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 7 septembre 2022
SUJET MISSION:	Analyse et réalisation d'audits automatisés de l'infrastructure
TUTEUR ENTREPRISE:	Valentin Baraise et Yves-Gaël Chény

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, 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 auteurs, 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 19 août 2022.

Remerciements

Je tiens à remercier Yves-Gaël Chény, Nicolas Gourichon et Valentin Baraise pour l'opportunité qu'ils m'ont donnée en m'acceptant en contrat de professionnalisation. L'expérience acquise lors de la période de Projet de Fin d'Etude (PFE) est inestimable comparée à celle que j'aurais eue 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'aider lorsque je rencontrais des difficultés. 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 lors de mes premières installations et utilisations d'Ansible. Ils m'ont apporté de nombreuses connaissances sur le sujet.

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

Table des matières

I L'environnement et le contexte du stage . . . 11

1 Empreinte Digitale . . . 11

1.1 Activités . . . 11
1.2 Structure . . . 12
1.3 Responsabilité sociétale et environnemental . . . 14
1.3.1 Label Lucie . . . 14
1.3.2 Design4Green . . . 14
1.3.3 Budget participatif . . . 15
1.3.4 Stratosfair . . . 15
1.4 Pôle datacenter . . . 16
1.5 Comité sécurité . . . 16
1.6 Gestion de projet . . . 16

2 Sujet . . . 18

2.1 Contexte . . . 18
2.2 Problématique . . . 18
2.3 Objectifs . . . 18
2.4 Outils et ressources . . . 18

II Préambule technique . . . 19

1 Proxmox . . . 19

2 Terraform . . . 20

3 Ansible . . . 21

III Travaux de sécurité . . . 22

1 Période d'alternance . . . 22

2 Inventaire des machines . . . 23

2.1 Objectif . . . 23
2.2 OCSInventory et GLPI . . . 23
2.3 Architecture . . . 23
2.4 Principe de fonctionnement . . . 24
2.5 Installations . . . 25
2.5.1 OCSInventory . . . 25
2.5.2 GLPI . . . 25
2.5.3 Traefik . . . 25

2.6 Ajout d'un plugin . . . 26
2.7 Installation et configuration de l'agent avec Ansible . . . 27
2.7.1 Bastion SSH . . . 27
2.7.2 Inventaire . . . 27
2.7.3 Rôle Ansible . . . 27
2.8 Bilan . . . 29
3 Durcissement Linux . . . 30
3.1 Objectif . . . 30
3.2 Openscap . . . 30
3.3 Création des machines virtuelles de test . . . 30
3.4 Création d'une archive Debian . . . 31
3.5 Installation et configuration avec Ansible . . . 31
3.6 Bilan . . . 32
4 Documentation . . . 33
4.1 Objectif . . . 33
4.2 Réalisation . . . 33
5 Autres . . . 34
IV Travaux d'administrateur système . . . 35
1 Nextcloud et Collabora . . . 35
1.1 Objectif . . . 35
1.2 Description . . . 35
1.3 Schéma applicatif . . . 36
1.4 Utilisation des variables . . . 37
1.5 Inventaire Ansible . . . 37
1.6 Utilisation d'AWX . . . 38
1.7 Rôle Ansible . . . 39
1.8 Conclusion . . . 40
2 Proxmox . . . 41
2.1 Rappel . . . 41
2.2 Objectif . . . 41
2.3 Installation physique . . . 41
2.4 Installation logiciel . . . 43
2.4.1 Image . . . 43
2.4.2 Réseau . . . 43
2.4.3 Regroupement en cluster . . . 44
2.5 Ceph . . . 45
2.5.1 Installation . . . 45

2.5.2 Object-based Storage Device . . . 45
2.6 Storage . . . 47
2.6.1 Pool de storage . . . 47
2.6.2 CephFS . . . 47
2.7 Template . . . 47
3 Projet Dehon . . . 48
3.1 Objectif . . . 48
3.2 Architecture sur trois sites . . . 48
3.3 Schéma de le partie applicative . . . 50
3.4 Déploiement des machines virtuelles avec Terraform . . . 51
3.4.1 Les machines et leur rôle . . . 51
3.4.2 Les providers . . . 51
3.4.3 Les modules . . . 51
3.5 Déploiement du cluster Kubernetes avec Kubespray . . . 52
3.5.1 Kubespray . . . 52
3.5.2 Mise à jour de l'inventaire . . . 52
3.5.3 Paramétrage de Kubespray . . . 52
3.5.4 Installation . . . 52
3.6 Configuration des deux Haproxy . . . 53
3.7 Configuration de la VIP sur les proxys . . . 53
3.8 Stockage NFS externalisé . . . 54
3.9 Les ressources Kubernetes . . . 54
3.9.1 Ingress Controller . . . 54
3.9.2 Cert Manager . . . 54
3.9.3 Rancher . . . 55
3.9.4 Monitoring . . . 55
3.9.5 Journaux de log . . . 55
3.9.6 Sauvegardes . . . 56
3.9.7 Base de données MongoDB et MongoArbiter . . . 56
3.10 Bilan . . . 57
4 Procédure d'arrivée . . . 58
4.1 Objectif . . . 58
4.2 Description . . . 58
4.3 Documentation . . . 58
4.4 Groupe de Travail Embarquement . . . 58
5 Autres . . . 59
5.1 Commandes Linux . . . 59
5.2 Tmux . . . 60

5.3 K9s 61

V Bilan personnel 62

Annexes 63

Les 16 thématiques de sécurité 63
CV 65
Planning détaillé de la période de stage 68
Bibliographie 78
Liste des figures 80
Liste des tables 81
Acronymes et définition 82

Fiche de synthèse

J'ai effectué mon stage dans le cadre d'un contrat de professionnalisation chez Empreinte Digitale située au 11 rue des Noyers à Angers. Cela signifie que j'y étais présent en tant qu'alternant du 7 septembre 2021 au 29 janvier 2022, puis en tant que stagiaire du 30 janvier 2022 au 8 septembre 2022.

Empreinte Digitale est une entreprise développant des applications web et hébergeant des applications open-source. De ce fait, celle-ci est impactée par la menance croissante des attaques informatiques.

Mon sujet de stage S10 a porté sur la mise en place de nouveau outils de sécurité ayant pour but l'amélioration du système d'information d'Empreinte Digitale. Ce sujet ne portait pas sur la mise en place d'un outil en particulier. J'ai donc dans un premier temps réaliser une veille technologique durant la période d'alternance. Cette veille consistait en des recherches sur Internet et la lecture d'un ensemble de livres blanc rédigés par l'ANSSI. Suite à cela, j'ai déterminé les axes d'améliorations de l'infrastructure.

J'ai travaillé sur deux aspects de sécurité:

- Inventaire des ressources: une entreprise doit être en mesure de lister l'ensemble des ressources informatiques. Afin de réaliser et automatiser cet inventaire, j'ai mis en place les applications OCSInventory et GLPI.
- Durcissement des systèmes Linux: suite à l'installation d'un système d'exploitation, il est nécessaire de le renforcer. Pour cela, j'ai utilisé l'application OpenSCAP.

En parallèle de mes travaux de sécurité, j'ai travaillé sur divers tâches d'administrateur système qui ont porté sur:

- L'automatisation des installations des applications Nextcloud et Collabora.
- L'installation d'un cluster Proxmox sur le site d'Angers.
- La mise en place d'une infrastructure complète pour Dehon.
- La mise à jours de la documentation et du processus pour les nouveaux arrivants.

De façon général, durant les sept derniers mois, j'ai passé 60% de mon temps sur les tâches d'administrateur système et 40% sur les travaux de sécurité. N'ayant pas d'appétence particulière sur le sujet de la sécurité, j'ai beaucoup apprécié cette bifurcation. Cela me conforte dans l'idée que je souhaite à l'avenir travailler dans le domaine de l'administration système et du DevOps.

Les difficultés rencontrée étaient toutes techniques. Mon manque de connaissances sur des aspects bas niveau, réseau notamment, m'ont parfois ralentie dans l'avancement de mes projets. Cela n'était pas un problème pour autant, car l'aide de l'ensemble de administrateurs systèmes et particulièrement de Valentin Baraise m'a permis d'avancer et d'apprendre.

Abstract

The threat of cyberattacks is a subject that has always existed for all companies. Nevertheless, in recent years, the scale of attacks has increased, to such an extent that it is difficult for companies to follow the movement. As a result, it has become essential for companies to implement a reinforced policy for the security of information systems.

I worked on improving the information system in order to make it more secure and thus be more serene in the face of attacks. Having no specific objective, I initially carried out a technological watch. For this, I relied on the many security white papers from the ANSSI, a French security agency.

ANSSI's documentation revolves around 16 themes. I selected two of them. First, the need for a company to keep an inventory of all the IT resources that make up the information system. Second, the need to harden an operating system as soon as the installation is completed. I then started researching to find a solution for these two subjects.

The criteria focused on: an open-source tool, free, without limitation in time or resources with a significant learning curve The final objective is to obtain a solution in production for the inventory and the reinforcement of the systems. This means that the use over time of these tools must be done with the minimum of manual actions.

For the inventory, this led me to the use of OCSInventory and GLPI. Both tools validate each of my criteria. Moreover, they have the advantage of being flexible in use.

For hardening Linux systems, I first considered developing a tool myself. Nevertheless, I finally found the OpenSCAP tool which also validates all the criteria.

To simplify the tool installations as much as possible, I decided to use docker. This makes it possible to synthetically declare parameters of the applications. Moreover, if it is necessary to carry out any modification, it is enough to modify the configuration file. At the end of my work, the two tools are in production.

I explain in this document the methodology implemented in the installation of these two tools. I also give the axes which will allow to go further on the implementation and the use.

Introduction

La menace des cyberattaques est un sujet qui a toujours existé pour toutes les entreprises. Néanmoins, ces dernières années, l'ampleur des attaques est grandissante, à un point tel qu'il est compliqué pour les entreprises de suivre le mouvement. En effet, d'après l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, le nombre d'attaques a augmentée de 37% entre 2020 et 2021. Cela représente un évolution de 786 intrusions avérées à 1082.

Une partie importante de la sécurité concerne l'amélioration du SI sur un vaste panel de sujets. Cependant, la plupart des attaques utilisent l'hameçonnage ou *phishing*. Cette technique consiste à récupérer des données personnelles par la tromperie puis de les utiliser de manière maveillante. Dans la vie courante, l'intêret peut être d'obtenir les informations bancaire d'un individu, mais dans le cadre d'une entreprise, cette méthode peut permettre une intrusion dans le SI. Pour cette raison, la sécurité d'une entreprise passe également par les utilisateurs qui y accèdent. On peut aller jusqu'à dire que si une priorisation devait être faite, la formation et la sensiblisation des salariés à la sécurité du SI est prioritaire.

Du fait de cette croissance des incidents de sécurité, Empreinte Digitale a décidé de renforcer son système d'information avec de nouveaux outils de sécurité. L'entreprise à également fait auditer le SI afin d'établir un premier état des lieux.

Mon rapport s'organise en quatre parties. Dans la première, j'exposerai l'environnement et le contexte du stage. La seconde partie sera consacrée à la présentation de trois outils techniques régulièrement utilisés et cités dans ce document. Dans une troisième partie, j'évoquerai les travaux de sécurité portant sur les thématiques de sécurité, l'inventaire des machines, le durcissement des systèmes Linux et la documentation. Je présenterai en quatrième partie 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 hypertexte, les liens vers des sections ou des acronymes et définitions sont interactifs. Les ressources sont disponibles sur le dépôt GitHub `https://github.com/theprobleme/stagereportS10`.

Partie I : L'environnement et le contexte du stage

1 Empreinte Digitale

Empreinte Digitale est une SCOP d'une cinquantaine de collaborateurs basée sur Angers depuis 29 ans. Elle travaille à la réalisation de solutions numériques responsables et sur-mesure. L'entreprise est basée à Angers, au 11 rue des Noyers.

empreinte digitale
Créateur de vos SOLUTIONS NUMÉRIQUES RESPONSABLES

1.1 Activités

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

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.

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

Hébergement en cloud privé: hébergement Web responsable en Cloud privé indépendant dans des datacenters en France. Les serveurs sont exclusivement gérés avec des technologies libres et open source, garantissant une indépendance vis-à-vis 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.

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.

Ligeo archives

Figure 1: Logos des prestations d'Empreinte Digitale

1.2 Structure

Juridiquement, une Société COopérative et Participative SCOP est une société coopérative de forme SA, SARL ou SAS dont les salariés sont les associés majoritaires et où le pouvoir 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. [1]

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 attractif pour les futur collaborateurs. La transparence et la collaboration est un facteur clé favorisation l'implication et la motivation des salariés.

Empreinte Digitale à débuté son évolution en SCOP en 2018 pour officiellement le devenir en janvier 2020.

Figure 2: Les étapes du passage en SCOP d'Empreinte Digitale

La gouvernance se découpe de la manière suivante:

Figure 3: 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 composée de 32 salariés. Un salarié ne peut pas rester dans l'entreprise si a ses 3 ans d'ancienneté il ne souhaite pas adhérer à la SCOP. Cette assemblée générale mandate le conseil d'administration constitué des membres élus et en retour, les membres de conseil animent, représentent et rendent compte aux associés.

La gouvernance de l'entreprise est assurée par un directeur général, responsable légale qui travaille avec un comité opérationnel. Ils travaillent avec les différents pôles dans la mise en oeuvre de la stratégie d'entreprise.

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

1.3 Responsabilité sociétale et environnemental

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

1.3.1 Label Lucie

Empreinte digitale est officiellement engagée dans une démarche de Responsabilité Sociétales des Entreprises (RSE) depuis 2018, année de sa labellisation Lucie ISO 26000. LUCIE est une certification attestant qu'une entreprise, un produit ou un service à réussie sa démarche en matières de RSE. [2]

1.3.2 Design4Green

Le Design4Green est un challenge organisé depuis 5 ans par l'ESAIP, une école d'ingénieur Angevine. Durant ce hackathon de 48h, les équipes doivent répondre sur un sujet autour d'un projet web et d'éco-conception. Le projet doit prendre en compte son empreinte environnementale.

En 2021, le thème portait sur le développement d'une interface pour les professionnels de suivi de l'éco-conception d'un projet web intégrant 491 critères. Empreinte Digitale à participé à cette édition et l'a remportée avec une application statique, éco-conçue et accessible.

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

Figure 4: Application web réalisé par Empreinte Digitale pour le Design4Green

1.3.3 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 au vote. Le prix gagné au Design4Green a 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 propositions fûrent nombreuses: console de jeu, abri pour oiseaux, salle de sport, jeu de fléchettes etc.

1.3.4 Stratosfair

En 2020, Empreinte Digitale a lancé un partenariat avec Stratosfair. L'objectif: créer un datacenter responsable. Ce nouveau datacenter a 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 vivants.
- 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 5: Maquette en trois dimensions 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 développées pour la création de machines virtuelles dans un cluster Proxmox depuis une interface web.

D'autres projet RSE sont accessible sur le site `https://blog.empreintedigitale.fr`.

1.4 Pôle datacenter

Empreinte Digitale est constituée 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 découpées 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 jusqu'à la conception et l'installation d'architectures spécifiques à un besoin. C'est le cas par exemple pour le projet Dehon.
- **Travaux internes**: deux personnes, moi y compris, travaillons sur divers travaux internes. Cela concerne par exemple les installations des postes de travail, les mails, les accès et les installations de nouveaux outils.
- **Commercial**: une personne gère la partie commerciale et facturation.
- **Chef de projet**: une personne travaille sur la gestion de projet, en lien avec le commercial.

Les activités ne sont pas à ce point-là segmentées. En raison des astreintes et à l'entre-aide collective, tout le monde "touche à tout". Par exemple, bien qu'ayant travaillé majoritairement sur des travaux internes, je également intervenu sur des offres cloud.

1.5 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.

Sa mission est pour le moment de maintenir une veille sur la sécurité afin d'apporter des axes d'améliorations dans les domaines du développement, de l'hébergement, de la documentation et des bonnes pratiques générales à l'attention de tous. Le comité se réuni une fois pas mois pour suivre l'avancement de divers sujets.

1.6 Gestion de projet

Deux outils sont très utilisés dans la gestion de projet chez Empreinte Digitale.

Tout d'abord Redmine, une application web libre de gestion de projets. Elle est utilisée pour le ticketing en interne et avec les clients. Ils possèdent des accès au Redmine et peuvent eux-même créer des tickets. L'outils permet également d'avoir une liste de contacts rattachées aux projets.

Redmine a un rôle important dans l'exploitation car il permet de gérer deux autres aspects.

- La comptabilisation du temps de travail qui est, via l'outil, calculé à partir de la saisie hebdomadaire de chaque employé (il n'y a pas de système de badgeage).
- La production d'analytiques comptables issus de la classification des tickets, par exemple l'évaluation du temps de travail consacré à une l'activité de développement.

Le second outil est Mattermost, un logiciel libre de messagerie instantanée auto-hébergeable. Il est une altervative libre à Slack ou Microsoft Teams. Certains clients possèdent des canaux Mattermost en plus de Redmine. Cela évite notamment de passer par les mails lors d'échanges répétés.

Le vendredi en début d'après-midi, une première liste des tâches à accomplir la semaine suivante est établie en réunion. Cela permet d'avoir une première idée du volume horaire à y consacrer. Le lundi après-midi, l'ensemble est validé pour le reste de la semaine.

En tant que stagiaire, je n'avais pas toujours de tickets. Mes travaux étant souvent internes, je créais, dans la même logique, des tickets que je m'attribuais.

2 Sujet

2.1 Contexte

Empreinte digitale développe son offre DATACENTER engendrant ainsi une évolution rapide de l'infrastructure et de nouveaux besoins notamment en matière de sécurité. En effet, l'entreprise ne possède actuelle pas d'outils de conformité, de contrôle de sécurité ni de CVE. Par ailleurs, les salariés ne disposent pas encore de documentation spécifiant le comportement à adopter lors de l'utilisation du SI ou en cas de faille de sécurité révélée.

2.2 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?

2.3 Objectifs

L'objectif est de 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 par de nouvelles procédures permettant de pérenniser les solutions. En parallèle, il y a des tâches annexes d'administration système comme installer des plateformes pour les clients, préparer le matériel pour les nouveaux arrivants, etc.

2.4 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 II.

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

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

Partie II : Préambule technique

1 Proxmox

Proxmox est une plateforme open-source complète pour la virtualisation d'entreprise. Grâce à l'interface Web intégrée, nous pouvons facilement gérer les machines virtuelles, les conteneurs, le stockage, 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.
- 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 à chaud, agir sur le template, accéder à la console etc.

Proxmox intègre une solution de stockage nommé Ceph. Ceph permet la haute disponibilité et durabilité des données dans un cluster.

2 Terraform

Terraformest un outil open source d'infrastructure as code (IaC) développé par Hashicorp. Il permet de déclarer sous forme de code l'état d'une infrastructure que l'on souhaite obtenir. Dans des fichiers de configuration structurés, on va manager l'infrastructure et mettre à jour 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 6: Workflow de Terraform

Après les premières 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, cet état peut être configuré sur GitLab de façon à assurer la cohérence des états entre 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.

À ces providers on spécifie des ressources. Chaque bloc de ressources décrit un ou plusieurs objets d'un service. La construction d'une ressource est basée sur le provider qui l'a 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.

3 Ansible

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'agent 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 l'état souhaité. On distingue trois principaux types de scripts:

- Les **rôles**. Ce sont un ensemble de playbooks qui s'assurent de la présence ou non 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'une machine. Cela peut être par exemple la présence ou non d'un paquet apt.

L'utilisation d'un rôle n'est pas toujours nécessaire. Un rôle a surtout pour vocation de créer une configuration qui sera réutilisée régulièrement. Il est donc possible de se limiter à l'utilisation de playbook. Les variables d'un rôle peuvent être mises dans un `vault` lorsqu'elles ont vocation à être secrètes. Cela revient à un fichier YAML chiffré. Pour accéder à son contenu, il est nécessaire d'en connaître le mot de passe.

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 trois de pré-requis: une connexion SSH vers ces cibles, l'installation de la bonne version de python 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 tâche Ansible est jouée, il y a quatre états principaux:

- **`OK`**: la configuration était déjà correcte, Ansible n'a rien changé.
- **`SKIPPED`**: les conditions d'application de la tâche ne sont pas validées. La tâche est ignorée.
- **`CHANGED`**: la configuration n'était pas correcte, Ansible a apporté les changements nécessaires avec succès.
- **`ERROR`**: la configuration ne s'est pas bien passée, Ansible renvoit l'erreur associée.

Partie III : Travaux de sécurité

1 Période d'alternance

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

- **Analyse abstraite et bonnes pratiques**. J'ai réalisé une veille technologique sur les logiciels et outils utilisés par les administrateurs systèmes. Par ailleurs, j'ai pris le temps de me développer des connaissances sur les sujets de sécurité avec les documentations et livres blanc de sécurité de l'ANSSI ainsi que les sites de conseils de sécurité.
- **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 la documentation.
- **Préconisations**. J'ai rédigé des documentations pour le pôle Sysadmin et l'ensemble des salariés : livre blanc de sécurité, PSSI (Plan de sécurité des systèmes d'information), etc.
- **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 présentées en annexe aux pages 63 et 64 .

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 7: 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 d'Empreinte Digitale et ceux qui ne l'étaient pas.

2 Inventaire des machines

2.1 Objectif

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 et les machines virtuelles qu'elles hébergent. La solution retenue est d'utiliser deux logiciels open-source :

2.2 OCSInventory et GLPI

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 logiciels.

Gestionnaire Libre de Parc Informatique (GLPI) est une solution open-source de gestion de parc informatique qui permet la classification des différentes ressources. GLPI ne récupère pas les informations lui-même, il a besoin d'un logiciel d'inventaire complémentaire tel que OCSInventory ou FusionInventory.

Finalement, GLPI va permettre de trier les informations récupérées par OCSInventory.

2.3 Architecture

Figure 8: Architecture entre OcsInventory et GLPI

2.4 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 envoyer des rapports quotidiennement via le protocole HTTP au serveur maître. Ensuite, l'application GLPI avec un plugin va se connecter à OCSInventory et lire les données. Finalement, par une action manuelle à réaliser dans GLPI, je valide les imports.

Un champ TAG, configuré au niveau des agents, permet une segmentation des machines. J'ai défini les TAGs suivant:

- **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 tri lors de l'import. Par exemple, les machines dont le TAG est **REN** seront placées dans l'entité "Datacenter de Rennes". Lorsqu'un import est validé, GLPI écrit les données dans une base de données qui lui est propre.

Figure 9: Interface de l'application GLPI

Figure 10: Interface de l'application OCSInventory

2.5 Installations

2.5.1 OCSInventory

Avant mon arrivé, des travaux avaient déjà été réalisés avec OCSInventory. Je n'ai donc pas eu à l'installer. L'application est installée dans un conteneur LXC sur le cluster Proxmox d'Angers.

2.5.2 GLPI

J'ai installé GLPI avec Docker sur une machine virtuelle dédiée aux conteneurs. Pour cela, j'ai utilisé `docker-compose` avec les trois services: mariadb, glpi et automysqlbackup. Ensuite, j'ai mis en place le monitoring avec Monit et UptimeRobot. Enfin, sur un serveur NAS, j'ai joué un playbook Ansible qui permet la synchronisation des backups d'automysqlbackup vers le serveur NAS.

2.5.3 Traefik

La partie réseau est gérée avec un routeur Traefik. Traefik était déjà installé. Il m'a suffit d'ajouter dans la partie `label` du fichier `docker-compose.yaml` quelques lignes de configuration.

Par défaut, Traefik est configuré afin de router les ports 80 et 443. Le point d'entrée 80 est nommé `web` et le 433 `web-secure`. Ainsi, dans les labels du `docker-compose`, j'ai spécifié l'utilisation du point d'entrée `web`. Je n'ai pas mis en place de redirection vers `web-secure` car l'application est accessible uniquement sur le réseau local.

2.6 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 de scripts Perl permettant d'inventorier les vhosts des serveurs web Nginx et des conteneurs Docker pour les écrire 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 table `vhost`. Si celle-ci existe déjà, il ne fait aucune action, sinon il créer la table.

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 la commande utilisée pour les vhosts des serveurs Nginx.

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

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

Cela donne la commande suivante pour les vhots des conteneurs docker:

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

2.7 Installation et configuration de l'agent avec Ansible

2.7.1 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.

2.7.2 Inventaire

Ansible se base sur des fichiers d'inventaire dans lesquel on décrit le nom des machines dans des groupes. La première chose que j'ai fai 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 le fait qu'il en manquait au niveau d'Ansible. J'ai alors fait 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 trois 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 erreurs. Je les ai corrigé peu à peu en me basant sur la représentation de l'inventaire sous forme de graphique.

2.7.3 Rôle Ansible

Mon rôle est découpé de la manière suivante:

```
ocsinventory-agent/
|-- /default     # Variables par défaut
|-- /files       # Fichiers supplémentaires
|-- /meta        # Nécessaire à Ansible Galaxy
|-- /tasks       # Ensemble des playbooks
|-- /vars        # Variables supplémentaires
```

- `default`: variables pour le TAG, le nom des paquets, etc.
- `files`: scripts supplémentaires d'installation du plugin.
- `meta`: enregistrement du créateur du rôle. Ce dossier est nécessaire pour utiliser Ansible-Galaxy.
- `tasks`: ensemble des tâches Ansible.
- `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 déroulées sans erreurs.

Figure 11: Diagramme de séquence de l'installation d'un agent avec Ansible

L'administrateur 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. Débute ensuite un paramétrage dépendant des facts. Dans le cas de cette installation d'OCSInventory, cela prend en compte la famille du système d'exploitation et sa version. À l'issue de ces étapes, diverses

tâches vont permettre l'installation et la configuration de l'agent sur la cible.

Afin que les salariés installent eux-même l'agent, j'ai rédigé une documentation décrivant comment installer et configurer l'agent OCSInventory sur Windows, Linux et ArchLinux. J'ai accompagné les salariés qui avaient des difficultés d'installation.

2.8 Bilan

Bilan des installations:

- L'installation sur les machines d'Angers est terminée.
- L'agent est installé sur la majorité des machines de Rennes.
- L'agent n'est pas installé sur les machines de Tours. Le réseau d'Angers et Tours n'étant pas encore reliés, les agents sur Tours ne peuvent pas communiquer avec le serveur maître sur Angers.
- L'ensemble des salariés ont installés l'agent.

Concernant les installations, mes travaux sont perfectibles. Pour le moment, je n'ai pas mis de règles de supression au niveau du serveur OCSInventory. C'est-à-dire qu'il faudrait paramétrer le serveur afin qu'il supprime une machine s'il n'a pas de nouvelles de celle-ci dans les 30 jours. On pourra alors considérer qu'elle n'existe plus.

Je n'ai pas paramétré de mailing. Il serait intéressant d'avoir une adresse mail dédiée à la réception des informations du serveur OCSInventory. Cela serait important notamment avant suppression d'une machine pour s'assurer que cela soit justifié.

La solution n'est pas pérenne dans le temps. La procédure d'installation du nouvelle machine est encore à revoir. Il faut prendre le temps de revoir la procédure d'installation d'une nouvelle machine afin d'y intégrer l'aspect OCSInventory.

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

3 Durcissement Linux

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 fonctionnalités 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 final après application des correctifs.

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 en ligne de commande (CLI), appelé oscap, offre un outil polyvalent pour analyser un système et en obtenir un rapport. [3]

Depuis ce même rapport, il est possible de générer une ensemble de tâches Ansible corrigeant les erreurs.

3.3 Création des 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, il faut d'abord éprouver la solution afin de s'assurer qu'il n'entraîne pas de modifications handicapantes 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 créées pour les tests avec OpenSCAP

3.4 Création d'une archive Debian

L'outil s'installe avec le gestionnaire de package `apt`. Cependant, celui-ci n'est pas dans les listes des sources 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.

3.5 Installation et configuration avec Ansible

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

Figure 12: Diagramme de séquence du fonctionnement d'Ansible avec OpenSCAP

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 les tests en fonction des distributions sont corrects. L'outil est donc fonctionnel excepté bien évidemment pour Debian 11.

Bien que l'application soit intéressante et facile à mettre en oeuvre, elle n'est pas suffisament paramétrable. Certaines règles appliquées sont trop restrictives.

Par exemple, une des modifications apportées avec OpenSCAP fait que la connexion SSH à l'utilisateur root est désactivée. Au première abord, cette règle est tout à justifiée, l'accès SSH en root est une mauvaise chose. Néanmoins, lorsque l'on passe par le Bastion SSH, toutes les connexions se font sur l'utilisateur root. Appliquer le script en l'état empêcherait l'utilisation du Bastion SSH. Cela n'est donc pour le moment pas compatible avec le fonctionnement chez Empreinte Digitale.

Néanmoins, le rapport généré permet permet d'obtenir une liste de modifications à apporter. Par exemple, il serait intéressant de retravailler sur l'installation et la configuration du paquet `auditd`, du découpage des différentes journaux de log etc.

4 Documentation

4.1 Objectif

Dans plusieurs des thématiques portant sur la sécurité, un aspect documentaire est mis en avant. Il s'agit de disposer de documents descriptifs de l'infrastructure, de procédures et processus liés à l'exploitation et de documents juridiques répertoriant les engagements qui devant être mis en oeuvre entre employeur et salariés, ainsi qu'entre clients et prestataire. L'objectif est d'avancer sur les documentations manquantes et de faire en sorte d'en assurer la pérennité.

4.2 Réalisation

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 repris la documentation interne du datacenter afin de rédiger en premier lieu 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 (PAS) spécifiant les devoirs entre prestataires et clients quant à l'exploitation des services installés par Empreinte Digitale.

La documentation dédiée au Sysadmin et à l'ensemble des salariés est rédigée sur un Wiki.js, une application open-source hébergée en interne. Cette application permet de rédiger des documents en markdown depuis une interface web. Dans le cadre de cette reprise de la documentation, j'ai installé une nouvelle instance avec Docker.

Figure 13: Interface web de l'application Wiki.js

5 Autres

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

Au cours de la période de d'alternance, j'ai fait des essais avec Ansible CMDB. Cette solution bien que non retenue pourrait être reconsidérée. En effet, l'aspect réseau est problématique. L'application Ligeo Gestion est majoritairement installée chez les clients. Pour les machines hébégergeant cette application, il faudrait mettre en place des mécanismes supplémentaires d'accès réseau. Cependant, nous avons une connexion SSH à ces machines. Cela serait donc plus aisé d'utiliser Ansible CMDB.

J'ai également testé Rudder. Techniquement, la solution est intéressante mais coûteuse.

De plus, j'ai essayé Wazuh, une plateforme gratuite et opensource de sécurité basée sur un fonctionnement d'agent. Celle-ci permet de réaliser du monitoring de sécurité ainsi que de l'application de correctifs. Néanmoins, le fonctionnement avec agent est contraignant et la configuration uniquement via des fichiers XML, rendant la création de règles fastidieuse.

Enfin, j'ai essayé OpenVas, un outil open-source de scan de vulnérabilités de site WEB. Je ne suis pas allé très loin dans l'expérimentation, l'outil mériterait d'y consacrer plus temps.

Partie IV : Travaux d'administrateur système

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 différentes types de fichier en collaboration. Cette suite logiciel est finalement une alternative libre et open-source à l'utilisation d'outils tels que Google Drive ou OneDrive.

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, quatre 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.
- **Jinja** couplé à Ansible pour permettre de générer les fichiers de configurations avec les bonnes variables en se basant sur des templates.

1.2 Description

L'application repose sur des conteneurs Docker hébergés sur une machine virtuelle, elle-même dans un cluster Proxmox. On compte cinq 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` représentés sur la figure 14 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**.

1.3 Schéma applicatif

Figure 14: Schéma applicatif de Nextcloud avec Collabora

1.4 Utilisation des variables

Automatiser au mieux l'installation revient à créer un template d'installation, n'utilisant que des variables. On distingue deux 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 mais cette fois sensibles et qui sont donc à protéger. C'est le cas notamment des identifiants et mots de passe des services.

Les variables sont utilisées à trois endroits:

- Dans le fichier `docker-compose`, où elles 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 `vault` Ansible.

J'ai créé un `template` Jinja qui génère le fichier `.env` en utilisant les variables de l' `inventory` AWX et le `vault` Ansible. Le fichier généré est par la suite déplacé dans le bon répertoire pour être utilisé lors du lancement de la commande `docker-compose up`.

L'opérateur, lors d'une nouvelle installation, doit donc dans un premier spécifier les variables dans l' `inventory` AWX et dans le `vault` Ansible.

1.5 Inventaire Ansible

Le paramétrage des variables pour le rôle et le vault était la première étape. Ensuite, il faut mettre à jour l'inventaire Ansible. Avec Ansible on peut créer des variables en fonction des groupes. Je me suis servis de ce mécanisme pour créer une distinction entre les différents vault. Tout d'abord, j'ai créé le dossier `group_vars`, dans lequel se trouvent deux dossiers:

- `aicla`: contient le fichier vault.yaml du client aicla.
- `ed`: contient le fichier vault.yaml du client ed.

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

Si un nouveau client doit être ajouté, il suffit de créer un nouveau dossier au nom du client et d'y mettre le fichier de vault.

Ensuite, pour que les `group_vars` soient effectifs, il faut créer un groupe dans l'inventaire Ansible portant le même nom. Le fichier `host` faisant office d'inventaire 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`, spécifiés dans le fichier `group_vars/vault.yaml`.

1.6 Utilisation d'AWX

Ansible AWX est un projet communautaire en code source libre qui fournit un logiciel pour la gestion des projets Ansible. Ainsi, par le biais d'une interface graphique, on va pouvoir exécuter des rôles ou playbooks Ansible. AWX est également associé à Ansible Tower, la version entreprise d'AWX développée par RedHat.

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

Figure 15: Interface web d'AWX

Dans AWX, j'ai créé un projet `Nextcloud`. Dans ce projet, j'ai fait appel à une source `Git` qui est mon dépôt GitLab avec le nom de la branche et les identifiants à utiliser.

Ce projet AWX n'a pas à être modifié. Dans la logique d'AWX, on peut avoir de multiples templates utilisant un unique projet. Ainsi, on aura plusieurs templates de création d'instance Nextcloud par client utilisant le même Projet.

Ensuite j'ai créé un `Template` utilisant mon projet `Nextcloud` et d'autres ressources. Les ressources supplémentaires à créer sont:

- **Inventories**: variables d'environnement.
- **Hosts**: nom de la machine et son adresse IP.
- **Credentials**: accès au dépôt GitLab et mot de passe du Vault Ansible.
- **Templates**: spécifie l'utilisation des éléments précédemment créé, c'est-à-dire l'inventory, l'host, les credentials et le projet Nextcloud.

1.7 Rôle Ansible

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

Figure 16: Diagramme de séquences des tâches Ansible lors de l'installation de Nextcloud

1.8 Conclusion

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

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 jour 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 installées. Si la version d'un composant de Nextcloud évolue, il suffit alors de modifier l'inventaire de chacun des modèles.

De plus, on assure une installation homogène du produit. Dans une situation d'astreinte, cela permet d'identifier toutes les ressources de l'application et cela peu importe l'instance sur laquelle il faut intervenir.

De plus, il arrive souvent de laisser le fichier `.env` directement sur la machine, ce qui est à proscire. Avec l'installation actuelle, le fichier `.env` est généré, utilisé puis supprimé. Pour l'administration, l'ensemble des administrateur systèmes enregistre les mots de passe des vaults dans l'application Bitwarden, ce qui leurs permet dans tous les cas de récupérer les accès à une base de données par exemple.

2 Proxmox

2.1 Rappel

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

2.2 Objectif

Les datacenters de Rennes et Tours utilisent une plateforme de virtualisation nommé Proxmox. L'objectif est de mettre en oeuvre la même plateforme de virtualisation à Angers. Pour cela, 3 serveurs physiques sont disponibles afin de construire un cluster à 3 noeuds.

2.3 Installation physique

Dans un premier temps, j'ai ajouté une carte fibre 10G pour disposer d'une interface supplémentaire. Cette interface est destinée à faire transiter du trafic réseau ayant besoin de plus de débit qu'une simple interface 1G. L'interface 1G quant à elle sert à l'administration du serveur.

Figure 17: Carte fibre 1 Gigabytes

Figure 18: Carte fibre 10 Gigabytes

Les deux cartes se distinguent par leur port. L'interface 1G nécessite un câble RJ45 alors que la 10G utilise un câble SFP+.

Figure 19: Câble réseau RJ45

Figure 20: Câble réseau SFP+

Dans un second temps, j'ai racké les serveurs dans une baie. Enfin, j'ai ajouté des disques SSD et HDD supplémentaires. Pour chaque serveur, un disque est réservé à l'installation du système d'exploitation et les autres servent au stockage pour les machines virtuelles. J'ai formaté chacun des disques destinés au stockage.

Figure 21: Disque HDD de 6To

Figure 22: Disque SSD de 500Go

2.4 Installation logiciel

2.4.1 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 basée sur l'image Debian 11 nommé Bullseye à partir d'un disque dur externe bootable IODD. Cela permet de ne pas avoir à créer une clé bootable dédiée.

2.4.2 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 192.168.23.0/23.

Une fois cette étape terminée, les interfaces web de Proxmox sont disponibles à l'adresse IP configurée sur le port par défaut 8006. Sur le DNS interne, j'ai créé trois enregistrements sur le domaine `.vt`: `an-virt-pmx-1.vt`, `an-virt-pmx-2.vt` et `an-virt-pmx-3.vt`. Le domaine utilisé est accessible uniquement sur le réseau local.

Figure 23: Configuration réseau de Proxmox à l'installation

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

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

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

Figure 24: Interface du cluster Proxmox an-virt-pmx

Arrivé à ce stade, le cluster est fonctionnel. Cependant, pour une raison de fiabilité du stockage, j'ai installé et paramétré une solution de stockage nommé Ceph.

2.5 Ceph

Ceph est une solution libre de stockage distribué qui propose trois protocoles: Bloc, Fichiers et Objets. L'objectif de Ceph est d'obtenir un stockage 100% distribué sans point unique de défaillance.

2.5.1 Installation

Par défaut, une section **Ceph** est disponible sur l'interface de chaque noeud de Proxmox. Cette section permet d'installer Ceph lorsque ce n'est pas déjà le cas. L'installation se fait par un simple clique à réaliser sur chacun des noeuds.

2.5.2 Object-based Storage Device

Ceph est basé sur l'utilisation de Object-based Storage Device (OSD). Cela représente un système de stockage qui organise les données sous forme d'objets et non pas sous forme de fichiers comme on peut en avoir l'habitude. Cela permet le stockage non structuré de n'importe quel type d'objet. Les données sont identifiables par un ID unique et des métadonnées comme les dates, les autorisations, les auteurs etc.

Figure 25: Représentation des types de storage par Scaleway's [4]

La configuration d'OSD nécessite que les disques soient vierges, d'où l'étape de formatage au niveau matériel. Ensuite, j'ai ajouté chacun des disques disponibles au cluster Ceph. Cela donne la représentation suivante si l'on regarde les quatre disques d' `an-virt-pmx-1`:

Figure 26: Disques présents sur le noeud an-virt-pmx-1

Directement depuis l'interface Ceph, on peut visualiser l'ensemble des OSDs du cluster:

Figure 27: Ensemble des OSD du cluster an-virt-pmx

J'ai installé deux autres composants pour Ceph:

- **Ceph Monitor**: démon qui conserve une copie maîtresse de la carte du cluster. La carte ou *crush map* est un fichier dans lequel est écrit l'ensemble de ressources Ceph: OSD, hosts, règles etc. Pour un niveau de disponiblité optimale, il est nécessaire d'avoir au moins trois monitors.
- **Ceph Manager**: démon qui s'éxecute parallèlement aux monitors pour surveiller l'état du cluster. Il y a toujours au moins un monitor présent, mais si il y en a plusieurs, alors un seul est actif à la fois.

2.6 Storage

2.6.1 Pool de storage

J'ai créé deux pools de storage pour le cluster. Le premier se nomme **ssd**. Il est dédié aux systèmes d'exploitation et aux services nécessitant une vitesse de lecture et écriture rapide. Le second se nomme **hdd**. Il est dédié au stockage volumineux qui n'est que très rarement lu.

Par exemple, pour une installation d'un Nextcloud volumineux, le système d'exploitation avec les applications de Nextcloud sont sur un pool **ssd** tandis que les données (les fichiers notamments) sont sur le pool **hdd**.

2.6.2 CephFS

Ceph possède son propre FileSystem nommé CephFS. J'ai créé un stockage CephFS afin d'y déposer l'ensemble des ISO qui pourraient être utiles. Cela permet de stocker ces images sur un seul noeud et de présenter ce stockage aux autres. J'y ai déposé des ISO pour Ubuntu, Debian, Fedora, CentOS et RockyLinux.

2.7 Template

L'utilisation de Proxmox et Terraform repose sur la création de Template Cloud Init. Pour faire un template, il suffit de créer une machine virtuelle avec le système d'exploitation souhaité puis de définir cette machine comme Template. Les noms de templates sont les mêmes pour Angers, Rennes et Tours. Ainsi, lors de l'utilisation de Terraform, il n'y a pas à changer le nom du template en fonction du cluster.

3 Projet Dehon

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 plateforme centralisée et consultable via un portail web.

Une évolution de la réglmentation impose aux détenteurs d'installations frigorifiques de justifier d'un contrôle continu de leurs installations et d'être en mesure de 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 travaillé à la réalisation de cette infrastructure avec deux autres membres du pôle sysadmin.

3.2 Architecture sur trois sites

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

- `virt1`: Proxmox de Rennes sur lequel se trouve un arbiter MongoDB.
- `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 replica du premier cluster de virt2.

En voici un schéma:

Figure 28: Infrastructure sur trois sites physiques du projet Dehon

Les serveurs étaient déjà mis en place pour `virt1` et `virt2`. Il a cependant été nécessaire de se rendre à Tours à Cogent pour y installer une machine. Cette machine contient un unique cluster Proxmox. J'ai fais le déplacement avec Yves-Gaël Chény.

Le rattachement du réseau de Cyrès vers Cogent s'est fait avec une fibre noir. Celle-ci a été installée par le personnel de Cyrès. La distance entre les deux bâtiments est d'environ 2km.

3.3 Schéma de le partie applicative

Le schéma ci-dessous présent l'architecture Kubernetes mise en oeuvre. Chacune des sections à venirs présentent les étapes d'installation de cette infrastructure.

Figure 29: Cluster Kubernetes de dehon sur virt2-prd-pmx

3.4 Déploiement des machines virtuelles avec Terraform

Nous avons commencé par developper l'infrastructure sur `virt2`. Nous nous sommes servis de terraform pour déployer les machines virtuelles sur le cluster.

3.4.1 Les machines et leur rôle

dehon-k8s-master: trois machines virtuelles destinées à être les masters. Dans le conception de Kubernetes, ces machines seront les cerveaux du cluster. C'est sur celles-ci que des composants de Kubernetes vont permettrent l'orchestration des runners.

dehon-k8s-run: trois machines virtuelles destinées à être les workers. Ces trois machines seront celles qui supportent la charge de travail dans le cluster.

dehon-k8s-pxy: deux machines virtuelles en tant que proxy. Elles seront le point d'entrée de l'infrastructure.

dehon-k8s-storage: une machine virtuelle pour le stockage. L'ensemble du cluster utilisera un stockage partagé.

La dénomination de ces machines est réfléchie afin d'identifier le client, le rôle et le nombre de chaque composant. Ces noms sont visibles sur le schéma de l'infrastructure.

3.4.2 Les providers

Contrairement aux travaux précémment réalisés avec Terraform, on travaille ici avec trois cluster Proxmox différents. Cela nécessite de déclarer trois providers: `proxmox-cogent`, `proxmox-virt1` et `proxmox-virt2`. Chacun des providers possède son url, son nom d'utilisateur et son mot de passe. Ces variables sensibles sont stockées dans un fichier `secret.tfvars`, le fichier Terraform pour les secrets.

3.4.3 Les modules

J'ai défini différents modules. Pour les clusters dupliqués, on utilise quatre modules:

dehon-k8s-master-virt2-main: module pour la création des masters sur `virt2`. Un champ spécifique permet de définir que ce module doit être utilisé trois fois pour ainsi créer trois machines virtuelles. Terraform permet de créer certains champs avec un système d'incrémentation, ainsi les adresses IP ou les noms des machines se feront automatiquement.

dehon-k8s-run-virt2-main: module pour la création des runners sur `virt2`. La logique est similaire à celle des masters.

dehon-k8s-pxy-virt2-main: module pour la création de deux proxy.

dehon-k8s-storage-virt2-main: module pour la machine de stockage. Celle-ci possède la particularité d'avoir deux disques, le premier pour le système d'exploitation et le second de 2 To pour les données.

Le rôle et l'architecture des machines installées avec les deux derniers modules de la liste ci-dessus seront présentés plus tard.

A l'issue de cette étape, on obtient le cluster présenté sur la figure 28 avec trois autres machines virtuelles.

3.5 Déploiement du cluster Kubernetes avec Kubespray

A présent que les machines virtuelles du cluster Kubernetes sont installées, il a fallu installer le cluster Kubernetes.

3.5.1 Kubespray

Kubespray est un utilitaire basé sur Ansible qui permet le déploiement automatisé d'un cluster Kubernetes. Le dépôt GitHub du projet est disponible ici:
`https://github.com/kubernetes-sigs/kubespray`.

3.5.2 Mise à jour de l'inventaire

La première étape consiste à mettre à jour l'inventaire Ansible. Pour cela, un exemple est donné dans le dépôt ici. On y voit un inventaire basé autour des composants vitaux de Kubernetes:

kube_controle_plane: cerveau de Kubernetes. Ce composant doit donc être installé sur les noeuds master.

etcd: base de données clé-valeur reposant sur un tableau à deux colonnes. La première contient la valeur. La second contient la clé. Cette base contient la totalité de la configuration du cluster Kubernetes. Ce fichier est vital à la reconstruction d'un cluster en cas de sinistre.

kube_node: ce sont les travailleurs.

Cette structure permet l'installation des bons composants de Kubernetes aux bons endroits.

3.5.3 Paramétrage de Kubespray

Le nombre de paramètres possibles est gigantesque. Pour cette partie je n'ai donc paramétré que les éléments que je connaissais, le reste ayant été fait pas mon tuteur:

loadbalancer_apiserver: les noeuds slaves communiquent via API aux masters.

loadbalancer_apiserver_port: port d'accès à l'API.

kube_network_plugin: différents plugin Kubernete existent pour le réseau. Dans notre cas, on utilise calico.

kube_apiserver_ip: même valeur que le loadbalancer_apiserver.

3.5.4 Installation

L'installation se lance comme un rôle Ansible avec la commande `ansible-playbook`. Cela lance un nombre importante de tâches. L'installation a une durée comprise entre 20 et 30 minutes.

3.6 Configuration des deux Haproxy

Deux Haproxys sont installés afin d'assurer la haute disponibilité. Si un seul Haproxy était installé, et que celui-ci venait à avoir des défaillances, alors le cluster ne serait plus accessible.

La configuration des proxys se fait avec un rôle Ansible. Le paramétrage des variables permet la génération des fichiers de configurations à partir de template Jinja. Quatre fichiers sont dédiés aux configurations de bases de l'Haproxy. Un autre fichier, qui est le plus important, contient les différentes configurations des frontend et backend.

J'ai édité le template Jinja des configurations des frontend et backend de façon à se qu'il génère le fichier de configuration en fonction du nom du projet, des adresses IP autorisées etc. La présence de boucle dans le template Jinja permet d'auto-générer un ensemble de champs `server` à partir de la liste des serveurs. C'est par exemple le cas pour les différents backend sur l'ensemble des master et runner.

A l'issue de cette configuration, les deux Haproxy possèdent la même configuration. Ils sont donc en mesure de jouer un rôle identique.

3.7 Configuration de la VIP sur les proxys

Toujours dans l'objectif d'assurer une haute disponiblité, une VIP (Virtual IP) est configurée sur les proxys. Concrètement, c'est une adresse IP qui "se balade" entre les deux proxys. Celle-ci est paramétré à l'adresse 10.2.11.100, adresse utilisée pour le `loadbalancer_apiserver`.

Par exemple, si le premier proxy à une défaillance, l'adresse IP 10.2.11.100 va être relocalisée sur le second proxy. Ainsi, nous n'avons plus de SPOF (Single Point Of Failure) pour l'API Server.

Pour mettre en place cette VIP , j'ai utilisé un playbook Ansible qui permet d'installer KeepAlived. eepAlived s'appuie sur le protocole VRRP (Virtual Router Redundancy Protocol) conçu pour gérer une adresse IP virtuelle entre plusieurs hôtes.

Après l'installation et la configuration de KeepAlived avec Ansible, l'interface réseau `eth0` de `dehon-k8s-pxy-1` possède deux adresses: `10.2.11.80`, son adresse sur le réseau local et `10.2.11.100`, la VIP. `eth0` de `dehon-k8s-pxy-2` ne possède que l'adresse `10.2.11.81`. Si le service KeepAlived ou Haproxy s'arrête, ou pire encore si une des machines s'éteind, alors la VIP `10.2.11.100` bascule sur l'autre machine. C'est alors `dehon-k8s-pxy-2` qui possède les adresses `10.2.11.81` et `10.2.11.100` sur l'interface `eth0`.

On assure ainsi une redondance de l'accessibilité à l'API server.

3.8 Stockage NFS externalisé

Externaliser les données permet de confier en un point l'ensemble des données. Cela permet également d'avoir un point unique à sauvegarder. De plus, en cas de sinistre, les données sont localisées à autre endroit. Afin d'externaliser les données, un serveur NFS est installé sur le `virt1`.

Ansible est à nouveau utilisé pour déployer le serveur NFS sur la machine de storage. L'installation est basée sur l'utilisation du paquet apt `nfs-kernel-server`. La machine possède un premier disque de 50G pour le système d'exploitation et un second pour le stockage de 2To. J'ai fait un point de montage `/srv/nfs/shared` sur l'entièreté du disque de stockage. Le chemin d'export est donc paramétré sur le point de montage `/srv/nfs/shared`.

La suite de la configuration se fait au niveau du cluster Kubernetes. Il faut déclarer une nouvelle `StorageClass` qui utilisera le serveur NFS. Pour cela, j'ai utilisé le provider "Helm" avec la ressource `kubernetes_storage_class`. Les paramètres principaux à spécifier sont l'adresse du serveur et le chemin:

```
parameters = {
    server = "10.2.11.70"
    share  = "/srv/nfs/shared"
}
```

Le `Physical Volume Claim` des applications utilisant la `StorageClass nfs-csi` sont alors montés sur le serveur NFS. A l'issue de cette installation, j'ai réalisé des tests de performance des disques. Pour cela, j'ai utilisé les commandes `hdparm` et `fio`. J'ai également créé un pod fictif utilisant la `StorageClass nfs-csi` afin de tester l'apparition du `Physical Volume Claim` sur le serveur NFS.

3.9 Les ressources Kubernetes

J'ai participé à l'installation de nombreuses ressources du Cluster Kubernetes. Toutes ces ressources on été installées avec le provider "Helm" de Terraform.

3.9.1 Ingress Controller

Un `Ingress` est un composant Kubernetes qui permet de relier une URL à un service. Un `IngressController` est un composant qui permet de piloter l'implémentation de l'ensemble des Ingress. L' `IngressController` va gérer le traffic externe au cluster vers l'ensemble des PODS.

L'image ci-dessous présente le fonctionnement de l' `IngressController` d'Nginx:

3.9.2 Cert Manager

Cert manager permet la centralisation des demandes de certificats pour les différentes ressources du cluster Kubernetes. Cela simplifie la mise en place, le renouvellement et l'utilisation des certificats.

Figure 30: Schéma de l'IngressController Nginx provenant de la documentation Nginx

3.9.3 Rancher

Rancher est une application qui permet de nombreuses possiblités dans un cluster Kubernetes: managements des ressources, droits utilisateurs, règles réseaux etc. Rancher fournit une interface WEB optimale pour la gestion d'un cluster.

Terraform m'a également permis de configurer les accès utilisateurs à l'application de Rancher ainsi que la création des namespaces prod, qualif et test.

3.9.4 Monitoring

Je n'ai pas travaillé sur la partie interface de monitoring. A titre indicatif, les solutions utilisées sont: Alertmanager, Grafana et Prometheus.

3.9.5 Journaux de log

La gestion de l'ensemble des logs se fait avec Loki. Loki est un système d'agrégation de journaux inspiré de Prometheus. Il est utilisé en combinaison de Grafana.

Figure 31: Interface Rancher de l'infrastructure Kubernetes du projet Dehon

3.9.6 Sauvegardes

La solution de backup retenue est Velero. C'est une solution de backup opensource dédié à Kubernetes. Cette solution permet le disaster recovery, la migration des données et leur protection.

Pour externaliser les sauvegardes, j'ai utilisé minIO. MinIO est un serveur compatible S3 facile à mettre en oeuvre. Un serveur S3 est un serveur de stockage sous forme d'objet manipulable via HTTP. Ainsi, on intéragit avec les objets avec des requêtes PUT, GET, DELETE etc.

3.9.7 Base de données MongoDB et MongoArbiter

Il faut garder à l'esprit qu'en cas de désastre, l'applicatif doit basculer l'écriture des données d'une base de données présente sur le premier cluster vers une autre base sur le cluster de Backup. Ce mécanismes est pris en compte avec MongoDB avec un composant MongoArbiter. MongoArbiter permet de simplement déclarer la base de données dans laquelle l'applicatif doit écrire.

Après l'installation de la machine virtuelle comme à son habitude avec Terraform, j'ai automatisé l'installation de l'Arbiter avec Terraform sur celle-ci. L'arbiter est dans une application docker. L'utilisation des commandes docker et docker-compose n'est pas prise en compte par défaut avec Ansible. Il est nécessaire dans un premier temps d'installer l'utilitaire `pip` et les modules `docker` et `docker-compose`.

Avec ce module, j'ai créé une tâche Ansible qui lance la création d'un conteneur à partir de l'image `killercentury/mongo-arbiter`. J'ai ajouté dans la section `environnement` les identifiants de connexion à la base de données maître ainsi que son URL.

3.10 Bilan

Ce projet a été extrêment enrichissant sur de nombreux points. Il a tout d'abord renforcé mes compétences dans l'utilisation d'Ansible et Terraform avec des besoins plus compliqués que ce que j'avais pu mettre en oeuvre précédemment.

De plus, le projet portant sur Kubernetes, j'ai pu mettre oeuvre les compétences acquises en cours. Cela m'a permis de renforcer mes compétences sur Kubernetes tout en les développant grâce à la découverte de nouveaux composants Kubernetes. J'ai vu la différence entre le cluster mis en place lors de cours et celui d'un cluster de production. Cela m'a permis de découvrir les helm, Kubespray, k9s etc.

Du début à la fin, j'ai pu travailler sur la mise en oeuvre de chaque étape d'une infrastructure: réseau, sécurité, supervision, sauvegarde, tests, redondance etc. J'ai observé tout le cheminement de pensée permettant de répondre à un besoin spécifique. Cela m'a permis de prendre du recule sur comment concevoir une architecture de A à Z.

4 Procédure d'arrivée

4.1 Objectif

L'arrivée d'une nouvelle personne au sein d'Empreinte Digitale nécessite l'installation et la configuration de nombreux logiciels. Une procédure existait déjà mais elle n'était pas exhaustive. L'objectif est d'étoffer l'existant afin de fluidifier l'arrivée d'un nouvel employé plus fluide.

4.2 Description

La documentation interne se trouve sur deux Wiki.js. Le premier est destiné à l'ensemble des salariés et le second concerne uniquement les sysadmins. La nouvelle documentation étant destiné uniquement aux sysadmins, celle-ci est sur le second wiki.js.

Précédemment, lorsqu'un nouvel employé arrivait, il lui appartenait de suivre la documentation interne pour installer les applications nécessaires. Aujourd'hui, lorsqu'un nouveau salarié arrive, tout est déjà prêt et il possède les accès minimum.

4.3 Documentation

J'ai rédigé un ensemble de fichier Markdown pour la documentation. On compte en tout 14 fichiers dont certaines sont spécifiques au rôle de l'employé dans l'entreprise.

La première partie concerne le matériel adapté aux besoins du nouveau salarié. En effet, en amont de son arrivée, le nouvel arrivant est contacté afin qu'il spécifie le matériel avec lequel il souhaite travailler : nombre d'écrans, taille de PC, système d'exploitation etc. La seconde partie décrit la création de comptes mail, LDAP etc. et le paramétrage des droits. Une fois cela déterminé, il convient de procéder à l'installation et au paramétrage de l'ensemble de près d'une dizaine d'applications. Cela comprend une petite dizaine d'applications.

L'installation d'un nouveau poste prend 2 heures mais j'y consacrais plus de temps car je rédigeais en même temps la documentation. Faute de documentation, il me fallait en outre rechercher les informations nécessaires.

4.4 Groupe de Travail Embarquement

Lorsqu'une problématique générale survient comme celle de la gestion des nouveaux arrivants, des groupes de travail (GT) se forment pour discuter et mettre en oeuvre une solution. Étant la personne en charge de l'installation des PCs pour les nouveaux arrivants, j'ai représenté la partie sysadmin au GT embarquement qui porte sur l'intégration et les prépratifs à une nouvelle arrivée. Le groupe de travail était constitué d'un sysadmin (moi), une RH et trois développeurs.

Celui-ci s'est conclue par l'ajout de nouvelles installations telles que docker, un système de bookmarks etc.

5 Autres

5.1 Commandes Linux

En 2ème année de cycle ingénieur, nous avons suivi des cours d'administration des systèmes Linux. Lors de mon stage, je n'ai travaillé que sur des OS Linux. Cela m'a permis de développer mes compétences sur ce domaine en découvrant de nombreux outils.

Ci-après, quelques commandes que je ne connaissais pas:

- `dig, nslookup`: outils permettant le questionnement sur un lien vers un serveur DNS.
- `dmesg`: affiche les logs du "kernel ring buffer" = espace mémoire qui contient les messages du noyau.
- `smartctl`: permet d'afficher des informations sur un disque dur.
- `env`: print les variables d'environnement du système.
- `dpkg-reconfigure`: permet de reconfigurer un paquet déjà installé.
- `zsh`: interpréteur de commandes, tout comme bash.
- `brctl`: permet de configurer les interfaces de bridges.
- `history`: permet de récupérer l'historique des commandes utilisées.
- `arp-scan`: utilise le protocole arp pour découvrir et marquer des hôtes IP sur le réseau local.
- `tcp-dump`: analyseur de paquets en ligne de commande.
- `tmux`: terminal multiplexeur.
- `time`: affiche un résumé des ressources utilisées par le système
- `iptables-save`: permet de faire un dump de l'ensemble des règles iptables
- `watch`: permet d'exécuter une commande en affichant directement la sortie.
- `docker-compose down -v`: stoppe tous les service et détruit les volumes.
- `blkid`: affiche les informations sur les block devices de la machine.
- `fio`: outils pour produire des écritures ou des processus d'entrées/sorties spécifié par l'utilisateur.
- `lsmod`: affiche la liste des modules du noyau chargés en mémoire.

Je tiens un fichier de l'ensemble des commandes que je ne connais pas. J'y note la description et parfois des exemples ou contextes d'utilisation.

5.2 Tmux

L'outil qui a totalement changé mon utilisation et mon efficacité sur une console est Tmux. Tmux est un multiplexeur de terminal. C'est-à-dire que depuis une même fenêtre je peux avoir plusieurs terminaux d'ouverts en même temps. Je peux agir sur le nom, la taille, le découpage etc. C'est un outil qui s'utilise uniquement avec des raccourcis clavier. Cela demande une période d'adaptation mais une fois maîtrisé le gain de temps est considérable.

Figure 32: Interface Tmux avec trois fenêtres

Un autre outil très utile tous les jours est l'interpréteur ZSH. C'est un interpréteur paramétrable avec beaucoup de fonctionnalités. Il est notamment intéressant dans l'utilisation de Git en terminal.

Figure 33: Interface zsh dans un dossier Git

5.3 K9s

Enfin, l'outils K9S est très pratique dans l'utilisation de Kubernetes. Il permet de facilement visualiser l'ensemble des informations d'un cluster et donne la possiblité d'agir dessus. On peut détruire, créer ou éditer des ressources directement depuis l'interface.

Dans le cadre du projet Dehon, je n'ai pas eu à m'en servir souvent. Cependant, pour les tâches à venir, je sais que c'est un outil que pourrais être amené à utiliser quotidiennement.

```
Context: kubernetes-admin-cluster.local@cluster.… <0> all       <a>      Attach     <l>       Logs
Cluster: cluster.local                             <1> default   <ctrl-d> Delete     <p>       Logs P
User:    kubernetes-admin-cluster.local                          <d>      Describe   <shift-f> Port-F
K9s Rev: v0.26.0 ⚡v0.26.3                                       <e>      Edit       <s>       Shell
K8s Rev: v1.23.7                                                 <?>      Help       <n>       Show N
CPU:     7%                                                      <ctrl-k> Kill       <f>       Show P
MEM:     52%

                                        Pods(all)[94]
NAMESPACE↑                 NAME                                          PF READY RESTARTS STATUS     CPU  MEM /R
backup                     debug                                         ● 1/1          0 Running      0    7 /a
backup                     minio-9554548b5-dsjc2                         ● 1/1          0 Running      2  165 /a
backup                     velero-d6844698b-lr5cs                        ● 1/1          0 Running      8  101  1
cattle-fleet-local-system  fleet-agent-699b5fb945-lz2bt                  ● 1/1          1 Running      6   99 /a
cattle-fleet-system        fleet-controller-784d6fbcd8-bmx5x             ● 1/1          1 Running      5   80 /a
cattle-fleet-system        gitjob-6b977748fc-p2r7h                       ● 1/1          1 Running      2   55 /a
cattle-monitoring-system   alertmanager-rancher-monitoring-alertmanager-0 ● 2/2          0 Running      1   45  0
cattle-monitoring-system   loki-distributed-distributor-6fffdcd6d9-z2rm5 ● 1/1          0 Running      8   38 /a
cattle-monitoring-system   loki-distributed-gateway-85569f4c77-fbw2m     ● 1/1          1 Running      2   10 /a
cattle-monitoring-system   loki-distributed-ingester-0                   ● 1/1          0 Running      6  300 /a
cattle-monitoring-system   loki-distributed-querier-0                    ● 1/1          0 Running      5   38 /a
cattle-monitoring-system   loki-distributed-query-frontend-56fb7b9fb9-8vbcz ● 1/1        0 Running      1   42 /a
cattle-monitoring-system   prometheus-rancher-monitoring-prometheus-0    ● 3/3          0 Running    248 1196 29
cattle-monitoring-system   promtail-4znfd                                ● 1/1          0 Running      8  104 /a
cattle-monitoring-system   promtail-22977                                ● 1/1          0 Running     13   79 /a
cattle-monitoring-system   promtail-bbrhz                                ● 1/1          0 Running     16  125 /a
cattle-monitoring-system   promtail-bpjg4                                ● 1/1          0 Running     12  156 /a
cattle-monitoring-system   promtail-crp79                                ● 1/1          0 Running     10   96 /a
cattle-monitoring-system   promtail-kzcxv                                ● 1/1          0 Running     18  143 /a
cattle-monitoring-system   rancher-monitoring-grafana-74c4fb795f-xnz2n   ● 3/3          2 Running     11  130 11

<pod>

0  0 HOME  1 ssh  2 zsh  3 k9s                                  2022-08-11  14:59  lefay
```

Figure 34: Visualisation des pods avec K9s

Vim est le prochain outil à prendre en main.

Partie V : Bilan personnel

Cela fait maintenant 1 an que je suis chez Empreinte Digitale et cette année fût passionnante. Dès mon arrivé, j'ai beaucoup apprécié le modèle d'une petite entreprise d'une cinquantaine de salarié sur un fonctionnement associatif. Ayant passé 4 années dans le milieu associatif avec le BDE de l'école, j'adhére complétement au modèle de SCOP.

Lors de mon précédent stage, du fait de la crise sanitaire, je n'avais pas eu l'occasion d'une expérience de stage "normal". Je n'avais pas pu partir à l'étranger ou être en entreprise. Les complications dans la recherche de stage technique m'avaient ammenées à réaliser mon stage dans l'incubateur de l'ESEO d'Angers. J'avais alors le sentiment d'aller en stage comme j'irais à l'école.

Dès les premiers cours de réseau en 1ère année de cycle ingénieur, j'ai su que c'était le domaine dans lequel je voudrais travailler. Je suis très heureux qu'à l'issue de mon stage technique j'ai pu rentrer dans l'option Cloud Système et Sécurité. J'y ai appris de nombreuses bases qui m'ont amplement permis de m'en sortir durant mon alternance.

Terminer cette dernière année d'étude à l'ESEO en contrat de professionnalisation était la meilleure chose possible. Durant la période d'alternance, j'ai eu le temps de me cultiver sur les domaines de l'infrastructure et la sécurité. J'y ai renforcé mes connaissances théoriques sur le sujet. Cette période n'était pas forcément évidente. En effet, le fonctionnement de l'alternance avec seulement deux jours par semaine en entreprise rend l'intégration en entreprise compliquée.

Mon expérience lors de la période de stage a été beaucoup plus enrichissante. Ces sept mois fûrent pour moi l'occasion de mettre en pratique de nombreux outils. Mon rapport fait état de Docker, Kubernetes, Proxmox et Ansible mais j'ai appris bien plus. Ces travaux, associés à divers autres tâches, m'ont fait approfondir mes connaissances sur des éléments de bases : pare-feu, DNS, DHCP, VRRP, VoIP etc. On m'a également laissé le temps de faire de la veille sur des technologies que je ne connaissais pas: Puppet, Chef, Salt, Jenkins, Oauth, etc.

Parmi l'ensemble de mes travaux, j'ai particulièrement apprécié ceux présentés dans la partie IV. Bien que mon sujet portait sur la sécurité, j'étais très heureux d'avoir été intégré sur ces tâches. Je n'ai pas d'appétence particulière pour le milieu de la sécurité, ce qui m'intéresse le plus est la partie infrastructure. Cela fait echo au fait que j'ai choisis l'axe infrastructure parmi les axes disponibles en option CSS.

Mon aventure chez Empreinte Digitale ne s'arrête pas. J'ai signé un contrat en CDD de 6 mois. Durant les mois à venir, je vais me distancer des travaux de sécurité pour travailler des projets cloud.

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 dans 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 sécurité à appliquer.
4	Gestion des actifs	Le matériel du personnel ainsi que toutes autres machines sur lesquelles reposent l'exploitation du SI doit être inventoriés.
5	Contrôle d'accès et gestion des identités	L'utilisation du SI doit se faire de manière à pouvoir a tout moment identité une personne l'exploitant. Même si cela peut être contraignant dans l'exploitation, il n'est pas question d'ouvrir les accès à une ressource 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 cryptographiques sécurisés doivent être employés lors de l'utilisation de protocoles tels que TLS, IPsec ou SSH.
7	Sécurité physique et environnementale	La sécurité des logiciels n'est pas suffisante. Un aspect réglementaire oblige le découpage de zone d'accès aux différents 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	I y a de nombreuses règles lié à l'exploitation. Celles-ci sont généralement liées aux autres sections du glsPSSI 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 nécessitent des configurations supplémentaires. Cela concerne les réseaux Wifi et 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 mais également ardue concerne la maintenance du système existant. Il s'agit de garder les systèmes à des niveaux de sécurité satisfaisants 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 ont 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 lister 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 compte 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 ce qui est 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 supplémentaires 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,

paul.lefay@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 infrascrture 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 cafétéria, d'un local ainsi que de la location d'un camion

BDE ESEOKAMI - Mandat 2019-2020
Membre du Bureau Des Etudiants en tant que Trésorier
Gestion d'un budget de 150 000 euros
Gestion financière d'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.
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 inconnus.
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 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 jour 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 médicale 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 sur le PSSI. Réunion de présentation finale 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 2021. 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'une pile 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 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 automatisé 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. Modification de différents problèmes empêchant l'installation des agents OCSInventory. Installation d'une nouvelle instance d'un site internet pour réaliser des Webinaires.

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 jour 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 plateforme 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 jour l'ensemble des Vhosts. En congé le vendredi 20. Début des mise à jour 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 jour l'ensemble des Vhosts. Poursuite des mise à jour 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 matière de sécurité des différentes machines et automatisation 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 d'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 six 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 des 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 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. Ajout d'un second disque et donc recréation d'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 trois 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 jour 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. Congés maladie pour Covid.
32	01/08/22 - 07/08/22	Rapport de stage et congé jusqu'à la rentrée.

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

Tickets réalisés lors de la période de stage

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
TOTAL	136,67	162,66	133,00	126,00	154,00	127,08	839,41
DATACENTER	83,50	154,66	64,25	14,50	12,00	0,17	329,08
Nom de domaine pour page Assistant RGAA	1,00						1,00
Déplacement datacenter 2022			4,00		7,00		11,00
Réunions internes Datacenter 2022	2,33						2,33
Installation Ceph sur le cluster de Test Proxmox	11,00	16,00					27,00
Installation Framemo	3,00						3,00
Installation de GLPI	23,00	4,50					27,50
Remplacement du disque	0,50						0,50
Installation de la derniére version	4,50						4,50
Compréhension du fonctionnement de GLPI	1,00						1,00
Installation du plugin OCS-Inventory	4,67						4,67
Ajout GLPI de la base de données OCSInventory et import de l'ancienne base de données	4,50						4,50
Configuration pour l'affectation aux entités	7,00	1,50					8,50
Configuration des éléments é importer		4,00					4,00
Configuration des dictionnaires	17,50						17,50
Install NocoDB		5,50					5,50
Mise en place du SNMP		13,00					13,00
Installation serveur de CVE	3,00						3,00
Rendez-vous suivi de stage école avec tuteur école	0,50						0,50
Reprise générale de la documentation lié au datacenter		24,50	31,00	4,00			59,50
HTTPS et certificat auto-signé pour OCSInventory		5,00					5,00

Table 10: Tickets réalisés lors de la période de stage - Partie 1

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
Documentation audit de sécurité		5,00					5,00
Réinstallation cluster Proxmox Angers		8,50					8,50
Installation pour Audit de sécurité		25,67					25,67
Ajout de l'ensemble des salariés		1,50					1,50
Installation PC de télé-travail pour Clélia		2,50					2,50
Mise en place local d'Ansible et reprise des travaux de Raphaél		5,00					5,00
Ajout des machines d'Angers sur OCSInventory via Ansible		7,00	7,00				14,00
Streaming d'un webinaire pour l'URSCOP le 12 mai				1,50			1,50
Ajout des machines de Tours sur OCSInventory via Ansible			1,00				1,00
Ajout des machines de Rennes sur OCSInventory via Ansible			4,00				4,00
Veille Kubernetes			11,75				11,75
Montée de version superset			1,50				1,50
Compréhension et configuration pour relier les DC d'Angers et Tours			4,00				4,00
Installation Zammad sur Tours				2,00			2,00
Mise en place d'une plateforme Peertube et tests streaming				7,00			7,00
Post it pour les JL 2022					2,00		2,00
Creation Compte mail associes@empreintedigitale.fr					1,00		1,00
Odoo test erreur 502 Bad Gateway					1,00		1,00
Faire une documentation sur automatiser le lancement de linphone ou jitsi au démarrage du PC					1,00		1,00
Procédure migration des mails						0,08	0,08
Adresse mail alias ne fonctionne pas						0,08	0,08
SADEL		0,50					0,50
Ouvertures accés bitwarden / gitlab ALI		0,50					0,50

Table 11: Tickets réalisés lors de la période de stage - Partie 2

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
RH	4,00		2,00	5,00	5,00	1,50	17,50
Procédure nouvel arrivant - Axel Liszkowski	4,00						4,00
Procédure nouvel arrivant : Marie ANDRE			2,00				2,00
Présentation des outils et configurations pour Marie André				3,00			3,00
Procédure Arrivé Bertrand Raes				2,00			2,00
Procédure départ Jochen Rousse						0,50	0,50
Arrivée Samuel MASSON					5,00		5,00
Arrivée Rodolphe REMY						0,50	0,50
Procédure nouvel arrivant : Thibault Dequidt						0,50	0,50
Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
FOURNITURES						1,00	1,00
Préparation de la commande pour les arrivé d'aout et septembre						1,00	1,00
AD07	0,50						0,50
Nombre de téléchargement	0,50						0,50
AD33				3,00			3,00
PAS Département de la gironde				3,00			3,00
Pôle sécurité			1,00				1,00
Réunion / Ateliers Sécurité			1,00				1,00
Fonctionnement interne			18,08	87,50			105,58
Linphone			0,08				0,08
Audit usage cpu / ram / disques par client			18,00	55,50			73,50
Mise en place d'un second Bastion SSH				18,00			18,00
Mise é jours des instances BBB d'Angers				14,00			14,00
Agence Lucie	2,33						2,33
Probléme de langue certificat	2,00						2,00
Demande d'installation d'un plug-in moodle	0,33						0,33

Table 12: Tickets réalisés lors de la période de stage - Partie 3

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
Fibat			0,25				0,25
Questions Divers			0,25				0,25
Cybersécurité	46,33	7,50	34,00	12,00	59,00	13,00	171,83
Analyse état actuel de l'infrastructure	3,00						3,00
POC Site Web monitoring/push	8,00						8,00
Installation OpenVAS	13,00						13,00
Mise à jours du tableau de suivi d'audit	14,00						14,00
POC DeepFence	2,00						2,00
Recherches de solutions d'audit de sécurité	2,00						2,00
Rapport de stage	3,00	5,50	1,00	1,00	13,50	10,00	34,00
Installation Log4j-RCE-Scanner	1,33						1,33
Installation locale avec test sur la machine OCS Inventory		2,00					2,00
Outils d'audit de sécurité automatisée			30,00				30,00
Parcours et recherche d'outils d'audit de sécurité			3,00				3,00
Découverte de l'outil en ligne de commande, installations tests - Automatisation via Ansible de l'installation				7,00			7,00
Création d'une archive .dev é partir des ressources pour l'installation sur les machines Debian dont la version est supérieure é 10				4,00			4,00
Création d'un role Ansible pour automatiser la récupération de document d'audit et l'application de correctifs					29,00		29,00
Test et corrections					10,00		10,00
Checklist de sécurité basé sur le bilan de l'audit de sécurité					1,50		1,50
Tests divers avec snort					1,00		1,00

Table 13: Tickets réalisés lors de la période de stage - Partie 4

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
Installation d'un Zammad pour Stratosfair					3,00		3,00
Réunion de restitution avec cogent					1,00		1,00
Suivi des travaux de valentin sur l'URSSAF						3,00	3,00
Réunions transverses						7,00	7,00
Divers réunions internes (transverses)						7,00	7,00
Groupe de travail						2,00	2,00
[Dev] GT Embarquement						2,00	2,00
Marketing et Commercial				1,00			1,00
Page webinaire pour le 12 mai				1,00			1,00
Marketing et Commercial - A11Y				1,00			1,00
Webinaire Lucie 20 mai				1,00			1,00
Marketing et commercial - RGPD					0,50		0,50
Webinaire RGPD Lucie le 7 juin					0,50		0,50
Iresa					16,00	0,92	16,92
Agenda Nextcloud et emails sur smartphone					16,00	0,92	16,92
J aime mes dents			13,42			2,00	15,42
Zammad			0,75				0,75
Nextcloud + collabora			12,67				12,67
Pas de proposition de répondre aux tickets par email sur Zammad						2,00	2,00
INSERM CLOUD				2,00	2,00		4,00
Création d'un petit redmine pour l'inserm - redmine.inserm.cloud-ed.fr				2,00	2,00		4,00

Table 14: Tickets réalisés lors de la période de stage - Partie 5

Demande	Février	Mars	Avril	Mai	Juin	Juillet	Temps total
Dehon with cyres					49,50	61,50	111,00
Installation machines Cogent						7,00	7,00
Déploiement des VMs avec le versionning dans TF					11,00		11,00
Configuration des VMs avec Kubespray en version 1.23.7 de kube					15,00		15,00
Configuration HA du cluster kube (Haproxy en gateway api)					18,50		18,50
Configuration des composants					4,00	17,50	21,50
Création du stockage						31,00	31,00
Install WikiJs					1,00		1,00
Rédaction de la documentation technique du projet						6,00	6,00
Region Normandie					10,00	5,00	15,00
Nom du service : matomo Nom du client : Région Normandie					10,00	5,00	15,00
AICLA						33,00	33,00
Install Nextcloud						33,00	33,00
TOTAUX	136,67	162,66	133,00	126,00	154,00	127,08	839,41

Table 15: Tickets réalisés lors de la période de stage - Partie 6

Bibliographie

[1] *Scop*, https://www.les-scop.coop/les-scop, site vitrine du mouvement SCOP.

[2] *Label lucie*, https://www.labellucie.com/, site vitrine du label Lucie.

[3] *Openscap*, https://www.open-scap.org/, site vitrine d'OpenSCAP.

[4] *Scaleway*, https://blog.scaleway.com/fr/comprendre-les-differents-types-de-stockage/, comprendre les différentes types de stockage.

[5] *Empreinte digitale*, https://empreintedigitale.fr/, site vitrine d'Empreinte Digitale.

[6] *Wikipédia*, https://fr.wikipedia.org/wiki/Accueil, encyclopédie libre.

[7] *Sharepoint*, https://reseaueseo.sharepoint.com/sites/etu/, ressources pour les étudiants de l'ESEO.

[8] *Docker hub*, https://hub.docker.com/, dépôt publique d'images Docker.

[9] *Github*, https://github.com/, dépôt de code source.

[10] *Gitlab*, https://git.vtech.fr/, dépôt de code source.

[11] *Ligeo*, https://www.ligeo-archives.com/, site vitrine du produit Ligeo Archive.

[12] *Design4green*, https://design4green.org/, site vitrine du Design4Green.

[13] *Stratosfair*, https://stratosfair.com/, site vitrine de Stratosfair.

[14] *Proxmox*, https://pve.proxmox.com/pve-docs/index.html, documentation de Proxmox.

[15] *Terraform*, https://www.terraform.io/docs, documentation de Terraform.

[16] *Ansible*, https://docs.ansible.com/, documentation d'Ansible.

[17] *Stackoverflow*, https://stackoverflow.com/, site d'entre-aide pour développeurs.

[18] *Anssi*, https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/, regroupement des bonnes pratiques pour les entreprises dans l'usage du numérique.

[19] *Ocsinventory*, https://wiki.ocsinventory-ng.org/, documentation d'OCSinventory.

[20] *Glpi*, https://glpi-install.readthedocs.io/en/latest/, documentation de GLPI.

[21] *Fusioninventory*, http://fusioninventory.org/, site vitre de FusionInventory.

[22] S. Robert, *Ansible cmdb*, https://blog.stephane-robert.info/post/ansible-cmdb/, tutorial d'utilisation d'Ansible CMDB.

[23] *Escalidraw*, https://excalidraw.com/, application de création de diagramme sous forme de dessin.

[24] *Wiki ubuntu*, https://doc.ubuntu-fr.org/tutoriel/creation_deb, création d'un paquet deb à partir d'une archive.

[25] *Wikijs*, https://docs.requarks.io/, documentation de Wikijs.

[26] *Nextcloud*, `https://docs.nextcloud.com/`, documentation de Nextcloud.

[27] *Awx*, `https://docs.ansible.com/ansible/latest/collections/awx/awx/index.html`, documentation d'AWX.

[28] *Ceph*, `https://docs.ceph.com/en/quincy/`, documentation de Ceph.

[29] *Kubespray*, `https://github.com/kubernetes-sigs/kubespray/`, ressource de l'outil kubespray.

[30] *Haproxy*, `https://www.haproxy.com/documentation/hapee/latest/onepage/`, documentation de Haproxy.

[31] J. Dordoigne, *Réseau informatique - Notions fondamentales*, Eni, Ed. 2022.

[32] *Nfs*, `https://docs.outscale.com/fr/userguide/Mettre-en-place-un-serveur-NFS.html`, mettre en place un stockage NFS.

[33] *Ingress controller nginx*, `https://docs.nginx.com/nginx-ingress-controller/`, mettre en place un Ingress Controller Nginx.

[34] *K9s*, `https://github.com/derailed/k9s`, code source de k9s.

Liste des figures

1 Logos des prestations d'Empreinte Digitale . . . 11
2 Les étapes du passage en SCOP d'Empreinte Digitale . . . 12
3 Schéma de la gouvernance chez Empreinte Digitale . . . 13
4 Application web réalisé par Empreinte Digitale pour le Design4Green . . . 14
5 Maquette en trois dimensions du datacenter de Stratosfair . . . 15
6 Workflow de Terraform . . . 20
7 Extrait du tableau de suivi de sécurité . . . 22
8 Architecture entre OcsInventory et GLPI . . . 23
9 Interface de l'application GLPI . . . 24
10 Interface de l'application OCSInventory . . . 25
11 Diagramme de séquence de l'installation d'un agent avec Ansible . . . 28
12 Diagramme de séquence du fonctionnement d'Ansible avec OpenSCAP . . . 31
13 Interface web de l'application Wiki.js . . . 33
14 Schéma applicatif de Nextcloud avec Collabora . . . 36
15 Interface web d'AWX . . . 38
16 Diagramme de séquences des tâches Ansible lors de l'installation de Nextcloud . 39
17 Carte fibre 1 Gigabytes . . . 41
18 Carte fibre 10 Gigabytes . . . 41
19 Câble réseau RJ45 . . . 42
20 Câble réseau SFP+ . . . 42
21 Disque HDD de 6To . . . 42
22 Disque SSD de 500Go . . . 42
23 Configuration réseau de Proxmox à l'installation . . . 43
24 Interface du cluster Proxmox an-virt-pmx . . . 44
25 Représentation des types de storage par Scaleway's [4] . . . 45
26 Disques présents sur le noeud an-virt-pmx-1 . . . 46
27 Ensemble des OSD du cluster an-virt-pmx . . . 46
28 Infrastructure sur trois sites physiques du projet Dehon . . . 49
29 Cluster Kubernetes de dehon sur virt2-prd-pmx . . . 50
30 Schéma de l'IngressController Nginx provenant de la documentation Nginx . . . 55
31 Interface Rancher de l'infrastructure Kubernetes du projet Dehon . . . 56
32 Interface Tmux avec trois fenêtres . . . 60
33 Interface zsh dans un dossier Git . . . 60
34 Visualisation des pods avec K9s . . . 61

Liste des tables

1 Machines virtuelles créées pour les tests avec OpenSCAP 30
2 Les 16 thématiques de sécurité - Partie 1 63
3 Les 16 thématiques de sécurité - Partie 2 64
4 Planning du travail effectué sur la période de d'alternance - Partie 1 66
5 Planning du travail effectué sur la période de d'alternance - Partie 2 67
6 Planning du travail effectué sur la période de stage - Partie 1 68
7 Planning du travail effectué sur la période de stage - Partie 2 69
8 Planning du travail effectué sur la période de stage - Partie 3 70
9 Planning du travail effectué sur la période de stage - Partie 4 71
10 Tickets réalisés lors de la période de stage - Partie 1 72
11 Tickets réalisés lors de la période de stage - Partie 2 73
12 Tickets réalisés lors de la période de stage - Partie 3 74
13 Tickets réalisés lors de la période de stage - Partie 4 75
14 Tickets réalisés lors de la période de stage - Partie 5 76
15 Tickets réalisés lors de la période de stage - Partie 6 77

Acronymes et définition

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

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

A

Alma Distrubtion Linux. Système d'exploitation d'entreprise de niveau production soutenu par la communauté et compatible binaire avec Red Hat Enterprise Linux 69, 81

Ansible Ansible est une plateforme logicielle libre pour la configuration et la gestion des ordinateurs 3, 21, 27, 28, 30, 31, 35, 37–40, 52–54, 56, 57, 62, 69–71, 79, 81

Ansible CMDB Ansible est une plateforme logicielle libre pour la configuration et la gestion des ordinateurs. Elle permet notamment de récupérer les informations des machines et d'en faire une synthèse dans une page web 22, 34, 66, 67, 81

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information. Organisme Français expert dans le domaine de la sécurité 8–10, 18, 22, 66, 81

Apache Serveur HTTP libre créé et maintenu au sein de la fondation Apache 70, 81

API Application Programming interface. 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. 15, 19, 52, 53, 71, 81

apt Advanced Packaging Tool. Gestionnaire de paquets utilisé par Debian et ses dérivés 31, 81

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 81

Bastion SSH Un bastion SSH est une brique d'infrastructure qui permet à une connexion SSH de "rebondir" avant d'atteindre sa cible 32, 70, 81

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, des présentations avec ou sans tableau blanc 70, 81

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 » 81

C

Calico Calico est un des nombreux CNI disponibles pour Kubernetes 70, 81

CentOS Distribution Linux. CentOS est une distribution GNU/Linux destinée aux serveurs 69, 81

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 19, 44–47, 68, 81

CLI Command Line Interface. Interface en ligne de commande 30, 81

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 11, 81

cluster Groupement de serveurs et d'autres ressources qui agissent comme un système unique et permettent une haute disponibilité 15, 19, 25, 35, 41, 44, 46–49, 51, 52, 54–57, 61, 68–71, 79, 81

CNI Container Network Interface. De façon simplifiée, 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 70, 81

Collabora Collabora est une suite bureautique en ligne basé 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. 8, 35, 36, 69, 79, 81

CVE Common Vulnerabilities and Exposures. Dictionnaire des informations publiques relatives aux vulnérabilités de sécurité 18, 68, 81

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 68, 81

Debian Debian est un système d'exploitation Linux composé exclusivement de logiciels libres, développés par le Debian Project. Chaque version majeure de Debian possède une dénomination : Buster pour la version 10, Bulleyes pour la version 11 etc. 31, 43, 81

DeepFence Deepfence est une solution de prévention et de détection de sécurité essentielle pour les environnements cloud et conteneurs natifs 81

DevOps Mouvement en ingénierie informatique et une pratique technique visant à l'unification du développement logiciel et de l'administration des infrastructures informatiques, notamment l'administration système 8, 81

DHCP Dynamic Host Configuration Protocol. 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 68, 81

DNI Détecteur de Niveau Intelligent 48, 81

DNS Domain Name System. Service informatique qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements 43, 59, 81

Docker Docker est une plateforme permettant de lancer certaines applications dans des conteneurs logiciels 62, 70, 81

Docker-compose Docker-compose, un outil pour déployer plusieurs conteneurs en même temps. En résumé, il faut retenir que Docker-compose permet de gérer un ensemble de conteneurs (services) 81

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 66, 81

E

ESEO École Supérieure d'Électronique de l'Ouest. Dans le présent rapport, il est fait mention d'ESEO Angers 2, 81

F

FileSystem Système de fichiers. Organisation des fichiers au sein d'un volume physique ou logique, qui peut être de différents types, et qui a également une racine mais peut en avoir plusieurs 47, 81

Framemo Application de tableau blanc avec des colonnes pour y déposer des postits 70, 81

G

GitLab GitLab est un logiciel libre de forge basé sur git proposant les fonctionnalités de wiki, un système de suivi des bugs, l'intégration continue et la livraison continue 20, 35, 38–40, 81

GLPI Gestionnaire Libre de Parc Informatique. 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 8, 9, 23–25, 29, 68, 79, 81

H

Haproxy High Availability Proxy. 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 71, 81

HDD Hard Disk Drive. Mémoire de masse à disque tournant magnétique utilisée principalement dans les ordinateurs 42, 81

Helm Helm est un outil d'empaquetage open source qui vous aide à installer et à gérer le cycle de vie d'applications Kubernetes 81

HTML HyperText Markup Language. Langage de balisage conçu pour représenter les pages web 81

HTTP Hypertext Transfer Protocol. Protocole de communication client-serveur 81

HTTPS HyperText Transfer Protocol Secure. 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 68, 81

I

IaC Infrastructure as Code. Consiste à gérer et à approvisionner une infrastructure à l'aide de code 20, 81

IP Internal Protocole. 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 38, 39, 43, 44, 51, 53, 59, 68, 81

IPsec Internet Protocol Security. Regroupe un ensemble de protocoles, qui utilisent des algorithmes destinés à transporter des données sur un réseau de façon sécurisée 66, 81

ISO Optical disc image. Image de disque qui contient tout ce qui serait écrit sur un disque optique, secteur de disque par secteur de disque, y compris le système de fichiers du disque optique 14, 43, 47, 81

J

Jinja Jinja est un moteur de templates pour le langage de programmation Python. Il aurait inspiré Twig, moteur de template PHP 35, 37, 53, 81

JSON JavaScript Object Notation. Format de données textuelles dérivé de la notation des objets du langage JavaScrip 26, 81

K

Kubernetes Kubernetes est un système open source qui vise à fournir une « plateforme permettant d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des clusters de serveurs » 48, 50–52, 54–57, 61, 62, 69, 70, 79, 81

Kubespray Utilitaire permettant de créer un cluster Kubernetes via Ansible 52, 57, 70, 81

L

LAMP Linux Apache MySQL Php. LAMP est un acronyme désignant un ensemble de logiciels libres permettant de construire des serveurs de sites web. Linux Apache Mysql Mariadb 67, 81

LDAP Lightweight Directory Access Protocol. Protocole permettant l'interrogation et la modification des services d'annuaire électronique. 58, 81

LimeSurvey Logiciel d'enquête statistique, de sondage, et de création de formulaires en ligne 68, 81

Linux Famille de systèmes d'exploitation open source de type Unix fondé sur le noyau Linux, créé en 1991 par Linus Torvalds 8, 10, 26, 29, 30, 59, 68, 81

M

Mariadb 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 70, 81

Markdown Langage de balisage léger. Il a été créé dans le but d'offrir une syntaxe facile à lire et à écrire. Un document balisé par Markdown peut être lu en l'état sans donner l'impression d'avoir été balisé ou formaté par des instructions particulières. 58, 81

Master/Slave Le principe de Master/Slave consiste à avoir deux logiciels ou bases de données interdépendant. Ainsi, une modification apportée au Master sera automatiquement appliquée au Slave. 70, 81

Matomo Logiciel libre et open source de mesures de statistiques web, successeur de PhpMyVisites et conçu pour être une alternative libre à Google Analytics 81

Mattermost Service de messagerie instantanée libre auto-hébergeable. 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 81

Microsoft Teams Microsoft Teams est une application de communication collaborative propriétaire en mode SaaS officiellement lancée par Microsoft en novembre 2016 17, 81

Monit outil open source de surveillance des services locaux installés sur une machine Unix 25, 81

Moodle Plateforme 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 81

N

NAS Network Atached Storage. Serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes 25, 81

Nextcloud Logiciel libre de site d'hébergement de Fichiers 8, 16, 35–40, 47, 69, 71, 79, 81

NFS Network File System. Protocole permettant d'accéder à des fichiers via un réseau 54, 81

Nginx Logiciel libre de serveur Web ainsi qu'un proxy inverse 70, 81

NocoDB Outils permettant le traitement en feuille de calcul de bases de données SQL 68, 81

O

OCSInventory Open Computer and Software Inventory. 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 8, 9, 23–26, 28, 29, 68–70, 79, 81

OpenSCAP Outils pour aider les administrateurs et les auditeurs à évaluer, mesurer et appliquer les lignes de base de sécurité 8, 30–32, 70, 71, 79–81

Openvas Scanner de vulnérabilité Nessus dont le but est de permettre un développement libre de l'outil qui est maintenant sous licence propriétaire 81

OSD Object Storage Deamon. Dans ceph, un OSD est le deamon responsable du suivi des stockages sous forme d'objet 45–47, 68, 79, 81

P

PAS Plan d'Assurance Sécurité a pour but de préciser comment les prestataires se conforment aux exigences de cybersécurité 33, 81

Passhport Solution de gestion et de sécurisation des accès SSH 69, 81

Passhport Solution de gestion et de sécurisation des accès SSH. PaSSHport est un bastion SSH protégeant les accès sécurisés des systèmes d'information 70, 81

Peertube 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 70, 81

PFE Projet de Fin d'Etude. Désigne à l'ESEO à un projet d'une durée d'un semestre pouvant être effectué en entreprise ou non 3, 66, 67, 81

PHP Hypertext Preprocessor. 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 81

plateforme web Une plateforme web est un ensemble de services web. Le contenu des plateformes web provient en grande partie des utilisateurs qui peuvent diffuser et partager des contenus de nature textuelle ou multimédia 70, 81

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 70, 81

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 81

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 la faisabilité ou pas 22, 66, 67, 81

Proxmox Solution de virtualisation libre basée sur l'hyperviseur Linux KVM et offre aussi une solution de containers avec LXC 8, 15, 19, 20, 25, 30, 35, 41, 43–45, 47–49, 51, 62, 68, 71, 79, 81

Proxy Composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges 81

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 22, 33, 67, 81

PWA Une progressive web app est une application web qui consiste en des pages ou des sites web, et qui peuvent apparaître à l'utilisateur de la même manière que les applications natives ou les applications mobiles 81

R

RBAC Role-Based Access Control. Le contrôle d'accès basé sur les rôles est un modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est associé 27, 81

Redmine Application web libre de gestion de projets, développée en Ruby sur la base du framework Ruby on Rails 16, 17, 68, 81

RGPD Règlement Général sur la Protection des Données 11, 66, 81

Rocky Linux Distribution Linux. Basée sur le code source du système d'exploitation Red Hat Enterprise Linux. 69, 81

RSE Responsabilité Sociétale des Entreprises. La responsabilité sociétale des entreprises désigne la prise en compte par les entreprises, sur une base volontaire, et parfois juridique, des enjeux environnementaux, sociaux, économiques et éthiques dans leurs activités. 14, 15, 81

Rudder 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 66, 81

S

SA Société Anonyme. Société commerciale où la responsabilité est limitée jusqu'à concurrence des apports, et qui présente des caractéristiques d'une société de personnes (2 à 100 personnes), notamment parce que les parts détenues dans le capital ne sont pas librement accessibles sans accord de tout ou partie des associés. 12, 81

SARL Société à Responsabilité Limitée. Société de capitaux à risque limité répandue dans les pays de tradition civiliste 12, 81

SAS Société par Actions Simplifiée 12, 81

SCAP Security Content Automation Protocol. Ses spécifications visent à faciliter et automatiser les échanges d'informations entre les outils de sécurité pour tous les types d'équipements connectés au réseau : inventaire, vulnérabilités, éléments de configuration et de durcissement 30, 81

SCOP Société COopérative et Participative 11–13, 62, 79, 81

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 10, 18, 27, 63, 64, 66, 81

Slack Slack est une plateforme de communication collaborative propriétaire ainsi qu'un logiciel de gestion de projets 17, 81

SNMP Simple Network Management Protocol ou Protocole simple de gestion de réseau. 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 68, 81

SQL 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 68, 81

SSD Solid State Drive. Matériel informatique permettant le stockage de données 42, 81

SSH Secure SHell. Protocole de communication sécurisée basé sur un échange de clé privé et publique 66, 81

SSL Secure Sockets Layer. Protocole cryptographique le plus largement utilisé pour assurer la sécurité des communications sur Internet 68, 81

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 22, 81

T

Terraform 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 20, 47, 51, 54–57, 70, 71, 79, 81

TLS Transport Layer Security ou Sécurité de la couche de transport. Protocole de sécurisation des échanges par réseau informatique, notamment par Internet 66, 81

Traefik Reverse-proxy et un load-balancer fait pour déployer principalement des conteneurs 25, 35, 81

U

UptimeRobot Outil qui permet de surveiller et d'analyser des sites, notamment en se bassant sur le protocole HTTP 25, 81

V

Vhosts Virutal Host. 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 70, 81

VIP Virtual IP. Adresse IP virtuelle 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, 71, 81

W

Wazuh Plateforme open source utilisée pour la prévention, la détection et la réponse aux menaces 69, 81

Webinaire 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 69, 70, 81

Wifi Protocole IEEE 802.11. Ensemble de normes concernant les réseaux sans fil locaux 66, 81

Windows 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 81

Y

YesWeHack Plateforme permettant la mise en contact entre des entreprises et des hackers éthiques 66, 81

Z

Zammad Service d'assistance gratuit ou un système de suivi des problèmes 81