une plate-forme gratuite et opensource de sécurité basé sur un fonctionnement d'agent était également intéressante. Celle-ci permet de réaliser du monitoring de sécurité ainsi que de l'application de correctifs. Reposant sur Elasticsearch et Kinana, l'interface web paramétrable permet une excellente vision de l'ensemble du SI en temps réel. Néanmoins, le fonctionnement par agent est contraignant et la configuration uniquement via des fichiers XML rend le travail fastidieux.

Enfin, OpenVas un outils opensource de scan de vulnérabilités de site WEB permet de générer des rapports sur un nombre illimité de sites. Je ne suis pas aller très loin dans l'expérimentation avec mais elle mériterait de passer plus de temps d'expérimentation.

7.7 Bilan

8 Travaux d'administrateur système

8.1 Nextcloud et Collabora

Nextcloud est une application web libre d'hébergement de fichiers et une plateforme de collaboration. Associé à Collabora, une suite bureautique, il est possible d'intégrer dans Nextcloud l'édition de fichiers en tout genre de façon Collaborative. Cette suite logiciel est finalement une alternative libre et open-source à l'utilisation d'outils tels que Google Drive ou OneDrive.



8.1.1 Objectif

Empreinte Digitale installe et héberge régulièrement des instances Nextcloud et Collabora. L'objectif est de simplifier et automatiser au mieux les installations mais également de faciliter les mises à jours.

Pour répondre à ces besoins, 4 outils sont utilisés :

- **GitLab** pour stocker l'ensemble des ressources nécessaires à l'installation.
- **Ansible** pour exécuter différentes tâches.
- **Ansible Tower/AWX** pour gérer depuis une interface graphique l'application des tâches Ansible et assurer un maintien dans le temps.
- et **Jinja** couplé à Ansible pour permettre de générer les fichiers de configurations avec les bonnes variables en se basant sur des templates.

8.1.2 Schéma applicatif

8.1.3 Description

L'application repose sur des conteneurs Docker hébergés sur une machine virtuelle, elle-même dans un cluster Promox. On compte 5 composants :

- **Nextcloud** notre application principale associée à un serveur web apache dans un unique conteneur.
- **Collabora** l'application supplémentaire pour l'édition de texte.
- **Traefik** le reverse proxy qui va exposer les sites web `collabora.cloud-ed.fr` et `nextcloud.cloud-ed.fr`. C'est également au niveau de Traefik que sont gérés les certificats HTTPS.
- Une base de donnée **PostgreSQL** pour l'applicatif.
- Un cache applicatif **Redis**.

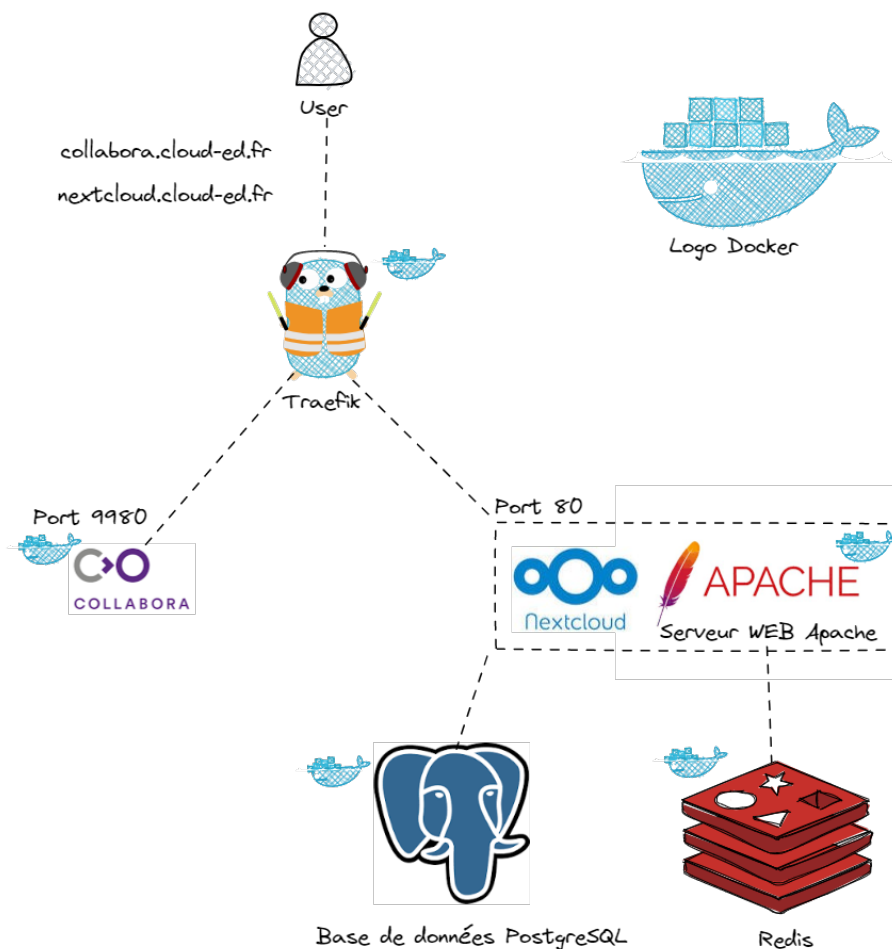


Figure 8.1: Schéma applicatif de Nextcloud avec Collabora

8.1.4 Utilisation des variables

Automatiser aux mieux l'installation revient à créer un "Template" d'installation, n'utilisant que des variables. On distingue 2 types de variables :

- **Les variables d'environnements.** Celles-ci vont décrire le nom du client, la version de Nextcloud à installer, les images Docker à utiliser etc. Ce sont les variables qui n'ont pas besoin d'être secrètes.
- **Les secrets.** Ce sont d'autres variables obligatoires sauf qu'elles sont sensibles et donc à protéger. C'est le cas notamment des identifiants et mots de passes des services.

Les variables sont utilisées à 3 endroits différents :

- Dans les fichiers `docker-compose`, qui prennent leurs valeurs dans le fichier `.env`.
- Dans le fichier `.env`, qui est généré depuis Ansible avec un template Jinja.
- Dans le template Jinja, qui prend ses valeurs dans l'inventaire AWX et également dans le coffre-fort Ansible.

La personne qui réalise l'installation doit spécifier les variables dans l'inventary AWX et dans le coffre-fort Ansible.

Finalement, à partir d'un template Jinja et d'Ansible, on génère un fichier `.env` que l'on place dans le dossier de l'application Nextcloud afin qu'il soit utilisé par les scripts docker-compose.

8.1.5 Inventaire Ansible

Le paramétrage des variables pour le rôle et le vault est la première étape. Ensuite, il faut mettre à jours l'inventaire Ansible du rôle. Dans le dépôt GitLab dans lequel se trouve le playbook générique, un dossier `group_vars` permet de distinguer les différentes vaults. Par exemple :

```
|-- group_vars
|   |-- aicla                # Vault du client aicla
|   |   |-- vault.yaml
|   |-- ed                  # Vault du client ed
|   |   |-- vault.yaml
```

Pour appliquer correctement le vault pour aicla et ed, il faut créer un groupe dans l'inventaire Ansible portant le même nom. Le fichier `host` contient :

```
[aicla]
aicla-cloud-1 ansible_host=192.168.X.X

[test]
an-nextcloud-test ansible_host=192.168.X.X
```

Il faut comprendre que le groupe `aicla` possède une machine nommée `aicla-cloud-1` dont l'adresse IP est `192.168.X.X`. Ce groupe possède des variables de groupe, d'où le nom `group_vars`, spécifié dans le fichier `group_vars/vault.yaml`.

8.1.6 Utilisation d'AWX

Une fois l'inventaire et les variables mis à jour, il faut paramétrer AWX. Tout se fait par le biais d'une interface web comme ci-dessous :

Dans AWX, j'ai créé un projet Nextcloud. Dans ce projet, je fais appel à une source Git qui est mon dépôt GitLab avec le nom de la branche et les identifiants à utiliser. Le principe est que ce projet n'est pas à être changer.

Ensuite je créer un Template, utilisant mon projet Nextcloud et d'autres ressources. Les ressources supplémentaires à créer sont :

1. Inventaires : variables d'environnement.
2. Script d'inventaire : nom de la machine et son adresse IP.
3. Informations d'identification : accès au dépôt GitLab et mot de passe du Vault Ansible.
4. Modèles : spécifier l'utilisation des éléments précédemment créé, c'est-à-dire l'inventary, l'host, les credentials et le projet Nextcloud.

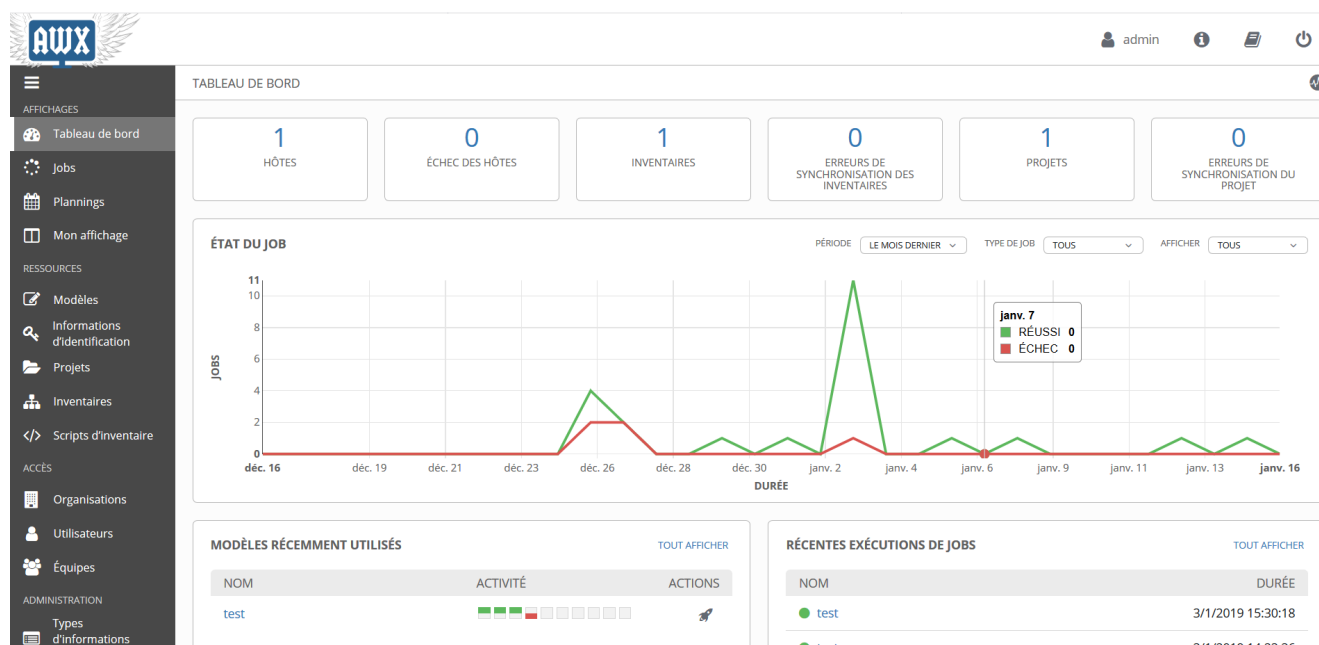


Figure 8.2: Interface web d'AWX

8.1.7 Rôle Ansible

Le schéma ci-dessous décrit les actions réalisées par le rôle Ansible appelé par Ansible AWX. Celui-ci ne fait pas apparaître les différentes tâches liées aux dépendances tels que l'installation du module `pip` pour Python.

8.1.8 Conclusion

Lorsqu'une personne souhaite installer une nouvelle instance, il lui suffit de télécharger le dépôt GitLab et éditer la partie inventaire et vault puis de push ses modifications. Ensuite, dans Ansible AWX, il ajoute les ressources dont un inventaire, un script d'inventaire, deux informations d'identification et un modèle. Enfin, il exécute le modèles, ce qui lance l'installation de l'application.

Dans le cadre d'une installation, il aurait été possible de se limiter à la partie avec les fichiers `docker-compose`, sans se servir d'AWX. Cependant, AWX est particulièrement intéressant dans le maintien à jours des différentes instances. En effet, depuis AWX, en allant sur le projet `nextcloud`, on peut y visualiser l'ensemble des ressources liées.

Cela fait donc office de listing de l'ensemble des instances `nextcloud` installé. Si la version d'un composant de `nextcloud` évolue, il suffit alors de modifier l'inventaire de chacun des modèles. Ajouté à cela, on assure une installation homogène du produit. Dans le cas d'astreinte, on sait où trouver les ressources de l'application directement et ceux peu importe le Nextcloud sur lequel il faut intervenir.

De plus, il arrive souvent de laisser le fichier `.env` directement sur la machine, ce qui est à éviter. Avec l'installation actuelle, le fichier `.env` est généré, utilisé puis supprimé. Pour l'administration, l'ensemble des sysadmins enregistrent les mots de passes des vaults dans

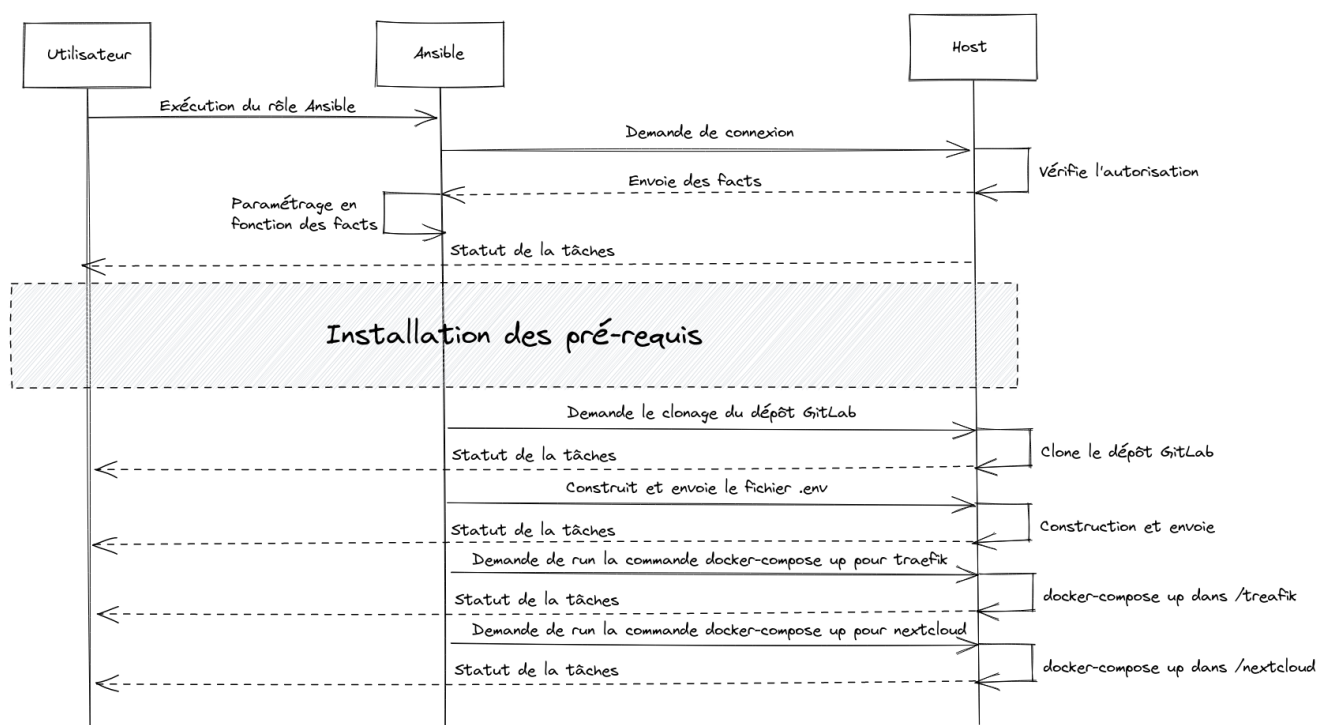


Figure 8.3: Diagramme de séquences des tâches Ansible lors de l'installation de Nextcloud

l'application Bitwarden, ce qui leurs permet dans tous les cas de récupérer les accès à une base de données par exemple.

8.2 Proxmox

8.2.1 Rappel

Proxmox est une plate-forme open-source complète pour la virtualisation d'entreprise. Grâce à l'interface Web intégrée, nous pouvons facilement gérer les machines virtuelles et les conteneurs, le stockage défini par logiciel, la mise en réseau, le clustering haute disponibilité et plusieurs outils prêts à l'emploi sur une seule solution.



8.2.2 Objectif

Les datacenters de Rennes et Tours utilisent une plate-forme de virtualisation nommé Proxmox. L'objectif est de mettre en oeuvre la même plate-forme de virtualisation à Angers pour que celle-ci puisse servir principalement à des tests. Pour cela, 3 serveurs sont disponibles afin de faire un cluster à 3 noeuds.

8.2.3 Matériel

Dans un premier temps, j'ai ajouté une carte fibre 10G pour ajouter une interface supplémentaire au serveur. Cette interface est destinée à faire transiter du trafic réseau ayant besoin de plus de débit qu'une simple interface 1G. L'interface 1G quant à elle sert à l'administration du serveur. Dans un second temps, j'ai racké les serveurs dans une baie. Cela revient à positionner les différents serveurs dans des tiroirs fixés. Enfin, j'ai formaté l'ensemble des disques durs. Dans chacun serveur, un disque est réservé à l'installation du système d'exploitation et les autres servent au stockage des machines virtuelles.

8.2.4 Logiciel

Image Le système d'exploitation de Proxmox s'installe à partir d'un fichier ISO. Celui-ci est basé sur une image Debian. J'ai installé une version Proxmox VE 7.0 basé sur l'image Debian 11 nommé Bullseye à partir d'un disque dur externe IODD directement bootable. Cela permet de ne pas avoir à créer une clé Bootable dédiée à cela.

Réseau Depuis l'interface graphique, j'ai configuré la partie DNS sur le DNS interne et changé l'adresse IP sur un réseau en 192.168.22.0/23. Le DHCP interne attribue par défaut des adresses sur le réseau 192.168.23.0/22.

Une fois cette étape terminée, les interfaces web de Proxmox sont disponibles à l'adresse IP configurée. Sur le DNS interne j'ai créé 3 enregistrements pour avoir les noms de domaines an-virt-pmx-1, an-virt-pmx-2 et an-virt-pmx-3 pour chacun des noeuds.

Regroupement en cluster Depuis l'interface graphique, dans la section cluster, j'ai créé un cluster en lui donnant un nom et un réseau. Il se nomme an-virt-pmx. Ensuite, afin d'ajouter

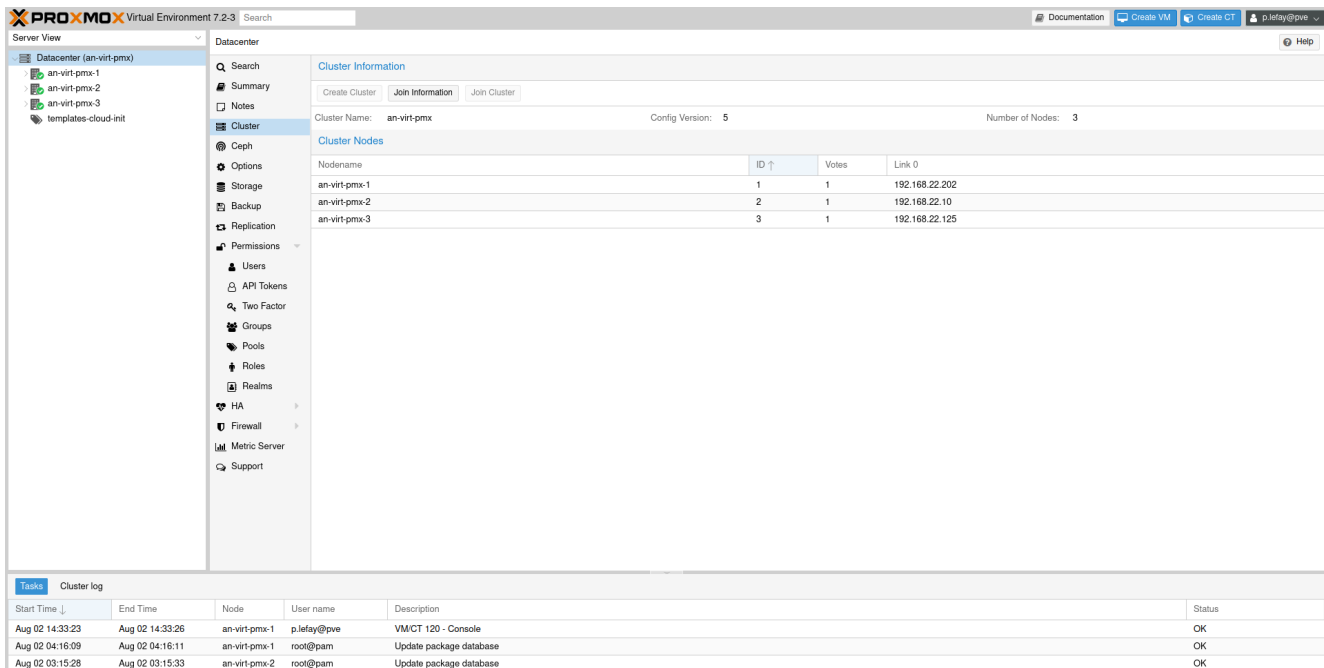


Figure 8.4: Interface du cluster Proxmox an-virt-pmx

les 2 noeuds restant, j'ai récupéré le token d'identification du cluster, puis je me suis connecté sur chacun des noeuds. Sur chacun d'entre-eux, j'ai spécifié :

- L'adresse IP du cluster, soit l'adresse IP d'an-virt-pmx-1.
- Le token d'identification.

A partir de cette étape, depuis l'interface graphique de n'importe quel noeud Proxmox, l'ensemble des noeuds sont visibles et accessibles.

OSDS et manager

Stockage J'ai créé un stockage CephFS afin d'y déposer l'ensemble des ISO qui pourraient être utiles. On y trouve différentes images pour Ubuntu, Debian, Fedora, CentOS et RockyLinux.

8.3 Projet Dehon

8.3.1 Objectif

Le groupe Dehon met en oeuvre un dispositif permettant la détection de fuite sur les installations frigorifiques. Un Détecteur de Niveau Intelligent (DNI) est donc installé sur chacune des installations frigorifique afin de détecter les fuites par méthodes de mesures indirectes. Chaque DNI est également connecté au système de l'entreprise et les données sont remontées sur une plate-forme centralisée et consultable via un portail web.

Une évolution des réglementation impose aux détenteurs d'installations frigorifiques de justifier d'un contrôle continu de leurs installations et de pouvoir présenter l'ensemble des vérifications ainsi que les opérations d'entretien effectuées.

L'objectif est donc de mettre en place une plateforme cloud pour centraliser l'exploitation de l'ensemble des DNI et proposer une offre de service complète de suivi et d'expertise en temps réel des installations frigorifiques.

J'ai travailler à la réalisation de cette infrastructure avec 2 autres administrateurs systèmes.

8.3.2 Installation matériel

Pour des raisons de disponibilité, l'infrastructure du projet se trouve sur 3 sites :

- **virt2** : Proxmox de Tours à Cyrès sur lequel se trouve un premier cluster Kubernetes.
- **cogent** : Proxmox de Tours à Cogent sur lequel se trouve un répliqua du premier cluster de virt2.
- **virt1** : Proxmox de Rennes sur lequel se trouve un arbiter MongoDB.

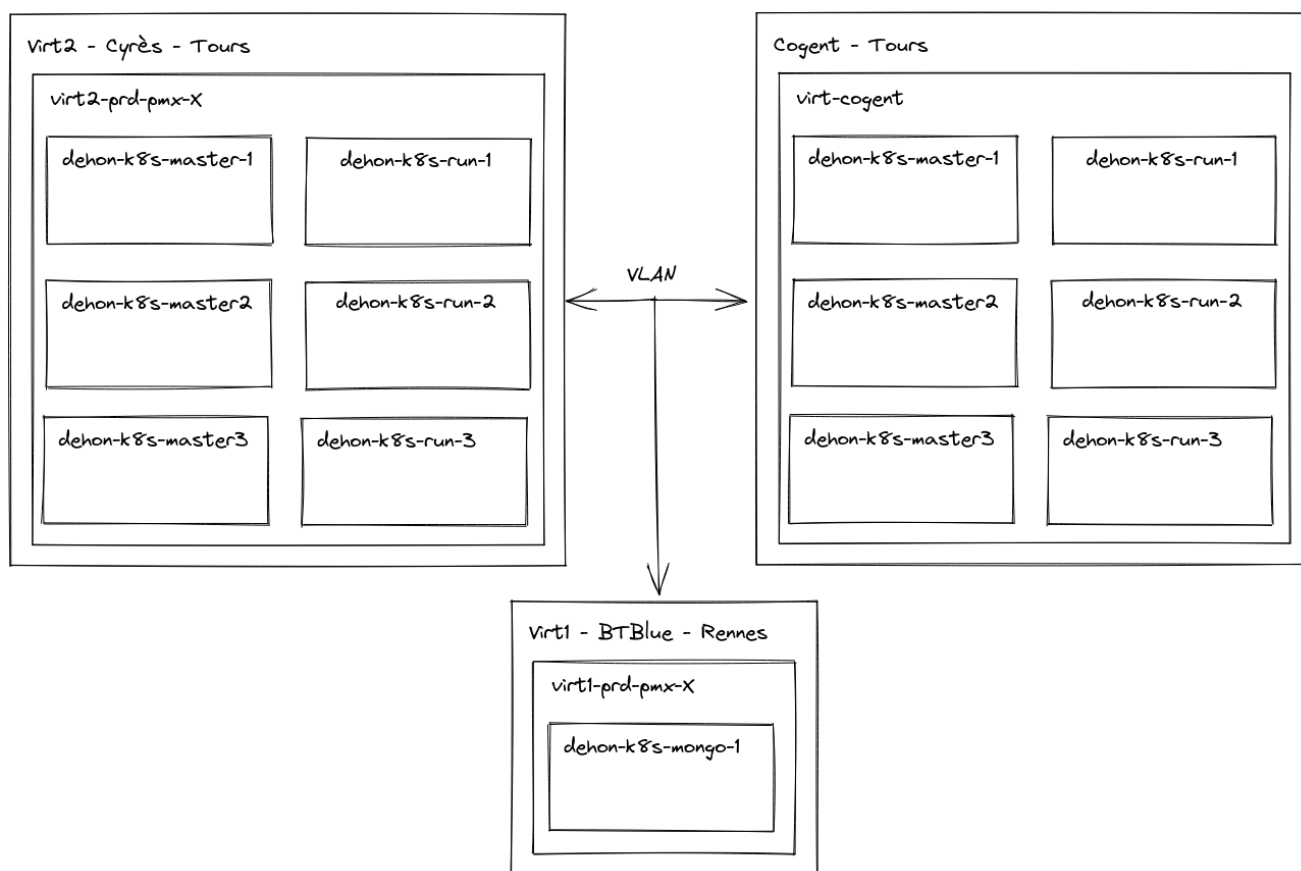


Figure 8.5: Infrastructure sur 3 sites physique du projet Dehon

En voici un schéma :

Les serveurs étaient déjà mis en place pour virt1 et virt2. Il a cependant fallu aller sur Tours chez cogent pour y installer une machine. Cette machine contient un unique cluster proxmox. Il a ensuite fallu relier les centres de Cogent et Cyrès. La distance entre les 2 bâtiments est d'environ 2 km. Une fibre noir, soit une fibre optique par encore activée à préalablement était installé par le personnel de Cyrès.

8.3.3 Création des cluster de machines physiques avec proxmox et terraform

Nous avons commencé par développer l'infrastructure sur virt2. Nous nous sommes servis de terraform pour deployer les machines virtuelles sur le cluster. Nous avons donc 9 machines :

- 3 machines virtuelles destinée a etre les masters. Dans le conception de kubernetes, ces machines vont etre les cerveaux du cluster. c'est sur ces machines que des composant de kuberne vont permettre l'orchestration de runner.
- 3 machines virtuelle destinée a etre les workers. ces 3 machines vont etre celles qui supportent la charge de travail dans le cluster.
- 2 machines virtuelle en tant que proxy. Elles seront le point d'entree de l'infrastructure.

- 1 machines virtuelle pour le stockage. L'ensemble du cluster utilisera un stockage partagé.

la denomination de ces machines est réfléchi afin d'identifier le client, le role et le nombre de chaque composant. Ces noms sont visibles sur le schema de l'infrastructure.

Avec Terragorm on declare dans un premier un format de machines virtuelle dans lequel on va attribuer des valeurs communes. Cela est dans notre cas par exemple le numero de vlan, le nom du client, les clés SSH a autorisées etc. La configurassions est par la suite appliquée a un template cloud_init deja present sur les clusters.

Ensuite, on declare des modules specifique. par exemple, etant donne que les master sont identiques et au nombre de 3, on va declarer que l'on souhaite 3 machines master, que chacune aura 50 Gb de Ram, 4 CPU etc.

une fois les fichiers de configuration terminé, on initialiser terraform pour lui specifier son etat, ses providers

Ensuite, on lance une "planification". c'est a dire que l'on va lancer la commande "terraform plan"

8.3.4 Installation du clusters Kubernetes via Kubespray

8.3.5 Configuration de proxy avec vip

8.3.6 IngressController, Certmanager, namespace, rancher rke

8.3.7 Stockage

8.3.8 Mongo Arbiter

8.4 Actualisation et mise en oeuvre de la procédure d'arrivée

8.4.1 Objectif

Formaliser le besoin afin de rendre l'arrivée d'une nouvelle personne plus fluide et simple

8.4.2 Description

8.4.3 Documentation

8.4.4 Groupe de Travail Embarquement

8.5 Bilan

9 Bilan personnel

10 Annexes

10.1 CV



COMPÉTENCES

Java	★★★★★
NodeJS	★★★★★
VueJS	★★★★★
Python	★★★★★
-	
Pack Office	★★★★★
Electronique	★★★★★
-	
Gestion de Projet	★★★★★
Gestion financière	★★★★★
Travail en équipe	★★★★★

CONTACT

06 73 46 44 03

18 rue Auguste Blandeau,

paullefoy@reseau.eseo.fr

www.linkedin.com/in/Paul-Lefay

LANGUES

✓ Anglais: B1
TOEIC: 870 / 990

✓ Espagnol : Débutant

Paul Lefay

Etudiant en 4^{ème} année à l'ESEO

En recherche d'une alternance dans le domaine de l'ingénierie réseau ou du développement WEB pour septembre 2021.

Formations

ESEO ANGERS
 Septembre 2016 - Actuellement
 Formation d'ingénieur généraliste avec spécialisation
 Etudiant en 1^{ère} année du cycle ingénieur (Bac+3).
 Formation en informatique, électronique et infrastructure et

LYCÉE DAVID D'ANGERS
 Septembre 2013 - Juillet 2016
 Baccalauréat scientifique
 Spécialisation Physique-Chimie

Expériences Professionnelles

STAGE TECHNIQUE ESEO START
 Septembre 2020 - Novembre 2020
 Stage de 3 mois dans l'incubateur de l'ESEO ANGERS.
 Développement d'une application WEB de compatibilité pour les associations étudiantes

STAGE DE PROFESSIONNALISATION
 Juillet 2017 - Août 2017
 Stage d'une durée d'un mois à la Caisse Primaire d'Assurance Maladie dans les services Logistique et Comptabilité

TENNIS ST LEONARD - ANGERS
 Juillet 2014
 Encadrement de 20 jeunes lors d'un stage de tennis.
 Organisation de tournois de tennis pour des jeunes de moins de 18 ans

VIE ASSOCIATIVE
BDE AVESEO - Mandat 2018-2019
 Membre du Bureau Des Etudiants dans le module logistique. Gestion d'une cafétéria, d'un local ainsi que de la location d'un camion

BDE ESEOKAMI - Mandat 2019-2020
 Membre du Bureau Des Etudiants en tant que Trésorier
 Gestion d'un budget de 150 000 euros
 Gestion financière d'événements tels que la Blue Moon, la plus grande soirée étudiante du grand Ouest

Centres d'intérêts

Culture Japonaise

Vie associative de l'école

Actualité cinématographique

Tennis

Musique

10.2 Planning détaillé de la période d'alternance

10.3 Planning détaillé de la période de stage

10.4 Bibliographie

10.5 Liste des figures

5.1	Schéma de la gouvernance chez Empreinte Digitale	11
5.2	Application web réalisé par Empreinte Digitale pour le Design4Green	12
5.3	Maquette 3D du datacenter de Stratosfair	13
6.1	Workflow de Terraform	18
7.1	Extrait du tableau de suivi de sécurité	21
7.2	Architecture entre OcsInventory et GLPI	25
7.3	Diagramme de séquence de l'installation d'OCSInventory avec Ansible	28
7.4	Diagramme de séquence du fonctionnement d'Ansible avec OpenSCAP	31
8.1	Schéma applicatif de Nextcloud avec Collabora	36
8.2	Interface web d'AWX	38
8.3	Diagramme de séquences des tâches Ansible lors de l'installation de Nextcloud .	39
8.4	Interface du cluster Proxmox an-virt-pmx	41
8.5	Infrastructure sur 3 sites physique du projet Dehon	43

10.6 Liste des tables

1	Planning du travail effectué sur la période de d'alternance - Partie 1	55
2	Planning du travail effectué sur la période de d'alternance - Partie 2	56
3	Planning du travail effectué sur la période de stage - Partie 1	57
4	Planning du travail effectué sur la période de stage - Partie 2	58
5	Planning du travail effectué sur la période de stage - Partie 3	59
6	Planning du travail effectué sur la période de stage - Partie 4	60

10.7 Acronymes et définition

L'ensemble des acronymes et définition du glossaires proviennent de Wikipédia.

N°	Semaine	Description
36	06/09/21 - 12/09/21	Découverte de l'entreprise et ses locaux. Sensibilisation à l'accessibilité numérique et formation à la RGPD. Début de recherches documentaires basées sur les documentations de l'ANSSI.
37	13/09/21 - 19/09/21	Pas de jours en entreprise cette semaine.
38	20/09/21 - 26/09/21	Poursuite des recherches documentaires. Rendez-vous de mise au point sur l'ensemble de l'infrastructure technique du SI. Veille technologique sur les technologies/logiciels inconnues.
39	27/09/21 - 03/10/21	Mise en place d'un compte sur YesWeHack. Poursuite de la veille technologique. Ouverture des accès aux machines physiques et virtuelles.
40	04/10/21 - 10/10/21	Réunion avec le responsable le DPO pour identifier les besoins de sécurité liés à la RGPD. POC sur le logiciel Rudder pour de la conformité d'infrastructure.
41	11/10/21 - 17/10/21	Ajout d'un agent et paramétrage de tests sur divers thématiques. Réalisation d'un tableau d'audit pour l'ensemble des points mis en avant par la documentation de l'ANSSI.
42	18/10/21 - 24/10/21	Pas de séance de PFE cette semaine.
43	25/10/21 - 31/10/21	Poursuite de l'audit de l'état actuel de l'infrastructure à partir du tableau d'audit. Ajout d'onglets plus spécifiques pour chacune des 15 sections du tableau.
44	01/11/21 - 07/11/21	Semaine complète excepté pour le lundi férié. Amélioration du tableau d'audit et poursuite de celle-ci. Veille sur les recommandations de l'ANSSI pour les protocoles IPsec, TLS et SSH. Rédaction du livre blanc de sécurité.
45	08/11/21 - 14/11/21	Séance de PFE le vendredi mais congés posé ce jours là pour le pont avec le jeudi.
46	15/11/21 - 21/11/21	Début de la POC Ansible CMDB dans le but d'auditer les paquets et leurs versions.
47	22/11/21 - 28/11/21	Poursuite des travaux sur Ansible CMDB. Travaux sur la configuration de bornes Wifi. Annulation des travaux pour cause de mauvaises configurations de ma part. Visite médical et réunion de mi-avancement le vendredi.
48	29/11/21 - 05/12/21	Fin des travaux sur Ansible CMDB et début de la rédaction du PSSI.
49	06/12/21 - 12/12/21	Avancement sur le POC Ansible. Mise en place de règles basées sur les facts. Mise au propre du compte rendu et établissement des éléments pouvant être audité en lien avec le tableau d'audit.

Table 1: Planning du travail effectué sur la période de d'alternance - Partie 1

50	13/12/21 - 19/11/21	Avancement le PSSI. Réunion de présentation final de la POC Ansible CMDB. Nouvelle POC plus poussé sur Rudder pour reproduire une conformité similaire à la POC Ansible CMDB.
51	20/12/21 - 26/12/21	Semaine complète en entreprise excepté le vendredi pour congé de Noël. Avancement sur le PSSI. Présentation bilan moral et financier de l'entreprise sur l'année 2020. Vision sur les objectifs de 2022. Premier ticket client réalisé.
52	27/12/21 - 02/01/22	Congé pour fermeture de l'entreprise en cette période de Noël.
1	03/01/22 - 09/01/2022	Poursuite des travaux sur la reprise du PSSI pour le faire correspondre au tableau de suivi d'audit. Intervention et découverte du datacenter de Rennes.
2	10/01/22 - 16/02/22	Avancement sur le PSSI, démonstration à un collégien du travail d'administrateur système avec l'installation d'un LAMP. Préparation de la soutenance de fin de PFE.
3	17/01/22 - 23/01/22	Soutenance de PFE. Pas de journées en entreprise.
4	24/01/22 - 30/01/22	Pas de journées en entreprise.

Table 2: Planning du travail effectué sur la période de d'alternance - Partie 2

N°	Semaine	Description
5	31/01/22 - 06/01/22	Début de la période de stage. Révision des documents précédemment réalisés. Installation sur d'Openvas. Déplacement physique d'un serveur, fixation de l'IP, ajout au DNS. Rattachement d'un nouveau noeud Proxmox à un Cluster. Migration de Proxmox 6.4 à 7.11.1. Migration de Debian 10 (Buster) à Debian 11 (Bullseyes).
6	07/02/22 - 13/02/22	Ajout de Ceph au nouveau Cluster Proxmox. Compréhension du fonctionnement de Ceph. Poursuite de la mise à jours du tableau d'audit. Installation de DeepFence, Framemo, Log4j-RCA-SCANNER. Début de l'installation de GLPI. Remplacement d'un disque défectueux avec remise en route du RAID1.
7	14/02/22 - 20/02/22	Poursuite de l'installation de GLPI. Ajout du Plugin OCSInventoryRE à GLPI. Installation du service OCSInventory. Liaison entre le Plugin et le serveur OCSInventory. Configuration du Plugin. Début de l'ajout de machines de test. Ticket client pour des configurations d'un Moodle. Pour suite de la rédaction du rapport en \LaTeX . Finalisation de la documentation de GLPI.
8	21/02/22 - 27/02/22	Résolution du problème du manque de toutes les informations des machines. Installation dual boot pour un nouveau développeur, création compte LDAP, mail, Mattermost. Test de l'ajout d'agent Windows avec label paramétré. Configurations des dictionnaires. Accompagnement sur une demi-journée d'un stagiaire en 3ème, accompagnement sur l'installation d'un système d'exploitation, d'une pile LAMP et quelques exercices pratique d'HTML et PHP
9	28/02/22 - 06/03/22	Installation d'un serveur de CVE. Ajout de l'import des logiciels à GLPI. Configuration d' OCSInventory pour prendre en compte les rapports de CVE. Configuration de l'ordinateur pour un développeur. Mise en place d'un scan SNMP rattaché à GLPI et OCSInventory. Installation de NocoDB avec sauvegarde SQL de la base de données de Redmine. Reprise de la documentation technique liée aux Datacenter.
10	07/03/22 - 13/03/22	Configuration du serveur OCSInventory en HTTPS avec un certificat auto-signé pour pouvoir effectuer des scans SNMP à partir d'agent spécifique. Modifications du comportement de l'agent vers HTTPS avec activation SSL. Poursuite des travaux sur la documentation technique et rédaction du rapport de stage. Maintenance d'un ordinateur qui ne boot plus : changements depuis un disque externe pour revenir sur un ancien noyau Linux mais problème lié au driver graphique.
Paul LEFAY		Installation d'une carte d'extension 10G sur un noeud Proxmox. Installation d'un LimeSurvey de test en conteneur pour un client. Installation d'un noeud Proxmox puis début de

N°	Semaine	Description
12	21/03/22 - 27/03/22	Préparation de la documentation nécessaire à l'audit de sécurité. Réinstallation de l'ensemble des noeuds Proxmox suite à l'ensemble du Cluster qui est tombé après mon installation du 3ème noeud. Restauration à partir des Backups des machines perdus. Diverses installations pour l'audit de sécurité : Matomo, Bitwarden, Nextcloud, Mattermost, Redmine. Ajout de configuration dans un Proxy Traefik déjà existant.
13	28/03/28 - 03/04/22	Fin des installations pour l'audit de sécurité avec l'installation de Passhport. Lancement de l'installation des agents OCSInventory sur l'ensemble des ordinateurs du personnel. Test de l'application Wazuh pour du monitoring de sécurité. Préparation de l'environnement local pour l'exécution de scripts Ansible en production. Correction du script Ansible pour la prise en compte des différences entre CentOS 7 et 8, avec spécification pour Rocky Linux, Alma etc. Ajout de l'agent OCSInventory sur toutes les machines du datacenter d'Angers.
14	04/04/22 - 10/04/22	Fin de l'installation des agents OCSInventory pour les machines du datacenter d'Angers. Début de l'installation des agents pour le datacenter de Tours. Poursuite des travaux sur la documentation. Installation pour un client d'un Nextcloud/Collabora pour un client sur le datacenter de Rennes via Docker-compose.
15	11/04/22 - 17/04/22	Ajout de l'agent OCSInventory sur toutes les machines du datacenters de Rennes. Installation et configuration de Wazuh pour réaliser un audit automatisés de l'infrastructure.
16	18/04/22 - 24/04/22	Intervention au datacenter pour le changement d'un serveur. Poursuite des travaux sur la documentation. Poursuite des travaux avec Wazuh. Installation d'un Cluster Kubernetes à 2 noeuds pour pouvoir y faire de la veille technologique. Mise en place du stockage du Cluster Kubernetes. Préparation d'un ordinateur pour un nouvel employé.
17	25/04/22 - 01/05/22	Poursuite de la veille sur Kubernetes. Début des travaux pour auditer les ressources des datacenters. L'idée est d'avoir un outil permettant de contrôler que ce qui est vendu au client est bien respecté en matière de ressources.
18	02/05/22 - 08/05/22	Mise à jour de l'inventaire Ansible qui avait des défauts dans sa constructions. Modifications de différents problèmes empêchant l'installation des agents OCSInventory. Installation d'une nouvelle instance d'un site internet pour réaliser des Webinaire.
		Mise à jours de l'une des instances de Webinaire.
Paul LEFAY		Modification des scripts Perl/Bash pour récupérer les Vhosts des machines que ce soit pour des vhosts hébergés sous Docker/Nginx ou Apache. Mise en place d'une plate-forme

N°	Semaine	Description
21	23/05/22 - 29/05/22	Poursuite de la ré-exécution des Playbook Ansible d'installation d'agent OCSInventory afin de mettre à jours l'ensemble des Vhosts. Poursuite des mise à jours des instances BigBlueButton. Congé le lundi 23, jeudi 26 et vendredi 27.
22	30/05/22 - 05/06/22	Fin de la ré-exécution des Playbook Ansible d'installation d'agent OCSInventory. Recherche d'une solution sans agent pour faire un état des lieux en matières de sécurité des différentes machines et automatiser la mise en oeuvre de correctif. Les tests s'appliquent à OpenSCAP. Rédaction d'un Plan d'Assurance de Sécurité dans le cadre d'une demande d'un client. Poursuite des travaux sur la documentation du datacenter.
23	06/06/22 - 12/06/22	Installation d'une nouvelle instance Framemo, sur un nom de domaine publique. Poursuite des travaux sur OpenSCAP. Réunion de lancement pour un projet d'infrastructure pour Dehon. Début des travaux sur le projet Dehon avec Terraform pour la création des machines virtuelles.
24	13/06/22 - 19/06/22	Création des machines virtuelles pour le projet Dehon. Création du Cluster Kubernetes avec Calico en CNI sur les 6 précédentes machines virtuelles avec Kubespray. Installation d'un ordinateur portable pour un nouvel arrivant. Poursuite des travaux sur OpenSCAP.
25	20/06/22 - 26/06/22	Poursuite des travaux sur OpenSCAP. Rédaction d'une documentation utilisateur sur la configuration de l'agenda Nextcloud sur téléphone. Début de recherches pour la mise en place d'un outil de scan du réseau. Rédaction du rapport de stage. Intervention aux datacenters de Tours et Cogent. Ticket client pour la configuration d'un agenda Nextcloud.
26	27/06/22 - 03/07/22	Recherche et intervention pour planifiée pour les travaux sur Nextcloud. Poursuite des travaux sur Dehon avec le lancement des 2 Haproxy avec vip. Configuration et test des configurations Haproxy. Mise en place sur Dehon des IngressController, CertManager, Namespaces et Rancher rke.
27	04/07/22 - 10/07/22	Mise en place sur Dehon de Rancher rke. Rédaction de la documentation technique du projet Dehon sur le déploiement de l'ensemble du projet. Journée Team Building au lac de Maine avec présentation du bilan du premier semestre de l'entreprise. Mise en place des environnements/namespaces de prod/qualif/test avec Terraform en passant l'API de Rancher. Installation de la machine de stockage avec Terraform. Particularité devoir ajouter un second disque et donc recréer un module Terraform.

Paul LEFAY

Déploiement de la machine Mongo-Architer sur Rennes.
 Configuration du service Mongo via Terraform pour une application sous Docker. Installation via Terraform de 3

Promotion Maitre d'Année 2022

N°	Semaine	Description
30	25/07/22 - 31/07/22	Installation d'un Nextcloud pour l'association AICLA. Automatisation de l'installation des instances Nextcloud via Docker-compose, Ansible, AWX et Terraform.
31	01/08/22 - 07/08/22	Configuration d'un stockage CephFS sur le Proxmox d'Angers. Accompagnement d'un client dans la configuration de son Nextcloud.

Table 6: Planning du travail effectué sur la période de stage - Partie 4