Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Étude de solutions pour le retrait des droits administrateurs aux utilisateurs

EDOUARD Mathieu

Groupe SNEF

Responsable entreprise : Mr Philippe VIAUD

Responsable académique : Mr Ivan MADJAROV

2019

Table des matières

1 Introduction

Le stage que j'ai effectué s'est déroulé sur une période de 10 semaines du 8 avril au 14 juin 2019. J'ai été intégré au sein du Groupe SNEF étant la 5e entreprise de Marseille et possédant son siège dans la zone des Arnavaux. Le service dans lequel j'ai évolué est celui de l'informatique CI.

L'objectif de ce stage était l'étude et la recherche de solutions dans le but de retirer les droits administrateurs aux utilisateurs et donc employés du groupe. En effet, dans le cadre d'un projet de sécurisation informatique, cette étape est à la fois cruciale et complexe car non sans conséquences. J'ai donc été amené à faire des tests et à rédiger des documents pour les différents choix et processus que j'ai présentés à l'entreprise.

Nous verrons donc à travers ce rapport le travail réalisé pour essayer de répondre à cette problématique et proposer des solutions adaptées et efficaces. Dans un premier temps, nous développerons sur l'entreprise et ses activités. Puis, nous verrons le cadre technique général du sujet avant d'aborder la présentation du travail réalisé.

2 Présentation de l'entreprise

Le Groupe SNEF a été créé en 1905 à Marseille. Depuis cette création, les compétences majeures de l'entreprise sont les domaines des énergies et des procédés industriels. Cependant, les activités de l'entreprise sont aujourd'hui vastes et sujettes à s'étendre au vu de la politique menée. En effet, le groupe dispose d'une grande diversité avec des corps de métiers variés avec les courants faibles, les télécommunications, le nucléaire, le génie climatique, la maintenance ou les procédés industriels. Depuis 2015, ces différentes activités sont regroupées en marques telles que SNEF Télécom, SNEF Nucléaire etc...
De plus, le groupe continue de s'étendre en acquérant de nouvelles filiales comme Ekium ou Watt Network.

Le Groupe SNEF est une entreprise disposant de 12000 collaborateurs dans 20 pays allant de l'Europe à l'Amérique du Sud en passant par l'Afrique et les Emirats Arabes Unis. C'est donc une multinationale. Elle a également réalisé un chiffre d'affaire d'1,4 milliards d'euros pour 2018 contre 1,1 milliards en 2017 et poursuit sur sa forte croissance depuis 3 ans. Son siège social (Figure 1) situé à Marseille dans la zone des Arnavaux compte près de 500 employés tandis que la direction s'est récemment installée dans la nouvelle tour La Marseillaise au cœur de la ville et du projet euroméditérannée.

Figure 1 : Siège du Groupe SNEF à Marseille

Les clients du groupe sont nombreux et à la fois de nature publique et privé. En effet, le groupe s'est illustré par de nombreuses réalisations avec par exemple la mise en lumière de la pyramide du Louvre à Paris, la réhabilitation de la galerie commerciale de l'aéroport de Lyon ou encore la participation à la construction de la tour D2 à Paris.

Une entreprise d'une telle envergure possède donc de nombreux types de métiers en son sein. J'ai donc personnellement intégré le service Informatique CI au siège à Marseille. Ce service est composé de 17 personnes assurant le maintien du réseau et de la téléphonie du groupe mais également le support aux utilisateurs. Le service est en relation avec un correspondant informatique par agence qui a pour fonction de communiquer avec le service et de réaliser, si nécessaire, les opérations sur place.

Le service Informatique CI est donc réparti sur 4 niveaux et organisé par ilots de 4 bureaux. Le premier ilot représente le niveau 1 avec comme missions principales le support client et le traitement des appels des utilisateurs mais aussi la préparation des ordinateurs et smartphones commandés par les employés. C'est à ce niveau qu'arrivent en priorité les appels des utilisateurs avant d'être soit traités directement par ce niveau soit d'être redirigés vers un autre niveau.

Le deuxième ilot représente le niveau 2 qui a aussi pour mission de traiter une partie des appels et les tickets liés à la gestion des comptes de l'annuaire de l'entreprise. De plus, la préparation des serveurs et équipements d'infrastructure est également gérée par ce niveau.

Le niveau 3 étant donc sur le 3eme ilot est le niveau des projets et assure donc en tant que mission principale la gestion des projets et de l'évolution de l'informatique dans le groupe. Ils effectuent aussi des tâches de support et de gestion de réseaux et systèmes.

Le niveau 4 est lui assigné à la gestion de la téléphonie et du réseau mais, ici encore, leurs tâches sont en réalité nombreuses et ils peuvent aussi être amenés à faire du support principalement avec les correspondants informatiques.

Enfin, le service dispose également d'un chef de service et d'un RSSI, Responsable de la Sécurité des Systèmes d'Information. Le service est en open space et la communication entre les différents niveaux est donc aisée. Cela m'a aussi permis de communiquer et d'apprendre facilement avec des personnes de tous les niveaux.

3 Présentation du cadre général

3.1 Contexte

Comme c'est le cas pour un nombre important d'entreprises et ce, par soucis de simplicité, le Groupe SNEF donnait à ces utilisateurs des droits d'administrateur local de leur poste. En effet, de nombreuses fonctionnalités de Windows sont inaccessibles aux utilisateurs standards comme par exemple l'installation de logiciels ou encore la modification de l'adresse IP.
Un retrait de ces droits administrateurs locaux sans mesures préalables serait donc très dangereux pour la productivité des utilisateurs et pourrait également surcharger le service informatique du fait d'un nombre élevé de demandes qui pourraient survenir.

Également, les postes commandés par les utilisateurs et préparés par le service informatique étaient souvent préparés avec un compte administrateur local possédant un mot de passe identique sur chaque poste.

Pour la gestion de ses utilisateurs, le groupe utilise le gestionnaire d'annuaire de Windows appelé Active Directory. Il est ainsi possible de gérer leurs droits, de les placer dans des groupes et possiblement de leur appliquer des stratégies de groupe pour gérer de nombreux paramètres.

Enfin, en ce qui concerne le contexte dans l'entreprise, j'ai donc eu accès à des ordinateurs et équipements réseaux pour réaliser ma maquette mais également à des licences de logiciels et Windows pour mes tests. J'avais un bureau personnel et était placé dans l'équipe projet avec qui le travail fut très agréable.

3.2 Objectifs

Le groupe recherchait donc un stagiaire afin de proposer des solutions pour amorcer le retrait des droits administrateurs tout en conservant la productivité des utilisateurs/employés du groupe. L'objectif était donc de réaliser une maquette puis trouver des solutions afin de pouvoir effectuer des tests des solutions choisies. Puis, en tant que trace de mon travail et de mon apport à l'entreprise, j'ai rédigé des documents afin de permettre au service de poursuivre le projet et prendre en compte mes recherches.

Les objectifs détaillés de mon projet étaient donc de trouver une solution pour, dans un premier temps, retirer les droits administrateurs à tous les comptes de l'Active Directory et donc à tous les

utilisateurs de l'entreprise (environ 5 000 postes). Puis, il a fallu trouver des solutions pour que ce retrait de droits ait un impact le moins important possible pour l'utilisateur afin d'éviter le plus de plaintes possibles qui pourraient faire reculer la direction sur le projet. Enfin, le 3e objectif était la sécurisation des comptes locaux disposants d'un mot de passe similaire.

Le dernier objectif, qui n'était pas prévu au début du stage, a été de trouver une solution aux problèmes de changement de mot de passe de compte en dehors du réseau de l'entreprise et donc en dehors de la connexion aux serveurs contrôleurs de domaine qui gèrent l'Active Directory de l'entreprise. En effet, les utilisateurs une fois en dehors du réseau se retrouvent dans l'impossibilité de changer leur mot de passe et leur compte est donc bloqué. Cela nécessitait donc un appel au support qui devait traiter ces demandes.

3.3 Profil

Lors de l'entretien de motivation, l'une des qualités qui était souhaitée était tout d'abord une bonne communication que cela soit pour l'oral ou pour l'écrit. L'autonomie était aussi importante pour ce stage car l'objectif n'était pas de perturber les personnes du service dans leur travail quotidien étant déjà conséquent. J'ai donc dû faire preuve d'autonomie mais cela ne m'a pas empêché tout d'abord d'apprendre beaucoup de choses mais aussi de communiquer avec mon équipe qui possède une variété de connaissances et compétences dont j'ai également pu me servir.

4 Présentation du travail réalisé

4.1 Mise en place de la maquette

Afin de réaliser mes tests et de pouvoir donner un avis exact des différentes solutions proposées, il m'a fallu créer une maquette pour reproduire de façon fictive et simple le fonctionnement de l'entreprise. J'ai donc créé une maquette assez simple suivant ce schéma (Figure 2). Elle est donc simplement constituée d'un switch et de deux ordinateurs physiques. Le premier étant un ordinateur portable relativement basique que pourrait utiliser un employé du groupe. Il est sous le système Windows 10 et possède 4go de mémoire ram*. Le deuxième ordinateur utilisé était un ordinateur qui avait pour but de jouer le rôle des différents serveurs du groupe. En effet, cet ordinateur exécutant Windows Server 2012 R2 et possédant 16go de mémoire ram, il a été possible via le système de virtualisation Hyper-V de créer des machines virtuelles* pour reproduire d'autres serveurs sur la même machine physique.

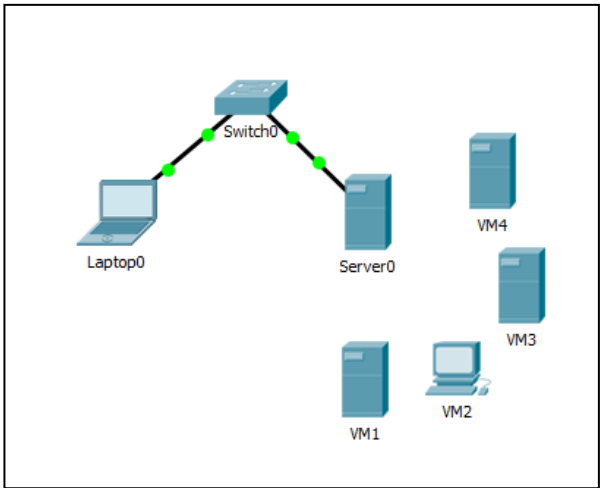

Figure 2 : Représentation de la maquette

Cette maquette représente donc grossièrement le réseau du groupe et permet de faire des tests afin de vérifier le fonctionnement et d'avoir le point de vue à la fois du système informatique gérant les serveurs et des employés/utilisateurs. Cela m'a notamment permis d'évaluer les solutions les plus équilibrées entre les deux parties en ne sacrifiant pas trop de temps de travail pour l'administration mais aussi en essayant de réduire l'impact des changements pour les utilisateurs quotidiens.

On remarque donc sur cette représentation de la maquette (Figure 2) à la gauche du switch le poste utilisateur et la droite le serveur avec les machines virtuels qu'il intègre autour de lui.

4.2 Introduction à l'Active Directory

Au cours de ce stage, le thème que j'ai le plus approfondi aura finalement été l'Active Directory de Microsoft. Nous avions déjà des bases dans le domaine de la gestion des annuaires grâce aux cours dispensés à l'IUT, Institut Universitaire de Technologie. Cependant, les connaissances que nous avions acquises étaient plutôt basiques et nous n'avions pas de référence concrète concernant son fonctionnement au sein d'une grande structure telle qu'une entreprise. Il est important de proposer une introduction à cet outil car nous aborderons par la suite des termes qui y sont liés et qu'il faudra connaître afin de comprendre le raisonnement global.

L'Active Directory est un annuaire dit LDAP, Lightweight Directory Access Protocol. Il a été introduit dans les années 2000 et est fait pour les systèmes d'exploitation Windows. Active Directory étant donc un annuaire, il contient différents objets comme des utilisateurs, des ordinateurs, des groupes etc…
Son objectif est l'identification et l'authentification au sein du système d'information. Il est particulièrement utilisé par les entreprises pour ses fonctionnalités de déploiement de stratégie de groupes, d'authentification des utilisateurs sur les postes, de déploiement de logiciels ou d'installation de mises à jour. En effet, l'annuaire Active Directory simplifie grandement la gestion d'un parc important de postes et permet aux administrateurs de l'entreprise de gérer finement les accès et les droits donnés aux différents utilisateurs.

L'annuaire Active Directory est organisé selon une structure précise. En effet, l'Active Directory est une très grande base de données et elle a donc besoin d'être structurée. Sur la partie infrastructure, Active Directory fonctionne sur le modèle simple de client-serveur. On peut voir sur le schéma (Figure 3) que le contrôleur de domaine (Domain Controller en anglais) est directement connecté au switch comme les autres périphériques tels que les ordinateurs, imprimantes etc…
Si l'on prend ce modèle client-serveur, notre contrôleur de domaine sera notre serveur car c'est lui qui stockera les informations du domaine et répondra aux requêtes.

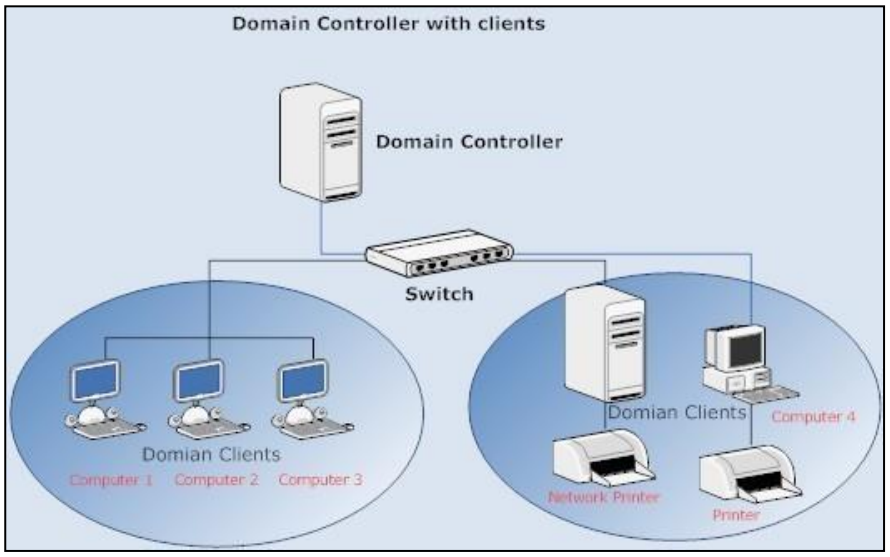

Figure 3 : Représentation d'un domaine Active Directory

En effet, le contrôleur de domaine contient les informations des objets présents dans le domaine (ordinateurs, utilisateurs, groupes…), du schéma du domaine, des stratégies de groupe et des informations d'authentification des utilisateurs. Les clients (ordinateurs, serveurs...) s'adressent à lui pour obtenir ces informations.

Sur le schéma (Figure 3), on peut par ailleurs voir la représentation d'un domaine. En effet, on a d'abord le grand rectangle dans lequel tous nos objets se trouvent qui représente un domaine. Un domaine peut-être une agence ou un service par exemple. Au sein d'une même entreprise on pourrait par exemple avoir un domaine pour la comptabilité, un autre pour l'administration et un autre pour les dirigeants comme sur la gauche du schéma (Figure 4) pour l'entreprise maboite. Cependant, le modèle le plus utilisé est celui qui fonctionne en fonction des emplacements. Il peut donc y avoir un domaine par localisation comme on peut le voir pour les domaines gtr à droite du schéma (Figure 4). En effet, on peut voir qu'il y a un domaine pour le Québec et un pour la France qui est potentiellement une agence de l'entreprise.

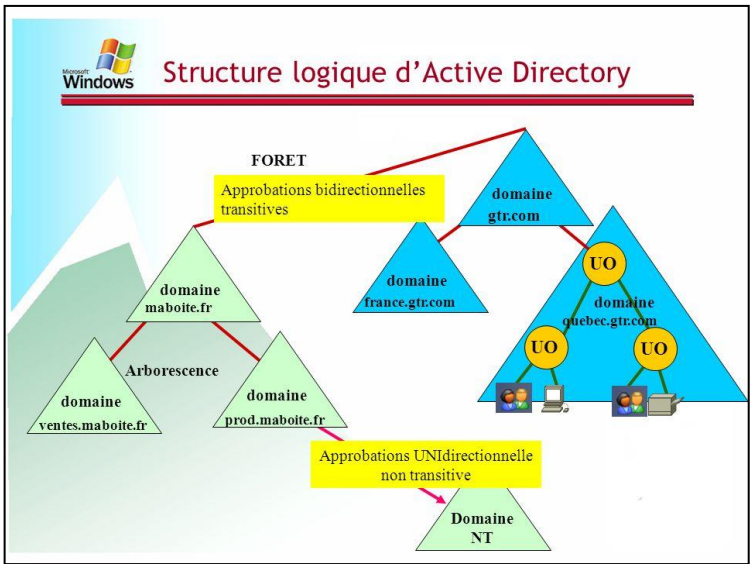

Figure 4 : Représentation d'une forêt Active Directory

Le schéma (Figure 4) introduit par ailleurs une notion que nous n'avons pas encore évoquée. Cette notion est celle de la forêt. Une forêt est en fait constituée de plusieurs domaines (que l'on pourrait donc caractériser par des arbres). Elle regroupe donc plusieurs domaines et permet de créer des relations d'approbation entre ceux-ci. Ces relations sont très utiles car elles permettent de mutualiser les informations des domaines concernés. Elles sont notamment utilisées lorsqu'une entreprise possédant son domaine acquiert une autre entreprise qui elle-même possède son propre domaine. Cela permet aux administrateurs de l'entreprise de simplifier la gestion de ces deux domaines en ayant accès sur l'un comme sur l'autre aux informations des deux domaines.

Nous pouvons à présent revenir sur notre premier schéma (Figure 3) pour évoquer le terme d'OU, Organizational Unit. En français, on le traduit par Unité d'organisation. Son nom est plutôt juste car les OUs permettent avant tout de « ranger » les différents objets que nous avons vu auparavant. En effet, on retrouve dans une OU principalement des ordinateurs, serveurs, utilisateurs et groupes. L'OU est en fait équivalent à un dossier dans lequel on rangerait nos objets. Par exemple, on peut tout à fait trier les utilisateurs, groupes et serveurs du service achat dans une OU « Achat ». Cela permet donc de mieux s'y retrouver lorsqu'on a un nombre important d'utilisateurs à gérer.
À titre d'illustration, dans notre schéma (Figure 3) l'OU est représenté par les cercles dans lesquels se trouvent des ordinateurs et imprimantes.

Le dernier élément que nous allons aborder sur l'Active Directory et le plus important à comprendre pour la suite de ce rapport est le terme de stratégie de groupe. Tout d'abord le terme que nous utiliserons pour les désigner est l'acronyme de son nom anglais GPO, Group Policy Object. La GPO donc, est une politique que l'on va appliquer à un ou plusieurs utilisateur(s) et/ou ordinateur(s). Les possibilités liées à la GPO sont immenses et ne pourront pas être toutes énoncées ici mais on peut en donner les fonctionnalités principales. Les GPOs sont utilisées dans les entreprises pour, par exemple, interdire une fonctionnalité Windows à un groupe d'utilisateurs (comme la personnalisation du bureau), déployer des logiciels, exécuter des scripts sur les postes à un moment défini, gérer le registre des postes ou encore définir des quotas de stockage pour les utilisateurs sur les postes. Cela ne s'arrête pas là et les possibilités sont nombreuses mais le principe de la GPO est donc d'agir sur les utilisateurs et les postes en créant des scénarios de fonctionnement le tout à distance sans action local sur les postes. À titre d'exemple, nous pourrions imaginer le cas d'une école possédant un domaine Active Directory et souhaitant que lorsque les élèves se connectent sur leur session ils n'aient pas accès au clic-droit sur le bureau afin d'éviter que l'élève crée des problèmes sur le poste. Cependant, l'école souhaiterait laisser ce droit aux professeurs et c'est donc avec la GPO que ceci sera réalisable. Afin de donner une illustration de sa configuration, nous pouvons nous référer au schéma ci-dessous (Figure 5) pour observer les paramètres que peuvent contenir une GPO.

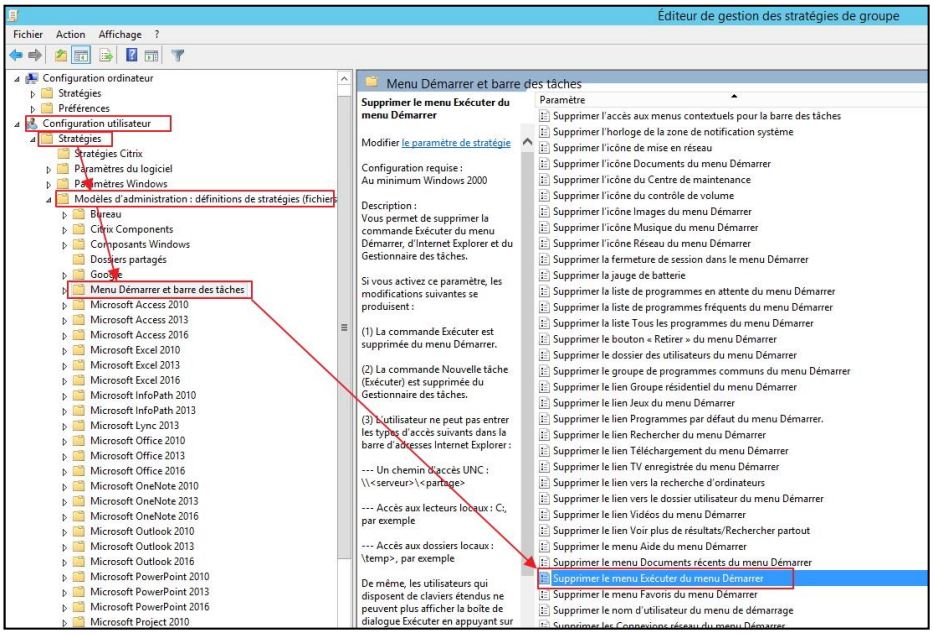

Figure 5 : Capture d'une fenêtre d'édition de GPO

On peut ci-dessus voir l'organisation de l'éditeur de GPO. Il y a donc une architecture des GPO avec des paramètres configurables étants ordonnés dans des dossiers et sous-dossiers. Ces paramètres possèdent tous une description pour donner des indications sur les effets qu'auront les différents états du paramètre. Il y a également à la tête de l'architecture les sections Configuration ordinateur et Configuration utilisateur. La différence entre les deux est que lorsque l'on choisit un paramètre dans Configuration ordinateur, le paramètre sera modifié pour tout l'ordinateur c'est-à-dire que peut importe avec quelle session nous nous connecterons dessus, le paramètre sera modifié suivant les informations que nous avons rentrées dans la GPO pour l'ordinateur. Également, une GPO Configuration ordinateur ne s'applique au poste que lorsqu'il démarre ou redémarre. À l'inverse, la Configuration utilisateur permet d'appliquer un paramètre à un ou plusieurs utilisateur(s) et ainsi de permettre, sur un même poste, à donner des règles différentes en fonction du compte avec lequel nous nous connectons. Ainsi, si l'on reprend le scénario de l'école précédemment énoncé, si un élève se connecte avec son compte sur le PC 1, il n'aura pas le droit d'effectuer un clic-droit sur le bureau. À l'inverse, si un professeur se connecte sur le PC 1 avec son compte, il aura le droit d'effectuer le clic-droit. Enfin, la GPO Configuration utilisateur s'applique lorsqu'un utilisateur se connecte à sa session.

4.3 Intérêt du retrait des droits administrateurs

Afin de bien comprendre la démarche de ce projet, il faut d'abord bien comprendre les conséquences et risque du non retrait des droits administrateurs aux utilisateurs. Tout d'abord, il faut comprendre que pendant de nombreuses années la sécurité informatique n'était pas une priorité pour les entreprises. En effet, l'informatique n'était déjà pas aussi rependue qu'aujourd'hui et les scénarios étaient bien plus simples à gérer. En effet, tout le monde ne possédait pas d'un ordinateur à son bureau, les attaques étaient moins présentes et la majorité des ordinateurs étaient fixes et reliés par câble et ne changeait ainsi quasiment jamais de réseau. Aujourd'hui, les choses ont évolué et la technologie étant plus utilisée et plus mobile, les failles sont plus importantes et les administrateurs doivent donc s'adapter pour proposer des solutions adaptées.

Les entreprises pouvant être par exemple amenées à travailler avec des systèmes d'exploitation ou des logiciels vieillissants, lorsque la sécurité dans le développement des applications n'était pas une priorité, les failles de ces logiciels ouvrent encore plus de failles aujourd'hui. Il est donc aujourd'hui important de proposer des solutions de sécurité informatique au sein des entreprises afin d'éviter de potentiels dégâts importants que peuvent créer des attaques informatiques. Cela est d'autant plus

important lorsque l'entreprise travaille avec des données sensibles. En effet, des virus ransomwares* comme WannaCry ou NotPetya ont fait perdre des millions d'euros à de grande entreprises. C'était par exemple le cas pour Saint-Gobain estimant sa perte de chiffre d'affaire à 220 millions d'euros sur la première moitié de l'année 2017 à cause des cyberattaques.

Figure 6 : Couverture d'article concernant le ransomware NotPetya

Les entreprises ont donc pris conscience de ces risques c'est pourquoi on retrouve une montée en puissance des postes de RSSI. Il y a également de nombreux projets de sécurisation menés par les entreprises. C'est donc dans ce contexte que mon projet a pris son sens. En effet, le Groupe SNEF a aussi entrepris un projet de sécurisation et le sujet du retrait des droits administrateurs sur lequel j'ai travaillé était donc une étape de ce projet que j'ai eu la chance de découvrir au travers d'une présentation menée par le RSSI à tout le service.

Concernant le seul problème des droits administrateurs, des études ont aussi été menées pour connaître l'impact des droits administrateurs sur les cyberattaques. C'est en autre ce que fait BeyondTrust avec son rapport annuel des failles Microsoft. En 2019, le résultat de ce rapport était donc que 81% des vulnérabilités des systèmes Microsoft pourraient être éliminées si les utilisateurs ne possédaient pas de droits administrateurs. Ce résultat est cependant à nuancer car BeyondTrust vend une solution facilitant le retrait des droits administrateurs mais cela donne tout de même un ordre d'idée de l'importance que représente cette question de droits administrateurs.

Le retrait de ces droits aura aussi l'effet d'un meilleur contrôle des logiciels installés par les utilisateurs/employés de l'entreprise car, auparavant, les utilisateurs étaient libres de télécharger les logiciels qu'ils souhaitaient sur les sites qu'ils souhaitaient. Mais, ce retrait impliquerait donc une incapacité d'installation des logiciels pour les utilisateurs sans avoir de mot de passe d'un compte possédant des droits administrateurs locaux de la machine. Il faudrait alors proposer une solution pour permettre aux utilisateurs de télécharger des applications/logiciels. Ainsi, la mise en place d'un store est cohérente et permettrait donc de ne proposer aux utilisateurs que des logiciels approuvés et ne disposant pas de virus dont la source est fiable.

4.4 Conséquences du retrait des droits administrateurs

Sur Windows, on distingue donc deux types d'utilisateurs. En effet, on peut être utilisateur standard ou administrateur de l'ordinateur. Contrairement à un administrateur de l'ordinateur, un utilisateur standard a donc des limitations dans ses droits. Il ne peut par exemple pas modifier la configuration du système ou installer des applications. En effet, des actions comme le changement d'adresse IP, la modification du mot de passe des autres utilisateurs, la création d'utilisateur sur le poste ou encore l'accès à certains documents du système sont interdites aux utilisateurs standards. Toutes ces

fonctionnalités et bien d'autres sont donc réservées aux administrateurs de l'ordinateur. L'utilisateur standard se retrouve donc avec peu de droits dans le cas de Windows mais peu cependant utiliser les applications déjà installées et peut tout de même largement travailler sur son poste.

Le retrait de ces droits administrateurs n'est donc clairement pas sans conséquences et les solutions aux problèmes éventuels que pourraient rencontrer les utilisateurs d'une entreprise avec un nombre important de postes sont donc à anticiper pour éviter un afflux important de demandes au service informatique. Dans la connaissance des contraintes qu'imposaient ce retrait, j'ai donc dû identifier dans un premier temps à partir de ma maquette et d'une configuration représentative d'un employé les effets indésirables du retrait des droits administrateurs. J'ai donc identifié trois problèmes majeurs : l'installation et la mise à jour des logiciels, la restriction de la modification des paramètres du poste et le lancement des logiciels demandant des droits administrateurs à l'exécution.

Ces paramètres sont donc très importants à solutionner pour permettre à l'utilisateur de garder une certaine autonomie à l'utilisation de son poste. En effet, l'intérêt est de ne pas obliger les employés à appeler le service informatique pour des demandes simples comme l'installation et la mise à jour des logiciels ou la modification de l'adresse IP du poste (souvent utilisé par les techniciens en déplacement). Le service informatique ayant déjà une grande charge de travail, il n'est donc clairement pas possible de déléguer des tâches supplémentaires comme celles-ci. De plus, cela ferait perdre de l'autonomie aux employés et empêcherait même certains de travailler s'ils sont en activité lorsque le service informatique est fermé.

J'ai donc recherché des solutions pour ces problématiques et ait pu les tester grâce à ma maquette afin d'en définir une procédure d'installation et d'administration. Je me suis également aidé de la présentation réalisée par la filiale Ekium du groupe sur leur projet de retrait des droits administrateurs fournie par le RSSI de mon service. Cela m'a donné une première idée des conséquences et des solutions possibles.

4.5 Installation des logiciels dans un contexte d'utilisateur standard

Afin de préserver la productivité et l'autonomie des employés, j'ai donc dû trouver et tester des solutions pour qu'ils puissent continuer à installer les logiciels dont ils ont besoin sans intervention du service informatique. J'ai donc retenu deux solutions pour effectuer cette tâche. Les deux solutions fonctionnent de la même manière : elles proposent, à la manière d'un magasin d'applications, des logiciels publiés par l'entreprise aux employés. Cette méthode de mise à disposition de logiciels par le service informatique permet deux choses importantes. En effet, le fait de proposer les logiciels que les utilisateurs pourront installer permet tout d'abord d'avoir un contrôle sur les logiciels qu'utiliseront les employés car ils devront être déployés et donc validés par le service informatique. Ensuite, cela permet de contrôler la source des logiciels installés et d'en finir avec les utilisateurs qui pourraient aller sur des sites malveillants et non officiels pour télécharger un installeur infecté d'un logiciel standard. Enfin, cela peut aussi avoir l'avantage d'être plus rapide pour l'utilisateur car il téléchargera son logiciel depuis le réseau de l'entreprise et il trouvera directement un installeur fonctionnel sans besoin de passer par internet.

Nous allons maintenant voir les solutions que j'ai retenues, installés et testés au cours du stage. Nous verrons dans un premier temps la solution du panneau de configuration puis dans un deuxième temps la solution SCCM, System Center Configuration Manager ou aujourd'hui Configuration Manager.

4.5.1 Solution du panneau de configuration

La première solution pour l'installation et la mise à jour des logiciels est la solution par le panneau de configuration. En effet, lorsque l'ordinateur fait partie d'un domaine, le panneau de configuration Windows possède une fonction de mise à disposition des programmes. Cette fonctionnalité se trouve dans : Panneau de Configuration > Programmes > Obtenir les programmes. Elle est également accessible d'une recherche dans le menu Démarrer de Windows en cherchant « Installer un programme à partir du réseau ». L'interface avec laquelle se retrouve l'utilisateur est donc celle-ci-dessous (Figure 7). On peut donc voir que son accès et son interface ne sont pas très facile à utiliser pour un utilisateur lambda. En effet, son accès par le panneau de configuration n'est pas optimal et l'interface proposée aux utilisateurs comporte plusieurs problèmes. La présentation des logiciels se fait sous forme de liste, l'utilisateur n'a pas la possibilité de trier les logiciels par catégorie pour effectuer des recherches plus rapides et trier les logiciels. Également, il est impossible de mettre une icône au logiciel installé. Du côté des utilisateurs cette solution n'est donc pas viable pour des employés ayant besoin d'un nombre important de logiciels mais peut être proposée pour mettre à disposition une liste courte de logiciels indispensables.

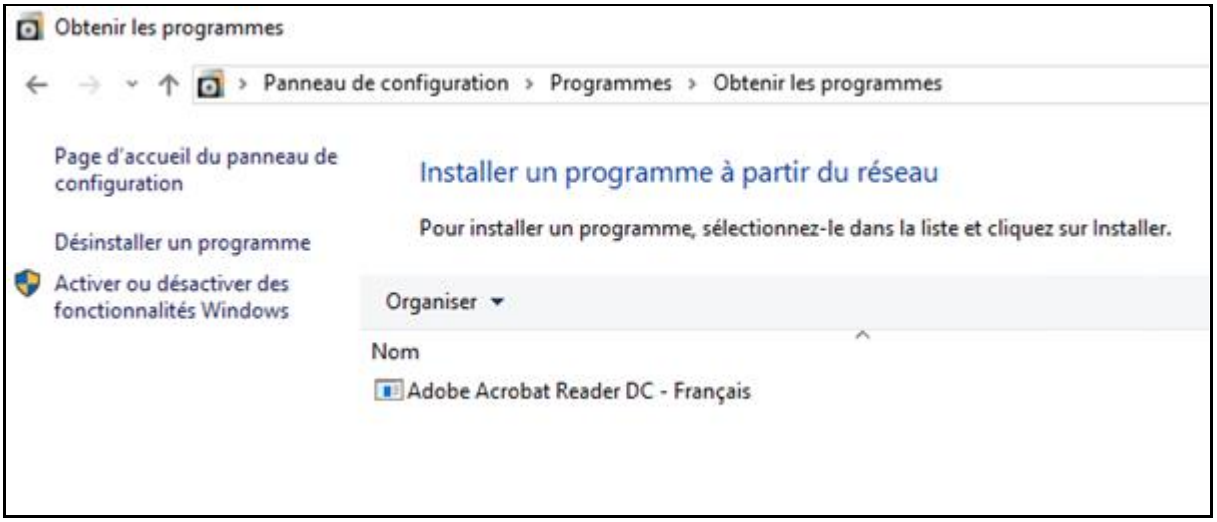

Figure 7 : Fenêtre "Obtenir les programmes" du panneau de configuration

Du côté des administrateurs et du service informatique, la solution est relativement simple à mettre en place car déjà intégré dans Windows et étant une fonctionnalité proposée dans l'Active Directory. En effet, le déploiement de logiciels dans le panneau de configuration s'effectue via une GPO*. Comme nous pouvons le voir dans la capture d'écran ci-dessous (Figure 8), nous retrouvons une catégorie « Installation de logiciel » dans l'éditeur de GPO.

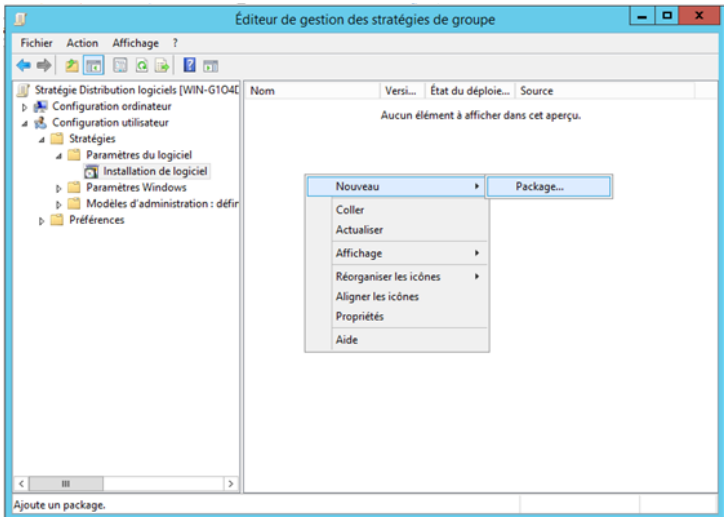

Figure 8 : Fenêtre d'édition de GPO avec la catégorie "Installation de logiciel"

Cette catégorie est disponible à la fois dans la partie « Configuration ordinateur » et « Configuration utilisateur ». Cependant, il faut faire attention à la partie dans laquelle on choisit de mettre notre package (installeur du logiciel). En effet, il n'est pas possible de déployer aux utilisateurs un logiciel en mode « publié » dans la partie « Configuration ordinateur ». Ce mode « Publié » est à distinguer des autres types de déploiement « Attribué » et « Avancé » parmi lesquels nous avons le choix lors de la procédure de déploiement du logiciel. Le mode « Publié » correspond à nos attentes car, pour les utilisateurs, il correspond au placement du logiciel dans la fenêtre « Obtenir les programmes ». En effet, le mode « Publié » indique que nous allons proposer le logiciel aux utilisateurs. À l'inverse, le type de déploiement « Attribué » permet aux administrateurs d'imposer un logiciel obligatoire à tous les utilisateurs concernés par la GPO. Ainsi, une fois la GPO prise en compte à la connexion d'un utilisateur ou au démarrage de l'ordinateur, le logiciel sera installé sur le poste sans confirmation de l'utilisateur. Enfin, le mode « Avancé » est similaire au mode « Attribué » mais permet par la suite de gérer d'autres paramètres de déploiement. Nous choisirons donc le type de déploiement « Publié » lorsque nous voudrons simplement mettre à disposition le logiciel aux utilisateurs sans leur imposer.

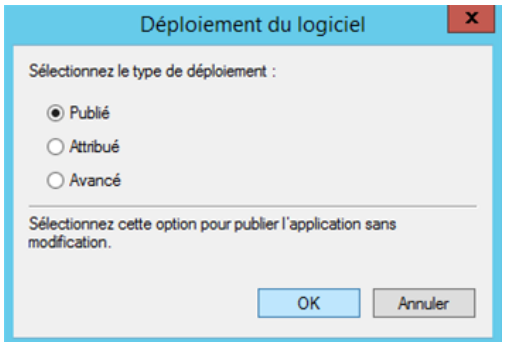

Figure 9 : Fenêtre de sélection du type de déploiement d'un logiciel

La solution du panneau de configuration est donc plutôt rapide à mettre en œuvre. Cependant, elle possède beaucoup d'inconvénients. En effet lorsque l'on propose un logiciel par cette méthode on spécifie dans la GPO un chemin d'accès vers un serveur qui contient le fichier installeur à récupérer pour installer le logiciel. Or, sachant que si nous ne créons qu'une GPO qui se répliquera sur les différents domaines la GPO sera la même pour toutes les agences. Cela signifie que toutes les agences de France et à l'étranger auront le même chemin pour le téléchargement de l'installeur et ainsi devront joindre le même serveur. Il n'est donc pas concevable que toutes les agences de l'entreprise téléchargent sur le même serveur car cela saturerait de part le serveur en lui-même et également le lien ce qui rendrait alors le téléchargement des logiciels très long pour les utilisateurs. Il reste cependant possible de proposer plusieurs serveurs sur lesquels récupérer l'installeur mais cela n'est pas possible à définir dans la GPO. En d'autres termes il faudrait créer une GPO pour chaque agence en modifiant le serveur de distribution pour chaque agence. Cela n'est donc pas possible sachant que le service devra déjà gérer les logiciels à rendre disponible et qu'il y a un nombre important d'agences.

4.5.2 Solution de SCCM ou Configuration Manager

La solution qui permettrait de résoudre tous les points négatifs de la solution du panneau de configuration est le SCCM (aujourd'hui Configuration Manager). SCCM est une solution proposée par Microsoft et étant donc adaptée à la plupart des systèmes d'exploitation Windows. Cette solution intègre le Centre logiciel qui permet aux utilisateurs d'avoir accès à un catalogue d'applications qu'ils peuvent télécharger sans avoir les droits administrateurs locaux. L'interface pour les utilisateurs se présente sous la forme de la fenêtre ci-dessous (Figure 10). Ce centre logiciel se présente pour l'utilisateur sous la forme d'un magasin d'application qu'il peut ouvrir du menu démarrer en cherchant « Centre logiciel ».

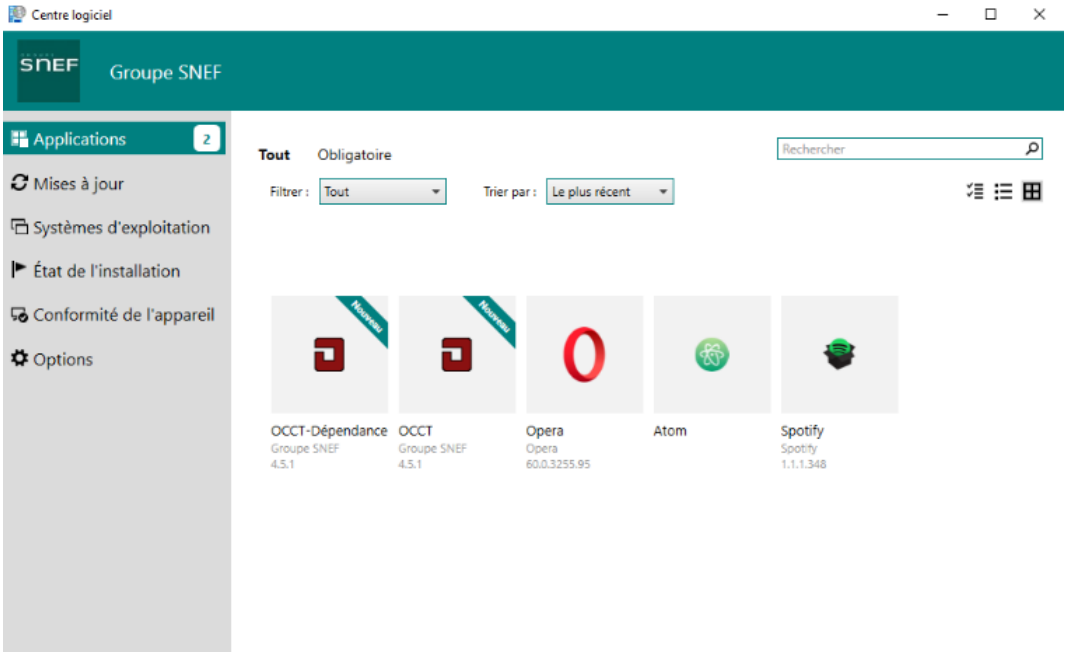

Figure 10 : Interface du centre logiciel client de SCCM

Pour l'utilisateur, on peut voir que ce centre logiciel est d'abord beaucoup plus ergonomique et agréable à utiliser. En effet, la possibilité d'ajouter des icônes, de repérer les applications fraichement ajoutées avec le bandeau « Nouveau » ou encore la possibilité de trier les logiciels par catégorie est un grand gain de simplicité et de clarté. De plus, comme on peut voir sur la gauche de la fenêtre (Figure 10) l'utilisateur a également la possibilité de voir les mises à jour disponibles pour les applications qu'il a installé ou encore si un nouveau système d'exploitation est disponible pour passer à un Windows plus récent.

Pour les administrateurs, avec la solution du centre logiciel, les choses sont à la fois plus et moins compliqué que pour la solution du panneau de configuration. En effet, utiliser le centre logiciel signifie aussi installer un serveur SCCM. Or, l'installation d'un serveur SCCM a non seulement un coût en licences mais également en infrastructure. SCCM a également besoin de communiquer avec une base de données SQL Server, et d'avoir différentes fonctionnalités installées sur ce même serveur. Il est en effet dépendant d'un WSUS, Windows Server Update Services afin de déployer des mises à jour Windows, de la modification des paramètres du pare-feu des clients etc.

Nous avons donc premièrement le coût des licences et de l'infrastructure qui peuvent représenter un frein à l'acquisition de SCCM. En effet, SCCM comme aujourd'hui de nombreux logiciels fonctionne sur le principe de l'abonnement au client. Ainsi, pour chaque poste qui voudra bénéficier des fonctionnalités de cet outil, il faudra payer une licence de client pour. Également, il faudra ajouter la licence pour le serveur SCCM et pour le serveur SQL. En termes de chiffres, cela revient à environ 2€ par poste client par mois puis jusqu'à 3500€ (en une fois) pour le serveur SCCM et près de 30 000€ pour SQL Server de Microsoft. Cela donnerait un total d'environ 250 000 € à payer tous les

2 ans (l'abonnement SCCM est un engagement de 2 ans) et un investissement de 30 000€ pour la licence SQL si l'on considère que l'on dispose d'un parc de 5000 ordinateurs.

Ce n'est pourtant pas tout car il faudra également ajouter le coût de l'infrastructure que demandera SCCM. On peut voir ci-dessous (Figure 11) les recommandations de Microsoft sur le sujet. Il est recommandé, si le site principal autonome intègre également la base de données SQL Server de prévoir un serveur possédant 16 cœurs avec 96 Go de mémoire vive. Cela permettrait, selon Microsoft, de gérer 150 000 ordinateurs sous Windows. N'ayant pas autant d'utilisateurs une infrastructure de ce type n'est pas nécessaire mais il faudra tout de même un serveur puissant.

Configuration de site	Cœurs de processeur	Mémoire (Go)	% d'allocation de mémoire pour SQL Server
Serveur de site principal autonome avec un rôle site de base de données sur le même serveur[1]	16	96	80
Serveur de site principal autonome avec une base de données de site distante	8	16	-
Serveur de bases de données distant pour un site principal autonome	16	72	90

Figure 11 : Configuration recommandée pour les serveurs SCCM et SQL

Le deuxième point qui peut être un frein est donc la difficulté de mise en place initial de ce serveur. En effet, il faut prévoir du temps pour mettre en place ce service car son installation est longue et complexe. Il faut installer le serveur SCCM, le serveur SQL ainsi qu'ajouter des rôles et fonctionnalités aux serveurs. De plus, il faut configurer le serveur SQL et revoir la configuration des pares-feux pour ouvrir les ports requis. Ayant réalisée l'installation sur la maquette, j'ai rencontré beaucoup de problèmes qui n'étaient pas prévu par les procédures que j'ai suivi sur internet et ai donc dû trouver les solutions à ces problèmes.

Cependant, une fois l'installation effectuée, les administrateurs pourront profiter des fonctionnalités de SCCM et de sa simplicité dans l'administration des logiciels. En effet, il faut aussi rappeler que SCCM fait de la gestion d'inventaire, gère les mises à jour Windows et peut intégrer un antivirus sous réserve de payer un abonnement supplémentaire.

Les administrateurs de SCCM disposent donc d'une console qui se retrouve sous la forme de cette interface ci-dessous (Figure 12). On y retrouve donc dans la partie en bas à gauche les quatre fonctionnalités de SCCM. Dans un premier temps, nous avons la partie ressources et conformité qui nous permet de voir quels ordinateurs sont reliés au site primaire mais qui permet également de lancer des détections de clients et de vérifier la conformité des clients grâce à des paramètres indiquant leur système d'exploitation par exemple. Nous retrouvons dans la deuxième section la partie qui nous intéresse c'est-à-dire la bibliothèque de logiciels. Dans cette section, nous pouvons déployer des logiciels, créer des packages (.msi), déployer des mises à jour de logiciel, définir des dépendances entre logiciels etc… Enfin les deux dernières sections sont les sections surveillance et administration qui permettent respectivement de faire de la gestion d'inventaire ou de la surveillance de « santé » des postes et de la gestion de l'infrastructure des sites SCCM, des paramètres de clients etc…

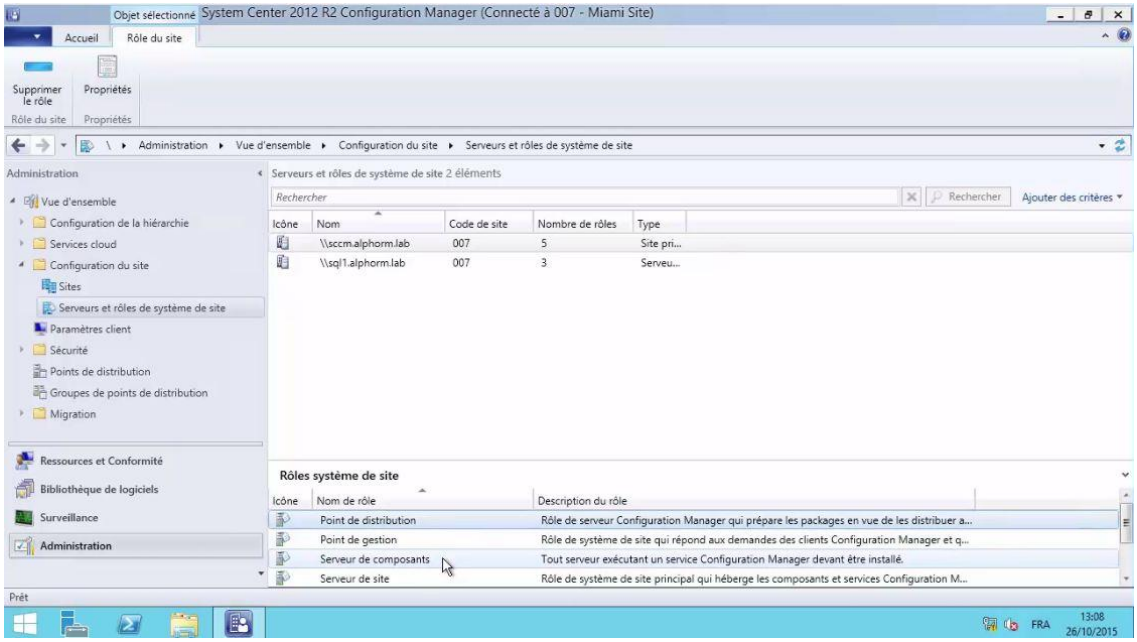

Figure 12 : Console d'administration de SCCM

La mise à disposition des logiciels s'effectue donc sur cette interface. Un des avantages pour les administrateurs est la gestion des points de distribution. En effet, ces points de distribution permettent aux administrateurs de définir des serveurs qui serviront de distributeurs des logiciels proposés par l'entreprise afin d'ajouter des points d'accès aux fichiers installeurs pour les utilisateurs et d'éviter la saturation des serveurs et du réseau. Concrètement, lorsqu'un administrateur fait un changement sur le site primaire pour le centre logiciel via la console (Figure 12), aucune action n'est requise pour que le changement s'effectue aussi sur les points de distribution distant. Ainsi, cela chargera moins le réseau car les informations et les fichiers d'installation ne circuleront qu'une fois entre le site primaire et les points de distribution.

Un autre avantage de SCCM comparé à la méthode du panneau de configuration est la possibilité de déploiement des fichiers exécutables. En effet, il est possible de déployer un installeur de logiciel au format d'exécutable (.exe). À première vue, cela paraît intéressant car faisant gagner du temps lors du déploiement d'un logiciel car n'ayant pas à convertir la plupart des installeurs qui se trouvent au format .exe dans le format .msi. Seulement, après avoir réalisé des tests depuis la maquette, je me suis rendu compte que la méthode de déploiement des exécutables proposée par SCCM est en fait bien plus longue et fastidieuse que la conversion de l'exécutable en package .msi. Afin de réduire au maximum la complexité des déploiements de logiciels, j'ai donc choisi de tester plusieurs solutions pour réaliser cette conversion.

4.5.3 Conversion d'exécutable en package .msi

Afin de déployer un logiciel de façon rapide pour le service informatique, il a donc fallu trouver une solution efficace de conversion des fichiers .exe en package .msi. Parmi les solutions testés (comme les solutions d'EMCO MSI Package Builder et exemsi) j'ai retenu le logiciel Advanced Installer. Ce logiciel est ce que l'on appelle un « wrapper » msi. Sa fonction n'est pas réellement de convertir le fichier .exe en fichier .msi mais plutôt d'intégrer au sein du package msi le fichier installeur au format .exe. Il réalise donc simplement un « emballage » du fichier .exe dans un package .msi.

Ce type de solution permet de gagner en rapidité car la fonction du logiciel étant simplement l'emballage du fichier, il n'y a pas beaucoup de paramètres à renseigner à la conversion. De plus, cela permet de livrer le fichier d'origine à l'utilisateur. Le package msi aura en fait seulement servi

d'intermédiaire dans la distribution et une fois exécuté, ouvrira le fichier .exe comme si l'utilisateur le récupérait depuis internet.

Advanced Installer n'est cependant pas seulement un wrapper msi. Son interface d'accueil se présente sous la forme de cette fenêtre (Figure 13). Afin de trouver le wrapper msi, il faut donc aller dans la section « Convert » et sélectionner l'outil MSI from EXE(s). La conversion du fichier peut ensuite s'effectuer en moins de 3 minutes car il n'y a qu'à indiquer le fichier à convertir, le chemin où le fichier converti se trouvera, le nom et la version du logiciel ainsi que son éditeur. Il y a également la possibilité d'ajouter un ou plusieurs autres fichiers au package msi ou encore le lancement du package en mode « silencieux » ou l'exécution d'une commande au lancement du package. Cependant, la plupart du temps, les paramètres par défaut sont suffisants et il est donc très rapide de « wrapper » son fichier installeur .exe.

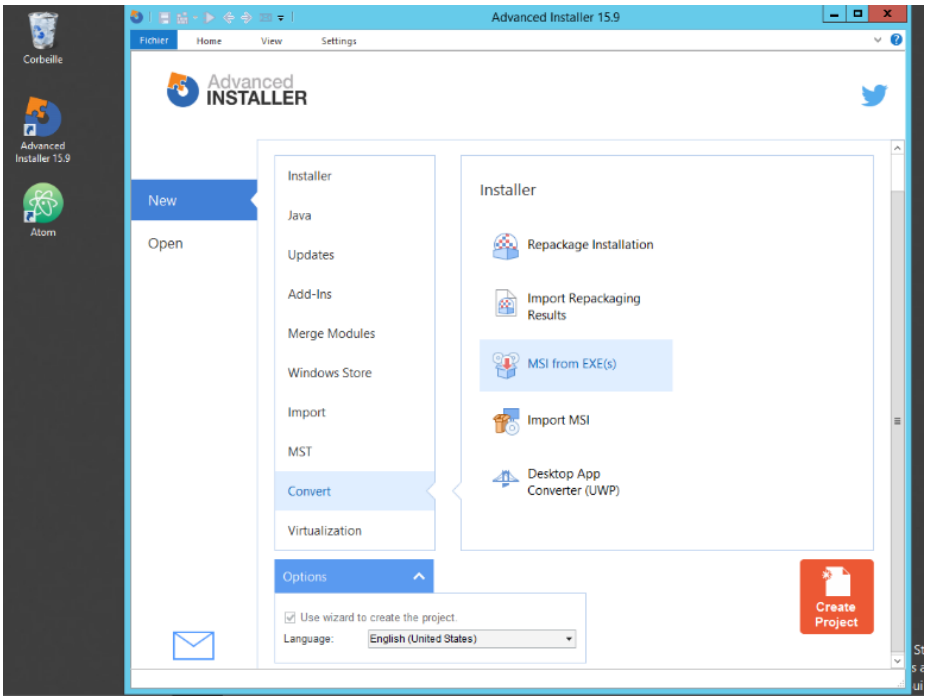

Figure 13 : Fenêtre d'accueil du logiciel Advanced Installer

Ce logiciel n'est malheureusement pas gratuit mais la licence entreprise est fixée à 1499$ à vie. Ce tarif inclus un support de 6 mois. Ce tarif reste relativement bas car il permettra une grande économie de temps et est un tarif à vie.

4.6 La solution LAPS

Afin de rendre le projet cohérent, j'ai dû, en plus des solutions permettant le retrait des droits administrateurs, trouver un moyen de régler le problème des comptes locaux identiques configurés par le service informatique lors de la préparation des nouveaux postes à distribuer aux employés. En effet, ces comptes servent à l'administration des postes par le service informatique en cas de problème avec les comptes des utilisateurs. Le problème est que ces comptes possèdent le même mot de passe. Afin de solutionner ce problème nous avons donc dû trouver une solution.

La solution qui a été retenue pour solutionner ce problème est l'outil LAPS, Local Administrator Password Solution proposé par Microsoft en complémentarité de la suppression des comptes administrateurs locaux existants afin de ne garder que le compte administrateur local de base aux postes. Cet outil a tout d'abord l'avantage d'être gratuit puis s'intègre facilement à l'Active Directory. Il agit sur le compte administrateur local des postes utilisateur en lui donnant un mot de passe aléatoire avec date d'expiration. On peut définir différents paramètres pour le mot de passe dans la GPO qu'il faut mettre en place pour distribuer le client de l'outil LAPS aux utilisateurs (Figure 14).

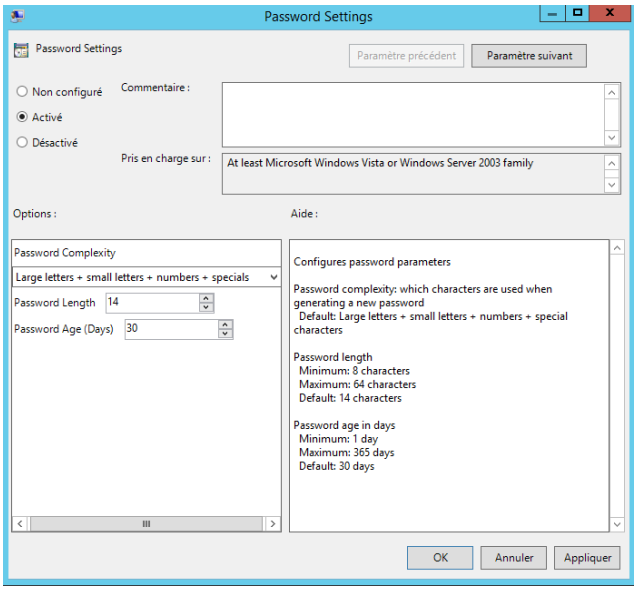

Figure 14 : Paramètre "Password Settings" de la GPO LAPS

On peut donc voir que l'on a le choix de définir une politique pour ces mots de passe. Dans un premier temps, on peut définir la complexité du mot de passe : avec ou sans caractères spéciaux ou majuscules etc… Nous pouvons aussi définir le nombre de caractère que les mots de passe contiendront ainsi que la durée de vie du mot de passe. Lors de l'application de la GPO aux utilisateurs, il est important de faire attention à ce qu'elle ne s'applique pas aux contrôleurs de domaine (en bloquant l'héritage aux contrôleurs de domaine par exemple) car sinon, cela attribuerait un mot de passe aléatoire au compte Administrateur de l'Active Directory. Or, les contrôleurs de domaine ne possédant pas de compte local mais seulement le compte Administrateur de l'AD, si l'on ne connaît pas le mot de passe et que l'on redémarre le contrôleur, on pourrait se retrouver bloqué et ne plus avoir accès au contrôleur de domaine.

Cependant, LAPS possède l'avantage de proposer différentes manières de retrouver le mot de passe du compte administrateur local des utilisateurs. En effet, lors de l'installation de cet outil sur le serveur contrôleur de domaine, il a fallu étendre le schéma Active Directory. Cela signifie que nous avons dû ajouter des attributs à l'Active Directory. Ces attributs sont l'attribut du mot de passe puis l'attribut de la date d'expiration du mot de passe. Ils se retrouvent ensuite dans l'annuaire dans les attributs des ordinateurs du domaine. Cependant, ces attributs sont stockés en clair et il est donc très important de faire attention à qui a les droits pour les consulter. C'est pourquoi il existe également des solutions payantes comme le « Local Administrator Password Management » de Synergix qui se veut plus sécurisé car cryptant les mots de passe et ne nécessitant pas de modification du schéma Active Directory. Cependant, nous resterons sur la solution LAPS car gratuite et tout de même sécurisée si les accès sont bien gérés.

Un autre avantage de LAPS est l'interface LAPS UI qu'il propose à l'installation sur le contrôleur de domaine. Cette interface se présente sous cette fenêtre (Figure 15) et est simple d'utilisation. Il suffit d'entrer le nom de l'ordinateur et d'appuyer sur le bouton « Search » et le mot de passe ainsi que sa date d'expiration s'affichent. Il est aussi possible grâce à cette interface de redéfinir la date d'expiration du mot de passe ou de le réinitialiser immédiatement en laissant le champ de la date vide et en cliquant sur le bouton « Set ».

Enfin, sur demande de mon tuteur de stage, j'ai également réalisé un script Powershell pour l'export des mots de passe dans un tableur au format .csv. Ce script est disponible en annexe.

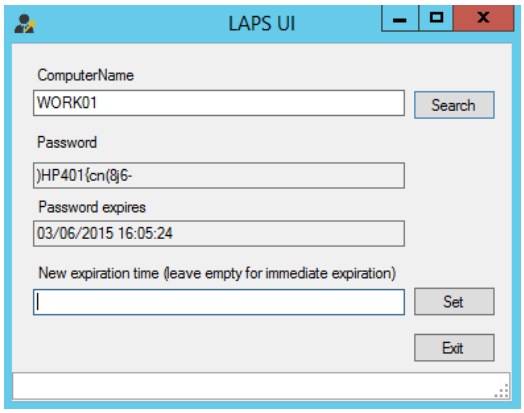

Figure 15 : Interface LAPS UI

4.7 Gestion des mots de passe hors domaine

Un autre sujet que nous avons dû traiter qui a été rajouté en cours de stage était le sujet des mots de passe expirant en dehors du réseau du groupe. En effet, la politique du groupe impose un changement de mot de passe régulier. Les utilisateurs sont prévenus lorsque leur mot de passe est proche de l'expiration et il leur est demandé de le changer rapidement en effectuant le Ctrl+Alt+Suppr afin d'accéder au menu du changement de mot de passe de compte Windows. Cependant, certains utilisateurs ne prennent pas en compte ces avertissements ou ne sont pas toujours connectés au réseau du groupe. Ainsi, lorsque leur mot de passe est expiré et qu'ils ne sont pas connectés au réseau de l'entreprise et donc à l'Active Directory, ils se retrouvent dans la situation où leur compte est bloqué et ils sont donc obligés d'appeler le service informatique pour demander le changement de leur mot de passe.

Afin de régler cela, j'ai donc recherché les solutions existantes à ce problème commun à de nombreuses entreprises. J'ai donc retenu deux solutions qui sont l'ADSelfService Plus de ManageEngine et la solution incluse au pack ADCE, Active Directory Client Extension de Synergix. Ces deux solutions proposent toutes deux de s'intégrer à l'Active Directory et via un serveur web de proposer une page internet qui permettra aux utilisateurs de réinitialiser leur mot de passe ou de débloquer leur compte sans connexion au réseau de l'entreprise. Ces deux fonctionnalités sont réalisables si l'utilisateur renseigne son nom de compte ainsi que son ancien mot de passe (expiré). Il pourra ensuite entrer un nouveau mot de passe et pourra enfin utiliser son poste. Ci-dessous (Figure 16) on peut prendre pour exemple l'interface proposée par la solution de ManageEngine.

Figure 16 : Interface web de la solution ADSelfService Plus de ManageEngine

Pour la solution de ManageEngine, il y a aussi la possibilité d'intégrer l'outil à Windows sur les postes afin de leur proposer une section en plus dans la partie de connexion du compte de Windows. Cela a pour avantage de ne pas obliger d'avoir un deuxième appareil connecté à internet pour accéder à la page web. L'utilisateur pourra ainsi directement débloquer son compte depuis l'ordinateur où il est bloqué.

Concernant les tarifs de ces solutions, Synergix ne les publie pas directement et mon tuteur de stage avait donc fait une demande auprès d'un revendeur mais nous n'avons pas reçu de réponse. Cependant, la solution de ManageEngine propose elle ses tarifs. Le prix est donc entre 3345$ et 4795$ pour un total de 5000 utilisateurs du domaine. Si on dispose de plus d'utilisateurs, le prix augmente pour passer à la tranche des 7500 utilisateurs. Également, ces tarifs sont à renouveler tous les ans car sont des tarifs d'abonnement annuel.

4.8 Logiciels s'exécutant avec les droits administrateurs

La dernière étape avant le retrait des droits administrateurs était de trouver une solution pour les logiciels demandant des droits administrateurs à l'exécution. En effet, certains logiciels que peuvent utiliser les employés peuvent ne pas fonctionner sans les droits administrateurs et demander le mot de passe de l'administrateur local pour s'exécuter. Les utilisateurs n'étant pas censés connaître le mot de passe du compte administrateur local, ils ne pourraient donc pas être capables de lancer ce type de logiciels.

Afin de solutionner ce problème, nous avons retenu plusieurs solutions que je n'ai cependant pas eu le temps de tester mais qui ont été proposées à l'entreprise. Les trois solutions retenues sont les solutions « Endpoint Privilege Management » de BeyondTrust, « Admin Rights Management » d'Ivanti et « Windows Privilege Management » de Securden. Les tarifs de ces solutions ne sont cependant pas connus car tous sur demande de devis.

La solution que nous avons cependant testée est celle proposée par Microsoft appelée SUA, Standard User Analyzer. Cette solution gratuite permet de gérer les restrictions liées au fonctionnement de certains logiciels dans un contexte d'utilisateur standard. Je l'ai donc testé pour plusieurs logiciels et ait obtenu des résultats plutôt satisfaisants mais malheureusement pas pour l'utilité recherchée. En effet, la solution permet de lancer le logiciel souhaité puis de capturer les actions que l'on effectue qui ne fonctionnent pas dans un contexte d'utilisateur standard. Par exemple, lorsque le logiciel demande un accès au registre, le SUA va capturer cet évènement et nous aurons ensuite la possibilité de générer un package .msi à déployer avec le logiciel pour donner les droits au logiciel d'accéder au registre de l'ordinateur par exemple.

J'ai donc proposé cette solution à l'entreprise dans l'éventualité où elle aurait un cas de logiciel demandant des droits administrateurs locaux après son exécution mais ai précisé que SUA ne pouvait pas effectuer la fonctionnalité que nous recherchons et qu'il faudrait donc se baser sur les trois solutions indiquées précédemment. Afin de donner une idée de l'interface, elle se trouve ci-dessous (Figure 17).

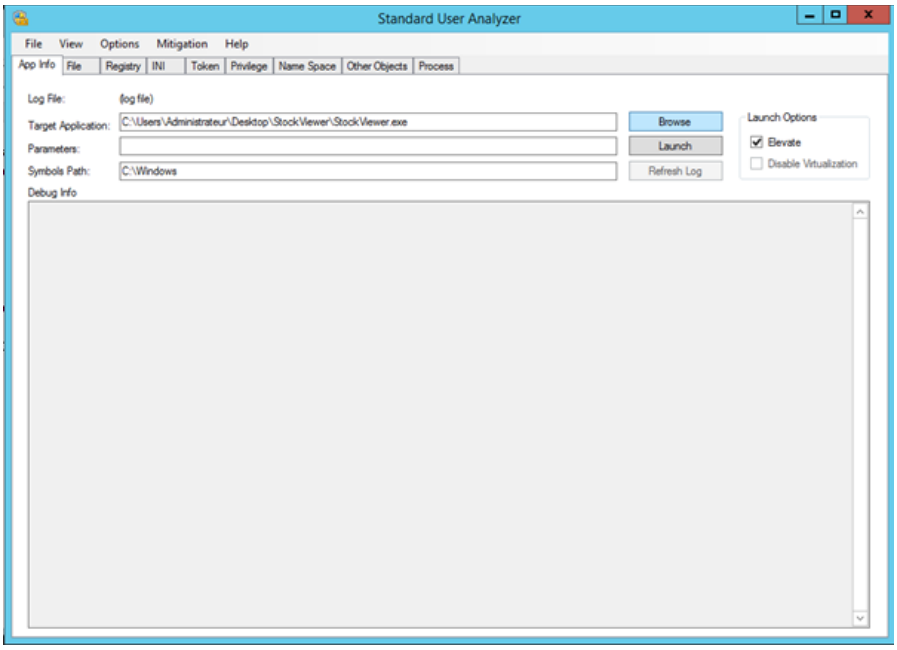

Figure 17 : Interface du Standard User Analyzer de Microsoft

4.9 GPO de retrait des droits administrateurs

En dernier lieu, l'étape finale est évidemment l'application de ce retrait des droits administrateurs. Ce retrait des droits se fera via une GPO qui modifiera le groupe local Administrateurs des postes. Il est très important de rappeler qu'elle doit s'appliquer en dernier lieu une fois que toutes les solutions de substitution pour les utilisateurs sont en place et fonctionnelles. En effet, si la GPO est appliqué trop brusquement, les utilisateurs ne pourront pas installer/mettre à jour leurs logiciels, lancer certains logiciels si les solutions présentées précédemment ne sont pas en place.

Afin d'assurer la réussite du projet, j'ai également proposé un plan d'action à l'entreprise pour assurer la transition avec le moins de problème possible. En effet, si la direction remarque qu'il y a trop de plaintes, elle peut annuler le projet. C'est pourquoi il faut prendre le temps d'abord de commencer par déployer ce changement en premier aux services qui seraient les moins impactés par ce retrait des droits administrateurs pour corriger pas à pas les problèmes rencontrés et ainsi déployer le retrait aux services les plus impactés. Il est également important d'informer la direction sur les risques de laisser les droits aux utilisateurs mais également accompagner les utilisateurs pour avoir le moins de plaintes possibles.

Ensuite, sur le plan technique, la GPO que nous allons déployer est une GPO qui modifiera la configuration des ordinateurs pour d'abord retirer tous les utilisateurs ou groupes d'utilisateurs qui font partie du groupe « Administrateurs » local sur les postes. Ensuite, il faudra évidemment y ajouter l'utilisateur administrateur local ainsi que le groupe « Administrateurs de l'entreprise » par exemple. Cette GPO s'appliquera également à tous les redémarrages des postes afin de supprimer des utilisateurs qui auraient été ajoutés au groupe « Administrateur » local de la machine de façon non réglementaire et interdite. Nous pouvons voir ci-dessous (Figure 18) la modification que nous allons apporter au groupe « Administrateur » local du poste via la GPO.

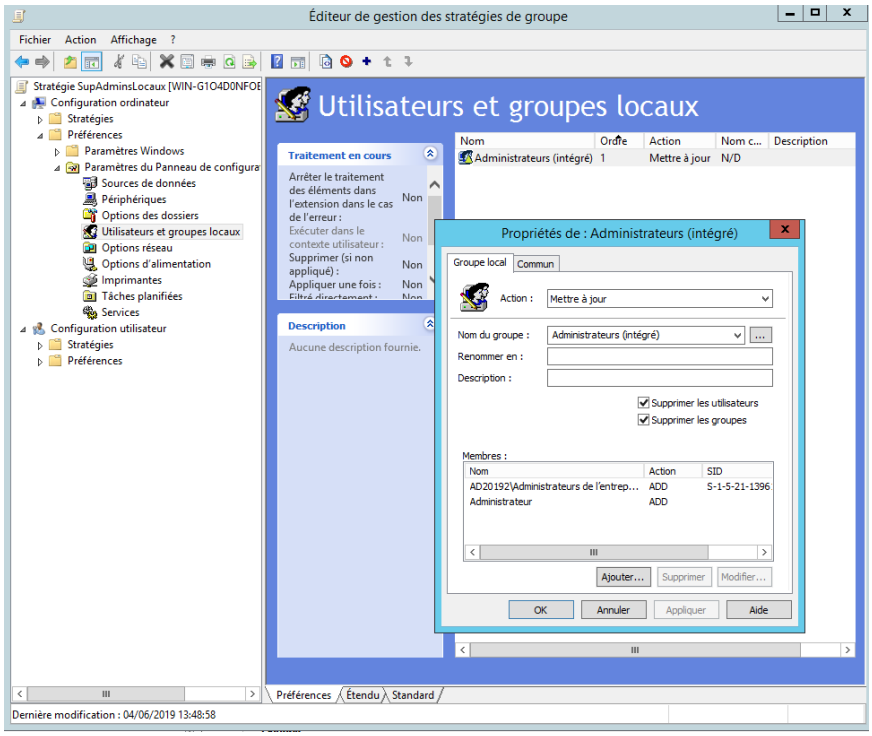

Figure 18 : Modification du groupe "Administrateurs" local via la GPO

5 Conclusion

En conclusion, mon projet permettra à l'entreprise d'avoir une vision des objectifs qu'elle pourra atteindre dans le but du retrait des droits administrateurs. En effet, mon projet ne sera pas immédiatement appliqué par le groupe car possédant de nombreux corps de métiers, la SNEF ne peut pas, pour le moment, se permettre de déployer un tel projet compte tenu de la taille du service informatique et de la charge de travail que représentent les solutions alternatives à proposer aux utilisateurs. Dans l'immédiat, le service testera donc ce retrait des droits sur certaines personnes du service informatique puis sélectionnera des utilisateurs « test » au sein de différent services. Cependant, mon projet servira à plus long terme et quelques solutions pourraient directement être appliquées comme le retrait des comptes locaux identiques avec l'application de LAPS ou encore une solution de gestion des mots de passe hors domaine.

En guise de trace laissé de mon travail dans le groupe, j'ai présenté au service un PowerPoint récapitulatif de mon projet ainsi que des fiches de procédures de mise en place de LAPS et du déploiement des applications dans un contexte d'utilisateur standard. Tous ces fichiers suivaient les codes de présentation de l'entreprise dites « corporate » fournies par les membres de mon service.

Sur le plan personnel, ce stage a vraiment eu un apport bénéfique. J'y ai découvert la vie en entreprise mais ai aussi beaucoup appris sur certains sujets comme l'Active Directory. Les échanges que j'ai pu avoir avec les personnes de mon service m'ont aussi beaucoup aidé à comprendre certains aspects du travail en entreprise. Ils ont également toujours été à l'écoute de mes questions malgré leur charge de travail et m'ont accueilli positivement. J'ai donc beaucoup apprécié travailler avec eux et apprendre de leurs compétences.

6 Remerciements

Je tenais donc tout d'abord à remercier tout le service informatique de la SNEF pour l'accueil bienveillant et sympathique que j'ai reçu mais aussi pour leur disponibilité lorsque j'avais besoin de leurs compétences pour avancer. Le travail fut très agréable et j'ai pu travailler dans la bonne humeur et rencontrer des gens à l'écoute pour mener ce projet à bien. Je remercie tout particulièrement Aurélie Armanet avec qui j'ai échangé pour la période post-stage afin de mettre en place ce stage avec la transmission de la convention et des autres pièces qui ont dû se faire rapidement car proche de la date de début du stage. Également, je remercie Philippe Viaud qui était mon tuteur de stage au cours de ces 10 semaines de m'avoir accompagné tout au long de cette période.
Enfin, je souhaitais remercier mon professeur Arnaud Février pour avoir transmis l'offre de stage a tous les étudiants de ma promotion et grâce à qui j'ai pu postuler à cette offre et donc réaliser ce projet.

7 Glossaire

DUT, Diplôme Universitaire de Technologie

Mémoire RAM, mémoire dite vive de l'ordinateur, support de stockage à court terme des données

Machine virtuelle, une machine virtuelle est un fichier informatique, généralement appelé image, qui se comporte comme un ordinateur réel. En d'autres termes, il s'agit d'un ordinateur (virtuel) créé à l'intérieur d'un ordinateur (physique).

GPO, Group Policy Object

Ransomware, rançongiciel en français, logiciel malveillant qui demande de l'argent en échange des données volées.

8 Sitographie

http://www.tech-faq.com/securing-domain-controllers.html : Tech-FAQ – Securing Domain Controllers

https://www.it-connect.fr/cours/notions-de-base-de-lactive-directory/ : Notions de base de l'Active Directory

https://www.prajwaldesai.com/ : Site de Prajwal Desai

https://slideplayer.fr/slide/1151103/ : Présentation d'Antoinette Bernard sur l'Active Directory sur le site SlidePlayer

https://www.upper-link.com/actus-cloud-it/securite-notpetya-attaque-informatique.html : article de Benoit Lecomte sur l'attaque informatique NotPetya sur le site Upper Link

https://docs.microsoft.com/fr-fr/sccm/core/plan-design/configs/support-for-sql-server-versions : Article de Microsoft sur la compatibilité des serveurs SQL avec SCCM

https://docs.microsoft.com/fr-fr/sccm/core/plan-design/configs/recommended-hardware : Article de Microsoft sur les recommandations de configuration du serveur SCCM

https://www.it-connect.fr/securite-proteger-les-comptes-administrateur-local-avec-laps/ : Article de Florian B. sur l'installation de LAPS sur le site it-connect.fr

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/manageengine.manageengine-adselfservice-plus : Page de téléchargement du logiciel ADSelfService Plus de ManageEngine sur le site du store de Microsoft Azure

https://www.manageengine.com/products/self-service-password/pricing-details.html : Détails des tarifs de la solution de ManageEngine ADSelfServicePlus.

https://labo-microsoft.supinfo.com/articles/la-compatibilite-des-applications/ : Article de SupInfo sur la compatibilité des applications par Benjamin Labastie

https://www.alphorm.com/tutoriel/formation-en-ligne-sccm-2012-r2-70-243/tuto-video-introduction-au-sccm-2012-r2 : Article vidéo sur la présentation de SCCM de Fabrice SFORZA CHRZANOWSKI sur le site Alphorm

9 Annexe

Script d'export CSV des mots de passe LAPS vers un fichier tableur CSV :

```
function Get-LAPSPasswords{

   [CmdletBinding()]
   Param(
      [Parameter(Mandatory=$false,
      HelpMessage="Credentials to use when connecting to a Domain Controller.")]
      [System.Management.Automation.PSCredential]
      [System.Management.Automation.Credential()]$Credential =
[System.Management.Automation.PSCredential]::Empty,

      [Parameter(Mandatory=$false,
      HelpMessage="Domain controller for Domain and Site that you want to query against.")]
      [string]$DomainController,

      [Parameter(Mandatory=$false,
      HelpMessage="Maximum number of Objects to pull from AD, limit is 1,000.")]
      [int]$Limit = 1000,

      [Parameter(Mandatory=$false,
      HelpMessage="scope of a search as either a base, one-level, or subtree search, default is
subtree.")]
      [ValidateSet("Subtree","OneLevel","Base")]
      [string]$SearchScope = "Subtree",

      [Parameter(Mandatory=$false,
      HelpMessage="Distinguished Name Path to limit search to.")]

      [string]$SearchDN
   )
   Begin
   {
      if ($DomainController -and $Credential.GetNetworkCredential().Password)
      {
         $objDomain = New-Object System.DirectoryServices.DirectoryEntry
"LDAP://$($DomainController)",
$Credential.UserName,$Credential.GetNetworkCredential().Password
         $objSearcher = New-Object System.DirectoryServices.DirectorySearcher $objDomain
      }
      else
      {
         $objDomain = [ADSI]""
         $objSearcher = New-Object System.DirectoryServices.DirectorySearcher $objDomain
      }
   }

   Process
   {
      # Status user
      Write-Verbose "[*] Grabbing computer accounts from Active Directory..."
```

```
    # Create data table for hostnames, and passwords from LDAP
    $TableAdsComputers = New-Object System.Data.DataTable
    $TableAdsComputers.Columns.Add('Hostname') | Out-Null
    $TableAdsComputers.Columns.Add('Stored') | Out-Null
    $TableAdsComputers.Columns.Add('Readable') | Out-Null
    $TableAdsComputers.Columns.Add('Password') | Out-Null
    $TableAdsComputers.Columns.Add('Expiration') | Out-Null

    # ----------------------------------------------------------------
    # Grab computer account information from Active Directory via LDAP
    # ----------------------------------------------------------------
    $CompFilter = "(&(objectCategory=Computer))"
    $ObjSearcher.PageSize = $Limit
    $ObjSearcher.Filter = $CompFilter
    $ObjSearcher.SearchScope = "Subtree"

    if ($SearchDN)
    {
      $objSearcher.SearchDN = New-Object
System.DirectoryServices.DirectoryEntry("LDAP://$($SearchDN)")
    }

    $ObjSearcher.FindAll() | ForEach-Object {

      # Setup fields
      $CurrentHost = $($_.properties['dnshostname'])
      $CurrentUac = $($_.properties['useraccountcontrol'])
                    $CurrentPassword = $($_.properties['ms-MCS-AdmPwd'])
      if ($_.properties['ms-MCS-AdmPwdExpirationTime'] -ge 0){$CurrentExpiration =
$([datetime]::FromFileTime([convert]::ToInt64($_.properties['ms-MCS-
AdmPwdExpirationTime'],10)))}
      else{$CurrentExpiration = "NA"}

      $PasswordAvailable = 0
      $PasswordStored = 1

      # Convert useraccountcontrol to binary so flags can be checked
      # http://support.microsoft.com/en-us/kb/305144
      # http://blogs.technet.com/b/askpfeplat/archive/2014/01/15/understanding-the-
useraccountcontrol-attribute-in-active-directory.aspx
      $CurrentUacBin = [convert]::ToString($CurrentUac,2)

      # Check the 2nd to last value to determine if its disabled
      $DisableOffset = $CurrentUacBin.Length - 2
      $CurrentDisabled = $CurrentUacBin.Substring($DisableOffset,1)

      # Set flag if stored password is not available
      if ($CurrentExpiration -eq "NA"){$PasswordStored = 0}


      if ($CurrentPassword.length -ge 1){$PasswordAvailable = 1}


      # Add computer to list if it's enabled
```

```
        if ($CurrentDisabled  -eq 0){
           # Add domain computer to data table

$TableAdsComputers.Rows.Add($CurrentHost,$PasswordStored,$PasswordAvailable,$CurrentPass
word, $CurrentExpiration) | Out-Null
        }

        # Display results
        $TableAdsComputers | Sort-Object {$_.Hostname} -Descending

      }
   }
   End
   {
   }
}


###################
##---VARIABLES---##
###################

$Path='C:\Users\Administrateur\Documents\LAPS_Tableau\LAPSPWD.csv'  #Chemin et nom du
tableau à créer (au format .csv)
$DC='192.168.1.2'                                  #Adresse IP du Contrôleur de Domaine
$AdminAD='ad20192.local\Administrateur'                    #Administrateur de l'Active Directory
(ex : ad.local\Administrateur)




#####################################################
##---EXPORT EN CSV ET RETRAIT DES DOUBLONS---##
#####################################################

Get-LAPSPasswords -DomainController $DC -Credential $AdminAD | Export-Csv $Path -
NoTypeInformation -Delimiter ';'
$ExtractFile=Import-Csv $Path -Delimiter ';'
$ExtractFile | Select-Object -Property Hostname,Stored,Readable,Password,Expiration -Unique |
Export-Csv $Path -NoTypeInformation -Delimiter ';'
```