

# EXAMEN PROFESSIONNEL DE TECHNICIEN DE CLASSE SUPERIEURE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION DU MINISTERE DE L'INTERIEUR

**- SESSION 2017 -**

**Epreuve écrite du jeudi 09 février 2017**

L'épreuve écrite unique d'admission consiste à partir d'un dossier à caractère technique, en une étude de cas faisant appel à des connaissances relatives à l'environnement et à la technique des systèmes d'information et de communication et permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

L'épreuve porte sur l'un des deux thèmes suivants soumis au choix du candidat le jour de l'épreuve écrite :

- Les réseaux de télécommunications et équipements associés ;
- La gestion des systèmes d'information

## **LA GESTION DES SYSTEMES D'INFORMATION**

Durée 3h00

**Le dossier documentaire comporte 20 pages.**

*IMPORTANT*

**IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT  
APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.**

**ECRIRE EN NOIR ET EN BLEU - PAS D'AUTRES COULEURS**

## SUJET

### **Contexte :**

Vous êtes affecté(e) à la Direction des Systèmes d'Information et de Communication (DSIC) du Ministère de l'Intérieur, dans une équipe d'administrateurs système et de support de proximité.

Dans le cadre de vos missions, vous devez gérer le parc informatique du site auquel vous êtes rattaché(e) et en assurer son évolutivité ainsi que son maintien en condition opérationnelle.

Après un audit effectué sur le parc informatique dépendant de votre service, il est ressorti que les 156 postes bureautiques inventoriés dans votre base de données sont hétérogènes aussi bien au niveau du matériel que des versions de système d'exploitation installés.

Afin de répondre aux enjeux liés à la standardisation et à la sécurisation du poste de travail, un projet de migration vers Windows 10 a été initié.

Vous êtes rattaché(e) à l'équipe en charge de ce dossier pour la partie industrialisation et déploiement d'une nouvelle image de référence.

### **Travail demandé :**

Votre chef de projet vous demande de rédiger à son attention un argumentaire détaillant votre démarche méthodologique vous permettant de créer l'image de référence d'installation et son déploiement.

Votre argumentaire pourra, en conclusion, se fonder sur des notions relatives à la sécurité des systèmes d'information du poste bureautique, à la fraîcheur des données de votre inventaire ou bien encore à la stratégie de maintien à jour des logiciels installés par défaut.

## Dossier documentaire :

Document 1	Comprendre l'industrialisation informatique <a href="http://www.journaldunet.com/solutions/dossiers/pratique/industrialisation-informatique.shtml">http://www.journaldunet.com/solutions/dossiers/pratique/industrialisation-informatique.shtml</a> 20 décembre 2005	Pages 1 et 2
Document 2	7 bonnes pratiques pour simplifier la gestion de son parc informatique <a href="http://www.indexel.net/management/7-bonnes-pratiques-pour-simplifier-la-gestion-de-son-parc-informatique-3361.html">http://www.indexel.net/management/7-bonnes-pratiques-pour-simplifier-la-gestion-de-son-parc-informatique-3361.html</a> 18 mai 2011, Alain Bastide	Pages 3 et 4
Document 3	Comment manipuler la base de registre Windows <a href="http://www.journaldunet.com/developpeur/outils/tutoriel-pratique/comment-manipuler-la-base-de-registre-windows.shtml">http://www.journaldunet.com/developpeur/outils/tutoriel-pratique/comment-manipuler-la-base-de-registre-windows.shtml</a> 27 mai 2008, Sandy HACYAN	Pages 5 et 6
Document 4	Débuter avec MDT 2013 (Extrait) <a href="http://www.it-connect.fr/debuter-avec-mdt-2013/">http://www.it-connect.fr/debuter-avec-mdt-2013/</a> 29 juin 2015, Christophe Mandin	Pages 7 à 9
Document 5	Master Windows 7_ A l'aide de MDT et WDS <a href="http://webcache.googleusercontent.com/search?q=cache:z0ZaPZfhjc8J:jbouhierit.over-blog.com/2015/09/masterwindows7.html+&amp;cd=1&amp;hl=fr&amp;ct=clnk&amp;gl=fr">http://webcache.googleusercontent.com/search?q=cache:z0ZaPZfhjc8J:jbouhierit.over-blog.com/2015/09/masterwindows7.html+&amp;cd=1&amp;hl=fr&amp;ct=clnk&amp;gl=fr</a> 22 septembre 2015, Justine Bouhier	Pages 10 à 14
Document 6	Windows 10 – Nouveautés sur le déploiement <a href="http://www.it-connect.fr/windows-10-nouveautes-sur-le-deploiement/">http://www.it-connect.fr/windows-10-nouveautes-sur-le-deploiement/</a> 16 mars 2016, Christophe Mandin	Pages 15 à 17
Document 7	WINDOWS 7 : Préparez votre migration <a href="http://www.linformaticien.com/dossiers/id/20016/pageid/10228/windows-7-preparez-votre-migration.aspx">http://www.linformaticien.com/dossiers/id/20016/pageid/10228/windows-7-preparez-votre-migration.aspx</a> 01 juin 2009, Emilien Ercolani	Pages 18 à 20

## **Document 1 - Comprendre l'industrialisation informatique**

### **Qu'est ce que l'industrialisation de l'informatique ?**

On peut définir l'industrialisation informatique comme une succession d'étapes qui conduisent à une meilleure gestion des ressources internes dans un contexte donné. Ce terme n'est pas à confondre avec l'automatisation des processus métiers, où il s'agit d'optimiser l'exécution des tâches quotidiennes par l'utilisation de l'outil informatique. En effet, dès qu'une direction parle d'industrialiser telle ou telle procédure, cela signifie que le processus a déjà été informatisé mais qu'il peut encore être amélioré.

Souvent, l'industrialisation du système d'information va de pair avec la croissance de la société ou des services concernés dans l'entreprise. Dans les sociétés multisites, l'industrialisation apparaît plus tôt que prévu, afin de dresser un cadre solide sur lequel vont pouvoir s'appuyer les différents sites distants et ce, afin d'éviter un désordre qui pourrait nuire à l'efficacité. Industrialiser passe non seulement par la codification de bonnes pratiques et par la formation de personnes, mais aussi par l'utilisation d'outils spécifiques ou par la création d'un service dédié doté d'un responsable, par exemple.

### **A quoi correspond l'industrialisation logicielle ?**

Elle couvre plusieurs aspects. D'abord, l'industrialisation des licences logicielles, c'est-à-dire la mise en place du côté de la direction informatique d'un suivi précis des licences achetées et utilisées sur le parc. Or, un décalage existe souvent dès lors que l'entreprise est étendue et grossit. Des outils d'inventaire permettent ainsi de découvrir les logiciels installés sur les postes, des outils de télédistribution peuvent automatiser l'installation de logiciels ou de mises à jour, et des solutions de gestion comptable facilitent le traitement financier des biens.

Mais l'industrialisation du logiciel s'étend à de nombreux autres domaines, notamment le support aux utilisateurs et la sécurité. Dans le premier cas, le support informatique va devoir s'adapter aux utilisateurs de logiciels avec le temps, en mettant en place une cellule dédiée, éventuellement à plusieurs niveaux d'expertise. Cette entité doit se baser sur de bonnes pratiques de gestion des dossiers d'incidents, une étape qui peut être simplifiée par des solutions du marché.

Dans le second cas (l'industrialisation de la sécurité informatique), la direction a tout intérêt à créer un département spécialisé dans la gestion de l'information de sécurité. L'objectif est de passer d'une stratégie de défense corrective à une prise en compte proactive des menaces. La gestion de l'information de sécurité nécessite dès lors une cellule de veille, rattachée ou non aux équipes de développement pour déceler les failles et risques d'une nouvelle application par exemple.

### **Comment industrialiser son infrastructure ?**

C'est le rôle de l'administrateur réseau et des responsables plates-formes. Cela consiste d'abord à prévoir des architectures redondantes et interconnectées pour les serveurs ou les environnements de stockage notamment. Puis, à traquer la sous-utilisation de machines ou, au contraire, leur sur-utilisation, pour ajuster au mieux le parc aux besoins.

En termes de réseau, industrialiser l'infrastructure se conjugue souvent avec une volonté de diminuer le budget fixe d'entretien. Une étape qui passe par la création d'une cartographie des équipements, le choix de matériels types et la configuration de règles métiers.

Pour les environnements Web, l'industrialisation de l'infrastructure est une étape nécessaire pour améliorer les performances globales de la plate-forme. A ses débuts, un site Web professionnel non optimisé pourra réunir ses machines et s'en servir pour diverses tâches afin de minimiser les frais d'investissements. En revanche, avec la montée en charge, beaucoup de directeurs techniques s'orientent vers une séparation de l'infrastructure en un environnement trois tiers, distinguant les serveurs frontaux, qui réceptionnent les requêtes des internautes, le *middleware*, qui se charge de l'interface et des communications, puis les serveurs de *back-office*, en charge des traitements lourds. Dans ce cas, la séparation garantit l'indépendance des serveurs et facilite l'optimisation des calculs par la suite.

### **Pourquoi parle-t-on d'industrialisation des services informatiques ou des projets ?**

Les services informatiques, tout comme les biens, peuvent être optimisés par l'intermédiaire de méthodes. Concrètement, elles permettent de qualifier le service rendu, d'en évaluer le coût et les délais moyens afin de s'engager sur des niveaux de services (SLA) ou des objectifs de services (SLO). Mesurer ces services facilite le rapport entre directions informatiques et prestataire de services. La demande d'outils précis facilitant cette industrialisation s'est récemment renforcée avec le développement de l'offshore où la distance place un risque supplémentaire.

En gestion de projet, l'industrialisation passe par la définition de *frameworks*, l'utilisation de méthodes clés en main, le recours à la tierce recette applicative (TRA) pour mesurer le travail rendu, la séparation des tâches et la gestion des calendriers. C'est avant tout à la direction de définir les bons indicateurs d'évaluation des projets pour connaître l'écart entre la volonté initiale et le rendu final. Un calcul du retour sur investissement entre en partie dans cette procédure mais ne saurait se suffire à lui-même car il ne rend compte que de l'aspect financier du projet.

### **Quelles sont les méthodes ou les outils accompagnant les procédures d'industrialisation ?**

Les méthodes les plus couramment utilisées sont CMM, ITIL ou COBIT. Elles décrivent comment optimiser la gestion de son infrastructure et de ses services informatiques et différents niveaux. La direction informatique peut dès lors tracer des axes d'améliorations à moyen terme et se donner les outils nécessaires pour les atteindre.

Ces méthodes n'imposent pas d'outil particulier mais recommandent de bonnes pratiques à adapter selon le contexte de l'entreprise. Des audits techniques réalisés par des consultants extérieurs peuvent aussi faciliter la découverte de dysfonctionnements ou de perte d'efficacité sur des domaines précis.

## Document 2 - 7 bonnes pratiques pour simplifier la gestion de son parc informatique

De la standardisation des configurations à l'automatisation des mises à jour, différentes approches techniques et méthodologiques simplifient la gestion du parc informatique tout en réduisant son coût de fonctionnement.

Le prix des équipements informatiques a fortement baissé ces quinze dernières années. À tel point que le modèle économique s'est inversé. Les investissements en matériel ne représentent plus le principal poste du coût total de possession (TCO). Les coûts de licence, la facture électrique et la maintenance sont aujourd'hui des postes budgétaires importants. Voici sept bonnes pratiques pour rationaliser la gestion de votre parc informatique et réduire son coût de fonctionnement.

### 1. Créer une CMDB

*"On ne peut améliorer que ce que l'on sait mesurer."* Ce vieux précepte de Lord Kelvin n'est toujours pas d'actualité dans un certain nombre d'entreprises. Pour simplifier et rationaliser la gestion du parc informatique, il faut pourtant commencer par créer une base de données décrivant toutes les entités du système d'information. C'est la fameuse CMDB (Configuration Management Data Base) de la méthode ITIL. Cette base contient des informations techniques (configuration, disponibilité, niveau de service, etc.) et administratives et financières : contrats avec les fournisseurs, licences rattachées au matériel, clé de répartition pour la refacturation interne, etc.

### 2. Automatiser le déploiement des logiciels et des mises à jour

La plupart des logiciels de gestion de parc propriétaires (EasyVista de Staff&Line, Gimi de PCI, LANDesk Management Suite...) ou libres tels que GPLI, permettent de créer une CMDB, de tenir l'inventaire matériel et logiciel à jour, de déployer les logiciels, etc. L'automatisation de la plupart de ces tâches simplifie la gestion quotidienne tout en réduisant les coûts. Pour les entreprises qui ne souhaitent pas déployer d'outil en interne, Dell et Microsoft proposent désormais des outils de gestion de parc hébergés "dans le nuage", c'est-à-dire en mode cloud computing.

### 3. Automatiser la gestion des licences

Les inventaires manuels des licences ne fonctionnent pas. Trop compliqués et trop consommateurs en temps. *"De nombreuses entreprises paient des licences qu'elles n'utilisent pas. La faute incombe souvent à un inventaire qui n'est pas à jour"*, confirme Pierre Choplain (photo), dirigeant de l'éditeur PCI spécialisé dans la gestion de parc informatique. La plupart des entreprises achètent donc généralement plus de licences qu'il n'y a d'utilisateurs ! En tenant automatiquement à jour un inventaire précis, les outils de gestion de parc permettent aux entreprises de plus de 500 personnes de réaliser des économies de l'ordre de 5 à 15 %.

### 4. Homogénéiser les matériels et les logiciels

C'est une évidence : la standardisation des équipements et des logiciels facilite leur maintenance. Moins le parc est hétérogène et plus il est facile et peu coûteux à maintenir. Avant un renouvellement, il est donc intéressant d'analyser les profils des utilisateurs et de

les regrouper autour de configurations matérielles et logicielles types. La définition des profils de postes doit également prendre en compte les connaissances des utilisateurs et de l'équipe de maintenance afin de capitaliser sur leurs savoir-faire.

### **5. Allonger la durée de vie des postes de travail**

Le renouvellement des postes de travail n'est pas si facile qu'il y paraît. Coûteuse, la migration s'accompagne souvent de problèmes imprévus : perte de données, incompatibilité d'un logiciel non recensé, etc. En allongeant la durée d'utilisation des postes de travail, par exemple de trois à six ans, on réduit considérablement le coût total de possession (TCO) tout en dégageant du temps pour l'équipe informatique qui peut se concentrer sur d'autres projets. Comme le dit le dicton, "If IT works don't fix IT".

### **6. Virtualiser les postes de travail**

La virtualisation des postes de travail (ou VDI pour Virtual Desktop Infrastructure) simplifie grandement leur maintenance. Côté matériel, les clients légers sont robustes et interchangeables en quelques minutes. Leur durée de vie est deux fois supérieure à celle d'un poste de travail traditionnel. Autant de migration de parc en moins. Côté logiciel, les images des postes de travail sont centralisées côté serveur ce qui simplifie leur maintenance et leur mise à jour.

### **7. Anticiper l'approche "BYOD" (Bring your own device)**

On parle aussi de "BYOT" pour "Bring Your Own Tools". Cette approche consiste à encourager les employés utiliser leur smartphone et leur ordinateur portable personnel au bureau. Elle leur évite de jongler entre deux téléphones et deux PC, l'un privé, l'autre professionnel. *"L'indemnisation mensuelle des employés pour l'utilisation de leurs appareils est minime comparée à la charge de maintenance et d'administration des postes de travail"* constate Richard Peynot, dirigeant du cabinet Acseit. En revanche, pour simplifier la gestion de ces équipements, l'entreprise doit impérativement les intégrer à sa CMDB.

## Document 3 - Comment manipuler la base de registre Windows

Au coeur du système, le registre Windows contient toutes les données relatives aux paramètres matériels et logiciels de l'OS. Une base qu'il est possible de modifier sans grande difficulté, en prenant certaines précautions.

La base de registre est constituée de deux fichiers nommés *USER.DAT* et *SYSTEM.DAT*, qui se construisent à chaque démarrage par le système et se placent dans le répertoire *Windows/System32/config*. Certaines informations du registre sont stockées sur le disque, et sont considérées comme permanentes, tandis que d'autres sont stockées dans des clés volatiles et remplacées à chaque démarrage du système d'exploitation. Les données sont enregistrées dans des formats différents.

Pour accéder au registre, il faut saisir la commande *regedit* dans *démarrer/exécuter*. Le registre est constitué de 5 grands dossiers contenant des clés, des sous-clés et des rubriques valuées.

**HKEY\_CLASSES\_ROOT** contient les paramètres les plus importants des programmes. Il gère les extensions des noms de fichiers, les liaisons avec les logiciels ainsi que les serveurs ActiveX, les composants communs de Windows, les contrôles complémentaires. Il faut éviter de les modifier manuellement.

**HKEY\_LOCAL\_MACHINE** : il s'agit des paramètres de l'ordinateur (profils utilisateurs, composants matériels, configuration réseau, paramètres de sécurité et système). Ne pas le modifier manuellement.

**HKEY\_USERS** contient tous les profils utilisateurs chargés activement.

**HKEY\_CURRENT\_CONFIG** supporte la configuration actuelle. Il est préférable de ne rien modifier.

**HKEY\_CURRENT\_USER** : contient les paramètres propres à l'utilisateur : apparence, curseur de la souris... Il est lié à **HKEY\_USERS**. Il est possible de modifier certains éléments, par exemple effacer les clés restantes d'un programme désinstallé.

Une manipulation utile et sans danger, est de faire une copie du registre : *Fichier>exporter*. Elle sera utile en cas d'attaque de la base de registre, ou d'erreur de modification. Dans la rubrique *Étendue de l'exportation*, sélectionner *tout*. Il est conseillé de toujours avoir une copie récente. Pour enregistrer certains éléments séparément, choisir *Branche sélectionnée* dans la rubrique *Étendue de l'exportation*. L'exportation se fait sous la forme d'un fichier dont l'extension est *.reg*.

Pour travailler régulièrement sur la même clé sans avoir à la rechercher à chaque fois, sélectionner dans le menu *Favoris>Ajouter aux favoris*.

L'accès au registre peut être sécurisé en cliquant sur *Edition>Autorisations*. Dans *Paramètres avancés*, attribuer les droits aux utilisateurs dans l'onglet *Autorisations*. L'onglet *Audit* permet de mettre une surveillance sur un utilisateur. L'observateur

d'évènement fournit ensuite la liste des accès. Il se trouve dans *Panneau de configuration/Outils d'administration/Gestion de l'ordinateur/Observateurs d'évènements*. Cliquer sur le journal *Sécurité*.

Chaque clé est éditable et modifiable. Elle correspond à un événement et contient une valeur. Redémarrer Windows après chaque modification est nécessaire et permet de vérifier si le système fonctionne toujours normalement. Attention, ces manipulations sont réservées à des utilisateurs experts. De mauvaises modifications peuvent mettre en péril l'ensemble du système.

Par exemple, pour supprimer l'icône *volume* dans la barre des tâches, ouvrir la clé *HKEY\_CURRENT\_USER/Software/Microsoft/Windows/Currentversion/Applets/SysTray*.

Elle contient le code suivant :

*Windows Registry Editor Version 5.00*

*[HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionAppletsSysTray]*

*"Services"=dword:0000001f*

Modifier la valeur de *Services* en la remplaçant par *dword:0000001b*

Pour désactiver le centre de sécurité Windows, ouvrir la clé *HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Services/wscsvc*

Dans le code :

*Windows Registry Editor Version 5.00*

*[HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSetServiceswscsvc]*

*"Start"=dword:00000002*

Modifier la valeur *Start* par *dword:00000004*. Pour passer en mode manuel, mettre la valeur *dword:00000003*.

Pour modifier le message *"Ne communiquez jamais votre mot de passe ou votre numéro de carte bancaire dans une conversation sur messagerie instantanée"* qui apparaît à l'ouverture d'une fenêtre de discussion sous Windows Messenger, modifier la clé :

*HKEY\_LOCAL\_MACHINE/SOFTWARE/Microsoft/MessengerService/Policie*.

Le message est à modifier dans le code :

*Windows Registry Editor Version 5.00*

*[+HKEY\_LOCAL\_MACHINESOFTWAREMicrosoftMessenger*

*ServicePolicieIMWarning] @="ici le message affiché dans Windows Messenger"*

## Document 4 - Débuter avec MDT 2013

### I. Présentation

Ce tutoriel s'adresse aux néophytes en matière de déploiement Windows, et a plus précisément pour but de vous de présenter l'installation de base de la solution de déploiement gratuite de Microsoft. J'ai nommé le désormais célèbre « **Microsoft Deployment Toolkit** » alias « *MDT* » .

Vous trouverez probablement sur la toile de nombreux tutoriels relatifs à MDT, et celui-ci n'a pas la prétention d'être meilleur que les autres. En fait, il s'agit là de vous présenter quelques fondamentaux que j'enrichirais par des articles complémentaires permettant de progresser à votre rythme et selon vos besoins.

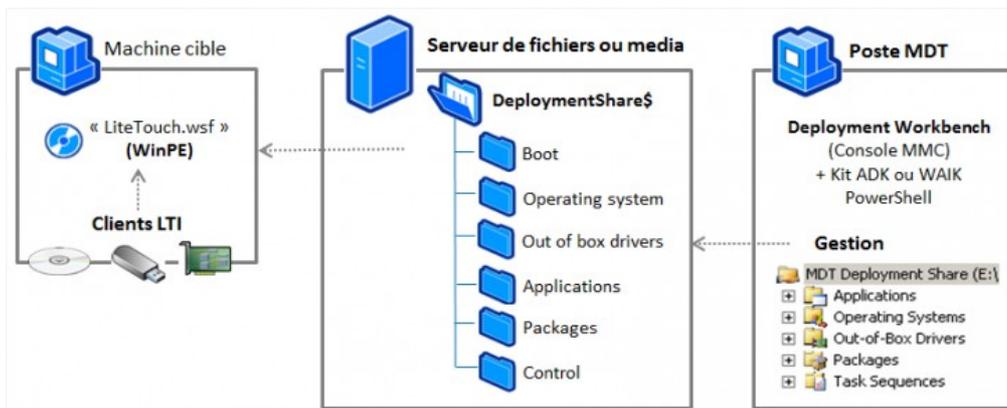
### II. Un peu de théorie

Loin de moi l'idée de détailler l'intégralité d'un outil aussi riche et complexe que le MDT, mais je pense quelques points de repères et de vocabulaire sont toujours bons à prendre pour les débutants :

#### A. Architecture et composants

Sur le plan technique, le MDT repose principalement sur le kit de déploiement Windows ADK, (anciennement WAIK) constituant un prérequis impératif. L'architecture de cet outil est articulée autour de 3 parties fondamentales :

- La **console de gestion** : Alias « **Deployment Workbench** » (ou « Atelier de déploiement ») : C'est une console graphique de type MMC, exécutée sur un poste Windows (32 ou 64 bits) sur lequel ont été installés le kit de déploiement Windows ADK, et le package MDT. Notez que Powershell est également un prérequis.
- Le **point de distribution** : Sauf dans le cas particulier d'usage d'un « Media », il s'agit d'un **dossier partagé** (Nom par défaut « **DeploymentShare\$** ») – Tout serveur de fichier SMB/CIFS, Windows ou Linux peut faire l'affaire...
- Le **client LiteTouch** : Basé sur un noyau WinPE utilisant principalement un script « **LiteTouch.wsf** » , ce client chargé de connecter et d'interpréter des scripts (.vbs/.wsf) et directives publiées (.xml) sur le point de distribution. Comme tous les noyaux WinPE, il peut être utilisé sur des supports flash USB, des CD/DVD ou bien via le réseau PXE, typiquement via les services WDS (Windows Deployment Services)



Pour rappel : Les services de déploiement Windows (WDS) constituent une composante facultative de l'architecture MDT.

Au besoin, reportez-vous à ma présentation sur « Vue d'ensemble de MDT-WDS et WinPE » qui aborde une synthèse de ces concepts.

## B. Mécanismes et éléments clés de configuration

A l'usage, vous constaterez que le MDT draine des notions de « scénarios de déploiement ». En fait, cela désigne la logique que les scripts vont emprunter pour traiter les différents cas de figures possibles.

Cette logique très complexe de scripts, sera pondérée et contrôlée par les réglages que vous pourrez définir dans les « **séquences de tâches** ». Pour traiter les cas courants, le MDT propose des séquences de tâches prédéfinies qui vous pourrez adapter à votre guise.

### 1. Les scénarios possibles

Les scénarios sont donc composés d'un ensemble de tâches pouvant débuter par un test de prérequis(\*), une sauvegarde des données d'utilisateur ou une capture de référence puis installer un système d'exploitation et d'éventuelles applications, pour s'achever par une restauration des données d'utilisateur. Les scénarios prennent en charge 4 cas de figure :

- **Upgrade Computer** : Mise à jour sur place d'un même ordinateur (Sous réserve que le système d'exploitation soit supporté)
- **Refresh Computer** : Réinstallation sur un même ordinateur (récupération préalable des données d'utilisateur)
- **Remplace Computer** : Installation sur un nouvel ordinateur (récupération des données d'utilisateur à partir de l'ancien ordinateur)
- **New Computer** : Installation d'un nouvel ordinateur (L'éventuel contenu existant est supprimé) – Ce scénario ne peut être exécuté que lorsque l'ordinateur est démarré à partir d'un noyau WinPE (Client LiteTouch) – En fait, c'est plutôt rationnel puisqu'il n'est tout bonnement pas possible de supprimer les partitions d'un système en cours d'utilisation.

(\*) – Pour votre gouverne et bien qu'il s'agisse d'un concept avancé, voire de spécialiste, sachez que durant l'initialisation du client LiteTouch, le script

« *ZTIGather.wsf* » effectue une collecte d'informations sur l'environnement afin de positionner des variables qui influenceront les séquences de tâches par la suite.

## 2. La ressource partagée « **DeploymentShare** »

Au niveau de la ressource partagée (« *DeploymentShare\$* » par défaut), on distingue particulièrement les dossiers suivants :

- **Boot** : Contient les fichiers .WIM et éventuellement .ISO correspondants aux images WinPE modifiées « LiteTouch », nécessaires à l'initialisation de la connexion et l'exécution des tâches définies sur le serveur de fichiers.
- **Operating Systems** : Contient les fichiers sources des distributions Windows (Copies intégrales des CD ou DVD d'origine ou images .WIM issues de capture)
- **Out-of-Box Drivers** : Contient les fichiers de pilote tiers au format .INF nécessaires aux images WinPE et aux systèmes d'exploitation à installer
- **Packages** : Contient les packs de langues, correctifs et mises à jour des systèmes d'exploitation au format .CAB ou .MSU
- **Applications** : Contient les applications au format .MSI ou .EXE. qui seront exécutées en post-installation.
- **Control** : Contient les séquences de tâches à exécuter (« ts.xml ») dans des sous-dossiers, ainsi que la plupart des fichiers .xml de configuration du MDT. Au passage, j'attire juste votre attention sur la présence de 2 fichiers .INI particulièrement intéressants et importants que sont « bootstrap.ini » et « CustomSettings.ini » sur lesquels nous aurons l'occasion de revenir.

En bref, la majeure partie des réglages du MDT est contenue dans des fichiers .XML Il fortement déconseillé de modifier ces fichiers, ou toute autre manipulation directement au sein de cette structure. En effet, la quasi-totalité des actions de configuration MDT, mais aussi les copies, renommages, déplacements, etc doivent impérativement être réalisés via la console « **Deployment Workbench** » .

Pour finir sur cette présentation théorique, notez que la structure MDT est « transportable ». Vous pouvez à loisir stocker vos travaux sur un disque amovible, un lecteur réseau ou un média de votre choix. Pour l'exploiter, il suffira d'utiliser une machine sur laquelle le MDT est installé, de connecter la ressource puis d'ouvrir cette structure existante à partir de la console.

## Document 5 - Master Windows 7\_ A l'aide de MDT et WDS

L'informatique est un outil de travail indispensable dans le monde de l'entreprise. La sécurisation et la standardisation des outils de travail évite les erreurs humaines et augmente la productivité.

Au niveau de la gestion des postes de travail dans les grosses entreprises l'automatisation de l'installation des systèmes d'exploitation, des applications, des patches de sécurités et des règles de sécurités est indispensable.

Pour mettre en œuvre ces procédures automatiques, nous nous appuyons sur les outils qui permettent d'automatiser des tâches de façon centralisée comme :

- Des outils de télédistribution de
  - système d'exploitation
  - patches
  - packages applicatifs
  - règles de sécurité
- Des outils de protection et de sécurisation
- Des outils de prise en main à distance

Pour répondre à ces besoins, nous avons fait le choix d'un déploiement de Windows 7 administré par biais d'un Master déployé à l'aide d'un serveur de télédistribution.

Nous allons décrire ci-dessous la conception d'un master Windows 7 à l'aide du kit MDT et WDS.

### 1. Objectifs et outils de Master Windows 7

Le Master a pour objectif d'automatiser l'installation des composants suivants :

- Windows 7 Pro X64 français/anglais.
- Les drivers.
- Framework Dot Net / C++ / XML
- Les applications sont communes aux entités.
- Les applications personnalisées par entités.
- Les customisations.

Les kits et service suivants vont être utilisés pour créer le Master.

- ADK 8.1
- MDT 2013 – Windows 7
- WDS sous windows 2008 R2 (Windows Deployment Services)

Hardware:

Un serveur de type HP ProLiant DL 360 (Génération 6 minimum) afin de supporter l'installation de dix machines en simultanées. Un simple poste de travail suffira pour deux postes en simultanés.

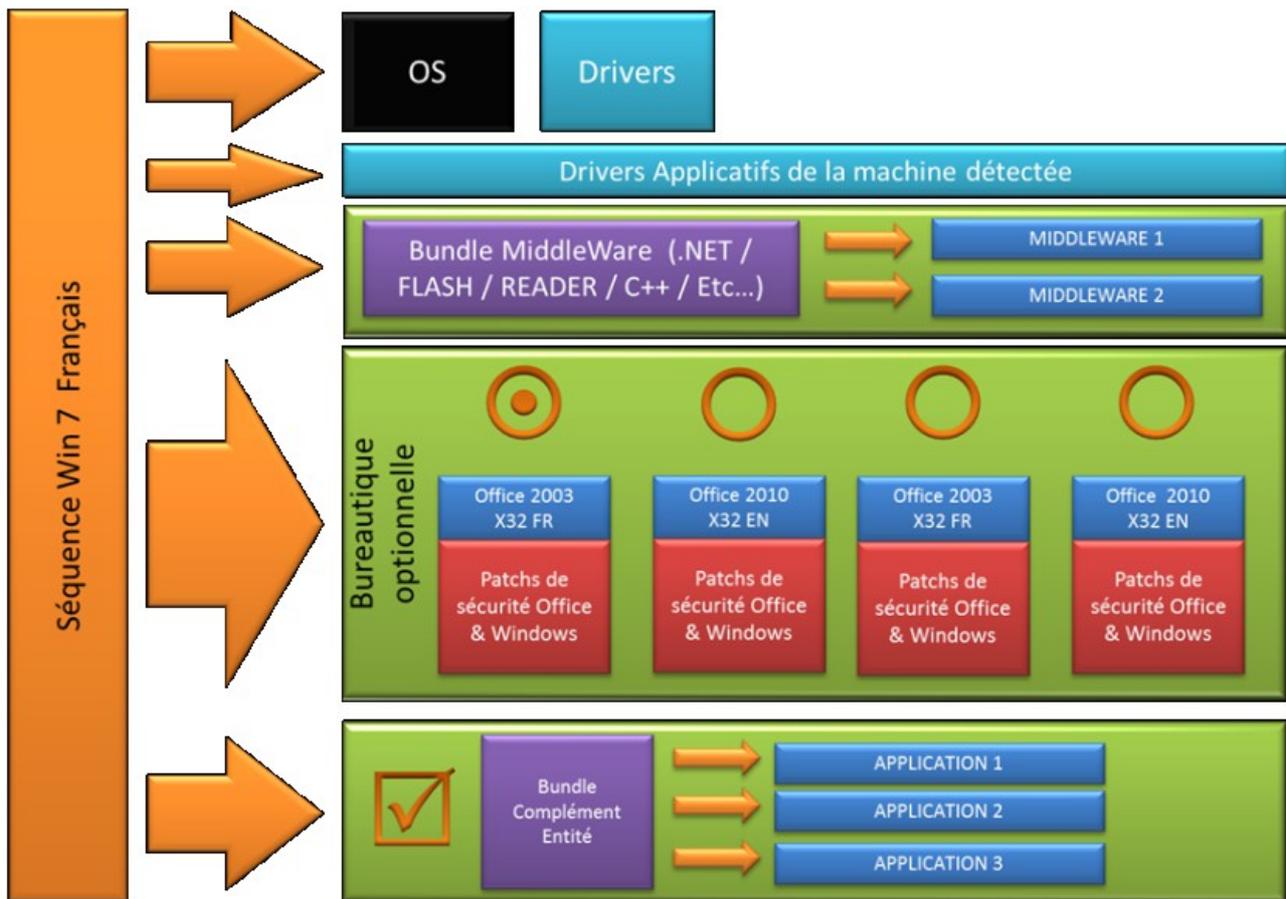
Réseau :

- Un switch Giga 4 ports minimum (avec un cache correct pour ne pas avoir des performances limitées par le réseau).

- Le serveur WDS sera dans un environnement isolé, hors du réseau de production. Le serveur suivra le principe d'une « nursery », les postes ne seront pas intégrés au domaine AD de production automatiquement mais permettront une masterisation de masse. Les postes seront ensuite envoyés sur les différents sites de production.

## 2. Création de l'environnement technique de masterisation

Les couches du master seront installées dans l'ordre suivant :



## 3. Les différents types d'images de masterisation.

Chaque type d'image a ses avantages et ses inconvénients. Nous allons les expliquer ci-dessous :

- Image fichier

Un fichier WIM contient des métadonnées et les fichiers contenus sur une partition. Contrairement aux fichiers images orientés secteurs (Ghost par exemple), WIM contient les informations sur les fichiers contenus dans la partition.

- Image binaire

Le ghost est un procédé de conversion du contenu d'un disque dur Bit à bit ainsi que ses paramètres de configuration et ses applications en une image.

#### **4. Les différentes architectures de master se basant sur les différents types d'images.**

La technologie de masterisation à utiliser dépend :

- Du nombre de type de machine
- Du nombre de langue
- De la possibilité ou non de faire des choix optionnels
- Du choix multiple de système d'exploitation

Deux types de master peuvent être créés avec des spécificités différentes.

- Le master de type image
  - Un seul type de machine
  - Une seule langue
  - Un seul système d'exploitation
- Le master séquentiel
  - Plusieurs types de machine
  - Plusieurs langues
  - Plusieurs systèmes d'exploitation
  - Installation d'applications optionnelles
  - Ajout d'action de type « intégration au domaine automatique »

Le mode image (ex : Ghost) ne peut pas apporter la flexibilité nécessaire à un master complexe et personnalisable. Nous lui préférons donc le mode séquentiel (Unattended).

#### **5. Le principe du fonctionnement de la télédistribution d'un système d'exploitation(WDS)**

WDS est un service Windows qui a pour fonction la distribution via le réseau, des images de système d'exploitation. Le service WDS se base sur les Protocoles PXE, TFTP, DHCP.

- PXE (Pré-boot exécution environnement)

Le Preboot Execution Environment (PXE ) est une interface client / serveur standard de l'industrie qui permet aux ordinateurs en réseau qui ne sont pas encore chargés avec un système d'exploitation d'être configurés et démarrés à distance par un administrateur . Le code PXE est typiquement livré avec un nouvel ordinateur sur une puce de mémoire en lecture seule (sur la carte réseau) ou un disque de démarrage qui permet à l'ordinateur (client) de communiquer avec le serveur de réseau. Un système d'exploitation peut alors être installé via le réseau sans CDROM ou clé USB. PXE se base sur offre trois choses:

Le Dynamic Host Configuration Protocol (DHCP), ce qui permet au client de recevoir une adresse IP pour accéder aux serveurs de réseau.

Un ensemble d'API qui sont utilisés par le BIOS de l'ordinateur client et qui permet de télécharger un NBP (Network Bootstrap Program), petit programme qui permet d'automatiser le démarrage du système d'exploitation ou de son installation.

- Activation du boot PXE

Pour activer le PXE, il faut que la carte réseau soit intégrée dans les périphériques de boot et que le technicien appuie sur la touche F12.

Les phases d'initialisation du PXE sont les suivantes :

- Téléchargement du fichier à amorcer depuis un serveur trivial FTP.
- Exécution du fichier à amorcer.

Déroulé des opérations préalables :

- ETAPE 1 : Préparation des disques
- ETAPE 2 : Installation d'un serveur Windows 2008

ETAPE 3 : Paramétrage de l'adresse IP du serveur

Le serveur sera ensuite promu contrôleur de domaine. Il faut donc définir une adresse IP fixe.

ETAPE 4 : Installation du contrôleur de domaine

WDS dans la version Windows 2008 R2 nécessite l'utilisation d'un contrôleur de domaine (contrairement à la version Windows server 2012 qui permet un mode stand-alone), nous allons donc promouvoir notre serveur en DC .

ETAPE 5 : Installation des services DHCP et WDS

Le service WDS nécessite l'installation du service DHCP. Nous allons donc l'installer en même temps que WDS.

ETAPE 6 : Installation de ADK 8.1

Nous allons installer le kit ADK 8.1 qui regroupe tous les outils en ligne commande permettant de gérer les images (WIM).C'est un prérequis à l'utilisation de MDT 2013.

ETAPE 7 : Préparation d'un environnement DeploymentShare dans l'outil Deployment Workbench.

## **6. Création d'un Master Windows 7**

L'environnement de masterisation étant prêt il faut avant de définir la séquence de tâche préparer les éléments suivants :

- Rechercher une correspondance pour les périphériques inconnus
- Télécharger les sources de drivers correspondants
- Télécharger les applications (Redistribuable), ne nécessitant pas de connexion internet pour s'installer.

Une fois les ressources intégrées au Deploymentshare, nous créerons une séquence de tâche pour ordonnancer les tâches d'installations.

## **7. Référencement et recherche de périphériques**

Lorsque des périphériques sont inconnus, c'est-à-dire qu'ils n'ont pas de drivers associés pour trouver le fabricant ou le nom du périphérique effectuez les actions suivantes :

## **8. Les différents types de drivers**

Il faut différencier les drivers Plug-And-Play, des drivers applicatifs.

Les drivers Plug-And-Play sont des drivers installable directement pendant l'installation de Windows. Ils sont souvent composés des fichiers Sys/ Inf /Cat.

Les drivers applicatifs sont quant à eux composés de drivers de base (Sys/ Inf /Cat), et d'une surcouche applicative permettant des fonctions avancées. Les sources d'installation sont en principe de type setup.exe.

Le driver applicatif est installé après l'installation du système d'exploitation et est déclenché par une séquence de tâche.

## **9. La gestion dynamique des drivers**

Pour ne copier sur le disque dur et n'installer que les drivers nécessaires à la machine, il faut mettre en place une detection de la machine et une gestion dynamique des drivers

La gestion dynamique des drivers se fait à deux niveaux :

Le premier niveau concerne les drivers Plug-and-Play. Une fois le chemin connu par le setup de Windows, le mécanisme de détection de driver Plug-and-Play s'effectue de façon automatique.

Le deuxième niveau concerne les packages de drivers applicatifs. Un filtre WMI permet de filtrer les packages à installer selon les machines. Les packages sont installés par la séquence de tâche après l'installation de Windows.

Déroulé des opérations :

ETAPE 1 : Intégration OS

ETAPE 2 : Création d'une séquence de tâche

La séquence de tâche est la colonne vertébrale de l'installation du master sous MDT 2013. Elle séquence et ordonne les tâches à effectuer.

Nous allons donc créer cette séquence de tâche.

## **10. Gestion des applications**

### **11. Personnalisation de l'installation de Windows**

### **12. Personnalisation de l'interface de l'assistant d'installation**

### **13. Intégration du boot dans WDS.**

## Document 6 - Windows 10 – Nouveautés sur le déploiement

### I. Présentation

Avec Windows 10, Microsoft assène un sérieux coup aux techniques de déploiement et de mise à jour de son système. L'idée de fond, n'est pas moins que le « zero-master » QU'ES ACO ? En gros, le technicien de déploiement devient une espèce en voie d'extinction !... Comment ? Eh bien, le deal est approximativement le suivant : L'utilisateur se procure un appareil quelconque (pré-équipé de Windows 10 bien sûr), et il doit être en mesure d'achever tout seul sa mise à jour et la configuration de son système (comme disent les anglo-saxons : « User Friendly » ).

Par quel moyen ? Eh bien soit via une simple clé USB, ou un média amovible (Technique FFU – Full Flash Upgrade), soit au travers d'une jonction à un domaine (direct ou Azure AD) afin qu'il reçoive en retour un package de configuration type pour que son appareil intègre son organisation d'entreprise) Waouh – rien que ça !

Avant toute chose, notez que depuis Windows 10, Microsoft supporte pleinement la mise à jour sur place d'un système, contrairement aux versions antérieures où cette pratique était déconseillée en raison des pollutions et des disparités engendrées.

Nous allons aborder dans cet article, le nouveau concept des « packages de mise en service », dont le but est de simplifier les opérations de préparation et de configuration des « appareils » (pour ne pas dire PC/tablettes/téléphones) à l'échelle d'une entreprise, sans que cette installation ne requière de compétence particulière. Cette nouvelle possibilité d'installation est dénommée « Provisioning » .

Schématiquement on peut considérer que dorénavant vous avez le choix entre 3 techniques de déploiement:

- L'installation traditionnelle via une image WIM (Wipe And Load)
- La migration sur place d'un système Windows 7 et ultérieur (In-Place)
- Le provisionnement qui consiste à transformer un appareil en poste d'entreprise (Provisioning)

### II. Analyse des nouveautés liées au déploiement

#### A. Aperçu rapide des évolutions

##### 1. Nouveau format .ESD

Principalement destiné à délivrer des images Windows 10 à grande échelle via Internet, ce format de fichier .ESD est en fait une déclinaison compressée et chiffrée des célèbres images .WIM.

Vous trouverez d'ailleurs ces fichiers dans le dossier « \Sources » des distributions de Windows 10 obtenues via Internet, en lieu et place des anciens fichiers « Install.wim ». Ce qui pose quelques difficultés pour la suite, si vous avez récupéré une version PRO via Internet (Windows Update ou Media Creation Tool)

Notez qu'il existe un moyen de déchiffrer des fichiers .ESD afin de les convertir au format .WIM standard mais je ne suis pas persuadé que Microsoft approuve cette méthode...

## **2. WinPE**

Je n'ai pas relevé de modification majeure en matière d'outillage pour ce nouveau noyau. La version de ce nouveau WinPE est « 10.0.10240.16384 »

## **3. ADK 10**

Windows ADK10 inclut désormais un nouvel outil dénommé « Windows ICD » soit « Windows Imaging and Configuration Designer », qui pour la version française a été traduit par « Concepteur de fonctions d'acquisition d'images et de configurations (ICD) » .

Les packages de mise en service pour Windows 10 portent l'extension .PPKG et se comportent un peu comme les fichiers de réponse unattend.xml. A l'instar des images .WIM vous pouvez utiliser l'outil DISM ou 7-zip pour en visualiser le contenu.

Remarque : Le kit de migration, alias USMT a également évolué et son outil « Scanstate » permet dorénavant de sauvegarder l'état des applications installées sur un poste Windows 10 vers un package de mise en service.

Le package de mise en service avec applications ainsi obtenu peut être ensuite importé dans Windows ICD afin de créer un média.

## **4. MDT2013 Update1**

En pratique, hormis les certaines corrections de bugs, c'est la copie conforme de MDT2013, sauf que cette version supporte officiellement Windows 10 et requiert l'ADK10.

## **5. MDT2013 Update2**

Au gré des évolutions de ce fameux kit MDT, la logique de version retenue par les équipes Microsoft est manifestement déroutante, ou pour le moins étonnante. En effet, alors que MDT2013 marquait la fin du support Windows XP/2003, on aurait pu s'attendre à un MDT « 2015 » mais c'est une version MDT2013 Update 1 qui apporta le support officiel de Windows 10. La nouvelle version MDT2013 Update 2 est en fait une simple mise à jour qui ne comporte que très peu de nouveautés fonctionnelles. Cette liste non exhaustive vous donnera une petite idée :

- Intégration des derniers binaires du séquenceur « Configuration Manager »
- Amélioration sensible des séquences de tâches relatives à la mise à niveau vers

Windows 10

- Meilleure gestion des fichiers WIM fractionnés (split)
- Amélioration du niveau de détail dans les journaux, tels que smsts.log
- Meilleure gestion des autorisations NTFS sur le partage de déploiement
- Evolution de la cryptographie avec le support de l'algorithme de hachage SHA256
- Intègre la surveillance des séquences de mises à niveau dans la rubrique «

Monitoring »

- Correction de bugs ...

## **B. Installation de l'ADK**

Le principe est très similaire à la version précédente, à la différence que vous disposez de quelques outils supplémentaires. Parmi les plus flagrantes :

- Concepteur de fonctions d'acquisition d'images et de configurations (ICD)
- Kit d'évaluation de Windows (sous-ensemble de Windows Performance Toolkit)

## **C. Présentation de Windows ICD**

Objectifs de Windows ICD :

- Créez un package de mise en service que vous pouvez utiliser pour personnaliser des PC/tablettes/téléphones sans avoir à recréer des images.
- Générez une image Windows personnalisée pour des régions et des segments de marché spécifiques

L'outil `icd.exe` est également utilisable en ligne de commande.

## Document 7 - WINDOWS 7 : Préparez votre migration

### Maîtriser les outils et les étapes

La création d'un master de déploiement est une opération relativement simple. Tous les outils utiles sont livrés gratuitement par Microsoft au travers du kit « Windows automated installation kit » (aussi dénommé Windows AIK). Elle comporte 6 étapes importantes.

#### 1 - La création du fichier de réponse

Depuis votre poste de travail, copiez l'image install.wim du DVD d'installation de Windows 7 sur votre disque dur. Lancez « Windows system image manager » (W-SIM). Dans le menu « Fichier », sélectionnez « New Answer File » et ouvrez le fichier install.wim. Validez la création d'un nouveau catalogue. Il faut ensuite ajouter un à un les composants que l'on veut personnaliser. Le plus simple est de suivre le guide pas à pas incorporé dans le kit qui permet notamment de créer une installation ne demandant aucun renseignement à l'utilisateur. Une fois tous les paramètres de personnalisation sélectionnés, allez dans le menu « File » et sélectionnez « Save answer file », puis sauvegardez le fichier Autounattend.xml dans la racine d'une clé USB.

#### 2 - La préparation de la machine master

Installez maintenant Windows 7 sur une machine de test qui servira de master. Réalisez une installation propre en partant d'un disque dur vierge. Lors du processus d'installation, veillez à ce que la clé USB contenant le fichier Autounattend.xml créé à l'étape 1 soit bien présente sur ce poste. Installez également les applications que vous voulez voir figurer sur tous les postes. Une fois la machine installée et testée, utilisez la commande :

```
sysprep /oobe /generalize /shutdown
```

Celle-ci prépare la machine pour la création de l'image master. Cette finalisation retire notamment toute information propre au matériel (autrement dit à la machine de tests) de sorte que l'image puisse être déployée sur différents modèles de PC.

#### 3 - La préparation du CD Windows PE

Nous allons maintenant créer un CD de démarrage qui nous permette de réaliser une image disque de la machine master. Depuis votre machine habituelle (la machine master devant elle rester éteinte après le Sysprep), lancez l'invite de commande et placez-vous dans le dossier C:\Program Files\Windows AIK\Tools. Puis lancez la commande :

```
copy cmd x86 c:\winpe_x86
```

Pensez également à copier le programme Imagex.exe dans la réparation Windows PE :

```
copy "c:\program files\Windows AIK\Tools\x86\imagex.exe"
```

```
c:\winpe_x86\iso\
```

Puis lancez la commande qui permet de générer le fichier ISO du CD de démarrage.

```
oscdimg -n -bc:\winpe_x86\letfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Il n'y a plus qu'à graver le CD de démarrage à l'aide de n'importe quel outil capable de graver une image ISO (le fichier image est ici dans le dossier C:\winpe\_x86).

#### **4 - La création de l'image WIM de la machine master**

Redémarrez votre machine master depuis le CD Rom créé à l'étape 3. Lorsque l'invite de commandes apparaît, utilisez la commande Net use pour déclarer un dossier partagé sur le réseau et la commande ImageX pour créer le fichier WIM à déployer.

```
net use N: \\Serveur_Fichiers\NosImages  
imagex /capture D: D:\win7image.wim "Exemple Install Win7" /compress fast /verify  
copy D:\win7image.wim N:
```

La commande ImageX est extrêmement puissante. Elle permet non seulement de créer et déployer des images master, mais également de les mettre à jour. Il est important que vous en appreniez toutes les subtilités.

#### **5 - Le déploiement de l'image WIM depuis un serveur**

Il ne reste plus qu'à vérifier que le master se déploie correctement. Prenez une machine de tests, démarrez la sur le CD Windows PE créé à l'étape 3 puis à l'invite de commande, saisissez les commandes suivantes:

```
diskpart  
select disk 0  
clean  
create partition primary size=100  
select partition 1  
format fs=ntfs label="system"  
assign letter=c  
active  
create partition primary  
select partition 2  
format fs=ntfs label="Windows"  
assign letter=d  
exit
```

Pour éviter d'avoir à ressaisir systématiquement toutes ces commandes, il est largement conseillé d'en faire un script et de l'installer sur l'image ISO (avec la commande ImageX). Il suffira alors d'appeler la commande: DISKPART /s MonScript.txt.

Puis il ne reste plus qu'à lancer la commande ImageX pour transférer l'image WIM sur la

machine de tests:

```
net use y: \\network_share\images
copy y:\myimage.wim d: e:\
imagex.exe /apply d:\myimage.wim 1 d:
d:\windows\system32\bcdboot d:\windows
```

## **6 - La maîtrise des outils DISM et USMT**

Il ne vous reste plus qu'à apprendre à maîtriser deux nouvelles composantes du Windows AIK : USMT et DISM.

USMT vous sera essentiel dans la récupération des anciennes configurations (paramètres et fichiers des utilisateurs) et leur injection sur les nouvelles machines. [...]

DISM (Deployment image servicing and management) est le nouvel outil qui centralise toute la gestion du cycle de vie de vos images « masters » : élaboration, maintenance et diffusion. Depuis cet outil unique, vous pouvez très facilement monter/démonter des images système, configurer les paramètres internationaux, gérer l'inventaire de vos différentes images masters, enrichir ou supprimer les pilotes qu'elles contiennent, mettre à jour les logiciels et patches qu'elles embarquent. En outre, DISM offre toutes ces fonctionnalités, aussi bien sur les fichiers WIM que sur les disques virtuels VHD. Un point particulièrement important lorsque l'on sait qu'il est désormais possible de démarrer Windows 7 depuis des disques virtuels, ce qui permet ainsi d'élaborer et tester bien plus facilement différents masters depuis une même machine de tests. En outre, cette capacité à démarrer sur des VHD permet aux administrateurs d'imaginer de nouveaux scénarios de maintenance. Enfin, DISM est entièrement pilotable, ce qui permet de très facilement créer des scripts de génération de nouvelles images et de masters. Cela devrait également faciliter l'apparition sur le marché de nouveaux outils d'aide au déploiement plus interactifs et basé sur DISM.