Déploiement de postes avec MDT 2012

François Clémence

Université de Lorraine – Direction du Numérique

UFR Sciences Humaines et Arts – Ile du Saulcy  
57000 Metz

Résumé

Pour déployer le plus efficacement possible leurs systèmes d'exploitation sur les postes de travail, les services informatiques optent souvent pour des configurations matérielles les plus homogènes possibles. Ces choix stratégiques favorisent l'utilisation d'outils de clonage de disques durs (libres ou propriétaires).  
  
Toutefois, depuis plusieurs années, l'utilisation de ces outils très populaires, est mise à mal par les évolutions matérielles incessantes des gammes de produits et par le multi-équipement constaté chez les utilisateurs. La gestion d'un nombre croissant de profils matériels devient rapidement un véritable casse-tête pour les équipes informatiques.  
  
Au sein de parcs machines composés 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.   
  
L'objectif de cette présentation est d'exposer les différentes solutions proposées par Microsoft et plus particulièrement le scénario "Lite-Touch" reposant sur le produit gratuit "Microsoft Deployment Toolkit" (version 2012).   
  
En 2012, un groupe de travail a été constitué au sein de l'Université de Lorraine, pour étudier cette technologie. Elle est aujourd'hui déployée dans plusieurs établissements et donne entière satisfaction. En complément, et sous forme de retour d'expérience, un bilan sera dressé sur la mise en place et les limites constatées de cette technologie.

Mots-clefs

Postes de travail, MDT, ADK, Microsoft, Déploiement, Lite-Touch

# Introduction

Pour déployer 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.

# Présentation générale

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 (fichiers 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. 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 qui apporte une réelle souplesse. Diverses solutions gratuites utilisant ce format d'image sont proposées par Microsoft :

* 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.
* Stratégie « Lite-Touch » : elle est adaptée à un environnement de 200 à 500 ordinateurs et s'appuie sur le programme Microsoft Deployment Toolkit 2012 (MDT 2012). 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. Cette méthode peut être compatible avec des parcs de plus de 500 machines.
* Solution « Zéro-Touch » : elle est conseillée sur des parcs de plus de 500 postes et s'appuie sur le produit Microsoft System Center Configuration Manager (SCCM). Elle nécessite donc une architecture appropriée. Le déploiement est alors entièrement automatisé.

Nous avons testé la suite Lite-Touch qui correspondait bien à notre besoin. L'infrastructure demandée est légère et facile à déployer. L'interface de l'application est claire et une documentation abondante est disponible pour une mise en production rapide. L'utilisation de séquence 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, un paramétrage en profondeur de Windows est possible.

Concernant les logiciels clients, 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 allons voir dans la partie suivante, le schéma de fonctionnement de MDT 2012 dans un scénario « Lite-Touch » de déploiement de Windows 7, puis nous ferons un retour d’expérience sur cette solution en abordant les points les plus délicats.

# Fonctionnement de MDT 2012

## Pré-requis serveurs et logiciels

Sans surprise, MDT s’appuie sur des briques Microsoft. Bien qu’un fonctionnement dans un environnement non Active Directory soit techniquement possible, cette configuration n’est pas recommandée. Nous considérerons donc qu’un domaine Active Directory et un serveur DNS Microsoft sont en place dans la suite de cette présentation.

Par ailleurs, bien que l’on puisse déployer les clients sans, un serveur DHCP, Microsoft ou non, est également fortement conseillé afin de faciliter la configuration réseau des machines. L’objectif est que les clients puissent récupérer automatiquement une adresse réseau afin de charger l’image de démarrage permettant de lancer l’environnement de travail. De la même façon, nous conseillons l’utilisation de Windows Deployment Services ou WDS, introduit avec Windows 2008, il fournit un système de déploiement automatisé permettant la distribution des images par le réseau. Ce scénario technique (DHCP et Boot PXE) est largement utilisé dans les outils de déploiement usuels (Clonezilla, FOG, Symantec Ghost Solution Suite…).

L’installation de MDT peut s’effectuer sur un OS type « poste de travail » comme Windows 7 ou Windows 8. Cependant, afin d’utiliser ultérieurement l’option de multidiffusion, il est plutôt conseillé d’utiliser Windows 2008R2 ou 2012. Le package MDT se présente sous la forme d’un fichier MSI. Son installation a été largement simplifiée depuis la version 2010, notamment pour les pré-requis logiciels.

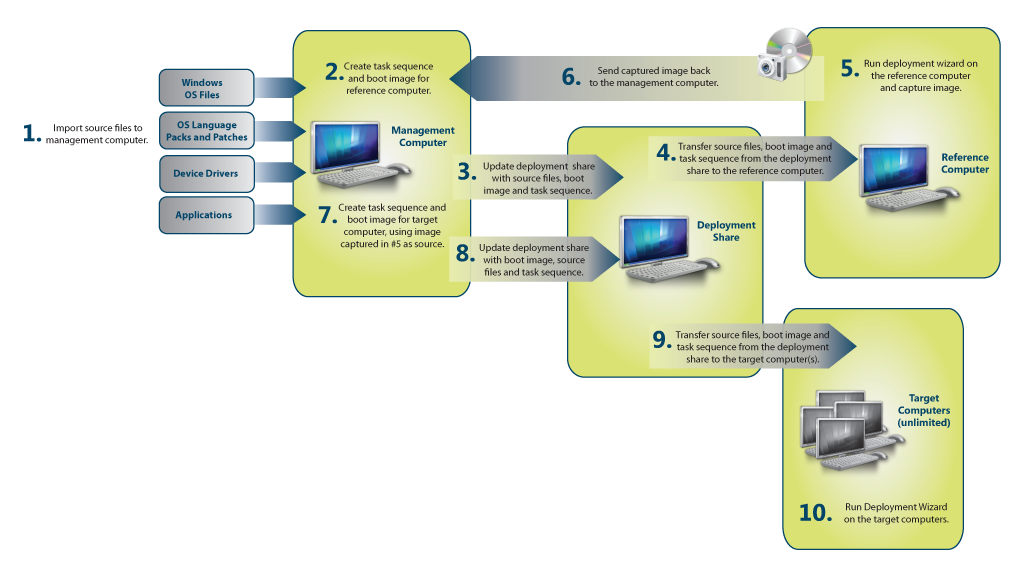
Le composant le plus critique reste cependant l’installation de la suite facilitant le déploiement des systèmes Windows. Deux choix sont possibles WAIK ou ADK.

* 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.
* 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.

WAIK étant un composant en fin de vie, ne permettant pas le déploiement de Windows 8, **nous conseillons donc l’utilisation systématique d’ADK**. Nous conseillons également l’installation de tous les composants du kit ADK dont SQL Server 2012 Express. En effet, ce produit peut être utilisé pour configurer les postes dans MDT et ainsi fournir un déploiement automatisé.

## Processus de capture et de déploiement

Le fonctionnement de MDT peut être illustré avec le schéma fourni (source *Microsoft)* :



1. processus MDT

Ce processus peut se résumer de la sorte :

* 1-4 : Collecter les fichiers et paramètres sur le serveur MDT afin d’installer automatiquement la machine de référence ou « maître » :

Les sources des OS à déployer

Les packs de langues si nécessaire

Les pilotes et les applications nécessaires à la machine de référence

Créer une séquence de tâche de déploiement qui va installer le poste référence

* 5-6 : Déployer le système sur la machine de référence puis capturer l’image ainsi obtenu sur le serveur MDT
* 7-9 : Créer et paramétrer une nouvelle séquence de tâche qui va déployer l’image précédemment capturée sur les postes clients
* 10 : Déployer en masse l’image de référence sur les postes clients

# Retour d’expérience et difficultés rencontrées

Il n’est pas possible dans cette présentation d’exposer tous les aspects d’une migration Windows XP vers Windows 7 et de présenter en profondeur MDT 2012. Ce logiciel est en effet très riche et de nombreux scénarios de déploiement existent dans le logiciel comme le remplacement d’un ordinateur en migrant les données de l’utilisateur ou la mise à niveau d’un poste existant. Nous allons cependant nous intéresser uniquement au scénario de déploiement sur de nouvelles machines où le disque dur est intégralement formaté.

Nous avons testé cette procédure avec succès dans notre périmètre sur plus de 500 machines. D’autres composantes ont également adopté le produit pour le déploiement Windows au sein de l’Université de Lorraine. Lors de notre projet, nous avons cependant rencontré quelques difficultés techniques. Nous allons donc revenir sur ces différents points.

## Gestion des partages de distribution

Une fois installée, MDT 2012 se présente sous la forme d’une console appelée « Deployment Workbench ». Elle comporte deux parties :

* le centre d’information qui présente les documentations et rappelle les composants installés
* 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, dossiers, applications, drivers, scripts et paramètres nécessaires aux opérations de production du poste de travail.

Un « Deployment Share » est piloté par deux fichiers de configuration, accessibles facilement dans les propriétés du partage de distribution :

BootStrap.ini : ce fichier est utilisé par le poste client 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

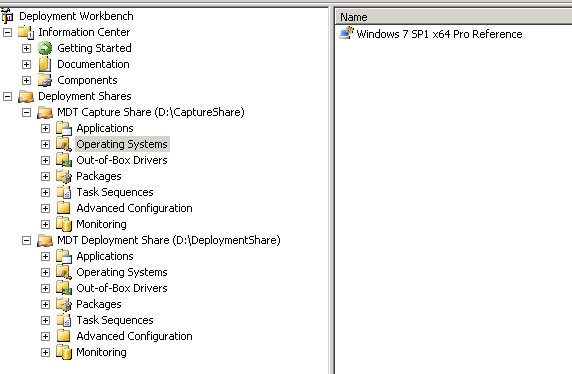
UserID=mdt

UserPassword=\*\*\*\*

CustomSettings.ini : ce fichier, également spécifique à chaque partage de distribution, pilote le déploiement du poste client. Il existe près de 300 options différentes et les possibilités de configuration sont extrêmement variées. Il existe essentiellement deux types de paramètres, les « skip » et les autres. Une option qui commence par « skip » va déterminer si l’assistant ou « Wizard » va être affiché (« skip=NO ») ou non (« skip=YES ») lors du processus de déploiement. L’objectif d’une installation silencieuse est donc de cacher le maximum d’écrans de configuration afin d’automatiser le processus.

Un problème subsiste: certains paramètres du CustomSettings.ini sont incompatibles entre eux. Par exemple, il n’est pas possible de combiner les paramètres liés à l’intégration dans un groupe de travail et 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 conseillons vivement l’utilisation de deux « Deployment Share » :**

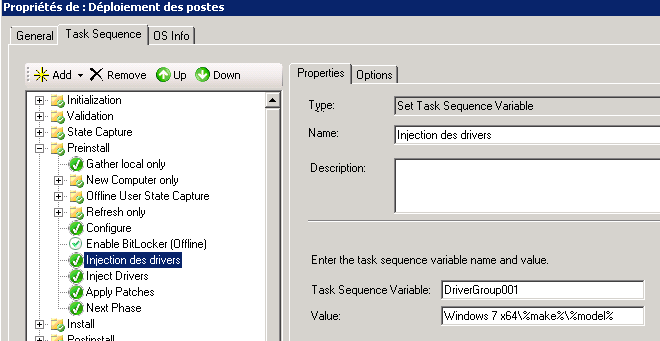
* un « Deployment Share » pour le déploiement et la capture de l’image de référence
* un autre « Deployment Share » pour le déploiement en masse des postes clients, comme illustré ci-dessous.

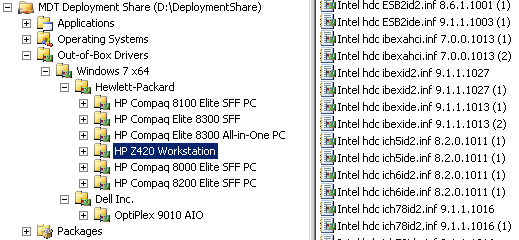


1. Utilisation de deux partages de distribution

## Gestion des pilotes

Nous allons nous intéresser ici à la gestion des pilotes pour les systèmes Windows que l’on souhaite déployer. Il existe en fait trois méthodes :

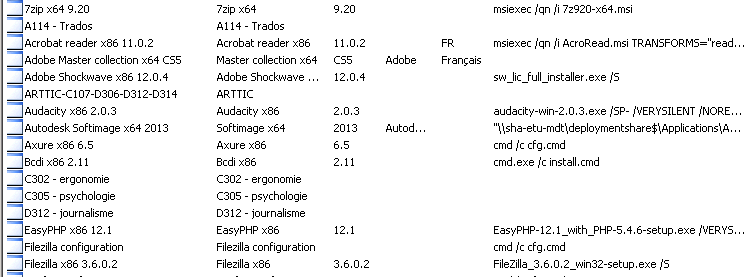
* Par système d’exploitation : on charge tous les pilotes dont on dispose par système d’exploitation, dans un répertoire « Out-of-Box Drivers » sur le serveur MDT. Cette méthode est efficace si l’on dispose de très peu de modèles différents de machines et d’un seul système d’exploitation à déployer.
* Par profil de sélection : cette méthode est une variante de la première. Ici on souhaite déployer plusieurs OS différents sur le parc avec toujours très peu de modèles de machines. Cette option fait appel à la création d’un profil de pilotes par système d’exploitation et à son injection dans la séquence de tâche de déploiement.
* **Par constructeur et par type de machine : c’est la méthode à systématiquement privilégier selon nous**. On va tout d’abord récupérer le nom exact du modèle (par la commande « systeminfo » par exemple) puis on va créer l’arborescence adéquate dans MDT. Le paramétrage de la séquence de tâches est indiqué ci-dessous.



1. La gestion des pilotes dans MDT

## Gestion des applications

La gestion des logiciels clients se fait dans le dossier « Applications » sur MDT. Chaque application doit être « préparée » avec les commutateurs silencieux adéquats. La tâche est aisée avec les fichiers MSI mais peut être beaucoup plus ardue selon les logiciels. Cette phase dépasse largement le cadre de la présentation. A noter, des « paquets » logiciels peuvent être réalisés, afin de gérer plus facilement les dépendances applicatives ou les logiciels utilisés dans les salles informatiques. Les applications peuvent être sélectionnées manuellement dans l’assistant de déploiement ou automatisées par le fichier CustomSettings.ini. L’utilisation d’une base de données est également possible.



1. Présentation des applications dans MDT

Une question importante concerne également la stratégie d’intégration des applications. Faut-il intégrer les applications directement dans l’image de référence ou les installer ensuite de façon silencieuse lors de l’installation du poste client ? Il existe trois approches différentes :

* Constituer une image « fine » : on déploie un système d’exploitation basique sur le poste référence. Aucune application n’est installée afin de garder une image système la plus légère possible. On va ensuite installer les applications et pratiquer le paramétrage du poste client via MDT.
* Image dite « épaisse » : c'est-à-dire effectuer une capture complète de l'environnement de l'ordinateur de bureau avec son système d'exploitation, ses pilotes, ses applications et son paramétrage, puis la restituer sur les postes clients. L’image .WIM sera très conséquente sur le serveur et peu « agile ».
* Une « image hybride », qui est un compromis entre les deux solutions précédentes, en incluant des applications et des personnalisations basiques qui s'appliqueront à chaque utilisateur. **C’est la solution que nous conseillons.** L’objectif est d’inclure dans l’image de base les applicatifs les moins susceptibles de varier et les plus répandus sur le parc, comme Microsoft Office. A l’inverse, il est préférable de déployer une application comme Firefox lors de l’installation du poste client, afin de profiter d’un logiciel toujours à jour lors des déploiements d’image.

## Utilisation de la base de données

MDT peut être couplé à une base de données SQL Server 2012 Express afin de peupler de façon dynamique le fichier CustomSettings.ini. Cette option peut être particulièrement utile pour associer par exemple une adresse réseau à un nom de machine ou des paramètres spécifiques. Les options générales seront appliquées à tous les postes, tandis que les spécificités seront gérées par les entrées de la base de données.

Les possibilités sont vraiment très nombreuses et il est possible d’aller très loin dans l’automatisation et la personnalisation. L’interface dans MDT reste cependant assez lourde et bien que des requêtes du type « Web Service » soient possibles, il n’existe pas d’interface Web de gestion et de saisie, ce qui réduit selon nous l’utilité de cette fonctionnalité. Un projet non-Microsoft, en version béta, existe cependant « MDT Web FrontEnd » mais son développement reste incertain. Pour toutes ces raisons, **nous n’utilisons pas l’outil base de données** et nous rentrons le nom de machine manuellement lors du lancement du poste client, opération qui peut être automatisée si nécessaire. L’installation des pilotes, des applications et le paramétrage restent ensuite totalement transparents.

# Conclusion

Nous avons présenté une solution permettant de déployer massivement et rapidement des postes Windows, portables ou fixes, sur un parc informatique constitué de solutions matérielles hétérogènes. Le scénario « Lite-Touch » utilisant MDT 2012 s’avère à l’usage particulièrement performant puisqu’il permet de minimiser drastiquement le nombre d’image système à gérer en s’appuyant sur les fichiers au format WIM. A titre indicatif, nous sommes passés de 25 fichiers imageà 2, pouvant être déployés dynamiquement avec des applications toujours à jour

Cette solution permet un déploiement du poste de travail de façon quasiment automatisée en s’appuyant sur deux fichiers de configuration et une base de données optionnelle. Riche et performante, cette approche est également totalement gratuite. L’infrastructure, basée sur des briques Microsoft, est également simple et peu coûteuse à mettre en place. Cette solution, que nous recommandons dans les environnements Windows, est particulièrement adaptée dans le cadre de migration visant à abandonner Windows XP. A condition de disposer cette fois de moyens financiers, les DSI pourront même s’orienter vers le scénario « Zéro-Touch » en s’appuyant sur la suite SCCM, offrant alors un déploiement de parc Windows totalement automatisé.

Annexe

Fichier CustomSettings.ini pour le « Deployment Share » de déploiement et capture du poste de référence. On remarquera l’utilisation d’un serveur « WUS » en fin de configuration pour faciliter les mises à jour Windows.

[Settings]

Priority=Default

Properties=MyCustomProperty

[Default]

\_SMSTSORGNAME=MDT2012

OSInstall=Y

SkipAppsOnUpgrade=NO

SkipAdminPassword=YES

SkipProductKey=YES

SkipComputerName=NO

SkipDomainMembership=YES

SkipUserData=YES

UserDataLocation=AUTO

SkipLocaleSelection=YES

SkipTaskSequence=NO

SkipTimeZone=YES

SkipApplications=NO

SkipBitLocker=YES

SkipSummary=YES

SkipBDDWelcome=YES

SkipCapture=NO

DoCapture=YES

SkipFinalSummary=NO

TimeZone=105

TimeZoneName=Romance Standard Time

UILanguage=fr-FR

KeyboardLocale=040c:0000040c

UserLocale=fr-FR

JoinWorkgroup=WORKGROUP

WSUSServer=http://\*\*\*\*.fr

Fichier CustomSettings.ini pour le « Deployment Share » de déploiement en masse avec intégration au domaine. On remarquera ici la centralisation des fichiers de « logs » et l’activation du suivi des déploiements « EventService » sur le serveur MDT.

[Settings]

Priority=Default

Properties=MyCustomProperty

[Default]

\_SMSTSORGNAME=MDT2012

OSInstall=Y

SkipAppsOnUpgrade=NO

SkipAdminPassword=YES

SkipProductKey=YES

SkipComputerName=NO

SkipDomainMembership=YES

SkipUserData=YES

UserDataLocation=AUTO

SkipLocaleSelection=YES

SkipTaskSequence=NO

SkipTimeZone=YES

SkipApplications=NO

SkipBitLocker=YES

SkipSummary=YES

SkipBDDWelcome=YES

SkipCapture=YES

SkipFinalSummary=NO

TimeZone=105

TimeZoneName=Romance Standard Time

UILanguage=fr-FR

KeyboardLocale=040c:0000040c

UserLocale=fr-FR

SLShareDynamicLogging=\\SHA-ETU-MDT\DeploymentShare$\Logs

JoinDomain=DOMAIN

DomainAdmin=DOMAIN\mdt

DomainAdminPassword=\*\*\*\*

WSUSServer=http://\*\*\*\*.fr

EventService=http://\*\*\*\*:9800

Bibliographie

1. **Microsoft**, Papier Blanc du format WIM. <http://go.microsoft.com/fwlink/?LinkId=92227>

2. **Microsoft**, Choix d'une stratégie de déploiement. <http://technet.microsoft.com/en-us/library/dd919185%28WS.10%29.aspx>

3. **Yannick Plavonil.** Blog sur le déploiement Windows. <http://www.revuedugeek.com>