Institut Universitaire de Technologie,

Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année

Bachelor Universitaire de Technologie

Spécialité Réseaux et Télécommunications

parcours cybersécurité

Déploiement d'un serveur WAPT

Eliott AUROUZE

Institut de Neurosciences de la Timone

Responsable entreprise : Mr Arnaud CRUZEL

Responsable académique : Mr Éric SOCCORCI

2023

Sommaire

1 Introduction

Le présent rapport de stage décrit mon expérience de déploiement de WAPT au sein de l'Institut de Neurosciences de la Timone (INT). Ce stage, réalisé dans le cadre de ma deuxième année en réseau et télécommunications, m'a permis de mettre en pratique les connaissances acquises durant ma formation et d'approfondir mes compétences dans le domaine.

Mon tuteur de stage, Arnaud Cruzel, a été d'une grande aide dans l'encadrement direct de mes activités au sein de l'INT. Grâce à son accompagnement, j'ai pu découvrir l'environnement spécifique de l'Institut et comprendre les besoins et les attentes des utilisateurs de WAPT.

Au cours de ce rapport, je détaillerai les différentes étapes du déploiement de WAPT, en mettant l'accent sur les défis rencontrés, les solutions mises en place et les résultats obtenus. Je soulignerai également l'importance de cette expérience dans mon parcours académique et professionnel, en mettant en avant les compétences techniques et relationnelles que j'ai pu développer.

Ce rapport de stage est l'occasion pour moi de partager mon expérience, d'analyser les enseignements tirés de ce projet et de mettre en perspective les connaissances acquises au sein de mon cursus universitaire. Je suis convaincu que ce stage a été une étape cruciale dans ma formation, me permettant d'acquérir des compétences pratiques et de consolider ma passion pour les réseaux et les télécommunications.

2 Présentation de l’entreprise

2.1 Institut de Neurosciences de la Timone

L’Institut de Neurosciences de la Timone est une unité mixte de recherche du CNRS en cotutelle avec Aix-Marseille Université. L’INT est situé dans le Campus Timone de la Faculté de médecine, dans le centre de Marseille.

Dès sa création, l’INT a été organisé autour de deux principes : les équipes de recherche et les services communs ou plateformes. Les équipes de recherche (14 en 2022) regroupent plusieurs chercheurs et enseignants-chercheurs avec leurs étudiants, postdoctorants et parfois des ingénieurs et techniciens. Ces équipes sont la brique de base de l’INT, favorisant les interactions scientifiques quotidiennes et l’émergence de projets interdisciplinaires. Les équipes sont évaluées et renouvelées pour 5 ans, mais l’INT a la capacité de créer ou fermer des équipes en fonction des besoins. La mobilité entre équipes est également favorisée.

Figure 1 Bâtiment de l'Int

Depuis sa création en 2012, l'INT occupe un bâtiment entier de 4500m2 sur le Campus de la Faculté de Médecine. Ce bâtiment a été totalement rénové en 2011 pour accueillir le laboratoire.

2.2 Les plateformes

En 2023, l'INT comporte 6 plateformes technologiques. L'une d'entre elles est une structure dédiée à la recherche sur l'animal et fonctionne comme une Unité de service indépendante, le Centre de Primatologie de la Méditerranée (MPRC, UAR2018, CNRS Aix-Marseille Université). Les autres plateformes sont :

- La Neuro-Bio-Tools (NBT) est une plateforme AMU soutenant la recherche en neurobiologie. Elle est formée de 4 services déployant des outils de biologie moléculaire et cellulaire et d'histologie. Elle est accessible par https://iris.science-it.ch/Landing/Provider/1329.

- La Human Investigation Platform (HIP) est une structure dédiée au soutien à la recherche clinique et fondamentale, conduite chez des volontaires sains et chez des patients. Les missions de HIP sont triples :
    - Animer la recherche clinique et fondamentale chez l'Homme
    - Accompagner le montage et le suivi des projets
    - Mettre en place des outils communs pour la recherche clinique

- La Plateforme de neuro-imagerie photonique in vivo et in vitro (INPHIM) la plateforme INPHIM organise les moyens technologiques d'imagerie photonique in vivo et in vitro. Le parc instrumental compte actuellement sept microscopes optiques, deux systèmes d'imagerie à grand champ (macroscopes), un poste pour la visualisation et l'analyse d'image avec le logiciel Arivis Vision4D.

- Le Centre d'imagerie par résonance magnétique-(IRM-INT) est une plateforme de recherche gérée par l'Institut de Neurosciences de la Timone (UMR 7289). Son rôle est de soutenir la communauté scientifique, médicale, locale, nationale et internationale, publique et privée, dans la réalisation de recherches en neurosciences fondamentales, cliniques et en psychologie cognitive.

- Le Service de Prototypage et d'Instrumentation mécanique et électronique (S-PrIME) de l'INT conçoit et construit des prototypes mécaniques ou électroniques pour les différents systèmes expérimentaux utilisés en imagerie, neurobiologie, neurophysiologie ou encore en psychologie expérimentale.

- Lev Neuroinformatics and Information Technology (NIT) est composé d'une cellule « Données et Calcul scientifique » et d'une cellule « Infrastructure Système, Réseau, et Calcul Haute Performance ». Comme les autres plateformes de l'INT, la direction du NIT est double, avec un responsable scientifique (O Coulon, DR) et un responsable technique (S Takerkart, IR).

2.3 Organigramme de l'INT

Voici l'organigramme de l'institut de neurosciences

2.4 Environnement

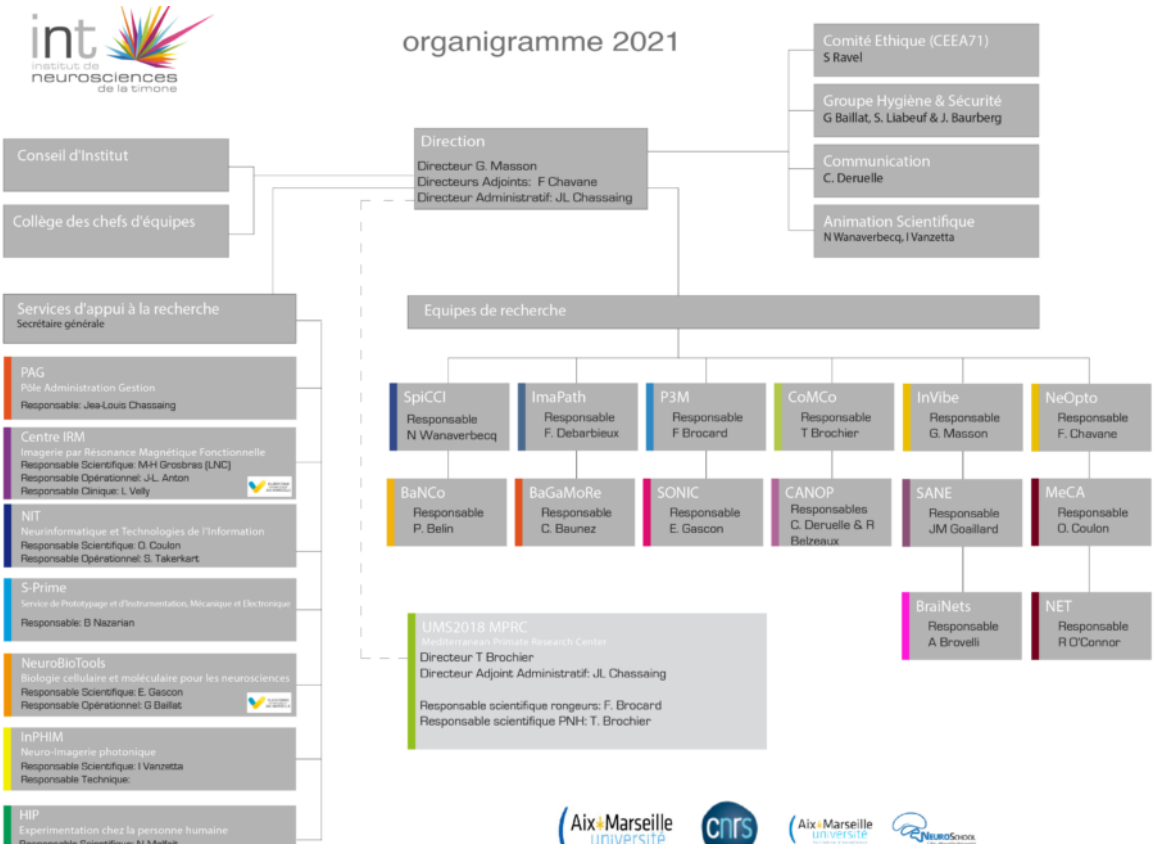

Figure 2 Organigramme de l'INT

L’INT accueille 14 équipes de recherche avec 4 services communs, comprenant le service informatique NIT (Neuroinformatics and Information Technology). Le NIT, qui est la plateforme à laquelle je suis rattachée, est dédiée à tout ce qui concerne l’informatique. Il propose et met en œuvre la stratégie de l’Institut en matière de télécommunication, de système d’information, de sécurité informatique, de développement et gestion du parc informatique et d’électronique. Il a aussi pour mission d’assurer l’administration et l’exploitation de l’ensemble des moyens informatiques du laboratoire matériels et logiciels (serveurs, équipements réseau), administrer les moyens et les procédures pour garantir les performances, la disponibilité du système d’information et la sécurité de l’infrastructure. Il vise aussi à apporter des outils informatiques innovants et performants pour tous les membres du laboratoire, tant au niveau matériel qu’au niveau logiciel.

L’équipe de travail est composée de 9 personnes qui assurent le NIT. Elle a à sa tête M. COULON Olivier (DR CNRS), responsable scientifique, et M. TAKERKART Sylvain (IRHC CNRS) responsable opérationnel. Ils dirigent une équipe dont M. CRUZEL Arnaud fait partie (IE CNRS) qui s’occupe de tout ce qui est administration système et réseau, et calcul haute performance.

Ensuite M. BACHAR Dipankar (IRCN CNRS), M. MEUNIER David (IRCN CRNS), Mme SPRENGER Julia (IR CDD) et M. LE TROTER Arnaud (IR CNRS) s’occupent du pôle donné et calculs scientifiques.

2.5 Organigramme de l'équipe NIT

Le diagramme ci-dessous représente l'organigramme de l'équipe du NIT ; je fais partie du pôle Systèmes d'information.

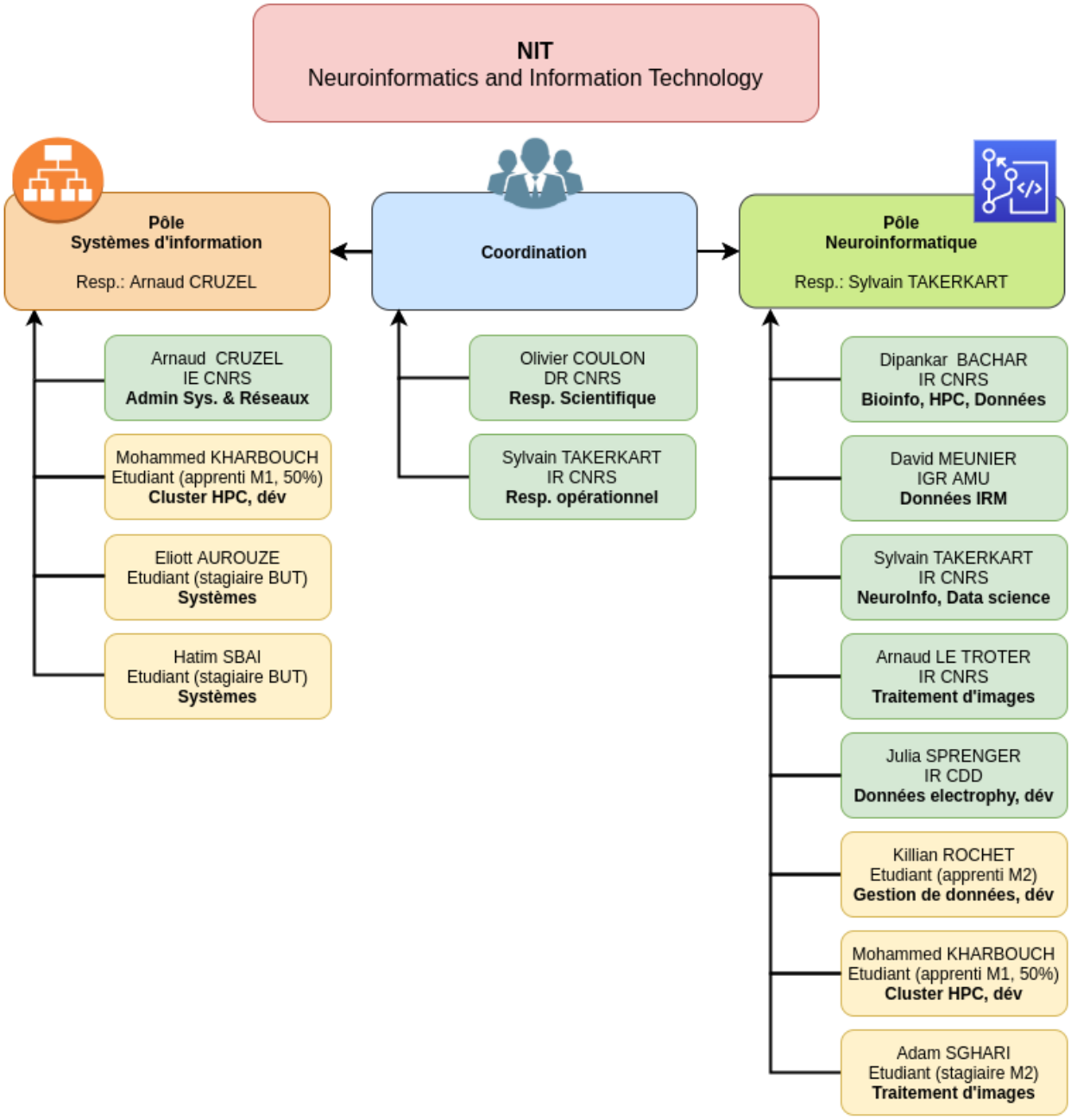

Figure 3 Organigramme du NIT

3 Contexte et mission

3.1 Problématique

Comme beaucoup d'entreprises et d'instituts, l'INT restreint le plus possible l'usage des comptes administrateur, la conséquence est que les utilisateurs ne peuvent pas installer de nouvelles applications sans l'intervention d'un membre de l'équipe du NIT, ce qui est une grande perte de temps, car à chaque fois qu'un utilisateur a besoin d'un nouveau logiciel sur sa machine nous devons, soit nous déplacer sur place pour taper le mot de passe, soit prendre le contrôle de sa machine à distance pour faire l'installation. En moyenne la moitié des tickets de l'INT concerne l'installation de logiciel d'où le besoin essentiel de trouver une solution à ce problème, satisfaisante à la fois en termes de sécurité et de simplicité d'utilisation.

3.2 Objectif

L'objectif principal de mon stage est de déployer un ensemble de services qui se nomme WAPT, il permet de gérer les installations de logiciels à distance beaucoup plus simplement, il permet aussi aux utilisateurs d'avoir accès au self-service qui est un store applicatif comme le Play store de Google ou l'App Store d'Apple, le but recherché étant que les utilisateurs aient accès à l'application souhaitée en quelques clics et d'enlever une importante charge de travail au NIT.

La mission secondaire du stage est de répondre aux tickets des utilisateurs en les aidant dans leurs demandes ou problèmes du quotidien, cela est très varié et peut aller du changement de cartouche d'imprimante, au dépannage d'un service sur le cluster de calcul en passant par le changement de composants défectueux sur leur machine.

3.3 Cahier des charges

Les compétences techniques pour réaliser ce projet sont :

- Avoir des connaissances sur la virtualisation et la conteneurisation pour la création du serveur Wapt.
- Prendre connaissance de l'ensemble du fonctionnement de la solution logiciel Wapt.
- Comprendre les concepts de l'Active Directory.
- Savoir configurer un reverse proxy pour que Wapt soit accessible de l'extérieure de manière sécurisé.
- Connaitre le système d'exploitation (OS*) Linux car c'est sur celui-ci que Wapt fonctionnera.

4 Environnement informatique du NIT

4.1 Réseau

L'INT possède plusieurs réseaux qui sont dédiés aux différents services ou usages, voici les réseaux que nous gérons :

- Réseau serveur (en violet sur le schéma) : Ce réseau comporte l'ensemble des serveurs de l'Int, il comprend 4 serveurs Proxmox et un cluster de calcul.
- Réseau INT (en vert) : Ce réseau est accessible depuis internet, c'est-à-dire même à l'extérieur de l'institut, il permet de rendre des services accessibles sur le web comme le Wiki, le site web de l'INT, le VPN et le service WAPT que j'ai déployé qui doit aussi être accessible depuis l'extérieur, donc j'ai dû faire une redirection du réseau INT vers le réseau serveur en utilisant un reverse proxy.
- Réseau user (en bleu) : C'est le réseau principal sur lequel toutes les machines sont branchées par câbles Ethernet, il est accessible seulement par câbles, ou bien à distance et en Wi-Fi à l'aide du VPN.
- Xpriment (en orange) : Ce réseau est spécifique aux machines de test, ce sont des vielles machines qui tournent sur Windows 7 ou Windows XP elles sont donc très dangereuses pour la sécurité, c'est pour ça qu'elles sont sur un réseau coupé des autres et surtout qui n'a pas accès à internet.

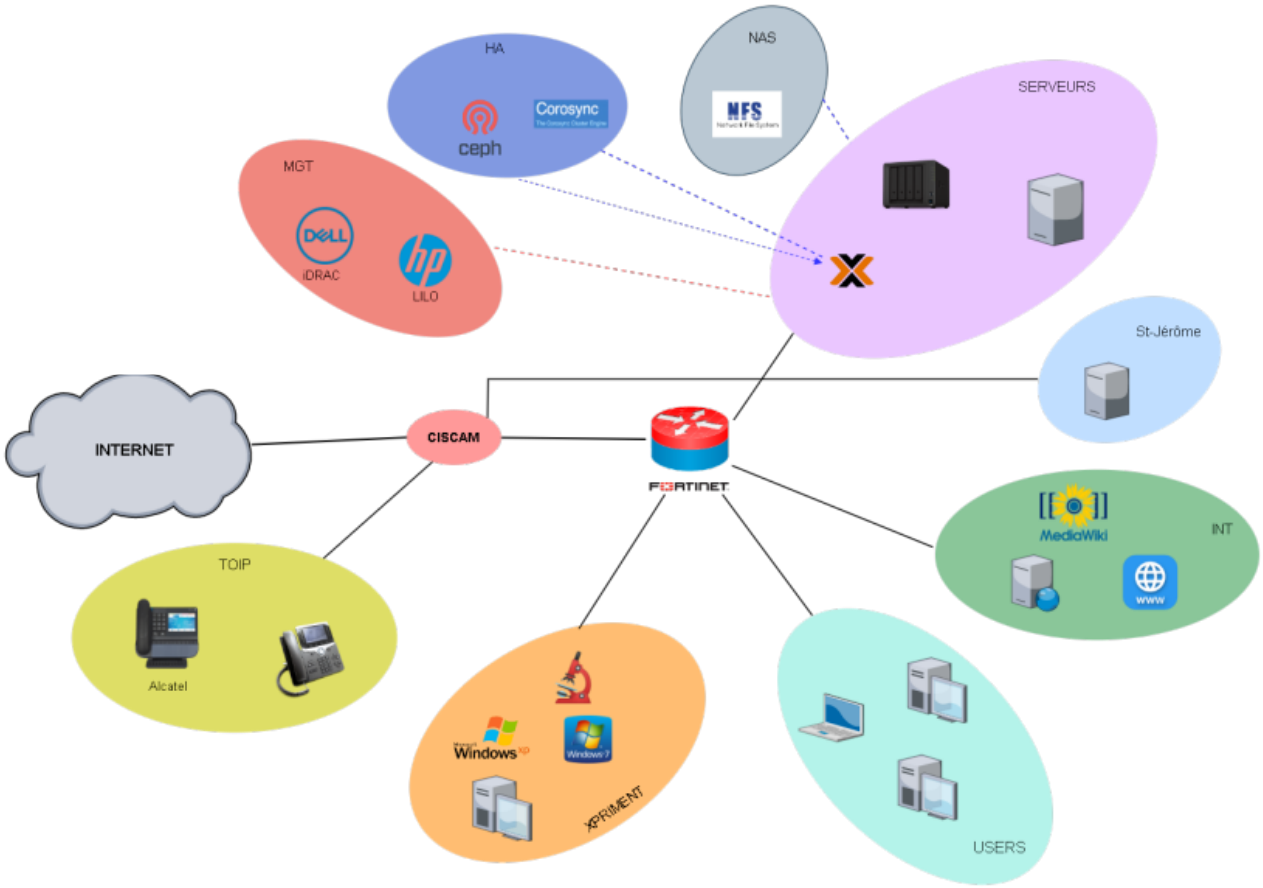

Figure 4 Diagramme Réseau de l'INT

4.2 Serveur

L'INT possède une salle de serveur comprenant 4 serveurs Proxmox et 7 nœuds de calcul.

Proxmox est un système d'exploitation qui permet de créer des Vm et des conteneurs avec une interface web, on appelle ça un hyperviseur de niveau 1, ce qui est très pratique avec Proxmox c'est la possibilité de faire un backup de nos machines et de pouvoir revenir à un état antérieur du conteneur ou VM, ce qui veut dire que même si on fait une erreur on a juste à utiliser la fonction rollback de proxmox pour revenir en arrière. Attention tout de même, le retour en arrière n'est pas disponible pour tout les sytèmes de fichier.

J'ai déployé le serveur dans un conteneur LXC sur un des nœuds du serveur Proxmox, un conteneur LXC peut s'apparenter à une Machine virtuelle, mais au lieu de virtualiser l'ensemble du système d'exploitation on utilise le kernel du serveur hôte ce qui permet d'avoir une machine beaucoup plus légère que si on virtualisait tout l'OS*.

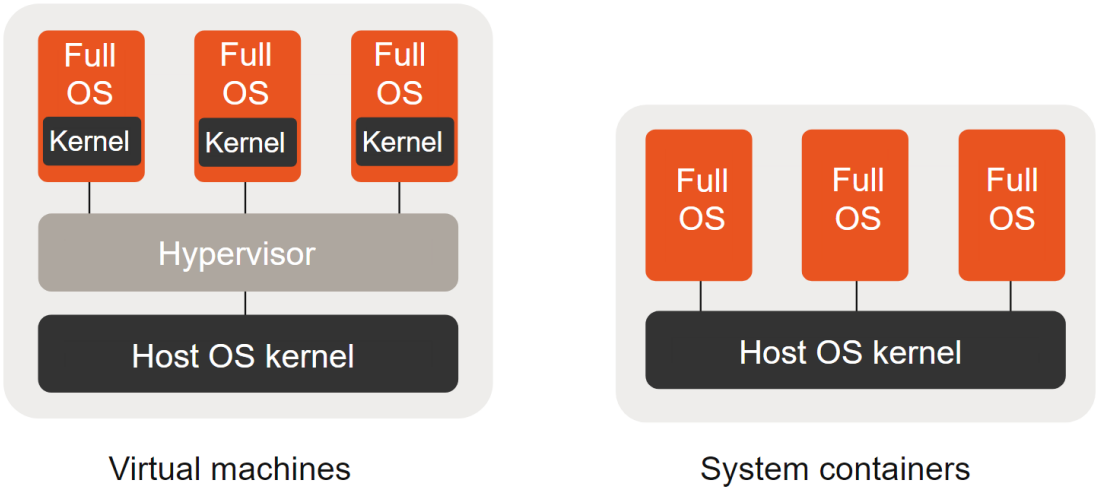

Figure 5 Schéma qui montre la différence entre un système Conteneurisé et un système Virtualisé

Comme on peut le voir sur le schéma, pour le conteneur, le kernel utilisé est celui de l'hôte, alors que pour la VM, le Kernel est lui virtualisé.

Il y a plusieurs avantages à utiliser un conteneur LXC plutôt qu'une VM :

- le premier est l'espace disque que le conteneur utilise est bien moindre que celui d'une VM ; cela permet donc de faire des backups beaucoup plus simplement et rapidement ;
- un autre avantage est au niveau des performances. Comme le conteneur utilise directement les ressources du serveur, celui-ci est donc beaucoup plus optimisé, car la VM doit virtualiser l'ensemble de son système, ce qui se traduit par des performances moins élevées.

5 WAPT

5.1 Fonctionnalité

WAPT est une solution de gestion de parc informatique et de déploiement de logiciels. L'acronyme WAPT signifie « Windows Automated Packaging Tool » ; il a été développé par Tranquil IT pour simplifier et automatiser le déploiement de logiciels sur un réseau d'ordinateurs fonctionnant sous le système d'exploitation Windows, bien que depuis peu, il permet aussi de gérer des PC* fonctionnant sur Mac et Linux.

WAPT permet aux administrateurs système de centraliser et de contrôler l'installation et la mise à jour des logiciels sur tous les postes de travail d'une organisation donnée.

Les 5 fonctionnalités les plus importantes sont les suivantes :

- Gestion des packages logiciels : WAPT offre un système de gestion des packages qui permet de créer, organiser et maintenir une bibliothèque de logiciels. Les administrateurs peuvent facilement créer des packages pour différents logiciels, incluant les fichiers d'installation, les paramètres et les dépendances nécessaires.

- Déploiement à distance : Une fois les packages créés, les administrateurs peuvent déployer les logiciels sur les postes de travail à distance, sans avoir besoin d'une intervention manuelle sur chaque ordinateur. Cela permet de gagner du temps et d'automatiser le processus de déploiement par exemple s'il faut forcer une mise à jour de Firefox, cela peut être fait instantanément sur tous les postes de l'organisation.

- Gestion des mises à jour : WAPT facilite également la gestion des mises à jour logiciels. Les administrateurs peuvent définir des règles de mise à jour automatique pour s'assurer que les logiciels sont maintenus à jour sur tous les postes de travail du réseau. Si un paquet du dépôt d'applications est mis à jour, alors la mise à jour s'applique sur tous les postes qui ont le paquet précédent installé.

- Rapports et surveillance : WAPT offre des fonctionnalités d'audit, ce qui permet de remonter des erreurs en cas de problème. Par exemple, si on crée un audit pour savoir si le chiffrement est activé sur toutes les machines, WAPT nous renverra des erreurs pour les machines qui ne sont pas chiffrées, alors qu'elle devrait l'être, ce qui nous permet d'aller corriger des problèmes ou des failles de sécurité.

- WAPT Self-service : La dernière fonctionnalité très utilisée est le self-service. Le principe est de créer un store applicatif, à l'instar du Play store de Google, ou de l'Apple store d'Apple. Les utilisateurs peuvent alors accéder à un ensemble d'applications qu'ils peuvent alors installer en quelques clics ,ou les désinstaller s'ils le souhaitent. Le grand avantage de ce système est que les utilisateurs n'ont pas besoin des droits administrateur pour installer les applications présentes dans le self-service, car elles ont été approuvées et rajoutés par le NIT.

5.2 Fonctionnement

Pour fonctionner, WAPT a besoin de deux choses :

- Un serveur sur lequel les clients Windows mac ou Linux devront se connecter pour pouvoir accéder à l'application proposé par celui-ci
- Un agent qui se nomme WAPT agent. Cet agent est à installer sur l'ensemble des machines du parc informatique. Il a pour rôle d'exécuter les ordres du serveur : par exemple, s'il faut mettre à jour Firefox, car il y a une nouvelle version, l'agent va télécharger la nouvelle version sur notre serveur privé et va l'installer.

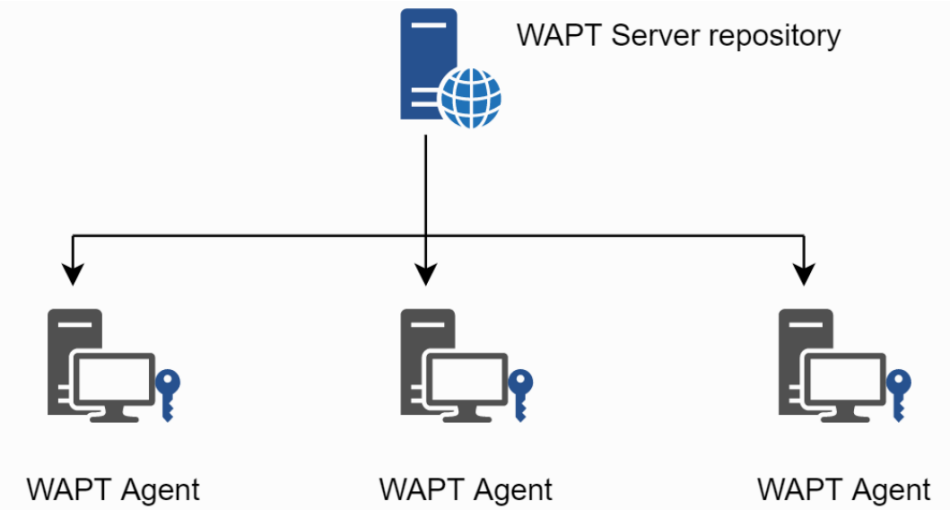

Figure 6 Schéma des interactions entre le serveur WAPT et les WAPT Agents

Sur le serveur WAPT qui est autohébergé, il y a un dépôt avec un ensemble de paquets, un paquet est un fichier qui va contenir tous les éléments nécessaires au bon fonctionnement du déploiement de l'application ou de la fonctionnalité.

5.3 Composition d'un paquet

Un paquet WAPT est composé de plusieurs fichiers que l'on peut voir sur la figure ci-dessous

- Il y a un dossier qui s'appelle WAPT. Il contient le certificat d'autorité qui permet aux agents de s'assurer que le paquet vient bien du serveur. Une somme de contrôle qui permet de vérifier que le fichier est arrivé en intégralité, et qu'il n'a pas était modifiée en chemin.
- L'icône de l'application. Il y a l'installateur de l'application en 32 bits ou en 64 bits ou les deux.
- Et pour finir il y a un fichier python Setup.py. Son utilisation est plus complexe, et sera détaillée dans la section « ajout de nouvelles applications » dans la section « travail réaliser ».

Tous ces éléments sont indispensables pour le fonctionnement du paquet dans WAPT.

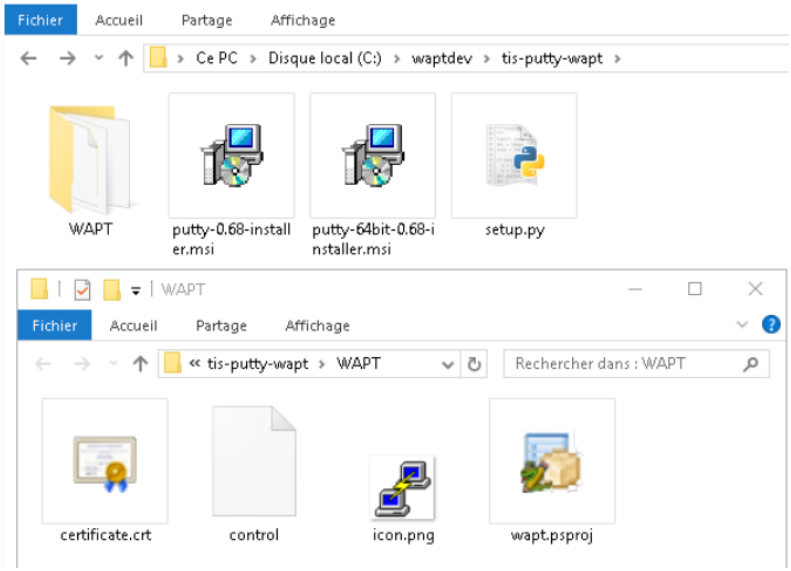

Figure 7 Capture d'écran de la composition d'un paquet Wapt

5.4 Comment est gérée la Sécurité

WAPT est un système extrêmement sécurisé, car il utilise un certain nombre de mécanismes pour permettre une sécurité forte. Pour pouvoir effectuer des actions sur des machines distantes, comme par exemple installer des applications, envoyer des messages ou encore redémarrer l'ordinateur, il faut posséder la clé privée ; les agents présents sur les machines client possèdent la clé publique associée à la clé privée.

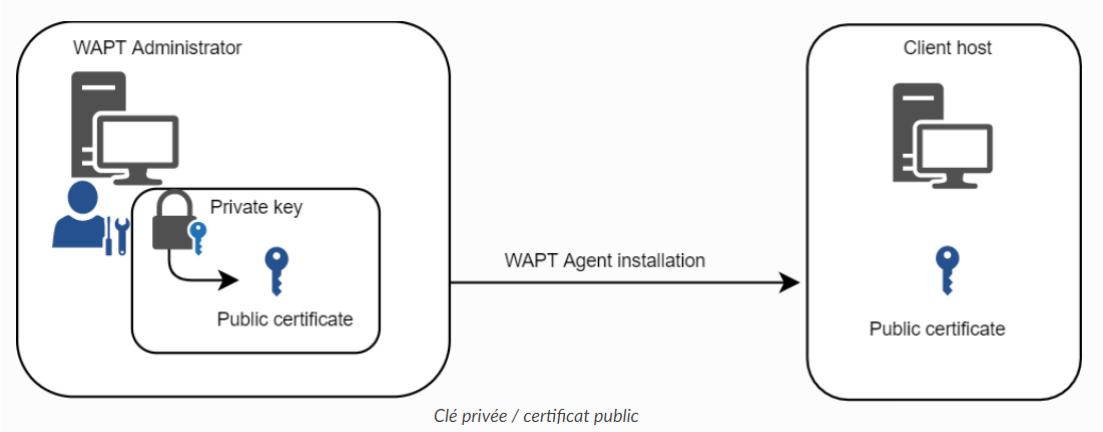

Figure 8 Schéma des interactions entre la console de l'administrateur et un WAPT Agent

Ce système permet de garantir que le paquet a bien était signé par l'administrateur, car seul lui possède la clé privée, cependant il faut faire extrêmement attention à la clé privée, car si une personne mal intentionnée arrive à se la procurer alors elle aurait l'accès à toutes les machines du réseau de l'entreprise.

Il est fortement recommandé de créer des certificats enfants qui héritent des droits du certificat principal, car il est possible de révoquer ces certificats à distance si l'un de ces certificats est compromis, alors qu'avec le certificat Administrateur il est impossible de le révoquer aussi simplement.

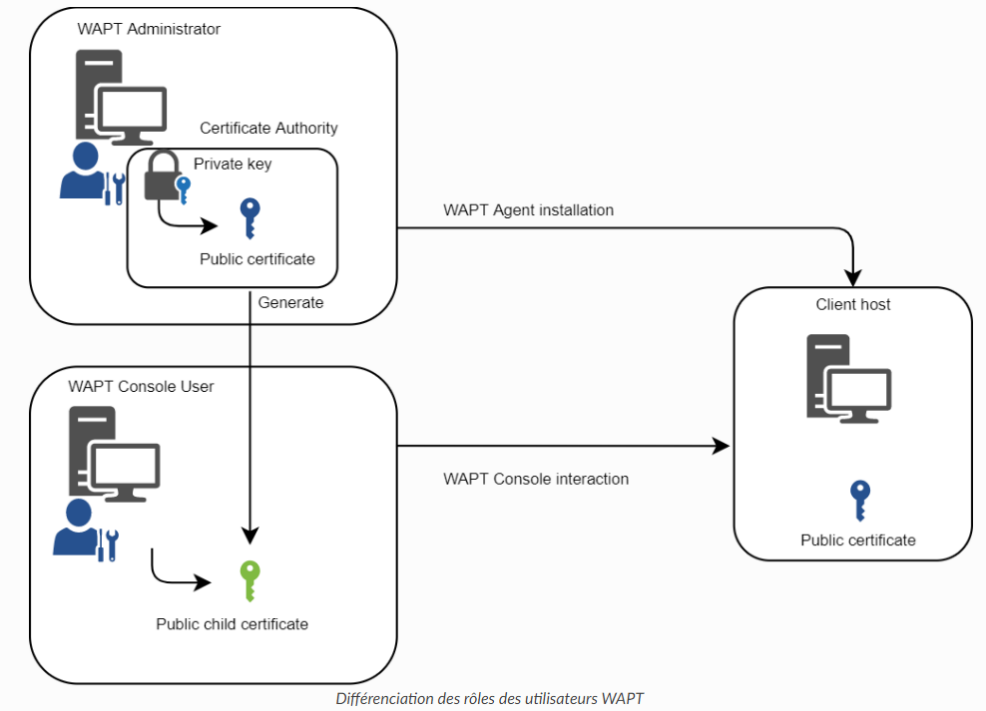

Figure 9 Schéma qui montre le système de clé enfant - Source : Documentation officiel Wapt

Comme nous le montre cette image, il est possible de créer des « Public child certificate » pour les administrateurs ce qui leur permet d'avoir les mêmes droits que le compte super admin, mais sans pour autant posséder le certificat super admin.

6 Travail réalisé

6.1 Déploiement du serveur

Après ces explications sur l'environnement et le fonctionnement WAPT, il est temps de déployer le serveur.

Pour commencer, j'ai créé le conteneur sur une base Debian avec 4 cœurs CPU et 8Gb de Ram*, et pour le stockage, j'ai créé un point de montage de 20Go. Cela n'est pas suffisant pour mettre toutes les applications, mais cela n'est pas un problème, car il est extrêmement facile d'augmenter le stockage. Par contre il est très difficile de le réduire, c'est pour cela que j'ai opté pour 20Go que j'ai augmenté en fonction des besoins.

Une fois le conteneur crée, je me suis connecté dessus en SSH.

La première chose à faire est de configurer le réseau du conteneur ; j'ai donc modifié le fichier /etc/hostname, et y renseigner le nom FQDN du serveur.

Puis il faut configurer le fichier /etc/hosts en mettant l'IP du conteneur plus le FQDN*

Pour finir, il faut configurer le fichier /etc/network/interfaces : il faut mettre les informations relatives à l'interface (adresse IP, masque, et la passerelle).

J'ai ensuite mis à jour le serveur avant l'installation de WAPT, avec la commande apt update && apt upgrade.

Pour que toutes ses modifications soient prises en compte, il faut redémarrer le serveur.

6.2 Installation de WAPT sur le serveur

Pour commencer j'ai dû mettre à jour les sources APT, récupérer la clé .gpg de Tranquil IT, puis ajouter le dépôt de Tranquil IT.

```
apt install apt-transport-https lsb-release gnupg wget -y
wget -O - https://wapt.tranquil.it/$(lsb_release -is)/tiswapt-pub.gpg | apt-key
add -
echo "deb https://wapt.tranquil.it/$(lsb_release -is)/wapt-2.3/ $(lsb_release -
c -s) main" > /etc/apt/sources.list.d/wapt.list
```

Il faut ensuite lancer le script de post-configuration avec la commande suivante :

/opt/wapt/waptserver/scripts/postconf.sh

Le script va vous poser plusieurs questions :

- Quel est votre nom de domaine ?
- Veuillez choisir un nom d'utilisateur administrateur et un mot de passe ?

Il y a une dizaine de questions, l'installation détaillée est disponible dans la documentation que j'ai écrite qui se trouve en annexe.

Les cours sur Linux m'on était d'une grande aide tout du long de cette parti car ils m'ont permit d'avoir de solides bases lors de l'installation du serveur en SSH.

6.3 Reverse proxy

Afin de garantir l'accessibilité sécurisée du service à distance, j'ai mis en place une règle dans le reverse proxy de l'INT. En effet, un reverse proxy agit comme un intermédiaire qui transfère les requêtes réseau provenant du proxy vers le serveur cible.

6.4 Installation de Waptconsole

Après avoir fini la configuration du serveur, sa mise en réseau et la configuration du reverse proxy, j'ai installé le logiciel de gestion de parc informatique Waptconsole. L'installation est basique, il suffit juste de suivre les étapes comme n'importe quel .exe sur Windows. Il y a une étape importante qui consiste à entrer le nom de domaine du serveur Wapt, configurée avec le reverse proxy qui est wapt.int.univ-amu.fr.

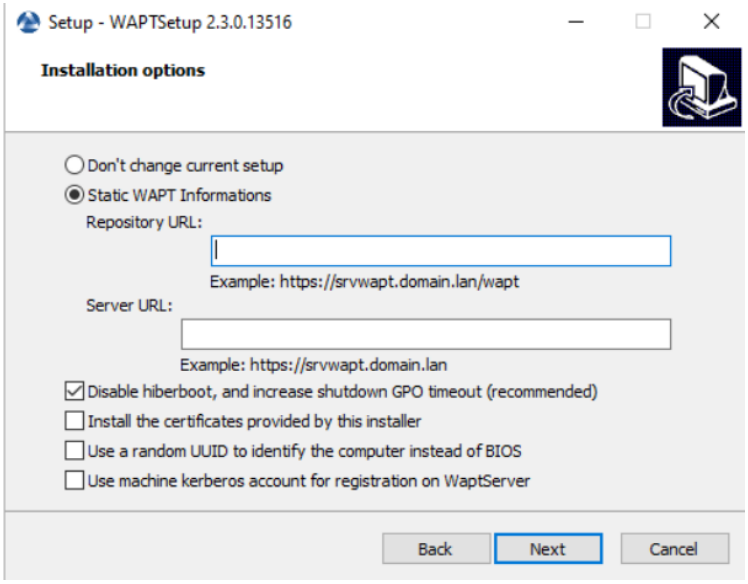

Figure 10 Fenêtre d'installation de Wapt

Une fois le logiciel de gestion installé sur mon PC, je peux me connecter avec le compte admin et le mot de passe configuré lors de l'installation de WAPT sur le serveur.

La première chose à faire quand je me suis connecté a été de rentrer le fichier de licences que Arnaud m'a fourni pour activer la version pro, car ce logiciel est payant.

Une fois cela réalisé j'ai pu créer des utilisateurs administrateurs, un compte pour moi et un pour mon maitre de stage.

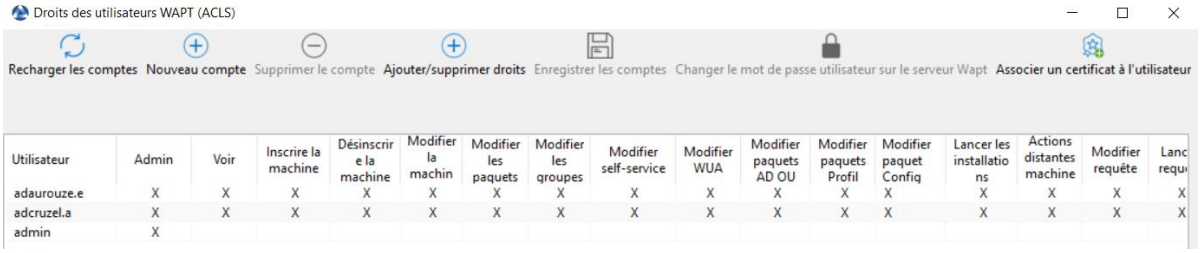

Figure 11 Fenêtre de création de compte administrateur

J'ai dû créer des certificats qui héritent des droits du compte Admin puis je les ai associés à l'utilisateur, cela permet d'avoir les mêmes droits que le Certificat d'autorité du compte super Admin, mais en utilisant nos propres certificats qui sont révocables.

Par la suite j'ai créé l'agent WAPT qui sera déployé sur toutes les machines de l'INT. Pour rappel, l'agent WAPT est un logiciel qui fonctionne en arrière-plan sur les machines des utilisateurs ; c'est lui qui va télécharger les logiciels sur le serveur configuré précédemment, et les installer.

Il faut bien choisir les options lors de la création de l'agent, comme l'utilisation de Kerberos et du SSO*, ou bien s'il gère ou non les mises à jour de Windows. Lors de la création, il y a seulement les options de base. Si l'on veut le configurer avec des options avancées, il faut créer un paquet de configuration WAPT qui se déploiera par la suite.

Une fois la création effectuée j'ai pu l'installer sur les PC des membres du NIT pour commencer à expérimenter les différentes options en condition réelle.

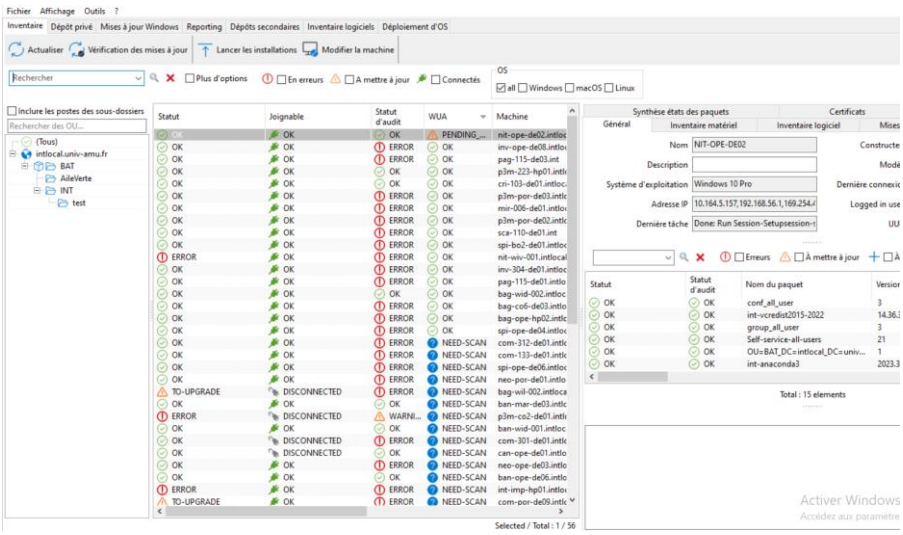

Figure 12 Interface administrateur de Wapt

Sur cette capture d'écran on peut voir tous les PC qui sont déjà enregistrés il y en a un grand nombre, car la capture d'écran a été prise après la mise en production, à ce moment-là il y avait donc toutes les machines de l'INT, mais lors des tests il y avait seulement 3 machines.

Pour effectuer les tests, j'ai donc téléchargé des logiciels simples comme Firefox, 7zip, et je les ai rajoutés à notre dépôt privé.

Pour effectuer des tests, j'ai forcé l'installations de logiciel sur certains postes, et tout a parfaitement fonctionné.

6.5 Self-service

L'une des fonctionnalités qui va être la plus utilisée et qui est le cœur du projet est le WAPT self-service. C'est une fonctionnalité proposée par WAPT qui permet de créer un store applicatif comme l'Apple store d'Apple ou encore le Play store de google. Cette fonctionnalité permet aux utilisateurs de choisir parmi une liste d'applications, de les installer ou les supprimer.
Les applications que les utilisateurs installent seront automatiquement mises à jour si une nouvelle version est détectée. Le grand avantage de ce système, et c'est le cœur du projet, est que les utilisateurs n'ont pas besoin d'avoir les droits administrateur pour installer de nouvelles applications, ce qui fait gagner un temps plus que précieux au NIT, car il n'a plus à installer les applications une par une.

Voici une capture d'écran du self-service :

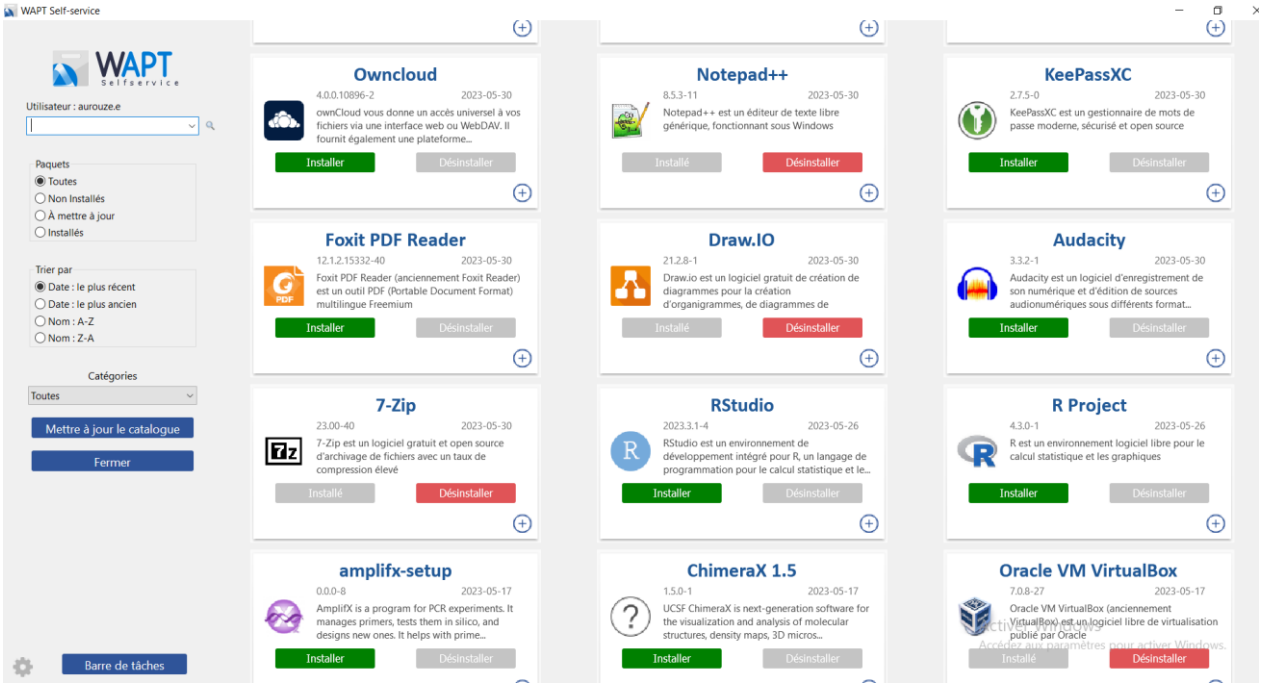

Figure 13 Interface Wapt self-service

Comme on peut le voir sur la capture d'écran, il est maintenant extrêmement simple d'installer ou de désinstaller des logiciels pour les utilisateurs. Il suffit simplement de cliquer sur installer ou désinstaller, et tout se fait automatiquement. De plus, les logiciels installer via le self-service sont automatiquement mis à jour.

Il est aussi possible de limiter l'accès de certaines applications à certaines personnes ou groupes de personnes. Par exemple, il pourrait exister un groupe d'utilisateurs scientifiques, et ce groupe aurait alors accès à plusieurs applications qui ne seraient pas accessibles par le groupe Administration.

6.6 Authentification automatique

L'une des fonctionnalités que j'ai implémentées est le SSO* (single sign-on), qui a besoin de Kerberos pour fonctionner.

La fonctionnalité SSO permet à l'utilisateur d'être authentifié automatiquement au self-service, car, par défaut les utilisateurs doivent se connecter avec leurs mots de passe pour accéder au self-service, ce qui est une perte de temps, car ils sont déjà connectés à leur session Windows.

6.6.1 Kerberos

Pour ce faire j'ai dû installer Kerberos sur la Machine virtuelle avec la commande :

apt install krb5-user msktutil libnginx-mod-http-auth-spnego

Ensuite j'ai modifié le fichier /etc/krb5.conf en éditant l'option du contrôleur de domaine pour qu'il corresponde à celui de l'Int.

Une fois Kerberos installé, il faut utiliser le Script de post configuration pour l'activer :

/opt/wapt/waptserver/scripts/postconf.sh --force-https

Durant le Script, une question vous demande si WAPT doit utiliser Kerberos, il faut répondre Oui. A ce moment-là Kerberos sera installé.

6.6.2 SSL/TLS

Pour que le Kerberos fonctionne, il faut activer SSL/TLS.

SSL/TLS active le chiffrement par un certificat, et il est indispensable pour Kerberos, car les données doivent être chiffrées. J'ai donc mis le certificat de l'INT dans le dossier /usr/local/share/ca-certificates/, puis pour mettre à jour le certificat, en utilisant la commande **update-ca-certificates**

Attention l'extension du certificat doit être .crt. Cela m'a posé problème, car je n'ai pas mis la bonne extension.

La dernière chose que j'ai faite est de rajouter cette ligne dans le fichier de configuration WAPT « ldap_auth_ssl_enabled = True »

6.6.3 Active directory

L'Active directory est un annuaire qui répertorie tous les appareils et les utilisateurs d'un domaine ; on appelle cela des objets. Dans active directory, tout est objet, que ce soit un utilisateur, une imprimante, ou encore un PC.

Pour en apprendre plus sur l'active directory, j'ai suivi le cours dédié à cet outil sur OpenClassRoom. Cela m'a été très utile pour mieux comprendre son fonctionnement.

L'un des impératifs pour configurer SSO est de créer un utilisateur dans l'active directory. Cet utilisateur a besoin d'avoir des droits en lecture pour pouvoir lister l'ensemble des utilisateurs de l'INT.

L'une des fonctionnalités de l'active directory que j'ai utilisé pour la mise en production, est GPO* Groupe Policy Object. Cette fonctionnalité permet d'affecter des paramètres sur un ensemble d'Object. La GPO que j'ai créé, permet d'installer l'agent WAPT à l'extinction, ou au démarrage de n'importe qu'elle machine de l'INT. Cela va permettre lors de la mise en production de déployer l'agent sur toute les machines automatiquement.

6.6.4 SSO

Maintenant que Kerberos est fonctionnel et configuré, ainsi que le SSL/TLS, nous pouvons activer SSO qui permettra à l'utilisateur d'être automatiquement connecté s'il est connecté à sa session Windows.

Il existe trois méthodes différentes pour utiliser SSO ; j'ai utilisé la troisième, qui est la plus sécurisée.

Pour commencer, j'ai à nouveau modifié le fichier de configuration WAPT, et rajouté ces deux lignes :

« ldap_auth_ssl_enabled = True »

« verify_cert_ldap = True »

Ces deux options permettent d'activer l'authentification ldap en SSL, ce qui sécurise les communications.

Et de vérifier le certificat ldap, ce qui permet de vérifier que l'information vienne bien du serveur Ldap, et non d'une personne mal intentionnée qui se ferait passer pour le serveur.

J'ai ensuite rajouté ces 4 lignes :

« ldap_account_service_login = wapt-ldap@intlocal.univ-amu.fr »

La première sert à renseigner le compte active directory précédemment créé, le rôle de ce compte est de vérifier si les informations de connexion sont exactes.

« ldap_account_service_password = ********** »

La deuxième sert à saisir le mot de passe du compte.

« ldap_auth_server = pdcad0.intlocal.univ-amu.fr »

La troisième ligne sert à spécifier le nom de domaine de l'Active Directory

« ldap_auth_base_dn = DC=intlocal,DC=univ-amu,DC=fr »

La quatrième sert de filtre de recherche ; avec cette option il recherchera les objets fr,intlocal,ldap_auth_base_dn

Une fois tout cela effectué, j'ai redémarré le service WAPT sur le serveur avec la commande :

systemctl restart waptserver wapttasks

Après le redémarrage je peux utiliser le self-service, sans devoir entrer mon nom d'utilisateur et mon mot de passe, car WAPT utilise directement le ticket Kerberos.

6.7 Installation de paquet par défaut

Avec WAPT, il est possible d'obliger les machines utilisateur à installer des paquets. Avec Arnaud, nous avons défini une liste de paquets que les machines doivent obligatoirement installer :

PAQUET	UTILITE
SELF-SERVICE	Permet à l'utilisateur d'avoir la liste d'application disponible dans le self-service
AUDIT BITLOCKER	Ce paquet permet de nous retourner une erreur si BitLocker est désactivé. BitLocker est le système de chiffrement de Windows ; donc s'il est désactivé, cela signifie que le PC n'est pas chiffré, ce qui est contraire à la politique de sécurité du NIT.
AUDIT LOCAL ADMIN	Ce paquet nous retourne une alerte si des comptes administrateur autres que les nôtres sont présents sur la machine, si des comptes sont admin alors nous devons intervenir pour supprimer le compte admin.
DISABLE CORTANA	Comme son nom l'indique, ce paquet désactive l'assistant vocal de Windows Cortana
DISABLE-UPDATE-TO-WINDOWS11	Ce paquet permet de désactiver la mise à jour automatique vers Windows 11
CONF-ALL-USER	Ce paquet permet de configurer l'agent WAPT présent sur l'ensemble des ordinateurs du NIT.
F-SECURE	F Secure est l'antivirus que l'on utilise à l'INT, et il est installé automatiquement sur toutes les machines.

Certains paquets sont donc installées automatiquement, dès qu'un ordinateur est ajouté dans le système WAPT. Le reste des Paquets / logiciels sont proposés en accès libre via le self-service, sauf les paquets obligatoires, et c'est à l'utilisateur de choisir ses outils de travail.

Il est tout à fait possible d'installer des paquets de base différents selon le type de machine, par exemple on pourrait créer un groupe d'utilisateur « Spécialiste imagerie », toutes les machines de ce groupe installerait automatiquement des logiciels d'imagerie.

6.8 Rajouter des nouveaux programmes dans le dépôt

Pour rajouter des programmes dans le dépôt il y a deux options :

- La première est la plus simple : c'est d'aller sur le dépôt de Tranquil It, et importer les logiciels que l'on veut directement dans notre dépôt.
- Si le logiciel que l'on souhaite rajouter n'est pas disponible, ça se complique : il faut alors trouver l'installateur en .exe, ou en .msi de préférence, puis on va devoir créer le paquet avec le logiciel pyscrypter, et l'environnement python fournit par Wapt.

Voici un exemple de paquet avec Pyscripter :

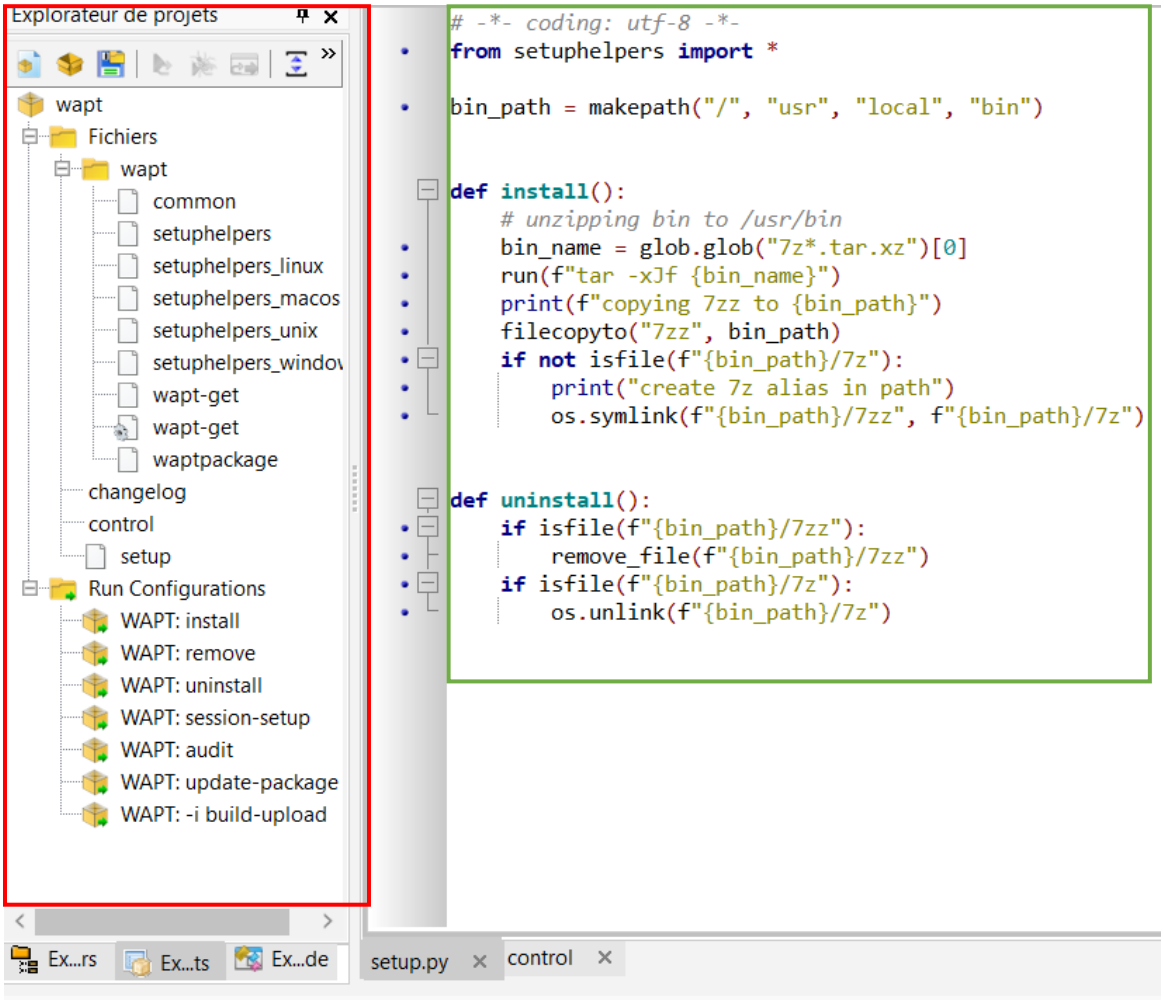

Figure 14 interface de Pyscripter

Sur la capture d'écran, on peut voir encadré en rouge les fonctions par default qui permettent d'installer ou de désinstaller le logiciel que l'on veut rajouter. Lors de la création, on doit modifier les fonctions encadrées en vert pour mettre les bonnes options d'installation ou de désinstallation. Par exemple, il faut mettre la bonne clé de d'installation, ou mettre /S pour que le logiciel s'installe en arrière-plan. Une fois cela fait, on peut essayer l'installation et la désinstallation sur notre pc. Si tout se passe bien, alors on lance la fonction « -i build-upload » qui vas compiler le paquet, le signer avec notre clé privée, puis l'envoyer dans le dépôt du serveur.

7 Mise en production

7.1 Création d'un QCM*

J'ai dû réaliser un questionnaire à choix multiples pour connaitre les problèmes éventuels que les utilisateurs auraient pu rencontrer. Pour cela, j'ai utilisé la plateforme LimeSurvey,

Question	Type de question
Avez vous apprécier votre expérience avec le self-service d'application Wapt noté de 1 a 5 ? 1 étant la plus mauvaise note et 5 la note maximal	5 point choice
Avez vous trouver le self-service simple d'utilisation ?	5 point choice
Avez vous rencontrer des problème en utilisant le self-service ?	Yes/No
Merci de décrire le ou les problèmes rencontrées	Long free text
Quel logiciel open source ou gratuit non present dans le self-service souhaiterier vous voir apparaitre ?	Long free text
Avez vous des remarque suplaimentaire ?	Long free text

Figure 15 QCM LimeSurvey que j'ai réalisé

Ce questionnaire va me servir par la suite pour avoir un retour des problèmes rencontrées par les utilisateurs, par exemple l'un des problèmes qui a était remonter a permis l'amélioration de la Documentation utilisateur.

7.2 Plan de mise en production

Pour la mise en production, j'ai effectué un plan de mise en production qui récapitule les étapes clés qui ont permis un bon déroulement du déploiement de WAPT :

1. Test de WAPT sur les machines de l'équipe du NIT

2. Avec l'aide de Arnaud, nous avons sélectionné plus d'utilisateurs pour qu'ils participent au bêta test.

3. Ensuite j'ai envoyé par mail le QCM pour avoir le retour des utilisateurs

4. Grâce au retour des questionnaires, nous avons pu mettre à jour la documentation que certains utilisateurs trouvaient un peu floue.

5. Mise en production grâce à la GPO*

La mise en production a parfaitement fonctionné, et les retours du QCM sont tous positifs. Il ne reste plus maintenant qu'à étoffer le plus possible notre Self-service avec le plus d'applications possibles.

Conclusion

Ce stage au sein de l'Institut de Neurosciences de la Timone (INT) a été une expérience extrêmement enrichissante et formatrice dans le cadre de ma deuxième année en BUT Réseaux et Télécommunications. Mon objectif principal était de déployer WAPT au sein de l'institut, et j'ai pu le réaliser avec succès, grâce à l'encadrement et le soutien de mon tuteur de stage, M. Arnaud Cruzel.

Ce projet de déploiement de WAPT a été l'occasion pour moi d'appliquer mes connaissances théoriques et techniques acquises tout au long de ma formation. J'ai pu mettre en pratique mes compétences en administration réseau, en gestion des systèmes d'information et en déploiement de logiciels. Cette expérience m'a permis d'approfondir mes connaissances sur les outils de gestion et de déploiement de logiciels, ainsi que sur les bonnes pratiques en matière de sécurité informatique.

Au-delà du déploiement de WAPT, j'ai également eu l'occasion d'interagir avec d'autres membres de l'INT et d'en apprendre davantage sur les enjeux et les avancées dans le domaine des neurosciences. Cette immersion au sein d'un institut de recherche a été particulièrement inspirante.

Mon intervention au sein de l'institut a permis une baisse importante des tickets au sein du NIT, car la majorité des tickets était des demandes d'installation de nouvelles applications. De plus ce système participe à augmenter le niveau de sécurité informatique de l'INT car il permet de remonter les anomalies au niveau des comptes administrateur non autorisés, ou encore des alertes en cas de pc qui n'a pas le chiffrement activé.

Une des fonctions de WAPT est le déploiement de système d'exploitation à distance, ce qui permet de déployer bien plus simplement de nouvelles machines. J'ai commencé à développer cette option supplémentaire, car cela pourrait être un bon outil à développer pour le futur.

Remerciement

Je souhaite remercier chaleureusement Arnaud Cruzel de m'avoir aidé à réaliser ce projet jusqu'au bout, et d'avoir répondu à toutes mes questions.

Je voudrais aussi remercier l'INT ainsi que l'ensemble du personnel du INT pour leur temps, leur confiance, ainsi que toute l'aide et les conseils apportés qui m'ont été bénéfiques.

Glossaire

RAM = « Random Access Memory », est le composant informatique qui met en mémoire les applications en cour d'exécution, cette mémoire est extrêmement rapide mais elle est aussi volatile cela signifie que en cas de coupure de courant toutes les données contenues dans cette mémoire seront perdues.

SSO = « Single Sign-onry », est un service d'authentification de session et d'utilisateur qui permet à un utilisateur d'utiliser un ensemble d'informations d'identification (par exemple, nom et mot de passe) pour accéder à plusieurs applications.

GPO = « Groupe Policy Object », une GPO permet d'effectuer des actions de configuration ou d'installation sur un ensemble d'objet, dans notre cas la GPO nous a servi à installer l'ensemble des agent Wapt sur tout les poste de l'Int.

Wapt = Wapt est une contraction entre le W de Windows et APT qui est l'outil d'installation de paquet sur les system Unix/Linux, d'où le nom WAPT

QCM = « Question à choix multiple »

OS = « Operating system » ou system exploitation en français, un system d'exploitation est le système principal d'un équipement informatique, sur nos pc ou serveur il s'agit très souvent de Linux, Windows ou MacOs.

Sitographie

Documentation official Wapt : https://www.wapt.fr/fr/doc/

Forum officiel Wapt : https://forum.tranquil.it/

OpenClassRooms : https://openclassrooms.com/fr/

Linux containers : https://linuxcontainers.org

Documentation Proxmox : https://pve.proxmox.com/pve-docs/

Page de l'institut de neurosciences INT : https://www.int.univ-amu.fr/

Image et schéma :

Figure 2 et 4 : Ressource Interne à l'Int

Figure 3 : Mr Sylvain TAKERKART, membre de l'équipe du NIT.

Figure 5 : linuxcontainers.org

Figure 6,7,8,9 et 11 : Documentation officiel Wapt

Figure 10,12,13,14 et 15 : Ressource personnel