DEPARTEMENT INFORMATIQUE - IUT 2 GRENOBLE

Année Universitaire 2015-2016

MEMOIRE DE STAGE

APPRENTISSAGE EN INFORMATIQUE

Crédit Agricole Sud Rhône-Alpes

Présenté par

Xavier MARRANT
LP SIL option MESSI

Jury

IUT : M MARTIN
IUT : M BONNAUD
Société : M CHABOT

Déclaration de respect des droits d'auteurs

Par la présente, je déclare être le seul auteur de ce rapport et assure qu'aucune autre ressource que celles indiquées n'ont été utilisées pour la réalisation de ce travail. Tout emprunt (citation ou référence) littéral ou non à des documents publiés ou inédits est référencé comme tel.

Je suis informé qu'en cas de flagrant délit de fraude, les sanctions prévues dans le règlement des études en cas de fraude aux examens par application du décret 92-657 du 13 juillet 1992 peuvent s'appliquer. Elles seront décidées par la commission disciplinaire de l'UGA.

A, Le,

Signature

Table des matières

Déclaration de respect des droits d'auteurs 2
1. Remerciements 4
1. Introduction 5
2. Support et maintenance du parc informatique 6
2.1 Contexte 6
2.2 Les travaux réalisés 6
2.2.1 Les tâches courantes 6
2.2.2 Les tâches occasionnelles 11
2.3 Bilan 13
3. Projet : Gestion du parc d'appareils mobiles 14
3.1 Fonctionnement de Mobile Iron 15
4.2 Réinstallation du système 16
4.3 Le mode kiosque 17
4.3.1 Configuration pour une seule application 18
4.3.2 Configuration pour plusieurs applications 18
4.3.3 Activation du mode kiosque 19
4.4 Le cryptage des données des tablettes Android 20
4.4.1 Dans Mobile Iron 20
4.4.2 Sur la tablette 20
4.4.3 Problématiques et remarques 21
4.5 Synthétisation des informations dans Mobile Iron 21
4 Conclusion 23
5 Glossaire 24
6 Références 25
7 Résumé et Abstract 26

Table des figures

Figure 1 : Les deux imprimantes à modifier 8
Figure 2 : Changement du pilote 8
Figure 3 : Demande de télédistribution d'un logiciel 9
Figure 4 : Configuration souhaitée après intervention 11
Figure 5 : Fonctionnement de MobileIron 16
Figure 6 : Tentative d'un « factory reset » refusée 16
Figure 7 : Tablette en mode kiosque 17
Figure 8 : Configuration du mode kiosque en application unique 18
Figure 9 : Configuration du mode kiosque en mode multiple applications 19
Figure 10 : Activation ou désactivation du mode kiosque 19
Figure 11 : Cryptage dans la politique de sécurité 20
Figure 12 : Tablette sans mot de passe 22

1. Remerciements

Je remercie l'équipe pédagogique de l'IUT 2 de l'UPMF de Grenoble qui s'occupe de la licence professionnelle SIL* pour leur formation dispensée depuis septembre 2015 qui m'a permis d'enrichir mes connaissances.

Je tiens à remercier particulièrement les personnes suivantes en leur témoignant toute ma reconnaissance pour leur soutien, l'aide et l'expérience qu'elles m'ont apportés durant cette année :

- Monsieur MARTIN, mon tuteur pédagogique,
- Monsieur CHABOT, mon tuteur et responsable de l'unité informatique, pour son accueil, sa bienveillance, son enseignement et pour m'avoir accepté au sein de son unité,
- Messieurs BRET, DUBOUCHET, FERIAU, PICTON, POLITANO, REMIGI, SIMONE, techniciens et analystes de l'équipe à Grenoble, pour leur aide précieuse, leur disponibilité et leur amabilité,
- L'ensemble de l'unité informatique répartie sur les sites de Grenoble, Valence et Privas pour sa participation à mon travail, son accueil et son soutien,
- L'ensemble du personnel du Crédit Agricole Sud Rhône-Alpes pour son accueil.

1. Introduction

Je réalise mon année d'apprentissage au sein de l'unité Assistance et Maintenance informatique (AMA) du Crédit Agricole Sud Rhône-Alpes au siège de Grenoble.
L'unité AMA est répartie sur les trois sites, Grenoble, Valence et Privas. Sur chacun d'entre eux, les techniciens doivent effectuer la maintenance des équipements, les interventions sur leurs sites respectifs, ainsi que celles en agence, et d'autres tâches notamment de gestion du parc.

Je participe aux missions de l'unité, mais principalement sur le site de Grenoble. Je peux donc intervenir sur différents matériels tels que des imprimantes, des téléphones IP, des unités centrales ou des écrans, pour résoudre ou assister un utilisateur qui aura déclaré un incident.
Je peux également gérer l'inventaire, m'occuper des livraisons de matériels…
Je parlerai de mon travail sur ces missions dans une première partie. Je décrirai des missions quotidiennes, et d'autres occasionnelles, telle que refaire une baie de brassage afin d'apporter plus de sécurité aux agences en ligne.

Mon projet est la gestion du parc d'appareils mobiles. De plus en plus de téléphones mobiles et de tablettes sont utilisés. En tant que banque, une forte sécurité doit être apportée sur le système informatique. Les appareils mobiles, plus sujets à des vols à cause de la proximité et de la manipulation par de nombreuses personnes, doivent donc avoir une attention toute particulière. Il m'a été demandé de leur apporter un supplément de sécurité, tels que des restrictions d'utilisation, le cryptage des données. L'application MobileIron est installée sur ces appareils, pour tout d'abord appliquer des politiques de sécurité et de verrouillage, et remonte des informations à un serveur, auquel on accède par une interface web. J'ai réalisé une analyse sur les alertes des configurations en anomalie du point de vue de la sécurité, afin de les corriger.
J'ai travaillé sur mon projet au cours du deuxième semestre de l'année universitaire, à environ 40% de mon temps de travail.
Ce projet est en évolution et amélioration permanente. Il faudra continuer à apporter une sécurité optimale aux appareils mobiles tant qu'ils seront utilisés.
Je présenterai donc de mon projet, et des différentes facettes de mon travail sur celui-ci dans une seconde partie.

2. Support et maintenance du parc informatique

2.1 Contexte

La mission principale missions de l'unité AMA consiste à résoudre les problèmes informatiques auxquels les collaborateurs peuvent être confrontés.

La bonne disponibilité des ressources telles que les comptes clients et les documents internes, permet un travail des collaborateurs dans des conditions optimales. Un incident gêne, baisse ou arrête la productivité d'un collaborateur, ce qui peut avoir des conséquences, parfois grave, telle que l'insatisfaction des clients de la banque.
C'est pourquoi il est important de résoudre les incidents dans des délais les plus brefs possibles.

Mais les incidents ne sont qu'une facette de notre travail.
Il y a également les installations ou déménagements de postes, les installations de logiciels…

2.2 Les travaux réalisés

Etant intégré dans l'unité AMA, je suis amené à faire toutes ces missions.

2.2.1 Les tâches courantes

- Les interventions au siège

Nous pouvons voir les incidents des utilisateurs dans Remedy, un outil de gestion de configuration, d'incidents et de parc, respectant les normes ITIL*. L'utilisateur a pour cela appelé le centre de service, qui lui-même nous transmet un ticket d'incident si un premier niveau de support, comportant par exemple une vérification des connectiques, n'a pas résolu le problème.
Il peut s'agir d'imprimantes, de tablettes, des unités centrales ou tout autre matériel informatique. Les interventions sont donc diverses. Le problème peut venir d'un logiciel spécifique, des connectiques, des profils utilisateurs…
Je peux donc intervenir par exemple pour des problèmes d'impression qui peuvent venir des drivers, ou bien un profil utilisateur qui s'est corrompu et qu'il faut donc que je supprime. Ainsi, leur de la prochaine connexion de cet utilisateur, son profil sera réinitialisé et fonctionnel.

La diversité du matériel et des logiciels m'a permis d'utiliser toutes mes capacités et compétences d'analyse et techniques pour résoudre les incidents.

Exemple d'une intervention :

Aux agences en lignes, des superviseurs gèrent les équipes. Ils établissent les plannings, répartissent les appels, valident des dossiers,…

Ces superviseurs peuvent se connecter à un serveur Windows Server 2003, à l'aide d'un script de connexion utilisant l'application « Bureau à distance (mstsc) » de Windows, afin d'accéder et utiliser l'application Planexa. Ce logiciel est un outil de planification des ressources humaines. En exploitant les données historiques de flux d'appels clients, il permet d'anticiper les ressources humaines nécessaires à toute heure de la journée pour y répondre, et de bâtir des emplois du temps individualisés pour le personnel permettant la couverture des besoins prioritaires et les autres tâches affectés dans les temps de moindre affluence, tout en respectant les contraintes légales, sociales et organisationnelles.

Quand les superviseurs ont fini le planning de la semaine, ils peuvent l'imprimer directement sur leur imprimante de poste ou alors l'imprimer en PDF sur leur poste de travail. Pour cela, lors de la connexion du superviseur sur le serveur distant, la couche applicative « Terminal Server », récupère l'accès aux imprimantes du poste de travail. Le « Terminal Server » est un composant de Microsoft Windows, clients et serveurs, qui permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant, via n'importe quel type de réseau.

Un jour, les superviseurs n'avaient plus accès à leur imprimante « PDF Creator », mais avait toujours accès à leur imprimante de poste. Ils devaient imprimer les plannings sur leur imprimante de poste, puis changer de poste pour pouvoir les scanner et enfin les partager avec les membres de leur équipe, plutôt que de l'avoir directement en PDF. L'incident entrainait donc une charge de travail supplémentaire et une baisse de qualité à cause du scan.

Mes premiers tests ont été de vérifier le bon fonctionnement de PDF Creator du poste de travail et de celui du serveur. Les deux fonctionnaient donc le problème venait de la remontée de l'imprimante PDF Creator du poste de travail vers le serveur.

En collaboration avec des personnes du GIE* CATS, fournissant un niveau de support technique supérieur au nôtre, nous avons déterminé que le problème avait commencé après une montée en version de drivers du côté du serveur. Ces personnes ont ensuite trouvé une incompatibilité entre le driver des imprimantes de poste (toutes du même modèle) des superviseurs, et les nouveaux drivers du Windows Server 2003, ce qui peut causer l'incident.

J'ai changé ce driver sur les postes en question. Après une déconnexion complète du serveur, fermeture de session normale plus suppression des connexions mal fermées sur le serveur, puis une nouvelle connexion, la session du « terminal server » avait de nouveau accès à l'imprimante PDF Creator du poste de travail.

L'incident était résolu. Le problème était issu de cette incompatibilité entre le driver de l'imprimante de poste de travail et des drivers du serveur.

Procédure que j'ai utilisée pour changer le driver :

- Aller dans le panneau de configuration, Matériel et audio, Périphériques et imprimantes.
- Clic droit sur l'imprimante de poste, Propriété de l'imprimante. Trois configurations sont possibles, seuls les deux commençant par « IARPP » nous intéressent. Sur ces deux configurations :

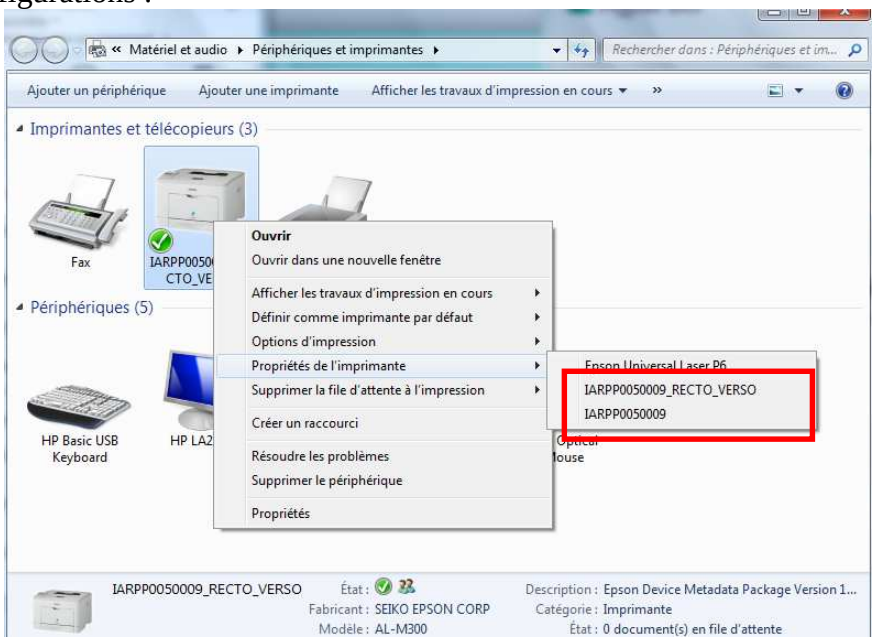

Figure 1 : Les deux imprimantes à modifier

- Onglet « Avancé »
- On modifie le pilote. De « Epson Universal Laser P6 », on met le pilote « EPSON AL-M300 Advanced ».

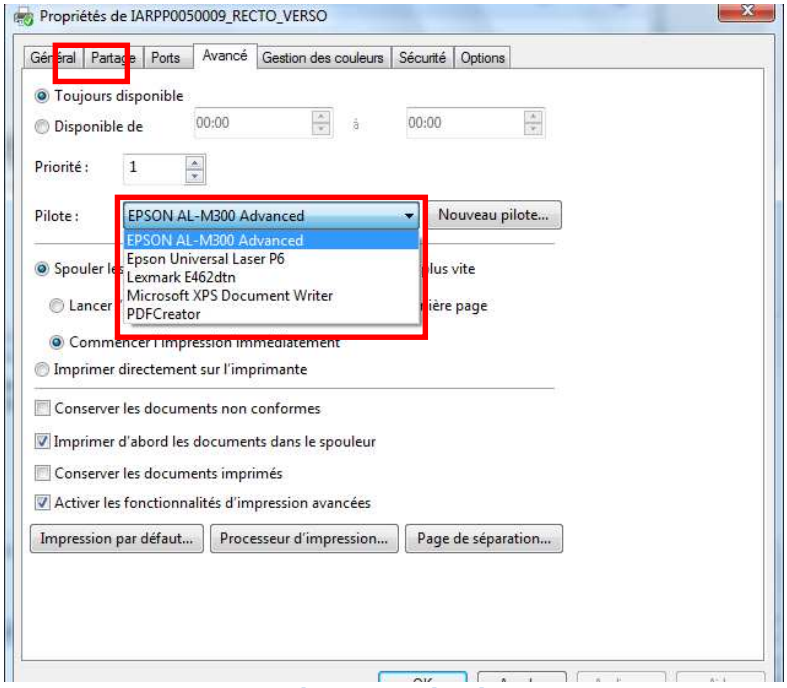

Figure 2 : Changement du pilote

- Télédistributions de logiciels métiers

Un collaborateur peut avoir besoin d'utiliser un logiciel pas encore installé dans le cadre de son travail. Pour que les installations soient sûres et uniformisées, une solution de télédistribution est en place. C'est également un gain de temps puisque nous n'avons pas à nous déplacer jusqu'aux postes concernés pour l'installer manuellement.
Pour ce faire, nous disposons d'un formulaire dans lequel nous renseignons le nom du poste et le logiciel à installer.

Si nous avons plusieurs logiciels à installer sur plusieurs postes, nous pouvons les mettre sur le même formulaire.

Le formulaire est ensuite envoyé par mail à un automate, qui télédistribuera les logiciels sur les postes en question durant la nuit, pour ne pas encombrer le réseau et pour qu'il n'y ait aucune session utilisateur d'ouverte, car une session verrouillée pourrait bloquer l'installation.

Demande de Télédistribution Applications à la demande (AAD) - Logiciels Nice W7

à envoyer sur la boite mail de MCO/MEP Outils Telediffusion Boreal Nice (MCO.Outils.Telediffusion@ca-technologies.fr)

Important : Les logiciels Windows 7 (hors compléments office) ne peuvent être télédistribués sur des postes de production en CR uniquement lorsque le projet de déploiement du siège est effectif.

Attention, veuillez noter que les demandes envoyées après 15h ne seront prises en compte qu'à partir du lendemain !
Les demandes envoyées avant 15h seront traités le soir même.

Demandeur (à renseigner) :		N° de CR (chosir dans la liste ci-dessous) :	07/12/2015
Nom CR (choisir dans liste) :	Nom	N° CR	[AD]

Poste de Travail : *(à renseigner)*	**Logiciel Spécifique et Version** : *(cliquez dans cellules ci-dessous pour choisir le logiciel - Touche Suppr pour effacer)*	**Commentaire technique :** *(apparait automatiquement si présent dans onglet Données Détail)*	**Vos commentaires :** *(ex : désinstallation...)*
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	
		#N/A	

Figure 3 : Demande de télédistribution d'un logiciel

- Les installations de postes

Si un nouveau collaborateur arrive ou un collaborateur change de bureau pour une mission, il est possible qu'une salle doit être équipée avec plus de postes qu'elle n'en a déjà. Il faut donc en réinstaller d'autres.

Tous les postes sont équipés d'une unité centrale, d'un clavier, d'une souris et d'un écran. Ils sont presque tous équipés d'un téléphone IP (TOIP*). Les salles de formation par exemple, n'en possèdent pas. Certains ont également une imprimante de poste et/ou un scanner.

Si un téléphone IP est installé ou changé, nous devons envoyer un mail à l'unité assurant la configuration des infrastructures téléphoniques centralisées avec l'adresse MAC du téléphone et le nom du poste pour qu'ils les associent, à cause du fonctionnement de la TOIP*. En effet, les téléphones IP servent à faire circuler les conversations vocales sur le réseau de l'entreprise. Pour cela, un serveur IPBX donne aux téléphones les configurations qu'ils doivent utiliser. Les unités centrales sont reliées aux téléphones qui eux-mêmes sont connectés au réseau. Le serveur apporte de la dynamique dans le processus : quand un utilisateur se connecte, le serveur donne une nouvelle configuration, plus spécifique à l'utilisateur, au téléphone. L'application téléphonique récupère l'état de la téléphonie auprès du serveur IPBX. Ainsi si un collaborateur est en communication, il est possible de le voir sur cette application. Pour cela, le serveur a besoin de l'adresse MAC du téléphone et du nom du poste, c'est pourquoi on doit envoyer ces deux informations cette unité.

La préparation d'une unité centrale se fait en deux phases.

- Une phase de « soclage » : un master du système d'exploitation Windows 7 est installé sur la machine. Pour cela, on branche la machine dans une salle « usine », puis on démarre la machine sur le réseau, afin d'accéder à un serveur fournissant les images systèmes. Le master est spécifique au type d'unité centrale afin de gérer au mieux les drivers.
- Une phase de « personnalisation » : la machine est configurée selon le service dans laquelle elle sera installée, et son nom d'hôte. La machine aura par exemple un accès prédéfini à certaines imprimantes selon le service, et pourra récupérer des logiciels spécifiques selon son nom d'hôte et les demandes faites par l'outil de télédistribution.

2.2.2 Les tâches occasionnelles

- Les interventions en agence
- Réorganisation d'une baie de brassage

Les agences en ligne sont très importantes, elles sont dédiées au canal de communication téléphonique, notamment pour les clients gérés en relation à distance quand ils sont à l'étranger par exemple, ou ne souhaitant pas se déplacer dans une agence de proximité. De nombreuses sécurités sont donc en place pour elles, pour qu'il y en ait toujours au moins une fonctionnelle, afin de garantir le service au client.

Tout d'abord, les agences sont réparties sur les sites de Grenoble et de Valence. Ainsi s'il y a un problème comme un incendie dans un bâtiment, au moins une agence est encore disponible sur l'autre site.

Ensuite des groupes électrogènes sont présents pour pallier à une panne électrique.

Chaque baie est équipée de trois commutateurs, plus couramment appelés switch. Dans une même baie, chaque switch est sur un disjoncteur électrique différent. Ainsi si un fusible saute à cause d'une surtension, seul un des trois switchs de la baie n'est plus alimenté électriquement.

Au siège de Grenoble, les deux agences en ligne et les autres services du même étage, suite à des interventions étalées dans le temps n'ayant pas respecté les normes d'installation initiales, étaient tous mélangés sur les trois switchs de la baie, avec de nombreux câbles Ethernet trop longs encombrant inutilement la baie. Pour continuer dans cette idée de sécurité, il fallait que chaque agence soit branchée sur un switch spécifique, et que les autres services occupent le troisième. Ainsi si un switch devient indisponible pour panne de courant, ou altération de la configuration, cela n'affecte qu'une agence, voire aucune, et n'affecte pas le fonctionnement de l'autre.

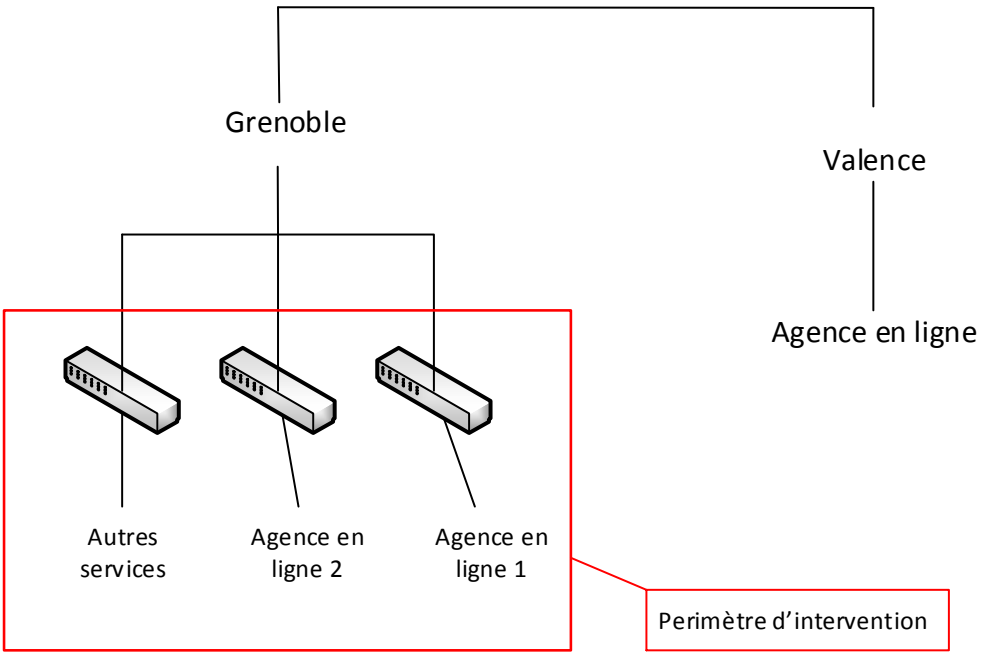

Figure 4 : Configuration souhaitée après intervention

Nous respectons également une norme qui consiste à mettre les imprimantes sur les derniers ports et le serveur ou le scanner chèque sur les premiers ports pour les agences en ligne. Ainsi, en cas d'intervention dans la baie, nous savons qu'il y a un switch pour chaque agence, le troisième pour les autres services, et que sur ces deux premiers, les imprimantes sont branchées sur les derniers ports, les serveurs et le scanner chèque sont sur les premiers. Ainsi nous pouvons être plus efficaces. J'ai également remplacé les câbles trop longs par des câbles de 2 mètres pour un gain considérable de place. Pour éviter que quelqu'un ne brasse une prise au hasard dans la baie, les ports des switchs non utilisés sont fermés. Il faudra donc obligatoirement passer par l'unité informatique.

Il a fallu un long travail de préparation pour bâtir un référentiel précis de l'existant pour préparer les corrections à y apporter pour revenir dans la norme de sécurisation, afin de ne faire aucune erreur, et de configurer les VLAN* pour la TOIP* sur les switchs.
Les conversations téléphoniques des agences en lignes sont enregistrées par des serveurs, c'est pourquoi les postes de ces agences sont sur un VLAN* spécifique.

En premier, il a fallu aller repérer dans les ailes où se situent les agences en ligne, toutes les prises réseaux dont celles utilisées. J'ai donc déjà pu mettre à jour nos plans avec la localisation des numéros de prises et des numéros de postes.

Cela fait, j'ai pu aller repérer le brassage des prises dans la baie pour mettre à jour le tableau Excel dans lequel est marqué, pour chaque port de chaque switch, quelle prise réseau est branchée sur celui-ci, et inversement, pour chaque prise réseau, sur quel port de quel switch elle est branchée.

Un port d'un switch n'a que 3 cas de fonctionnement :

- Port libre
- Port occupé avec de l'activité
- Port occupé mais sans activité : peut être un point d'accès pour un ordinateur portable dans une salle de réunion par exemple.

N'ayant pas ce troisième cas à cet étage, j'ai enlevé tous les câbles où aucun trafic ne passait, après vérification qu'un ordinateur éteint n'était pas branché dessus.

J'ai donc par la suite pu préparer les mêmes tableaux mais en marquant ce que l'on devait obtenir, et faire un autre tableau pour pouvoir voir plus clairement les changements que l'on devait faire. J'ai également établi l'ordre des modifications que nous allions faire pour gagner du temps, en commençant par les prises qui étaient à destination d'un port vide.
Parallèlement, j'ai modifié la configuration des switchs pour mettre les bons numéros de VLAN* sur les ports selon les postes qui y sont branchés.
Pour modifier ces configurations, j'ai utilisé les commandes suivantes :

Pour rentrer dans le mode configuration du terminal :

```
GRE_SW_UTIL_BPA43-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Pour rentrer dans une interface :

```
GRE_SW_UTIL_BPA43-01(config)#int fa0/6
```

Pour changer son numéro de VLAN* pour la TOIP* :

```
GRE_SW_UTIL_BPA43-01(config-if)#switchport voice vlan 343
```

Pour changer sa description :

```
GRE_SW_UTIL_BPA43-01(config-if)#description **** BURROUGHS ****
```

Pour quitter le mode de configuration :

```
GRE_SW_UTIL_BPA43-01(config-if)#end
```

Et pour sauvegarder la nouvelle configuration :

```
GRE_SW_UTIL_BPA43-01(config-if)#write
```

Nous avons refait le brassage tôt le matin, avant l'ouverture des agences pour ne pas prendre le risque de couper des télécommunications, et en plusieurs fois. Peu avant l'ouverture des agences, nous nous arrêtions pour faire le tour des deux agences pour vérifier que les postes étaient tous connectés sur le réseau.

Nous avions plusieurs niveaux de tests pour vérifier le bon fonctionnement des postes. Nous avions déjà les diodes sur les switchs pour signaler la présence de trafic sur un port. Donc si un câble était branché mais la diode du port correspondant était éteinte, cela signifiait qu'il y avait un problème.

Un deuxième test consistait à faire le tour des agences, puis de regarder si les téléphones IP affichaient bien une configuration sur leur écran.

Un dernier test m'amenait à voir le statut des ports en ligne de commande sur les switchs. La commande est :

```
GRE_SW_UTIL_BPA43-01(config-if)#show interface status
```

Le port peut être connecté ou déconnecté, mais également en erreur. Il faut alors exécuter les commandes « **`shutdown`** » et « **`no shutdown`** » pour redémarrer le port

Les enseignements que j'ai reçus sur les réseaux informatiques m'ont été utiles, notamment pour refaire la configuration des switchs en ligne de commandes et de vérifier l'état des ports pour valider mon travail.

2.3 Bilan

Les missions de l'unité AMA sont essentielles. Elles permettent le bon fonctionnement du système informatique, hors serveurs qui eux sont gérés par le GIE* CATS*. Sans le système informatique, que ce soit dans les sites ou dans les agences, les collaborateurs ne peuvent plus travailler pour répondre aux attentes des clients. Notre travail permet donc à tous de travailler dans des conditions optimales.

J'ai appris comment gérer un parc informatique, à intervenir sur de nombreux matériels, et à assister les utilisateurs. J'ai pu approfondir des compétences et des connaissances, et en apprendre d'autres.

Ces missions, au siège de Grenoble, me prenait la majorité de mon temps de travail. Le reste du temps, je travaillais sur mon projet : la gestion du parc d'appareils mobiles.

3. Projet : Gestion du parc d'appareils mobiles

Mon projet est la gestion du parc d'appareils mobiles. Ce parc, croissant, est composé d'Iphones et de tablettes, qui sont soit sous Android, soit sous IOS. Les téléphones sont principalement utilisés par des collaborateurs des sites et des agences, tandis que les tablettes sont essentiellement en agences car utilisées en relation avec des clients. Les tablettes sous Ios sont à la disposition des clients pour accéder à des sites internet appartenant au groupe Crédit Agricole, tandis que les tablettes Android sont utilisées par les clients pour la signature électronique, disponible pour des actions bancaires des clients tels que le retrait d'un chéquier ou un virement bancaire. Progressivement, les tablettes seront utilisées pour la signature de tous les contrats : ouverture de comptes, avenants aux contrats d'assurance ou opérations sur titres.
Elles seront donc une source de problèmes de sécurité : elles pourront être volées, possèderont des données sur les clients… Il faut donc sécuriser aux mieux ces tablettes pour garantir la confidentialité et l'intégrité des données.

Notre gestion de ces appareils mobiles, ou MDM* pour « Mobile Device Management », consiste en l'installation de l'application Mobile@Work sur l'appareil. L'appareil est ensuite enregistré, et l'application remonte des informations sur un serveur dédié à l'entreprise, dans les infrastructures du cloud du fournisseur. Une interface web de ce serveur nous permet de recenser tous nos appareils et de les gérer
Depuis cette interface, il est possible de trier les appareils selon différents critères définis tels que les tablettes qui ne sont pas à jour, de les localiser, de vérifier la présence d'une application donnée…. On peut également faire une télédistribution d'une application. Si la tablette est volée ou perdue, il est possible de verrouiller la tablette et de supprimer les données qui sont stockées dessus.
L'avantage du MDM* est qu'il est possible de faire pratiquement tout à distance, et de voir diverses informations concernant nos appareils mobiles

Mon projet se divise en plusieurs points. Tout d'abord, je dois améliorer la sécurité des tablettes. Le standard est devenu de crypter les données sur les appareils, il faut que je fasse en sorte que toutes les tablettes s'y conforment. Cette sécurité aura l'avantage d'améliorer la confidentialité. En cas de vol de la tablette, les données ne pourront pas être récupérées pour un usage malveillant.

D'autre part, sur l'interface graphique du MDM*, la navigation entre les appareils n'est pas très intuitive puisque la plupart du temps, il faut regarder appareil par appareil. Je dois donc trouver un moyen pour synthétiser les informations, comme afficher tous les appareils qui ne sont pas à jour, ou bien afficher tous les appareils sur lesquels sont installées des applications non professionnelles, et ainsi pouvoir faire une action sur eux.

Je parlerai dans mon mémoire de stage principalement des tablettes sous Android, se trouvant principalement en agence.

Il n'y avait pas d'enseignements spécifiques aux parcs mobiles lors de cette année de licence professionnelle. Cependant j'ai pu appliquer des méthodes de gestion et de réflexion que nous avions apprises pour les postes de travail sur le parc d'appareils mobiles.

3.1 Fonctionnement de Mobile Iron

Le fonctionnement de MobileIron est relativement simple une fois compris et que l'on est habitué à celui-ci.

Des utilisateurs ont été créés. Les utilisateurs correspondent aux postes des agences. Par exemple, l'agence 302 est équipée de 18 postes. Les noms de ces postes vont de QARPP0030201 à QARPP0030218. Les utilisateurs sont donc QARPP0030201, QARPP0030202,… QARPP0030218. D'autres utilisateurs sont plus génériques. Il y a notamment 50 utilisateurs, de FOR01 à FOR50, utilisés pour les formations. Il y a également des utilisateurs pour le service digital qui développe ou teste des applications, et d'autres pour le service AMA.

Les appareils enregistrés sont reliés à un et un seul utilisateur. En agence, les tablettes sont considérées soit comme extension du poste de travail, soit dédiées à l'information des clients, elles n'ont pas de personnes attitrées. De ce fait, les utilisateurs dans Mobile Iron ont été calés sur le nom des machines. Pour les IPhones et IPads, les utilisateurs de Mobile Iron correspondent aux utilisateurs physiques. Un de ces derniers utilisateurs peut donc avoir plusieurs équipements. Des utilisateurs peuvent ne pas avoir d'appareils. Par exemple, en agence, seuls les postes dans les bureaux utilisés pour des rendez-vous avec des clients, ou les postes à l'accueil, sont équipés d'une tablette. Des postes peuvent donc ne pas être équipés de tablettes, donc aucun appareil n'est relié à l'utilisateur correspondant.

Ces appareils sont reliés à des groupes. Un groupe a différentes utilités. Il peut être organisationnel : un groupe par agence, qui rassemble les appareils de l'agence en question ; télédistribution d'application, ou pour définir des politiques de sécurité et / ou de verrouillage.

Des applications sont ajoutées au serveur. Il y a deux types d'applications :

- Un lien vers une bibliothèque d'application, « play store » pour Android,
- Un exécutable, en .APK pour Android. L'application se trouve directement dans Mobile Iron.

Nous privilégions les exécutables puisque ceux-ci peuvent être télédistribués et s'installer silencieusement. C'est pourquoi nous commençons à récupérer les exécutables des applications venant de bibliothèques, à l'aide d'une application tierce.
Les applications sont ensuite reliées à des groupes, et elles seront télédistribuées sur les appareils de ces groupes.

Puis nous avons les configurations et les politiques.
Les configurations sont de plusieurs types : elles peuvent être un simple ajout d'URL sur l'écran d'accueil pour les appareils Ios, une configuration de messagerie, une configuration de wifi, ou un certificat. Ces configurations permettent le déploiement en masse d'une configuration, évitant ainsi de devoir intervenir sur les appareils.
Deux politiques nous intéressent ici : les politiques de sécurité et celles de verrouillage.
Les politiques de sécurités permettent de définir la stratégie de mot de passe, la politique de cryptage des données, et la politique des remontées en alerte des configurations.
Les politiques de verrouillage, quant à elles, permettent de restreindre le cadre d'utilisation des tablettes : par exemple, interdire l'accès à la caméra.

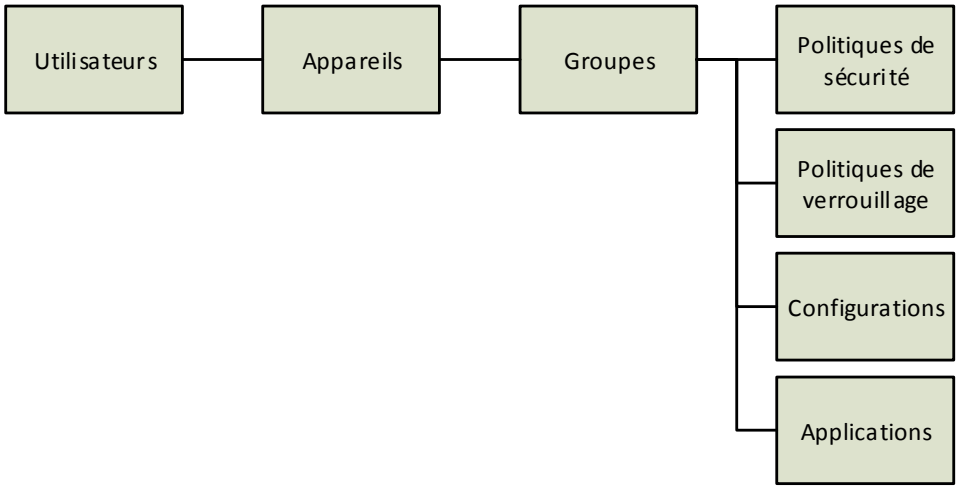

Figure 5 : Fonctionnement de MobileIron

4.2 Réinstallation du système

Une première étape vers la sécurité consiste en l'interdiction de la réinstallation du système, plus communément appelé « factory reset ». Par sécurité, l'application Mobile@Work ne peut pas être désinstallée quand l'appareil est enrôlé. Donc tant qu'elle est installée, nous pouvons modifier les configurations, et avons ainsi la possibilité de bloquer l'appareil en cas de vol.
Mais si le « factory reset » est autorisé et exécuté, l'application disparaît, tout comme notre contrôle sur l'appareil.
Ainsi, avec le « factory reset » interdit, l'application ne peut pas disparaître, et on garde le contrôle de tous nos appareils, même en cas de vol, tant qu'ils sont connectés à un réseau.

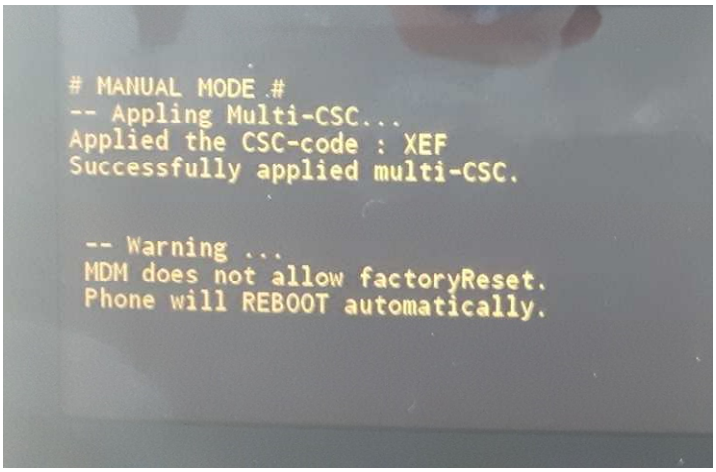

Figure 6 : Tentative d'un « factory reset » refusée

J'ai interdit le « factory reset » sur toutes les politiques de verrouillage des appareils en production. Dans le cas où nous devrions effectuer un « factory reset » pour une raison ou pour une autre, il suffira de créer une nouvelle politique de verrouillage, d'autoriser celui-ci, et de l'appliquer à l'appareil en question.

4.3 Le mode kiosque

L'évolution des agences amènera les clients à utiliser des tablettes Android, pour pouvoir accéder à un certain nombre de contenus.
Il est donc nécessaire de restreindre au maximum l'utilisation possible de ces tablettes, pour éviter que les clients puissent par exemple accéder aux paramètres, ou à d'autres applications.

J'ai dû rechercher comment mettre en place le mode kiosque et toutes ces options, présent dans la gamme des tablettes du fabriquant Samsung.

Ce mode, configurable *via* MobileIron, permet de limiter l'utilisation de la tablette à des applications prédéfinies.
Il en existe deux modes :

- Utilisation d'une seule application : une application est lancée, et il est impossible d'en sortir.
- Utilisation de plusieurs applications : une page d'accueil personnalisable permet l'accès à ces applications. En quittant une application, l'appareil revient sur cette page d'accueil et il est impossible de quitter celle-ci.

En plus de définir le nombre d'applications et potentiellement la page d'accueil, il est possible d'autoriser d'autres applications telles que le gestionnaire de tâche, la barre système, l'option de partage…
Pour restreindre au mieux, nous n'autorisons pas l'option de partage, pour éviter l'accès potentiel à des applications non voulues dans le mode kiosque, tout comme l'extension de la barre de notification qui permet d'accéder aux applications qui ont émis une notification.

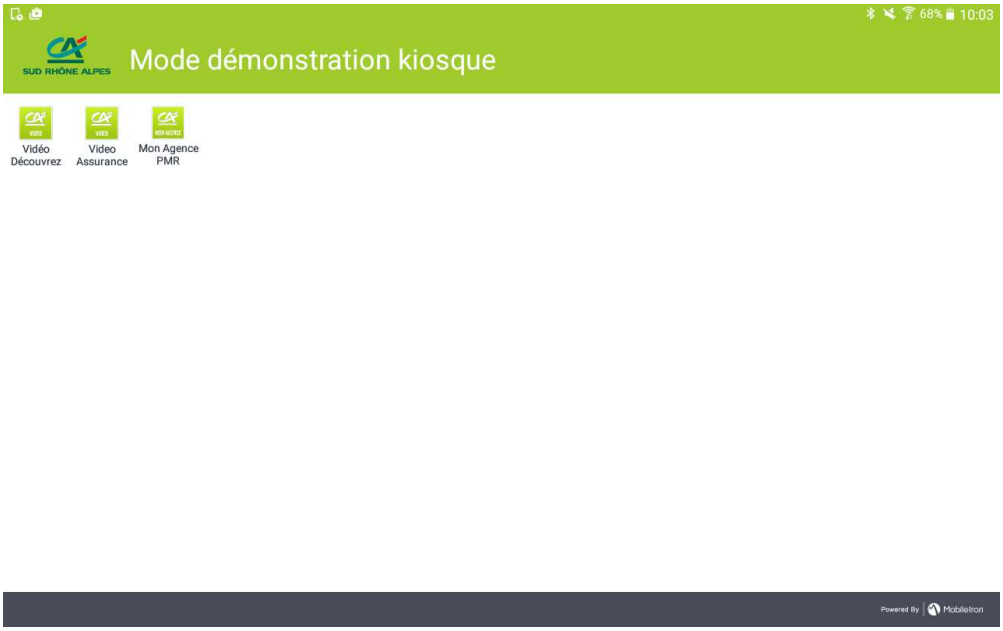

Figure 7 : Tablette en mode kiosque

Le mode kiosque est prévu dans un court terme pour des tablettes utilisées par les clients. Une application leur permettra d'accéder à des vidéos, et de naviguer sur trois sites prédéfinis. Le déploiement de ces tablettes n'a pas commencé car le développement de cette application n'est pas terminé.

4.3.1 Configuration pour une seule application

Pour configurer ce mode, il suffit d'une politique de type kiosque, que l'on paramètre en mode application unique. De plus, on ne coche que les trois applications systèmes que l'on souhaite, et on saisit le nom du paquet de l'application.
Si l'application est installée depuis le Play Store, le nom de paquet est visible dans l'URL de l'application sur le Store : play.google.com/store/apps/details?id=com.dropbox.android&hl=fr
Dans le cas d'une télédistribution via le MDM*, le nom est disponible dans les détails de l'application.

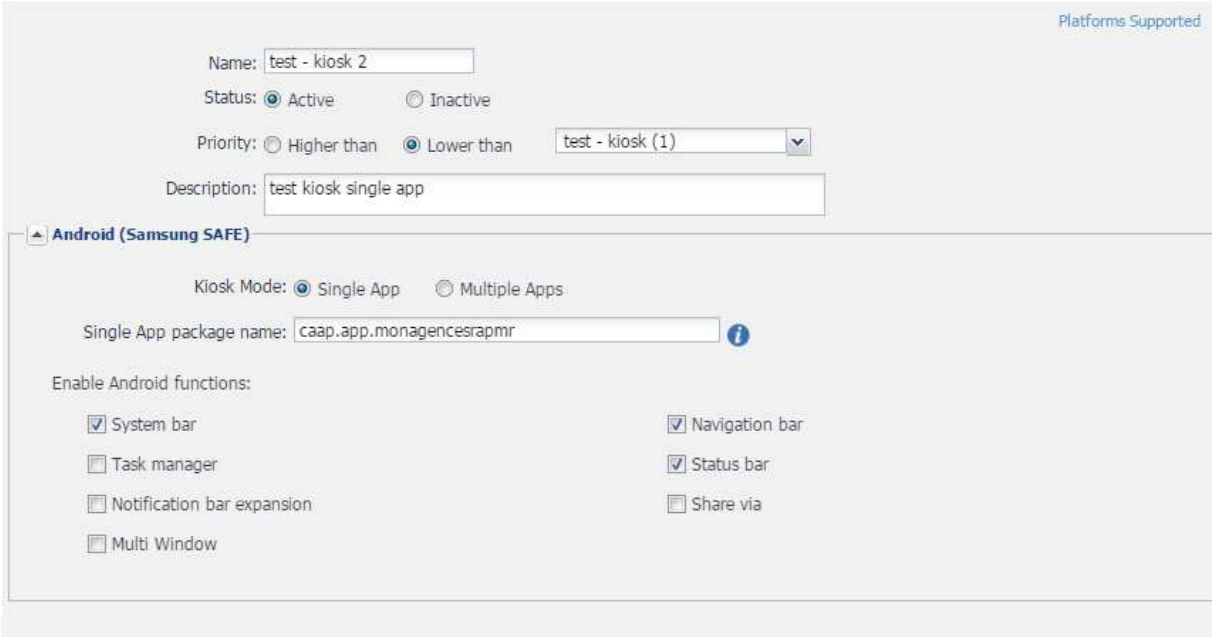

Figure 8 : Configuration du mode kiosque en application unique

4.3.2 Configuration pour plusieurs applications

Pour ce mode, il faut non seulement la politique de type kiosque, mais également une configuration de ce même type.

Pour la politique, il s'agit de la même que précédemment mais dans laquelle on définit la page d'accueil en plus, avec le mode multiple applications.

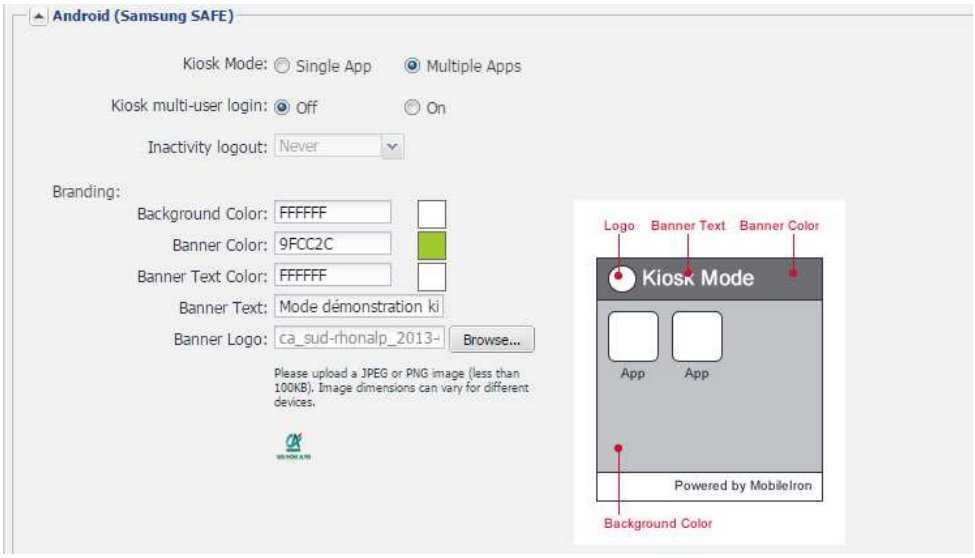

Figure 9 : Configuration du mode kiosque en mode multiple applications

La configuration du type kiosque n'est autre qu'une liste des noms de paquets des applications que l'on souhaite utiliser sur la tablette.

4.3.3 Activation du mode kiosque

Comme pour toutes autres politiques ou configurations, il faut placer celles de type kiosque créées précédemment dans le groupe souhaité.
Ensuite il ne reste plus qu'à aller dans la liste des appareils, sélectionner les tablettes du groupe sur lesquelles on souhaite établir ce mode, et de l'activer ou le désactiver.

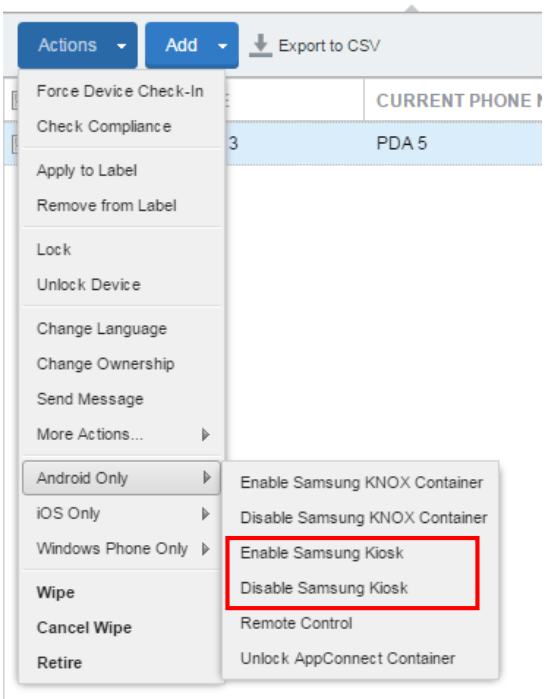

Figure 10 : Activation ou désactivation du mode kiosque

4.4 Le cryptage des données des tablettes Android

Pour un supplément de sécurité, le cryptage des données est devenu très important. En cas de vol de l'appareil, le voleur ne pourra pas récupérer les données.
Je devais trouver le moyen de crypter les données à partir du MDM*.
Mon travail a abouti sur une procédure se divisant en deux parties.

4.4.1 Dans Mobile Iron

Dans MobileIron, il faut modifier les politiques de sécurité. Dans ces politiques, il est possible d'activer le cryptage, et de choisir les types de données et de fichiers à crypter. Il est également possible de crypter la carte SD et les logs.

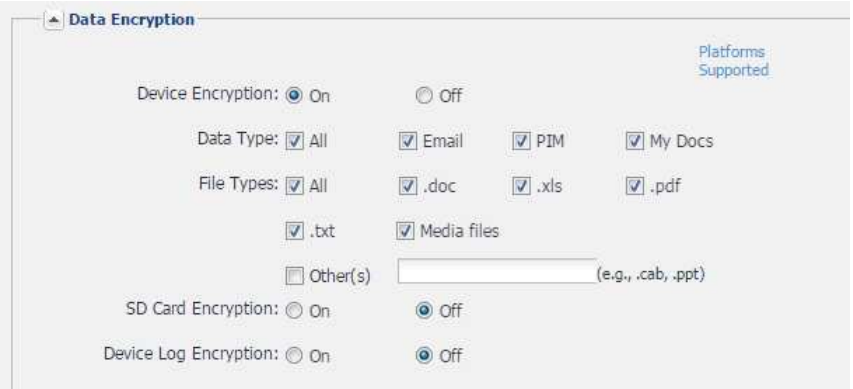

Figure 11 : Cryptage dans la politique de sécurité

Les tablettes se trouvant dans le groupe où est appliquée une telle politique de sécurité pourront alors crypter leurs données, mais cette partie, côté MDM*, ne suffit pas, il est nécessaire de faire des actions sur les appareils.

Dans la politique de sécurité, il est également possible de faire remonter en anomalie les tablettes qui n'ont pas leur cryptage effectué alors qu'il est demandé. Cela permet de voir l'avancée de cette mesure de sécurité.

4.4.2 Sur la tablette

La tablette, qui voit le cryptage activé dans la politique de sécurité qui lui est attribuée, active son option de cryptage.
Il est donc nécessaire maintenant d'aller dans les paramètres de la tablette et d'aller activer le cryptage en respectant certains prérequis tels qu'un mot de passe (code PIN refusé à partir d'Android 5), un niveau de batterie minimum de 80%, et un raccordement électrique.
Il faut bien penser à crypter la tablette entièrement, c'est-à-dire vérifier que l'option de cryptage rapide, qui ne crypte que l'espace utilisé sur le moment, soit désactivée afin que les futurs fichiers créées soient aux aussi cryptés.
J'ai testé et documenté toute cette procédure.

4.4.3 Problématiques et remarques

J'ai identifié un certain nombre de problématiques que pose le cryptage.

La première est le cas où le mot de passe contient une erreur lors du cryptage de la tablette, par exemple « C@sr@839 » à la place de « C@sr@0839 », et que nous ne savons donc pas quel est le mot de passe de la tablette. Quand la tablette s'éteindra, il ne sera plus possible de la rallumer sans connaitre le mot de passe, et il ne sera pas possible de faire un « factory reset » de la tablette puisque je l'ai interdit précédemment. La tablette serait alors inutilisable.

D'où une deuxième problématique : qui met en place le cryptage ? Soit nous distribuons ma documentation aux collaborateurs des agences et ils le mettent eux-mêmes en place. Nous prenons alors le risque qu'ils se trompent dans le mot de passe. Soit les techniciens de l'équipe passent pour le mettre en place dans les agences, mais le risque d'une erreur existe toujours même s'il est moindre, et cela veut dire qu'ils doivent passer dans plus de 200 agences, dont certaines sont loin, ouvertes seulement quelques jours dans la semaine ou uniquement les matins par exemple.

D'un point de vue organisationnel, j'ai cloné le groupe contenant les certificats, les applications et les politiques à appliquer sur les tablettes en agence. Dans ce clone, j'ai simplement changé la politique de sécurité par une autre, où le cryptage est activé, et une stratégie de mot de passe plus adaptée.
Ainsi, quand on déploiera le cryptage, j'aurais juste à appliquer ce groupe aux tablettes et à enlever le premier, au fur et à mesure que les agences seront traitées.
Dans le cas où nous le ferions faire par les collaborateurs, je pensais ne traiter, par exemple, que 5 agences par jour afin de permettre un support efficace.

4.5 Synthétisation des informations dans Mobile Iron

Comme dit précédemment, il est possible de faire remonter des configurations d'appareils en anomalies. Cependant, quand on accède à la liste de ces appareils à partir de la page d'accueil, ils sont tous mélangés, quelle que soit l'anomalie. Mon but était donc de visualiser tous ces appareils, mais regroupés par anomalies, pour savoir directement le problème de l'appareil.

Pour ce faire, il est possible, dans la recherche avancée des appareils, il est possible de visualiser les appareils selon des filtres tels que le numéro de version, le nom du fabriquant…
J'ai donc cherché un filtre pour afficher les appareils qui ont une certaine anomalie.
Une fois ce filtre trouvé, je l'ai relié à un groupe. De cette manière, on a plus qu'à visualiser ce groupe pour avoir la liste des appareils correspondants.

L’avantage de cette méthode est que le groupe est dynamique. Dès que l’appareil a une anomalie, il rentre dans le groupe filtré sur celle-ci, et dès qu’il ne l’a plus, il en sort automatiquement. De plus, quand on va voir les détails d’un appareil, notamment sa liste de groupe, on voit s’il est dans un groupe d’anomalies, et si oui qu’elle est son anomalie.

J’ai créé des groupes pour chacune des anomalies qu’on peut rencontrer sur nos appareils Android :

- Les droits administrateurs pour l’application Mobile@Work n’ont pas été validés
- Des applications ne respectant pas la liste blanche ont été installées
- Android est compromis
- L’appareil ne s’est pas connecté depuis une certaine période de temps

Pour anticiper sur la mise en place du cryptage, j’ai également créé un groupe pour les appareils qui ne sont pas cryptés alors qu’ils devraient l’être.

Cependant, je n’ai pas encore trouvé le moyen de mettre une alarme sur certaines anomalies, ni un filtre pour avoir la liste des appareils avec ces anomalies. Par exemple, dans la politique de sécurité, il est défini que les appareils doivent avoir un mot de passe. Quand un appareil est détecté sans mot de passe, c’est-à-dire qu’il ne respecte pas sa politique de sécurité, une notification sur l’appareil apparait, et on peut voir dans les détails cette incohérence.

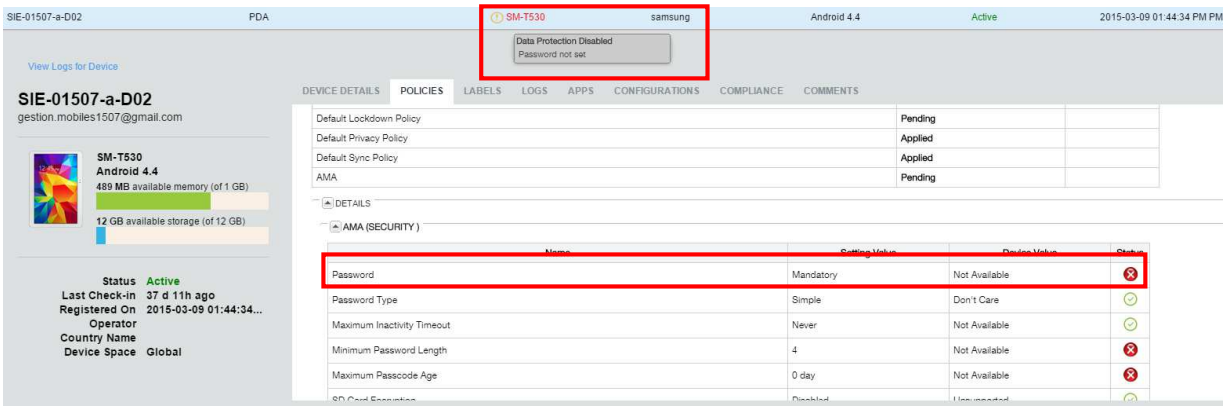

Figure 12 : Tablette sans mot de passe

Malgré toutes mes recherches sur internet, je n’ai pas encore trouvé le moyen de faire ressortir ces appareils en alerte, ni trouvé un filtre pour tous les afficher sur ce détail. C’est un grave problème de sécurité car la tablette n’est pas protégé par un mot de passe, donc n’importe qui peut l’utiliser. Il me reste cependant une piste, des APIs de Mobile Iron.

4 Conclusion

Pour conclure mon mémoire de stage sur cette année d'apprentissage, réalisée au sein du Crédit Agricole Sud Rhône-Alpes, plusieurs missions m'ont été attribuées.

La première est le support et la maintenance du parc. J'ai résolu les incidents que les utilisateurs pouvaient rencontrer avec leur divers matériel de travail, et j'ai su les assister. Pour la gestion du parc informatique, j'ai réalisé des inventaires, géré les livraisons de matériels. J'ai également assuré des opérations de câblages et de configurations des switchs, et réfléchi à des solutions de sécurisations physiques des installations techniques.

Mes connaissances et compétences techniques acquises lors du BTS Services Informatiques aux Organisations et lors de cette année à l'IUT, m'ont été fortes utiles. Je me suis servi par exemple de celles concernant les réseaux : configuration et sécurisation des switchs, ainsi que celles sur la manière de penser pour sécuriser et gérer le parc.

Je n'avais pas encore travaillé sur certains équipements avant cette année, tels que les imprimantes. J'ai appris au fur et à mesure de mes interventions, et grâce à l'aide de mes collègues, comment les gérer et comment intervenir dessus.

Ce travail permet d'assurer le bon fonctionnement du système informatique, pour que les collaborateurs puissent travailler dans des conditions optimales. Les collaborateurs en agence peuvent ainsi accéder aux comptes des clients, les renseigner et faire des actions avec eux, tandis que les collaborateurs des sites peuvent faire leur travail d'analyse de prêt, de communication…

Dans le cadre de mon projet, j'ai dû gérer le parc d'appareils mobiles en les sécurisant, synthétiser les informations sur l'interface web, et analyser les différentes configurations des appareils remontant en erreur. J'ai dû adapter mes connaissances diverses et utiliser mes connaissances personnelles pour les appliquer sur les appareils mobiles.
Ce projet s'inscrit dans le cadre de garantie de confidentialité et d'intégrité des données, que doit assurer une banque.

J'ai eu diverses difficultés, notamment sur le temps d'adaptation pour connaître les matériels sur lesquels je n'avais encore jamais travaillé. J'ai également dû apprendre à utiliser MobileIron, et apprendre comment gérer un parc d'appareils mobiles, ce que je n'avais jamais abordé lors de mes études.

J'estime m'être bien intégré dans l'équipe, et dans le siège du Crédit Agricole de Grenoble, et avoir accompli au mieux mon projet et mes missions.

Cette année d'alternance m'a permis, tout en continuant une année d'étude, de découvrir dans la durée le monde professionnel. Cette année combinée avec mes deux stages en informatique lors du BTS SIO et mes travails d'été m'ont permis d'avoir une idée complète de ce monde. J'ai pu approfondir mes connaissances et développer mes compétences dans le domaine de la sécurité informatique, de la gestion de parc, d'appareils mobiles ou de postes de travail « standards ».
Après mon alternance, je souhaiterais rester dans l'équipe si une place s'ouvre, sinon un poste d'administrateur systèmes me plairait.

5 Glossaire

CATS : Crédit Agricole Technologies et Services : GIE* dont la mission est de développer et d'exploiter un système d'information commun pour toutes les caisses régionales du groupe Crédit Agricole.

GIE : Groupement d'Intérêt Economique. Ici, il s'agit du regroupement des caisses régionales pour développer des services communs, en réalisant des économies d'échelle.

MDM : Mobile Device Management : gestion d'appareils mobiles

SIL MESSI : licence professionnelle Systèmes Informatiques et Logiciels, option MEtiers de l'administration de la Sécurité des Systèmes d'Informations.

TOIP : « Telephony Over Internet Protocol » consiste à mettre en place des services téléphoniques sur un réseau IP en utilisant la technique de la voix sur IP. Les communications vocales sont transmises via un réseau IP.

VLAN : Un réseau local virtuel est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même switch de niveau 2 du modèle OSI (couche liaison). Ils présentent les intérêts suivants :

- Améliorer la gestion du réseau,
- Optimiser la bande passante,
- Séparer les flux,
- Fragmentation : réduire la taille d'un domaine de broadcast,
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines de différents VLAN est de passer par un routeur.

6 Références

Documents webographiques :

Références :

- Coat F. Consignes de rédaction du mémoire de stage. 2016. Rapport interne. IUT2, Université Grenoble-Alpes.
- www.creditagricole.info/
  Site d'informations du Crédit Agricole.
- www.ca-sudrhonealpes.fr/
  Site du Crédit Agricole Sud Rhône-Alpes
- Intranet du Crédit Agricole
- www.wikipedia.fr

7 Résumé et Abstract

Dans le cadre de ma formation en licence professionnelle Systèmes Informatiques et Logiciels option MEtiers de l'administration et de la Sécurité des Systèmes d'Information, j'ai réalisé mon alternance au sein de l'unité assistance et maintenance informatique du Crédit Agricole Sud Rhône-Alpes (CASRA) au siège social de Grenoble en Isère. CASRA est leader de la banque-assurance sur son territoire.

Plusieurs missions et un projet m'ont été attribués pour cette année.
Ces missions ont été le support et la maintenance du parc informatique. Cela passe par de nombreuses et diverses actions telles que l'assistance ou le dépannage des utilisateurs, l'installation de logiciel ou de postes, et l'inventaire de matériel.

Mon projet a consisté à travailler sur un outil de gestion du parc d'appareils mobiles. L'objectif était d'apporter à ces appareils un supplément de sécurité, et d'améliorer la gestion du parc en facilitant la détection des appareils en défaut de conformité. J'ai également analysé et classifié les modes de fonctionnements des appareils, comme le mode kiosque pour les tablettes Android.

Mots clés : Crédit Agricole, maintenance d'un parc informatique, support utilisateur, parc d'appareils mobiles, sécurité informatique.

One Year of Apprenticeship

abstract: During my professional license computer and software systems option administration and security of the information system, I did a year of apprenticeship in the support and computer maintenance unit in the administrative site of Crédit Agricole Sud Rhône-alpes (CASRA) in Grenoble. CASRA is the leader of bank and insurance of his territory. I had several missions and a project to do. First, I had to work for the help desk and the maintenance of the computing network. This goes through numerous and various tasks like assistance and troubleshooting of the users, installation of software or computer station, and inventories. My project was the management of the mobile devices. I had to bring a supplement of security to them, and to improve this management by facilitating the detection of devices in non-compliance. Furthermore, I thought and analysed operating modes like the kiosk mode for Android's tablets.

Key words: Crédit Agricole, maintenance of the computing network, help desk, mobile devices, computing security.