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

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.

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 compare 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 connaissance sur le sujet, ce qui fait qu'à ce jour, je suis automome sur l'utilisation des outils Ansible et AWX.

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

Table des matières

Introduction

Mon sujet de stage S10 porte sur la mise en place de nouveaux outils de sécurité 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 11 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 la sécurité de l'infrastructure. 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 LaTeXà partir du template de M Woodward. Les liens internet, les liens vers des sections ou des acronymes et définition sont interractifs. Les ressources sont disponibles sur le dépôt GitHub `https://github.com/theprobleme/stagereportS10`.

Abstract

1 L'environnement et le contexte du stage

1.1 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 débuté 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.

1.2 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.

empreinte digitale
Créateur de vos SOLUTIONS NUMÉRIQUES RESPONSABLES

1.2.1 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.

Ligeo archives

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.

1.2.2 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.

Empreinte Digitale à commencé sa transition en SCOP à partir de 2018 pour officiellement le devenir en janvier 2020.

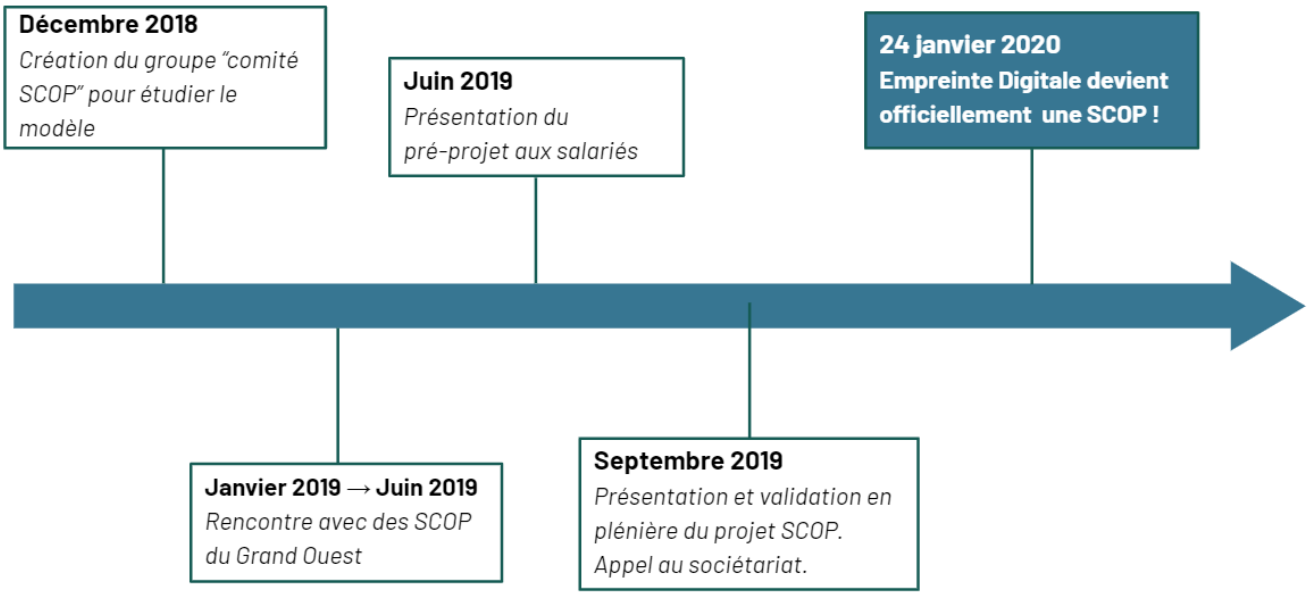


Figure 1.1: Les étapes du passage en SCOP d'Empreinte Digitale

La gouvernance se découpe de la manière suivante :

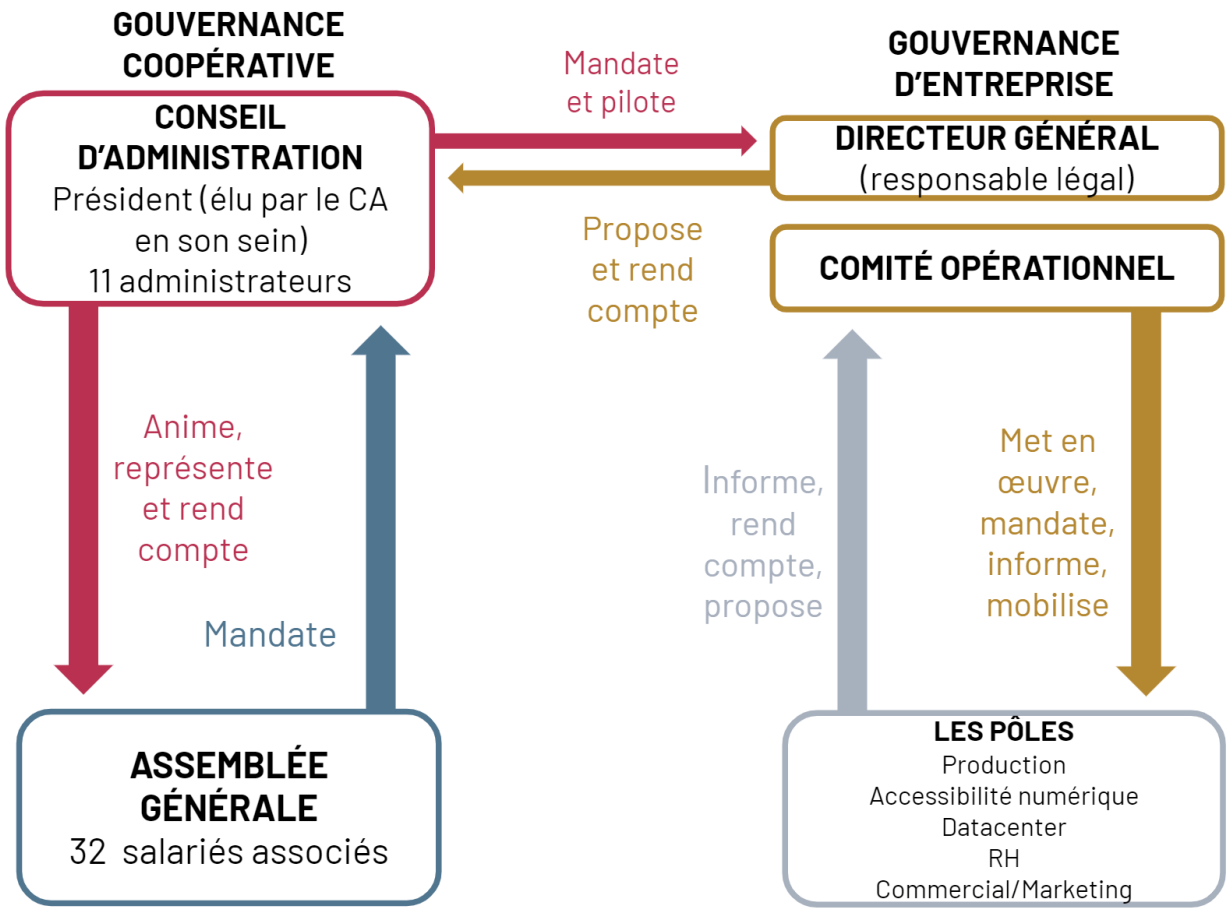


Figure 1.2: Schéma de la gouvernance chez Empreinte Digitale

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.

1.2.3 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.

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 depuis 5 par l'ESAIP, une école d'ingénieur Angevine. Durant ce hackathon de 48h, les équipes doivent répondre sur un sujet autour de l'éco-conception. Le sujet porte chaque année sur la réalisation d'un projet web avec l'obligation de limiter 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 Digitale à participé à cette édition et l'a remporté avec une application statique, éco-conçu et accessible. Le site est une "Progressive Web App" (PWA), il est alors téléchargé une seule fois et mise en cache dans le navigateur, ainsi il n'y a pas d'aller-retour avec le serveur.

A la clé de ce challenge, un chèque de 1000€ qui fut par la suite placé dans un autre projet RSE, le budget participatif.

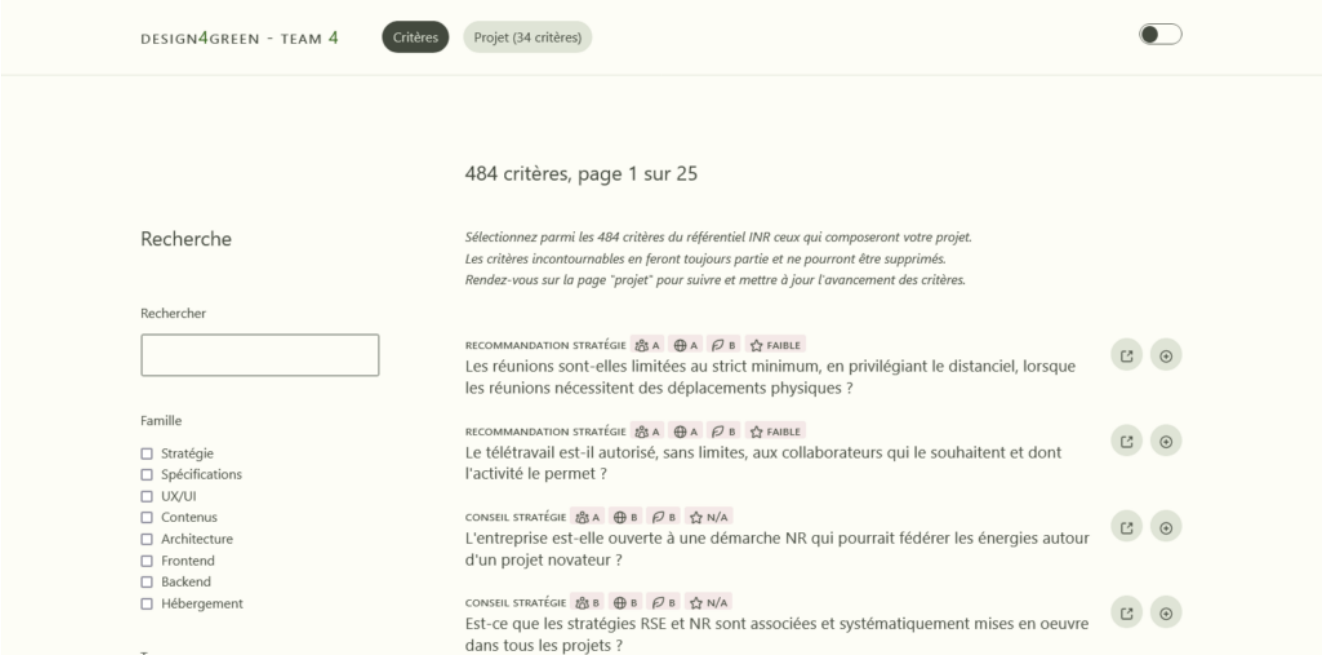


Figure 1.3: Application web réalisé par Empreinte Digitale pour le Design4Green

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. Le prix gagné au Design4Green à été mis en jeu et une participation supplémentaire de 1000€ a été attribué par l'entreprise. Ainsi, c'est 2000€ de projets, proposés par les salariés, qui ont vu le jours. Les proposotions fûrent nombreuses : console de jeu, abri pour oiseaux, salle de sport, jeu de fléchette etc.

Stratosfair En 2020, Empreinte Digitale à lancé un partenariat avec Stratosfair. L'objectif : créer un datacenter responsable. Ce nouveau datacenter à vu le jour deux ans après à Lanester, une ville voisine de Lorient. L'idée est d'utiliser des énergies renouvelables produites sur place, 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.
- Une partie de l'énergie qui alimente les serveurs est une énergie renouvelable générée par des panneaux solaires.
- La chaleur des serveurs est redirigée dans une serre pour la culture de légumes bio.

Figure 1.4: Maquette 3D du datacenter de Stratosfair

Avec ce datacenter, Stratosfair et Empreinte Digitale lancent une offre similaire à celle OVH avec la location de machines virtuelles. Une application et une API ont été développés pour la création de machines virtuelles dans un cluster Proxmox depuis une interface web.

Vous pouvez retrouver d'autres projets RSE ici : `https://blog.empreintedigitale.fr`.

1.2.4 Pôle datacenter

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

J'étais intégré dans le pôle datacenter composé de 7 personnes. Les activités sont découpeés 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.
- **Travaux interne** : deux personnes, moi y compris, travaillons sur divers travaux interne. Cela concerne notamment les besoins de salariés : PC, mail, comptes, accès, nouveaux outils etc.
- **Commercial** : une personne gère la partie commercial et facturation.
- **Chef de projet** : une personne travaille 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.

1.2.5 Comité sécurité

Empreinte Digitale possède un comité sécurité dans lequel j'ai été intégré à mon arrivé. Celui-ci est composé d'une dizaine de personnes aux profils variés : développeurs, administrateurs systèmes, 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. Le pôle a une réunion hebdomadaire pour suivre l'avancement de divers sujets.

1.3 Sujet

1.3.1 Contexte

Empreinte digitale développe son offre DATACENTER. Cela engendre une évolution rapide de l'infrastructure ce 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 spécifier le comportement à avoir lors de l'utilisation du SI ou en cas de faille de sécurité révélée.

1.3.2 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 ?

1.3.3 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, travailler sur des tâches annexes d'administration système comme installer des plateformes pour les clients, préparer le matériel pour les nouveaux arrivants, etc.

1.3.4 Outils et ressources

Les outils sont nombreux et il n'y a pas de restriction à en mettre en oeuvre de nouveaux. Les principaux sont ceux cités dans la section 2.

Il n'y a pas de limitation de ressources et matériels. L'accès aux plateformes vitales à la réalisation des projets est donné avec des droits administrateurs. Pour les autres plateformes, l'accès est donné ponctuellement lorsque cela est nécessaire et justifié.

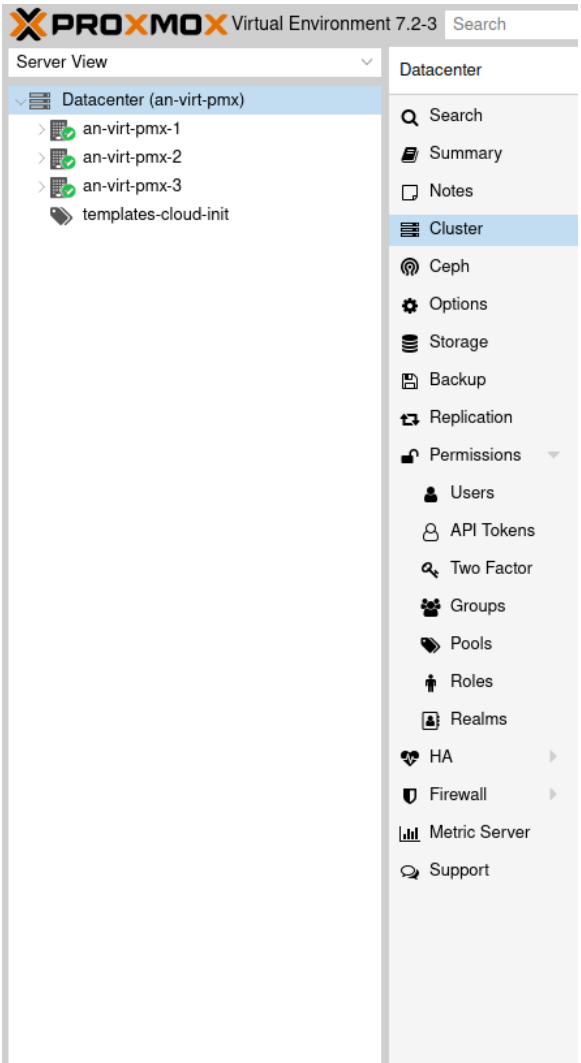
L'objectif n'étant pas concentré sur un sujet en particulier, les divers documentations de l'ANSSI servent de conseil.

2 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.

2.1 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. On peut y modifier les noeuds, les différents stockages, la configuration de backup avec l'ajout de serveur de backup, les permissions utilisateurs, la haute disponibilité du cluster (HA), les statistiques et le support.

Il est également possible d'agir sur les machines virtuelles. La vision sur les machines virtuelles résume son état, ses caractéristiques telles que l'usage du CPU, de la mémoire, la taille du disque et les adresses IPs. On peut y modifier les caractéristiques hardware des machines virtuelles directement à chaud, agir sur le template, accéder à la console de la machine etc.

2.2 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 décrit l'état de l'infrastructure souhaité. Son workflow le rend facile à comprendre et à mettre en oeuvre :

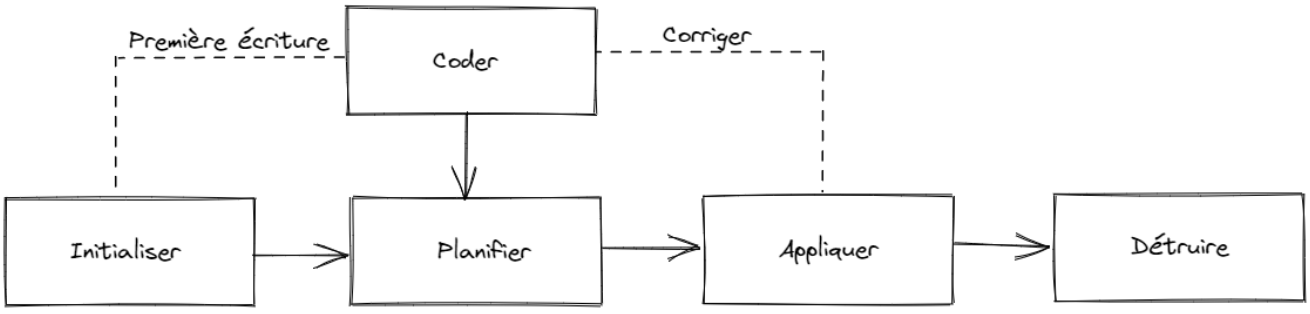


Figure 2.1: Workflow de Terraform

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 *providers* ou fournisseurs. Un provider est là pour manager une ressource donnée. Ces provider sont nombreux : Amazon Web Services, Google Cloud Plateform, 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 fournie.

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 sur des cluster Proxmox. Par la suite, Terraform permet d'installer des composants sur ces machines telles que des ressources Kubernetes, MongoDB, Helm, etc.

2.3 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 là 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 de ne pas avoir besoin d'installer d'agents sur les machines, parfois consommateur de ressources.

Au travers de scripts 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 et 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 on peut 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 à apporté les changements nécessaires avec succès.
- **ERROR** : la configuration ne s'est pas bien passé, Ansible renvoit l'erreur associée.

3 Travaux de sécurité

3.1 Période d'alternance

Mon sujet **Analyse et réalisation d'audits automatisés de l'infrastructure** s'est découpé en 4 phases :

1. **Analyse abstraite et bonnes pratiques**. J'ai réalisé une veille technologique sur les logiciels et outils utilisés par les administrateurs systèmes. De plus, j'ai pris le temps de me cultiver sur les sujets de sécurité avec les documentations et livres blanc de sécurité de l'ANSSI ainsi que les sites de conseils de sécurité sur Internet.

2. **Analyse**. J'ai débuté une analyse de l'infrastructure en me basant sur les critères du référentiel secNumCloud de l'ANSSI. Cette analyse n'était pas uniquement technique car parmi les critères de certification, de nombreux points concernent de la documentation.

3. **Préconisations**. J'ai rédigé des documentations pour le pôle Sysadmin et l'ensemble des salariées : livre blanc de sécurité, PSSI (Plan de sécurité des systèmes d'information), etc.

4. **Mise en oeuvre**. J'ai effectué des POC sur 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 en annexe de ce document aux pages 45 et 46.

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 conventio	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 3.1: Extrait du tableau de suivi de sécurité

J'ai par la suite complété ce tableau afin de mettre en avant les points déjà mis en oeuvre au sein et ceux qui ne l'était pas.

3.2 Inventaire des machines

3.2.1 Description

Dans le cadre de la 4ème 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 au différents datacenters ainsi que les machines virtuelles qu'elles hébergent. La solution retenue est d'utiliser 2 logiciels open-source :

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 matériels et les logiciels qui y sont installés.

Gestionnaire Libre de Parc Informatique (GLPI) est une solution open-source de gestion de parc informatique qui permet la classification des différentes ressources. Ce logiciel libre permet l'inventaire hardware et software. On va ainsi inventorier des machines avec leurs caractéristiques matériels et les logiciels qui y sont installés.

OCSInventory va permettre de récupérer les informations tandis que GLPI va les trier en fonction de règles.

3.2.2 Architecture

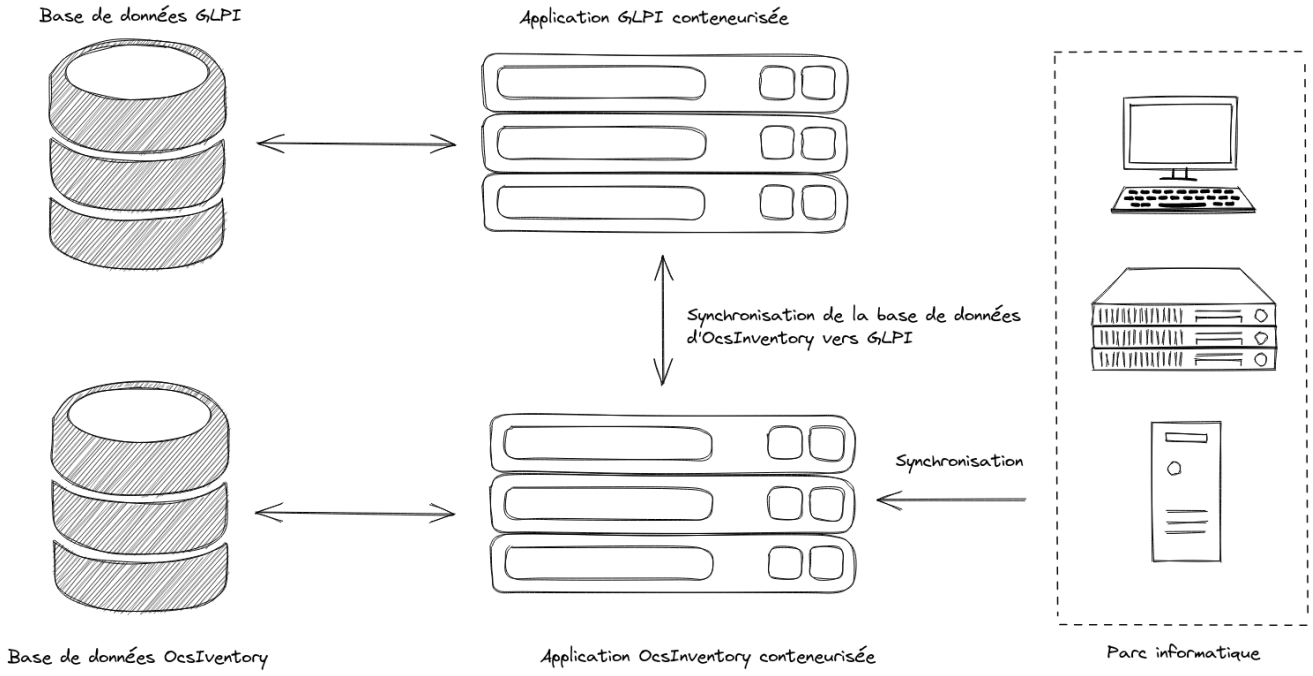


Figure 3.2: Architecture entre OcsInventory et GLPI

3.2.3 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 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. Finalement, par une action manuelle à réaliser dans GLPI, je valide les imports.

L'agent est paramétré avec un champ TAG pouvant être :

- **ANG-ORD** : ordinateurs des salariés d'Angers.
- **ANG-DC** : serveurs physiques et machines virtuelles d'Angers.
- **REN** : serveurs physiques et machines virtuelles de Rennes.
- **TRS** : serveurs physiques et machines virtuelles de Tours.

Une fois l'import fait, je peux dans GLPI visualiser les machines avec les TAGs associés. Le TAG va alors permettre d'effectuer un trie lors de l'import. Par exemple, les machines dont le TAG est *REN* seront placé dans l'entité "Datacenter de Rennes". 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 FusionInventory 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.

3.2.4 Serveur maitre

Le serveur maitre de d'OCSInventory est installé dans un conteneur dans le cluster Proxmox d'Angers. Je n'ai pas eu à installer cette partie, l'application existait déjà.

J'ai installé GLPI avec Docker sur une machine dédié aux conteneurs.

3.2.5 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 et il est intéréssant de pouvoir déterminer sur quelle machine est installé un site. 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, des conteneurs Docker et de les écrires dans la base de données d'OCSInventory. 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 une nouvelle table spécifiquement pour le nom des clients. Cela se fait pas un traitement du même résultat que pour les vhost.

Ce script va dans un premier temps vérifier la présence ou non de la base de données *vhost*. Si celle-ci existe déjà, il ne fait aucune action, sinon il créer la base de données. Ensuite, pour

récupérer les vhosts des serveurs Nginx, les fichiers de configuration présents dans `/etc/nginx/sites-enabled` sont filtrés par une série de commandes Linux. Voici le résultat :

```
grep -EhR 'server_name\\s' $dir |
sed 's/^.*server_name\\s\\+\\(.\\+\\)\\s*;/\\1/' |
sort | uniq |
```

Enfin, pour récupérer les vhosts des conteneur dockers, cela se fait avec la commande docker et jquery (jq). La commande `docker ps` permet de récupérer l'ensemble des identifiants de conteneurs, une boucle va ensuite effectuer un `docker inspect` sur chacun des conteneurs puis la commande `jq` va en sortir le vhost. Cela donne la commande :

```
docker inspect $1 | jq '.[0] |
.Config.Labels | to_entries |
.[] | select(.key | test(".*http.*rule")) |
.value' | sed 's/.*`\(.*\)`.*/\1/' | uniq
```

Merci à Raphaël Poitevin qui avait largement entamé ce travail avant que je le reprenne.

3.2.6 Installation et configuration 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. La machine Passhport permet d'avoir un accès SSH à l'ensemble des machines virtuelles. C'est donc par cette machine que les scripts Ansible seront exécutés.

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 celui-ci, 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`, 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 pour d'Ansible Galaxy
|   |-- /tasks              # Ensemble des playbooks
|   |-- /vars               # Fichier de variables supplémentaires
```

- **Default** : variables pour le TAG, le nom des paquets, etc.
- **Files** : scripts supplémentaire d'installation du plugin.
- **Meta** : enregistrement du créateur du rôle. Ce dossier est nécessaire pour utiliser Ansible-Galaxy.
- **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.

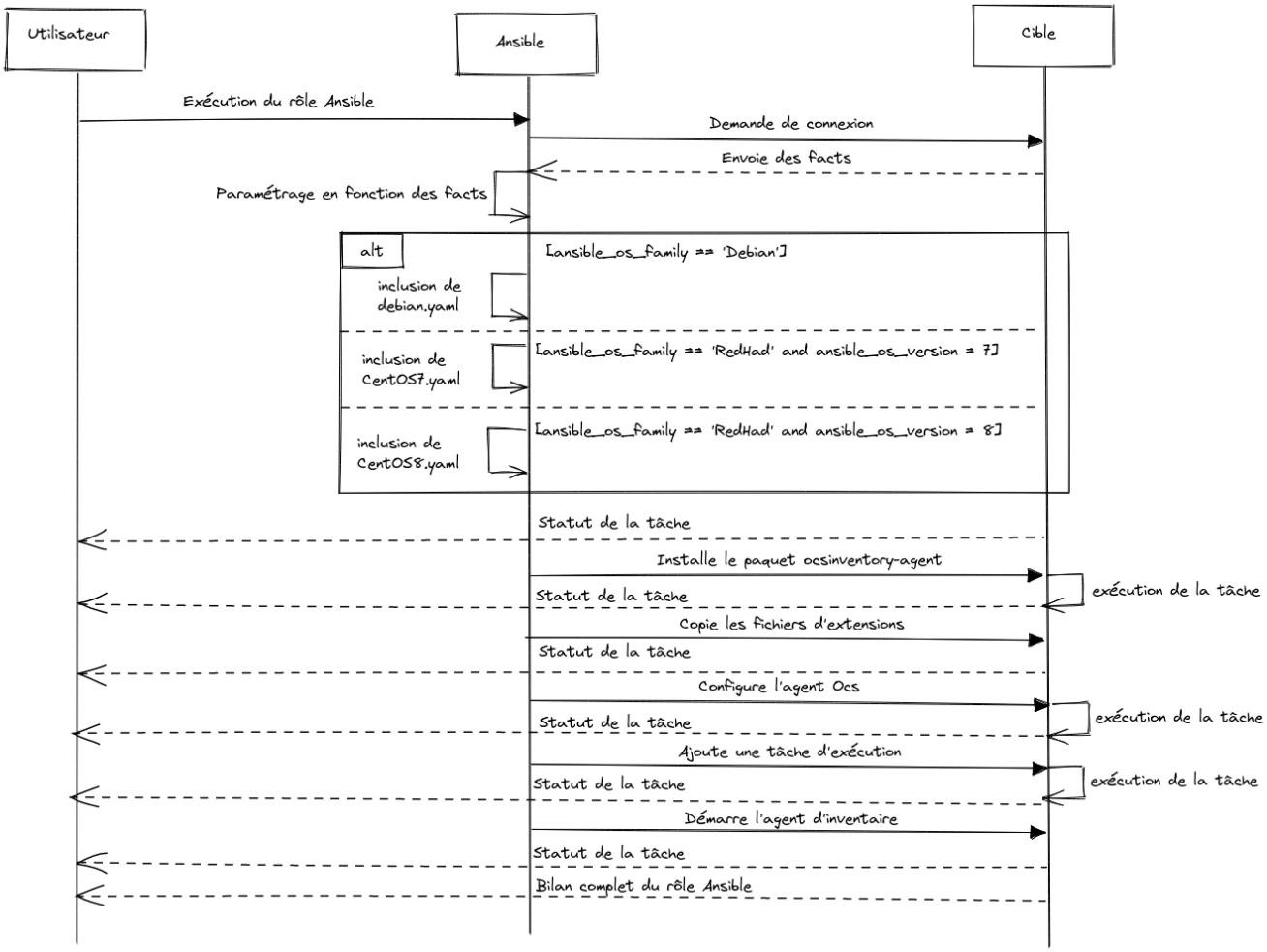


Figure 3.3: Diagramme de séquence de l'installation d'OCSInventory avec Ansible

L'utilisateur exécute le rôle Ansible. Cela va lancer une série d'étapes durant lesquelles Ansible va se connecter en SSH à la cible. Dans un soucis de simplicité, on considère ici que la connexion est acceptée et Ansible récupère l'ensemble des facts. A lieu ensuite un paramétrage dépendant des facts. Dans le cas de cette installation d'OCSInventory, cela prend en compte la famille du systèmes d'exploitation et sa version. A l'issues de ces étapes, divers tâches vont permettre l'installation et la configuration de l'agent sur la cible.

Afin que les salariés installent pas eux-même l'agent, j'ai rédigé une documentation décrivant comment installer et configurer l'agent OCSInventory sur Windows, Linux et ArchLinux.

3.2.7 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.

3.3 Durcissement Linux

3.3.1 Objectif

Dans le cadre de la 8ème 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 machine installée à partir de l'image d'origine n'est pas suffisamment sécurisée.

Pour répondre à ce besoin, j'ai décidé d'utiliser OpenSCAP et Ansible. L'objectif est d'utiliser les fonctionnalité d'OpenSCAP en les automatisant avec Ansible. Je cherche à obtenir pour chaque machine un rapport initial, le script Ansible de correctif et un rapport finale après application des correctifs.

3.3.2 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.

Egalement, il permet d'effectuer un scan d'une machine et de générer un rapport HTML. Depuis ce même rapport, il est possible de générer une ensemble de tâches Ansible corrigeant les erreurs.

3.3.3 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 handicapent 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 :

Nom de la distribution	Version	Espace disque	CPU	Ram
Debian	10	32 Gb	2	2 Gb
Debian	11	32 Gb	2	2 Gb
Ubuntu	20.04	32 Gb	2	2 Gb
Fedora	36	32 Gb	2	2 Gb
Centos	7	32 Gb	2	2 Gb
Centos	8	32 Gb	2	2 Gb

Table 1: Machines virtuelles créés pour les tests avec OpenSCAP

3.3.4 Création d'une archive Debian

Le paquet ne se trouve pas dans les listes des sources apt de Debian 11. J'ai débuté la création de l'archive Debian à partir des sources du paquet mais je n'ai pas réussi pour le moment.

3.3.5 Installation et configuration avec Ansible

A nouveau, c'est avec Ansible que la configuration d'Openscap est faite. Le diagramme de séquence suivant décrit le processus d'installation. Afin de le simplifier, la différenciation entre distribution et version n'est pas représentée.

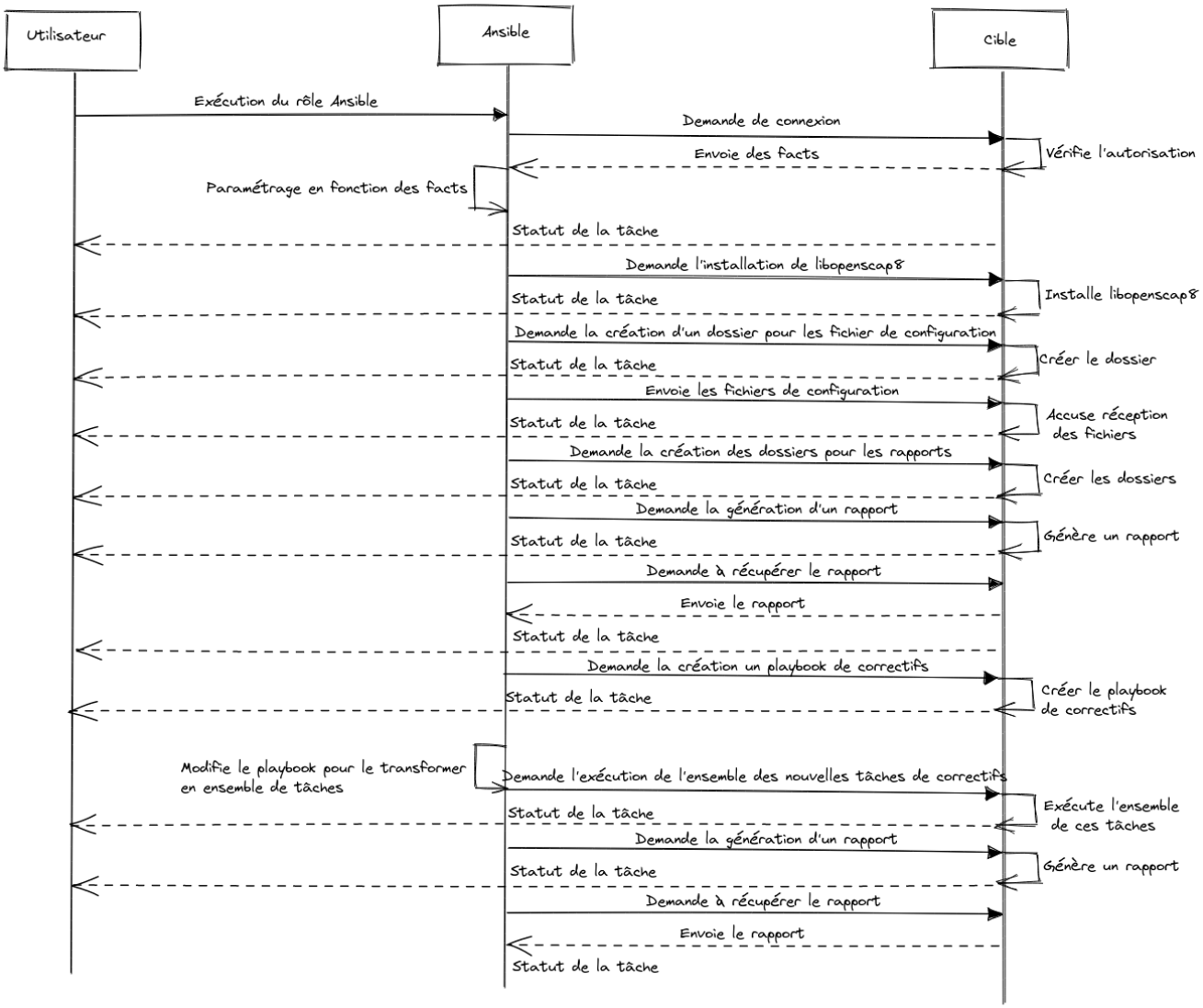


Figure 3.4: Diagramme de séquence du fonctionnement d'Ansible avec OpenSCAP

3.3.6 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. En l'état, l'outil est intéressant. Il ne peut pour autant pas être mis oeuvre tel quel car certaines règles sont trop restrictives. Par exemple, une des modifications apportées avec OpenSCAP fait que la connexion SSH à l'utilisateur root est désactivée. Cependant, lorsque l'on passe par le bastion SSH, toutes les connexions se font sur l'utilisateur root. Appliqué la script en l'état empêcherait l'utilisation du bastion.

3.4 Documentation

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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 :

3.5 Autres pistes d'étude

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

Durant la période de d'alternance, j'ai fais des essaies 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 contraignent 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.

3.6 Bilan

4 Travaux d'administrateur système

4.1 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.

4.1.1 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.

4.1.2 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**.

4.1.3 Schéma applicatif

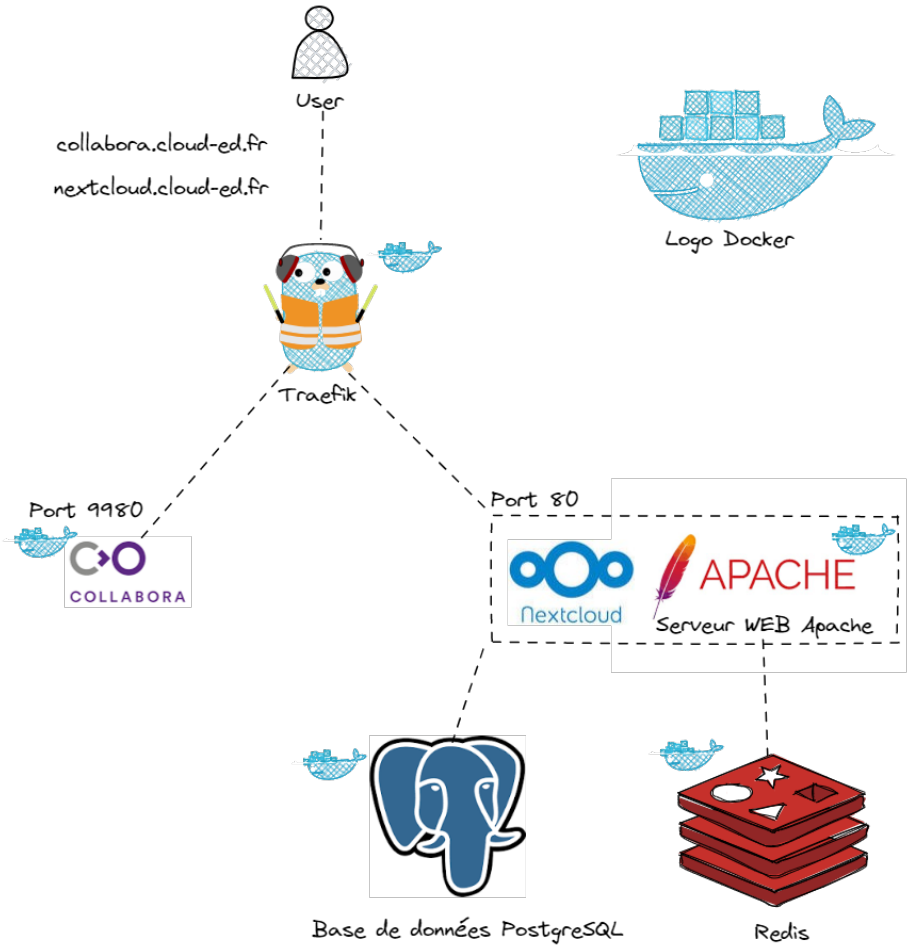


Figure 4.1: Schéma applicatif de Nextcloud avec Collabora

4.1.4 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'êtres secrètes.
- **Les secrets**. Ce sont d'autres variables obligatoires sauf qu'elles sont sensibles et donc à protéger. C'est le cas notamment des identifiant 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'`inventory` AWX et également dans le coffre-fort Ansible.

La personne qui réalise l'installation doit spécifier les variables dans l'`inventory` 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.

4.1.5 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`.

4.1.6 Utilisation d'AWX

Une fois l'inventaire et les variables mis à jour, il faut paramétrer AXW. 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.

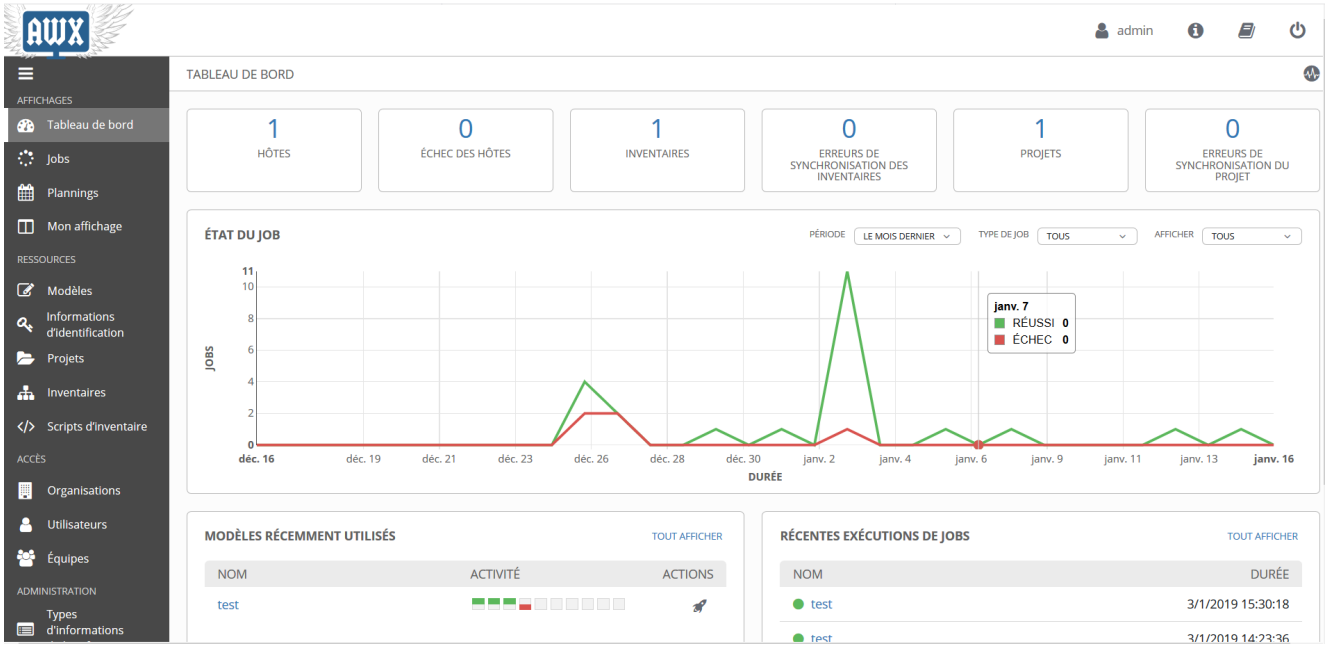


Figure 4.2: Interface web d'AWX

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'inventory, l'host, les credentials et le projet Nextcloud.

4.1.7 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 liés aux dépendances tels que l'installation du module `pip` pour Python.

4.1.8 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.

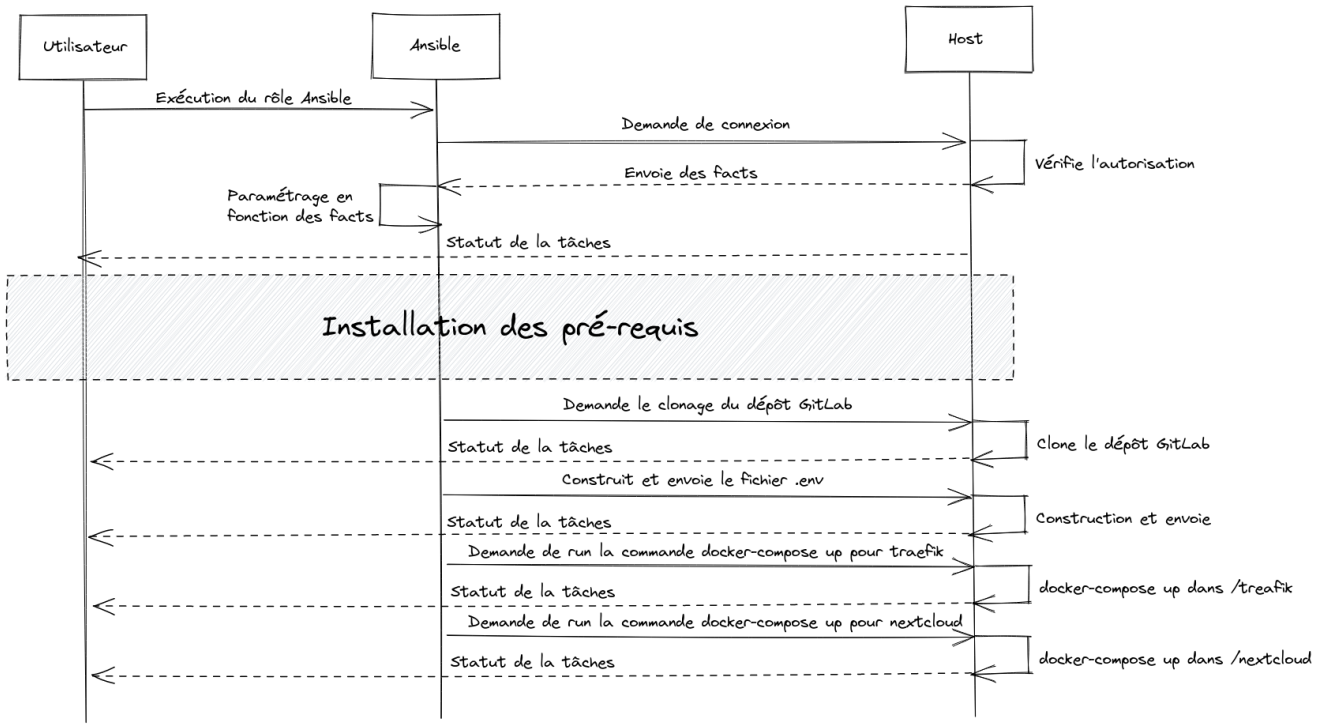


Figure 4.3: Diagramme de séquences des tâches Ansible lors de l'installation de Nextcloud

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

4.2 Proxmox

4.2.1 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.

4.2.2 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.

4.2.3 Matériel

Dans un premier temps, j'ai ajouté une carte fibre 10G pour ajouter une interface supplémentaire au serveur. Cette interface est destiné à faire transiter du traffic 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 baies. Cela revient à positionner les différentes 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.

4.2.4 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 dédié 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

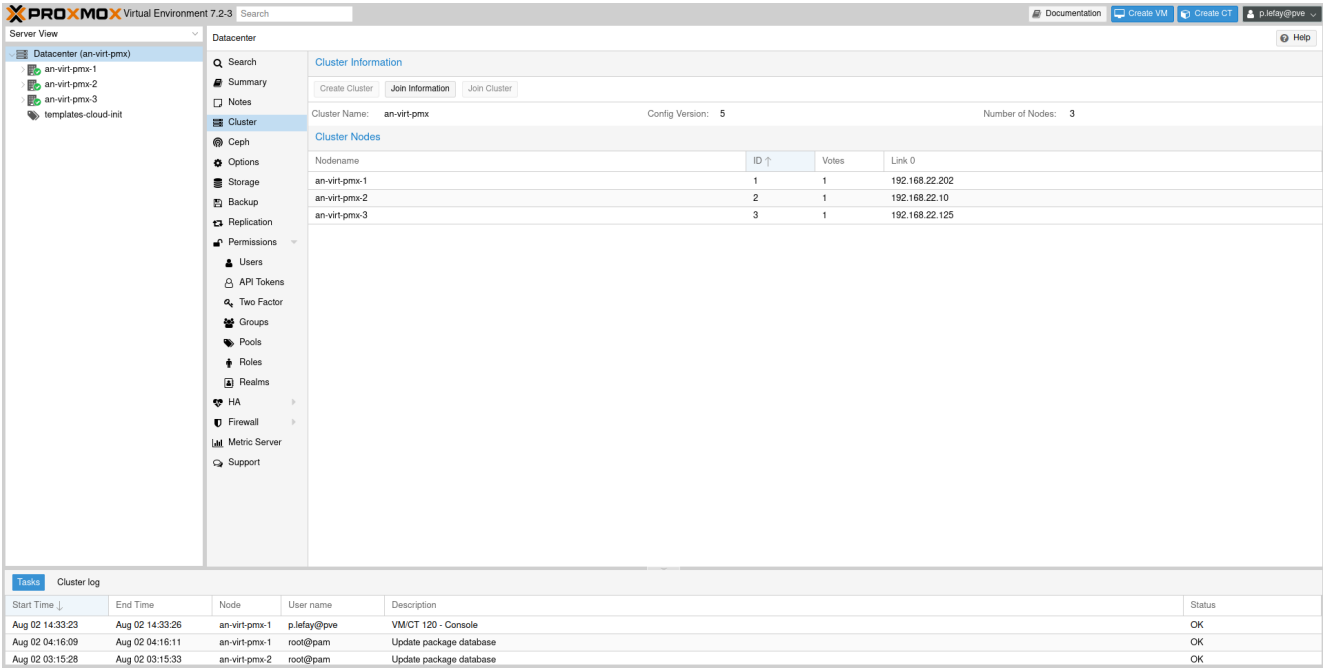


Figure 4.4: Interface du cluster Proxmox an-virt-pmx

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'entres-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.

4.3 Projet Dehon

4.3.1 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.

4.3.2 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.

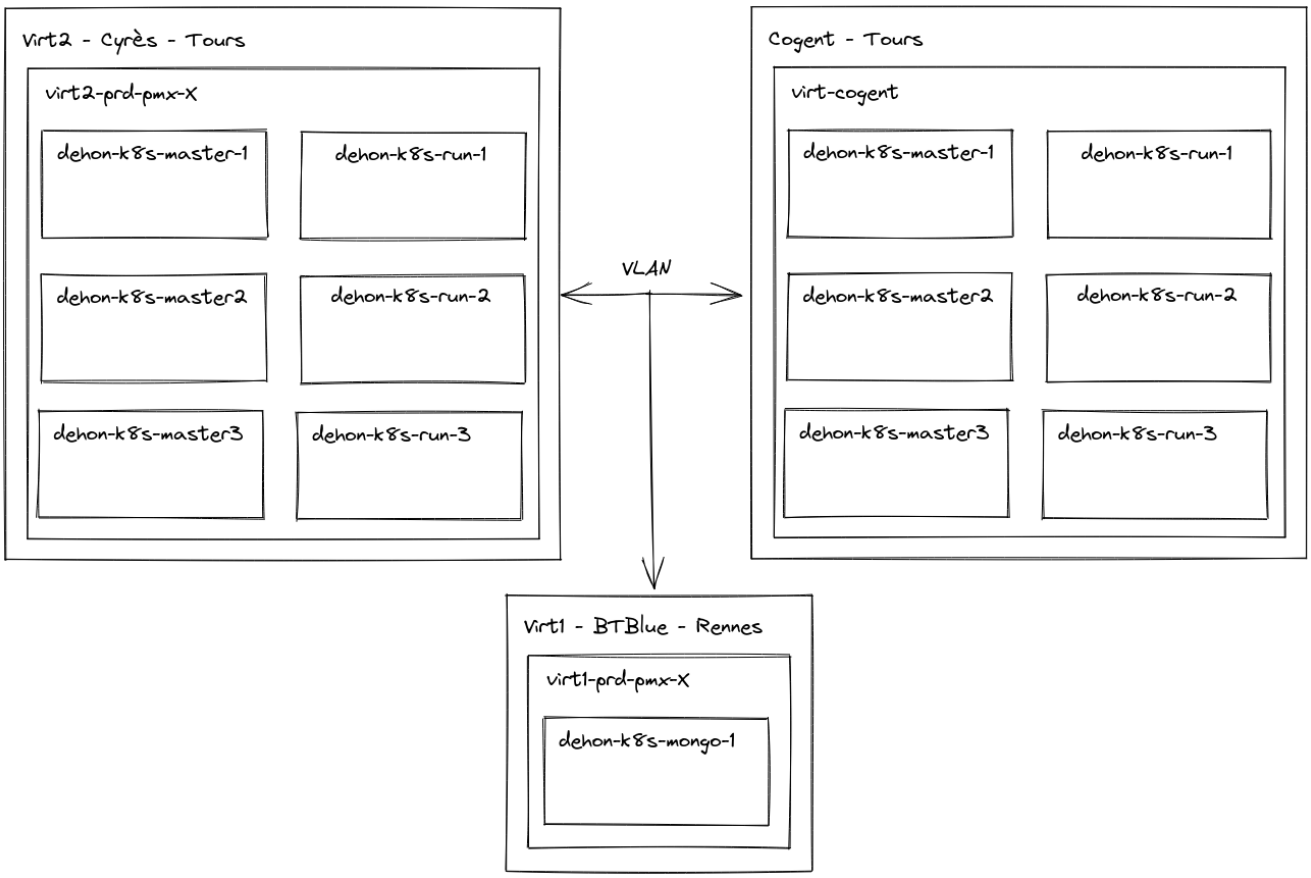


Figure 4.5: Infrastructure sur 3 sites physique du projet Dehon

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.

4.3.3 Création des cluster de machines physiques avec proxmox et terraform

Nous avons commencé par developper l'infrastructure sur virt2. Nous nous sommes servis de terraform pour deployer les machinnes 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 réfléchie 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 clées 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"

4.3.4 Installation du clusters Kubernetes via Kubespray

4.3.5 Configuration de proxy avec vip

4.3.6 IngressController, Certmanager, namespace, rancher rke

4.3.7 Stockage

4.3.8 Autres éléments

Ex : mongo arbiter

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

4.4.1 Objectif

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

4.4.2 Description

4.4.3 Documentation

4.4.4 Groupe de Travail Embarquement

4.5 Bilan

5 Bilan personnel

6 Annexes

Les 16 thématiques de sécurité

N°	Thèmes	Description
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.

Table 2: Les 16 thématiques de sécurité - Partie 1

N°	Thèmes	Description
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.

Table 3: Les 16 thématiques de sécurité - Partie 2

CV

Paul Lefay

Etudiant en 4ème année à l'ESEO

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

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,

paullefay@reseau.eseo.fr

www.linkedin.com/in/Paul-Lefay

LANGUES

- ✓ Anglais: B1
  TOEIC: 870 / 990
- ✓ Espagnol : Débutant

Formations

ESEO ANGERS
Septembre 2016 - Actuellement
Formation d'ingénieur généraliste avec spécialisation
Etudiant en 1ère année du cycle ingénieur (Bac+3).
Formation en informatique, électronique et infrascture 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 compabilité 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 cafeteria, 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'évènements 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

Planning détaillé de la période d'alternance

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.

Table 4: Planning du travail effectué sur la période de d'alternance - Partie 1

48	29/11/21 - 05/12/21	Fin des travaux sur Ansible CMDB et 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 à auditer.
50	13/12/21 - 19/11/21	Avancement le PSSI. Réunion de présentation final de la POC Ansible CMDB. Nouvelle POC sur Rudder pour reproduire une conformité similaire à 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	Congés pour Noël.
1	03/01/22 - 09/01/22	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 5: Planning du travail effectué sur la période de d'alternance - Partie 2

Planning détaillé de la période de stage

N°	Semaine	Description
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. 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 configuration d'un Cluster Ceph.
11	14/03/22 - 20/03/22	Réunion de lancement d'audit de sécurité avec la société Cogiceo. Poursuite de la configuration du Cluster Ceph, ajout des OSD. Configuration en pause pour le moment en attendant de faire la conception des pools et storages. Modification des configurations DHCP de façon à ce que tout le monde soit sur une adresse IP en 22. Reprise de la configuration des règles GLPI avant l'ajout de tous les périphériques. Installation de NetData pour vérifier le fonctionnement d'une machine défectueuse. Installation et configuration d'un nouveau noeud Proxmox ajouté au Cluster de test. Fin de paramétrage de GLPI avant d'ajouter l'ensemble du matériel du personnel.

Table 6: Planning du travail effectué sur la période de stage - Partie 1

N°	Semaine	Description
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.

Table 7: Planning du travail effectué sur la période de stage - Partie 2

N°	Semaine	Description
19	09/05/22 - 15/05/22	Mise à jours de l'une des instances de Webinaire. 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 webPeertube pour faire de l'hébergement vidéo et des lives. Installation d'un 2nd Bastion SSH (Passhport) destiné à être un slave du 1er afin d'y exécuter des Playbook Ansible globaux sans impact sur l'utilisation des autres utilisateurs. Création de la 2nd base de données en Master/Slave sur Mariadb.
20	16/05/22 - 22/05/22	Fin de l'installation du 2nd Bastion SSH (Passhport). Ré-exécution des Playbook Ansible d'installation d'agent OCSInventory afin de mettre à jours l'ensemble des Vhosts. En congé le vendredi 20. Début des mise à jours des instances BigBlueButton
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.

Table 8: Planning du travail effectué sur la période de stage - Partie 3

N°	Semaine	Description
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.
28	11/07/22 - 17/07/22	Déploiement de la machine Mongo Arbiter sur Rennes. Configuration du service Mongo via Terraform pour une application sous Docker. Installation via Terraform de 3 opérateurs percona pour les environnements de test, qualif et prod. Installation de mongoarbiter via Ansible. Congé le vendredi, pont de 4 jours.
29	18/07/22 - 24/07/22	Commandes pour les nouveaux arrivants. Création de compte rancher depuis Terraform. Déploiement de Loki lié à Grafana en tant que serveur de log pour l'ensemble du cluster. Ajout de minio en serveur S3. Ajout de Velero-server pour les backups. Fin de la mise à jours de la documentation pour les nouveaux arrivants. Reprise de la partie backup pour un matomo de la région Normandie.
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. Congés maladie pour Covid.

Table 9: Planning du travail effectué sur la période de stage - Partie 4

Bibliographie

Liste des figures

Liste des tables

Acronymes et définition

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

A | B | C | D | E | F | G | H | I | K | L | M | N | O | P | R | S | T | V | W | Y | Z

A

Alma AlmaLinux est une distribution Linux gratuite et open source, créée à l'origine par CloudLinux pour fournir un système d'exploitation d'entreprise de niveau production soutenu par la communauté et compatible binaire avec Red Hat Enterprise Linux 51, 57

Ansible Ansible est une plate-forme logicielle libre pour la configuration et la gestion des ordinateurs 51, 52, 57

Ansible CMDB Ansible est une plate-forme logicielle libre pour la configuration et la gestion des ordinateurs. Il permet notamment de récupéré les informations des machines et d'en faire une synthèse dans une page web. C'est ce à quoi sert Ansible CMDB 48, 49, 57

ANSSI Agence nationale de la sécurité des systèmes d'information 48, 57

Apache Le logiciel libre Apache HTTP Server est un serveur HTTP créé et maintenu au sein de la fondation Apache 52, 57

API Une API (application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. 53, 57

B

Backups En informatique, la sauvegarde ou backup est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique 57

Bastion SSH Un bastion SSH est une brique d'infrastructure qui permet à une connexion SSH de "rebondir" avant d'atteindre sa cible 52, 57

BigBlueButton BigBlueButton est un système de visioconférence développé pour la formation à distance. Il permet le partage de la voix et de l'image vidéo, de présentations avec ou sans tableau blanc 52, 57

Bitwarden Bitwarden est un gestionnaire de mots de passe freemium et open source sous licence AGPL, qui permet de générer et de conserver des mots de passe de manière sécurisée. Ces éléments sont protégés par un seul et unique mot de passe appelé « mot de passe maître » 57

C

Calico Calico est un nombreux CNI disponibles pour Kubernetes 52, 57

CentOS CentOS est une distribution GNU/Linux destinée aux serveurs 51, 57

Ceph Ceph est une solution libre de stockage distribué très populaire qui propose trois protocoles en un avec : Bloc, Fichiers et Objet. Les objectifs principaux de Ceph sont d'être complètement distribués sans point unique de défaillance, extensible jusqu'à l'exaoctet et librement disponible 50, 57

Cloud privé Le terme Cloud privé décrit un modèle de déploiement de Cloud à la demande avec lequel les services et l'infrastructure de Cloud Computing sont hébergés en privé sur l'intranet ou le Data Center de la société via des ressources propriétaires et ne sont pas partagés avec d'autres entreprises 9, 57

Cluster Groupe de serveurs et d'autres ressources qui agissent comme un système unique et permettent une haute disponibilité 50–52, 57

CNI CNI signifie Container Network Interface. De façon simplifier, les conteneurs dans un cluster Kubernetes ont besoin d'un réseau pour communiquer entre eux. C'est le rôle du CNI. Il existe de nombreux CNI disponibles pour Kubernetes 52, 57

Collabora Collabora est une suite bureautique en ligne basée sur LibreOffice avec des fonctions d'édition collaborative, qui prend en charge tous les principaux formats de documents, feuilles de calcul et fichiers de présentation, et fonctionne dans tous les navigateurs modernes. 51, 57

CVE Common Vulnerabilities and Exposures. Dictionnaire des informations publiques relatives aux vulnérabilités de sécurité 15, 50, 57

D

Datacenter Lieu où sont regroupés les équipements constituants d'un système d'information. Ce regroupement permet de faciliter la sécurisation, la gestion et la maintenance des équipements et des données stockées 50, 57

Debian Debian est un système d'exploitation Linux composée exclusivement de logiciels libres, développé par le Debian Project. Chaque version majeur de Debian possède une dénomination : Buster pour la version 10, Bulleyes pour la version 11 etc. 57

DeepFence Deepfence est une solution de prévention et de détection de sécurité essentielle pour les environnements cloud et conteneurs natifs 57

DHCP Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau 50, 57

DNS Le Domain Name System ou DNS est un service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements 57

Docker Docker est une plate-forme permettant de lancer certaines applications dans des conteneurs logiciels 52, 57

Docker-compose Docker-compose, un outil pour déployer plusieurs conteneurs en même temps. En gros, il faut retenir que Docker-compose permet de gérer un ensemble de conteneurs (services) 57

DPO Délégué à la protection des données. En droit européen, le Délégué à la protection des données est la personne chargée de la protection des données personnelles au sein d'une organisation 48, 57

E

ESEO École Supérieure d'Électronique de l'Ouest. Dans le présent rapport, il est fait mention d'ESEO Angers 2, 57

F

Framemo Application de tableau blanc avec des colonnnes pour y déposer des postits 52, 57

G

GLPI GLPI est un logiciel libre de gestion des services informatiques et de gestion des services d'assistance. Cette solution libre est éditée en PHP et distribuée sous licence GPL. En tant que technologie libre, toute personne peut exécuter, modifier ou développer le code qui est libre 50, 57

H

Haproxy HAProxy est un logiciel gratuit et open source qui fournit un équilibreur de charge haute disponibilité et un proxy inverse pour les applications TCP et HTTP qui répartissent les requêtes sur plusieurs serveurs 53, 57

HTML Le HyperText Markup Language, généralement abrégé HTML ou, dans sa dernière version, HTML5, est le langage de balisage conçu pour représenter les pages web 57

HTTP L'Hypertext Transfer Protocol, généralement abrégé HTTP, littéralement « protocole de transfert hypertexte », est un protocole de communication client-serveur 57

HTTPS L'HyperText Transfer Protocol Secure est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable 50, 57

I

IP Une adresse IP est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol. L'adresse IP est à la base du système d'acheminement des paquets de données sur Internet 50, 57

IPsec Internet Protocol Security .Regroupe un ensemble de protocoles, qui utilisent des algorithmes destinés à transporter des données sur un réseau de façon sécurisée 48, 57

K

Kubernetes Kubernetes est un système open source qui vise à fournir une « plate-forme permettant d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des clusters de serveurs » 51, 52, 57

Kubespray Utilitaire permettant de créer un cluster Kubernetes via Ansible 52, 57

L

LAMP LAMP est un acronyme désignant un ensemble de logiciels libres permettant de construire des serveurs de sites web. Linux Apache Mysql Mariadb 49, 57

LDAP Lightweight Directory Access Protocol est un protocole permettant l'interrogation et la modification des services d'annuaire électronique. 57

LimeSurvey LimeSurvey est un logiciel d'enquête statistique, de sondage, et de création de formulaires en ligne 50, 57

Linux Linux ou GNU/Linux est une famille de systèmes d'exploitation open source de type Unix fondé sur le noyau Linux, créé en 1991 par Linus Torvalds 57

M

Mariadb MariaDB est un système de gestion de base de données édité sous licence GPL. Il s'agit d'un embranchement communautaire de MySQL : la gouvernance du projet est assurée par la fondation MariaDB, et sa maintenance par la société Monty Program AB, créateur du projet 52, 57

Master/Slave Le principe de Master/Slave consiste à avoir 2 logiciels ou base de données interdépendant. Dans l'idée, une modification apportée au Master sera par la suite automatiquement appliquée au Slave. 52, 57

Matomo Matomo, anciennement Piwik jusqu'au début de 2018, est un logiciel libre et open source de mesure de statistiques web, successeur de PhpMyVisites et conçu pour être une alternative libre à Google Analytics 57

Mattermost Mattermost est un logiciel et un service de messagerie instantanée libre autohébergeable. Il est conçu comme un chat interne pour les organisations et les entreprises, et il est présenté comme une alternative à Slack et Microsoft Teams 57

Moodle Moodle est une plate-forme d'apprentissage en ligne libre distribuée sous la Licence publique générale GNU écrite en PHP. Développée à partir de principes pédagogiques, elle permet de créer des communautés s'instruisant autour de contenus et d'activités 57

N

Nextcloud Nextcloud est un logiciel libre de site d'hébergement de fichiers et une plate-forme de collaboration 51, 53, 57

Nginx Nginx est un logiciel libre de serveur Web ainsi qu'un proxy inverse 52, 57

NocoDB Outils permettant le traitement en feuille de calcul de bases de données SQL 50, 57

O

OCSInventory OCS Inventory NG soit Open Computer and Software Inventory est une application permettant de réaliser un inventaire sur la configuration matérielle des machines du réseau, sur les logiciels qui y sont installés et de visualiser ces informations grâce à une interface web 50–52, 57

OpenSCAP OpenSCAP fournit plusieurs outils pour aider les administrateurs et les auditeurs à évaluer, mesurer et appliquer les lignes de base de sécurité 52, 53, 57

Openvas OpenVAS, est un fork sous licence GNU GPL du scanner de vulnérabilité Nessus dont le but est de permettre un développement libre de l'outil qui est maintenant sous licence propriétaire 57

OSD Object Storage Deamon. Dans ceph, un OSD est le deamon responsable du suivi des stockages sous forme d'objet 50, 57

P

Passhport Passhport est une solution de gestion et de sécurisation des accès SSH 51, 57

Passhport Solution de gestion et de sécurisation des accès SSH. PaSSHport est un bastion SSH protégeant les accès sécurisés des systèmes d'information 52, 57

Peertube PeerTube est un logiciel libre d'hébergement de vidéo décentralisé permettant la diffusion en pair à pair, et un média social sur lequel les utilisateurs peuvent envoyer, regarder, commenter, évaluer et partager des vidéos en streaming 52, 57

PFE Projet de fin d'étude. Désigne à l'ESEO à un projet d'une durée d'un semestre pouvant être effectué en entreprise ou non 48, 49, 57

PHP PHP: Hypertext Preprocessor est un langage de programmation principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet 57

plate-forme web Une plate-forme web est un ensemble de services web. Le contenu des plate-formes web provient en grande partie des utilisateurs qui peuvent diffuser et partager des contenus de nature textuelle ou multimédia 52, 57

Playbook Les Playbooks Ansible offrent un système de gestion de configuration et de déploiement multi-machine reproductible, réutilisable et simple, bien adapté au déploiement d'applications complexes 52, 57

Plugin En informatique, un plugin ou plug-in, aussi nommé module d'extension, module externe, greffon, plugiciel, ainsi qu'add-in ou add-on en France, est un logiciel conçu pour être greffé à un autre logiciel à travers une interface prévue à cet effet, et apporter à ce dernier de nouvelles fonctionnalités 57

POC Proof of Concept ou Preuve de concept. Démonstration de faisabilité, c'est à dire une réalisation expérimentale concrète et préliminaire, courte ou incomplète, illustrant une certaine méthode ou idée afin d'en démontrer ou pas la faisabilité 19, 48, 49, 57

Proxmox Proxmox Virtual Environment est une solution de virtualisation libre basée sur l'hyperviseur Linux KVM, et offre aussi une solution de containers avec LXC 50, 57

Proxy Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges 57

PSSI Politique de sécurité du système d'information. Plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information 49, 57

R

Redmine Redmine est une application web libre de gestion de projets, développée en Ruby sur la base du framework Ruby on Rails 50, 57

RGPD Règlement Générale sur la Protection des Données 9, 48, 57

Rocky Linux Rocky Linux est une distribution Linux basée sur le code source du système d'exploitation Red Hat Enterprise Linux. 51, 57

Rudder Rudder est un logiciel libre de configuration automatique de serveurs. Il se veut simple d'utilisation, orienté web et applique un raisonnement dirigé par les rôles. Il s'appuie sur des agents légers installés localement sur chaque machine gérée 48, 57

S

SCOP Société coopérative et participative 9, 10, 57

SI Système d'information. Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs 48, 57

SNMP Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance 50, 57

SQL SQL est un langage informatique normalisé servant à exploiter des bases de données relationnelles. La partie langage de manipulation des données de SQL permet de rechercher, d'ajouter, de modifier ou de supprimer des données dans les bases de données relationnelles 50, 57

SSH Protocole de communication sécurisée basé sur un échange de clé privé et publique 48, 57

SSL Le protocole SSL (Secure Sockets Layer) était le protocole cryptographique le plus largement utilisé pour assurer la sécurité des communications sur Internet 50, 57

Sysadmin Le pôle sysadmin est en charge du développement, du suivi et de la maintenance du SI de l'entreprise. C'est l'équivalent d'administrateurs systèmes 19, 57

T

Terraform Terraform est un environnement logiciel d'« infrastructure as code » publié en open-source par la société HashiCorp. Cet outil permet d'automatiser la construction des ressources d'une infrastructure de centre de données comme un réseau, des machines virtuelles, un groupe de sécurité ou une base de données 52, 53, 57

TLS Transport Layer Security ou Sécurité de la couche de transport est un protocole de sécurisation des échanges par réseau informatique, notamment par Internet 48, 57

Traefik Traefik est donc un reverse-proxy et un load-balancer fait pour déployer principalement des conteneurs 57

V

Vhosts En informatique, l'hébergement virtuel est une méthode que les serveurs tels que serveurs Web utilisent pour accueillir plus d'un nom de domaine sur le même ordinateur, parfois sur la même adresse IP, tout en maintenant une gestion séparée de chacun de ces noms 52, 57

vip Une adresse IP virtuelle est une adresse IP non connectée à un ordinateur ou une carte réseau spécifiques. Les paquets entrants sont envoyés à l'adresse IP virtuelle, mais en réalité ils circulent tous via des interfaces réseau réelles 53, 57

W

Wazuh Wazuh est une plate-forme open source utilisée pour la prévention, la détection et la réponse aux menaces 51, 57

Webinaire Webinaire est un mot-valise associant les mots Web et séminaire, créé pour désigner toutes les formes de réunions interactives de type séminaire faites par Internet généralement dans un but de travail collaboratif ou de transmission d'informations pour une audience plus ou moins importante en nombre 51, 52, 57

Wifi Le terme Wifi correspond au protocole IEEE 802.11 est un ensemble de normes concernant les réseaux sans fil locaux 48, 57

Windows Windows est au départ une interface graphique unifiée produite par Microsoft, qui est devenue ensuite une gamme de systèmes d'exploitation à part entière, principalement destinés aux ordinateurs compatibles PC 57

Y

YesWeHack YesWeHack est une plate-forme permettant la mise en contact entre des entreprises et des hackers éthiques 48, 57

Z

Zammad Zammad est un service d'assistance gratuit ou un système de suivi des problèmes 57