

WAPT ou le déploiement de logiciel facilité

Florent Fareneau

Direction des Systèmes d'Information
Université Polytechnique Hauts-de-France
Le Mont-Houy - 59313 VALENCIENNES CEDEX 9

Jean-Luc Petit

Direction des Systèmes d'Information
Université Polytechnique Hauts-de-France
Le Mont-Houy - 59313 VALENCIENNES CEDEX 9

Benjamin Burnouf

Direction des Systèmes d'Information
Université Polytechnique Hauts-de-France
Le Mont-Houy - 59313 VALENCIENNES CEDEX 9

Résumé

L'Université de Valenciennes a revu depuis 2013 ses solutions de déploiement et de maintenance logicielle de l'ensemble de son parc machine. En effet, avant cette date, les machines étaient déployées à partir d'images masterisées nécessitant un stockage important. Il fallait régulièrement procéder à des ajustements logiciels directement sur le poste client.

Le suivi des mises à jour de ces postes devenait alors problématique (patches de sécurité, hétérogénéité des versions déployées...).

Nos besoins : faciliter le déploiement, la prise en main et la montée en compétences ; gérer de manière centralisée l'ensemble des sites et les aspects financiers pour plus de 2000 postes clients.

Un état de l'art des solutions de déploiement de systèmes d'exploitation et de logiciels a été effectué : Dell Kace, SCCM, UpdateEngine, Landesk, GPO, OCS, WPKG.

Notre choix s'est arrêté sur le couple MDT (déploiement d'OS Windows) et WAPT (déploiement de logiciels).

Les points forts de WAPT : un produit opensource, une console simple d'utilisation, une bibliothèque de paquets logiciels, une application évoluant rapidement, une solution supportée par une entreprise française, un système de mise à jour en mode push et non bloquante...

La solution doit permettre de déléguer, à l'équipe de proximité, des droits d'usages afin de créer, déployer et fiabiliser les paquets. Nous évoquerons dans ce retour d'expérience l'expression de nos besoins initiaux, nos études de solutions de déploiement, notre choix pour ce logiciel, nos réussites et limites dans l'usage sur ces 5 dernières années et nos prospectives dans celles à venir avec une API en plein développement ou un self-service applicatif ...

Mots-clefs

Déploiement logiciel, WAPT, Paquet

1 Introduction

En 2013, lors du lancement de notre projet de déploiement, l'Université de Valenciennes et du Hainaut Cambrésis comptait environ 10000 étudiants, 1300 personnels pour un parc d'environ 2000 postes Windows. Les autres systèmes d'exploitations présents au sein du parc étaient gérés spécifiquement. Une grande partie de ces machines connectées sur le réseau LAN était à la charge de la Direction des Systèmes d'Informations (DSI) de l'établissement. Ce service était composé de trois pôles : Appui au Système d'Information, Infrastructure de Services et Réseau, Cellule TICE-Médiatisation. Le pôle infrastructure était organisé autour d'une équipe chargée des aspects système et réseau et de techniciens informatiques. 4 ingénieurs et 7 techniciens avaient en charge l'ensemble des postes administratifs et pédagogiques de plusieurs composantes, de la bibliothèque et des sites délocalisés distants d'environ 30 kilomètres du site principal.

Comme dans tous les établissements, le nombre de machines pédagogiques et administratives à déployer et de logiciels à installer était en constante augmentation. De plus, suite à des restructurations, le service informatique a vu son périmètre s'étendre avec la gestion complémentaire de domaine pédagogique ou administratif qui jusque là étaient indépendants.

En plus de ce périmètre purement comptable en nombre de postes à gérer, les équipes en charge de la gestion du parc machine ont vu les usages de logiciels augmenter tant en diversité qu'en complexité. Ainsi, certains de ces départements exprimaient des besoins de logiciels métiers en nombre, très spécifiques et souvent interopérables entre eux : mécanique, simulation numérique, ... La mise en conformité de ces nouvelles salles pédagogiques et des comptes associés s'ajoutait au renouvellement de celles déjà existantes.

A tout cela s'ajoutait un besoin de sécurisation et de maîtrise de nos environnements numériques mis à disposition qui se faisait de plus en plus prégnants.

Les effectifs au sein du service informatique, tant au niveau des ingénieurs en charge des systèmes et des réseaux que des techniciens restaient constant malgré un contexte toujours en pleine expansion.

L'ensemble des facteurs cités nous a amené à nous questionner sur nos pratiques et à chercher des solutions d'optimisation des déploiements des systèmes d'exploitation et de logiciels.

Nous verrons donc dans un premier temps un bref historique de nos pratiques de l'époque et les contraintes de nos choix quant aux plateformes de déploiements choisies ainsi que nos perspectives pour les années à venir.

2 Méthodes de travail historiques

2.1 Principes de déploiement

Avant 2013, le déploiement de systèmes d'exploitation et de logiciels se faisait depuis des images de postes masterisés.

Cette méthode, que toute personne en charge de ce type de mission connaît, demandait la préparation d'une machine issue du stock de machine à déployer, l'installation du système d'exploitation (OS), des mises à jours système, des pilotes de périphériques et de la suite des logiciels nécessaires aux objectifs fixés à son usage. À la suite de cette installation fastidieuse, une image était extraite grâce au logiciel de déploiement utilisé : la suite Ghost (General Hardware-Oriented System Transfer) de Symantec.

Ensuite cette image était stockée sur un périphérique de stockage suivant une règle de nommage la rendant accessible parmi les GigaOctets de données d'images masterisées déjà présentes.

Ce déploiement d'images s'effectuait ensuite en utilisant un réseau local déployé dans la salle. Les postes à installer étaient connectés à un commutateur indépendant du réseau où était également relié un ordinateur portable jouant le rôle de serveur de déploiement multicast. L'objectif était de paralléliser le déploiement de l'ensemble des postes.

Le collègue technicien devait ensuite effectuer des tâches de post-traitement pour modifier les identifiants et mots de passes locaux et les identifiants de la machine Windows.

Le temps d'installation d'une nouvelle salle de travaux pratiques (TP), avec l'ensemble des tâches constituant ce processus de déploiement, était d'environ 5 jours.

2.2 Problématiques et besoins

En lisant le processus de déploiement d'un poste de travail décrit ci-dessus, vous pouvez constater les problèmes auxquels l'ensemble de l'équipe était confronté : le délai de préparation des images, le volume de stockage très important, la dépendance des images aux matériels et périphériques issue de la masterisation (« Hardware dépendant¹ »).

De plus, le suivi de ces images présentait aussi la difficulté de connaître la version de chacun de ses composants et donc de maintenir une bibliothèque d'images avec tout ce que cela implique : métadonnée de stockage, durée et pertinence de conservation des images.

Enfin, il se posait aussi le problème du maintien en conditions opérationnelles du parc sur le long terme, comme la gestion des mises à jour de sécurité et de fonctionnalité des logiciels installés. Ce mode de gestion impliquait de nombreuses interventions sur site de l'équipe de techniciens afin de mettre à jour ou désinstaller les logiciels.

Nous rencontrions donc trois besoins majeurs auxquels il était nécessaire de trouver des réponses.

Il nous fallait dans un premier temps réduire le temps de déploiement d'une salle pour gagner en réactivité. Les principaux points sur lesquels il était facile de gagner du temps

1. Dépendantes du matériel. Une image par configuration matériel.

étaient le déploiement de l'OS et une installation automatisée des logiciels depuis un gestionnaire centralisé. Une première étape de ces expérimentations a été effectuée sur la base des solutions de déploiement d'image déjà utilisées en y intégrant la dimension réseau avec pour les systèmes Linux , FOG² et pour le périmètre Windows, Ghost. Celle-ci restant très dépendante des caractéristiques matérielles des machines, une seconde étape de réflexion, développée sur le chapitre suivant, a été effectuée.

Le second point à faire évoluer était de garder le parc en conditions opérationnelles après le déploiement. Afin de respecter la politique de sécurité des systèmes d'information (PSSI) et les bonnes pratiques, il fallait que les logiciels soient faciles à maintenir à jour. L'équipe technique devait pouvoir maintenir les applications à distance, de façon synchrone et/ou asynchrone. Elle devait pouvoir aussi installer un nouveau logiciel à distance et de manière automatisée.

Enfin, il fallait également pouvoir mettre en œuvre de la délégation de droits à différents niveaux³.

2.3 L'étude des solutions

Maintenant que les besoins ont été identifiés il est temps d'étudier le marché. Cela nous a permis ainsi de connaître les différentes solutions qui pourraient correspondre au projet. Il a fallu ensuite les comparer entre elles et effectuer un choix.

Nous découperons ce chapitre en deux parties, d'un côté l'étude sur les solutions de déploiement de systèmes d'exploitation, de l'autre sur celles de déploiement de logiciels.

La réponse à notre problématique pouvait être une solution capable de gérer à la fois le déploiement de systèmes d'exploitation et de logiciels, ou être composée de deux solutions (une pour l'OS, l'autre pour les logiciels) qui collaboreraient entre elles ; nous n'avons aucune préférence sur ce point.

Les différentes solutions alternatives que nous avons évalué sont DELL Kace, Microsoft SCCM, UpdateEngine, GPO, OCS, WPKG.

2.3.1 Les solutions de déploiement d'OS

DELL KACE K2000

Cette application était, au moment de notre test en 2013, accessible sous forme d'appliance virtuelle exposant une interface Web d'administration. Solution commerciale proposée par la société DELL suite au rachat de Quest, la plateforme K2000 propose le déploiement de systèmes d'exploitations via le réseau uniquement de type Microsoft Windows par création d'image disque non dépendante du matériel.

SCCM / MDT

Cette solution Microsoft de déploiement de système d'exploitation Windows et de distribution logicielle est une référence sur le segment. Elle permet entre autres la remontée d'inventaire de parc et d'administration à travers une console de type client

2. Free OpenSource Ghost - <https://fogproject.org/>

3. Administrateurs globaux, équipe de proximité, administrateurs locaux, utilisateurs

lourd. Celle-ci est basée sur les solutions Microsoft Deployment Toolkit (MDT) et Windows Deployment Service (WDS), pour le démarrage réseau via PXE, qui sont également accessibles sans surcoût, contrairement à SCCM qui est une solution payante. Nous avons retiré SCCM rapidement car les deux solutions retenues sont similaires. MDT, correspond à un SCCM simplifié. Elle semble répondre parfaitement à nos besoins, bien que seul le déploiement Windows ne soit possible, mais le parc de l'université étant composé à plus de 90% de système Windows, MDT semble le bon candidat. Il permet de créer une image Windows à déployer sur les postes avec une gestion de pilotes possible.

2.3.2 Les solutions de distribution de logiciel

DELL KACE K1000

Dans la gamme des appliances Kace, une seconde plateforme de déploiement de logiciels, la plateforme K1000, est présentée de la même manière permettant la gestion des inventaires et la distribution de logiciels, la gestion des correctifs, des actifs et un helpdesk. Pour effectuer les déploiements de paquets logiciels il est nécessaire de déployer un agent sur chacun des postes clients à administrer. Une troisième solution DELL, la K3000, permettait de gérer des périphériques mobiles de type tablette et smartphone.

Malgré une solution logicielle intéressante, le coût de l'ensemble de la suite est assez important au vu du nombre de machines du parc et du budget prévisionnel alloué.

WPKG

La solution WPKG a été éliminée assez rapidement pour la principale raison qu'elle ne permettait pas d'avoir une visibilité et une gestion centralisée du parc informatique et des logiciels déployés sur les postes. De plus, la distribution logicielle s'effectuait au démarrage du poste client et n'est pas reportable.

Elle permet simplement de créer des paquets sur le serveur WPKG, puis ensuite il faut installer un client sur les postes, client qui permettra de récupérer et installer automatiquement les paquets que l'on souhaite, présents sur le serveur, ou de faire les mises à jour de ceux-ci. Mais cette manipulation d'installation et de mise à jour est à faire manuellement sur les postes par lignes de commande.

WAPT

La solution WAPT permet de déployer les logiciels en les préparant préalablement sous forme de paquet et de gérer leur cycle de vie sur le parc informatique par l'intermédiaire d'une console centralisée de gestion lourde. Elle peut également programmer les installations ou mises à jour des logiciels.

Ce déploiement logiciel s'effectue à la fermeture de la session utilisateur

La création des paquets logiciels est un peu plus lourde puisque cette solution est entièrement basée sur l'utilisation du langage Python, mais cela offre donc plus de possibilités pour la personnalisation des paquets.

En réalité, grâce au langage Python adopté par les paquets, presque tout est possible du lancement d'une simple commande, à la copie de fichier, jusqu'à la modification de clés de registre. Il est également possible d'effectuer les actions d'installation de paquets, mises à jour ou encore désinstallation grâce à l'utilisation de l'invite de commandes Windows à la manière de apt de Debian (les créateurs de cette solution se sont d'ailleurs inspirés du fonctionnement de apt, d'où le nom WAPT). Seul bémol à cette solution, il n'y a pas de délégation de droits au niveau de la console de gestion.

Du côté des solutions purement orientées distribution de logiciels, nous avons aussi étudié les solutions suivantes :

- UpdateEngine : accessible depuis un client web, développement effectué par une communauté très restreinte. Le déploiement s'effectue via des paquets logiciels sur le même principe que WAPT ;
- GPO: issu de stratégie de l'Active Directory du domaine, le déploiement logiciel est lié à l'application de ces dernières sur le poste client sans visibilité sur le bon déploiement ni le moment exact du déploiement ;
- OCS: cette application propose une interface Web de gestion d'inventaire avec une extension de distribution de paquet logiciel.

Nous noterons que même s'il est possible de déployer des logiciels avec MDT et SCCM, nous n'avons retenu que ces solutions car leurs fondamentaux sont le déploiement de systèmes d'exploitation.

Nom	Propriétaire / Open source	Payant	OS des clients	Type de déploiement	Remarques
OPSI (Open PC Server Integration)	Open source	Non	Windows	Installation initiale + gestion	Client-serveur
MDT (Microsoft Deployment Toolkit)	Propriétaire	Non	Windows	Installation post-déploiement système	Pas de gestion post installation
FOG (Free Opensource Ghost)	Open source	Non	Linux	Installation post-installation système	
Dell KACE K1000	Propriétaire	Oui	Windows, Linux et Mac	Installation initiale + gestion	Client-serveur + licence pour 100 postes puis licence par poste supplémentaire
WAPT (Windows APT)	Open source	Non	Windows	Installation initiale + gestion	Client-serveur + paquets codés avec python + interface web disponible pour les postes sur lesquels le client est installé
UpdatEngine	Open source	Non	Windows et Linux	Installation initiale + gestion	Client-serveur + Interface web + pas de désinstallation possible + Programmation du déploiement
WPKG (Windows Package)	Open source	Non	Windows	Installation initiale	Client-serveur
SCCM	Propriétaire	Oui	Windows	Installation post-installation système	Pas de gestion post installation

Tableau comparatif des solutions étudiées pour déploiement de logiciels

2.3.3 Les solutions retenues

Les critères de choix pour la solution de déploiement de système d'exploitation pour notre parc Windows étaient les suivants :

- déploiement par le réseau ;
- image non dépendante du matériel ;
- parallélisation des déploiements.

La solution retenue était MDT avec le démarrage réseau WDS.

En ce qui concerne le choix de l'outil de déploiement de logiciel nous avons écrit un cahier des charges afin de trouver la solution qui correspond le plus à nos besoins.

Les critères étaient de permettre :

- l'installation de logiciels de manière automatique et silencieuse ;
- le retour d'information sur la réussite ou l'échec d'un déploiement ;

- la gestion du cycle de vie⁴ des logiciels ;
- l’inventaire du parc au niveau des logiciels déployés.

La solution WAPT correspondait à l’ensemble des critères évoqués en plus d’être OpenSource et de ne pas présenter de surcoût.

3 WAPT au sein de l’Université de Valenciennes

3.1 POC de la solution et tests

Bien que des tests furent faits avant le choix définitif des solutions, des tests plus avancés devaient être effectués pour s’assurer que les solutions répondent entièrement à nos besoins. Nous avons installé une première version sur un environnement de pré-production, afin d’effectuer des tests de performance et d’utilisation sur le réseau de l’université.

Ce passage en environnement de pré-production nous a également permis de faire une démonstration plus poussée du déploiement des postes clients à laquelle a participé l’ensemble du personnel du pôle infrastructure de services et réseau. Ainsi, les techniciens ont pu tester réellement l’utilisation des solutions MDT et WAPT, ce qui nous a permis de recueillir leurs impressions sur le système proposé. Ils ont donc pu tester le déploiement de 3 ordinateurs, chacun avec une configuration spécifique, l’un dans le domaine administratif, un autre dans le domaine enseignement et le dernier hors domaine. À l’issue de cette démonstration les techniciens étaient enthousiastes et semblaient prêt à utiliser cette solution le plus tôt possible.

Ces tests nous ont aussi permis d’évaluer les performances des deux solutions, ainsi nous avons mis entre 30 et 40 minutes pour déployer des machines de moyenne gamme en termes de matériel, mais dans de bonnes conditions réseau⁵, pour une installation de Windows 7 Professionnel 64 bits et un socle commun de 13 logiciels. Ce temps est similaire pour un poste isolé ou pour le déploiement de plusieurs postes simultanément (tester pour 3 à 5 postes). À noter qu’auparavant le temps moyen de déploiement d’une salle allait d’une à deux journées.

Dans l’objectif de standardisation de la méthode de déploiement des postes clients, cette démonstration et des réunions antérieures avec les techniciens nous ont permis de dresser une liste de 13 logiciels qui feront partie d’un socle commun qui sera déployé sur toutes les nouvelles machines. Ainsi chaque poste de l’université aura une base commune que ce soit en termes de configuration du système, mais aussi en termes logiciels. À ce socle commun de logiciels, deux « sous socles » viennent s’ajouter l’un pour les machines du domaine administratif, l’autre pour celles du domaine enseignement.

WAPT installera les paquets ou effectuera les mises à jour à des moments précis. Il y a donc plusieurs possibilités pour lancer l’installation ou les mises à jour, on le force via la

4. Mise à jour ou désinstallation de ces logiciels

5. Entre 100 Mbit/sec et 1Gbit/sec, dans le même bâtiment que le serveur

console, en ligne de commande sur le poste client ou lors de l'arrêt ou du redémarrage de la machine.

C'est cette dernière méthode qui sera utilisée la plupart du temps et qui permettra de maintenir à jour le parc informatique. L'installation forcée depuis la console servira aux gestionnaires de parc afin de gérer une demande utilisateur de façon synchrone et rapide.

3.2 Installation et configuration

Cette installation est plutôt un passage de l'environnement de pré-production à l'environnement de production. En effet, en ce qui concerne MDT, les tests avaient été effectués sur un serveur physique dédié uniquement à cette solution, et pour WAPT il s'agissait d'un serveur virtuel sous VMWare. Il a juste fallu modifier les configurations des serveurs pour qu'ils soient visibles sur le réseau de l'université. Ces modifications de configurations ont été surtout de l'ordre d'ajout de résolution de nom DNS, de modifications du DHCP pour indiquer l'adresse du serveur PXE (MDT WDS), et des VLANs pour qu'ils acceptent le démarrage sur le réseau et trouvent le serveur PXE.

La configuration du serveur WAPT, pour le déploiement des logiciels, est assez simple. Elle est guidée lors de l'installation de la solution sur le serveur, et l'on peut trouver un tutoriel d'installation en français et en anglais sur le wiki officiel de WAPT⁶. Nous pouvons installer la partie serveur de WAPT sur un serveur Linux Debian ou un serveur Windows. Dans notre cas nous avons choisi de mettre en place, arbitrairement, la solution WAPT sur un serveur Windows, serveur virtuel sous VMWare.

La dernière configuration au niveau du serveur est la création d'une clé de signature. Cette clé est générée automatiquement et est primordiale dans l'utilisation de la solution. En effet, tous les paquets de logiciel créés sont signés par cette clé. Si la machine cliente ne possède pas la clé de signature publique propre au serveur, alors elle refusera d'effectuer les actions d'installation, de mise à jour ou de désinstallation du paquet. C'est une sécurité pour éviter l'installation par la solution de paquets qui ne sont pas vérifiés.

Une fois le serveur configuré, la solution WAPT propose de créer un agent personnalisé. La création de cet agent personnalisé permet d'adapter le client à l'environnement de l'université et son serveur WAPT. Une fois cet agent personnalisé configuré, le serveur crée un exécutable qui permettra d'installer le client WAPT sur les machines du réseau de l'Université. L'installation de l'agent peut se faire de plusieurs manières : soit une installation classique, en téléchargeant l'exécutable et en l'installant silencieusement ou non, soit par stratégie réseau (GPO).

Pour terminer la configuration de WAPT, il ne reste que la création des paquets logiciels. En effet, il faut créer un paquet sous un format particulier pour chaque logiciel à installer. WAPT utilise le langage Python pour la création des paquets et leur gestion à travers le parc informatique.

Un paquet WAPT c'est donc les sources d'installation du logiciel, un fichier d'identification du paquet (nom logiciel, version, dépendances et conflits logiciels, ...), et un fichier écrit en Python avec les instructions d'installation, de mise à jour et de

6. <https://www.wapt.fr/fr/doc/>

désinstallation. C'est ce dernier fichier qui est le plus important car il va définir les actions à effectuer lors du déploiement des logiciels. Typiquement on trouve dans ce fichier les lignes de commandes d'installation silencieuse du logiciel.

L'installation silencieuse, c'est une installation automatisée et scriptée, sans interface utilisateur. Pourquoi vouloir mettre en place des installations silencieuses ? Tout simplement car de cette manière si les ordinateurs cibles sont utilisés, nous pourrons effectuer des installations, désinstallations ou mises à jour de manière transparente pour l'utilisateur.

Le dernier point intéressant de la solution est la mise à disposition de bibliothèques⁷ de paquets logiciels nous permettant une réutilisation de ces paquets existants, simplifiant la prise en main et la mise à jour de notre catalogue local.

3.3 Les adaptations locales

Sur le premier déploiement de la solution, une ombre reste au tableau.

En effet, malgré toutes les fonctionnalités proposées par cette plateforme, un point important reste en suspens : la délégation et différenciation de droits des utilisateurs de la console. En effet, seul un compte administrateur est proposé.

Sur ce constat, une interface Web en surcouche de l'agent WAPT a été développée utilisant les mécanismes (flux JSON) et API natif de l'application et ainsi permettre la délégation de droits auprès de l'équipe de techniciens de proximité.

Une autre limite à l'usage de WAPT : les paquets lourds (plusieurs Giga) et la gestion des ordinateurs portables se connectant peu au sein de l'établissement pour lesquels des solutions manuelles doivent être mises en œuvre en limitant l'automatisation de la distribution.

4 WAPT aujourd'hui

4.1 Ré-Organisation

Les évolutions du produit ont continué et TranquilIt a choisi de proposer une nouvelle version, la version *Entreprise*.

Cette nouvelle version ajoute les fonctionnalités suivantes :

- Séparation des rôles entre les développeurs de paquets et les *déploieurs*⁸ de paquets. De cette façon, les paquets WAPT peuvent être conçus par les équipes informatiques de l'entreprise pour suivre les directives de sécurité de celle-ci et ils sont ensuite déployés par les équipes informatiques locales. Une telle différenciation est mise en œuvre au moyen de jeux de certificats SSL différenciés ;
- Authentification Active Directory des développeurs et des déploieurs de paquets WAPT ;

7. <https://wapt.tranquil.it/> ou <https://wapt.lesfourmisduweb.org/>

8. Néologisme afin d'imager la tâche de ce rôle ; comprendre : personne qui gère le déploiement des paquets.

- Affichage des périphériques dans la console de gestion WAPT suivant la structure hiérarchique de nos UO⁹ Active Directory ; Possibilité d’assigner les paquets au niveau de ces UO ;
- Utilisation de self-services différents qui permet d’assigner des paquets à des groupes Active Directory. Les utilisateurs peuvent être autorisés à installer eux-mêmes des paquets depuis la liste des applications autorisés sans demande d’intervention à l’équipe de techniciens et sans être administrateurs locaux ;
- WAPT WUA¹⁰ permet de gérer les mises à jour Windows ;
- Reporting avancé pour les équipes de direction. Ces rapports complètent les rapports opérationnels déjà disponibles dans la console de gestion.

Afin de faciliter l’exploitation d’un parc en constante évolution, le choix a été fait de prendre cette version *Entreprise*. Cet abonnement nous donne aussi accès au support pour l’usage courant de Wapt ainsi qu’à des formations sur n’importe quel aspect du produit.

Nous avons décidé de réorganiser nos méthodes de travail afin de prendre en compte la fonctionnalité de séparation des rôles de développeurs et de déployeurs. Nous avons créé pour chaque technicien un couple de clés afin que chacun accède à ces deux rôles. Ainsi nous avons découpé notre infrastructure en deux parties afin de sécuriser les développements, ce que nous détaillerons dans le chapitre suivant.

L’utilisation de compte nominatif ainsi que de clés personnelles permet à chacun de suivre l’évolution des paquets en sachant par exemple si un collègue a fait évoluer un paquet ou si quelqu’un travaille sur la mise à jour de tel ou tel produit.

Nous avons créé au sein de nos équipes deux populations : les *administrateurs* et les *gestionnaires de parc*¹¹.

4.2 Infrastructure WAPT

Pour rattraper les mises à jour de la solution, nous avons voulu repenser notre installation pour intégrer les évolutions qui remplacent nos développements maison. Nous avons réinstallé la solution avec une version à jour en intégrant les paquets déjà développés et mis en production.

Mais pour prendre en compte la nouvelle séparation des rôles, nous avons mis en place deux environnements distincts : un environnement de production et un environnement de développement.

Depuis la console, les *gestionnaires de parc* peuvent accéder à ces deux environnements avec une clé différente. Sur l’environnement de production ils ont les droits de déployeurs, ce qui permet de créer des groupes de machines ou de choisir quels paquets y déployer.

Sur l’environnement de développement ils ont tous les droits (développeurs et déployeurs) afin de leur permettre d’avoir un environnement où chacun peut importer, développer et tester des paquets sans impacter l’environnement de production.

9. Unité d’Organisation au sens Active Directory.

10. Windows Update Agent

11. Ces deux rôles seront développés dans le chapitre suivant

Une fois le paquet testé et validé, un administrateur l'importe en production pour commencer à le déployer sur le parc. Cette « validation » évite surtout les doublons ou l'écrasement d'un paquet en production.

5 Conclusion

En 2013, au vu des problèmes mentionnés au début de cet article dans le déploiement et mise à jour des postes clients, nous avons choisi et déployé la solution Wapt car celle-ci correspondait pleinement à nos besoins et à notre politique de sécurité. Cette infrastructure a largement contribué à une meilleure gestion des postes et un gain de temps indéniable. Les développements internes avaient pallié le manque de délégation de droits sans toutefois nous satisfaire pleinement.

Devant la réussite de l'intégration de Wapt dans notre environnement de travail, en 2019 nous avons fait le choix de poursuivre avec la nouvelle version *Entreprise* .

La délégation des droits, la séparation des rôles ainsi que la modification de nos habitudes de travail nous ont encore permis de passer un pallier dans la gestion de parc ; à la satisfaction de tous les membres de la DSI.

Des points restent cependant à améliorer : la gestion des logiciels « lourds » ainsi que les ordinateurs portables.

Nous sommes toujours en permanente recherche d'amélioration de notre parc. C'est pourquoi nous évaluerons, dans l'avenir, la mise en place de briques de Wapt que nous n'avons pas encore testé jusqu'ici: gestion des mises à jour de Windows ou self-service pour les paquets communs. Cette dernière fonctionnalité sera probablement la prochaine étape dans notre évolution de l'utilisation du produit car elle apporterait un complément de service aux utilisateurs finaux mais surtout une réactivité bien plus importante. Et ce sans sacrifier la sécurité des machines concernées car les paquets seront vérifiés, testés et maintenus par la DSI.