Mise en place d'un annuaire unique et intégration des postes clients sur l'Université de Lorraine

François Clémence

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE STRASBOURG

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : INFORMATIQUE

OPTION : Informatique Système d'information

par

François Clémence

Mise en place d'un annuaire unique et intégration des postes clients sur l'Université de Lorraine

Soutenu le 20 janvier 2015

JURY

PRESIDENT : Madame Isabelle Wattiau

MEMBRES : Monsieur François Benavoli
Monsieur Cédric Kleinpeter
Monsieur Olivier Mathieu
Monsieur Emmanuel Maurice

Remerciements

M. Cédric Kleinpeter, mon directeur de mémoire

Les membres du jury

M. Olivier Mathieu, responsable informatique du site de Metz pour les Services aux Usagers

M. Eric Sand, sous-directeur des Services aux Usagers

M. Michaël Becker, M. Alain Gomez, M. Nicolas Kutscheck, mes collègues de travail, ainsi que les informaticiens du site de Metz et de Nancy

Ma famille et mes amis

Liste des abréviations

AD : Active Directory

AMUE : Agence de Modernisation des Universités et Etablissements

DHCP : Dynamic Host Configuration Protocol

DN : Direction du Numérique

DNS : Domain Name System

ENT : Environnement Numérique de Travail

GPO : Group Policy Objects

INPL : Institut National Polytechnique de Lorraine

MDT : Microsoft Deployment Toolkit

MSI : Windows Installer

OU : Unités d'Organisation

PRES : Pôle de Recherche et d'Enseignement Supérieur

PXE : Preboot eXecution Environment

SU : Services aux Usagers

UFR : Unité de Formation et de Recherche

UHP : Université Henri Poincaré

UL : Université de Lorraine

UPVM : Université Paul Verlaine - Metz

WDS : Windows Deployment Services

WIM : Windows Imaging

Glossaire

Active Directory : service d'annuaire qui va fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows

Apogée : logiciel de l'AMUE permettant la gestion des étudiants d'un établissement

Dynamic Host Configuration Protocol : protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres réseau d'une station

Domain Name System : service permettant la corrélation entre les adresses réseau et le nom de domaine associé

Environnement Numérique de Travail : désigne un ensemble d'outils en ligne qui agrège l'information et permet un accès à distance des ressources numériques

Group Policy Objects : fonctions de gestion centralisées de la famille Microsoft Windows

Harpège : logiciel de l'AMUE permettant la gestion des personnels d'un établissement

Microsoft Deployment Toolkit : outil Microsoft permettant le déploiement des postes de travail

Windows Installer : moteur d'installation, de mise à jour et de désinstallation de logiciel, propre aux systèmes d'exploitation de Microsoft

Unités d'Organisation : conteneurs d'Active Directory

Preboot eXecution Environment : permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur

SIFAC : logiciel de l'AMUE permettant la gestion financière d'un établissement

Wikidocs : le Wiki de l'Université de Lorraine

Windows Deployment Services : services de déploiement réseau Microsoft

Windows Imaging : format Microsoft d'image de disque

Table des matières

Introduction

« Le mardi 25 janvier 2011, les conseils d'administration des universités de Lorraine (INPL, Université Henri Poincaré, Université Nancy2, Université Paul Verlaine-Metz) ont approuvé le décret constitutif de l'Université de Lorraine. C'est au sein de chacun des établissements que les conseils d'administration ont adopté le principe de fusion, l'acte fondateur d'un établissement unique en Lorraine au 1er janvier 2012 », indiquait le communiqué de presse publié par le PRES Lorrain. L'Université de Lorraine était née ! Cette fusion résulte d'un mouvement amorcé dès 2007 et qui a progressivement rassemblé tous les acteurs locaux soucieux de trouver des réponses adaptées au contexte lorrain.

Au-delà des enjeux politiques et de ceux liés à l'offre de formation, le rapprochement des établissements a nécessité une refonte totale du système d'information afin d'offrir un service uniforme sur tous les périmètres géographiques, tout en garantissant la pertinence et la cohérence des données. Cet énorme chantier a débuté un an avant la fusion, dès 2011. Il a été facilité par l'utilisation d'outils communs au sein des établissements lorrains, pour la plupart issus de l'AMUE ou du monde libre. En 2012, une dernière brique restait à poser : la mise en place d'un annuaire commun permettant l'authentification des utilisateurs sur les postes de travail. Ce chantier majeur s'intègre également dans une réflexion sur le processus de production du poste client.

Je vais donc vous présenter mon travail sur ces deux projets. Après une présentation de l'Université de Lorraine et de la Direction du Numérique, nous détaillerons la mise en place d'un annuaire Microsoft sur l'université. La deuxième partie de ce mémoire sera ensuite consacrée à l'intégration des postes clients dans ce nouveau référentiel.

I Première partie : mise en place d'un Active Directory unique à l'Université de Lorraine

Dans cette première partie, nous allons présenter l'Université de Lorraine où je travaille, la Direction du Numérique et le projet de mise en place d'un annuaire unique. En particulier, nous parlerons du contexte du projet et de ses objectifs, des choix techniques effectués, de sa réalisation et de son suivi. Dans la deuxième partie, nous étudierons la façon dont les postes clients se sont connectés à ce nouveau référentiel.

I.1 Présentation de l'Université de Lorraine (UL)

Pour présenter cette institution, je vais m'appuyer sur un rapport de 2013 de l'Agence d'évaluation de la recherche et de l'enseignement supérieur[1]. L'université de Lorraine existe depuis le 1er janvier 2012, création qui s'inscrit dans une histoire, une dynamique et un contexte.

I.1.1 Une histoire

L'UL rassemble des entités anciennes, aux identités affirmées : les deux universités de Nancy, l'université de Metz et l'Institut National Polytechnique de Lorraine (INPL). En 2010-2011, l'université Henri Poincaré, Nancy 1, (2 559 emplois d'enseignants et de non enseignants[2] ; 17 566 étudiants inscrits) couvrait les domaines des sciences, des technologies et de la santé (STS), avec 5 facultés, 3 écoles d'ingénieurs, 3 IUT et 1 IUFM. L'université Nancy 2 (1 073 emplois ; 16 806 étudiants) était active en arts, lettre, langues (ALL) ; sciences humaines et sociales (SHS) et droit, économie et gestion (DEG), avec 7 UFR, 7 instituts dont 2 IUT, et un centre d'enseignement à distance.

L'université Paul Verlaine de Metz (1 204 emplois ; 13 823 étudiants) couvrait les mêmes secteurs que les deux universités nancéiennes sauf celui de la santé, avec 6 UFR, 3 IUT et 2 départements d'université. L'INPL (742 emplois ; 3 844 étudiants) déployait ses 7 écoles d'ingénieurs et un cycle préparatoire polytechnique.

[1] http://www.aeres-evaluation.fr/Etablissements/UNIVERSITE-DE-LORRAINE
[2] Indicateurs de l'enseignement supérieur, portail d'aide au pilotage de l'enseignement supérieur et de la recherche (PapESR) 2010-2011.

Au final, le nouvel ensemble regroupe plus de 52 000 étudiants et 5 578 emplois d'enseignants et de non enseignants, occupant 830 000 m2 de surface bâtie répartis sur 53 sites en Lorraine. Le budget prévisionnel de l'UL pour 2012 est de l'ordre de 560 M€.

I.1.2 Une dynamique

L'UL résulte d'un mouvement amorcé dès 2007 et qui a progressivement rassemblé tous les acteurs locaux soucieux de trouver des réponses adaptées au contexte lorrain. La création du pôle de recherche et d'enseignement supérieur (PRES) Nancy-Université en 2007, l'opération Campus en 2008 pour laquelle les quatre universités ont déposé un projet commun, la signature d'un contrat quadriennal unique entre Nancy 1, Nancy 2 et l'INPL en 2009, et la création du PRES de l'université de Lorraine en 2009 ont été les étapes déterminantes du processus. Il faut souligner aussi le rôle moteur du comité de coordination et d'orientation scientifique lorrain (CCOSL), créé en 2007 et associant les quatre établissements universitaires, les organismes de recherche présents en Lorraine et le CHU. C'est dans le cadre de ces étapes qu'a été engagée une discussion, d'abord sur un rapprochement des quatre universités, dès 2008, puis sur une fusion, en 2010. Le soutien des collectivités territoriales, matérialisé notamment par la signature d'un pacte territorial en juillet 2008, et celui des partenaires socio-économiques, ont favorisé l'aboutissement du projet.

I.1.3 Un contexte

Le contexte était porteur. La région Lorraine, avec ses 2,35 millions d'habitants en 2010, est marquée par des difficultés économiques : les restructurations ont fortement touché un secteur industriel qui a perdu un cinquième de ses emplois entre 2001 et 2009 et qui représentait encore en 2009 près de 20 % des emplois lorrains. Le secteur tertiaire compte environ 60 % des salariés lorrains[3]. Le taux de chômage est élevé (9,9 % à fin 2010), la croissance démographique est plus faible que la moyenne nationale.

Face à la situation industrielle dégradée de la région, les responsables politiques, universitaires et ceux du monde socio-économique, ont fait le pari de développer l'économie de la connaissance. Aucun établissement universitaire lorrain n'ayant la notoriété suffisante pour jouer un rôle moteur dans le rebond régional, la construction d'une université lorraine de rang international s'est progressivement révélée incontournable avec l'ambition de "relever le double

[3] http://www.insee.fr/fr/regions/lor/default.asp?page=faitsetchiffres/presentation/presentation/htm [15/07/12]

défi de l'excellence et de la proximité". Si excellence et proximité sont des ambitions louablement partagées par de nombreuses universités européennes, la volonté de construire une "région-campus" est un trait distinctif de l'UL. À l'échelle régionale, les tensions historiques, bien que déjà considérablement estompées, nécessitaient encore un subtil équilibre territorial. Au niveau transfrontalier, le développement des ambitions universitaires, notamment au Luxembourg et en Sarre, plaidait également pour un établissement lorrain de grande taille capable en même temps d'assurer la présence de l'université sur les territoires et au cœur des villes, de contribuer au développement socio-économique de la région et de participer à son rayonnement.

Tel est le contexte dans lequel a vu le jour l'UL. Pour réussir la fusion et relever les défis, les porteurs du projet ont adopté une méthode et des solutions originales, qui se traduisent dans un décret statutaire de création de grand établissement[4], par des structures, des répartitions de compétences et des modes d'organisation particuliers.

I.1.4 Une organisation ouverte

À la différence de la plupart des autres établissements universitaires, l'UL a opté pour un statut de grand établissement[5], qui lui permet de déroger à un certain nombre de dispositions propres aux universités et de mieux prendre en compte les spécificités de la réalité lorraine. Les dérogations mises en places à l'UL portent sur la composition du conseil d'administration (CA), le mode de désignation du président, la durée des mandats, la création d'entités nouvelles (directoire, sénat académique, conseil de la vie universitaire [CVU], pôles scientifiques [PS] et collégiums), les modalités d'approbation des accords et des conventions ainsi que celles relatives aux règlements d'examens et aux modalités de contrôle des connaissances (MCC). Ces innovations répondent à des motivations diverses et relèvent de la démarche pragmatique adoptée pour la fusion ; elles permettent de rassurer certaines composantes, ce qui garantit la pérennité des regroupements, en particulier pour les écoles d'ingénieurs.

I.1.4.1 Pôles scientifiques et collégiums : de nouvelles entités

L'UL a fait le choix de la subsidiarité. Ainsi a-t-elle introduit, entre le niveau central et celui des composantes, un échelon supplémentaire, constitué de pôles scientifiques regroupant des unités de recherche (UR), et de collégiums regroupant des composantes (UFR, écoles,

[4] Décret 2011-1169 du 22/09/2011.
[5] Décret 2011-1169 du 22/09/2011, art. 1 et 13.

instituts). Huit collégiums et dix pôles scientifiques sont ainsi créés. Le décret statutaire fixe leurs prérogatives ; ces entités peuvent également se voir attribuer des missions, fixées par leur règlement intérieur, et approuvées par le CA de l'université. Celles-ci sont ainsi différentes d'un collégium à un autre ou d'un PS à l'autre. D'autres compétences pourront leur être confiées par délégation du président, ou transférées par leurs composantes. Cette situation est à l'image de l'organisation d'ensemble de l'UL : la structure est ouverte aux modifications, gage de souplesse pour l'avenir, parfois aussi source d'inquiétude pour de nombreux acteurs.

I.1.4.2 Des innovations dans les organes centraux

L'équipe de la présidence est constituée du président et de plusieurs vice-présidents (VP). Outre les VP statutaires (VP CA, VP étudiant, VP CS, VP CF et VP CVU), des VP fonctionnels ont été nommés par le CA sur proposition du président. Les attributions de ces derniers reflètent des choix de priorités : moyens et ressources humaines (VP et VP adjoint), partenariats socio-économiques et relations internationales, politique immobilière, politique numérique et systèmes d'information[6]. Cette équipe est entourée de l'agent comptable, du directeur général des services (DGS) et de chargés de mission. À terme, la direction générale des services sera renforcée par un adjoint et trois délégués dédiés aux relations et conditions de travail, à la vie institutionnelle et aux processus opérationnels.

Les conseils centraux, qui jouent à l'UL, dans l'ensemble, le même rôle que dans une université traditionnelle, dérogent aux règles communes sur plusieurs points et profitent des latitudes offertes par le statut de grand établissement.

Lieu d'arbitrage et d'impulsion, le directoire rassemble les directeurs de pôles scientifiques et de collégiums autour du président et de l'ensemble des vice-présidents. S'il peut être assimilé au bureau ou comité de direction des universités traditionnelles, il est appelé à jouer à l'UL un rôle particulier, et central, consistant à assurer la coordination entre l'organisation des missions de formation et de recherche, et à préparer les grandes décisions qui y seront discutées avant d'être soumises au vote du CA.

[6] http://www.univ-lorraine.fr/content/constitution-de-léquipe-du-président [15/07/2012].

Nouvelle instance statutaire permettant d'apporter plus de collégialité dans la gouvernance de l'UL, le sénat académique est strictement consultatif. Il ne pourra jouer un rôle important que si ses avis sont pris en compte par le président et le CA.

Le conseil des études et de la vie universitaire (CEVU) habituel a été remplacé par deux conseils, le conseil de la formation (CF) et le conseil de la vie universitaire (CVU), ce qui constitue une réelle innovation. Cette originalité est perçue par beaucoup comme le moyen de traiter en profondeur des sujets transversaux habituellement délaissés : emploi du temps des étudiants et des personnels, vie sur le campus, services innovants sont autant de pistes évoquées. L'UL s'appuie sur ce CVU pour mettre la qualité de vie, notamment étudiante, au cœur de la stratégie de l'établissement et en faire un facteur d'attractivité et de développement.

I.1.5 La Direction du Numérique (DN)

La Direction du Numérique est chargée de la mise en œuvre opérationnelle de la stratégie numérique de l'Université de Lorraine et assure la sécurité du système d'information.

I.1.5.1 Ses missions

Ses missions, d'une grande diversité, sont déclinées en quatre grandes thématiques :

- La mise en œuvre du système d'information de gestion : développement, intégration et suivi opérationnel des applications de gestion.
- Le développement et le maintien des infrastructures systèmes et réseaux.
- Le service aux usagers de l'établissement et l'ingénierie du poste de travail.
- Le développement de services numériques, la promotion de leurs usages, et la production de contenus numériques ou audiovisuels.

Pour mener à bien les différentes facettes de ces missions plus de 160 collaborateurs mobilisent des compétences variées et complémentaires : architectes de système d'information, administrateurs systèmes et réseaux, développeurs d'application, audiovisualistes, chefs de projet multimédia, ingénieurs pédagogues, techniciens de proximité…

I.1.5.2 Son organisation

Depuis 2012, la Direction du Numérique est organisée en quatre sous-directions faisant écho à ses quatre missions principales[7]. Afin de mieux comprendre les enjeux, nous allons rapidement présenter les périmètres de chaque sous-direction :

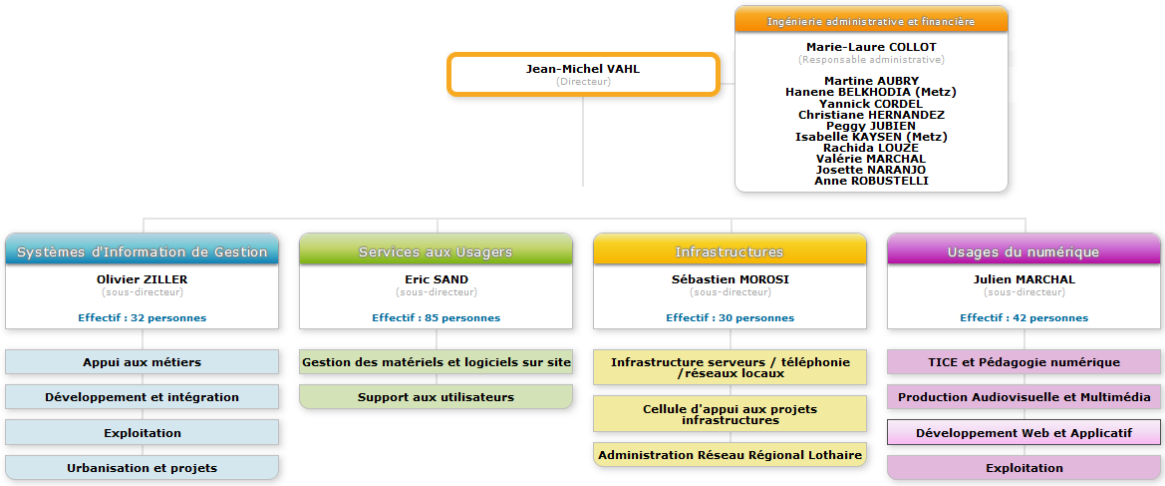


Figure 1 - Organigramme de la Direction du Numérique

Les missions principales de la sous-direction Système d'Information de Gestion sont :

- La conception d'applications de gestion spécifiques à l'Université de Lorraine
- L'intégration au système d'information d'applications de gestion fournies par des éditeurs tiers
- Le déploiement et la mise en œuvre de toutes les applications de gestion
- L'accompagnement des directions métiers dans leurs projets d'évolution du système d'information
- L'assistance technique sur les applications de gestion
- Les extractions de données pour des besoins de pilotage

La sous-direction Services aux Usagers conseille et assiste les utilisateurs dans le choix et l'usage des solutions numériques. Afin d'assurer ses missions, les personnels qui la composent

[7] http://numerique.univ-lorraine.fr/la-direction-du-numerique-de-luniversite-de-lorraine

sont basés géographiquement à proximité des utilisateurs. Elle installe et assure le maintien en condition opérationnelle ainsi que la sécurité des équipements dont elle a la responsabilité :

- Les postes de travail et les périphériques
- Les serveurs locaux
- L'infrastructure d'authentification

La sous-direction Infrastructure quant à elle, assure le déploiement des infrastructures matérielles, systèmes et réseaux de l'université. Elle assure le maintien en condition opérationnelle des infrastructures et en assure la sécurité. Les principales infrastructures déployées et services rendus sont :

- L'infrastructure système pour l'hébergement des services numériques et les services aux usagers comme l'ENT
- L'infrastructure de stockage et de sauvegarde
- L'infrastructure système pour le SI de gestion
- L'infrastructure réseau des sites de l'université de Lorraine
- Le service de messagerie Zimbra
- Les services centraux d'authentification (CAS, Shibboleth, radius …)

Enfin, la sous-direction des Usages du Numérique a pour missions essentielles le développement et la mise en œuvre d'outils et d'interfaces, la production de contenus numériques ainsi que l'accompagnement des utilisateurs, étudiants, enseignants et personnels, dans leur utilisation de l'ensemble des services numériques de l'établissement. L'ensemble de la sous-direction est répartie sur les sites de Brabois et du Saulcy.

Cette sous-direction développe aussi la thématique de l'accompagnement des équipes pédagogiques dans le cadre de l'utilisation de solutions numériques dans les cours réalisés en présentiel, hybride ou à distance et dans le cadre de l'accompagnement et de l'évolution des pratiques pédagogiques.

I.1.5.3 Mon affectation à l'UL

J'ai été nommé responsable des équipes informatiques des UFR Sciences Humaines et Sociales, Arts Lettres et Langues en 2008 à Metz[8]. J'encadre une équipe de deux techniciens informatiques et d'un assistant ingénieur. Nous pilotons près de 1000 postes clients ainsi qu'une trentaine de serveurs sous Windows et Linux. Par ailleurs, je gère un budget annuel de près de 200000 € qui couvre les achats de matériels, de périphériques, de logiciels et de fournitures. Interlocuteurs privilégiés de 5000 étudiants, 250 enseignants et 80 personnels, nous sommes des acteurs irremplaçables sur notre périmètre.

Site pilote sur Metz et suite à ma demande, nous avons intégré la Direction du Numérique et les Services aux Usagers dès 2012. En effet, je souhaitais que les agents puissent échanger plus facilement avec leurs collègues lorrains et bénéficier de l'expertise de l'ensemble des informaticiens. A la fois participant et pilote sur de nombreux projets informatiques sur Metz, j'ai été enthousiaste à l'idée d'un projet d'annuaire commun.

I.2 Mise en place d'un annuaire unique

La fusion des établissements a nécessité une refonte totale du système d'information afin d'offrir un service uniforme sur tous les périmètres géographiques tout en garantissant la pertinence et la cohérence de l'information. Cet énorme chantier a débuté 1 an avant la fusion, dès 2011. Il a été facilité par l'utilisation d'outils communs au sein des établissements lorrains, pour la plupart issus de l'AMUE (Apogée, Harpège, SIFAC)[9] ou issus du monde libre comme l'annuaire LDAP. En effet, le SI d'un établissement s'appuie typiquement sur trois briques métiers et un annuaire central :

- SIFAC, utilisant SAP et assurant la gestion financière de l'entité.
- Apogée, composant « scolarité » de l'AMUE et permettant une gestion des étudiants et des enseignements tout en intégrant les dispositifs réglementaires en vigueur.

[8] http://shs-metz.univ-lorraine.fr/
[9] http://www.amue.fr/

- Harpège, brique « ressource humaine » provenant également de l'AMUE et nécessaire à la bonne gestion des personnels et enseignants, de l'affectation initiale à la gestion de carrière.

- Un annuaire LDAP basé sur OpenLDAP. Ce composant est au centre du SI de l'établissement. Il va contenir de nombreuses informations critiques comme la structure d'accueil de l'utilisateur ou la formation de l'étudiant. Par ailleurs, il va contenir l'identifiant et le mot de passe des étudiants et des personnels, nécessaires à toute application qui souhaite baser son authentification sur l'annuaire. Il va également enregistrer toutes les informations indispensables au système de messagerie (adresse email, redirections, quotas…). De la même façon, cette brique centrale est utilisée par les postes clients Windows et Linux pour procéder à l'authentification de l'utilisateur sur la machine.

Le schéma ci-dessous montre le mécanisme d'alimentation du LDAP central, similaire pour les 4 ex-établissements. Les traitements (ETL) s'effectuaient une fois par jour, pendant la nuit afin de ne pas perturber le bon fonctionnement de l'annuaire. Enfin, une interface Web en PHP est aussi utilisée pour compléter les imports automatiques selon une procédure définie par chaque établissement.

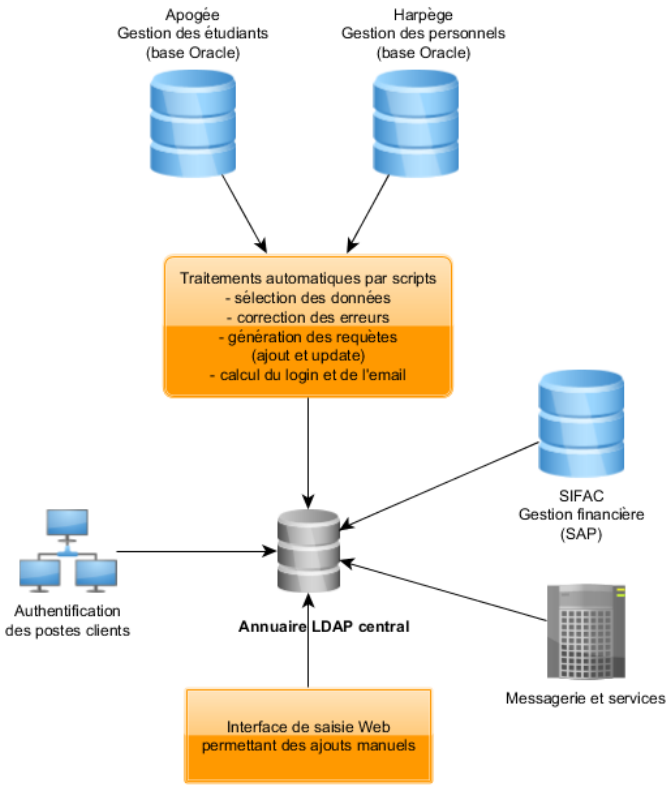


Figure 2 – SI type d'un établissement universitaire

Les bases de données et les annuaires ont été fusionnés et consolidés afin de permettre le bon fonctionnement du nouvel établissement. La Direction du Numérique s'est mobilisée afin de fournir dès 2012 un SI unique permettant une gestion centralisée des étudiants et personnels ainsi qu'un accès homogène aux services centraux (messagerie, annuaire, sites Internet…). Cette opération lourde a permis le bon déroulement des inscriptions pédagogiques en 2012/2013, tout en offrant des outils performants dans le domaine des ressources humaines et des applications de gestion financière, indispensables au pilotage de l'UL. Je ne détaillerais pas plus cette opération, qui nécessiterait l'écriture d'un second mémoire.

I.2.1 La problématique de l'authentification des postes clients

L'utilisation de briques communes provenant de l'AMUE a grandement facilité les opérations de fusion dans les domaines clefs de la scolarité, des ressources humaines et de la gestion financière. Un seul problème persistait : l'authentification du poste client. Contrairement aux chantiers précédents, les écarts dans chaque établissement étaient très importants et les technologies employées parfois antagonistes, rendant impossible une interopérabilité des systèmes.

Bien que cet aspect soit moins critique que les trois chantiers précédemment évoqués, la mise en place d'une authentification unique des postes clients est un chantier d'envergure. En effet, la création de l'UL a modifié l'offre pédagogique qui était auparavant cantonnée à un établissement unique. De nombreuses formations s'effectuent désormais sur plusieurs sites différents et un cycle d'étude peut commencer à Metz pour finir à Nancy. La mobilité des étudiants s'est renforcée et engendre de nouveaux usages et de nouveaux besoins. Il était impératif pour la Direction du Numérique de gérer ce scénario qui s'inscrit dans la fusion des systèmes d'information des anciens établissements.

Eric Sand, sous-directeur des Services aux Usagers a pris ce dossier en charge et a lancé en février 2012 un groupe de travail sur le sujet. Etant un des référents des systèmes Windows dans l'ex-Université de Metz, j'ai décidé d'intégrer cette équipe projet et de relever ce nouveau défi avec l'aval de mon supérieur, Olivier Mathieu. La première réunion s'est déroulée le 31 janvier 2012. Son unique objectif était une présentation des usages concernant l'authentification du poste de travail sur les anciens établissements.

I.2.2 Les usages à Nancy 2

Les informaticiens de Nancy 2 utilisaient historiquement un annuaire OpenLDAP pour gérer les utilisateurs et les connexions aux applications. Cette pierre angulaire est alimentée par

les logiciels de l'AMUE, Apogée et Harpège. En 2006, un projet d'annuaire Active Directory a vu le jour afin de gérer plus efficacement l'authentification et la gestion du poste de travail sous Windows. Ce projet d'annuaire Microsoft, synchronisé à l'annuaire central, a rassemblé des informaticiens de la présidence, des campus et de diverses équipes transverses. Une dizaine de personnes ont procédé à une étude de faisabilité avant le démarrage du projet. Le périmètre de l'étude s'est tout d'abord limité aux postes pédagogiques. En mai 2006, les premiers postes clients sous Windows XP ont rejoint le domaine Active Directory et de nombreuses documentations ont été rédigées afin d'accompagner le changement. Devant le succès de l'opération, une réflexion a été menée par le groupe de travail pour intégrer les postes des personnels dans l'annuaire, opération achevée en 2008.

L'annuaire Active Directory de Nancy 2 était synchronisé à l'annuaire central OpenLDAP par l'intermédiaire de différents scripts quotidiens, afin d'alimenter les comptes des utilisateurs. L'annuaire Windows contenait 4000 comptes personnels, 30000 comptes étudiants et plus de 2500 machines. L'architecture matérielle s'appuyait sur 5 serveurs ou contrôleurs de domaine, assurant le traitement des connexions des postes clients et la haute disponibilité de l'ensemble sur Nancy et Epinal. Un espace de stockage commun (NAS ou Network Attached Storage) complétait l'ensemble et permettait une centralisation des documents des utilisateurs, ainsi qu'une sauvegarde efficace et aisée.

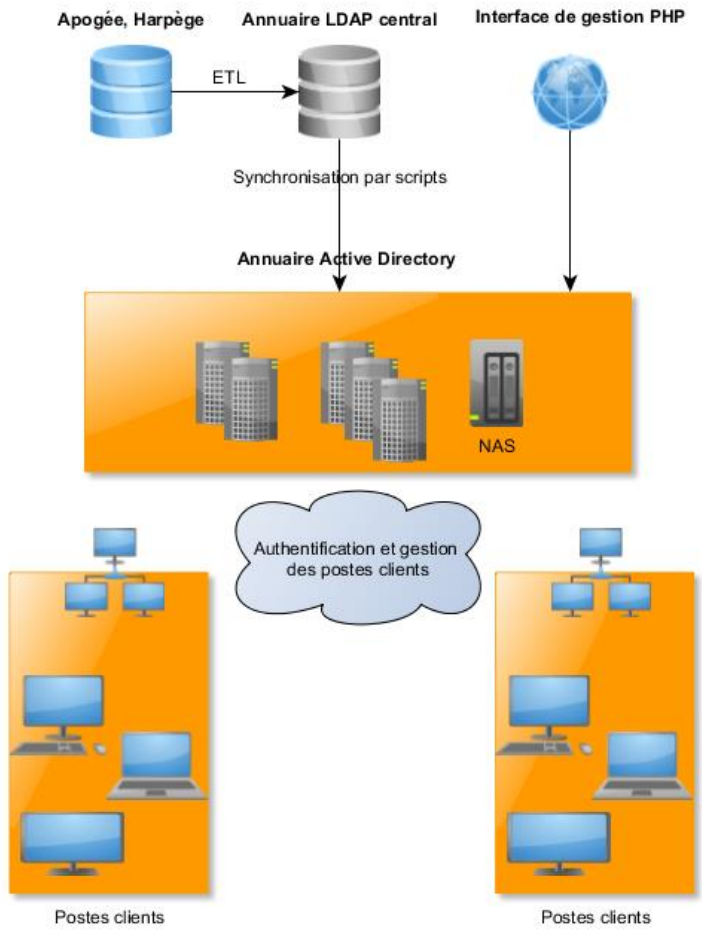


Figure 3 – Le SI à Nancy 2

Concernant la structure de l'annuaire, le groupe de travail a choisi de regrouper toutes les entrées au sein d'une seule forêt et d'un seul domaine Active Directory, notions dont nous reparlerons ultérieurement. Un système de délégation de droits a été aussi mis en place pour que les équipes locales puissent intervenir sans passer obligatoirement par un référent central. Des outils Web en PHP ont également été développés pour permettre la manipulation des objets de l'annuaire Microsoft, sans altérer l'annuaire OpenLDAP. Enfin, des règles de gestion ont été éditées et validées par l'ensemble des informaticiens afin de gérer de façon efficace et collaborative ce nouvel outil.

I.2.3 Les usages à l'UHP

Le système utilisé à l'UHP est relativement similaire à celui de Nancy 2. La différence principale réside dans le choix de la base centrale qui n'est ici pas un annuaire OpenLDAP mais une base MySQL. Ce système est alimenté en amont par des extractions et des ETL provenant des applications de l'AMUE, Apogée et Harpège. L'objectif est similaire à l'utilisation d'un annuaire

OpenLDAP, il s'agit de recenser tous les personnels et étudiants de l'établissement ainsi que les informations nécessaires aux différents applicatifs.

Cette base de données, nommée « LOGIN », est devenue le centre d'information principal pour les administrateurs systèmes ainsi que pour la génération des annuaires de l'établissement. Une interface Web a été ajoutée afin de consulter les entrées. Par ailleurs, des traitements manuels sont également possibles par les gestionnaires. A partir de cette base de données, l'UHP a construit plusieurs annuaires :

- Un annuaire OpenLDAP, afin de gérer le système de messagerie et les machines sous Linux
- Un annuaire Active Directory pour gérer les étudiants utilisant Windows
- Un annuaire Active Directory pour les personnels

Dès 2003, l'UHP a mis en place un annuaire Active Directory au sein de son établissement, fédérant ainsi toutes les entités du campus. Cette première mouture concernait uniquement les comptes étudiants. Comme à Nancy 2, le choix s'est porté sur une forêt et un domaine unique afin de faciliter l'administration du système, tout en préservant l'autonomie des responsables de sites en utilisant des délégations de droits. Un second annuaire Active Directory a été ultérieurement créé, entièrement dédié aux personnels (Antonelli, Bisaro, & Maillard, 2005). Un tel choix se justifie par la volonté d'isoler physiquement et logiquement les réseaux et les données de ces deux populations. Au niveau physique, les serveurs se trouvent en central ou dans les composantes. Enfin, l'UHP est également équipée d'un stockage central afin de gérer efficacement les fichiers des utilisateurs.

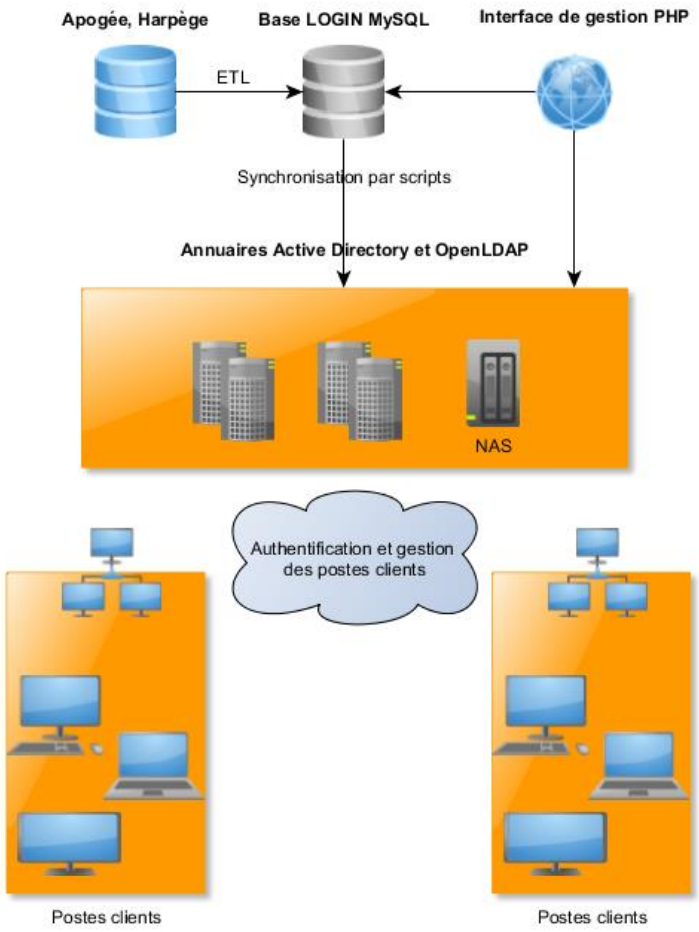


Figure 4 – Le SI à l'UHP

I.2.4 Les usages à l'INPL

Le site de l'INPL regroupe plus de 20 laboratoires sur 5 pôles. Ces laboratoires sont parfois des UMR associés au CNRS, à l'INRA, à l'INRIA et à des universités. Historiquement, ces structures sont gérées de façon autonome y compris au niveau informatique. Une majorité d'Active Directory cohabitent avec des annuaires OpenLDAP ou NIS. Cette situation est compliquée pour l'utilisateur qui va alors posséder plusieurs comptes informatiques suivant ses affections et ses besoins.

La direction de l'INPL a lancé en 2011 un vaste chantier afin d'unifier le SI par un annuaire OpenLDAP et de centraliser la gestion des comptes vers un annuaire Active Directory commun. Une majorité des entités ont déjà rejoint ce référentiel unique même si des écoles souhaitent préserver leur autonomie informatique. Là encore, la topologie s'articule autour d'une forêt et d'un domaine unique, tout en préservant l'autonomie des équipes de sites par un

système de délégation de droits. Par ailleurs, l'INPL dispose d'un serveur de fichier pour centraliser les travaux des étudiants et des chercheurs.

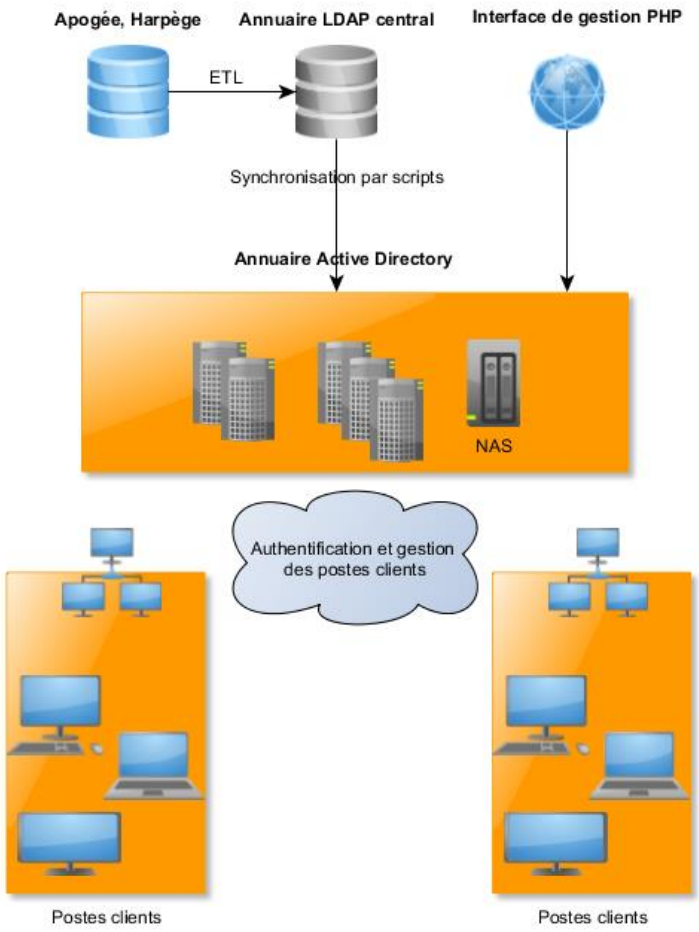


Figure 5 - Le SI àl'INPL

I.2.5 Les usages sur l'UPVM

La situation sur l'Université de Metz est très différente. En effet, les compétences des équipes sont très orientées vers les systèmes Linux et les solutions libres sont privilégiées, bien que le parc informatique soit composé de 80% de systèmes Windows. Par ailleurs, la gestion des comptes est totalement déléguée aux composantes notamment en terme de stockage, l'université ne disposant pas d'un système central.

L'UPVM utilise cependant un annuaire central OpenLDAP qui va exporter toutes les heures les nouveaux comptes sous la forme d'un fichier plat contenant l'identifiant, le nom, le prénom, la formation et le mot de passe crypté vers le serveur distant de la composante. Le traitement est ensuite effectué par script sur le serveur local. La majorité des entités dispose donc d'un annuaire OpenLDAP, autonome mais alimenté par le serveur central, autour duquel

s'architecture un serveur SAMBA permettant de gérer les postes Windows. Bien que stable et performant ce système montre rapidement ses limites sur un parc informatique majoritairement Windows. En effet, les fonctionnalités se rapprochent d'un serveur Windows NT4, sorti en 1996. Enfin, l'administration d'un tel système demande paradoxalement des compétences poussées et freine une délégation fine des tâches.

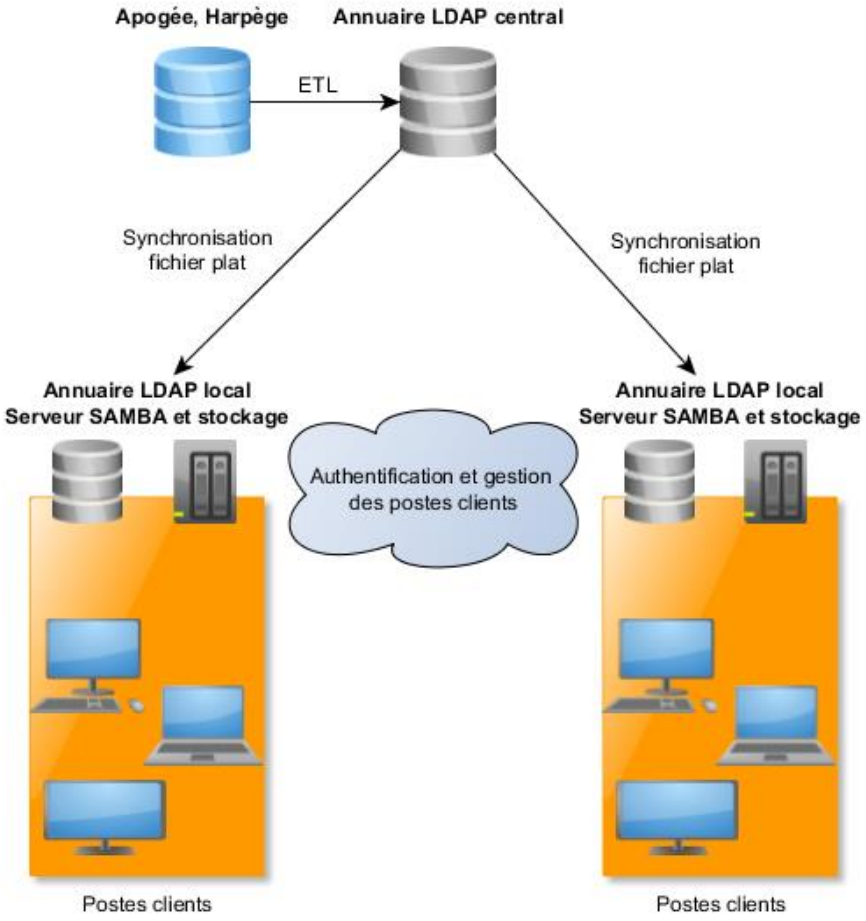


Figure 6 – Le SI à l'UPVM

I.2.6 Active Directory à Metz

Dès 2011 nous avons évoqué la situation informatique de l'Université de Metz avec mon supérieur Olivier Mathieu. De façon officieuse, nous savions qu'un projet commun portant sur l'authentification du poste client allait voir le jour à l'Université de Lorraine en 2012. Par ailleurs, nous savions aussi que les technologies employées sur les autres établissements étaient très différentes des nôtres. De façon réaliste, il nous paraissait peu probable de voir le modèle messin, un annuaire OpenLDAP et SAMBA, se généraliser sur les trois autres structures. A l'inverse, nous présentions des discussions autour du système d'authentification Microsoft, Active Directory, largement utilisé sur la Lorraine.

De plus, sur une trentaine d'informaticiens messins, seulement deux personnes possédaient des compétences sur les serveurs Windows, un collègue de l'IUT de Metz et moi-même. Mon supérieur m'a donc missionné en février 2011 afin de constituer un groupe de travail, visant à :

- Se familiariser avec la technologie Active Directory
- Proposer et maquetter une architecture physique et logique pour le site de Metz et la future université de Lorraine
- Explorer les outils d'administration sous Windows Serveur

Je vais détailler ici la réalisation de cette étude.

I.2.6.1 Réalisation d'une étude Active Directory à Metz

Dès le mois de février 2011, j'ai composé un groupe de travail constitué de 6 personnes de 3 services différents afin de répondre à cette demande. Ce projet s'est effectué en plus des tâches quotidiennes et a nécessité un investissement important, cette technologie étant nouvelle pour la majorité des participants.

J'ai identifié quatre lots autour de ce projet :

- Définir l'arborescence et l'organisation logique du futur annuaire
- Valider l'organisation physique, la disposition des serveurs et l'architecture réseau
- Proposer une maquette fonctionnelle de l'ensemble
- Mettre en place les outils d'administration Microsoft relatifs à la gestion du poste de travail

Les technologies Microsoft étant totalement nouvelles pour quatre des six participants, j'ai décidé que tous les membres du groupe du travail participeraient à l'intégralité des lots spécifiés. Mon objectif était plus la formation des participants plutôt qu'une optimisation du projet.

I.2.6.2 Prévisions des délais et des coûts de l'étude

Les échéances calendaires étaient incertaines au lancement du projet. Nous savions Olivier et moi, que cette étude ne se matérialiserait pas directement sur Metz. En effet, la

Direction du Numérique préparait un projet sur le sujet dès 2012. Dès lors, j'avais moins de contraintes concernant la gestion des délais. Je me suis donc fixé une date butoir pour la fin de l'année 2011. La figure suivante illustre la planification initiale du projet.

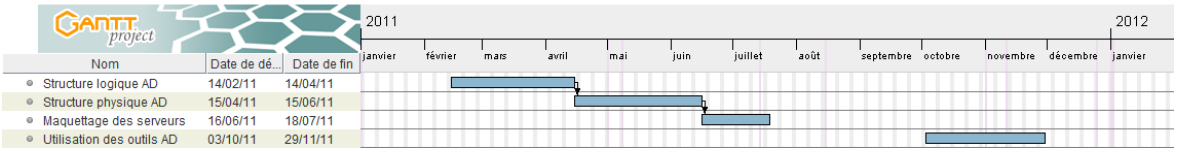


Figure 7 – Délais indicatifs de l'étude

J'ai prévu initialement quatre mois pour l'étude théorique, un mois pour la réalisation de la maquette et deux mois pour la prise en main des outils de gestion. Ces prévisions peuvent paraître exagérées mais je devais intégrer plusieurs paramètres à mon calcul :

- Le travail sur le projet intervient en supplément du travail usuel qui reste prioritaire. Par ailleurs les mois de juin, juillet et septembre sont particulièrement chargés afin de préparer la rentrée universitaire.

- La majorité des participants n'ont jamais utilisé les technologies Microsoft serveur. J'ai donc laissé le temps nécessaire à la formation de chaque intervenant.

Au niveau des coûts, l'estimation était aisée à réaliser. En effet, je dispose d'une infrastructure de serveurs virtualisés que j'ai mise en place fin 2010. L'ajout de plusieurs serveurs de test est donc transparent et ne génère aucun coût supplémentaire. Au niveau des licences Microsoft, j'utilise des licences gratuites « lab » qui permettent de déployer un environnement de développement. Ce projet n'a donc nécessité aucun financement particulier.

I.2.6.3 Présentation de Microsoft Active Directory

L'équipe projet s'est plongée pendant plusieurs mois dans les documentations Microsoft pour se familiariser avec cette nouvelle technologie. Par ailleurs, nous sommes allés aux TechDays 2011 à Paris, afin de discuter avec les ingénieurs Microsoft et connaitre les bonnes pratiques techniques. Nous avons assisté à diverses conférences en matière de gestion et d'authentification du poste client, ce qui a été particulièrement utile pour la suite. Sans entrer dans le détail, il me parait essentiel de présenter le fonctionnement d'Active Directory. Je vais donc m'appuyer sur

des extraits du livre blanc de Microsoft[10], de mes cours à l'université et de la littérature disponible sur Internet[11].

I.2.6.3.1 Objectifs et fonctionnalités

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés ou les imprimantes. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées (Policelli, 2009).

Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 et Samba 4. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ». Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

I.2.6.3.2 Historique et fonctionnement

Active Directory fut présenté pour la première fois en 1996, mais sa première utilisation remonte à Windows 2000 Server en 1999. Il fut mis à jour dans Windows Server 2003 pour étendre ses fonctionnalités et améliorer son administration. Des améliorations supplémentaires lui ont depuis été adjointes dans Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 et Windows Server 2012.

D'un point de vue sémantique, Active Directory est un annuaire LDAP, tout comme l'annuaire d'Exchange 5.5. Exchange 5.5 n'est pas pour autant le seul antécédent technologique à Active Directory, citons également l'annuaire Novell NDS. Active Directory peut donc être

[10] http://technet.microsoft.com/en-us/library/bb727030.aspx
[11] http://fr.wikipedia.org/wiki/Active_Directory

considéré comme la réponse technologique aux technologies d'annuaire Novell, les deux systèmes étant dérivés de X.500.

Active Directory revoit complètement le stockage des informations de sécurité du domaine, de la structure de la base jusqu'au niveau sémantique. Tout d'abord, le moteur de base de données retenu pour sa mise en œuvre est le moteur de stockage extensible ESENT, dérivé de ESE98, également connu sous le nom de Jet Blue. La différence principale entre ESENT et ESE98 est la taille des pages utilisées et la taille des journaux de transaction. Active Directory est également conçu pour garantir un niveau de performance et de sécurité adéquat : la base de données ESENT est journalisée et répond à la contrainte ACID. Le moteur est conçu pour supporter des bases dimensionnées pour stocker des millions d'objets.

I.2.6.3.3 Structure et organisation

Active Directory introduit la notion de hiérarchie, inhérente aux annuaires objets dérivés de X.500, sous la forme d'une arborescence dans laquelle les utilisateurs et les ordinateurs sont organisés en groupes et sous-groupes afin de faciliter l'administration des droits. C'est aussi Active Directory qui gère l'authentification des utilisateurs sur le réseau Windows. Active Directory exploite cette notion de hiérarchie intensivement, puisque l'entité de sécurité appelée « domaine » est également hiérarchisée dans un ensemble partageant un espace de nom commun, appelé « arborescence », enfin, l'entité de plus haut niveau regroupant les arborescences de domaines constitue la forêt Active Directory.

Active Directory permet une réplication multi-maître, c'est-à-dire que chaque contrôleur de domaine peut être le siège de modifications (ajout, modification, suppression) de l'annuaire, sous réserve de permission accordée par ACL, qui seront répliquées sur les autres contrôleurs de domaine. Le mécanisme de réplication de ces modifications peut profiter de RPC (liaisons TCP/IP rapides et disponibles) ou SMTP dans les autres cas. La topologie de réplication est générée automatiquement mais elle peut être personnalisée par l'administrateur, tout comme sa planification.

À noter que les ensembles d'espaces de nom correspondant aux arborescences d'Active Directory formant la forêt Active Directory sont superposables à l'espace de nom formé par les zones DNS. DNS est un service indispensable pour le bon fonctionnement de toute l'architecture Active Directory, la localisation des contrôleurs de domaine, la réplication…

Une arborescence Active Directory est donc composée de :

- La forêt : structure hiérarchique d'un ou plusieurs domaines indépendants (ensemble de tous les sous domaines Active Directory).

- L'arbre ou l'arborescence : domaine de toutes les ramifications. Par exemple, dans l'arbre cnam.fr, paris.cnam.fr, stras.cnam.fr sont des sous-domaines de cnam.fr

- Le domaine : constitue les feuilles de l'arborescence : stras.cnam.fr peut-être un domaine au même titre que cnam.fr. Ces notions sont illustrées ci-dessous :

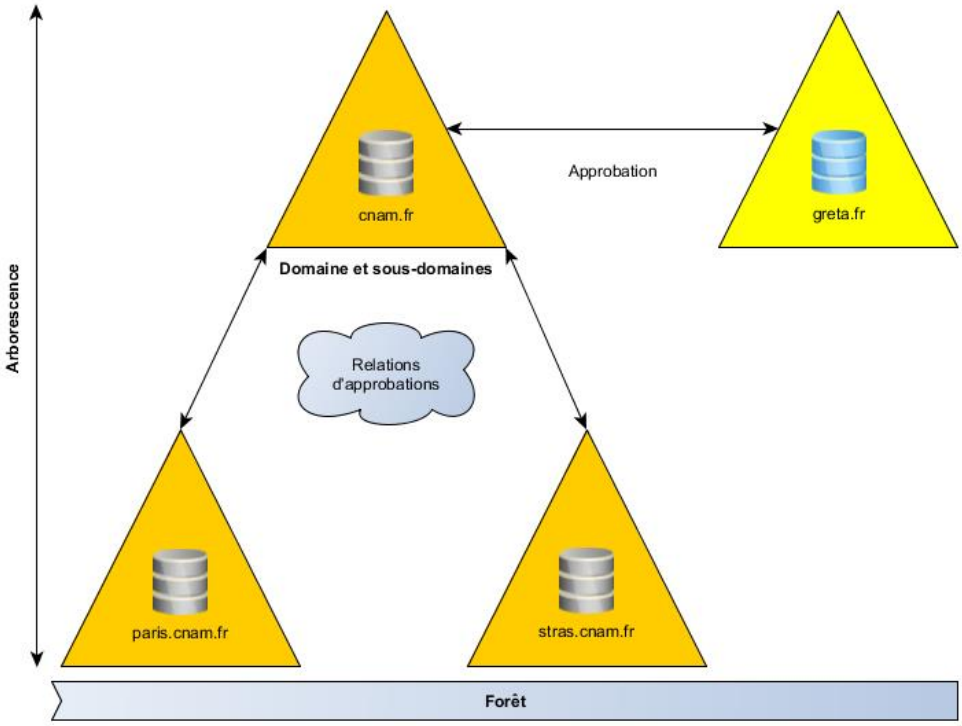


Figure 8 – Forêts et domaines Active Directory

Le modèle de données Active Directory est dérivé du modèle de données de la norme X.500 : l'annuaire contient des objets représentant des éléments de différents types décrits par des attributs. Les objets sont classés en trois grandes catégories : les ressources, par exemple les ordinateurs, les services comme le courrier électronique et afin les utilisateurs. L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

Par ailleurs, un objet est identifié de manière unique dans l'AD par son nom et possède son propre jeu d'attributs : les caractéristiques et les informations que l'objet peut contenir. Ces types d'objets et leurs attributs sont définis par un schéma. Active Directory étant un annuaire objet, la notion de schéma définit les contraintes concernant la dérivation et l'héritage des objets, sensiblement de la même manière qu'en programmation objet. Cela introduit également la notion d'extension, permettant d'ouvrir l'annuaire à toutes sortes d'applications souhaitant

stocker des objets personnalisés au niveau du ou des domaines constituant la forêt Active Directory. Enfin, les stratégies de groupe (GPO) sont des paramètres de configuration appliqués aux ordinateurs ou aux utilisateurs lors de leur initialisation, ils sont également gérés dans Active Directory.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour ajouter, modifier ou supprimer des données.

I.2.6.4 Spécifications de l'architecture logique de l'annuaire

J'ai séparé ici l'architecture logique, l'organisation de l'annuaire et la partie physique, la disposition et la configuration des serveurs.

Il est important de planifier la structure avant de l'implanter. La structure logique s'articule autour de la décomposition de l'entreprise en domaines, arborescences, unités d'organisation. Cette décomposition pourra être guidée par la structure de l'organisation et par les besoins d'administration (délégation, contrôle d'accès, ACL…)

I.2.6.4.1 Architecture de la forêt et du domaine

Je me suis fortement appuyé sur le document de Microsoft : IPD (The Infrastructure Planning and Design) for Active Directory Domaine Services[12]. Ce guide de 50 pages contient une mine d'information sur le sujet et fourni un canevas complet sur la mise en place d'un tel projet. Il détaille non seulement l'ensemble des tâches à mener, leur ordonnancement, le chemin critique du projet ainsi que des informations techniques sur les prérequis matériels et logiciels. J'ai lu ce document plusieurs fois et je l'ai mis en œuvre avec l'équipe jusqu'à obtenir un schéma d'infrastructure que nous avons validé, puis maquetté sur des serveurs physiques.

[12] http://msdn.microsoft.com/en-us/library/cc268216.aspx

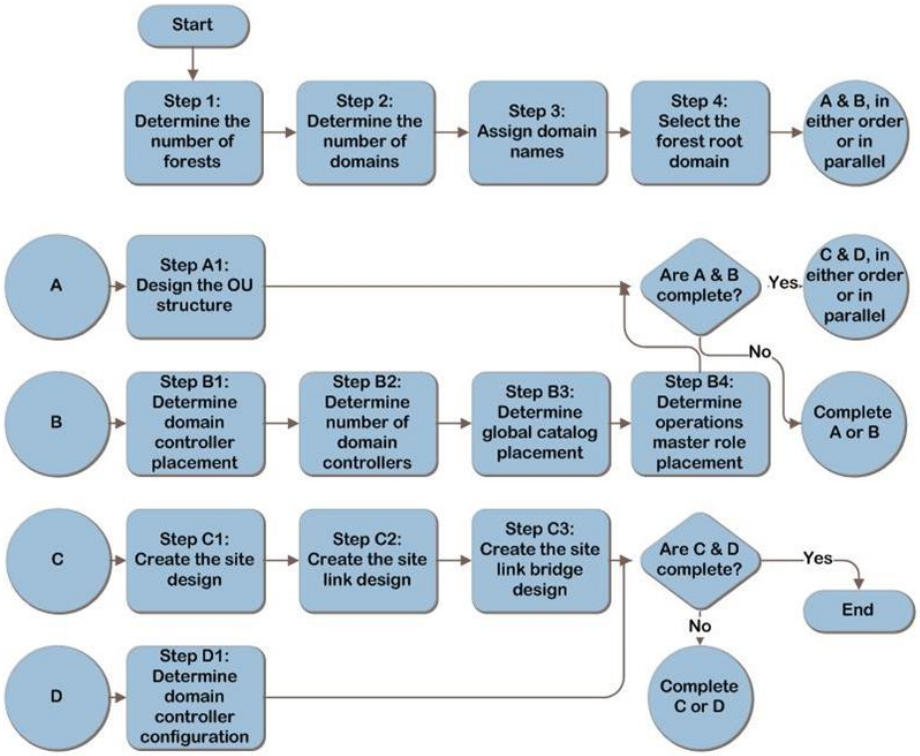


Figure 9 – Extrait de l'IPD Microsoft

La première tâche a été de déterminer le nombre de forêt. La meilleure pratique est de commencer par une seule forêt puis d'éventuellement ajouter des forêts supplémentaires suivant les besoins de l'organisation. Par ailleurs, les autres établissements avaient également fait le choix de partir sur une forêt unique. Enfin, selon l'IPD, gérer une seule forêt est moins complexe et moins couteux en ressources humaines et matérielles qu'une structure basée sur plusieurs forêts. J'ai donc adopté ce choix.

J'ai appliqué cette même démarche sur la création des domaines. Là encore je me suis appuyé sur les bonnes pratiques, le document de Microsoft et les expériences de nos collègues nancéens. Utiliser un seul domaine permet une gestion efficace tout en limitant les coûts matériels et logiciels. Plusieurs domaines sont recommandés afin de limiter les problèmes de réplication quand l'infrastructure réseau est lente ou le nombre d'objets trop important (plus de 100000), ce qui n'est pas notre cas. J'ai donc choisi un domaine unique pour notre étude « univ-metz.local ».

I.2.6.4.2 Création des unités d'organisation

L'étape suivante concerne la création des OU, ou unités d'organisation. Il s'agit d'un objet conteneur de la norme LDAP, qui est utilisé pour hiérarchiser Active Directory. À l'intérieur

des domaines, il existe maintenant des possibilités de structuration et de hiérarchisation des utilisateurs et des données.

Les OU sont le meilleur moyen de créer ces structures hiérarchiques dans Active Directory. Outre la structuration d'informations, qui offre une clarté accrue dans les annuaires complexes notamment, les OU présentent un avantage important : elles tiennent lieu de frontière pour la délégation d'autorisations administratives. Il est donc possible de personnaliser les droits des différents utilisateurs et groupes de façon ciblée afin de proposer une délégation fine.

J'ai donc défini des OU de composantes, calquées sur l'organisation du campus, afin que chaque structure puisse gérer en toute indépendance ses comptes, ses groupes, ses GPO… Un profil d'administrateur d'OU a été défini afin de permettre un libre accès aux objets dont il est responsable. Un administrateur d'OU n'est donc pas obligé d'être administrateur du domaine pour gérer ses entrées. Il a délégation uniquement sur son périmètre sans pouvoir modifier les autres conteneurs de l'annuaire.

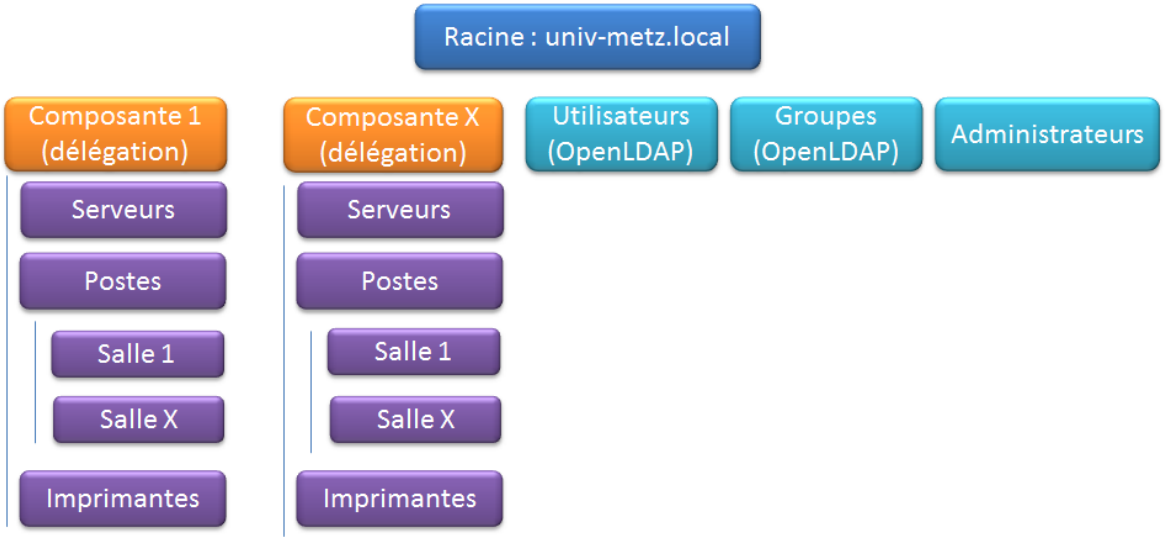


Figure 10 – L'organisation des OU

La version initiale prévoit une OU par structure, ainsi que des OU références comme les utilisateurs et les groupes. L'objectif est ici une alimentation uniquement automatique à partir du référentiel OpenLDAP afin de fournir à toutes les composantes les données nécessaires à la bonne connexion des utilisateurs. Aucun traitement manuel ne doit être effectué sur ces conteneurs afin de refléter la totale synchronisation avec l'annuaire central. Enfin, une OU séparée va contenir les comptes des administrateurs du domaine, afin de renforcer la sécurité du système.

Plusieurs semaines de recherches documentaires ont été nécessaires au groupe de travail afin de pleinement intégrer les spécificités du système d'annuaire Microsoft. Nous avons terminé ce premier lot en mai 2011.

I.2.6.5 Spécification de l'architecture physique

La structure physique d'Active Directory est distincte de sa structure logique. La structure physique permet de gérer et d'optimiser le trafic réseau et la communication entre les machines. Elle se compose de deux éléments : les contrôleurs de domaine et les sites (Apréa, 2008).

Un site est un ensemble de plusieurs réseaux IP reliés entre eux par des liaisons à haut débit. Les liaisons entre sites peuvent être plus lentes ou plus coûteuses. Définir des sites, c'est donner des informations au système qui lui permettront d'optimiser le trafic lié à la duplication entre contrôleurs de domaines et la connexion des utilisateurs.

La notion de site est indépendante de la notion de domaine : un domaine peut contenir plusieurs sites et un site peut contenir plusieurs domaines. Un contrôleur de domaine est un ordinateur sous Windows serveur qui stocke et gère une copie de la base d'Active Directory. Il duplique les modifications de l'annuaire vers les autres contrôleurs. Le processus d'ouverture de session des utilisateurs met forcément en jeu au moins un contrôleur de domaine. Il est donc important que tout utilisateur puisse avoir une liaison rapide et fiable pour se connecter au poste de travail.

Nous avons simplifié cette problématique en utilisant un réseau en étoile : un site central pour le campus messin et plusieurs satellites connectés en haut débit. On peut citer le campus du technopôle à Bridoux, celui de la Lorraine nord et Moselle Est. Nous avons aussi associé plusieurs contrôleurs de domaine sur le site central et un par site distant. Même si une coupure réseau intervient entre le site central et le site distant, les utilisateurs pourront continuer leurs travaux en utilisant le contrôleur de domaine local. Les ordinateurs seront automatiquement connectés au nœud le plus proche suivant leur adresse IP.

Par ailleurs, il faut maîtriser le fonctionnement de la réplication entre contrôleurs de domaine et les rôles des maîtres d'opérations. Les contrôleurs de domaines sont globalement tous équivalents et hébergent une copie des informations de la base d'annuaire accessible en lecture et écriture. La base est dupliquée et distribuée sur chaque contrôleur de domaine d'où le terme de réplication multi-maître. Les opérations habituelles, telles que les créations de comptes

ou les changements de mot de passe, peuvent être réalisées sur n'importe quel contrôleur du domaine. Si des modifications incompatibles sont réalisées sur des contrôleurs à un moment où ils sont coupés du réseau, seule l'une de ces modifications sera prise en compte.

I.2.6.5.1 Architecture physique : les maîtres d'opérations

Active Directory a été conçu pour limiter au maximum cette problématique de « split-brain ». Certaines opérations critiques sont donc prises en charge par une seule machine. Pour ces cas de figure, on retrouve un fonctionnement en maître unique bien qu'une copie en lecture soit accessible par les autres contrôleurs. Les ordinateurs réalisant ces opérations critiques sont appelés des maîtres d'opérations ou FSMO (Flexible Single Master Operation) :

- Maître de schéma : un par forêt. Il gère les modifications sur le schéma d'annuaire.

- Maître d'attribution de nom de domaine : un par forêt. Il permet d'ajouter ou retirer un domaine de la forêt et les objets de référence croisés avec les annuaires externes.

- Maître émulateur PDC : un par domaine. Il assure quatre fonctions et son bon fonctionnement est donc crucial pour chaque domaine de la forêt. En effet, il permet la compatibilité avec les anciens contrôleurs de domaine du type Windows NT. De plus, il gère les changements des mots de passe des utilisateurs, le verrouillage des comptes et les mécanismes de synchronisation horaire sur tous les contrôleurs du domaine. Enfin, il réalise les modifications de stratégie de groupe afin d'interdire toute possibilité d'effacement et conflit.

- Maître des identifiants relatifs (RID) : un par domaine. Il distribue des paquets d'identificateurs relatifs aux contrôleurs de domaine. Les contrôleurs de domaines peuvent ainsi utiliser ces identifiants relatifs lors de la création des principaux objets de sécurité (utilisateurs, groupes ou ordinateurs). Quand un contrôleur de domaine a épuisé son stock d'identifiants relatifs, il doit contacter le maître RID pour en obtenir de nouveaux.

- Maître d'infrastructure : un par domaine. Quand un utilisateur et un groupe sont dans deux domaines différents, le changement de nom de l'utilisateur n'est pas pris en compte tout de suite au niveau du groupe. Le maître d'infrastructure est responsable de la référence inter-domaine de façon à mettre à jour le nom de l'objet là où il est utilisé dans les autres domaines. Le maître d'infrastructure

compare ses données à celles du serveur de catalogue global. Les deux rôles ne doivent pas être assurés par le même ordinateur. En cas d'indisponibilité du maître d'infrastructure, les mises à jour seront retardées.

En cas de défaillance d'un rôle, il est possible de transférer le rôle à un contrôleur existant. Pour éviter les pertes d'informations, il est utile de repérer les contrôleurs de domaines qui sont partenaires de réplication de chaque maître d'opération. En tant que partenaire direct, ces ordinateurs auront la base de données la plus à jour possible et sont des remplaçants idéaux. Le tableau ci-dessous récapitule les rôles FSMO :

	Description	Niveau
Maître de schéma	Mise à jour du schéma	Forêt
Maître d'attribution de nom de domaine	Ajout/suppression de domaine Renommage de domaine	Forêt
Maître émulateur PDC	Prise en charge des serveurs et client NT Réplication des modifications des mots de passe Gestion des erreurs d'authentification Serveur de temps	Domaine
Maître des identifiants relatifs	Distribution des plages RID	Domaine
Maître d'infrastructure	Mise à jour et réplication des objets inter-domaines	Domaine

Tableau 1 – Présentation des rôles FSMO

J'ai suivi les recommandations Microsoft concernant le placement des maîtres d'opérations. J'ai séparé les cinq rôles sur deux serveurs différents situés sur le site central afin d'assurer la montée en charge des connexions et la haute disponibilité de l'infrastructure. Un serveur assure les rôles de maître de schéma et de nom de domaine, tandis que l'autre assure les trois autres rôles. Cette disposition évite un point de défaillance unique si les rôles étaient concentrés sur le même serveur.

I.2.6.5.2 Le rôle du catalogue global

Un annuaire Active Directory a besoin d'une somme d'éléments essentiels pour assurer sa bonne marche au sein d'un environnement de production. Nous avons les maîtres d'opérations

qui assurent des tâches spécifiques, mais également le catalogue global (GC) que nous allons présenter.

Un serveur de catalogue global est un contrôleur de domaine possédant une copie en lecture seule des attributs les plus utilisés de tous les objets de la forêt. Le premier contrôleur de la forêt est serveur de catalogue global. Les administrateurs de domaines peuvent transformer n'importe quel contrôleur de domaine en serveur de catalogue global. Le serveur de catalogue global va être utilisé pour des recherches à l'échelle de la forêt.

Il est conseillé d'avoir un serveur de catalogue global par site pour optimiser la bande passante et d'avoir un serveur de catalogue global par domaine. Le serveur de catalogue global est consulté pendant l'ouverture de session des utilisateurs. Il fournit les informations sur l'appartenance de l'utilisateur à des groupes universels nécessaires à la création du jeton de sécurité de l'utilisateur.

Là encore, j'ai suivi les conseils du document officiel de Microsoft dans l'optique d'un domaine unique. Celui-ci conseille que tous les contrôleurs de domaine soient configurés comme catalogue global, y compris la machine ayant le rôle de maître d'infrastructure. Dans un scénario impliquant plusieurs domaines, cette pratique est à bannir.

A l'image de la partie précédente, un important travail documentaire a été réalisé afin de proposer une solution viable en juin 2011.

I.2.6.6 Synthèse et maquettage

Avec toutes ces informations, j'ai pu éditer le schéma de l'infrastructure cible. J'ai aussi rajouté différents éléments comme l'intégration du service DNS, DHCP et WSUS ainsi que l'ajout d'un stockage central, projet lancé en 2011 à l'université de Metz.

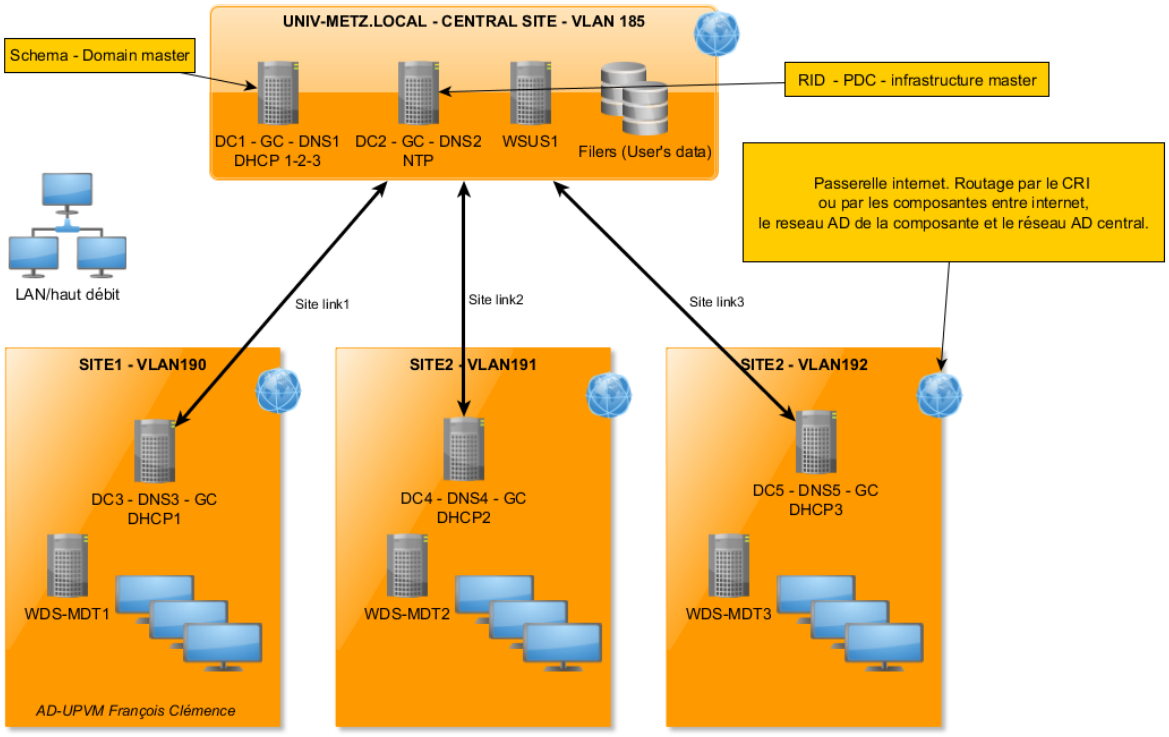


Figure 11 – Schéma Active Directory UPVM

Ce schéma a été validé par mon supérieur courant 2011 et nous sommes ensuite passés au maquettage de la solution. L'objectif principal de cette tâche était de simuler le fonctionnement du site central et d'un site satellite et de valider la communication et la réplication entre les serveurs. Cette base a ensuite été utilisée pour se familiariser avec les outils de gestion de l'annuaire comme les GPO.

J'ai donc utilisé notre plateforme vSphere pour virtualiser l'environnement du site central. J'ai créé plusieurs machines virtuelles que j'ai utilisées comme contrôleurs de domaine pour construire le domaine « univ-metz.local ». J'ai paramétré les rôles FSMO et le catalogue global conformément au schéma initial. En parallèle, j'ai configuré les sites et les liens de sites dans l'interface d'administration. A côté, mes collègues ont mis en place deux autres sites, chacun doté d'un contrôleur de domaine, simulant ainsi la topologie en étoile. L'équipe a intégré les machines dans le domaine initial puis a vérifié la bonne configuration de la réplication et des sites.

Nous avons ensuite paramétré la structure logique et configuré les différentes OU, sur lesquelles nous avons appliqué des délégations de droits. L'équipe s'est ainsi familiarisée avec la gestion des objets de l'annuaire. De son coté, Olivier Mathieu a configuré la synchronisation de l'annuaire OpenLDAP vers Active Directory en utilisant un script Perl qui va alimenter à intervalles réguliers la base Microsoft. Nous avons validé cette étape importante fin juillet 2011.

I.2.6.7 Outils d'administration et GPO

Après avoir construit la structure physique et logique de l'annuaire, nous nous sommes intéressés aux outils de gestion du poste de travail, fournis par Microsoft. Il s'agit en particulier des stratégies de groupe (GPO pour Group Policy Object). Ce sont des fonctions de gestion centralisée de la famille Microsoft Windows qui permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.

Les stratégies de groupe peuvent contrôler des clés de registre, la sécurité NTFS, la politique de sécurité et d'audit, l'installation de logiciel, les scripts de connexion et de déconnexion, la redirection des dossiers et les paramètres d'Internet Explorer. Les paramétrages sont stockés dans les stratégies de groupe. Chaque stratégie de groupe possède un identifiant unique appelé GUID (« Globally Unique Identifier »). Chaque stratégie de groupe peut être liée à un ou plusieurs domaines, site ou unité d'organisation. Cela permet à plusieurs objets ordinateurs ou utilisateurs d'être contrôlés par une seule stratégie de groupe et donc de diminuer le coût d'administration globale de ces éléments.

Les stratégies de groupe utilisent des fichiers de modèle d'administration avec les extensions .ADM ou .ADMX qui décrivent les clés de registre modifiées par l'application des stratégies de groupe. Sur un ordinateur de travail, les modèles d'administration sont stockés dans le répertoire %WinDir%\Inf, alors que sur un contrôleur de domaine Active Directory, ils sont stockés dans un répertoire individuel, le « group policy template » ou GPT, au sein du répertoire Sysvol. Les fichiers .ADMX sont des fichiers basés sur le format XML et introduits par Windows Vista pour la gestion des stratégies de groupe.

Les stratégies de groupe sont analysées et appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les ordinateurs rafraîchissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120 minutes, ce paramètre étant ajustable (Svidergol & Allen, 2013).

I.2.6.7.1 Création des GPO

Les stratégies de groupe peuvent être éditées avec deux outils – le Group Policy Object Editor (Gpedit.msc) et la Group Policy Management Console (gpmc.msc). Gpedit est utilisé pour créer et éditer une stratégie de groupe de façon unitaire. La GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil permettant une gestion centralisée et collective des objets. La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de

sauvegarde et de restauration et d'autres outils graphiques intégrés à la MMC. Le nom d'une stratégie de groupe peut être déterminé en utilisant l'outil GPOTool.exe.

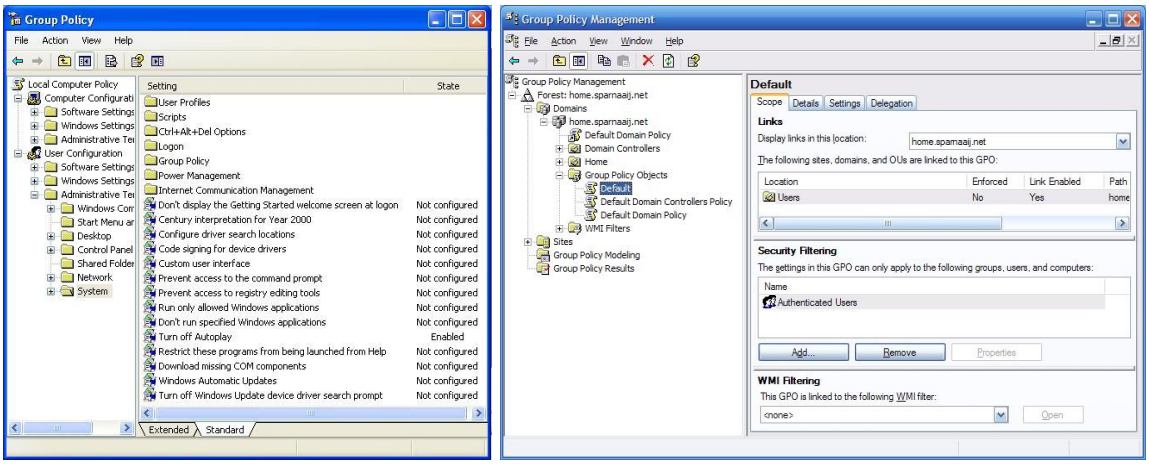


Figure 12 – Aperçu de la configuration des GPO

Après avoir créé une stratégie de groupe, elle peut être liée à un site Active Directory, à un domaine ou à une unité d'organisation (OU).

Le client de stratégie de groupe du poste récupère la configuration dans un intervalle aléatoire compris entre 60 et 120 minutes. Elle est ensuite appliquée en tenant compte des différents critères de sécurité et d'affectation.

I.2.6.7.2 Stratégies utilisées

Après avoir approfondi les documentations Microsoft, j'ai créé trois catégories de GPO afin de gérer plus efficacement le poste de travail : le paramétrage de l'environnement utilisateur, les redirections de documents, le réseau et la configuration système.

J'ai créé plusieurs GPO pour améliorer l'expérience de l'utilisateur. Tout d'abord, j'ai amélioré la sécurité en effaçant le dernier utilisateur connecté lors du choix de la session. Par ailleurs, j'ai désactivé le changement de mot de passe afin de ne pas créer de distorsion entre le SI et le compte de l'usager. Enfin, nous avons monté les différents lecteurs réseaux nécessaires, qu'il s'agisse du répertoire personnel ou de partages communs.

Concernant les données de l'utilisateur, l'objectif était de ne garder aucun document de travail sur la machine. En effet, nos utilisateurs sont itinérants et stocker leurs documents sur une machine unique n'est pas adapté. J'ai donc utilisé le système de redirection, afin que les fichiers de nos utilisateurs soient directement stockés dans un répertoire réseau distant. Ainsi, les fichiers

du « bureau », « mes documents » et les « favoris » accompagnent l'usager dans ses déplacements.

Nous avons enfin validé des stratégies pour renforcer la sécurité des postes clients. Nous avons positionné des ACL sur les partitions du disque dur, afin d'interdire le dépôt sauvage de documents. Nous avons également paramétré l'utilisation du proxy sur le poste client et les fichiers hors connexion. Enfin, nous avons configuré les interactions avec notre infrastructure comme le serveur WSUS de mise à jour et le serveur antivirus.

Nous avons mené cette étape d'octobre à décembre 2011.

I.2.6.8 Bilan et fin de l'étude

J'ai mené ce projet pendant 8 mois avec mes collaborateurs. L'étude s'est terminée en décembre 2011 et nous avons respecté les objectifs initiaux. En partant de zéro, nous nous sommes tous formés à une nouvelle technologie. En suivant les bonnes pratiques, j'ai proposé une maquette pour l'université de Metz en vue d'une intégration à l'Université de Lorraine. Cette étape a demandé beaucoup d'investissement en plus du travail quotidien.

Enfin nous avons maquetté une partie de la solution à l'aide de la virtualisation de serveurs puis nous avons appliqué les concepts théoriques à la pratique, tout en suivant les recommandations du domaine. Cette étape a demandé un travail en équipe efficace afin de valider ensemble le bon fonctionnement de l'architecture. Par ailleurs, mes collègues ont découvert les stratégies de groupe et la gestion Microsoft du poste de travail. Pour avoir travaillé uniquement sur des serveurs Linux, mes collaborateurs étaient sceptiques au départ, mais ils ont finalement reconnu la puissance d'une telle solution face aux produits libres comme Samba.

Quant à moi, cette étude a été une réussite et une grande satisfaction. Au niveau technique, j'ai pu approfondir mes connaissances Microsoft et les mettre en œuvre dans un projet d'envergure. En effet, lors de mon précédent poste à Besançon, j'avais mis en place une infrastructure basique pour une centaine d'étudiants. Le passage à l'échelle, près de 50000 étudiants et des dizaines de structures, m'a permis de renforcer mes acquis. Au niveau humain, j'ai apprécié de pouvoir travailler avec des collègues d'autres composantes et des services centraux.

Pour conclure, cette étude était stratégique pour l'Université de Metz. En effet, nous étions en retrait au regard de l'utilisation des technologies Microsoft sur le campus. Or elles sont

utilisées depuis plusieurs années dans les 3 autres établissements. Il était donc important pour nous de mener une étude sur le sujet afin de préparer le changement qui s'annonçait.

I.2.7 Lancement du projet commun

Le tableau ci-dessous permet d'évaluer rapidement la situation des différents établissements avant la fusion, en matière d'authentification et de gestion du poste de travail. J'ai listé plusieurs critères qui me paraissent importants :

- Nombre d'annuaires : indique le nombre d'annuaires en production utilisés pour gérer les postes clients sur le campus. Cette information ne prend pas en compte les structures autonomes, comme certaines écoles d'ingénieurs.

- Pilotage central : il représente le degré de centralisation de l'infrastructure d'authentification. Le site de Nancy 2 dispose de 5 serveurs centraux, à l'opposé de Metz, où chaque entité dispose de son serveur propre. Entre les deux, l'UHP et l'INPL dispose non seulement de serveurs administrés en central mais aussi de machines gérées de façon autonome dans les composantes.

- Autonomie des sites : représente le degré de liberté des équipes locales, gérant les UFR, IUT ou services communs. Les équipes messines disposent d'un large degré d'autonomie puisqu'elles gèrent les comptes et les problématiques relatives au stockage des données.

- Stockage central : indique la présence d'un dispositif de stockage réseau commun sur l'établissement (NAS/SAN)

- Synchronisation des comptes : renseigne la fréquence à laquelle le dispositif d'authentification du poste client est synchronisé au SI de l'établissement.

	Technologie	Nombre d'annuaires	Pilotage central	Autonomie des sites	Stockage central	Synchronisation des comptes
Nancy 2	Active Directory	1	+++	+	OUI	En continu
UHP	Active Directory	2	++	++	OUI	En continu
INPL	Active Directory	1	++	++	OUI	En continu

UPVM	OpenLDAP Samba	1 par structure	+	+++	NON	Chaque heure

Figure 13 – Résumé des SI des établissements

D'après ce tableau, on remarque que les technologies et les usages sont relativement similaires dans les établissements, sauf sur le site de Metz ou l'écart est très important que ce soit au niveau des technologies ou des compétences. Les systèmes utilisés proviennent du monde libre et se basent sur des serveurs Linux. De ce fait, les compétences sur les systèmes Windows sont peu répandues sur Metz. Par ailleurs, les informaticiens messins travaillent en autonomie et développent des solutions, parfois redondantes, dans chaque composante. Le projet d'une solution unique représente donc un défi de taille, malgré l'étude Active Directory menée au préalable.

Cette première réunion a permis aux participants de connaître en détail la situation des 4 établissements de l'Université de Lorraine. La nécessité d'un dispositif commun dans le domaine se positionne de façon évidente. D'un point de vue technologie, 3 établissements sur 4 utilisent un annuaire Microsoft et disposent d'une expérience de plusieurs années. La décision a donc été prise à l'unanimité par le groupe de travail : la mise en place d'un annuaire Active Directory pour l'ensemble de la Lorraine et de ses établissements.

I.3 Le projet Active Directory Lorrain

Le projet a été annoncé officiellement aux informaticiens de l'UL en février 2012, suite à la seconde réunion du groupe de travail.

I.3.1 Analyse des besoins et objectifs

La réunion des quatre ex-universités en une seule conduit à la fusion obligatoire de l'ensemble des bases et des annuaires existants. Dans ce cadre, la fusion des Active Directory est une obligation. Cette fusion doit conserver les fonctionnalités des AD existants et doit permettre le rattachement des composantes qui le souhaitent. Ce changement d'échelle amène une réflexion sur l'administration de cette nouvelle structure dans le respect d'une certaine autonomie des sites qui la composent.

L'AD UL se compose d'une partie globale qui concerne les utilisateurs institutionnels (étudiants et personnels) ainsi que les groupes institutionnels nécessaires à son bon

fonctionnement ainsi que les sites (campus, composantes, services, …) qui se raccordent à la structure AD.

La partie globale est alimentée automatiquement par le SI pour la partie « comptes » et aucune modification ne doit être faite « manuellement ». Elle contient aussi la stratégie globale et le paramétrage au travers notamment des GPO positionnées par les administrateurs de l'AD. Elle est le garant du bon fonctionnement de l'annuaire.

Par contre, les sites raccordés doivent disposer d'une autonomie de gestion nécessaire à la fourniture des services à leurs utilisateurs. Tous les sites n'ont pas les mêmes besoins et ne fournissent pas obligatoirement les mêmes services. Pour déléguer cette autonomie en toute sécurité aux sites, il est possible de le faire au travers d'outils qui fiabilisent les modifications.

La conduite de ce projet ainsi que la mise en place et l'administration de la solution AD UL incombe à la sous-direction Services aux Usagers via un groupe de travail.

I.3.2 Formation du groupe de travail et premières propositions

Eric Sand a consolidé le groupe de travail en rassemblant les personnes volontaires de chaque établissement et possédant des connaissances dans le domaine. Au total, 13 personnes constituent le groupe de travail dont 3 personnes pour Metz (Olivier Mathieu, Eric Sénet et moi). Tous les établissements sont représentés. Un tel projet d'établissement nécessite des ressources importantes mais il faut qu'il reste gérable.

Cette première réunion a également été l'occasion de faire un tour de table technique et de demander à chaque établissement comment il voyait le futur annuaire commun. Le site de Metz a donc proposé une première ébauche du projet. Je me suis chargé de cette tâche en m'appuyant sur mon étude précédente, tout en tenant compte du passage à l'échelle :

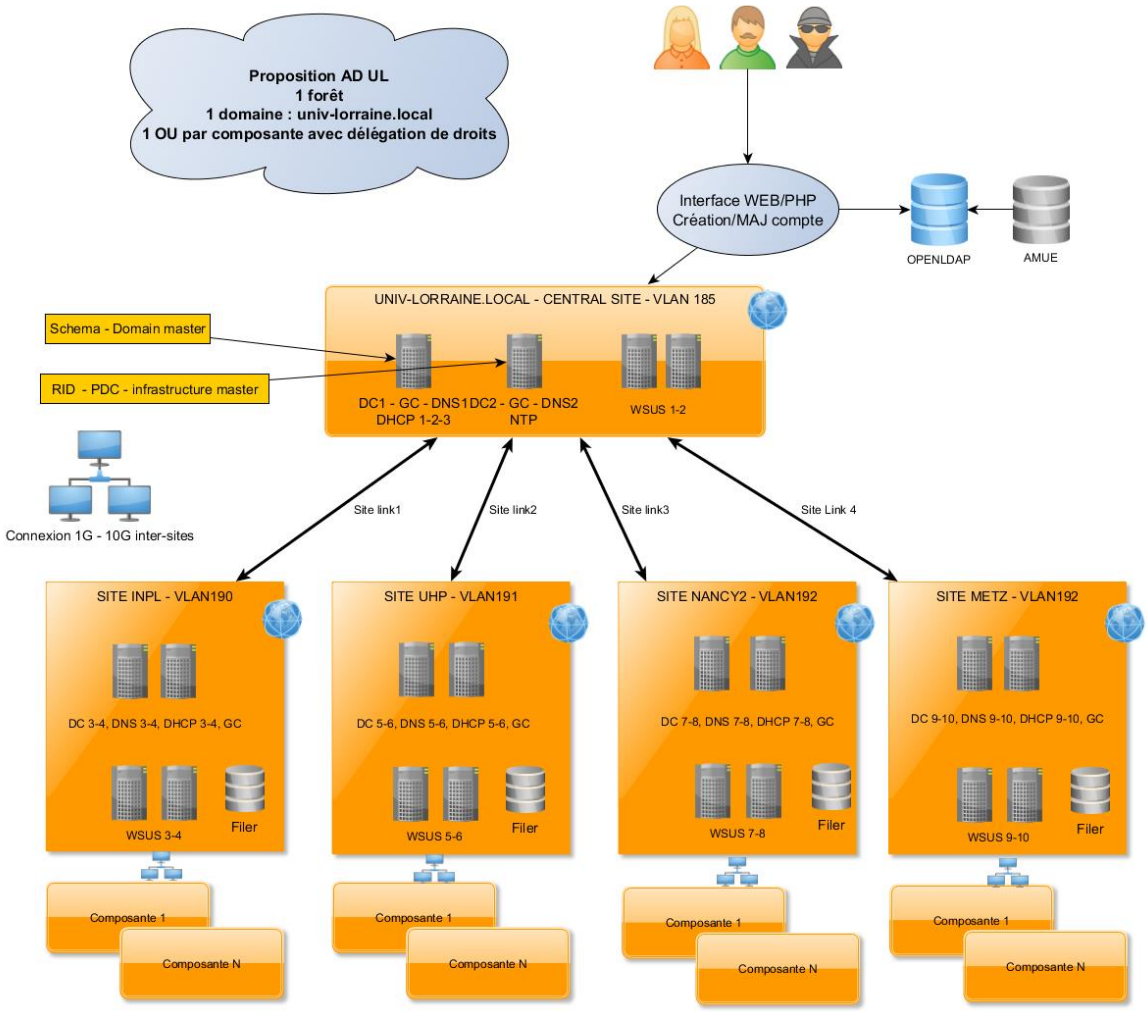


Figure 14 - Proposition d'une architecture AD UL

Les comptes provenant des logiciels de l'AMUE sont extraits et injectés dans l'annuaire central OpenLDAP. Cet annuaire central va ensuite alimenter l'annuaire Microsoft par des scripts et des requêtes LDAP. Ce dispositif est complété par une interface Web qui va permettre aux étudiants d'initialiser leur compte et de positionner leur mot de passe à la fois dans l'annuaire OpenLDAP et dans l'annuaire Microsoft. Cette interface doit également gérer le changement de mot de passe.

L'architecture physique est ensuite similaire à ce que j'ai développé pour l'étude messine : un site central hébergeant les contrôleurs de domaine possédant les rôles FSMO, puis des satellites liés aux anciens établissements. Chaque site peut héberger lui aussi un ou plusieurs contrôleurs de domaine, tous configurés en tant que catalogue global. Enfin, des systèmes de stockage réseau (NAS/SAN) renforcent le dispositif ainsi que divers serveurs d'infrastructure Microsoft (DHCP, WSUS).

Nos autres collègues nancéiens ont également proposé une approche similaire et un consensus s'est formé sur la possibilité d'une forêt et d'un domaine unique pour l'Université de Lorraine.

I.3.3 Découpage et lotissement du projet

Le groupe de travail s'est réuni début mars afin d'établir la plan de management du projet, de lister les lots et les tâches, les référents et le planning. Nous avons effectué ensemble un brainstorming autour du projet, puis Eric Sand a classé ces idées en lots et tâches que nous avons ensuite commentés et complétés.

Sept lots ont été identifiés, chacun piloté par une équipe projet. Ces équipes sont constituées de volontaires appartenant au groupe de travail principal :

- Les besoins fonctionnels du nouvel annuaire
- L'alimentation automatique de l'Active Directory
- L'alimentation manuelle de l'AD
- La structure logique de l'annuaire
- La structure physique
- L'interface d'administration Web
- La mise en place

A titre personnel, j'ai participé à la définition des besoins fonctionnels, à la structure logique, à la structure physique et à la mise en place de la solution. Un extrait de l'organigramme du projet est indiqué en annexe 1.

I.3.4 Les besoins fonctionnels du nouvel annuaire

L'objectif est de mettre à disposition des composantes pour le 15 juin 2012 (date cible) et au maximum pour le 1er Juillet 2012 (date limite) :

- Un annuaire Active Directory fonctionnel avec une structure logique et physique.
- Un outil d'administration afin que chaque informaticien puisse gérer de façon simple et efficace les objets de sa structure.

- Des règles d'usage et de nommage, afin d'éviter les mauvaises pratiques, les doublons et les objets orphelins.

- Les explications et/ou formations nécessaires. En particulier, la plateforme collaborative Wikidocs sera utilisée pour centraliser la documentation et les explications concernant le système en place.

- Les comptes étudiants provenant de l'annuaire OpenLDAP central. Ils devront être déversés en priorité afin d'assurer la rentrée 2012/2013.

Les informaticiens des structures doivent pour assurer :

- L'authentification des utilisateurs :

    - Pour un poste joint au domaine

    - Pour des postes mac, linux, (sfu, pam_smb, winbind)

    - Avec la possibilité de monter un partage réseau « en tant que ».

- Une authentification radius, utilisée notamment à Nancy 2

- Le parcours de l'annuaire avec des requêtes simples au format LDAP.

- Le lien avec les espaces de stockage des personnels et des étudiants, afin que chaque utilisateur puisse retrouver ses documents de façon transparente.

- Une gestion locale déléguée avec la mise en place d'OU et d'un profil d'administration.

- La mise en œuvre de GPO directement au sein de la composante, sans passer par le niveau central.

Par ailleurs, il nous paraissait également essentiel d'indiquer les objets qui seront présents dans cet annuaire :

- Tous les personnels de l'UL (6700 personnes).

- Tous les étudiants de l'UL (53000 étudiants).

- Certains tiers (ex : personnels hébergés, lecteurs autorisés de BU).

- Des postes de travail (Windows version > XP SP3, Mac, Linux), installés nativement en français ou anglais. Pour les postes de travail dont l'utilisateur est administrateur du poste, les règles d'intégration dans le SI UL (réseau, AD …) et les services offerts doivent être définis, afin de ne pas compromettre la sécurité de l'ensemble.

- Des serveurs de version minima Windows 2003.

Nous avons aussi qualifié ce qui ne sera pas dans cet annuaire :

- Des postes de travails dont la version de Windows est inférieure à XP SP3.

- Des postes de travail installés nativement dans une langue autre que le français ou l'anglais qui posent soucis pour les GPO et n'ont pas vocation à entrer dans l'AD.

- Les imprimantes, leur gestion se faisant sur des serveurs membres du domaine.

- Des serveurs de version Windows inférieure à 2003.

I.3.5 Alimentation automatique de l'AD

L'objectif de ce lot est de définir la procédure de synchronisation entre l'annuaire OpenLDAP et l'annuaire Active Directory. Il est en effet essentiel qu'un nouvel utilisateur déclaré dans la base de données des étudiants ou des personnels dispose le plus rapidement possible d'un accès informatique. Cette opération automatique est réalisée à l'aide d'un script PERL qui fait office d'ETL.

Le groupe de travail a également défini les critères relatifs à l'ajout, la modification et à la suppression d'un compte dans l'annuaire Microsoft. La première règle de gestion concerne l'ajout d'une entrée. L'objectif est ici un ajout au plus tôt, dès que les informations minimales sont renseignées dans la base Apogée ou Harpège et ce quel que soit l'état administratif du dossier. Cette mesure permet en particulier aux étudiants en attente de paiement de disposer d'un compte informatique afin d'assister aux enseignements.

Quant aux opérations de mise à jour des entrées, la synchronisation entre l'annuaire central et l'annuaire Microsoft est programmée une fois par jour, pendant la nuit. En effet, il s'agit d'une opération lourde puisqu'il faut parcourir l'intégralité de l'annuaire et vérifier les différences. Par ailleurs, cette opération est moins critique que la création des nouveaux comptes.

La suppression d'un compte passe par un champ « date d'expiration du compte » dans l'annuaire central. Le compte est tout d'abord désactivé puis automatiquement supprimé après un délai adapté à chaque population, par exemple 6 mois pour les étudiants. Ce mécanisme a pour objectif de se prémunir d'une suppression brutale dans l'AD, comptes qui sont par la suite extrêmement couteux à remonter.

De plus, cette étape a pour objectif de ventiler les utilisateurs dans les groupes appropriés, afin d'affecter les bonnes ressources. Les groupes générés automatiquement ne peuvent être modifiés manuellement.

Les étudiants sont affectés dans les groupes suivants :

- Un groupe « Etudiants » qui rassemble tous les étudiants de l'Université de Lorraine
- Un groupe par Diplôme
- Un groupe par étape d'un diplôme
- Un groupe par composante
- Un groupe par serveur de stockage

Quant aux personnels, ils sont ventilés dans les groupes suivants :

- Un groupe « personnels »
- Un groupe par Business Catégorie ou groupe de BC
- Un groupe par serveur de stockage
- Un groupe par structure (composante, laboratoire)

Cette alimentation est réalisée automatiquement par un script PERL situé sur un serveur dédié et qui va s'exécuter à intervalles réguliers. Ce script à le même rôle qu'un ETL et fait la correspondance entre les champs de l'annuaire OpenLDAP et celui de l'Active Directory.

I.3.6 Alimentation manuelle

Toutes les personnes qui sont entrées dans Harpège ou Apogée ont un compte informatique créé automatiquement. Bien que cette procédure couvre les étudiants, les enseignants et les personnels, qu'en est-il des intervenants extérieurs ou des invités ?

L'objectif de ce lot est donc de définir les critères liés à une alimentation manuelle de l'annuaire Microsoft, en parallèle des scripts d'alimentation automatiques. Nous avons envisagé la création de comptes provisoires individuels, des comptes de test et des comptes de service.

Les comptes provisoires :

- Ils sont réservés à des extérieurs.
- ils sont nominatifs (nom, prénom, date de naissance).
- ils sont provisoires (maximum une année universitaire).

Ils permettent :

- D'ouvrir une session sur certains ordinateurs en libre accès.
- De bénéficier, si nécessaire, d'un espace de stockage.

De plus, pour éviter toute confusion, les identifiants doivent avoir une construction différente de ceux des personnels ou des élèves inscrits. Ces comptes sont activés sur un portail qui permet aux utilisateurs de signer la charte informatique. Ils sont utilisés pour des élèves extérieurs (CNAM, formation continue…) qui doivent suivre des cours dans les salles informatiques mais aussi pour les auditeurs de la BU. Dans le cas de comptes génériques (CNAM 01, CNAM02…) il faut impérativement prévoir un tableau papier qui permet à l'enseignant d'associer un compte à une personne et lui faire signer la charte informatique.

Enfin, les comptes de test permettent de faire des tests de script ou de vérifier les droits d'un groupe particulier. Ils doivent être associés à l'informaticien qui l'a créé et qui est seul à l'utiliser. De la même façon, les comptes de service ou applicatif permettent à un logiciel d'accéder à des ressources qui nécessitent une authentification.

I.3.7 Structure logique de l'AD

La structure logique de l'annuaire va permettre d'organiser les ressources de façon hiérarchique en respectant au mieux l'organisation de l'entreprise. Cette étape passe par la définition des forêts, des domaines, de l'arborescence et des unités d'organisation. Par ailleurs, le groupe de travail a aussi précisé les règles de nommage des objets.

Un important travail de réflexion a été mené pour déterminer les paramètres les plus adaptés au futur annuaire de l'Université de Lorraine. La principale question portait sur la

détermination du nombre de forêts et de domaines. Le groupe de travail s'est appuyé sur les bonnes pratiques publiées par Microsoft et les recherches empiriques de chaque participant. Un tableau récapitulatif permet de synthétiser les différentes hypothèses :

	Forêt unique	Plusieurs forêts	Domaine unique	Plusieurs domaines
Complexité	+	+++	+	+++
Coût	+	+++	+	+++
Sécurité	+	++	+	++

Tableau 2 – Résumé relatif aux forêts et domaines

Le scénario d'une seule forêt et d'un seul domaine avait clairement les faveurs du groupe de travail. Il facilite l'administration de l'annuaire tout en réduisant les coûts matériels et humains. Au niveau de la sécurité, le passage à plusieurs forêts et plusieurs domaines ne compense pas la lourdeur de la solution et n'offre que de modestes améliorations. Ce scénario s'est dessiné dès notre première réunion de travail.

L'AD s'articulera donc autour d'une seule forêt et d'un seul domaine « ad.univ-lorraine.fr ». Il contiendra tous les personnels et les étudiants de l'Université de Lorraine. Les objets sont créés dans une OU spécifique : l'OU UL, afin de faciliter la lecture de l'arborescence. Tous les comptes utilisateurs institutionnels (personnels, étudiants) sont alimentés automatiquement et créés dans l'OU UL

I.3.7.1 Arborescence

L'arborescence de l'annuaire est définie comme ci-dessous :

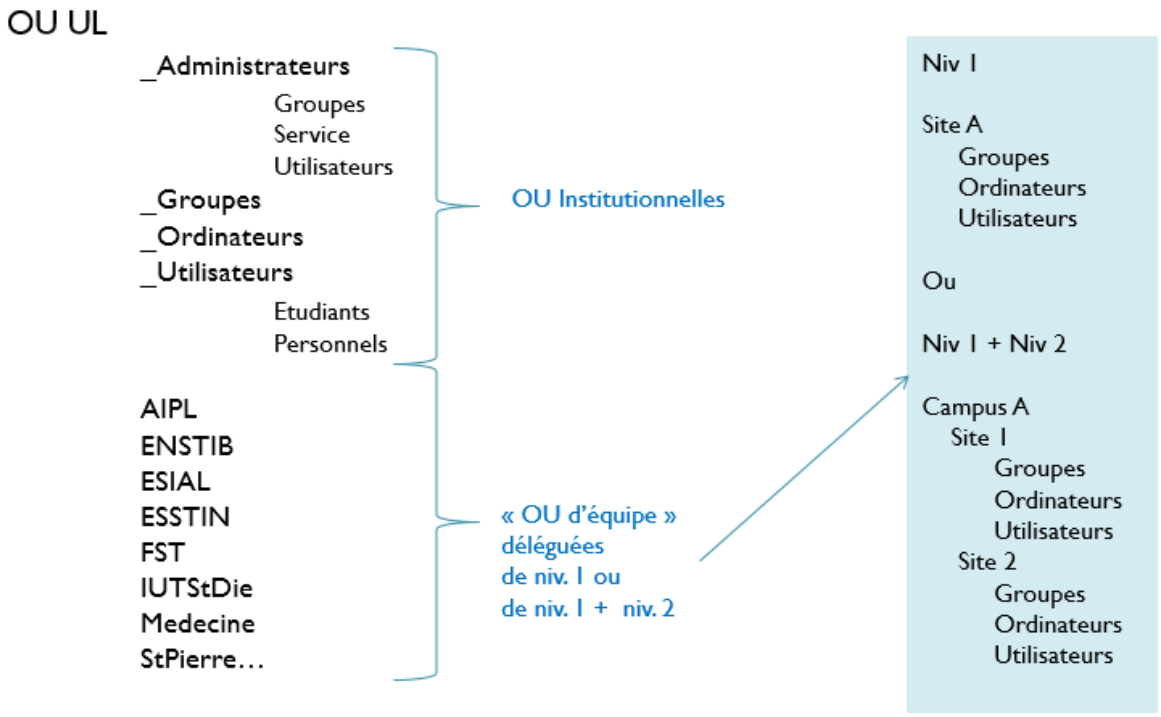


Figure 15 – Organisation des OU UL

L'objectif est de laisser de l'autonomie aux équipes locales tout en assurant une alimentation automatique et fiable de l'annuaire. Il s'agit du modèle utilisé dans les anciens établissements et aussi celui que j'avais proposé sur Metz.

A noter, la création de comptes utilisateurs manuels se fait dans l'OU « niveau de délégation » et surtout pas dans l'OU Personnels.

I.3.7.2 Règles de nommage

Afin d'assurer l'homogénéité des objets, le groupe de travail a indiqué plusieurs convention de nommage :

- Règle de nommage des objets (hors OU) : Tous les objets, ordinateurs, GPO, groupes, possèdent comme préfixe le code court (3 caractères) de la structure logique à laquelle ils appartiennent, comme par exemple SHS, SHA, ALL.

- Règle de nommage des OU : pas de règle. La préconisation est d'utiliser les libellés longs ou court existants et d'éviter les accents, caractères spéciaux (voir aussi la possibilité d'utiliser le « petit nom » informatique qui est aussi utilisé pour les noms de liste).

- Règle de nommage des groupes : les groupes créés au sein d'une OU de niveau délégation, sont nommés selon la règle suivante : Code court de la structure_ le type de groupe _ le nom du groupe. Exemple : FEA_GL_accessalle

- Règle de nommage des groupes de formation / promotion :

    - Groupe année courante : Codes court structure_GGA_CodeEtape

    - Groupe année N-1 : Codes court structure_GGA_CodeEtape_N-1

Par ailleurs, il nous fallait prévoir les changements d'année universitaire :

- Les étudiants qui étaient membres du groupe GGA-Code Etape sont migrés automatiquement dans le groupe GGA-Code-N-1, le groupe GGA-Code Etape est donc vide.

- Au fur et à mesure des inscriptions, le groupe GGA-Code Etape est alimenté avec les nouveaux membres.

- A une date déterminée le groupe « GGA-Code-N-1 » est vidé en masse.

- Règle de nommage des groupes globaux au niveau UL :

    - GGA : préfixe utilisé pour les Groupes Globaux Automatique

    - GGM : préfixe utilisé pour les Groupes Globaux Manuels (ex : les départements d'IUT)

I.3.8 Structure physique

La structure physique doit pouvoir garantir la continuité de service en cas de coupure du réseau Lothaire. Dès lors, chaque nœud du réseau doit disposer d'au moins un contrôleur de domaine.

Les sites Active Directory sont calqués sur les sites géographiques : Nancy, Metz, Thionville, Longwy, Moselle Est, Epinal, Saint-Dié ainsi que le site racine. Nous avons adopté une topologie en étoile, avec un site cœur à Nancy et des satellites sur toute la Lorraine. Enfin, toutes les créations automatiques et via l'interface sont faites directement sur le site cœur.

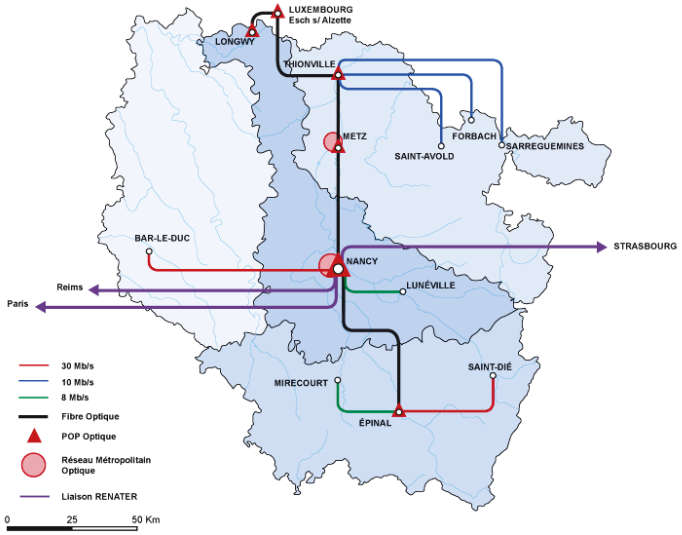


Figure 16 – Le réseau Lorrain

Nous allons maintenant nous intéresser au site de Nancy. Celui-ci est constitué de 4 réseaux distincts (VLAN) irriguant les campus nancéiens. Pour assurer la haute disponibilité, nous avons décidé de placer au minimum 2 contrôleurs de domaine par réseau afin de garantir une continuité de service optimum pour les postes clients. Nous avons donc planifié l'installation de 8 serveurs pour le site de Nancy.

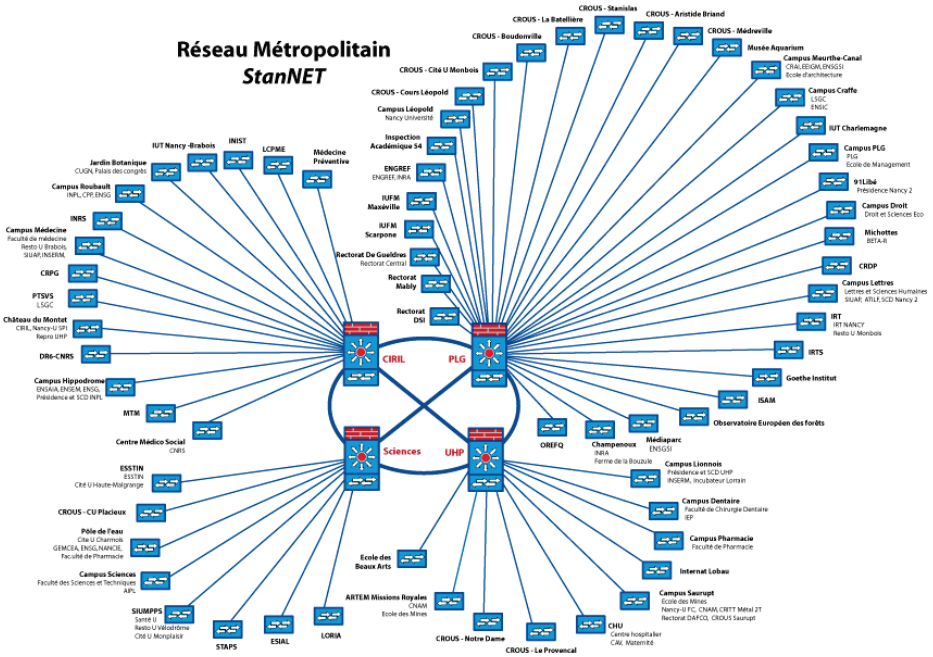


Figure 17 – Le réseau à Nancy

De la même façon, il me semble intéressant de détailler l'infrastructure physique de Metz. La plateforme messine est composée de deux réseaux distincts : le site du Saulcy et le

technopôle. En suivant la même logique, nous avons décidé de déployer 4 serveurs sur Metz, 2 sur l'ile du Saulcy et 2 sur le site de Bridoux. Là encore, l'objectif est d'assurer une continuité de service pour les postes clients ainsi qu'une bonne répartition de la charge.

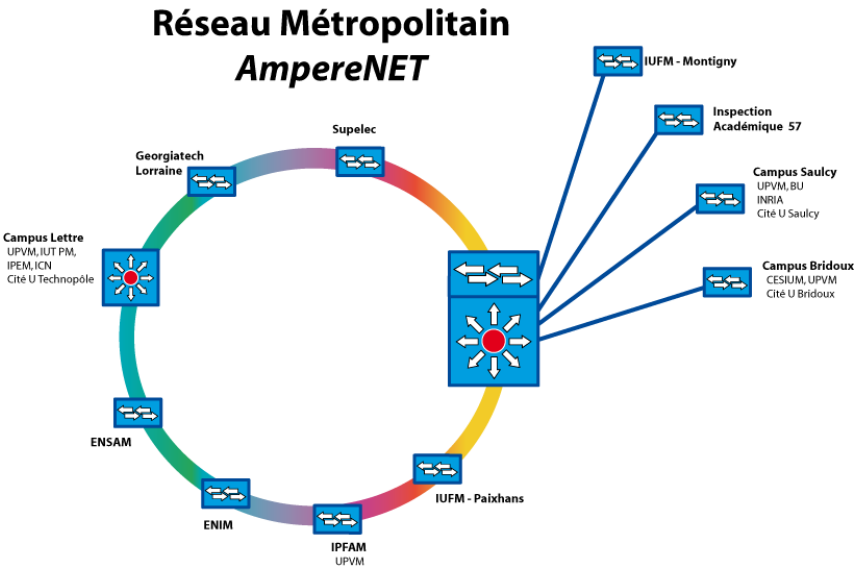


Figure 18 – Le réseau à Metz

Pour finir, voici le schéma de synthèse de l'infrastructure physique. Par manque de place, seuls 5 sites ont été représentés sur les 8 mais le principe est similaire. Tous les liens réseaux sont haut débit, ce qui facilite la réplication des objets entre les contrôleurs de domaine et simplifie l'administration des sites. Nous avons suivi le principe : 1 site géographique, 1 site Active Directory, 1 ou plusieurs contrôleurs de domaine. De cette façon, les postes clients iront s'authentifier sur l'équipement le plus proche sans émettre de trames sur les sites distants. Pour conclure, ce schéma de principe est très proche de celui que j'avais déterminé lors de mon étude sur le site de Metz, point I.2.6.6.

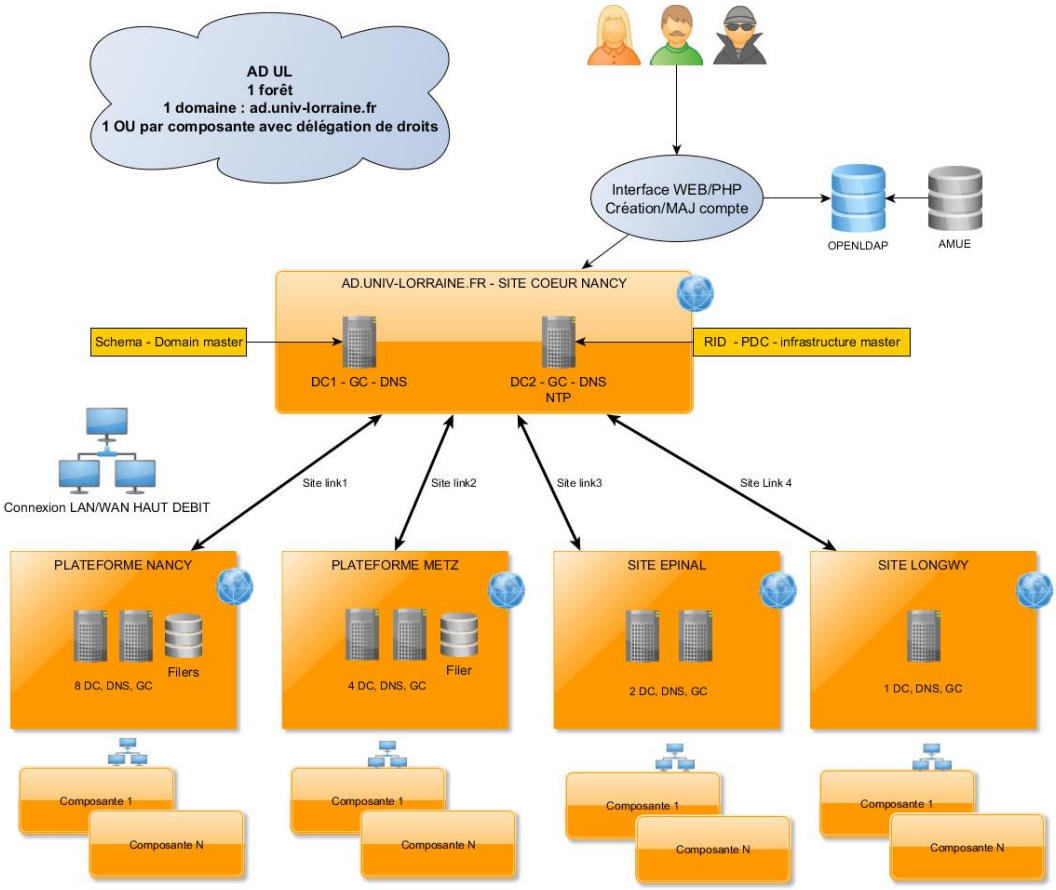


Figure 19 – L'architecture AD UL finale

I.3.9 L'interface d'administration Web

L'objectif d'une console d'administration est de fournir à l'ensemble des informaticiens de l'UL des outils simples et efficaces afin d'effectuer des opérations indispensables sur l'annuaire, comme la gestion des utilisateurs et des groupes. Bien qu'il soit possible de passer par l'interface de gestion de l'annuaire, une solution Web est plus élégante et évite de mauvaises manipulations sur la base. Ce problème est limité dans une petite structure où tous les informaticiens peuvent être formés en profondeur aux subtilités d'Active Directory. Au niveau de l'UL, la formation de 150 informaticiens semble en effet peu réaliste.

I.3.9.1 Etude de l'existant

L'ex-UHP et l'ex-Nancy 2 disposent déjà d'outils sur leurs AD respectifs mais aucune des deux interfaces ne contient l'ensemble des fonctionnalités actuellement utilisées sur les AD actuels. On peut citer la gestion de formations et de groupes, plus développée côté ex-Nancy 2 et la fourniture de services pour les annuaires autonomes côté ex-UHP.

L'interface de Nancy 2 pourrait être adaptable au nouvel AD dans des temps raisonnables dans la mesure où aucun nouveau module ne serait à intégrer. L'interface de l'UHP, plus flexible, est un outil qui permet d'intégrer de nouveaux modules mais l'ensemble des modules existants est à revoir avec le passage à l'échelle.

Il est donc été décidé d'utiliser l'interface ex-UHP et de réécrire l'ensemble des modules "indispensables" pour fournir les services actuels. D'autres modules seront réalisés dans un second temps, après la mise en production du projet.

I.3.9.2 Les fonctionnalités de l'interface

Chaque responsable d'équipe a envoyé la liste des besoins nécessaires au bon fonctionnement de sa structure. Il s'agit de fonctionnalités déjà présentes dans les interfaces existantes ou de besoins non encore implémentés. Voici les modules de base validés par le groupe de travail :

- Gestion des OU
- Gestion des objets ordinateurs
- Gestion des invités, personnels ou étudiants
- Gestion des groupes
- Gestion des formations avec la possibilité d'un traitement en masse
- Aide en ligne
- Gestion et archivage des fichiers journaux

I.3.9.3 Les moyens humains

Sachant que les personnes du Service aux Usagers ne peuvent consacrer qu'une partie de leur temps à développer les modules, il a été demandé à chaque responsable d'équipe de donner le nom d'une personne susceptible de participer à ce développement.

Au final, une équipe de cinq personnes s'est constituée afin de mener à bien cet important projet.

I.3.9.4 Les moyens matériels

Un AD de test a été installé à l'UHP pour des tests en interne et pour commencer à développer et tester les nouveaux modules. Cette plateforme n'a pas vocation à rester indéfiniment mais elle restera opérationnelle tant qu'une plateforme AD UL de développement ne sera pas installée.

Les premiers développements peuvent se faire à partir de serveurs locaux (environnement LAMP ou WAMP) mais il est absolument nécessaire d'installer un serveur UL pour tester les programmes avant production. Le serveur apache doit fournir un accès sécurisé et pouvoir utiliser le protocole LDAPS. Un certificat doit être installé sur l'AD de test et sur le serveur de développement pour permettre la création des entrées dans l'annuaire Microsoft.

I.3.9.5 L'administration de l'interface

Un groupe d'administrateurs de l'interface sera créé par le groupe de travail AD. Ce groupe aura les responsabilités suivantes :

- Mettre les nouvelles fonctionnalités en ligne
- Configurer les groupes d'accès à l'interface en relation avec les administrateurs AD
- Répondre aux besoins éventuels des responsables de sites

Chaque fonctionnalité sera testée et validée sur la plateforme de test par un panel d'utilisateurs potentiels de la fonctionnalité. Ce panel sera désigné par le groupe de travail AD. La fonctionnalité sera mise en production par le groupe des administrateurs de l'interface.

La maintenance sera faite par l'équipe de développement sur sollicitation du groupe de travail AD pour le développement de nouveaux modules et pour la correction d'anomalies.

I.3.9.6 La gestion des droits entre l'annuaire et l'interface

Deux stratégies différentes ont été implémentées sur les AD de Nancy 2 et de l'UHP :

	Environnement	Les choix	Avantages	Inconvénients
Nancy 2	1 AD	Délégation des droits au niveau de l'AD L'application authentifie	Gestion fine des droits par utilisateur Sécurité renforcée	Il faut appartenir à l'AD pour se connecter

		sur l'annuaire		
UHP	2 AD	Délégation des droits au niveau de l'interface L'application utilise un compte de service	Pas de configuration sur l'annuaire Authentification connecté au SI	Création d'un compte de service dans l'annuaire

Tableau 3 – Comparaison des solutions Nancy 2 et UHP

Les deux solutions ayant des avantages et des inconvénients, le groupe décide de choisir la solution ex-UHP avec :

- Un compte de délégation sur les OU de sites. Il n'y a pas de délégation sur les OU hébergeant les comptes institutionnels.
- Le compte ne peut se connecter directement sur l'AD.
- Le mot de passe est stocké crypté et est modifié à intervalles réguliers.
- L'authentification des utilisateurs se fera sur l'annuaire OpenLDAP.

Le développement sera également prévu pour changer facilement de mode de délégation si le besoin s'en fait sentir. Bien que l'interface proposée puisse s'adapter à n'importe quelle architecture logique de l'AD, le groupe souhaite que cette structure soit la plus simple possible dans le respect des contraintes techniques de gestion de l'AD pour en faciliter sa gestion soit par l'interface, soit directement.

Il est aussi décidé que les OU (utilisateurs, ordinateurs et groupes) soient des OU « obligatoires » sous l'OU de site, toujours dans le souci de faciliter la gestion de l'AD.

I.3.10 La mise en place

Nous avons validé le système Windows 2008R2 Entreprise afin d'assurer une cohérence sur l'ensemble de l'infrastructure, tout en profitant des dernières fonctionnalités Microsoft. L'usage des machines virtuelles est encouragé sauf sur les serveurs hébergeant les rôles FSMO qui seront des serveurs physiques. Enfin, une vérification complète des salles systèmes hébergeant les serveurs ou machines virtuelles est planifiée.

Concernant les machines, nous avons suivi les recommandations de Microsoft pour calibrer au mieux la puissance nécessaire et nous avons commandé deux serveurs DELL pour

assurer le cœur du réseau. De la même façon, nous avons validé un patron générique pour les machines virtuelles.

Après une première maquette, nous avons tout d'abord installé les contrôleurs de domaine principaux à Nancy, puis nous avons configuré le domaine « ad.univ-lorraine.fr » en suivant les indications provenant des lots précédents. Nous avons tout d'abord créé l'arborescence logique puis nous avons déversé les comptes et les groupes provenant de l'annuaire OpenLDAP

En parallèle, je me suis occupé de l'installation et de la configuration du site de Metz avec mon collègue Eric Senet. Nous avons déployé les 2 contrôleurs de domaine sur une infrastructure virtualisée puis nous les avons reliés au site central. Nous avons ensuite configuré les serveurs, les outils de supervision, les sites Active Directory, les liens inter-sites, les GPO, la réplication des données ainsi que la sauvegarde.

Des équipes ont installé les contrôleurs sur les sites satellites courant mai puis nous avons ensuite validé le bon fonctionnement de l'ensemble du système avec le groupe de travail. Au final, l'annuaire était fonctionnel fin juin 2012.

I.3.11 Accompagnement du changement et bilan

La mise ne place d'un tel projet représente un changement important pour les informaticiens, en particulier sur la plateforme de Metz. Un sentiment de perte d'autonomie peut se faire sentir. En effet, les responsables de site ne sont plus administrateurs du domaine et leur vue sur l'arborescence est limitée. De plus, le contrôleur de domaine n'est plus forcément hébergé dans la structure ce qui renforce ce sentiment de perte de contrôle. Enfin, le passage conseillé par l'interface Web peut perturber les habitudes de gestion.

Néanmoins, dans un contexte de raréfaction des crédits et des moyens humains, l'optimisation des infrastructures et du SI est indispensable. Par ailleurs, l'objectif est de construire ensemble un système adapté au besoin de chacun, plutôt que de se voir imposer l'externalisation du service. Bien que les informaticiens soient mitigés au début quant à l'aboutissement d'un tel projet, les collègues sont maintenant satisfaits du nouveau système qui permet une gestion efficace et robuste des utilisateurs et des postes clients.

Afin d'accompagner le changement, nous avons développé 4 axes :

- La centralisation des documentations sur Wikidocs. Une grande partie des informations sont ouvertes à tous les informaticiens de l'Université de Lorraine. Toutes les procédures utiles sont recensées sur le site ainsi que les problèmes courants et les remédiations nécessaires. Le site est maintenu par le groupe de travail.

- Le groupe de travail a régulièrement communiqué sur l'état du projet et organisé plusieurs réunions d'informations auprès des responsables de sites et des informaticiens. Par ailleurs, des campagnes de formations ont été lancées sur Nancy et Metz portant non seulement sur le fonctionnement basique de l'annuaire mais sur l'utilisation de l'interface Web. Tous les informaticiens de sites sont désormais opérationnels.

- Enfin, nous avons créé une file dédiée aux problématiques de l'Active Directory dans le système de helpdesk. Les questions des informaticiens sont prises en charge par les membres du groupe de travail et un historique est consigné.

- Un délai supplémentaire est donné sur le site messin quant à l'intégration dans l'AD. *En effet, l'écart technologique étant trop marqué entre les usages de Metz et les usages nancéens, l'intégration des postes clients est reportée à septembre 2013*.

De mon côté, je suis particulièrement satisfait d'avoir participé à un projet de cette envergure. J'ai travaillé efficacement avec mes collègues nancéiens et messins et nous avons relevé avec succès le défi d'un annuaire unique. A l'heure actuelle, la base contient plus de 100000 entrées, utilisateurs et ordinateurs. Le système est fonctionnel, stable et donne entière satisfaction. Ce projet m'a permis d'acquérir de nouvelles compétences techniques et d'améliorer également mes compétences en gestion de projet.

Nous disposions d'un an pour intégrer l'intégralité des postes clients sur le site de Metz, l'échéance ayant été reportée à septembre 2013 sur le site messin. Il s'agit d'un travail colossal, puisque 4600 ordinateurs sont touchés. Une migration manuelle représente en moyenne 2 heures. Dès lors, il fallait trouver une solution pour industrialiser ce processus et réduire les délais. C'est ainsi que commence la deuxième partie de mon mémoire : l'intégration du poste client, projet que j'ai entièrement supervisé et réalisé.

II Deuxième partie : intégration du poste client

Dans une précédente partie, nous avons vu la mise en place d'un annuaire centralisé Active Directory. Dans cette seconde partie, nous allons nous intéresser à l'intégration du poste de travail dans le nouveau système d'information de l'Université de Lorraine. Nous allons donc tout d'abord traiter la problématique de la production des postes de travail, puis nous étudierons les stratégies mise en place permettant de répondre au passage à l'échelle.

II.1 La problématique du poste de travail

II.1.1 Des contraintes fortes

Afin que les utilisateurs puissent bénéficier d'une authentification unifiée au niveau de l'Université de Lorraine, il est impératif que les ordinateurs concernés joignent le nouvel annuaire Microsoft. Une fois cette opération accomplie, les usagers pourront s'identifier avec un compte unique et profiter de leurs nouveaux services numériques.

Par ailleurs, il est nécessaire de distinguer trois types d'utilisateurs, les contraintes et échéances du projet étant propres à chaque population :

- La pédagogie: les étudiants doivent pouvoir s'authentifier sur la nouvelle infrastructure informatique dès septembre 2012 dans les cas des établissements nancéens et en septembre 2013 pour l'ex-UPVM. Cette échéance est prioritaire et ne doit souffrir d'aucun retard afin de ne pas handicaper la tenue des cours et des travaux dirigés. Cette contrainte est particulièrement forte et ne peut être différée.

- L'administration : avec la multiplication des échanges de documents, la connexion des machines des personnels représente un enjeu de taille. Cette phase intervient après la migration des postes pédagogiques, à partir de septembre 2013 pour la plate-forme messine. Contrairement à la population précédente, cette étape, bien qu'obligatoire, peut courir sur plusieurs semaines et être différée fin 2013.

- Les enseignants et chercheurs : de façon similaire aux personnels administratifs, les enseignants échangent un nombre croissant d'informations et de documents au niveau de l'Université de Lorraine. Par ailleurs, l'intégration des machines permettrait une amélioration de la sécurité, les ordinateurs étant souvent dépourvus de mot de passe de connexion. Cependant après une rapide étude, il apparait que cette population est extrêmement mobile,

utilisant leur machines dans la sphère professionnelle mais également privée. De la même façon, les usages et la maitrise de l'outil informatique sont également disparates suivant les spécialités ou les laboratoires. Bien qu'il soit souhaitable à terme que cette population soit connectée à un système d'authentification unique, aucune échéance n'est précisée. Le choix d'une bascule vers la nouvelle infrastructure est donc laissé à la discrétion de chaque responsable de site, en fonction de sa connaissance du terrain et de ses utilisateurs.

II.1.2 Une problématique d'échelle

La problématique de départ est simple : enfin de migrer les ordinateurs de l'infrastructure ex-UPVM vers le nouveau système d'information, une opération de changement de domaine doit être effectuée sur chacun des postes. L'ordinateur doit quitter l'ancien domaine afin de basculer vers le nouveau périmètre UL.

Bien que cette opération puisse paraître triviale, c'est le passage à l'échelle qui pose ici problème puisque dans le cas de l'UFR Sciences Humaines et Sociales, ce sont près de 1000 ordinateurs qui doivent être basculés et au total plus de 5000 postes sur le campus messin. Ce chiffre est ventilé en 2700 ordinateurs pédagogiques et 2400 machines liées aux personnels administratifs et enseignants.

Par ailleurs, cette modification impacte directement les utilisateurs puisqu'elle engendre un changement d'identifiant et de mot de passe pour les personnels et les enseignants qui devront désormais utiliser leur mot de passe UL. Enfin, l'intégration d'un poste informatique dans le nouveau référentiel doit se faire sans perte de documents.

II.1.3 L'obsolescence de Windows XP

Ce changement sur le poste de travail intervient dans un contexte informatique particulier puisque Microsoft va arrêter le support du système d'exploitation Windows XP en avril 2014. Ce système d'exploitation ne sera plus mis à jour et sera donc vulnérable aux attaques informatiques.

Par ailleurs, les éditeurs de logiciels arrêtent également graduellement le support de cette plateforme en privilégiant désormais Windows 8 et surtout Windows 7 pour accueillir leurs applicatifs. Ne pas moderniser le système de nos postes clients sera à long terme dommageable pour le fonctionnement de nos applications métiers.

Cette phase de migration représente un défi réel dans nos environnements puisque la majorité de nos machines sont encore équipées de Windows XP, en particulier les postes pédagogiques et administratifs. Les enseignants sont moins impactés car le renouvellement de leurs équipements possède un cycle court d'amortissement de 3 ans. Cette population est donc déjà équipée d'une nouvelle version de Windows, situation de cohabitation que Gartner appelle la « diversité gérée »[13].

II.1.4 Le projet poste de travail

En partant d'un besoin simple, basculer les ordinateurs dans le référentiel de l'Université de Lorraine afin d'offrir de nouveaux services aux utilisateurs, cette problématique fait apparaitre deux volets plus complexes : gérer le passage à l'échelle d'une telle opération ainsi que l'obsolescence de Windows XP.

Il me paraissait donc essentiel d'aborder la gestion du poste de travail dans sa globalité et non comme des briques séparées afin de minimiser les interruptions sur le poste utilisateur et diminuer les coûts. J'ai donc proposé mi-2012 un projet de production du poste de travail à mon responsable M. Mathieu et à la direction. Les objectifs initiaux étaient multiples :

- Faciliter l'intégration des machines pédagogiques et administratives vers le périmètre de l'Université de Lorraine en respectant les contraintes
- Valider un outil de migration de Windows XP vers un système plus récent
- Mettre en place une base de connaissance sur cette problématique

L'objectif principal du projet était de proposer aux informaticiens de l'Université de Lorraine une méthodologie et des outils adaptés, afin d'effectuer cette importante phase de migration dans les meilleurs conditions possibles que ce soit du côté des utilisateurs ou des équipes informatiques. Le projet est complexe car il doit intégrer l'existant, en particulier les matériels et applicatifs déjà déployés, ainsi que les données utilisateurs.

Par ailleurs, plutôt que de mener une réflexion purement messine, ce projet a été proposé aux informaticiens de l'Université de Lorraine. Au final, huit personnes provenant des

[13] http://www.adelanto.fr/upload/di35/vmware/Gartner_Migration_Windows7.pdf

quatre ex-établissements ont répondu à cette proposition. Par ailleurs, à un niveau plus local, des enseignants sont intervenus ponctuellement afin de valider le bon fonctionnement des postes et leur adéquation aux enseignements dispensés. Enfin un suivi du projet est assuré par Olivier Mathieu.

II.1.5 Périmètre du projet

Dès le lancement du projet, j'ai précisé le périmètre, notamment par rapport à Windows 8 et à la stratégie de migration.

II.1.5.1 Choix de Windows 7

La migration de Windows XP est au cœur des préoccupations dans les entreprises puisque selon la société Net Applications, qui établit des statistiques sur les nouvelles technologies[14], plus de 38% des entreprises utilisent encore Windows XP en 2013. Selon Gartner, près de 60% des entreprises sont encore aux débuts de leur projet de migration de Windows XP.

De plus, toujours selon Gartner, une migration vers Windows 7 est préférable à un changement brutal vers Windows 8 afin de ne pas bouleverser l'expérience des utilisateurs et profiter de pilotes matériels stables et certifiés[15]. Gartner estime que Windows 7 est un jalon majeur dans les systèmes d'exploitation Microsoft et qu'une migration directe vers Windows 8 est trop risquée pour les entreprises sauf dans le domaine des tablettes PC.

Une étude récente du cabinet Forrester[16] indique que la majorité des entreprises n'adopterait pas Windows 8 en tant que système d'exploitation principal. En France, 68 % des ordinateurs à usage professionnel sont sous Windows 7 et 50 % des participants français planifient de déployer cette version du système lors du prochain renouvellement de leur parc informatique, contre seulement 28 % d'intentions en faveur de Windows 8. Cette étude révèle également que les décideurs informatiques ne voient pas le nouveau Windows comme une amélioration par rapport à l'ancienne version.

---

[14] http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qptimeframe=M&qpsp=170
[15] http://redmondmag.com/articles/2012/09/26/windows-8-no-escape-from-xp-danger-zone.aspx
[16] http://pro.01net.com/editorial/595863/seules-28-pour-cent-des-entreprises-francaises-s-appretent-a-migrer-vers-windows/

Après quelques tests internes qui ont confirmé nos recherches, je me suis donc focalisé sur le déploiement de Windows 7 au sein de notre organisation, système qui apparait comme plus mature et mieux supporté au niveau matériel et logiciel (Bories & Duchêne, 2010). Cependant, je voulais laisser la possibilité technique de déployer Windows 8 pour les structures le souhaitant.

II.1.6 Stratégie de migration

Nous nous sommes intéressés ici à la méthodologie de migration : en deux temps ou de façon unique ?

II.1.6.1 Premier scénario : une migration en deux temps

La première solution s'appuierait sur une phase d'intégration manuelle des postes informatiques vers la nouvelle infrastructure de l'Université de Lorraine, puis d'une migration ultérieure des postes de Windows XP à Windows 7.

La première étape nécessite un passage obligatoire sur les postes clients afin de changer le domaine d'authentification et de migrer les documents des utilisateurs. Ces opérations sont techniquement simples et certaines parties peuvent être automatisées bien que le passage d'un technicien sur chaque machine reste obligatoire. Après la mise en place d'une maquette technique, j'ai calculé qu'une quinzaine de minutes par machine étaient nécessaires suivant la complexité de l'environnement utilisateur.

Cette première phase ne nécessite pas d'infrastructure particulière et les coûts matériels et logiciels sont négligeables. Elle peut être rapidement mise en œuvre dans l'entreprise et les postes intégrés au fil de l'eau. Cependant, elle nécessite une bonne planification puisqu'un technicien doit intervenir sur toutes les machines ce qui peut pénaliser l'utilisateur dans son travail et réduire sa productivité. Par ailleurs, une période de transition sera nécessaire où les deux architecture techniques cohabiteront, engendrant de possibles problèmes de stockage et d'échange de documents. Cette opération est également répétitive pour l'équipe informatique et l'absence d'automatisation poussée peut engendrer des erreurs.

Par ailleurs, cette première phase ne résout pas l'épineuse problématique de migration vers Windows 7 pour laquelle une seconde intervention sur le poste utilisateur est nécessaire. Il s'agit ici d'une opération lourde nécessitant l'audit du parc matériel et applicatif, le choix d'un outil adaptée, la mise en place d'une infrastructure technique et la formation des utilisateurs.

II.1.6.2 Second scénario : une migration unique

Le scénario est ici simple : pourquoi ne pas profiter de la migration vers Windows 7 pour intégrer directement les postes de travail dans le référentiel de l'Université de Lorraine ? En effet, quel que soit l'outil choisit pour assurer cette migration, celui-ci gère nécessairement la jonction du poste client vers un domaine Windows. Dès lors, il suffit de renseigner ce paramètre dans le fichier de configuration pour que la machine soit automatiquement basculée vers le domaine UL au premier démarrage sous Windows 7. Ce scénario transforme la problématique de changement de référentiel en un simple paramètre à renseigner sur l'outil de migration. Dès lors cette opération est totalement automatisable et ne nécessité aucune intervention supplémentaire sur le poste client.

Cette opération ne peut cependant pas être déployée en urgence, puisqu'elle nécessite une totale validation du processus de migration vers Windows 7. En effet, une vérification des configurations matérielles est nécessaire afin de valider leur adéquation avec les recommandations fournies par Microsoft quant à l'utilisation de Windows 7. Cette phase s'accompagne d'un audit applicatif afin de vérifier la compatibilité des programmes avec ce nouveau système.

Il faut également accompagner l'utilisateur afin qu'il s'approprie son nouvel outil de travail tout en minimisant le temps de migration à l'aide d'un outil approprié. Gartner estime que 12 à 18 mois sont nécessaires pour planifier et tester une stratégie de migration[17]. Par ailleurs, toujours selon Gartner le coût de migration varie grandement, de 1000 à 2000 dollars par utilisateur.

II.1.6.3 Validation du scénario de migration

Mon responsable était partisan d'une migration en deux temps alors que j'étais plutôt en faveur d'une migration unique. M. Mathieu souhaitait séparer le processus de changement de référentiel et la problématique de migration vers Windows 7. L'objectif était ici de s'appuyer rapidement sur le nouveau référentiel de l'Université de Lorraine afin de profiter d'une authentification unifiée et des nouvelles infrastructures informatiques dès que possible.

[17] https://www.gartner.com/doc/1719116/creating-timeline-deploying-windows-

De mon côté, bien que plus complexe à mettre en œuvre, une migration unique me paraissait plus appropriée. En effet, une intervention unique me paraissait plus simple à expliquer aux utilisateurs et à la direction que deux manipulations successives. Pour l'équipe informatique, ce scénario semblait moins contraignant et plus stimulant que la première alternative. J'ai essayé de quantifier les données des deux scénarios ci-dessous.

	Temps global nécessaire à la migration	Impact sur la production	Coûts de la solution	Complexité technique	Charge de travail pour l'informatique
Migration en deux temps	+++	++	80 €/poste	+++	+++
Migration unique	++	+	80 €/poste	++	++

Tableau 4 – Comparaison des scénarios de migration

J'ai ensuite proposé ces deux options à la direction de la composante courant 2012. La question du coût n'a pas été déterminante puisque cette facette était similaire dans les deux alternatives proposées. Une première estimation incluant l'infrastructure et les licences nécessaires faisait état de 80 € HT par poste au maximum. Les tarifs très compétitifs proposés par Microsoft et ses partenaires à l'Université de Lorraine expliquent en partie le faible coût global. Par ailleurs, ayant déjà déployé une infrastructure totalement virtualisée avec VMware Vsphere en 2011, je n'avais pas besoin d'inclure des dépenses supplémentaires liées à des équipements et serveurs informatiques. Ces deux paramètres expliquent ce résultat, comparé aux estimations fournies par les cabinets d'audit informatiques. Enfin, il ne s'agit pas d'un changement de matériel mais seulement de sa reconfiguration.

Au vu de ces informations, la direction a donc choisi une migration en une phase unique, afin d'impacter le moins possible les utilisateurs. Cette migration vers Windows 7 a été planifiée entre juin et août 2013 pour la pédagogie qui représente plus de 500 machines, puis entre septembre et décembre 2013 pour la partie administrative. Plusieurs vagues de migration ont été programmées sur ces périmètres afin de ne pas surcharger le réseau et de ne pas paralyser l'ensemble des personnels administratifs au même moment.

Ces réunions avec la direction ont permis de cadrer le projet et de communiquer avec les utilisateurs concernant les modifications de leur environnement de travail et les échéances envisagées. Ayant le feu vert d'un point de vue hiérarchique, financier et organisationnel, nous nous sommes donc intéressés à l'étude de technique.

II.2 Etat de l'art du poste client

Un état de l'art des techniques de production du poste de travail était nécessaire afin de préciser le projet. L'objectif de cette étape était donc de réaliser un panorama des solutions répondant aux besoins spécifiés, afin de ne retenir ensuite qu'une solution technique à approfondir.

Dans cette optique, je me suis appuyé sur une étude que j'avais réalisée fin 2011 avec mon responsable Olivier Mathieu. Cette présentation a fait lieu d'une conférence de 30 minutes que j'ai présentée aux Journées Réseaux à Toulouse. Disponible en ligne, je vais vous présenter les grandes lignes de ce travail qui m'a servi de point de départ pour lancer le projet (Clémence & Mathieu, 2011).

II.2.1 Etat des lieux et tendances

L'objectif de cette présentation était de dresser un panorama des technologies actuelles permettant de gérer le poste de travail en 2011. En effet, l'apparition de nouveaux usages et de nouvelles tendances a largement complexifié cette tâche. Les utilisateurs sont de plus en plus mobiles et multi-équipés ce qui pousse les services informatiques à repenser le cycle de production du poste de travail

Tout d'abord, on peut remarquer que les habitudes des utilisateurs ont fortement évolués ces dernières années. Dans la majorité des cas, chaque usager disposait auparavant d'un poste fixe unique, installé dans son bureau. Les ordinateurs portables étaient encore onéreux et les performances systèmes étaient en retrait par rapport aux machines de bureaux.

En quelques années, la tendance a rapidement changé : l'utilisateur est devenu mobile et multi-équipé. En 2008 les ventes d'ordinateurs portables ont dépassé les ventes d'ordinateurs fixes (ISuppli, 2008). De l'ultraportable muni d'un écran 12 pouces au transportable de 17 pouces, les gammes de produits se sont désormais largement démocratisées et les performances se sont améliorées. Les écrans se démultiplient au travail ou à la maison poussés par une grande tendance : le multi-équipement. Ce phénomène s'explique en particulier par les ventes de miniportables ou Netbook qui ont explosé, passant de moins d'un million d'unités à plus de 14 millions d'appareils vendus (DisplayBank, 2008). On assiste à un véritable engouement pour ces machines abordables, de très petites tailles, aux performances modestes, calibrées pour la

navigation internet et les outils bureautiques. Une nouvelle source de croissance est par ailleurs apparue avec la démocratisation des téléphones intelligents et des tablettes tactiles dominées par Apple. Selon une étude DELL en 2011[18], le nombre d'ordinateurs de bureau connectés à internet a dépassé le milliard en 2005. Or plus de 10 milliards d'équipements mobiles connectés à Internet sont attendus à l'horizon 2020.

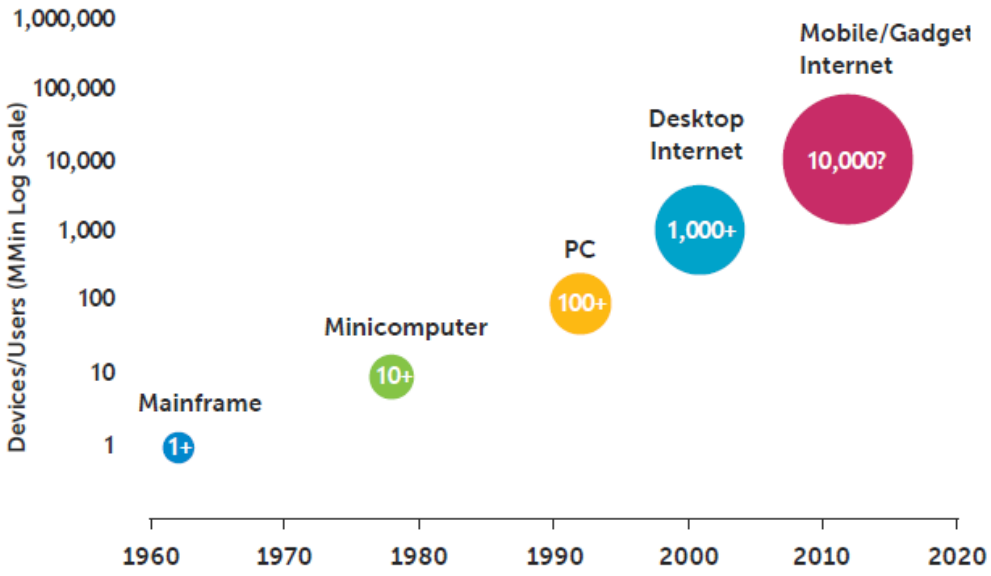


Figure 20 – Croissance des équipements informatiques

Avec ces nouveaux usages, la séparation entre sphère personnelle et la vie professionnelle est devenue de plus en plus mince. Les usagers utilisent régulièrement leurs propres matériels pour leurs besoins professionnels car ils ont développé des usages à titre personnel, qu'ils souhaitent maintenant retrouver dans leur environnement de travail. Cette « *consumérisation* » [19] de l'informatique révèle de nouveaux enjeux notamment liés à la sécurisation de ces dispositifs mobiles et aux modes d'accès des applications internes. Une étude

[18] DELL, CIO Strategies for Consumerization : The future of enterprise mobile computing, http://i.zdnet.com/whitepapers/DellMicrosoft_CIO_Strategies_for_Consumerization_The_future_of_enterprise_mobile_computing.pdf

[19] Wikipédia, Définition de la *consumérisation*. http://en.wikipedia.org/wiki/Consumerization

de Trend Micro en 2011[20], indique que 45% des utilisateurs interrogés comptent utiliser leur « smartphone » personnel à des fins professionnelles.

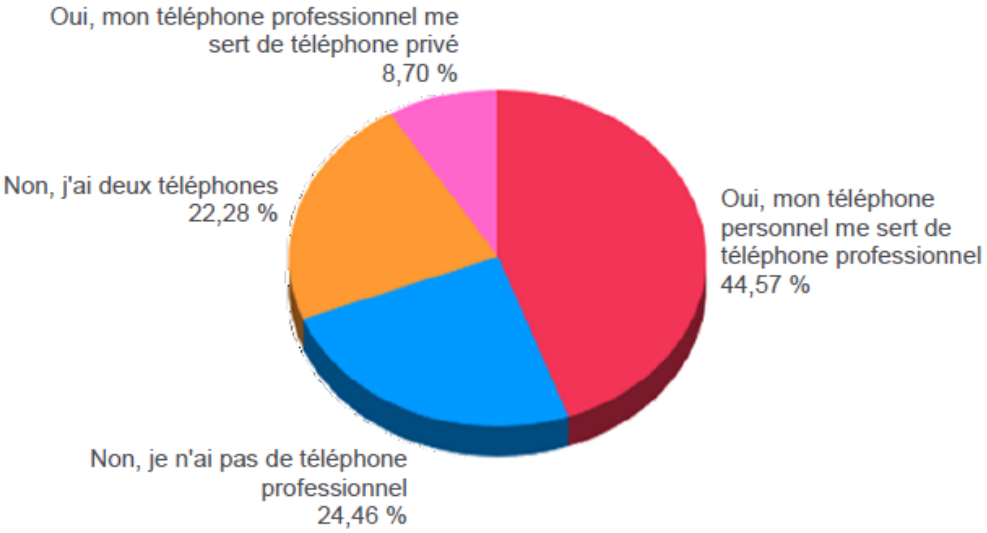


Figure 21 – L'usage des smartphones personnels au travail

Avec la multiplication des appareils, les services informatiques doivent désormais administrer un nombre toujours plus important de configurations matérielles et logicielles. Il est désormais courant qu'un usager possède à la fois un ordinateur fixe, un ordinateur portable et une tablette.

Par ailleurs, le renouvellement des postes informatiques, la migration d'un système d'exploitation comme c'est le cas avec Windows 7, l'intégration de logiciels, sont des tâches très chronophages pour les équipes techniques. Pour chaque euro dépensé en matériel, les entreprises dépenseraient 3 euros en gestion d'après une étude d'*IDC Study* en 2009. Il faut par ailleurs gérer de plus en plus d'équipements et de programmes avec des moyens humains au mieux constants.

Face à ces problématiques et ces contraintes, existe-t-il une solution idéale ? Différentes approches sont possibles pour traiter le sujet. Nous allons tout d'abord présenter les technologies permettant de gérer le poste de travail en séparant les solutions locales fonctionnant sur le poste client, puis les solutions distantes exécutées sur un serveur central. Nous présenterons

[20] Trend Micro, La consumérisation de l'informatique, http://www.trendmicro.fr/media/wp/wp-consumerizaton-of-ent-mobility-fr.pdf

rapidement ces solutions, que nous évaluerons ensuite aux travers de différents scénarios d'utilisation dans un cadre universitaire.

II.2.2 Technologies exécutées sur le poste de travail

Dans cette partie, nous avons diverses solutions qui s'exécutent directement sur le poste client.

II.2.2.1 Le format WIM de Microsoft

Afin d'installer le plus efficacement possible de nombreux systèmes d'exploitation sur un parc d'ordinateurs, les services informatiques tendent à choisir des configurations matérielles les plus homogènes possibles. En effet, l'utilisation d'outils de clonage des disques durs, qu'ils soient libres ou propriétaires, est aujourd'hui largement répandue. Une fois le système d'exploitation installé et paramétré avec les applications, ces programmes permettent de copier le contenu du disque dur de la machine vers une image système qui sera ensuite déployée sur des postes matériellement identiques. Cependant, le multi-équipement des utilisateurs et le changement rapide des gammes de produits, rend cette tâche de plus en plus ardue car il faut gérer un nombre croissant de profils matériels alternatifs, et donc d'images différentes.

Dans un parc composé majoritairement de systèmes Windows comme dans notre établissement, les migrations vers Windows Vista mais surtout vers Windows 7 ont permis de repenser l'installation des postes de travail. Le format WIM (Windows Imaging Format) est la pierre angulaire du système de déploiement de ces nouveaux environnements. Grâce à lui, les images systèmes peuvent être facilement maintenues, corrigées et étendues. Elles peuvent inclure des applications spécifiques, puis être déployées sur les équipements en réduisant au minimum l'intervention d'un administrateur.

Contrairement aux méthodes les plus connus (GHO, ISO ..) le format WIM ne contient pas d'image des secteurs du disque ou de la partition, mais des métadonnées et les fichiers contenus dans la partition. L'illustration suivante montre la structure d'un fichier WIM contenant deux images systèmes distinctes :

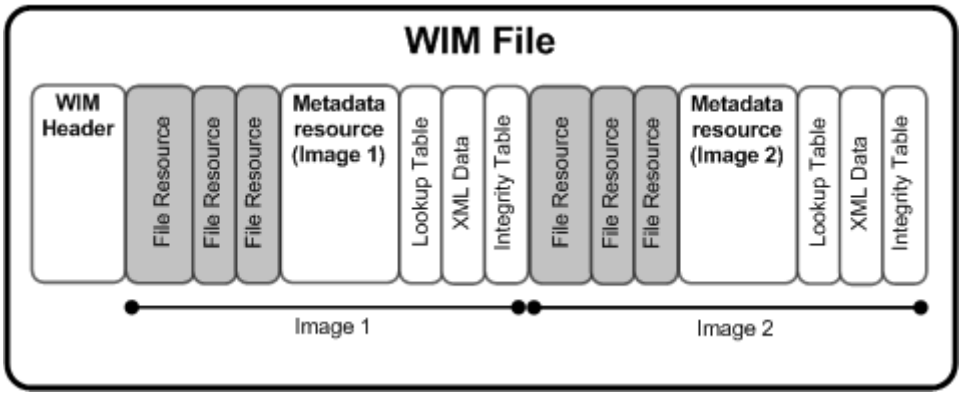


Figure 22 – Le format .WIM

La structure d'un fichier WIM est composée de six blocs distincts

- L'en-tête WIM : elle définit le contenu du fichier WIM et les adresses mémoires pointant vers les ressources clefs du fichier
- Les fichiers ressources : il s'agit des fichiers et des données qui ont été capturés lors du processus de création du fichier WIM
- Les métadonnées : elles contiennent des informations sur les fichiers ressources comme la structure des répertoires et les attributs des fichiers
- Un tableau de pointeurs : il contient les emplacements mémoire des fichiers ressources du fichier WIM
- Un tableau d'intégrité : les informations de hachage sont utilisées à chaque opération sur le fichier WIM afin de garantir l'intégrité des informations

Ce format rend les images indépendantes du matériel. Par ailleurs, un fichier référencé plusieurs fois dans le système de fichiers ne sera stocké au final qu'une seule fois dans l'image système. C'est une approche radicalement différente des solutions traditionnelles et beaucoup plus souple. Ce format sert de pierre angulaire aux solutions de déploiement Microsoft.

II.2.2.2 Le streaming d'OS

L'OS streaming peut être vu comme un super « Youtube » délivrant un accès à des images de postes de travail. Le streaming de système d'exploitation permet de dématérialiser complètement le contenu des postes sous la forme d'une image, stockée dans des volumes logiques sur un serveur ou un espace de stockage distant. La machine ne démarre plus sur son disque local mais accède directement à son image en streaming par sa carte réseau.

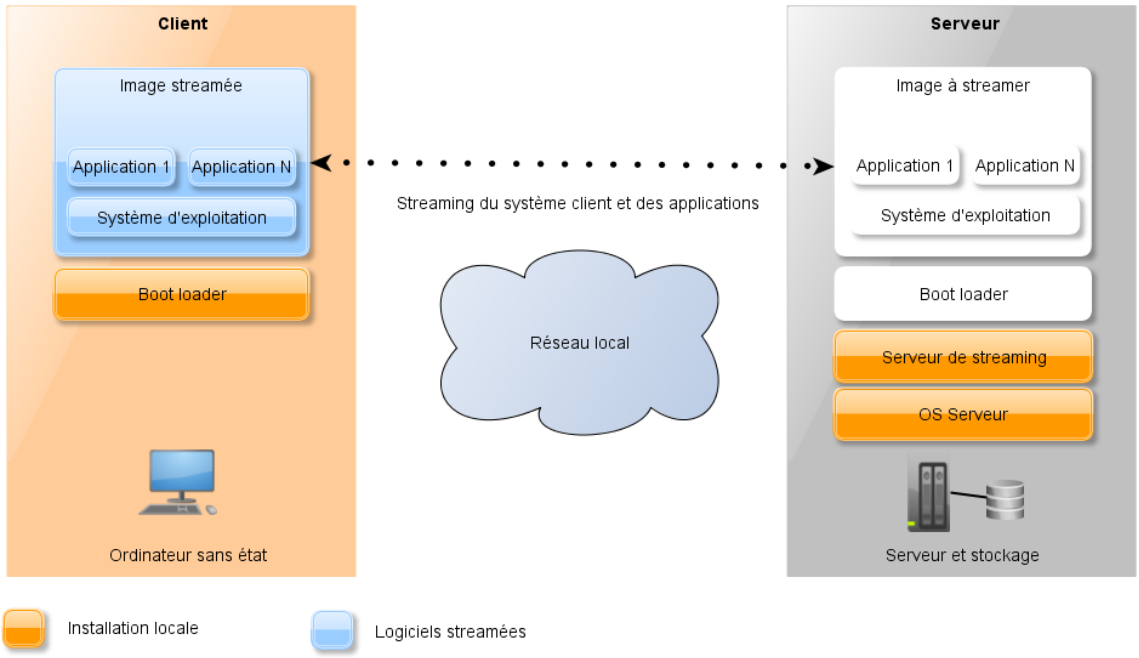


Figure 23 – Le streaming d'OS

Une console de gestion permet en outre de gérer de manière centrale l'empreinte obtenue, de la mettre à jour, de configurer le système d'exploitation, d'injecter des applications et des pilotes, facilitant grandement le travail d'administration. Ces modifications seront alors automatiquement déployées sur les postes clients lors de leur prochain amorçage sur le réseau. La restauration et la sauvegarde de l'image principale est également aisée avec l'utilisation « d'instantanés » sur le serveur de stockage. Cette technologie supporte les différentes versions de Windows et certaines distributions de Linux, ce qui permet à l'utilisateur de choisir l'environnement à lancer ou de migrer facilement d'un système d'exploitation à un autre. Cette fonctionnalité est particulièrement utile pour les organisations qui souhaitent migrer vers Windows 7 puisqu'il suffit de créer une image uniquement sur le serveur puis de la streamer vers les postes clients, fonctionnalité que j'ai pu tester avec succès.

II.2.2.3 L'hyperviseur client

L'impact de la virtualisation des serveurs n'est plus à démontrer sur la gestion d'infrastructure. Une alternative est désormais disponible pour le poste client sur le même concept : installer un hyperviseur type 1 sur le poste de travail de l'utilisateur. Ce type d'hyperviseur s'installe directement sur la couche matérielle de l'ordinateur contrairement à un hyperviseur type 2 qui est hébergé dans le système d'exploitation. Avec cette méthode, il n'y a plus besoin d'installer un système d'exploitation hôte pour lancer des machines virtuelles. L'ensemble des périphériques de l'ordinateur est alors virtualisé et l'hyperviseur client charge une

ou plusieurs machines virtuelles sur le poste de travail de façon transparente pour l'usager. Avec cette approche un utilisateur peut démarrer son équipement et manipuler de façon indépendante et simultanée des systèmes sous Windows ou sous Linux comme indiqué ci-dessous :

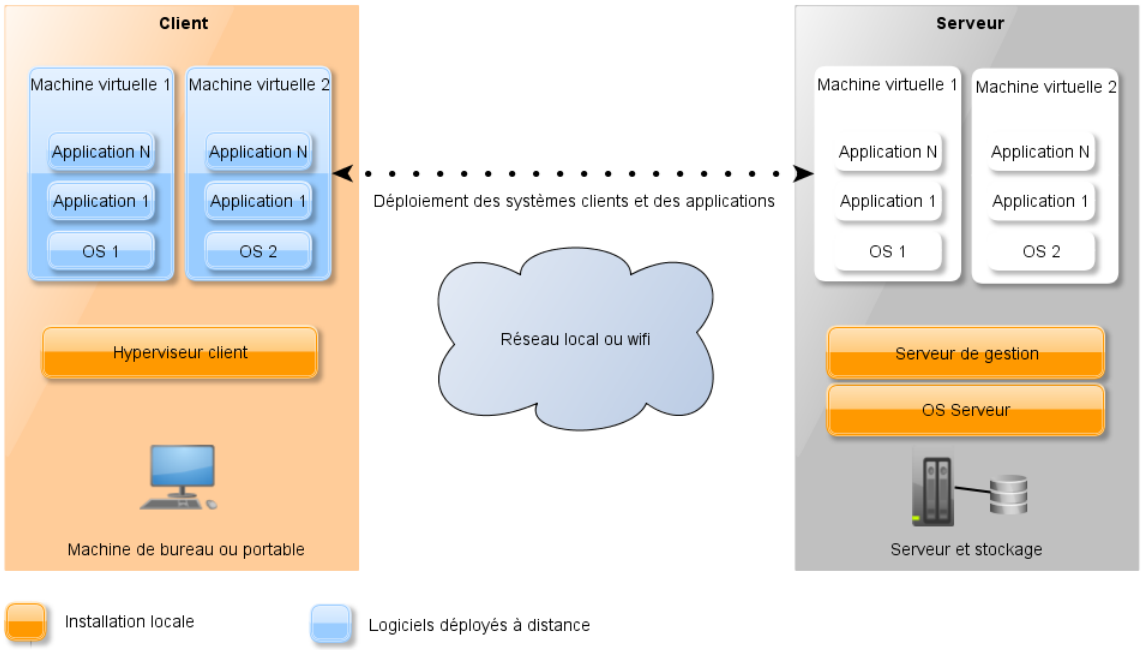


Figure 24 - Fonctionnement de l'hyperviseur client

Par ailleurs, une console de gestion permet de communiquer avec les hyperviseurs clients et de piloter de façon centrale les images virtuelles qui seront déployées par le réseau filaire ou par le wifi. Ce processus simplifie la configuration et la maintenance des mises à jour des systèmes d'exploitation ainsi que l'intégration des applications. Là encore la migration vers Windows 7 est grandement facilitée puisqu'il suffit de diffuser aux clients l'image produite en central. J'ai testé ce scénario avec NxTop de Vitual Computer, société rachetée par Citrix.

Les problèmes de pilotes sont également définitivement résolus puisque les périphériques sont désormais virtualisés. Elle offre aussi une interface pour gérer les utilisateurs et sauvegarder leurs données qui peuvent être cryptées suivant les solutions.

Un autre argument en faveur de cette technologie est qu'elle permet de travailler en mode déconnecté. L'usager a accès à l'image virtuelle qui est stockée localement, que la machine soit connectée au réseau universitaire ou non. Suivant les autorisations qui ont été positionnées, l'utilisateur peut également déployer des machines virtuelles indépendantes qu'il peut exploiter à titre personnel. On peut donc très bien imaginer un scénario avec une machine virtuelle pour l'environnement professionnel, paramétrée par la console d'administration, et un autre environnement pour une utilisation privée.

II.2.3 Les technologies exécutées à distance

Nous abordons ici deux solutions de virtualisations du poste de travail où les applications sont hébergées dans le centre de données. Ces alternatives, plus ou moins complexes, sont liées à des usages différents et peuvent même être imbriquées.

II.2.3.1 Les solutions du type publication d'applications (Server Based Computing)

La première de ces solutions en mode connecté n'est pas récente puisque proposée depuis l'origine d'X11 sous Unix ou l'apparition de NT 4.0 sous Windows. Cette « vieille » technologie n'a cessé d'évoluer et reste encore d'actualité.

L'objectif initial de la publication d'applications ou de sessions (SBC) est simple : avec un poste de travail toujours plus lourd à administrer, l'idée est d'utiliser le client pour ne traiter que les tâches d'affichage, de gestion du réseau et de l'interface utilisateur. L'ensemble de la puissance de calcul et des logiciels est déporté sur une infrastructure centralisée de serveurs qui va gérer les sessions des multiples utilisateurs.

Le poste client se connectant au serveur peut être un ordinateur fixe, un portable, ou un client dit léger comme une tablette tactile, un téléphone intelligent ou un équipement spécifique. Ce poste n'a besoin au minimum que d'un système d'exploitation et de la partie cliente de la solution de publication qui peut même y être intégrée. Après authentification via l'annuaire central, l'utilisateur a ainsi accès aux programmes configurés pour sa session.

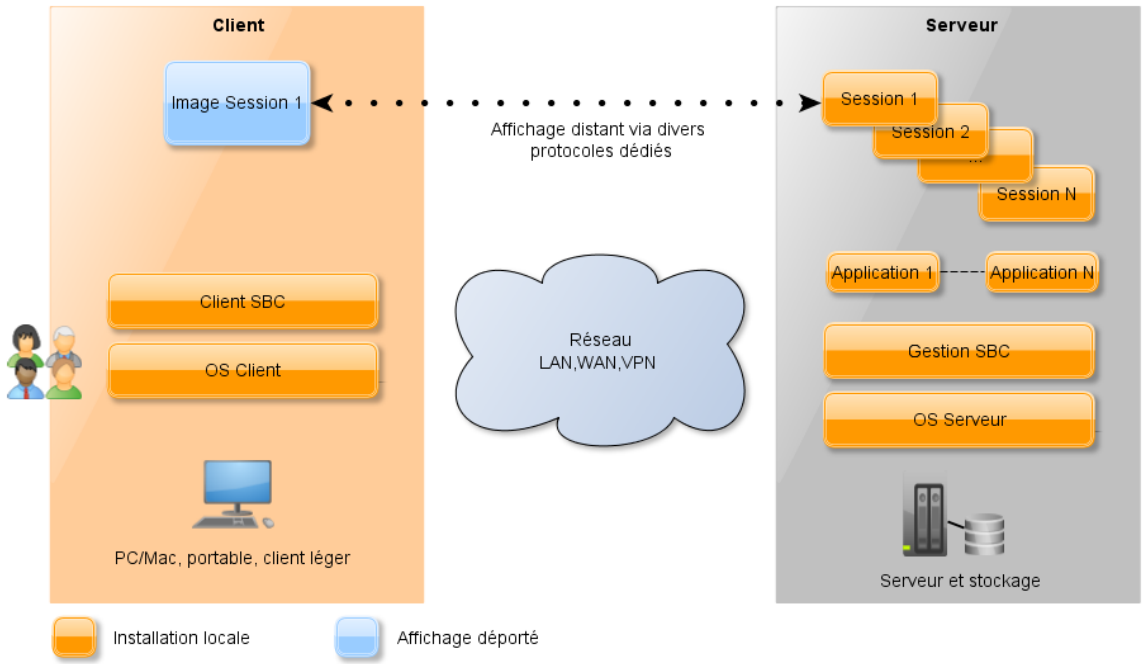


Figure 25 - Fonctionnement de SBC

La technologie SBC éprouvée depuis longtemps a de nombreux avantages. En premier lieu, la gestion du poste de travail est largement simplifiée puisque celle-ci peut être réduite à l'installation d'un simple système d'exploitation et du client de la solution SBC. Les programmes utilisés sont indépendantes du système local, on s'affranchit alors des éventuelles problématiques de comptabilité entre applications et systèmes hétérogènes. La gestion centralisée permet par ailleurs de mieux sécuriser les services applicatifs (mises à jour logicielles, sauvegarde des données, …) et offre une grande souplesse aux utilisateurs, en étant accessible depuis un grand nombre d'équipements connectés. L'infrastructure serveurs, d'un coût maitrisé, permet aux administrateurs systèmes de publier facilement de nombreuses d'applications.

Cette solution présente malgré tout quelques inconvénients dont certains sont liés au mode de connexion. Toutes les applications ne sont pas éligibles au SBC, notamment celles nécessitant des ressources multimédia avancées, de l'affichage 3D intensif ou des calculs poussés. Ce point est cependant en train de changer avec l'apparition de divers protocoles améliorant l'expérience utilisateur. Intrinsèquement liée à la technologie, une exploitation n'est pas possible sans réseau et suivant les produits il convient d'étudier et de valider l'utilisation qui peut induire une charge réseau non négligeable. Autre frein, cette fois plus psychologique, certains usagers peuvent avoir un sentiment de désappropriation de leurs outils de travail, qui peut être limité en combinant mode local et distant.

Depuis 15 ans, les offres autour du SBC se sont multipliées et n'ont eu de cesse d'évoluer afin d'optimiser les performances d'accès ou la gestion du service de publication. Afin d'améliorer encore les possibilités du mode connecté, et après le succès de la virtualisation des infrastructures serveurs, d'autres méthodes de virtualisation ont progressivement émergé.

II.2.3.2 Les solutions d'infrastructure de bureau virtuel (Virtual Desktop Infrastructure)

Apparue en 2006 avec la popularisation de la virtualisation des serveurs, cette technologie est au cœur des discussions et en plein essor d'après Gartner en 2009. Le concept est de stocker et d'exécuter au sein de serveurs centraux les postes de travail ainsi que leur architecture dans des machines virtuelles *(VM)*, afin d'optimiser leur fonctionnement. L'accès à distance se fait depuis un poste client similaire à celui évoqué sur le SBC sauf qu'ici le concept va encore plus loin en virtualisant, cette fois-ci, l'ensemble « système et applications » comme illustré ci-dessous :

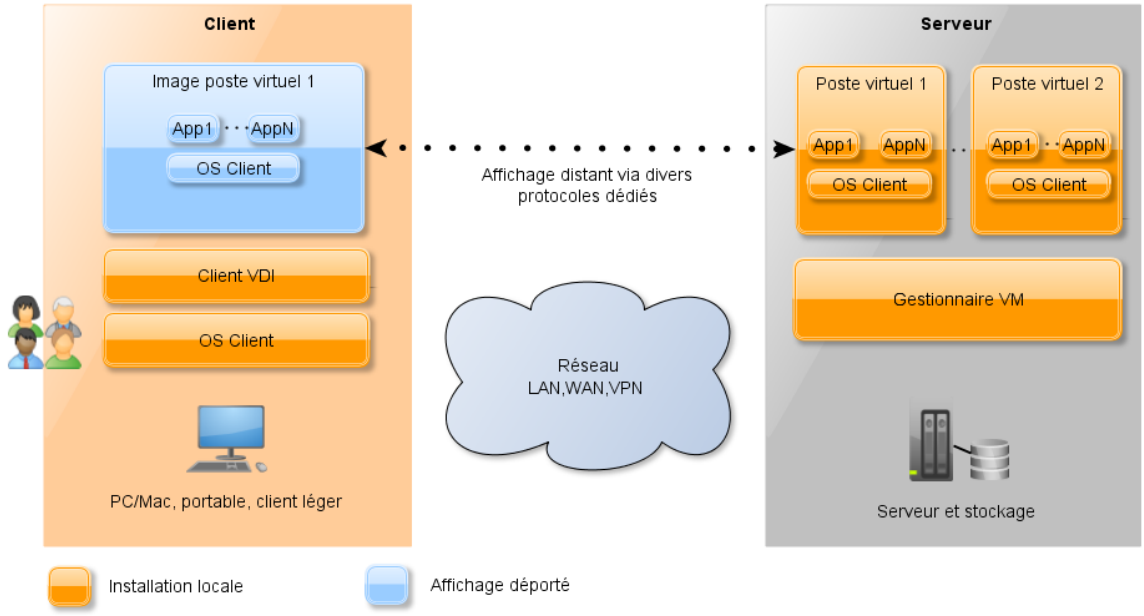


Figure 26 - Fonctionnement de VDI

VDI apporte encore plus de souplesse à la fois aux équipes informatiques et aux utilisateurs. Un ingénieur système peut par exemple provisionner une image prédéfinie à une ou plusieurs salles de TP grâce à quelques manipulations ou offrir le choix d'un environnement Windows et Linux tout aussi facilement à une population d'utilisateurs. Les données des images pouvant être persistantes ou non (très utile pour des TP), les VM sont accessibles depuis n'importe quel équipement. VDI peut également être utile pour déployer simplement et rapidement des images sur des machines isolées n'ayant pas de techniciens sur site.

Autre avantage indéniable de VDI, l'usager a l'impression de travailler avec un environnement de travail semblable à celui utilisé localement sans la contrainte induite par un poste dédié. L'utilisation du poste virtuel étant très proche du poste physique, l'utilisateur ne subit que peu de changements avec une très grande accessibilité. A titre d'exemple d'utilisation de VDI dans un environnement universitaire, citons le cas de l'université Rennes 2 qui a entrepris, depuis 2008, la démarche de virtualiser une partie de ses postes de travail.

La sécurisation des systèmes et des données des usagers est encore améliorée puisque plus aucune donnée sensible n'est stockée sur le poste de travail. Celui-ci se banalise d'ailleurs complètement et sa gestion est simplifiée à l'extrême. Sa durée de vie est même largement prolongée car son utilisation n'est plus du tout liée à ces performances matérielles. La grande souplesse de VDI associée à sa haute disponibilité font d'ailleurs de cette solution un point clé des projets de PRA ou PCA.

Bien que très séduisant, VDI ne s'affranchit pas de quelques inconvénients qui ralentissent son adhésion massive aussi bien dans le secteur privé que public (IDC, 2010). Ces principaux défauts sont clairement le coût et le dimensionnement de l'infrastructure serveurs. Même si on rationalise le stockage en dédupliquant les données, celui-ci reste sensible d'autant plus que l'infrastructure devient hautement critique, le paramétrage et l'optimisation étant loin d'être triviaux. Et malgré l'argumentaire commercial longtemps mis en avant, il est actuellement constaté que le coût global reste bien trop souvent plus élevé qu'une infrastructure classique sur postes physiques. Autre point à prendre en considération, VDI créé une très forte dépendance, sur plusieurs années, avec l'éditeur de la solution qui impose alors ses évolutions, y compris tarifaires, quand bon lui semble...

VDI malgré ces grands attraits, un peu enjolivés, il est vrai, par un discours des éditeurs pas toujours très transparent a du mal à s'implanter largement. La tendance depuis quelques temps est d'ailleurs de coupler la plupart des solutions évoquées ici au sein d'une même offre, permettant ainsi une adhésion progressive. Les grands acteurs du domaine proposent désormais des suites VDI associant : mode connecté et déconnecté à base d'hyperviseur client, publication ou virtualisation d'applications et streaming (d'OS et/ou d'applications) pour apporter encore plus de souplesse et d'optimisation notamment sur la gestion du stockage.

La technologie est-elle donc intéressante pour nos établissements ? La réponse n'est évidemment pas simple. Hormis le coût global de la solution sur plusieurs année qui sous-entend de connaître précisément les coûts de possession de nos parcs, il est également indispensable d'un point de vue technique d'avoir à disposition une équipe d'ingénieurs système et réseau aguerrie à ces technologies et qui surtout peut maintenir efficacement ce service central devenu hautement critique. Autant la virtualisation des serveurs a été un processus naturel pour les équipes techniques, autant la virtualisation du poste client est confronté à des obstacles structurels bien plus importants.

On peut se demander si la souplesse apportée par VDI, notamment la facilité de migration vers Windows 7, a une réelle valeur ajoutée par rapport aux contraintes (coûts, criticités notamment) ? Cela est à étudier finement au cas par cas mais pour des établissements comme le nôtre avec des équipes informatiques éclatées sur plusieurs sites, ayant principalement des compétences au niveau du poste client, et avec une équipe centrale d'ingénieurs systèmes réduite, cette solution ne semble actuellement pas envisageable.

II.2.4 Scénarios d'utilisation

Après avoir dressé un état de l'art du domaine, nous avons approfondi ces technologies aux travers de cinq scénarios d'utilisation dans un milieu universitaire. Pour chaque solution, nous avons procédé à un maquettage rapide et à une batterie de tests sur des machines types. Concernant VDI, j'ai assisté à une journée de formation et de démonstration chez Citrix à Paris. Voici les cinq scénarios que nous avons joués :

- « Station de calcul » : poste fixe avec utilisation intensive de logiciels de PAO/CAO/SIG...
- « Poste pédagogique » : utilisation de logiciels bureautiques, calculs légers et ponctuels par les étudiants.
- « Poste bureautique » : poste type utilisé par les personnels administratifs.
- « Mobilité » : un enseignant ou chercheur nomade se servant d'un ordinateur portable sur son lieu de travail et à domicile de façon égale.
- « Hyper-mobilité » : miniportables, téléphones intelligents et tablettes tactiles.
- « Coûts » : pour chaque solution, nous avons donné un ordre d'idée du coût de revient d'un poste informatique, incluant les licences et l'infrastructure technique nécessaire. Cette échelle va du plus abordable « + », au plus onéreux « +++ ».

	Station de calcul	Poste pédagogique	Poste bureautique	Mobilité	Hyper-mobilité	Coûts
Déploiement WIM	++	++	++	++	-	+
Streaming d'OS	+	++	++	-	-	++
Hyperviseur client	++	++	++	++	-	++
SBC	-	+	+	++	++	++/+++
VDI	-	++	++	++	++	+++

Figure 27 - Etude des scénarios du poste client

II.2.5 Conclusion de l'étude

D'année en année, nous constatons que les habitudes de nos utilisateurs évoluent. D'un poste de travail unique et fixe, nos usagers sont devenus mieux équipés et surtout plus mobiles. A moyens humains constants voire décroissants, les services informatiques doivent gérer un nombre croissant de machines et de profils applicatifs tout en essayant de proposer un niveau de service équivalent quel que soit la méthode d'accès. L'approche est désormais plus centrée sur l'utilisateur, son environnement de travail, ses logiciels que sur l'ordinateur en lui-même. Pour tenter de résoudre cette équation, nous avons étudié et testé différentes technologies qu'elles soient installées sur la machine cliente ou utilisées à distance.

Nous ne pouvons que constater qu'il n'existe pas une réponse universelle concernant la gestion du poste de travail. L'infrastructure de bureau virtuel semble séduisante en virtualisant l'intégralité du poste client mais elle cache des coûts considérables aussi bien sur l'infrastructure à déployer que sur son maintien par une équipe d'ingénieurs systèmes expérimentés dans de multiples domaines. Sa mise en place est donc à étudier au cas par cas dans chaque établissement.

Une piste possible suggère une combinaison de plusieurs technologies afin de répondre aux profils d'utilisation les plus courants dans les universités. On pourrait par exemple profiter du renouvellement d'un parc informatique pour installer un hyperviseur client sur les équipements et le compléter avec un produit du type SBC. Cette solution permettrait de gérer de façon centrale non seulement les machines des salles informatiques, les ordinateurs fixes et portables tout en diminuant considérablement les tâches d'administrations des équipes techniques. Par ailleurs, les clients les plus mobiles ou les accès à distance disposeraient d'un panel de logiciels grâce à un service de publication d'applications.

Le coût des licences et la maintenance associée à cette approche représente cependant un important écueil. A titre d'exemple, une licence d'hyperviseur client coutait 76 € HT/poste, à associer à une maintenance annuelle de 34 € HT/poste. Cette technologie appliquée aux seuls 2700 postes pédagogiques reviendrait donc à près de 300000 € sur le périmètre de l'ex-UPVM la première année, puis à 92000€ les années suivantes.

Néanmoins, des alternatives plus économiques existent comme l'utilisation de solutions basées sur le format WIM de Microsoft. Ce nouveau format de capture des images permet un déploiement optimisé des postes de travail tout en réduisant le cycle de production des postes clients. Bien entendu, cette solution possède des limites puisqu'elle ne s'adresse qu'aux

environnements purement Microsoft. J'ai assisté à une démonstration de cette technologie lors des Microsoft Techdays à Paris début 2011 et cette solution m'avait paru prometteuse. Par ailleurs, dans un contexte de restrictions budgétaires, cette piste a définitivement retenu mon attention et c'est cette technologie que j'ai retenue dans le cadre du projet de production des postes clients.

II.3 Lancement du second projet

II.3.1 Le choix d'un outil Microsoft

Le format WIM est exploité par trois solutions Microsoft pour la production du poste de travail. Le choix d'un outil de déploiement est dicté par le nombre de postes clients à installer selon les recommandations de Microsoft :

	High-Touch avec média (DVD…)	High-Touch avec image WIM	Lite-Touch	Zéro-Touch
Niveau de compétence	Informaticien généraliste	Professionnel de l'informatique	Professionnel de l'informatique avec expérience en déploiement	Professionnel de l'informatique, expert en déploiement
Nombre de postes client	<100	100-200	200-500	>500
Infrastructure	Petits réseaux non gérés	Petits réseaux	Réseaux gérés Environnement Windows Server	Réseaux gérés Environnement Windows Server Configuration Manager
Interaction avec l'utilisateur	Déploiement manuel	Déploiement manuel	Interaction limitée au lancement de l'opération	Totale automatisation
Prise en charge des applications	Installées manuellement	Installées manuellement	Installées automatiquement	Installées automatiquement
Coûts	+	+	++	+++

Tableau 5 - Solutions basées sur le format WIM

Déploiement « High-Touch » avec image standard : ce scénario est adapté aux parcs informatiques de 100 à 200 ordinateurs. Il est basé sur la création d'une image WIM et d'un fichier de réponse. Un informaticien doit exécuter cette procédure sur chaque machine, la rendant inadaptée à grande échelle. Nous passons volontairement sur le scénario « High-Touch » avec média standard à destination des petits réseaux non gérés.

Stratégie « Lite-Touch » : Elle est adaptée pour un environnement de 200 à 500 ordinateurs et s'appuie sur le programme Microsoft Deployment Toolkit (MDT). Cette alternative ne demande qu'une faible interaction lors de son initialisation. Par ailleurs, l'administrateur peut écrire ses propres scripts et utiliser une base de données Sql Server Express pour automatiser en profondeur le processus. En pratique, cette méthode peut être utilisée pour plus de 500 machines.

Solution « Zéro-Touch » : Elle est conseillée sur des parcs de plus de 500 postes et s'appuie sur Configuration Manager dont la licence est payante. Elle nécessite donc une architecture appropriée avec des serveurs redondants. Le déploiement est alors entièrement automatisé et lancé à distance par l'équipe technique.

Nous avons sélectionné la suite Lite-Touch avec MDT 2012 qui correspondait bien à notre besoin puisque nous n'utilisons pas Configuration Manager dans notre environnement de travail. L'infrastructure demandée est économique puisqu'un seul serveur d'entrée de gamme suffit pour déployer les postes clients.

De plus, l'interface de l'application est claire et une documentation abondante est disponible pour une mise en production rapide. L'utilisation de séquences de tâches est un point clef dans le programme, non seulement pour capturer l'image initiale, mais également pour la déployer sur les postes cibles. Grâce à ce dispositif et depuis la version 2008, un paramétrage en profondeur de Windows est possible (Comvalius, 2009).

Concernant les logiciels, ils peuvent être installés sur l'image référence (image dite « épaisse ») ou de façon silencieuse lors du déploiement de l'image sur le poste client (image dite « fine »). On peut également choisir de capturer les applications les plus critiques dans l'image initiale, puis installer les divers utilitaires ultérieurement (image dite « hybride »). C'est la stratégie que nous avons retenue pour notre environnement. Concernant les périphériques qui ne seraient éventuellement pas reconnu lors de l'installation, il est possible de créer sur le serveur Lite-Touch une collection de pilotes qui seront ensuite automatiquement injectés lors de la restauration de l'image. Nous reviendrons sur ces fonctionnalités dans les lots spécifiques.

II.3.2 Définition des livrables

Cette étude détaillée nous a permis de sélectionner la solution Microsoft la plus adaptée à nos besoins et de définir les livrables du projet. Pour cela, j'ai utilisé l'approche Work Breakdown Structure ou WBS pour décomposer le projet en livrables simples et fonctionnels. Ce travail a été effectué de façon collaborative lors de la première réunion d'équipe. L'objectif était d'identifier les étapes et sous-étapes clefs afin de de faciliter la compréhension du projet, son suivi, ainsi que le travail à fournir, les coûts et délais engendrés. Par ailleurs, pour plus de facilité, la figure ci-dessous illustre les livrables principaux. Le détail figure en annexe 2.

Codification et tâches		
1 Production du poste de travail		
	1.1 Piloter le projet	
		1.1.1 Suivi et animation du projet
		1.1.2 Rédaction de la documentation
	1.2 Créer un prototype	
		1.2.1 Spécification d'une infrastructure réseau
		1.2.2 Spécification d'une infrastructure serveur
		1.2.3 Intégration du serveur MDT
	1.3 Gérer les matériels	
		1.3.1 Spécification d'une méthode d'intégration
		1.3.2 Intégration des pilotes
	1.4 Gérer les applications	
		1.4.1 Spécification d'une méthode d'intégration
		1.4.2 Validation des applications usuelles
		1.4.3 Intrégration des logiciels
	1.5 Mise en production	
		1.5.1 Spécification d'une image Windows 7
		1.5.2 Production des postes clients

Figure 28 - Lotissement du projet

Pour chaque lot, nous allons décrire les objectifs attendus, les durées planifiées et les ressources affectées.

II.3.2.1 Piloter le projet

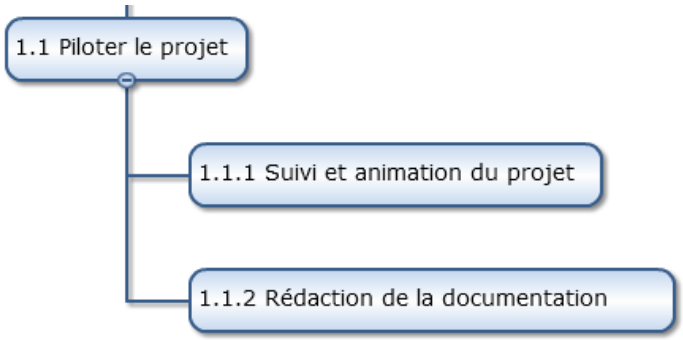


Figure 29 - Lot 1

J'ai choisi de faire apparaitre cette étape car elle perdure tout au long de la vie du projet. Je l'estime à 10 jours/homme en comptant les réunions et la rédaction de documentations.

Par ailleurs, les participants étant répartis entre Nancy et Metz, j'ai déployé plusieurs outils afin de faciliter les échanges :

- Une liste de diffusion dn-mdt-projet@univ-lorraine.fr utilisable par toute l'équipe. Cette adresse a ainsi permis de faire des points réguliers par mails.

- Le site Wikidocs de l'Université de Lorraine. Basé sur le logiciel Confluence, ce puissant outil permet de créer et partager du contenu entre les utilisateurs. Un espace documentaire a été dédié au projet sur lequel l'équipe s'est appuyée pour diffuser les documentations, procédures et suivi du projet.

II.3.2.2 Créer un prototype

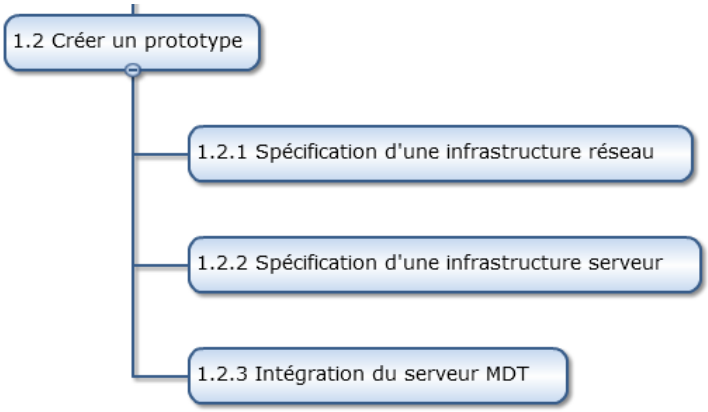


Figure 30 - Lot 2

L'objectif du livrable est de produire un prototype fonctionnel du serveur MDT ainsi que de valider la procédure de déploiement d'un poste sous Windows 7 et son intégration dans le nouveau système d'information. L'équipe projet a choisi de ne pas centraliser cette maquette, mais plutôt de la répliquer sur chaque site participant. Au final ce sont donc cinq installations autonomes de MDT qui ont été déployées localement, en s'appuyant sur une méthodologie commune diffusée sur Wikidocs.

Ayant une expérience du format WIM et de MDT en 2011 lors de mes recherches empiriques, je me suis proposé pour animer ce lot. Ma première préoccupation a donc été une recherche documentaire sur le sujet afin que les membres de l'équipe se familiarisent avec cette nouvelle technologie. J'ai en particulier utilisé les vidéos prévenant des Techdays Microsoft 2012 sur le sujet.

Les tâches suivantes concernaient la spécification des infrastructures réseaux et serveurs nécessaires au bon fonctionnement du système de déploiement. Nous nous sommes appuyés sur les recommandations de Microsoft pour déployer un environnement fonctionnel. Ces prévisions nous ont permis d'estimer plus finement le coût du projet ainsi que les composants matériels et logiciels requis, comme l'installation d'un serveur DHCP et WDS.

L'étape suivante concernant l'installation et le paramétrage de MDT. Cet outil est en fait un environnement, un « framework » de déploiement, constitué d'une multitude de briques de plus bas niveau, en particulier le kit de déploiement et d'évaluation Windows (ADK). Là encore, nous avons suivi les bonnes pratiques du domaine afin d'arriver à nos objectifs. La production d'un poste de travail sous Windows 7 avec le serveur MDT clôture ce lot.

Estimée à 40 jours/homme, cette partie a été décisive dans la suite du projet puisqu'elle a permis à toute l'équipe de se former sur l'outil MDT et sur les nouveaux concepts de production du poste de travail.

II.3.2.3 Gestion des matériels

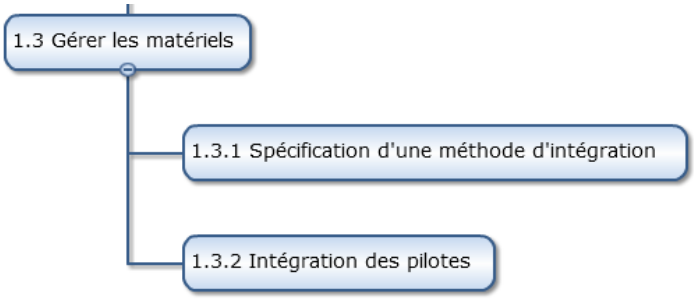


Figure 31 - Lot 3

Nous avons vu dans l'étude précédente que nos utilisateurs sont de mieux en mieux équipés et possèdent désormais plusieurs ordinateurs au profil matériel différent. Cette tendance complexifie le processus de production du poste de travail pour les équipes informatiques qui utilisent un système de déploiement basé sur l'image des secteurs du disque ou de la partition. En effet, il faut soit une image dédiée par configuration, soit inclure une large bibliothèque de pilotes de référence dans l'image de base.

A l'opposé, le format WIM et les outils de déploiement de Microsoft révolutionnent cette façon de procéder puisque l'image est indépendante de l'architecture matérielle. L'objectif de ce lot est de spécifier la configuration la plus efficace pour gérer les pilotes, puis de tester cette procédure sur les configurations sur les plus répandues à l'Université. Herve Hounzandji de l'IUT de Metz, s'est chargé de la coordination et de l'animation de ce lot. Estimée à 10 jours/homme, 3 personnes ont collaboré à cette activité.

II.3.2.4 Gérer les applications

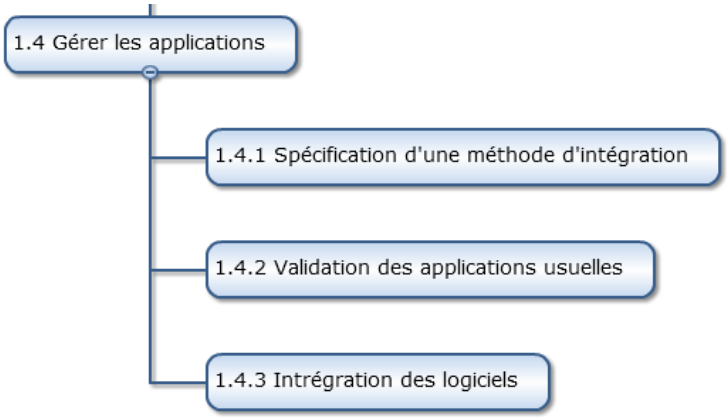


Figure 32 - Lot 4

Avec une approche classique, les services informatiques installaient les logiciels usuels ainsi que les applications métiers dans le système de référence. Une image était ensuite générée en copiant les secteurs du disque ou de la partition. Bien que cette solution était fonctionnelle, elle souffrait de deux inconvénients majeurs :

- Une fois capturée, l'image système était figée et il était impossible de mettre à jour les logiciels sans refaire une itération ou sans utiliser un système de déploiement tiers.

- Par ailleurs, l'installation des logiciels n'était pas centralisée et à chaque nouvelle image, il fallait procéder à une nouvelle installation des logiciels. Malgré une

certaine automatisation, la gestion des logiciels était rigide et chronophage pour le service informatique.

La première tâche consistait donc à recenser les logiciels les plus utilisés ainsi que les logiciels métiers à déployer comme Matlab ou la suite Adobe. Lors de cette étude, nous avons ciblé une quarantaine de logiciels différents puis nous avons ensuite validé la compatibilité de chaque programme avec Windows 7.

Contrairement à une approche traditionnelle, MDT permet un déploiement dynamique et automatique des applications dans l'environnement utilisateur. Les logiciels sont ainsi installés lors du premier démarrage du poste client. Cependant, cette fonctionnalité nécessite un important travail puisqu'il faut auparavant configurer chaque programme afin qu'il s'installe de façon silencieuse, sans interaction avec l'utilisateur.

M. Yann *Walterthum* de l'UFR des Sciences Fondamentales et Appliquées, s'est proposé pour animer ce lot pour lequel sept personnes participaient. Cette étape a été estimée à l'origine à 40 jours/homme.

II.3.2.5 Mise en production

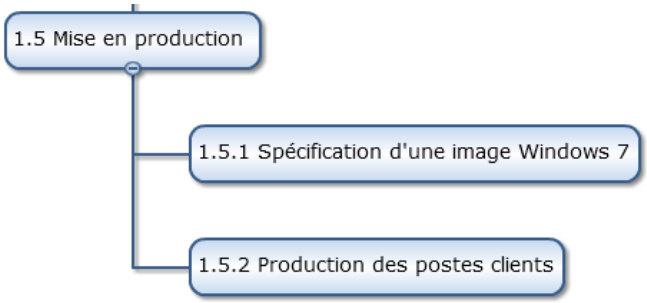


Figure 33 - Lot 5

La dernière activité concerne la mise en production du système pour les composantes qui le souhaitent. Comme spécifié dans les objectifs du projet, il n'est ici pas question d'imposer une solution technique pour l'Université de Lorraine, mais de donner un canevas technique aux structures souhaitant optimiser leur gestion du poste de travail. Nous avons consigné et archivé tout le travail fourni sur la plateforme collaborative Wikidocs. Il suffit ainsi de suivre les documentations techniques pour déployer cette technologie.

La mise en production du système étant laissée à la discrétion de chaque responsable de site, nous n'avons pas indiqué de gestionnaire pour cette étape. La durée du lot était estimée à 20

jours/homme, mais elle diffère sur chaque site en fonction des contraintes locales, du nombre de postes à installer et des logiciels à déployer.

II.3.3 Gestion des coûts

Un projet pouvant être vu comme un équilibre entre les objectifs, les coûts et les délais, nous allons préciser ces deux derniers axes. Dès l'étude préalable, je savais que la contrainte liée aux coûts serait très forte. Les budgets informatiques étant en diminution à la fois dans les composantes mais aussi au niveau de la Direction du Numérique, je savais qu'une solution coûteuse comme l'hyperviseur client serait vouée à l'échec, bien que techniquement plus performante. Or la solution de Microsoft, bien que propriétaire, est gratuite.

Cependant, la mise en place des serveurs et le coût des licences Windows 7 engendrent des dépenses :

- Infrastructure serveur : un serveur DHCP et un serveur de déploiement sont nécessaires. Microsoft conseille deux machines distinctes. Les entités disposant d'une infrastructure virtuelle pourront pleinement profiter de cette technologie. Dans le cas d'une installation physique et en suivant les recommandations de Microsoft, deux serveurs d'entrée de gamme comme le modèle R320 suffisent. Nous avons estimé le coût à 2500 € HT avec les marchés publics.

- Licences Windows : chaque machine migrant vers Windows 7 doit s'assurer de posséder une licence adéquate. Cependant, grâce aux accords avec Microsoft et à l'existence du programme Dreamspark à destination de l'enseignement supérieur, les établissements peuvent utiliser Windows 7 gratuitement sur les machines pédagogiques. La situation est cependant différentes pour les administratifs et les enseignants puisqu'une licence doit être achetée auprès du détenteur des marchés. Concrètement, il faut compter 52 euros HT par poste migrant vers Windows 7.

Les coûts sont donc constitués d'une partie fixe, les serveurs de déploiement, et d'une partie variable, les licences :

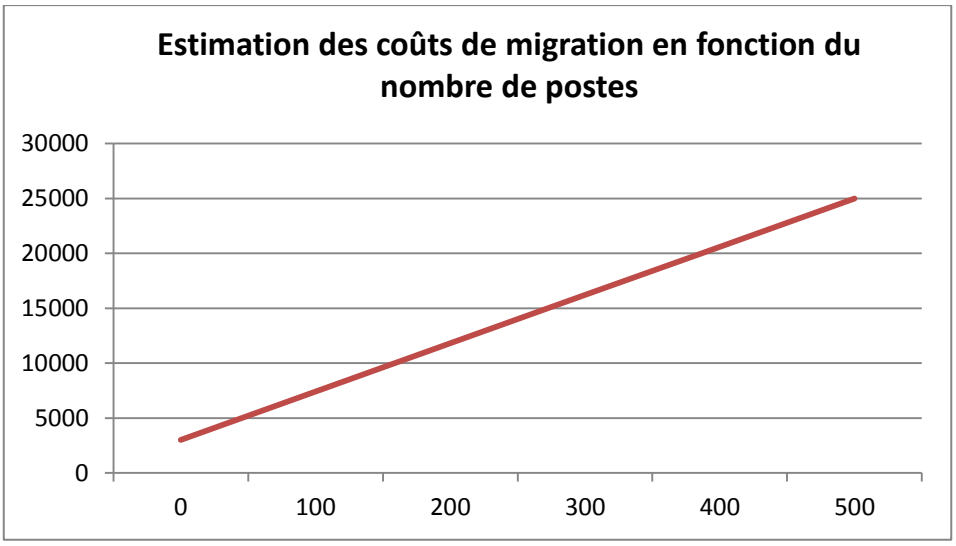


Figure 34 - Estimation des coûts du projet

II.3.4 Gestion des délais

L'étude de la charge du projet a été facilitée par les multiples conférences Microsoft sur le sujet. Estimée à 120 jours/hommes, plusieurs semaines étaient tout d'abord nécessaires pour que l'équipe se forme sur ce nouvel outil. Par ailleurs, le groupe savait également que la partie dédiée à la gestion des applications serait particulièrement longue afin de tester l'installation de chaque logiciel. C'est un risque que nous avons identifié comme nous le verrons ultérieurement.

II.3.5 Ordonnancement et planning

A partir du découpage du projet en lots et tâches, nous pouvons produire l'organigramme ci-dessous :

Codification et tâches			Durée en jours			Responsable et participants
1 Production du poste de travail			120			F, Y, N, V, M, H, O, P
	1.1 Piloter le projet			20		F, Y, N, V, M, H, O, P
		1.1.1 Suivi et animation du projet			10	
		1.1.2 Rédaction de la documentation			10	
	1.2 Créer un prototype			30		F, Y, N, V, M, H, O, P
		1.2.1 Spécification d'une infrastructure réseau			10	
		1.2.2 Spécification d'une infrastructure serveur			10	
		1.2.3 Intégration du serveur MDT			10	
	1.3 Gérer les matériels			20		V, H
		1.3.1 Spécification d'une méthode d'intégration			10	
		1.3.2 Intégration des pilotes			10	
	1.4 Gérer les applications			30		F, Y, N, M, O, P
		1.4.1 Spécification d'une méthode d'intégration			10	
		1.4.2 Validation des applications usuelles			10	
		1.4.3 Intrégration des logiciels			10	
	1.5 Mise en production			20		Gestion locale
		1.5.1 Spécification d'une image Windows 7			10	
		1.5.2 Production des postes clients			10	

Figure 35 - WBS, lots et tâches

Nous avons ensuite modélisé l'ordonnancement du projet avec GanttProject, le chemin critique figurant en jaune.

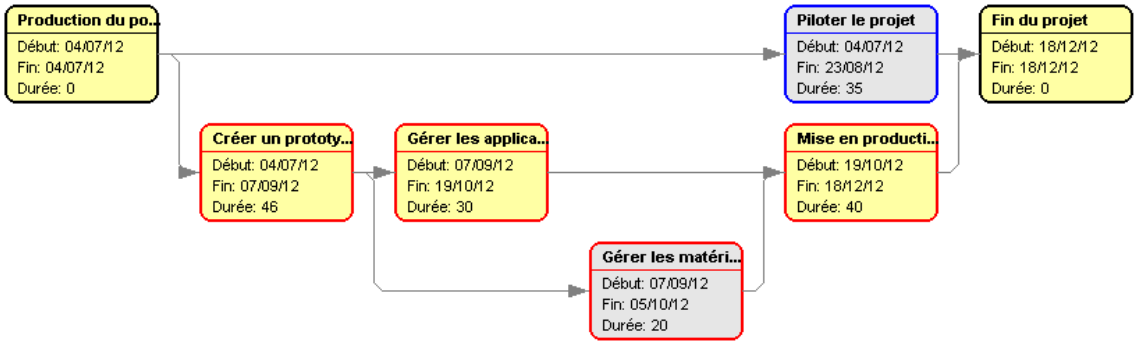


Figure 36 - Diagramme de PERT

Nous avons ensuite généré un diagramme de Gantt basique. Il s'agit ici de la version initiale, tenant compte des congés d'été :

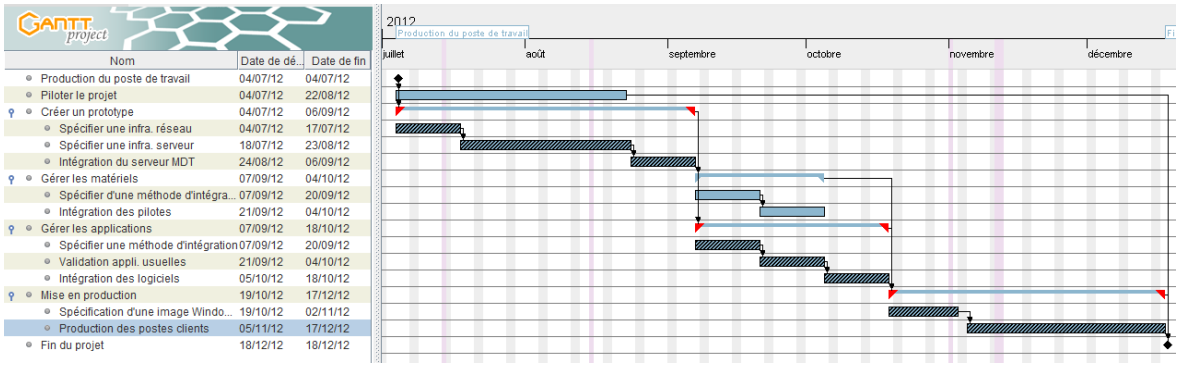


Figure 37 - Diagramme de Gantt

II.3.6 Evaluation et gestion des risques

Lors de la première réunion d'équipe, nous avons également évalué les risques pouvant impacter sur le projet en adoptant une méthodologie simple. Cette notion étant nouvelle pour la majorité des participants, nous avons procédé à un brainstorming afin de dresser les facteurs de risques pouvant impacter le projet. Ces facteurs peuvent être catalogués en cinq grandes catégories : organisationnelle, technique, financière, juridique ou humaine.

Nous avons ensuite quantifié ces risques en tenant compte de leur impact sur le projet et de leur probabilité d'apparition. Pour cela, nous avons affecté deux notes de 1 à 4 pour chaque scénario évoqué. Par exemple, un impact de 4 compromet l'existence même du projet. A l'opposé, une faible probabilité d'apparition d'un problème est notée 1.

Le but de cette évaluation est de définir la criticité des risques. La criticité est le produit de la probabilité de son occurrence par les impacts du risque. A partir de ces éléments, nous avons construit une matrice de criticité. Nous avons ensuite déterminé si ce risque était

acceptable ou non, afin de déterminer les priorités à adresser. L'objectif est ici d'identifier au mieux les problèmes pour ensuite les maîtriser.

Par ailleurs, ce projet restant modeste, je ne voulais pas surcharger sa gestion en multipliant les indicateurs et les procédures inutiles. Ainsi, en tenant compte de la loi de Pareto, qui indique que 20% des causes sont responsables de 80% des conséquences, nous avons retenu trois facteurs de risques, deux techniques et un organisationnel.

II.3.6.1 Risque 1 : Compatibilité applicative et Windows 7

Le premier risque technique concerne la compatibilité des applications avec Windows 7. En effet, nous devons nous assurer que les applications critiques sont compatibles avec ce système d'exploitation. Nous nous sommes donc appuyés sur le site de l'éditeur ainsi que sur les bases de connaissances Microsoft[21] et son outil Application Compatibility Toolkit ou ACT. Cependant que faire avec une application incompatible avec Windows 7 ? Certains logiciels indispensables pour l'enseignement et la recherche ne sont parfois que compatibles avec Windows XP. De la même façon, l'éditeur peut avoir disparu rendant d'éventuelles mises à jour impossibles.

Afin de répondre à cette éventualité, l'équipe a apporté deux réponses techniques. La première consiste en l'utilisation des techniques de virtualisation de systèmes d'exploitation telles que VirtualBox ou Vmware Workstation. En utilisant les ressources matérielles de l'ordinateur, appelé système hôte, cette technologie permet la création d'un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation nommés systèmes invités. Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur. Enfin, les systèmes invités n'interagissent pas directement avec le système hôte ce qui permet l'exécution des logiciels incompatibles au sein d'une machine virtuelle sous Windows XP.

Le deuxième élément de réponse concerne la virtualisation d'applications. Elle est basée sur une couche d'abstraction qui isole les logiciels et le système d'exploitation local. Les programmes vont se présenter sous la forme d'une bulle applicative qui va contenir tous les fichiers de données et de configurations utilisés par l'application comme indiqué sur la figure 38.

[21] http://www.microsoft.com/fr-fr/windows/compatibility/win7/CompatCenter/Home?Language=fr-FR

Cette bulle s'exécutera localement dans un environnement totalement virtualisé préservant ainsi les paramètres de l'ordinateur. On peut désormais faire cohabiter plusieurs programmes incompatibles entre eux sans jamais les installer sur la machine hôte.

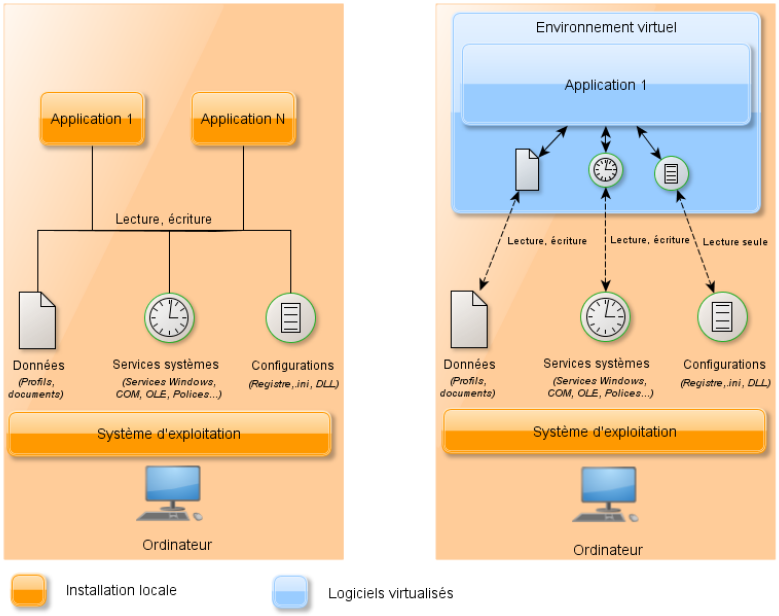


Figure 38 - Différences entre une application classique à gauche et virtualisée à droite

Cette technologie permet par ailleurs de déployer et migrer rapidement les logiciels sur les postes de travail. En 2008, Gartner indique que les applications virtualisées peuvent réduire de 60 % le coût lié au test, à la création de modules et à la prise en charge d'une application. Suivant la solution retenue, l'installation d'un client peut être nécessaire sur le poste de travail afin de contacter le serveur d'applications. De la même façon, il existe plusieurs modes d'accès à notre paquet virtuel, présenté sous la forme d'un fichier exécutable. Du simple partage réseau, à la publication d'applications en passant par le streaming à la demande et à la mise en cache, différentes options sont envisageables.

II.3.6.2 Risque 2 : Difficulté d'intégration des logiciels

Le second risque technique que nous avons défini concerne l'intégration des logiciels lors du déploiement. L'objectif du projet est de fournir une image système flexible, pouvant être déployée sur le poste client de façon dynamique et modulaire qu'il s'agisse des pilotes matériels ou des applicatifs. Cette technique nécessite un important travail en amont au niveau des logiciels afin que le déploiement se fasse de façon silencieuse, sans interaction avec l'utilisateur lors de l'installation du programme.

Malheureusement, il n'existe pas de procédure standardisée pour cette étape et chaque logiciel dispose de son propre mode opératoire. Il faut donc pour chaque logiciel identifier la méthode à employer en s'appuyant sur le site de l'éditeur ou sur des bases de connaissances disponibles sur Internet comme le site ITNinja[22] racheté par DELL récemment. En effet, toutes les solutions de déploiement, libres ou propriétaires, s'appuient sur ce principe d'installation automatisée.

Cependant, nous savions de façon empirique que certains logiciels ne permettaient pas une installation silencieuse. Dès lors, comment faire pour automatiser le processus de déploiement applicatif ?

Nous avons identifié deux réponses techniques face à cette problématique. La première utilise la virtualisation d'applications que nous avons étudiée au paragraphe précédent. La deuxième solution s'appuie sur le système d'installation standardisé Microsoft, pourtant le nom de Windows Installer. Apparu avec Windows 2000, le service Windows Installer offre une interface entre le processus d'installation et le système d'exploitation. Toutes les actions qui doivent être réalisées pour achever correctement l'installation d'un logiciel transitent par ce service. Pour répondre à ces règles, l'application a seulement besoin de se présenter sous la forme d'un package dont l'extension se termine en .MSI

Le package MSI est en fait une base de données qui contient les informations nécessaires à la réalisation de l'installation. Le service Windows Installer s'occupe ensuite de transmettre ces informations au système qui effectuera alors les actions nécessaires. Cette interface permet d'automatiser et de standardiser les procédures d'installation, permettant ainsi de réduire les problèmes courants d'installation (Darwin & Moskowitz, 2002).

Le fichier exécutable (msiexec.exe) ouvre le fichier MSI contenant les informations contenues dans le package, les lit et exécute les actions à réaliser. D'autres fonctions, telles que le redémarrage de l'ordinateur, la vérification de l'espace disque disponible ou les règles de gestion de version des fichiers, sont gérées par le moteur de Windows Installer. Il peut également contenir les ressources installables (fichiers, clés de registre…) comme l'illustre la figure ci-dessous :

[22] http://www.itninja.com/about

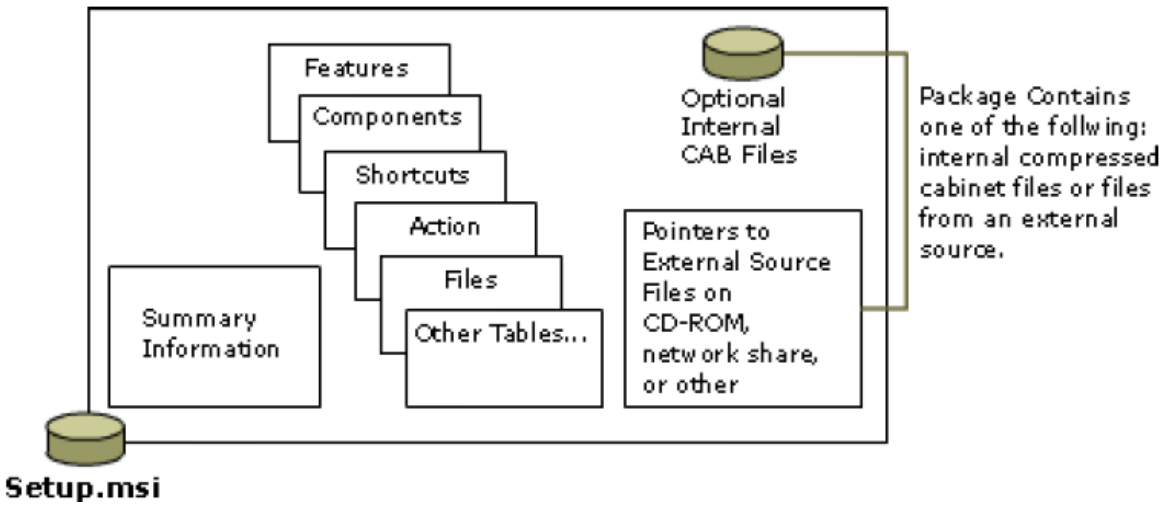


Figure 39 - Fonctionnement d'un fichier MSI

Le déploiement a été grandement facilité en adoptant le format de référence Microsoft et en utilisant des outils permettant de générer un fichier .MSI.

II.3.6.3 Risque 3 : Organisation transverse du projet

Dès le début du projet, l'équipe a évoqué les problèmes de charge de travail. Ce risque organisationnel et humain était particulièrement fort puisque nous lui avons octroyé une criticité de 12 sur 16.

La réalisation du projet se faisait en plus du travail usuel des collègues. Dès le départ, nous savions qu'une charge de travail importante ralentirait la réalisation du projet. Par ailleurs, le lancement du projet coïncidait avec la rentrée universitaire de 2012, une période chargée pour les équipes de proximité.

Nous avons donc évoqué différentes pistes afin de gérer ce risque efficacement. La première alternative consistait dans le renfort de l'équipe projet par des membres supplémentaires voir des stagiaires. Bien qu'efficace, cette approche nous paraissait peu réaliste.

Une autre possibilité consistait à réviser les ambitions du projet. Néanmoins, il me paraissait difficile de réduire le contenu des lots. Les spécifications d'une architecture de déploiement, la gestion des pilotes et des applications sont des phases essentielles dans un projet de migration vers Windows 7.

Enfin, l'option la plus réaliste consistait à allonger les délais. Dès le lancement, nous avons précisé deux dates de fin de projet. L'approche optimiste respectait la planification initiale

avec une réalisation prévue en novembre. Le scénario plus pessimiste repoussait la clôture du projet en février 2013.

II.4 Exécution du projet

Nous avons vu dans la partie précédente le contexte et le plan d'exécution du projet. En tant que responsable de ce projet, je savais que cette vision idéale serait bousculée à plusieurs reprises. Dans cette partie, il me parait intéressant de revenir sur l'exécution du projet, les solutions techniques mises en œuvre par l'équipe, mais surtout de mesurer et analyser les écarts observés en regard de la planification initiale.

II.4.1 Piloter le projet

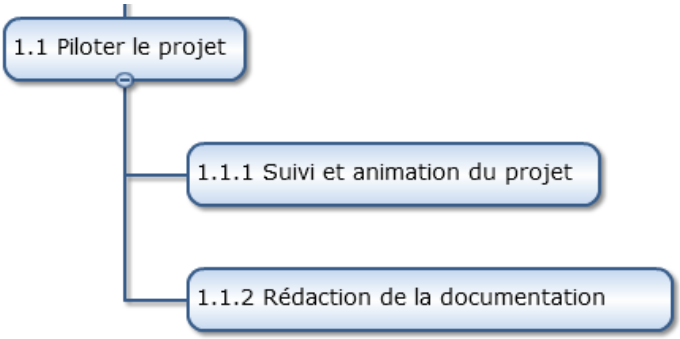


Figure 40 – Exécution du lot 1

En tant que chef de projet, la première difficulté a été de m'assurer de la disponibilité de chaque intervenant. Ayant eu le feu vert de la Direction du Numérique, cette tâche a été facilitée avec les collègues rattachés à cette entité. Concernant les informaticiens de composantes qui ne sont donc pas rattachés à la Direction du Numérique, je me suis assuré que la hiérarchie validait la participation à ce projet en supplément des missions quotidiennes assurées par les agents. Par ailleurs, ce projet permet non seulement d'apporter une réponse à des problématiques techniques, mais il est également enrichissant pour l'agent qui peut élargir ses compétences et enrichir son dossier.

La première réunion du projet s'est tenue en juillet 2012 avec les huit participants. Nous avons fait un tour de table afin d'affiner les attentes de chaque participant. J'ai choisi ce mode d'action afin de m'assurer que l'équipe allait dans le même sens et que nous partagions des objectifs communs. Le projet a été officiellement lancé à cette date, mais n'a vraiment commencé que fin septembre 2012 après la rentrée universitaire.

Afin de gérer efficacement le projet, j'ai utilisé les grandes lignes de la méthodologie PMI, PMBOK. Elle permet un découpage du projet, un suivi des tâches, des coûts, des délais et de

la qualité. Je me suis servi d'un document Excel pour établir la charte projet et assurer le suivi des opérations. Par ailleurs, j'ai utilisé GanttProject pour modéliser le déroulement du projet. Je n'ai pas utilisé d'outils plus élaborés pour deux raisons :

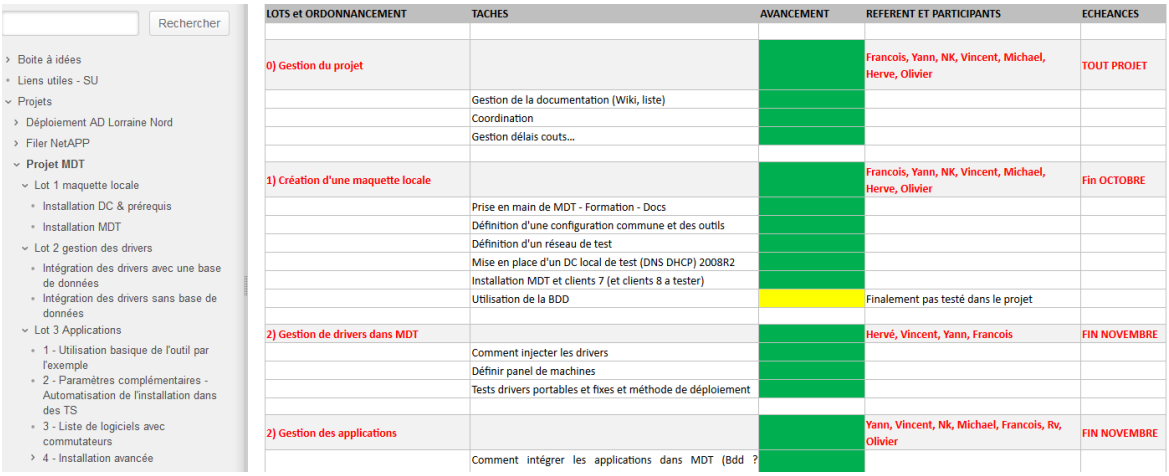
- Nous avions estimé entre 100 et 120 j/h la taille du projet, ce qui correspond à un petit projet selon les critères usuels. Utiliser des outils plus complexes comme Microsoft Projet me paraissait donc peu adapté.

- La gestion de projet étant encore peu répandue à l'Université de Lorraine, je me suis plutôt focalisé sur des outils et méthodes simples. J'ai expliqué mon approche lors de la première réunion en insistant sur les avantages de découper et suivre le projet à l'aide d'un tableur et d'un outil documentaire. J'ai donc volontairement adapté la méthode de gestion de projet qui m'a été enseignée, afin de ne conserver que les composants les plus adaptés.

Au final, le groupe de travail s'est réuni trois fois pendant la durée du projet. Cela peut paraitre peu, mais je devais jongler avec les disponibilités et la charge de travail de chaque participant. Par ailleurs, un participant a quitté le projet en route à la fin de son CDD. Un collègue de l'ex-INPL l'a remplacé en octobre 2012. Cet évènement a provoqué un retard sur le planning initial. Une formation a été dispensée au nouvel arrivant qui a rattrapé le projet en marche. Par ailleurs, nous avons dû revoir la feuille de projet afin de redéfinir les attributions et tâches.

Afin de maintenir une communication efficace au sein de l'équipe, nous avons surtout utilisé les listes de diffusion et le Wiki de l'Université. J'ai également organisé des réunions téléphoniques et des dépannages à distance pour les aspects techniques les plus sensibles. La plateforme Wikidocs de l'Université de Lorraine a joué un rôle majeur. Elle a facilité le travail collaboratif entre les membres et représente véritablement la mémoire du projet.

Bien que le projet soit clôturé, l'espace documentaire, riche d'une quinzaine de pages, continue de s'enrichir des remarques et expérimentations des informaticiens de l'Université de Lorraine. Par ailleurs, il sert de référence aux composantes souhaitant déployer Microsoft Deployment Toolkit dans leur environnement.



LOTS et ORDONNANCEMENT	TACHES	AVANCEMENT	REFERENT ET PARTICIPANTS	ECHEANCES
0) Gestion du projet			Francois, Yann, NK, Vincent, Michael, Herve, Olivier	TOUT PROJET
	Gestion de la documentation (Wiki, liste)			
	Coordination			
	Gestion délais couts...			
1) Création d'une maquette locale			Francois, Yann, NK, Vincent, Michael, Herve, Olivier	Fin OCTOBRE
	Prise en main de MDT - Formation - Docs			
	Définition d'une configuration commune et des outils			
	Définition d'un réseau de test			
	Mise en place d'un DC local de test (DNS DHCP) 2008R2			
	Installation MDT et clients 7 (et clients 8 a tester)			
	Utilisation de la BDD		Finalement pas testé dans le projet	
2) Gestion de drivers dans MDT			Hervé, Vincent, Yann, Francois	FIN NOVEMBRE
	Comment injecter les drivers			
	Définir panel de machines			
	Tests drivers portables et fixes et méthode de déploiement			
2) Gestion des applications			Yann, Vincent, Nk, Michael, Francois, Rv, Olivier	FIN NOVEMBRE
	Comment intégrer les applications dans MDT (Bdd ?			

Figure 41 - Page d'accueil du projet

Le pilotage de ce projet a été vraiment très enrichissant pour moi, non seulement d'un point de vue humain, mais aussi organisationnel et technique. La gestion de projet est un outil indispensable qui selon moi fait la différence entre un projet réussi et un échec. Par ailleurs, un simple document Excel permet de rapidement visualiser les étapes terminées et à venir. Il est facilement compréhensible par l'équipe et facilite les échanges avec les participants et la hiérarchie. Enfin, les cours de gestion de projet dispensés par le CNAM m'ont été d'une aide inestimable dans la réussite de ma mission.

II.4.2 Créer un prototype

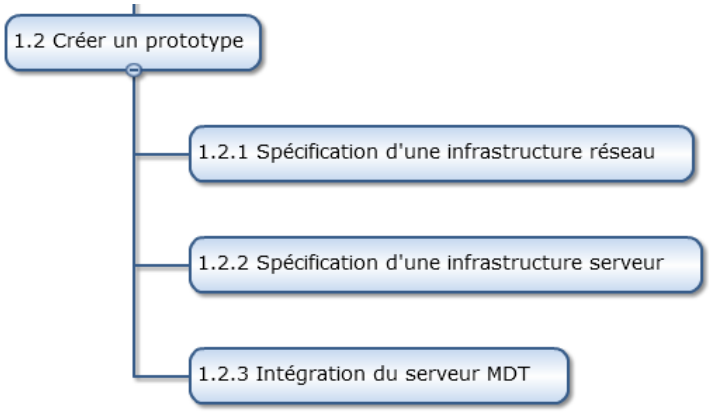


Figure 42- Exécution du lot 2

L'objectif du livrable est de produire un prototype fonctionnel du serveur Microsoft Deployment Toolkit scénario « Lite-Touch » ainsi que de valider la procédure de déploiement d'un poste sous Windows 7 et son intégration dans le nouveau système d'information.

Lancé en septembre 2012, ce lot était particulièrement important puisqu'il représentait la fondation sur laquelle les livrables allaient s'imbriquer. Par ailleurs, étant animateur de cette étape, je devais non seulement m'assurer des spécifications des architectures réseaux et serveurs

mais également de la formation des participants. En effet, nous avions choisi dès le début du projet une maquette décentralisée, propre à chaque composante.

Dès cette phase amorcée, j'ai déposé sur Wikidocs toutes les informations que j'avais collectées lors de mon étude sur le poste client. Les documentations Microsoft sur le format WIM et Microsoft Deployment Toolkit sont particulièrement abondantes et bien réalisées. Des vidéos provenant des conférences Techdays 2012[23] ainsi les documentations officielles[24] ont été particulièrement utiles.

L'équipe s'est ensuite plongée dans les documentations afin de s'assurer des pré-requis logiciels et matériels. Nous nous sommes appuyés sur la virtualisation des serveurs afin de produire un maquettage rapide de la solution technique. En effet, il est facile de revenir en arrière grâce aux « instantanés » ou « snapshot ». Cette technologie, maintenant largement utilisée permet de réduire drastiquement le temps de maquettage. Nous avons procédé par itérations en rajoutant à chaque nouvelle boucle un paramètre supplémentaire, tout en notant le résultat de nos recherches sur Wikidocs. Cette opération a été longue et fastidieuse, car Microsoft Deployment Toolkit est un environnement s'appuyant sur d'autres briques Microsoft.

II.4.2.1 Spécifications réseaux et serveurs

Il me parait peu judicieux de reprendre les documentations Microsoft point par point. Je vais donc seulement évoquer les aspects les plus importants.

Après avoir étudié les documentations et listé les outils nécessaires, nous avons virtualisé un environnement Microsoft sur un réseau dédié, isolé des serveurs de production. Nous avons suivi les recommandations de Microsoft afin de permettre une automatisation des processus de déploiement et une prise en main aisée. Dans ce cadre, l'infrastructure serveur se compose d'au minimum 3 serveurs dotés de services (Finn, Gibson, & Van Surksum, 2011):

- « services de domaine Active Directory » : service d'annuaire Microsoft, il est utilisé par MDT pour vérifier si l'entrée machine existe dans l'annuaire et authentifier les comptes utilisateurs. Notre maquette suit les bonnes pratiques Microsoft et

[23] http://www.microsoft.com/france/mstechdays/programmes/parcours.aspx#DomID=2e8b813d-6afc-48f7-a9ac-527ca7df50e0

[24] http://technet.microsoft.com/fr-fr/windows/dn475741.aspx

comporte deux contrôleurs de domaine afin d'assurer une tolérance aux pannes. Par ailleurs, tous les serveurs mentionnés ci-dessous sont membres du domaine Active Directory.

- DNS ou « Domain Name System » : c'est un service critique, indissociable d'Active Directory. Le serveur DHCP va enregistrer automatiquement et dynamiquement les machines déployées par MDT sur le serveur DNS.

- DHCP ou « Dynamic Host Configuration Protocol » : ce serveur permet d'attribuer de façon automatique une adresse IP à une machine cliente. Il permet une gestion souple des ressources réseaux.

- WDS ou « Windows Deployment Services » : introduit avec Windows 2008, il fournit un système de déploiement automatisé permettant la distribution des images par le réseau.

- MDT ou « Microsoft Deployment Toolkit » : utilisé pour capturer, déployer et paramétrer les images Windows sur les postes clients.

- Un groupe de machines virtuelles clientes, reflétant les caractéristiques matérielles de notre parc informatique.

Lors du maquettage nous avons utilisé 3 serveurs différents sous Windows 2008R2 et nous conseillons de séparer les services et d'affecter un serveur, virtualisé ou non à chaque rôle. Il est cependant possible de regrouper les rôles comme WDS et DHCP sur la même machine. Par ailleurs, les accès nécessaires doivent être positionnés sur les routeurs afin que les serveurs puissent communiquer entre eux lors d'un déploiement sur différentes plages réseaux.

II.4.2.2 Principes de fonctionnement

L'objectif de Windows Deployment Toolkit est d'industrialiser le processus de production du poste client en utilisant l'infrastructure réseau. Cette approche limite l'intervention humaine sur les stations de travail et permet de nettement diminuer les coûts en automatisant le déploiement du système d'exploitation. MDT s'appuie sur le protocole PXE ou « Pre-Boot Execution Environment » pour déployer l'image par le réseau. PXE est une technologie utilisée pour démarrer un ordinateur à distance à travers un réseau et éventuellement installer une image en guise de système d'exploitation. Pour le mettre en œuvre, Microsoft a mis à disposition avec

Windows 2008 le service WDS ou « Windows Deployment Service » destiné à remplacer RIS ou « Remote Installation Service ». Voici le schéma fonctionnel lors du démarrage d'un poste client :

Figure 43- Le boot PXE

Le serveur WDS ne va pas directement charger une image Windows 7 sur le poste client. En fait, il va lancer un environnement Windows minimaliste, appelé WinPE ou Windows Preinstallation Environnement qui est un système d'exploitation Windows basique permettant d'effectuer des actions sur un ordinateur sans avoir démarré le système d'exploitation cible. Ce système est semblable aux distributions de type LiveCD avec un chargement intégral du système en mémoire. Cet environnement spécialement paramétré pour l'outil MDT va nous permettre de déployer notre fichier WIM sur le poste client.

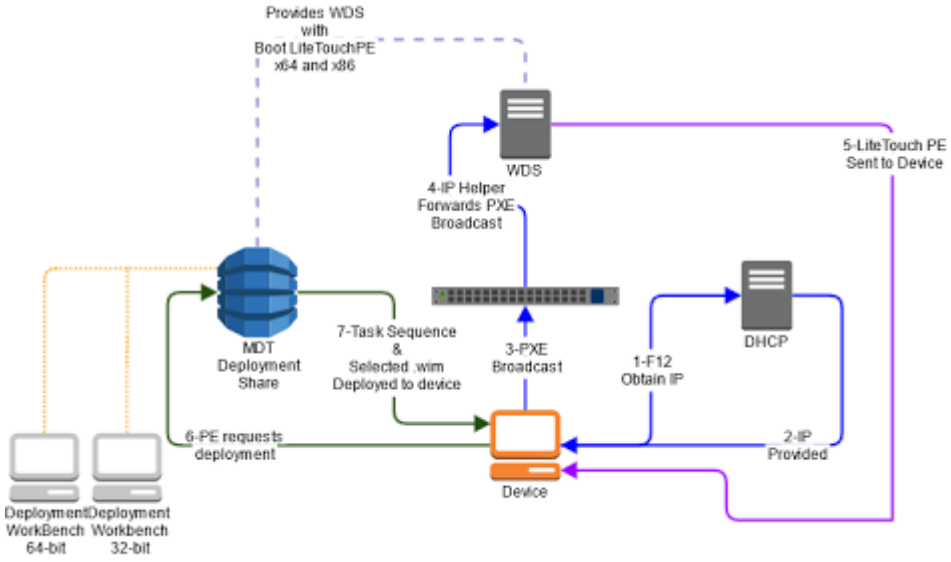


Figure 44 – Communication entre MDT, le client et le serveur DHCP

Après avoir récupéré une adresse IP par le serveur DHCP, le client va charger par le réseau le système WinPE en mémoire vive. Une fois la bonne tâche sélectionnée, l'assistant va

contacter le serveur MDT. Celui-ci va ensuite déployer le fichier WIM correspondant. Bien entendu, l'objectif est un paramétrage en amont afin que le déploiement s'effectue automatiquement, avec le minimum d'interaction humaine. Cette configuration se fait directement sur le serveur MDT comme nous le verrons ultérieurement.

II.4.2.3 Paramétrage de la multidiffusion

La monodiffusion est l'envoi de trafic réseau à un point de terminaison. La multidiffusion est l'envoi de trafic réseau à un groupe de points de terminaison. Seuls les membres du groupe de points de terminaison qui écoutent le trafic de multidiffusion (le groupe de multidiffusion) traitent le trafic de multidiffusion. Tous les autres nœuds ignorent le trafic de multidiffusion.

La figure suivante, provenant de Microsoft, illustre un réseau compatible avec la multidiffusion :

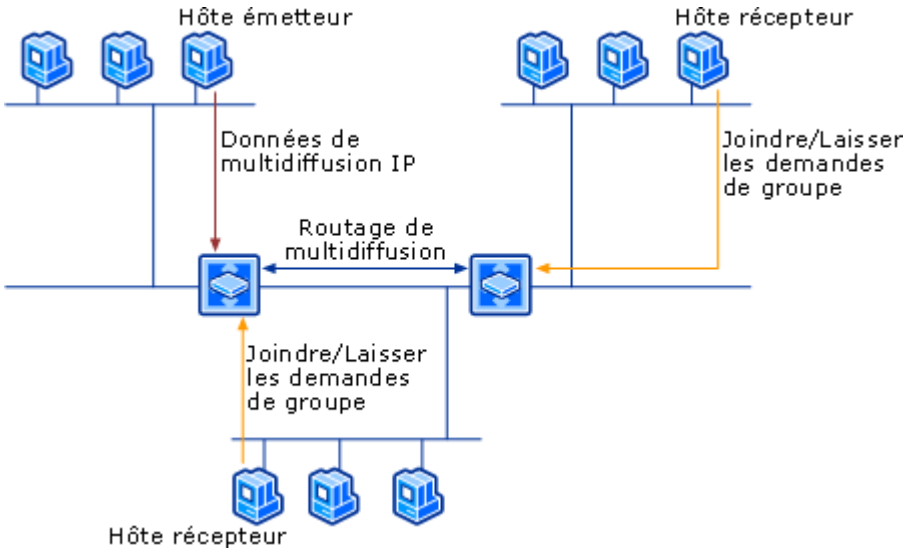


Figure 45 – La multidiffusion

- L'hôte expéditeur envoie des datagrammes de multidiffusion à une adresse de groupe désignée.

- Les routeurs transfèrent les datagrammes de multidiffusion à tout segment réseau qui inclut des membres du groupe. Les routeurs peuvent transférer le trafic de multidiffusion sur un réseau, sur plusieurs réseaux et sur Internet.

- Les hôtes destinataires signalent à un routeur local qu'ils rejoignent le groupe, puis ils reçoivent tous les datagrammes ultérieurs envoyés à l'adresse de groupe.

- Si un hôte destinataire quitte le groupe et détecte qu'il peut être le dernier membre de groupe sur le sous-réseau, il peut contacter le routeur local pour quitter le groupe et lui demander d'arrêter de transférer les datagrammes de multidiffusion à ce sous-réseau.

Afin d'optimiser l'utilisation du réseau, nous avons utilisé la multidiffusion. En effet, plutôt que de charger le fichier WIM de point à point sur chaque client de façon séquentielle, il semblait plus judicieux de diffuser cette image de façon simultanée à un groupe de clients. J'ai donc activé cette fonctionnalité sur le serveur Windows 2008 et sur le service WDS. Lors de nos tests, nous avons pu valider une image WIM sur plus de 40 machines clientes en même temps en moins de 20 minutes. Il faut cependant faire attention à ce que les machines soient toutes conformes car la vitesse de transfert globale est calquée sur la configuration la plus lente.

II.4.2.4 Installation de MDT

Après avoir installé et configuré le système d'annuaire Active Directory, le service DNS, DHCP et WDS, nous avons procédé à l'installation du serveur MDT. Celui-ci peut s'effectuer sur un OS type « poste de travail » comme Windows 7 ou Windows 8. Cependant, afin d'harmoniser l'environnement serveur, nous avons choisi Windows 2008R2. L'exécutable MDT se présente sous la forme d'un fichier MSI disponible sur le site de Microsoft[25]. Nous avons utilisé la version 2012 update 1 disponible en septembre 2012. Son installation a été largement simplifiée depuis la version 2010, utilisée pour mon étude sur le poste client. En particulier, les prérequis logiciels ont été simplifiés, seuls le .NET 4 et le kit de déploiement et d'évaluation Windows sont désormais nécessaires.

Bien que l'installation soit simplifiée, un arbitrage est nécessaire dans le processus d'installation. En effet, deux kits de déploiement et d'évaluation Windows sont compatibles avec le logiciel MDT, qui s'appuie sur ces bibliothèques. Deux choix sont donc possibles : WAIK, Windows Automated Installation Kit ou ADK, Windows Assessment and Deployment Kit :

- Le Kit WAIK (Windows Automated Installation Kit) est un ensemble d'outils et de documents de prise en charge de la configuration et du déploiement des systèmes d'exploitation Windows.

[25] http://www.microsoft.com/en-us/download/details.aspx?id=25175

- Windows 8 apportant son lot de nouveautés, une nouvelle gamme d'outils remplace le WAIK : le Windows Assessment and Deployment Kit (ADK). L'installation est désormais plus rapide car elle permet d'installer uniquement les composants souhaités, ou de télécharger le kit complet pour une installation ultérieure.

	Systèmes d'exploitation supportés	Manipulation des fichiers WIM	Analyse de la conformité du poste client	Version WinPE
WAIK	XP, Vista, W7, W2008	ImageX	-	3.0
ADK	XP, Vista, W7, W2008, W8, W2012	DISM	Windows Assessment Toolkit Windows Performance Toolkit	4.0

Tableau 6 - Choix d'un environnement

WAIK étant un composant en fin de vie, ne permettant pas le déploiement de Windows 8, nous avons choisi le composant ADK dans une optique d'utilisation future de Windows 8. Par ailleurs, il dispose de deux outils supplémentaires :

- Windows Assessment Toolkit qui contient des outils pour diagnostiquer les problèmes et évaluer les performances du système d'exploitation sur un ordinateur particulier.

- Windows Performance Toolkit permet l'analyse des performances des systèmes d'exploitation Windows et des applicatifs. Une fois lancé, il va enregistrer les évènements Windows et les indicateurs spécifiés (mémoire utilisée, charge réseau…) afin de créer un tableau de bord permettant de facilement déterminer les problèmes de performances.

Enfin, le nouvel environnement WinPE 4.0 basé sur le code de Windows 8, supporte désormais le PowerShell 3.0, le .NET Framework 4.0 ainsi que la prise en charge native du 802.1x. Il est maintenant possible de lancer des scripts dans l'environnement de démarrage et de pousser encore plus loin l'automatisation.

II.4.2.5 Processus de déploiement

Nous avons vu le principe de fonctionnement du logiciel MDT ainsi que la mise en place d'un environnement de test. Nous allons maintenant nous intéresser aux processus de capture et de déploiement nécessaires à la diffusion de notre image Windows 7. Nous allons donc détailler le schéma de fonctionnement :

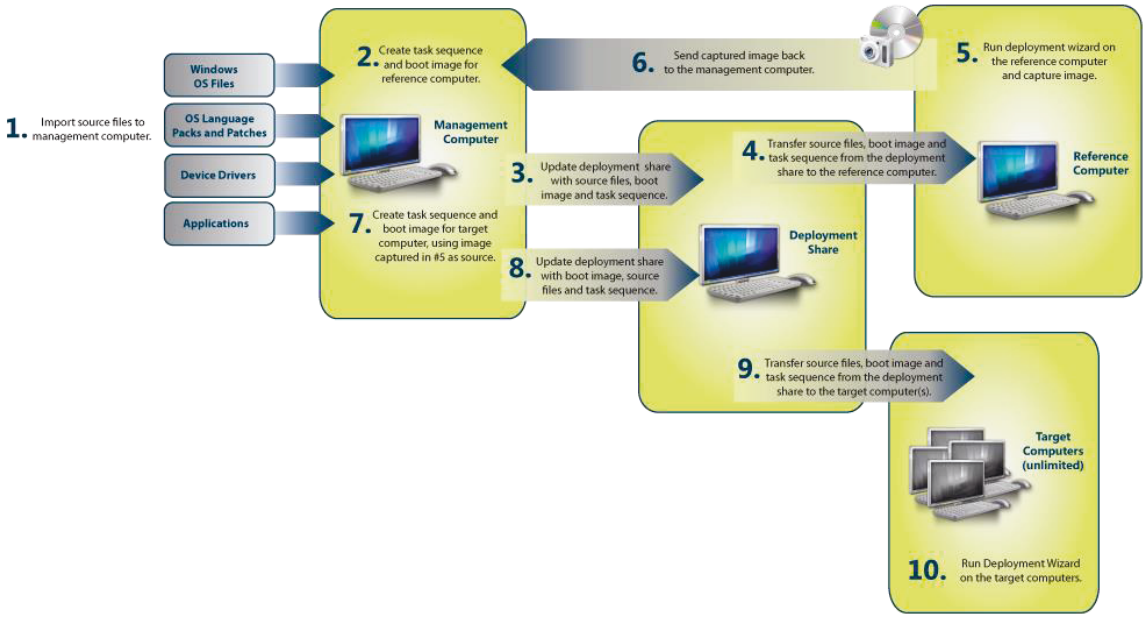


Figure 46 - Processus de déploiement

Le processus de déploiement s'architecture autour de trois grandes phases :

- Le déploiement de l'image de référence qui va servir de modèle pour les déploiements futurs, étapes 1 à 4 sur le schéma.
- La capture de cette image de référence sur le serveur MDT, étapes 5 et 6.
- Le paramétrage puis le déploiement de cette image sur les postes clients, étapes 7 à 10.

Dans la première étape, nous injectons les sources (DVD) de notre système Windows 7 Professional sur le serveur MDT. Par ailleurs, comme indiqué plus haut, nous avons utilisé uniquement des machines virtuelles pour ce maquettage. Cette décision nous affranchit d'éventuels pilotes puisqu'une machine virtuelle s'appuie sur des composants standards, reconnus nativement par Windows 7.

Nous allons ensuite paramétrer cette image brute à l'aide d'une séquence de tâche. Les séquences de tâches sont le cœur du logiciel MDT et permettent de gérer et configurer toutes les étapes nécessaires au déploiement de Windows. Bien qu'il ne s'agisse pas d'un langage de script, il est possible de lancer des scripts PowerShell depuis une séquence de tâches. J'ai donc paramétré une première séquence qui renseigne le compte administrateur, force les mises à jour Windows et enfin active Windows 7 sur le serveur de l'Université.

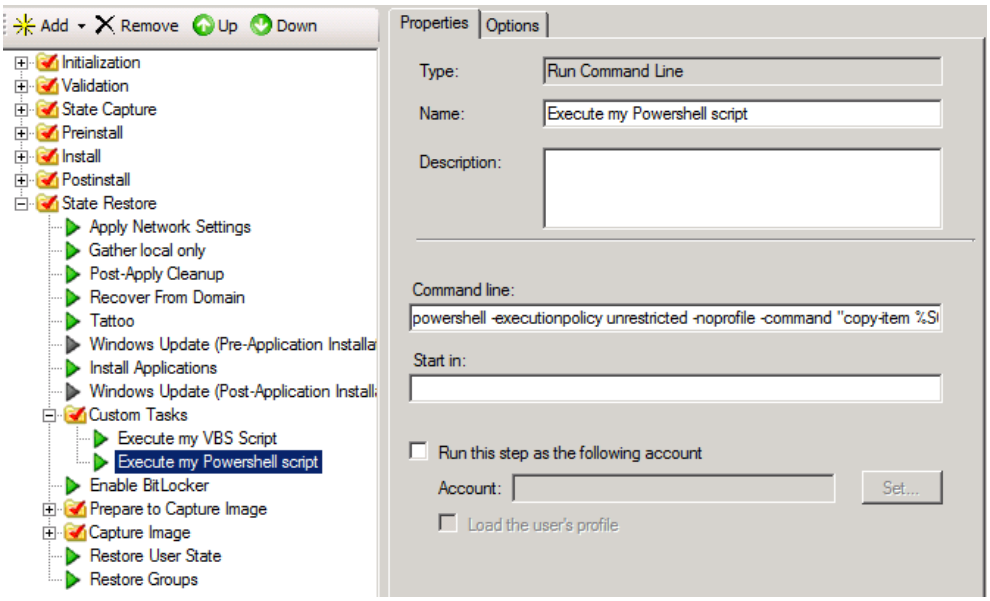


Figure 47 - Activation de Windows

Une fois cette étape accomplie, nous allons « compiler » cette tâche. Nous allons également générer un environnement WinPE afin de le déposer sur le serveur WDS. De cette façon, lorsque le client de référence va démarrer sur le réseau, il va charger le noyau WinPE, contacter le serveur MDT, puis procéder au déploiement de notre système Windows 7 Professional. Nous allons ainsi obtenir une machine virtuelle disposant d'un système Windows mis à jour et activé.

L'étape suivante consiste à capturer notre système source sur le serveur. Nous allons lancer l'assistant de capture dans l'environnement Windows puis nous allons paramétrer le chemin et le nom du fichier WIM à conserver. D'après nos tests, il faut compter près de 50 minutes pour copier les fichiers sur le serveur. En effet, contrairement à une solution classique de clonage, le processus de capture génère une archive des fichiers, ce qui explique le temps d'exécution.

Nous allons ensuite utiliser une nouvelle séquence de tâche afin de paramétrer en profondeur l'image que nous venons de capturer. Par exemple, nous allons préparer les pilotes nécessaires au déploiement sur les postes clients, gérer les applications, les scripts et la jonction au domaine Active Directory. Cette gestion s'effectue non seulement à partir de la séquence de tâche mais également au niveau du serveur.

Enfin, nous allons compiler cette nouvelle tâche puis mettre à jour le noyau WinPE sur le serveur WDS. Enfin, nous allons démarrer nos postes cibles en sélectionnant la carte réseau, puis charger l'environnement de travail, afin de sélectionner notre image de déploiement. Les étapes

suivantes sont ensuite automatisées et ne demandent pas d'intervention humaine. La multidiffusion étant activée, nous avons validé avec succès un scénario de 40 machines en simultané.

II.4.2.6 Paramétrage des partages de distribution

Une fois installée, MDT se présente sous la forme d'une console appelée « Deployment Workbench ». Elle est accessible depuis le menu démarrer et se compose de deux parties :

- le centre d'information qui centralise les documentations, rappelle les composants installés et permet de vérifier la présence d'éventuelles mises à jour disponibles

- les partages de distribution ou « Deployment Share ». Un « Deployment Share » est en fait un dossier partagé sur le serveur qui va héberger l'ensemble des fichiers, images, dossiers, applications, pilotes, scripts séquences de tâches et paramètres nécessaires aux opérations de production du poste de travail. Une connexion sera initialisée depuis le système WinPE vers le serveur afin de récupérer les objets nécessaires.

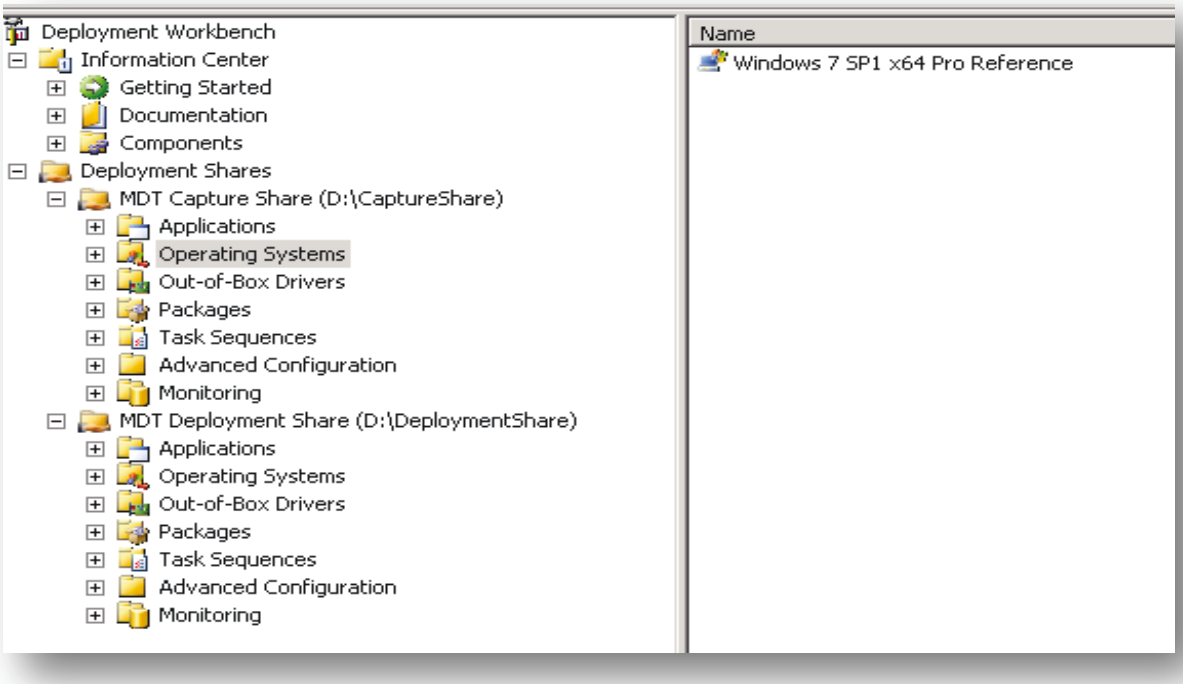


Figure 48 - La console de gestion MDT

Les partages de distribution sont essentiels et nous avons procédé à de nombreuses itérations avant de trouver une configuration adaptée, permettant une installation silencieuse du

poste de travail. En effet, les paramètres du partage de distribution s'appliquent à toutes les séquences de tâches générées dans l'espace de travail. Il s'agit donc de trouver les bonnes options dans une liste comportant plus de 300 entrées. Par ailleurs, ces indications affectent non seulement le déploiement des systèmes d'exploitation mais la création du noyau WinPE.

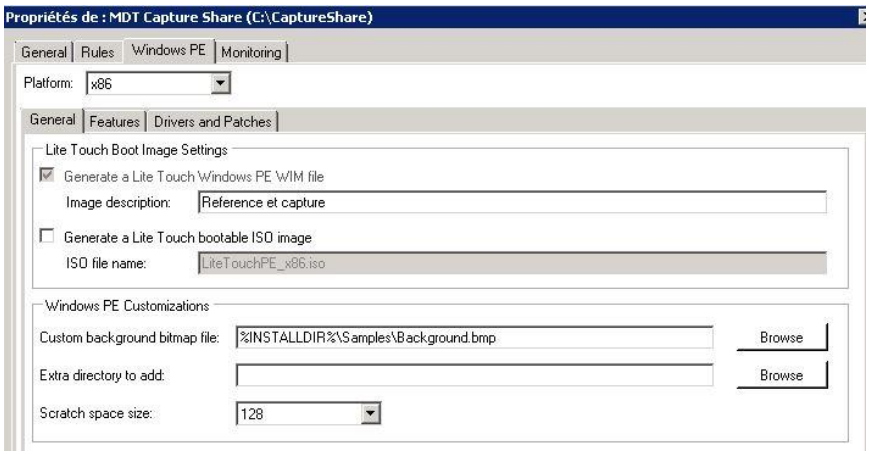


Figure 49 - Paramétrage de MDT

Deux fichiers principaux pilotent le partage de distribution. Il s'agit du BootStrap.ini et du CustomSettings.ini, accessibles directement depuis les propriétés du partage ou modifiables directement dans l'arborescence du partage réseau.

- BootStrap.ini : ce fichier est utilisé par le noyau WinPE lors de sa connexion au « Deployment Share » par le réseau. Il contient le chemin vers le partage et les informations nécessaires à la connexion.

```
[Settings]
Priority=Default
[Default]
DeployRoot=\\SHA-ETU-MDT\CaptureShare$
SkipBDDWelcome=YES
KeyboardLocalePE=040c:0000040c
UserDomain=DOMAIN
UserID=mdt
UserPassword=****
```

- CustomSettings.ini : ce fichier est utilisé après l'utilisation des paramètres provenant du fichier Bootstrap.ini. Il représente le fichier principal de configuration du partage de distribution et va piloter le reste du processus de déploiement. Un long travail documentaire a été nécessaire afin de spécifier les paramètres les plus adaptés à notre projet. L'objectif d'une installation silencieuse est donc de cacher le maximum

d'écrans de configuration afin d'automatiser le processus. Voici un extrait d'un fichier de configuration :

```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
_SMSTSORGNAME=MDT2012
OSInstall=Y
SkipAppsOnUpgrade=NO
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerName=NO
UILanguage=fr-FR
KeyboardLocale=040c:0000040c
UserLocale=fr-FR
SLShareDynamicLogging=\\SHA-ETU-MDT\DeploymentShare$\Logs
JoinDomain=DOMAIN
DomainAdmin=DOMAIN\mdt
DomainAdminPassword=****
WSUSServer=http://wsus.ad.univ-lorraine.fr
EventService=http://sha-etu-mdt.ad.univ-lorraine.fr:9800
……
```

II.4.2.7 Problèmes rencontrés

La première partie, liée à l'installation des serveurs et services, s'est correctement déroulée. Le réel défi fût le paramétrage du serveur MDT dans l'optique d'un déploiement automatisé. Nous avons rencontré deux problèmes majeurs.

Le premier problème concerne la gestion du partage de distribution. En effet, certains paramètres du CustomSettings.ini sont incompatibles entre eux, ce qui provoque une erreur lors du déploiement. Par exemple, il n'est pas possible de combiner les paramètres liés au déploiement du poste de référence, dans un groupe de travail, et le déploiement des postes clients dans un domaine. De la même façon, il n'est pas possible de configurer un partage de distribution pour gérer à la fois une capture d'image et un déploiement en masse. Bien que des solutions de contournement existent, nous avons choisi de créer deux « Deployment Share » :

- un pour le déploiement et la capture de l'image de référence
- un autre pour le déploiement en masse des postes clients, comme illustré ci-dessous.

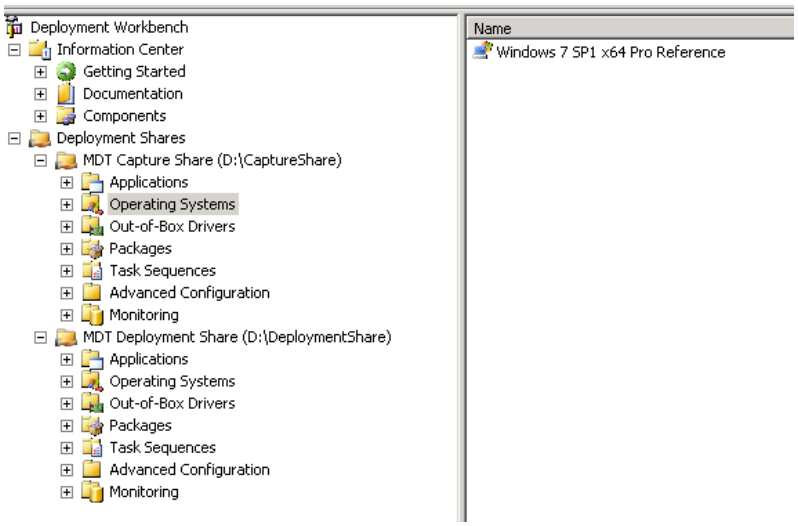


Figure 50 – Les deux environnements MDT

Un second problème concerne la sécurisation du serveur MDT. En effet, le nom d'utilisateur et le mot de passe ne sont pas cryptés. Nous avons donc généré un compte de service dans l'annuaire Active Directory puis nous l'avons autorisé à activer uniquement de nouveaux ordinateurs dans le domaine Windows, en configurant les ACL de l'unité d'organisation regroupant les comptes de machines :

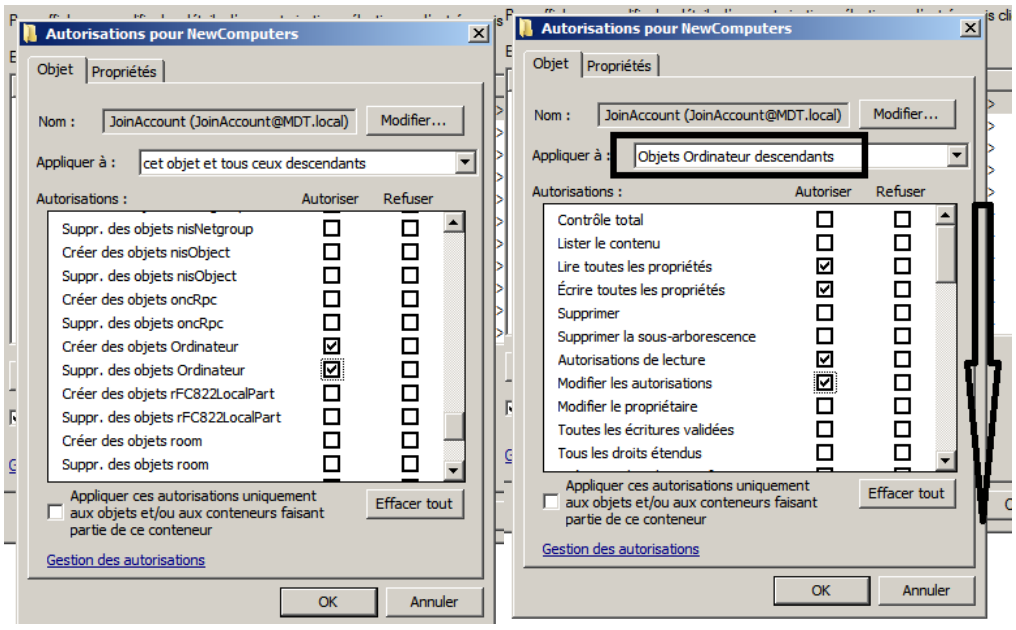


Figure 51 – Gestion des ACL

Enfin, nous avons configuré l'interface de supervision des déploiements en paramétrant le serveur MDT. Il s'agit en fait de l'activation d'un WebService qui va écouter les ports 9800 et 9801 du serveur. Celui-ci stockera les données envoyées par les clients sur le port 9800, dans une base de données SQL Compact. L'accès se fait ensuite sur le partage de distribution dans la

rubrique « Monitoring ». Nous avons rencontré quelques difficultés à faire marcher cet outil mais elles ont été résolues par la mise à jour vers MDT 2012 update 1.

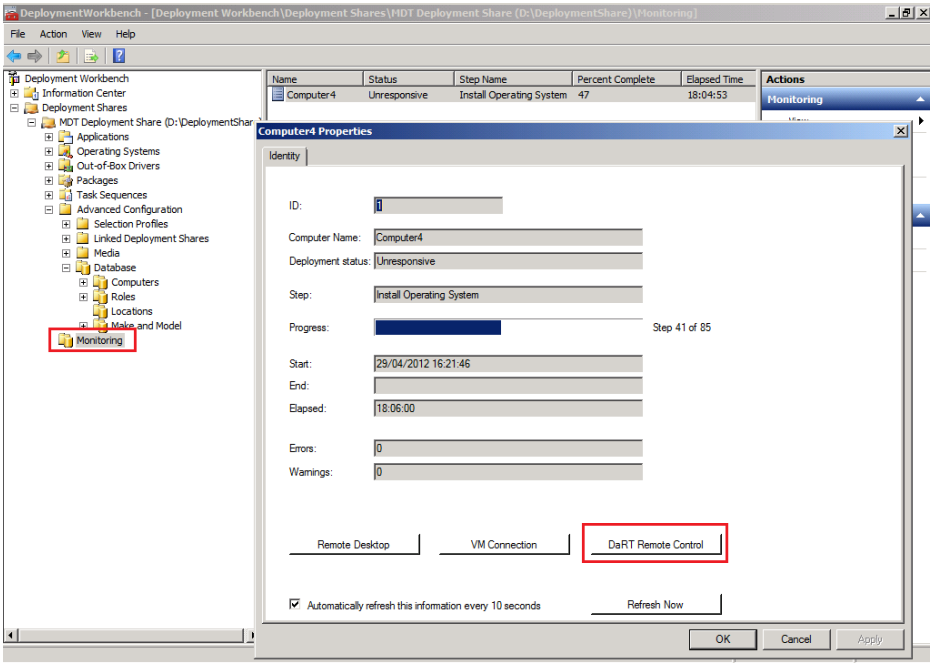


Figure 52 – Suivi des déploiements

Même si je n'ai pas détaillé la totalité des manipulations dans cette partie, MDT est un outil complexe qui a demandé à l'équipe un lourd investissement. Une fois la maquette commune terminée et la page Wikidocs complétée, nous avons dupliqué son architecture dans les 4 autres équipes.

II.4.3 Gestion des matériels

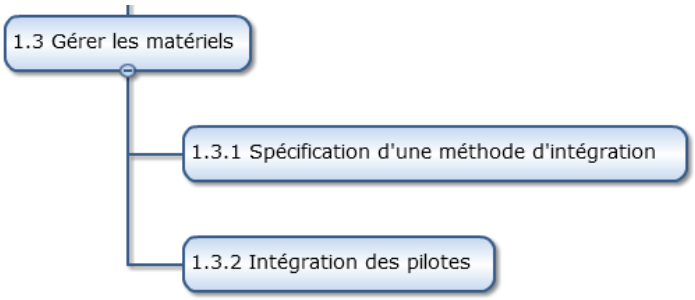


Figure 53 – Exécution du lot 3

Une fois chaque structure dotée d'un environnement de test fonctionnel, nous sommes passé au lot suivant, la gestion des pilotes. L'objectif de ce lot était de spécifier la gestion la plus efficace pour gérer les matériels, puis de tester cette implémentation sur les configurations les plus répandues à l'Université. Herve Hounzandji de l'IUT de Metz, s'est chargé de la coordination

et de l'animation de ce lot. Estimée à 10 jours/homme, 3 personnes ont collaborés à cette activité.

Le groupe a d'abord sélectionné un panel de machines représentatives du parc informatique de l'Université de Lorraine. Toutes les structures de l'Université s'alimentent dans le même marché public depuis 2009, à savoir DELL pour les portables et HP pour les fixes. Par ailleurs, même si plusieurs modèles sont proposés par ces fournisseurs, ils sont tous compatibles avec Windows 7 et les fabricants proposent les pilotes adéquats. Cette situation a facilité la réalisation du livrable et nous n'avons pas utilisé d'outil d'audit.

Nous nous sommes ensuite appuyés sur notre logiciel d'inventaire GLPI, afin de sélectionner les quatre modèles les plus répandus :

- Ordinateur de bureau de la famille HP Elite 8000 de 2009
- Ordinateur de bureau de la famille HP Elite 8200 de 2012
- Ordinateur de bureau de la famille HP Compaq Pro 6200 de 2012
- Ordinateur portable DELL Latitude E5520 de 2012

Le groupe a ensuite rapidement identifié deux problématiques : il y a 2 types de pilotes à prendre en compte lors du déploiement d'un système Windows. D'un côté, les pilotes pour le noyau WinPE, utilisés lors de l'initialisation du client et de l'autre les pilotes pour le système Windows qu'on déploie.

Dans MDT 2012 Update 1 avec ADK, l'image de démarrage utilisée pour le déploiement est basée sur WinPE 4.0 qui reprend le code de Windows 8. Il est impératif que les pilotes de la carte réseau soient correctement chargés ainsi que les pilotes de stockage de masse comme les contrôleurs RAID. Dans le cas contraire, il n'est pas possible de se connecter au serveur de déploiement et d'initialiser l'installation.

WinPE 4.0 supporte les mêmes matériels que Windows 8. Dans la majorité des cas, nous avons remarqué qu'il n'y a aucun pilote à rajouter. Nous avons cependant constaté sur la machine HP Compaq Pro 6200 qu'une carte réseau n'était pas reconnue nativement et interdisait le lancement du noyau WinPE. Sur le serveur MDT, nous avons créé un dossier « WinPE x86 » dans la rubrique « Out-of-Box Drivers » puis nous avons chargé le pilote de la carte réseau récupéré sur le site du constructeur. Dans la configuration WinPE, il faut aussi modifier l'option « Scratch

Space size » à 128 Mo pour augmenter l'espace temporaire de stockage qui est utilisé quand l'installeur injecte les drivers. En effet, une bibliothèque trop importante de pilotes peut saturer la mémoire vive allouée au déploiement. Enfin nous avons mis à jour le partage de distribution pour compiler le noyau WinPE, que nous avons déposé ensuite sur le serveur WDS.

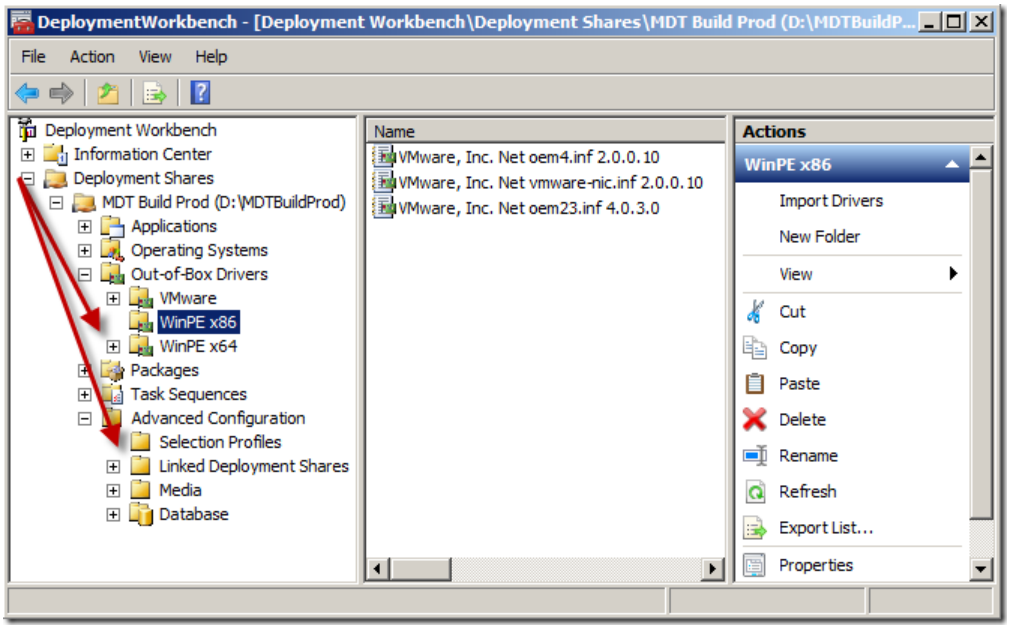


Figure 54 – Gestion des drivers pour WinPE

En ce qui concerne les pilotes pour le système d'exploitation, il existe trois approches que nous avons testées :

- Gestion d'un unique système d'exploitation avec un matériel homogène
- Gestion de plusieurs systèmes d'exploitation avec un matériel homogène
- Gestion de plusieurs systèmes d'exploitation avec un matériel hétérogène

La première approche est la plus simple et permet une découverte des mécanismes relatifs à la gestion des pilotes. Le scénario est le suivant : on déploie un système d'exploitation sur un matériel provenant d'un vendeur unique. Il suffit de télécharger les pilotes sur le site du fabricant puis de créer un répertoire sur la console de gestion et enfin d'importer tous les pilotes dans ce dossier.

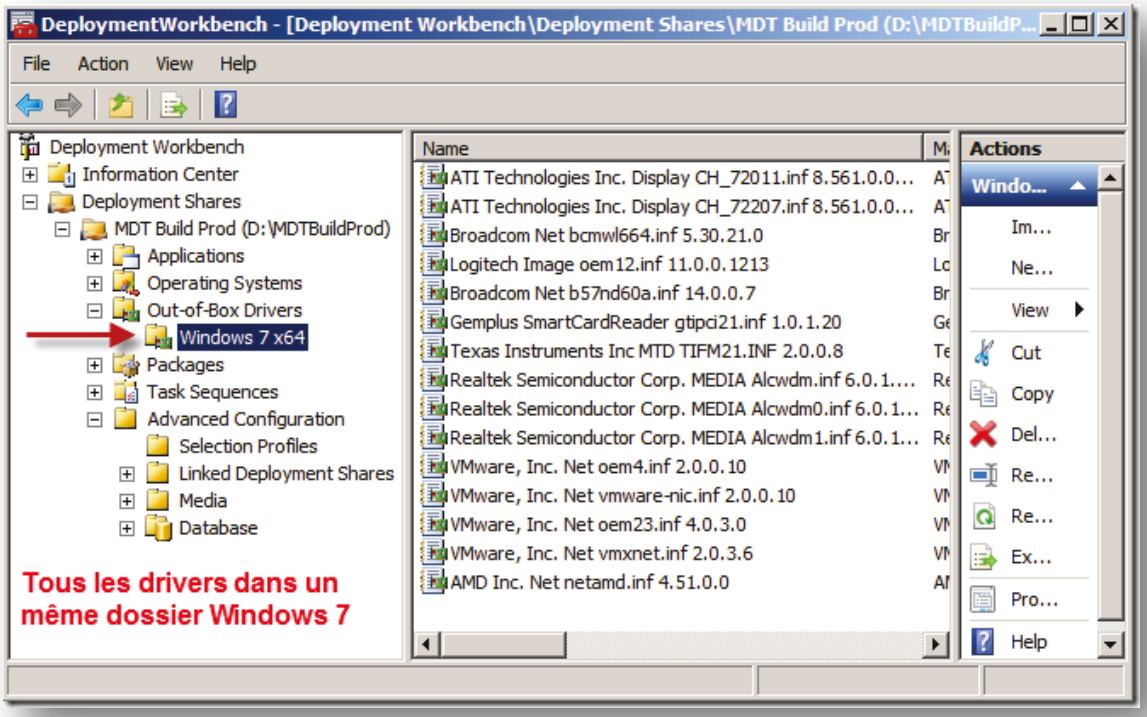


Figure 55 – Tous les pilotes dans un répertoire

Pour la seconde approche, la différence majeure est le déploiement de plusieurs systèmes d'exploitation. Comme dans ces deux méthodes la détection se fait par l'identifiant Plug and Play, il faut créer un filtre afin que les pilotes propres au système d'exploitation soient pris en compte lors de son déploiement. C'est une fonctionnalité de MDT appelé « Selection Profiles » qui permet de faire le filtrage.

La dernière méthode correspondant à un scénario proche de notre environnement avec plusieurs systèmes d'exploitation, plusieurs marques et modèles de machines. Nous devons donc appliquer un filtre par système d'exploitation comme au point précédent mais également par type de machine. En plus de la détection par Plug and Play, on va utiliser la fonction « DriverGroup » qui permet de faire un filtrage avancé.

Plutôt que de détailler chaque opération technique, je préfère présenter la synthèse de ces différentes approches :

	Facilité de paramétrage	Gestion de multiples configurations	Evolutivité
Pas de filtrage	+++	-	-
Filtrage par système d'exploitation	++	+	+
Filtrage par fabricant et modèle	+	+++	+++

Tableau 7 – Choix d'une technique de gestion des pilotes

Nous avons finalement retenu une gestion par fabricant et modèle, plus adaptée dans un environnement comme l'Université de Lorraine. Nous avons validé ce scénario en déployant nos 4 machines de test avec succès.

II.4.4 Gérer les applications

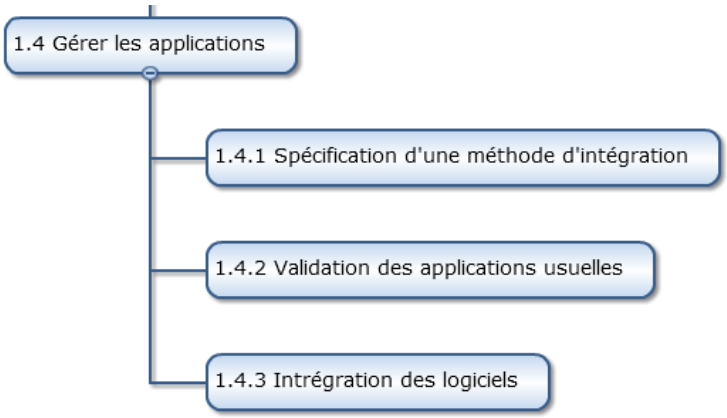


Figure 56 – Exécution du lot 4

M. Yann *Walterthum* de l'UFR des Sciences Fondamentales et Appliquées, s'est proposé pour animer ce lot pour lequel sept personnes participaient. Cette étape a été estimée à l'origine à 40 jours/homme.

II.4.4.1 Recensement des logiciels

Le recensement des logiciels était une étape déterminante afin d'avoir une vue pertinente du parc informatique. Etant donné qu'il n'existe pas de configuration logicielle recommandée sur l'Université de Lorraine, nous savions qu'il n'était pas possible de recenser tous les programmes utilisés sur le périmètre Lorrain. Nous avons donc décidé de faire deux groupes :

- Les logiciels pédagogiques les plus utilisés notamment dans le cadre du C2i (certificat informatique).

- Les logiciels usuels et les applicatifs métiers utilisés par l'administration et permettant la gestion des étudiants, des personnels, des budgets et des emplois du temps. Ces logiciels sont clairement identifiés et utilisés dans toutes les structures.

Grâce à notre outil d'inventaire, l'équipe a déterminé une liste d'une quarantaine de logiciels critiques utilisés au quotidien par les étudiants, enseignants et administratif. A côté des logiciels comme Microsoft Office et Matlab, de nombreux logiciels libres étaient présents comme EasyPHP, Gimp, VLC ou Open Office. Pour l'administration, en dehors des suites bureautiques et des outils Acrobat, nous avons recensé une dizaine de logiciels métiers.

II.4.4.2 Tests de compatibilité avec Windows 7

Après avoir dressé la cartographie des logiciels, nous avons procédé à des tests unitaires afin de vérifier le bon fonctionnement de chaque programme sous Windows 7. Lors de notre recherche documentaire, cette opération semblait critique dans les scénarios de migration vers Windows 7. Un applicatif sur deux était présenté comme partiellement utilisable voir incompatible.

Il faut cependant noter que ces études dataient de 2009 ou 2010, peu après la sortie de Windows 7 et que Windows XP était encore solidement ancré dans les organisations. La situation a changé au fil des années avec l'adoption massive de Windows 7, l'annonce en 2011 de la sortie de Windows 8 et la fin du support de Windows XP en 2014. Avoir commencé le projet courant 2012 s'est finalement révélé un avantage !

Avant de choisir une méthodologie d'intégration, nous avons utilisé deux produits Microsoft pour tester la compatibilité des logiciels avec Windows 7 : le centre de compatibilité Microsoft et l'outil Application Compatibility Toolkit.

Le centre de compatibilité Windows[26] est un outil Internet que l'on peut utiliser pour déterminer si nos logiciels et matériels sont compatibles avec les systèmes d'exploitation

[26] http://www.microsoft.com/fr-fr/windows/compatibility/CompatCenter/Home

Windows 7 et Windows 8. L'interface se présente sous la forme d'un simple formulaire dans lequel on peut indiquer le produit que l'on souhaite vérifier.

Les résultats de recherche nous apportent plusieurs informations. Tout d'abord un statut de compatibilité qui peut être « compatible », « certifié », « incompatible » ou partiellement compatible. Par ailleurs, un retour de la communauté figure sur la page du produit, sous la forme d'un vote sur la compatibilité du produit. Il s'agit juste d'une indication et les retours de certains utilisateurs restent fantaisistes. Par exemple, Office 2010 est gratifié de 25 votes négatifs sur les 245 positifs. Enfin, le site indique la version du programme pleinement compatible avec Windows 7 ce qui a été particulièrement utile.

Sur les postes de l'administration nous avons automatisé ces tests de compatibilité en utilisant l'Application Compatibiliy Toolkit (ACT)[27] de Microsoft, disponible à travers l'ADK. ACT est une collection d'outils dédiés aux développeurs, aux éditeurs et aux services informatiques. Il permet de faire un inventaire des applications et de vérifier leur compatibilité avec un système Windows cible par rapport à une base de connaissances. Ce processus est totalement automatisé et permet une collecte et une analyse des postes clients. ACT est composé de plusieurs briques dont l'Application Compatibility Manager (ACM) que nous avons utilisée. Cette console de gestion permet de créer des packages pour collecter les données sur les postes clients afin de connaitre le niveau de compatibilité des applications avec le système cible. Des rapports présentent l'état du parc applicatif et fournissent des pistes de remédiation, application par application.

[27] http://www.microsoft.com/en-us/download/details.aspx?id=7352

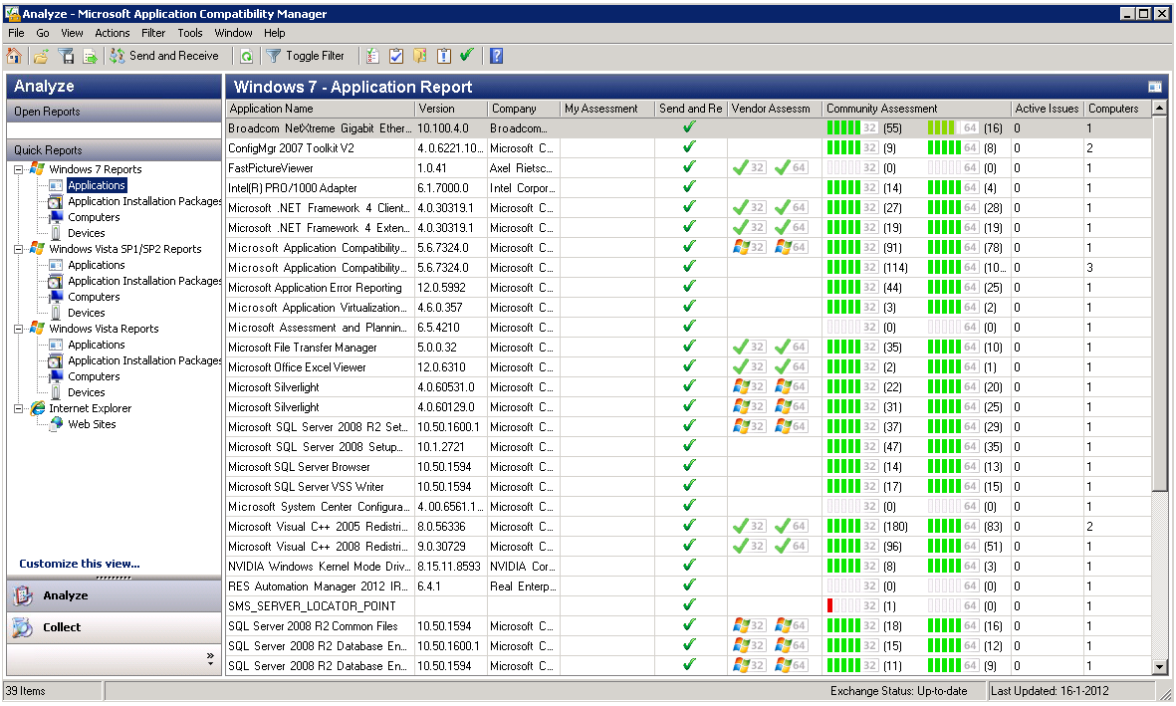


Figure 57 – Présention de l'ACM

Cet outil a permis d'industrialiser les tests de compatibilité sur le poste client en complément du portail Microsoft. En pratique, nous n'avons rencontré qu'un problème avec Adobe Acrobat 8, partiellement compatible avec Windows 7. Le passage à une version supérieure corrige ce comportement.

II.4.4.3 Le cas Office

Office 2003 arrivant également en fin de support en 2014, nous avons profité de ce projet de migration vers Windows 7 pour aussi intégrer Office 2010. Microsoft Office est particulièrement utilisé dans le périmètre de l'administration. Pour cette raison, nous avons analysé la compatibilité des documents de l'administration avec Office 2010. Par ailleurs, nous avons sensibilisé les directions sur ce sujet et encouragé les utilisateurs à suivre les formations dispensées à l'Université de Lorraine.

Cette compatibilité des documents Office se joue tout d'abord sur les différents formats des fichiers utilisés. Depuis toujours, les outils de la suite manipulaient des fichiers binaires. Office 2007 SP2 a marqué l'apparition d'un nouveau format standardisé : OpenXML, devenu une norme ISO. Ce format est basé sur les standards ZIP et XML, ce qui le rend interopérable, sécurisé et

robuste. La documentation Microsoft[28] indique que la taille des fichiers Open XML peut être jusqu'à 75% inférieure à celle des fichiers binaires.

Un autre problème concerne le rendu des documents Office. En effet, la version 2007 a introduit un nouveau moteur graphique qui diffère fondamentalement des versions précédentes. On constate parfois une altération du rendu des documents, comme à l'ouverture de documents dotés de graphiques.

Enfin le dernier point concerne les macros qui sont composées de code VBA (Visual Basic for Applications). L'interaction avec les fonctionnalités offertes par Office via du code VBA passe par la manipulation d'un élément nommé « modèle objet ». Ces modèles objets sont impactés par chaque nouvelle version d'Office. Il faut donc s'assurer du bon fonctionnement des macros sous Office 2010. Cela peut impliquer un changement de quelques lignes de codes voir un redéveloppement complet dans les cas les plus difficiles.

Une fois ces problématiques maîtrisées, nous sommes passés à la phase d'inventaire des documents Office. Là encore, il existe deux approches :

- Approche traditionnelle : il s'agit d'inventorier, tester et valider tous les documents, macros et applications Office. C'est une méthode très chronophage puisqu'il faut analyser la base documentaire de chaque structure et chaque service. Elle réduit cependant les risques d'incompatibilité applicative en concentrant l'effort sur la phase avant migration.

- Approche agile : il s'agit d'impliquer les utilisateurs métiers pour identifier les documents et applications Office les plus critiques. Ces fichiers, essentiels pour l'activité, sont donc traités en amont tandis que les autres documents seront traités après migration en mode réactif.

C'est cette dernière approche que j'ai choisi en contactant le service scolarité de notre organisation afin de vérifier ensemble la compatibilité de leurs documents. En effet, il s'agit du service administratif qui produit le plus de documents bureautiques. Une vingtaine de personnes utilisent au quotidien ces données. Bien que focalisée sur un seul service administratif, cette

[28] http://technet.microsoft.com/en-us/library/cc179190.aspx#section1

approche nous a permis d'établir une méthodologie d'analyse et de migration applicable à l'ensemble des structures de l'Université. Concrètement, nous avons testé 35 Gigas de documents Word et Excel.

J'ai utilisé l'Office Migration Planning Manager 2010 (OMPM)[29] de Microsoft pour valider la migration vers Office 2010. Cette boite à outils permet d'auditer son parc documentaire pour détecter d'éventuels problèmes de conversion des fichiers vers Office 2010. Un scanner de fichier va lire les documents selon 3 manières : à partir d'un ordinateur d'administration, localement sur les ordinateurs clients ou à partir d'un partage réseau.

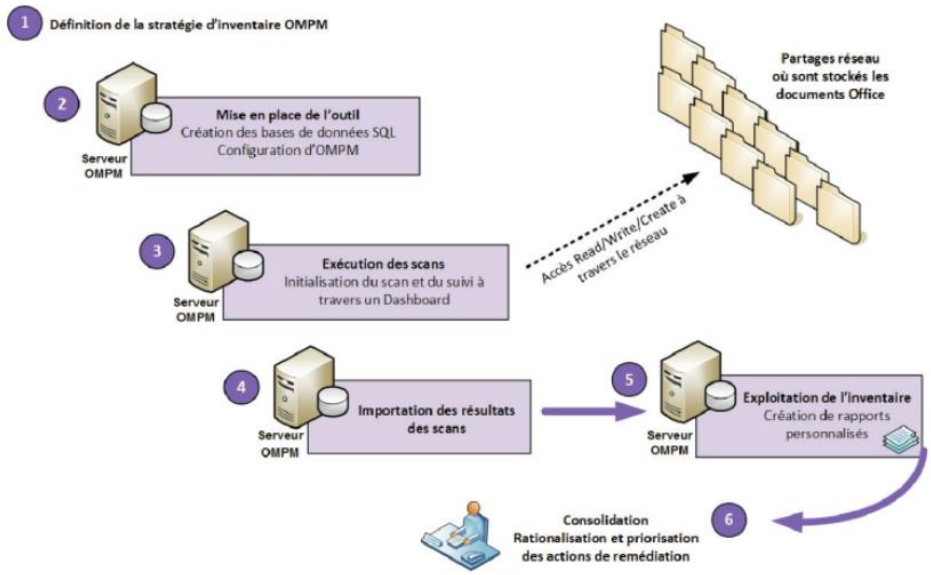


Figure 58 – Présentation de l'OMPM

Notre base documentaire étant stockée sur un serveur commun, nous avons choisi la dernière solution. Une fois paramétré, le logiciel va scanner l'intégralité des documents. Ces résultats seront ensuite injectés dans une base de données SQL Server Express, puis mis en forme dans un document Access afin de faciliter la lecture sous forme de tableaux de bord. Les problèmes « rouges » ou « jaunes » peuvent s'avérer préjudiciables et entrainer une perte de données ou de fonctionnalités. Les problèmes « verts » sont bénins et n'auront probablement aucun impact.

[29] http://technet.microsoft.com/fr-fr/library/dd630727%28v=office.12%29.aspx

Use Manage Issues for help with issues or to change issue levels.

Issue frequency across the filtered file set:

Issue Level	Issue Type	Issue Count	Resolved	Issue
Yellow	Upgrade Issue	3	Faux	File format is prior to Excel 97
Yellow	Tool Issue	83	Faux	Warning: File Not Scanned
Yellow	Upgrade Issue	71	Faux	Save format not supported
Yellow	Upgrade Issue	17	Faux	Embedded documents in the file
Yellow	Upgrade Issue	3	Faux	Embedded documents
Yellow	Upgrade Issue	124	Faux	Linked workbooks in the file
Yellow	File Skipped	36334	Faux	Scan Skipped: Old Last Modified Date
Green	Upgrade Issue	67	Faux	English Language Formulas in the workbook
Green	Upgrade Issue	2	Faux	Charts in the workbook.

Figure 59 – La console de résultat d'OMPM

Finalement, ce sont plus de 40000 fichiers qui ont été analysés. J'ai ensuite filtré ces résultats afin de ne prendre que les documents accédés ou modifiés ces 10 derniers mois, ce qui correspond à une année universitaire. Il nous semblait en effet peu utile d'analyser les archives du service qui sont rarement accédées et où un traitement en mode réactif est plus adapté. Nous avons donc ramenés le chiffre des documents critiques à 3900 fichiers.

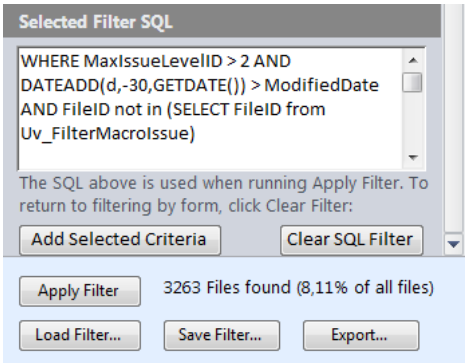


Figure 60 – Filtrage des résultats d'OMPM

Ensuite, j'ai créé une requête afin de quantifier les documents à faible risque de migration. Il s'agit des documents qui n'ont pas été modifiés depuis plus de 30 jours, qui ne sont ni « jaunes » ni « rouges » et qui ne présentent pas de problème de macro. 3300 documents, soit 85% des fichiers identifiés ne présentent aucun risque de migration dans notre analyse. Une conversion automatique est ensuite réalisée par le programme OFC.exe d'OMPM. Cette méthodologie a l'avantage de se focaliser uniquement sur les documents critiques pour l'activité en collaborant avec les utilisateurs métiers, tout en automatisant le processus de conversion.

II.4.4.4 Stratégie de gestion des images

L'objectif suivant était le choix d'une méthodologie d'intégration des logiciels dans le processus de déploiement du poste client. Cette étape demande une reflexion particulière : faut-il intégrer les applications directement dans l'image de référence ou les installer ensuite de façon

silencieuse lors du déploiement de la machine ? Trois approches sont possibles : constituer une image dite « épaisse », une image « fine » ou enfin « hybride »

Utiliser une image dite épaisse est une approche traditionnelle, où l'on va injecter toutes les applications de l'organisation, leurs paramétrages et les mises à jour dans le poste de référence. Ensuite, on va capturer l'image et la déployer sur les postes clients. Bien que cette procédure soit simple, le principal problème concerne la taille des images générées qui peut atteindre plusieurs dizaines de Go suivant les programmes installés, ce qui risque d'engendrer une saturation du réseau lors du déploiement. Par ailleurs, toutes les applications de l'entreprise étant intégrées, les utilisateurs risquent de se trouver en face de logiciels qu'ils n'utilisent pas, provoquant de fausses manipulations. Enfin, les images épaisses sont difficiles à mettre à jour et à maintenir à cause de leur complexité. Mettre à jour un composant nécessite une refonte et une nouvelle validation de l'image de base, ce qui est très chronophage pour l'équipe informatique.

L'image fine est l'approche opposée. L'emprunte du système référence est ici minimale et contient uniquement les composants et applications critiques pour le système d'exploitation. L'image résultante sera légère, facile à manipuler et à maintenir. L'inconvénient majeur de cette approche concerne la nécessité d'une infrastructure informatique à même de déployer les logiciels additionnels et leurs mises à jour. Par exemple, on peut utiliser Windows Software Update Services (WSUS) pour déployer les mises à jour Windows et les stratégies de groupes pour installer les logiciels. Dans de plus larges environnements, SCCM semble plus adapté pour packager et déployer les programmes. Par ailleurs, des outils de virtualisations d'applications comme App-V ou RemoteApp expriment ici leur plein potentiel. Cette approche demande donc une infrastructure adaptée et une formation poussée des personnels informatiques.

L'approche hybride est un compromis des deux techniques précédentes. Il s'agit ici de trouver un équilibre entre efficacité du déploiement et paramétrage de l'image de référence. Cette image source peut donc contenir des applications clefs pour l'organisation, des logiciels utilisés par toutes les populations. Par exemple, on peut imager une image de base composée de Microsoft Office et d'un anti-virus, les autres logiciels étant déployés par la suite suivant le profil de l'utilisateur. En effet, il est intéressant d'inclure les applications les plus statiques dans l'image de référence puis de déployer les applications fréquemment mise à jour lors de l'initialisation du poste client.

Le tableau suivant permet de récapituler les trois scénarios :

	Taille de l'image	Complexité du déploiement	Coûts en infrastructure	Agilité du déploiement	Facilité de gestion
Image épaisse	+++	+	+	+	+
Image fine	+	+++	+++	+++	++
Image hybride	++	++	++	++	+++

Tableau 8 – Choix d'une stratégie de gestion des images

J'ai donc choisi une image hybride pour gérer les images systèmes. Cette approche me paraissait le meilleur compromis entre facilité de gestion et taille de l'image. En outre, l'Université de Lorraine étant dépourvue de système de distribution des logiciels tels que SCCM ou App-V, une image fine, bien que séduisante, était impossible.

Notre image hybride est composée de Windows 7 et de ses mises à jour critiques, de Microsoft Office 2010 SP1 et de l'antivirus Symantec Endpoint Protection. Nous avons choisi des composants qui seront peu mis à jour, à l'opposé de logiciels comme le navigateur Firefox. Les autres logiciels seront déployés lors de la première initialisation du poste client.

II.4.4.5 Création des paquets applicatifs

Le groupe de travail ayant choisi l'utilisation d'une image hybride, le déploiement des applications s'effectue lors de l'initialisation du poste de travail sous Windows. C'est ici qu'un travail important de préparation s'effectue. En effet, des écrans de configuration apparaissent lors de l'installation des applications, qui permettent de renseigner le chemin d'installation, la licence à utiliser ou les modules à configurer. L'utilisateur doit être présent et doit valider manuellement chaque décision. Le véritable défi de cette étape consiste à cacher ces interactions à l'utilisateur final ou au technicien informatique afin que les installations de logiciels se fassent de façon silencieuse. Aucune boite de dialogue ne doit apparaitre à l'écran afin de permettre une automatisation complète du processus.

Concrètement deux possibilités techniques s'offrent à nous afin d'automatiser l'installation de nos quarante logiciels :

- Forger un paquet applicatif en utilisant un outil tiers, le plus souvent payant, qui va paramétrer en amont les fichiers et les clefs de registre à installer sur le poste client sans interaction avec l'utilisateur. En dépit des efforts de nombreuses solutions professionnelles, le processus reste complexe.

- Utiliser le programme d'installation officiel et le personnaliser. Dans la majorité des cas, des packages préexistants peuvent servir à une installation en mode silencieux avec un minimum de savoir-faire et de tests.

C'est cette dernière solution que nous avons privilégiée sur notre projet, pour des raisons de fiabilité, de coûts et de simplicité.

II.4.4.5.1 Installation silencieuse des applicatifs

Une des premières étapes consiste à récupérer le programme d'installation du logiciel et à effectuer des recherches sur le site de l'éditeur. En effet, une documentation présentant le processus d'installation sans assistance accompagne la plupart des logiciels. Dans la pratique, nous avons analysé les notes d'installation, le guide d'installation et le forum technique de chaque application.

En outre, on remarque que cette problématique est récurrente dans le domaine informatique et des dizaines de milliers d'administrateurs systèmes sont confrontés à ces questions lors de l'installation ou de la mise à jour des postes. En plus de la documentation fournie par l'éditeur, des bases de connaissances sont disponibles en ligne dont le site ITNinja.com, lancé par DELL en 2012. Ce site communautaire indique les mécanismes d'automatisation de milliers de logiciels et il est enrichi chaque semaine par des centaines de contributions d'internautes.

Il existe de nombreux types de programmes d'installation. Sous Windows, les deux types les plus courants sont les fichiers « EXE » et « MSI ». Généralement, un fichier MSI or EXE utilise un commutateur en ligne de commande pour indiquer les paramètres d'installation. En transmettant ces instructions de manière silencieuse, le programme d'installation est en mesure de s'exécuter de bout en bout sans que l'utilisateur n'intervienne. La quasi-totalité des logiciels actuels proposent un mode de déploiement simple à partir d'un commutateur.

En outre, de nombreuses applications gèrent le commutateur /help ou /? qui fournit à l'administrateur la liste des commutateurs d'application pris en charge par le package d'application. Voici un exemple appliqué à un programme d'installation d'Acrobat Reader 10 :

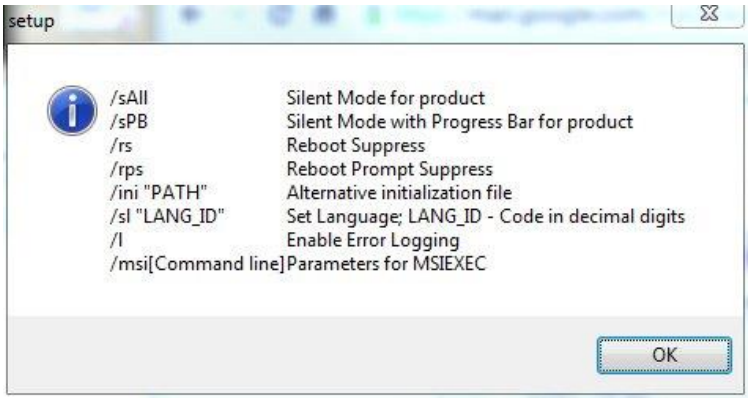


Figure 61 – Commandes d'un .MSI

Par ailleurs avec les fichiers MSI, il est possible de générer en amont un fichier pour contrôler les options d'installation. Ce fichier est appelé un fichier de transformation et porte l'extension .MST. Il est appliqué au moment de l'installation du paquet MSI afin de modifier le comportement de l'opération en cours d'exécution. Certains éditeurs de logiciels fournissent un outil spécial comme Microsoft Office ou Adobe mais il est toujours possible d'utiliser un logiciel spécialisé comme InstEd ou ORCA MSI, afin d'éditer les propriétés.

A l'aide de ces informations, nous avons ventilé les applications à tester entre les participants. Chaque application a nécessité une recherche documentaire et une validation technique dans une machine virtuelle, l'objectif étant de trouver pour chaque application les commutateurs adaptés à une installation totalement silencieuse. Cette tâche a été particulièrement longue et fastidieuse avec de nombreuses itérations pour chaque logiciel. Des logiciels en apparence simple comme Firefox, se révèlent complexes à manipuler. Tous les résultats ont ensuite été consolidés dans un fichier Excel, partagé sur Wikidocs, dont voici un court extrait :

	Version	7x64	7x86	Commutateur/ligne de commande	OK	Remarques/ URL/Référence
LibreOffice	4.1		x	Similaire OOO		http://www.itninja.com/software/libreoffice/libreoffice-1
Open Office 3	3.4.1		X	msiexec /qb /i openofficeorg341.msi SETUP_USED=1 ALLUSERS=1 ADDLOCAL=ALL REMOVE=gm_o_Quickstart,gm_o_Onlineupdate CREATEDESKTOPLINK=0		http://wpkg.org/OpenOffice.org_3.x
7 zip	9.20	X	X	/S		http://www.7-zip.org/faq.html
Adobe Acrobat reader	11.0	X	X	msiexec /qn /i "AdbeRdr11_fr_FR.msi" TRANSFORMS="reader11.mst"		ftp://ftp.adobe.com/pub/adobe/acrobat/win/11.x/11.0.00/misc/CustWiz1 exe pour créer le mst qui va bien
PDFCreator	1,X		X	PDFCreator-1_2_0_setup.exe /LOADINF="PATH_TO_INF_FILE\filename.inf" /ForceInstall /norestart /nocancel /SP- /silent		http://www.itninja.com/software/open-source-1/pdfcreator-1/1-
Filezilla	3.6.0	X	X	/S		Désactiver auto-update : http://www.itninja.com/software/filezilla/client-7/3-
VLC	2.0.4		X	/S		Message utilisateur au premier démarrage, créer un fichie interface.ini contenant [General] IsFirstRun=0 dans le répertoire %APPADATA%\Roaming\ \Users\Default\AppData\Roaming\vlc
Gimp	2.8.2	X		/VERYSILENT /SUPPRESSMSGBOXES /NORESTART /SP-		http://www.itninja.com/software/open-source-1/gimp-5/
Audacity	2.0.2		X	/SP- /VERYSILENT /NORESTART /MERGETASKS="!desktopicon"		http://www.itninja.com/software/audacity-version/audacity-

Figure 62 – Feuille de route des applicatifs

II.4.4.5.2 Intégration des applicatifs dans MDT

L'intégration des logiciels est facilitée par l'utilisation d'assistants dans la console de gestion. Il faut donc lancer le partage de distribution, se placer dans le répertoire Applications puis lancer l'assistant. Celui-ci va nous demander le chemin de l'application qui peut se trouver sur le serveur ou sur un partage réseau, puis la ligne de commande. C'est ici que nous allons utiliser les instructions d'installation recensées dans notre fichier Excel.

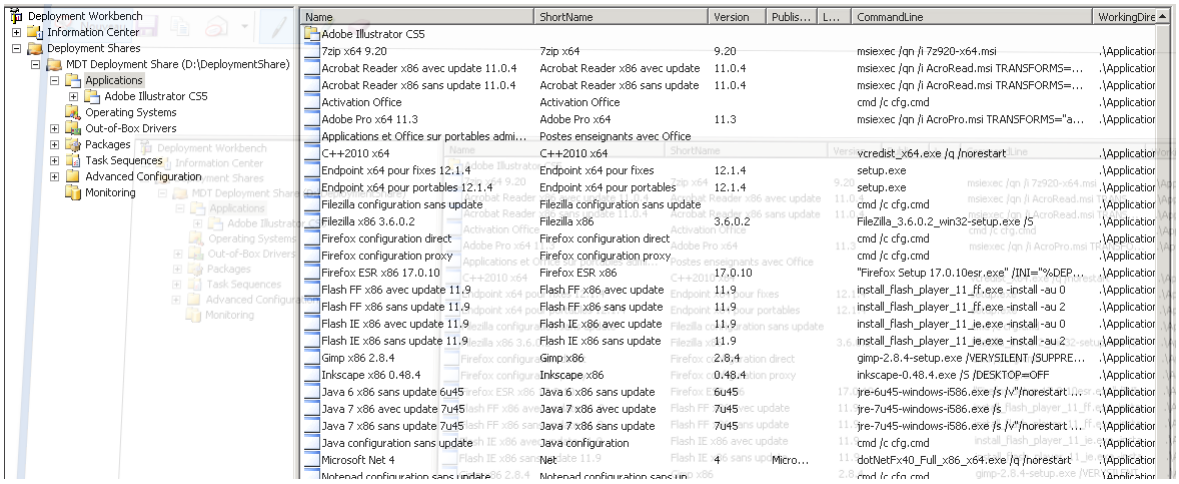


Figure 63 – La gestion des applications dans MDT

D'autre part, nous avons paramétré des ensembles applicatifs ou « application bundles » pour les différents types de client. Il s'agit en fait d'une entrée qui va contenir plusieurs logiciels prédéfinis. L'intérêt ici est une meilleure lisibilité lors de l'initialisation des déploiements par l'équipe informatique. Au lieu de proposer une liste exhaustive de logiciels, les programmes sont classés selon le département, la localisation ou l'utilisateur final.

Figure 64 – L'écran de démarrage du poste client

Une fois les logiciels sélectionnés, ils vont se déployer automatiquement sur le poste client lors du premier démarrage sous Windows. Des fichiers journaux sont générés afin de vérifier le bon déroulement du processus de déploiement qui s'exécute de façon totalement automatique sur le poste client.

II.4.5 Mise en production

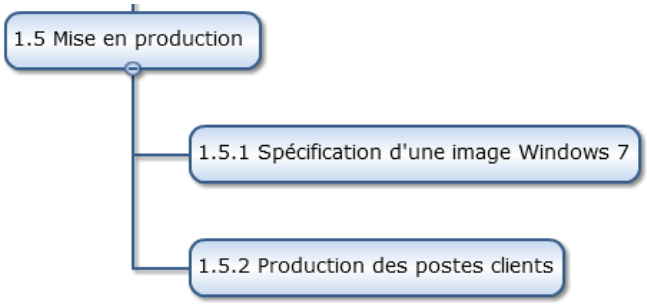


Figure 65 – Exécution du lot 5

Notre prototype est maintenant terminé. Tous les participants du projet disposent d'une maquette totalement fonctionnelle gérant les images systèmes Windows 7, les pilotes et les logiciels.

Concernant le dernier lot, rappelons que l'objectif initial du projet est de proposer un canevas technique aux équipes informatiques. L'adoption de l'outil est donc laissée à la discrétion des responsables de site et aucune obligation technique n'émane de la Direction du Numérique.

A l'heure actuelle, diverses structures ont adopté le format WIM et MDT pour leur production du poste de travail. On peut citer l'ex-établissement de Nancy 2, l'Institut National Polytechnique de Lorraine et l'UFR Sciences Humaines et Sociales ainsi l'UFR Arts Lettres et Langues de Metz. A terme, nous espérons que cette solution sera utilisée sur toute l'Université de Lorraine.

En tant que responsable informatique des deux UFR citées dans le paragraphe précédent, je vais détailler la méthodologie et le planning de la mise en production de ce nouvel outil de déploiement. Ce travail de mise en production a commencé en mai 2013 et s'est terminé en janvier 2014. Là encore j'ai procédé à un découpage en lots afin de gérer plus facilement le projet et ses ressources. Mes trois collègues, Michaël, Alain et Nicolas, ont activement participé à ce projet.

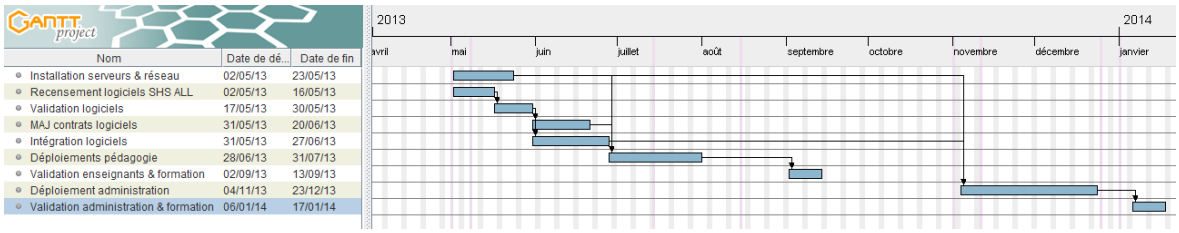


Figure 66 – Planning de déploiement

II.4.5.1 Installation et paramétrage des serveurs

En suivant les recommandations du projet, nous avons déployé 6 services sur 4 serveurs Windows 2008R2 en utilisant notre infrastructure virtualisée vSphere. Nos contraintes de sécurité étant fortes, les postes pédagogiques et les machines administratives se trouvent sur des réseaux totalement séparés. Nous avons donc dupliqué les services DHCP, WDS et MDT afin de répondre aux requêtes des clients des deux zones. Quant au domaine Active Directory et au service DNS, ils sont joignables par l'intégralité des postes de travail.

Nous avons ensuite suivi le canevas technique pour installer puis paramétrer le serveur MDT. Nous avons ensuite capturé une image hybride de référence contenant juste Windows 7 et Microsoft Office. Sur cette base, nous avons paramétré plusieurs séquences de tâches permettant un déploiement en masse de l'image. Nous avons afin injectés les pilotes matériels afin de prendre en charge les différentes configurations de notre parc informatique.

II.4.5.2 Recensement, validation et intégration des logiciels

Cette partie regroupe l'ensemble des tâches relatives aux logiciels des UFR SHS et ALL. Bien qu'un important travail ait été fait lors du maquettage collectif, certains logiciels propres à notre environnement existaient.

Nous avons donc tout d'abord listé l'intégralité des programmes utilisés dans les salles informatiques et sur les postes administratifs en utilisant notre logiciel d'inventaire. Ensuite, nous avons envoyé cette liste aux référents des salles informatiques et à l'administration afin qu'il valide la pertinence des entrées.

En parallèle, nous avons testé le bon fonctionnement de chaque logiciel sous Windows 7 puis nous l'avons ajouté sur le serveur MDT en indiquant la ligne de commande relative à l'installation silencieuse. Cette étape a monopolisé deux personnes sur un mois. Nous avons intégré près de 20 logiciels métiers propres à notre périmètre comme Autocad, SAP, SPSS ou Map Info, en plus des logiciels usuels.

II.4.5.3 Déploiement des postes pédagogiques

Ce lot concerne le déploiement des postes informatiques dans les salles pédagogiques. En un mois, nous avons déployé 550 postes informatiques répartis sur 27 salles pédagogiques. Nous avons déployé Windows 7 de façon automatisée et agile en intégrant près de 60 logiciels sur 12 profils matériels.

Contrairement à notre précédente solution de déploiement où une salle informatique était associée à une image système, nous avons utilisé une image WIM pour l'ensemble de nos salles. Par ailleurs, cette image est déployée en multicast sur les postes clients en moins de 20 minutes par lien gigabit. Le déploiement des logiciels s'effectue ensuite en unicast, poste à poste. Le temps nécessaire pour cette dernière étape varie selon le nombre de logiciels à installer.

Cependant, après avoir déployé une centaine de postes, nous avons rencontré un problème sur un logiciel, VLC. En effet, j'avais utilisé une nouvelle version du logiciel, livrée en paquet MSI afin de faciliter le déploiement. Malheureusement à l'usage, il était impossible de lire une vidéo. Après consultation des forums de l'éditeur, il s'avérait que cette version était buggée. Nous avons donc intégré une révision différente puis redéployé nos 100 machines. Cet épisode nous a couté 7 jours de travail et montre la difficulté à valider le bon fonctionnement d'un logiciel, une fois l'installation achevée.

Nous avons comparé notre ancienne solution de déploiement Clonezilla, avec notre nouvelle installation. Bien que les deux technologies soient gratuites, les différences techniques sont importantes. Le format WIM apporte une grande souplesse d'exploitation et permet une image unique par structure en opposition avec les images monolithiques de Clonezilla, basées sur les secteurs du disque. Pour conclure, le temps de mise en place de l'infrastructure MDT est largement compensé par les fonctionnalités du produit.

	Technologie	Coût & Licence	Complexité	Ergonomie	Temps de création des images	Agilité	Vitesse de déploiement
MDT	WIM	Gratuit Propriétaire	+++	+++	+	+++	++
Clonezilla	Copie de disque	Gratuit Libre	+	+	+++	+	++

Tableau 9 – Comparaison de MDT et Clonezilla

II.4.5.4 Validation des installations et formation

Une fois les installations terminées, nous avons procédé à une première validation technique en suivant un protocole simple :

- Connexion de l'ordinateur au domaine Active Directory
- Vérification des montages réseaux
- Validation de l'accès à Internet
- Lancement des applications métiers

Une fois cette étape réalisée, nous avons ensuite effectué une validation par l'enseignant responsable de la formation. Cette étape est très importante car seul le professeur est en mesure de réaliser des tests unitaires sur les applications métiers. Nous avons donc procédé à la recette des 25 salles informatiques juste avant la rentrée. Par ailleurs, nous avons accompagné les personnes souhaitant une rapide formation sur Windows 7 et Office 2010. Cette dernière action est capitale car elle permet une adhésion de tous les participants.

II.4.5.5 Déploiement des postes administratifs

Une fois la période de rentrée passée, nous nous sommes intéressés à la seconde phase de notre mise en production. Cette étape, bien que moins critique, est plus sensible. En effet, il faut tout d'abord s'assurer de produire une image système compatible avec tous les applicatifs métiers de l'UL mais il faut aussi être attentif à la bonne migration des données des utilisateurs. Enfin, la partie formation des personnels est également un point important.

Les points concernant le recensement des logiciels, la validation, la gestion des contrats et l'intégration ont déjà été développés dans les parties précédentes. Je ne vais donc pas revenir sur ces aspects similaires. Les seuls points critiques concernent la validation d'une version de Java et d'Internet Explorer. En effet, nos principaux logiciels métiers (Apogée, Harpège, SAP) utilisent ces technologies. J'ai donc contacté la branche SIG de la Direction du Numérique afin de demander leurs recommandations. Voici la matrice sur laquelle nous nous sommes appuyés :

Application	Navigateurs compatibles	Java
APOGEE	• Internet Explorer 7.x, 8.x ou 9.x ou 10.x ou 11.x • Firefox 5+ et <= 21	1.6.0_35+ et 1.7.0_07+ Meilleure version:1.7.0.21
SNW	• Internet Explorer 8.x, 9.x,10.x, 11.x (sous réserve d'activer le mode de compatibilité) • Firefox <22	
HARPEGE	• Internet Explorer 7.x, 8.x ou 9.x ou 10.x ou 11.x • Firefox 5+ et <= 21	1.6.0_35+ et 1.7.0_07+ et <= 45 Meilleure version:1.7.0.21
SIFAC WEB	• Internet Explorer 8.x ou 9.x ou 10.x	
Client leger SIFAC	• Internet Explorer 8.x ou 9.x ou 10.x	
BO Webi	• Internet Explorer 7.x, 8.x ou 9.x, 10.x et 11.x • Firefox	Validé en java 7 update 21

Figure 67 – Les recommandations applicatives

Ces données datent cependant de janvier 2014. En juin 2013, Java 7 n'était pas supporté ainsi qu'Internet Explorer 10/11. On note un décalage important entre les recommandations de l'AMUE, groupement d'intérêt public, et les mises à jour de Java et d'Internet Explorer. Il est donc fondamental de trouver un équilibre entre la sécurité applicative et le bon fonctionnement des produits. C'est pour cette raison que nous n'utilisons pas les dernières versions des logiciels évoqués, bien que des failles critiques soient corrigées à chaque mise à jour. Afin de garder une compatibilité maximale, nous avons validé la version 1.6 update 45 de Java et Internet Explorer 8. Nous effectuons de plus un suivi régulier de cette page afin de vérifier d'éventuels changements de versions.

Concernant la phase de migration en novembre 2013, nous avons tout d'abord mis en place un protocole de déploiement :

- transfert des documents de l'utilisateur vers le nouvel espace de stockage UL

- déploiement du poste puis validation de l'environnement avec l'usager

Cette procédure a été appliquée sur les 70 postes informatiques des personnels. Malheureusement pour des questions techniques, le transfert des données n'a pu s'effectuer de serveur à serveur. Une intervention manuelle était donc nécessaire. Nous avons également choisi de ne pas garder l'ancien profil de l'utilisateur, contenant les paramètres applicatifs, afin de ne pas mélanger des données provenant de Windows XP à Windows 7. En effet, les chemins d'accès (Mes documents, Application Data, Program Files) sont différents d'un système à l'autre, rendant

un éventuel portage hasardeux. Ces contraintes ont largement augmenté le temps de production d'un poste de travail, d'une heure à 2h en moyenne.

Enfin concernant la formation des usagers, nous avons accompagné l'utilisateur sur son nouvel environnement. En parallèle, l'Université de Lorraine a proposé des formations complètes pour Office 2010, dans le cadre du plan de formation continue des personnels.

II.4.6 Bilan des coûts

Les coûts ont été parfaitement respectés sur le projet. Comme détaillé au point 1.3.3, la solution de Microsoft est gratuite. Les seules dépenses sont liées à la mise en place de l'infrastructure serveur et à la régularisation des licences Windows 7. Nous avons modélisé ces données précédemment. Je vais donc me limiter au coût de revient sur mon périmètre : les UFR SHS et ALL.

Au niveau des serveurs, nous avons utilisé notre infrastructure existante, sans aucun coût supplémentaire. Pour les licences Windows, nous avons un contrat Dreamspark[30] avec Microsoft pour les postes pédagogiques. Enfin pour les postes administratifs, où l'accord Microsoft ne s'applique pas, nous disposons d'un tarif préférentiel de 52 € HT par licence, soit 3650 € pour 70 machines. L'aspect financier a donc été bien respecté.

II.4.7 Bilan des délais

Le projet a subi plusieurs retards importants notamment lors de la mise en production. Ce risque avait été identifié dès le lancement du projet au paragraphe 2.3.6.3. En effet, l'équipe du projet est composée de personnes provenant de différentes structures, parfois ne dépendant pas de la Direction du Numérique.

Par ailleurs, la rentrée de septembre 2012 ayant été particulièrement riche en changements, les collègues n'ont eu que peu de temps pour se former et s'investir sur les premières étapes. Fin septembre, certains participants n'avaient pas eu la possibilité de se consacrer au projet, alors que d'autres avaient terminé la mise en place de leur prototype. Le planning du projet a donc été modifié à plusieurs reprises afin de tenir compte de ces évènements.

[30] https://www.dreamspark.com/What-Is-Dreamspark.aspx

Chaque participant avançait dans le projet quand il en avait le temps. Il ne s'agit donc pas d'un écart temporel entre la date initiale et la date réelle mais plutôt d'un allongement des durées des tâches et des lots. Le temps de travail réel planifié dans le WBS est donc juste, simplement il est grandement dilué dans le temps. Seules deux tâches ont été réellement sous-estimées, il s'agit de l'intégration des logiciels, paragraphe 2.4.4, et la production des postes clients, tâche 2.4.5.

En effet, la complexité des installations silencieuses, sujet sur lequel nous étions peu expérimentés, nous a posé plusieurs problèmes techniques. C'est un risque que nous avions identifié au point 2.3.6.2. Ce risque s'étant déclenché sur plusieurs applications, nous avons mis en œuvre les réponses techniques nécessaires. Au final, en intégrant les difficultés organisationnelles et les problèmes techniques, la durée de cette tâche est passée de 10 à 50 jours.

Concernant le lot de mise en production, sa réalisation était laissée à la discrétion du responsable informatique local. Dans mon cas, j'ai constaté un écart important de 6 mois entre la date planifiée (octobre 2012) et la date effective (mai 2013). Là encore, ce décalage s'explique par une charge de travail quotidienne trop importante pour l'équipe. De la même façon, nous avons été absorbés par la rentrée de septembre 2013, où nous avons mis en pause le projet pendant deux mois avant d'aborder la gestion des postes administratifs.

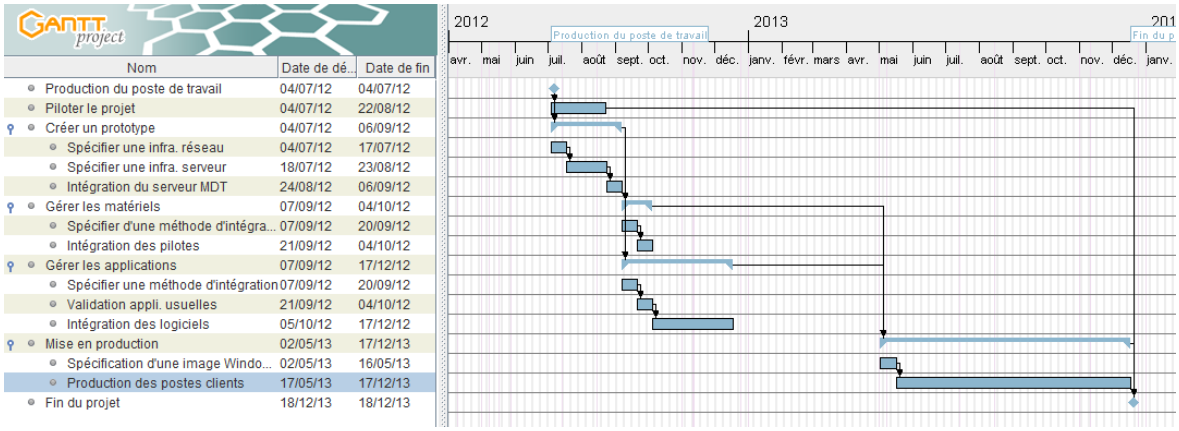


Figure 68 – Le planning réel du projet dans mon périmètre

Au final, l'écart en le délai théorique et le délai réel est bien réel. Cependant, nous avons respecté les contraintes initiales figurant au point 2.1.1, définies par la Direction du Numérique :

- Les postes pédagogiques doivent être absolument connectés au SI de l'Université de Lorraine au plus tard en septembre 2013.

- Une migration des postes administratifs est conseillée à partir de septembre 2013 et peut s'étendre sur plusieurs mois.

Concernant la phase de déploiement des postes, nous sommes en fait les premiers sur le site de Metz et de Lorraine Nord à avoir terminé ce chantier. A ce jour, certains sites n'ont pas encore commencé la migration des postes administratifs dans le nouveau référentiel, faute de temps ou de moyens.

Les contraintes budgétaires et organisationnelles étant fortes, je suis à postériori satisfait de la gestion de nos délais. En effet, un recrutement tel qu'un contractuel ou un stagiaire était impossible. De la même façon, il ne me paraissait pas judicieux de revoir les objectifs du projet et de supprimer des fonctionnalités clefs.

II.4.8 Bilan du projet

Concernant l'aspect technique, le projet est une totale réussite. Cette technologie nous a permis de considérablement réduire le temps de production du poste de travail tout en ajoutant de la souplesse lors des déploiements. La base de connaissance, enrichie tout au long du projet, est solide et permet une prise en main accélérée du logiciel et une configuration rapide de l'infrastructure serveur. Elle adopte les meilleures pratiques Microsoft et les recommandations du groupe de travail afin de fournir un ensemble homogène, sécurisé, s'intégrant parfaitement à l'environnement informatique de l'Université de Lorraine. Plusieurs structures utilisent déjà l'outil de Microsoft et nous espérons que ce produit sera retenu à l'Université comme un outil de référence. Une réflexion est d'ailleurs entamée sur le sujet au sein de la sous-direction du Service aux Usagers.

Ce projet est aussi été l'occasion de travailler avec des collègues d'autres structures, de Metz ou Nancy. Il nous a permis d'échanger nos points de vue sur la problématique des postes clients et de s'apercevoir que nous étions confrontés aux mêmes défis. Cette organisation transverse a permis d'apporter un regard neuf sur les enjeux de la migration vers Windows 7. Ce fût aussi paradoxalement une des faiblesses du projet, car il a fallu jongler avec les plannings et les impératifs de chaque participant, sans pouvoir s'appuyer sur une direction centrale qui aurait apporté une lettre de cadrage. Un tel scénario aurait permis d'optimiser le travail et de libérer du temps. Là encore une réflexion sur l'organisation de la sous-direction des Services aux Usagers est en cours.

Conclusion

La mise en place d'un annuaire commun et le déploiement des postes clients ont été des expériences particulièrement enrichissantes pour moi. Ces projets s'inscrivent dans la durée, ils ont en effet nécessité près de deux ans de travail, de février 2012 à décembre 2013. Ces expériences m'ont permis tout d'abord d'utiliser les enseignements du CNAM en matière de gestion de projet et en systèmes d'information. J'avais déjà mené de petits projets dans mon périmètre, mais sans jamais utiliser une méthode de projet. Ma formation m'a permis d'être plus efficace dans la conduite du projet et d'apporter un canevas à mes collègues et à la direction. En particulier la gestion des coûts, des délais et des risques a été grandement facilitée par l'adoption d'outils simples.

J'ai également mieux perçu le rôle du chef de projet qui est un véritable chef d'orchestre. Il doit être polyvalent, souple, posséder des bases techniques et constamment réévaluer les hypothèses initiales. Je comprends également mieux l'approche systémique sur le domaine car le projet peut être vu comme un être vivant qui évolue dans l'environnement de l'entreprise et qui nait, évolue et meurt. Par ailleurs, ma formation en systèmes d'information m'a permis de mieux percevoir les enjeux de l'organisation et l'organisation du SI de l'Université.

Pour conclure, cette expérience m'a particulièrement intéressé et j'ai décidé de changer de poste suite à cette expérience. A compter d'octobre 2014, je vais rejoindre la division Systèmes d'Information et de Gestion de l'Université de Lorraine où j'aurai des missions d'exploitation des applications de gestion et une casquette de chef de projet. Je quitte donc définitivement la branche Services aux Usagers après 6 ans dans ce poste.

Bibliographie

Antonelli, A., Bisaro, S., & Maillard, C. (2005). *Une Solution d'Authentification Unifiée dans un réseau hétérogène*. Disponible sur http://2005.jres.org/paper/108.pdf

Apréa, J.-F. (2008). *Configuration d'une infrastructure Active Directory avec Windows Server 2008.* Editions ENI. 767 pages.

Bories, W., & Duchêne, J.-S. (2010). *Windows 7 Déploiement et migration.* Dunod. 392 pages.

Clémence, F., & Mathieu, O. (2011). *La gestion du poste de travail en 2011 : panorama des technologies.* Disponible sur https://2011.jres.org/archives/16/index.htm

Comvalius, R. (2009). *Windows 7 for XP Professionals.* Books4Brains. 366 pages.

Darwin, S., & Moskowitz, J. (2002). *The Definitive Guide to Windows Installer Technology for System Administrators.* Realtimepublishers.com. 172 pages.

Finn, A., Gibson, D., & Van Surksum, K. (2011). *Mastering Windows 7 Deployment. 504* pages.

Policelli, J. (2009). *Active Directory Domain Services 2008 How-To.* Sams Publishing. 528 pages.

Svidergol, B., & Allen, R. (2013). *Active Directory Cookbook.* O'Reilly Media, Inc. 860 pages.

Annexe 1 : Extrait du projet AD

		Projet AD (attention au passage à l'échelle !)				
			nom : AD.UNIV-LORRAINE.FR			
Ordre		**Conception**		**Charge estimée**	**Participants**	
	AD - C	stratégie mot de passe	Un seul identifiant / un seul mot de passe			
	AD - C	Profil pour les étudiants	pas de profil			
	AD - C	Profil pour les personnels	profil local			
	AD - AA	Alimentation de l'AD (y compris nettoyage, évolution ...)				
	AD - AA		Quels sont les infos / besoins qui doivent être remontés au groupe de travail LDAP UL	1 réunion	**MD**, AV,MS, CM, VM, OM	09/03 de 9h30 à 12h00
	AD - AA		Alimentation "automatique" basée sur le SI de gestion			
	AD -		Gestion des modifications au fil de l'eau			
	AD -		Suppression (quand, comment ?)			
	AD - AA		Q : Quel lien avec les groupes géré avec GROUPEUR ?			
	AD-AM		Alimentation "manuelle" pour les cas particuliers (ex : invités, lecteurs autorisés BU ...) -> avec limitation dans le temps de la durée de vie des comptes	1 réunion	**MD**, PMag, AA, PMaf, Ese	06/03 de 9h30 à 12h00
	AD-AM		Ajout des machines, des groupes de machine			
			Q : autorisation pour une machine d'intégrer l'AD si admin du poste			
	AD-C	Formalisation du périmètre fonctionnel utilisateur (commencer par les bases, puis déployer des nouveaux services par la suite)	**WARNING : interroger les composantes (possibilité d'enrichir le groupe avec des personnels de composante)**	Préparation Interrogation des composantes Synthèse	**AV**, MS, EM, YL (à confirmer), FC	le 20/03 après-midi
	AD-C					
	AD-C		Quels sont les services proposés aux utilisateurs via l'AD (ex: authentification, impressions, ...) ?			
	AD-C		Quels sont les services qui ne pourront plus être proposés aux utilisateurs via l'AD (ex: synchro des mots de passe en AD UL et AD local) ?			
	AD-C		Q : Inclusion des comptes des personnels des labos ?			
	AD-C		Authentification unique des utilisateurs			
	AD-C		GPO			
	AD-C		Déploiement d'applications (O/N), limitations techniques ??			
	AD-C	Formalisation du périmètre fonctionnel matériel (pc, portable, OS ...)				
			Q : Inclusion des matériels des laboratoires ?			
Faire la doc	AD-C	Structure logique de l'AD -> décider AD unique O/N, Forêt, Arborescence			**Ese**,Ese, FC, MS, AA, EM, Pmag, VM, Pmaff	le 12/03 et le 13/03 de 9h30 à 12h30
Faire la doc	AD-C		AD unique (pers + etud), mono domaine, mono forêt			
Faire la doc	AD-C		DNS			
	AD-C	Règles de nommage			**Ese**,Ese, FC, MS, AA, EM, Pmag, VM, Pmaff	le 12/03 et le 13/03 de 9h30 à 12h30
	AD-C	Règles d'usage (ex: travail avec des groupes "au sens AD")	Utilisation de groupes locaux / globaux			
	AD-C	Structure physique de l'AD -> controleurs		Préparation + 1 journée de travail	**Ese**,Ese, FC, MS, AA, EM, Pmag, VM, Pmaff	le 12/03 et le 13/03 de 9h30 à 12h30
	AD-C		Q : Controleurs read only ?			
	AD-C		Quel maillage pour l'AD (en fonction de l'infra réseau et des localisations géographiques)?			
	AD-C		Dimensionner l'architecture physique (de la maquette / de la production)			
	AD-C		Quels sont les matériels à commander / réutiliser			
	AD-C		DNS			
	AD-C	Règles de délégation des droits d'administration et de gestion				
	AD-AM	Outils d'administration et de gestion	Cahier des charges de l'outil d'administration (contenu, modularité, technologie ....)	1 réunion	**CM**, MD, OM, Pmaff, AV	le 07/03 à partir de 10h30
	AD-AM		Fonctionnalités			
	AD-AM		Architecture			
	AD-AM		Outils / Langages			
	AD-AM		Gestion des sources			
	AD-AM		Q : possibilité d'importer / de créer en masse			
	AD-AM		Sur quel serveur sera hebergée l'application			
	AD-AM		Sur quel serveur seront hebergée les programmes			

Annexe 2 : Extrait du projet poste de travail

LOTS et ORDONNANCEMENT	TACHES	AVANCEMENT	REFERENT ET PARTICIPANTS	ECHEANCES
0) Gestion du projet			Francois, Yann, NK, Vincent, Michael,	TOUT PROJET
	Gestion de la documentation (Wiki, liste)			
	Coordination			
	Gestion délais couts...			
1) Création d'une maquette locale			Francois, Yann, NK, Vincent, Michael,	Fin OCTOBRE
	Prise en main de MDT - Formation - Docs			
	Définition d'une configuration commune et des outils			
	Définition d'un réseau de test			
	Mise en place d'un DC local de test (DNS DHCP) 2008R2			
	Installation MDT et clients 7 (et clients 8 a tester)			
	Utilisation de la BDD		Finalement pas testé dans le projet	
2) Gestion de drivers dans MDT			Hervé, Vincent, Yann, Francois	FIN NOVEMBRE
	Comment injecter les drivers			
	Définir panel de machines			
	Tests drivers portables et fixes et méthode de déploiement			
2) Gestion des applications			Yann, Vincent, Nk, Michael, Francois,	FIN NOVEMBRE
	Comment intégrer les applications dans MDT (Bdd ? Sequence ? Template ?)			
	Définir les appli a tester, les plus utilisées			
	Packager chaque applications (ITninja, Msfn, wpkg)			
3) Maquette avancée			TOUT LE MONDE	DECEMBRE
	Concaténation des deux lots précédents			
	Démonstration			
	Mise en production pour les composantes le souhaitant		En production sur ex-Nancy2, INPL et SHA	
Risques	**Probabilité**	**Impact**	**Criticité**	**Réponses**
Volume d'intervention dans les composa	4	4	16	Demande d'un renfort - stagiaire - priorités - redéfinition du projet, des
Production : problèmes de licence	2	1	2	Risque acceptable
Applications scientifiques avancées : dif	3	3	9	Installation dans l'image
Compatibilité Win7 de certaines appli	3	2	6	Mode Xp - Vmware -

Francois:
Vert : terminé
Jaune : en cours
Orange : pas commencé

Liste des figures

Mise en place d'un annuaire unique et intégration des postes clients sur l'Université de Lorraine

Mémoire d'ingénieur C.N.A.M 2014

RESUME

La fusion de plusieurs universités est une tâche colossale d'un point de vue informatique. Elle nécessité des mois de préparation et mobilise toutes les équipes sur le terrain. Dans la cadre de la création de l'Université de Lorraine en 2012, j'ai activement participé à la mise en place d'un annuaire commun permettant de gérer les postes de travail. Je vais donc revenir sur cet important chantier.

Ensuite, je détaillerais le second projet que j'ai mené. Il s'agit du processus de production des postes clients, l'objectif étant un déploiement le plus efficace possible dans le nouveau référentiel de l'Université de Lorraine.

Mots clés : Annuaire, Authentification, Active Directory, Microsoft Deployment Toolkit, Microsoft, Gestion de postes informatiques, Gestion de projets

---

SUMMARY

The University of Lorraine was created on 1 January 2012 by the merger of Henri Poincaré, Nancy 2 and Paul Verlaine Universities, and the National Polytechnic Institute of Lorraine (INPL). The merger process started in 2009 with the creation of a "Pôle de Recherche et d'Enseignement Supérieur" or PRES.

IT departments play an increasingly larger role in the long-term success or failure of this kind of operation. Technology has become so pervasive, IT touches virtually all aspects of a company's operations, and many of these functions are mission-critical.

We'll speak about the foundation of a new, single directory service for the whole University of Lorraine. Then, we'll see how to connect our workstations to this new infrastructure.

Key words : Directory service, Authentication service, Active Directory, Microsoft Deployment Toolkit, Microsoft, Workstation management, Project management