

# Vue d'ensemble de MDT-WDS et WinPE | Déploiement MDT - WDS | IT-Connect

Christophe Mandin

## I. Présentation

Avant d'aborder un sujet aussi vaste que celui du déploiement Windows, je pense qu'il convient de préciser quelques points et par la même occasion combattre quelques idées reçues.

En premier lieu, pour ceux qui débarqueraient d'une autre planète, je vais vous parler des principales technologies de déploiement Microsoft.

### A. WDS (Windows Deployment Services)

C'est le service de déploiement Windows. Autrement dit un « rôle » facultatif disponible sur toutes les versions Windows Server depuis 2003R2. (Pour la petite histoire, son ancêtre se dénommait RIS pour « *Remote Installation Service* ») – En quelques mots, ce service assure 2 fonctions majeures : Le déploiement des images WIM pour les systèmes d'exploitation Windows et la fourniture d'images de démarrage (via PXE) pour l'initialisation des processus d'installation (ou de réparation).

### B. MDT (Microsoft Deployment Toolkit)

C'est l'outil d'automatisation de la fabrication (et d'installation) des systèmes Windows. Pour la petite histoire, son ancêtre se dénommait « BDD2007 » pour « *Business Desktop Deployment* ». Puis le produit a évolué au fil des années pour devenir MDT2008, 2010, 2012 puis dernièrement 2013. La version sera très probablement revue lors de la sortie de Windows 10. Ce produit est donc disponible en téléchargement gratuit, mais son usage requiert un kit complémentaire nommé WAIK (Pour *Windows Automated Installation Kit*) devenu Windows ADK (Pour *Assessment and Deployment Kit*)

**Le MDT est en fait une console graphique (de type MMC) dont l'objectif est de fédérer des sources, réaliser l'assemblage et proposer des séquences de tâches pour piloter le tout...**

En quelques mots, la solution de déploiement fait référence à 2 grands types d'usage ou d'implémentation :

– Si vous utilisez MDT sans le produit commercial Microsoft SCCM (*System Center Configuration Manager*), les scénarios proposés par MDT seront de type « LiteTouch » ou « LTI » en abrégé. C'est-à-dire qu'en l'absence de mécanisme tiers, il restera donc toujours une intervention humaine, aussi infime

soit-elle pour les déploiements, d'où le nom « LiteTouch », pour légère intervention.

– Dès lors que la solution MDT est couplée à SCCM, il est possible de fédérer entièrement les processus de déploiement, jusqu'à la planification du déclenchement. Microsoft a donc déposé le nom « ZeroTouch » ou « ZTI » en abrégé pour désigner ce type de scénarios de déploiement, sans intervention humaine, sauf en cas de problème bien sûr



Cette précision reste toutefois purement culturelle, car la composition du MDT et les principes de fonctionnement restent les mêmes. Vous pourrez simplement constater que les raccourcis MDT [autres](#) que le « *Deployment Workbench* » mentionnés ci-après, sont inopérants en l'absence d'infrastructure SCCM.

### **C. WinPE (Windows Pre-execution Environment)**

C'est un incontournable. Très grossièrement, si cette allusion vous parle, c'est le remplaçant de l'ancestrale

disquette DOS. Il s'agit en fait d'un noyau système minimaliste est présent pratiquement partout depuis Vista. C'est-à-dire que vous pourrez le trouver, à quelques nuances près, sur un DVD d'installation, dans le MDT sous la forme d'un client **LiteTouch**, au sein des images de démarrage WDS, sans oublier sa déclinaison « **WinRE** » pour les procédures de réparation.

## II. Combattre quelques idées reçues

### A. Que me faut-il pour déployer automatiquement Windows ?

L'installation automatisée d'un système Windows requiert un fichier de réponse. Par exemple un fichier « *autounattend.xml* » présent sur un support amovible ou le DVD, pourra faire l'affaire. En utilisant WDS vous aurez l'avantage de ne pas être limité par le support (disques du serveur), mais l'inconvénient du transport de fichiers volumineux (bande passante du réseau).

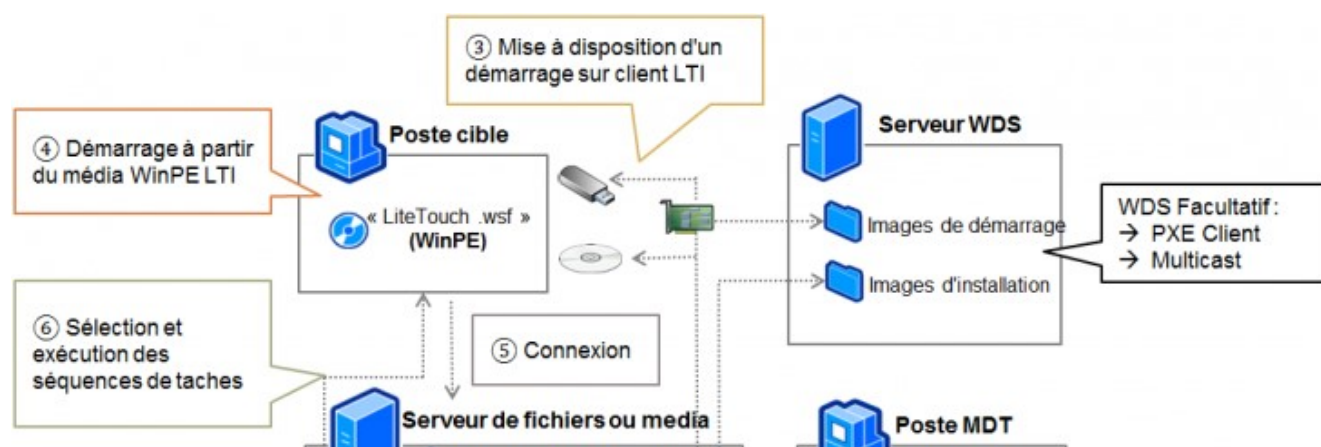
**Le premier intérêt de WDS est d'offrir une « dématérialisation » des DVD de distribution afin de les centraliser sur un serveur et fournir par la même occasion un système d'amorçage via le réseau PXE.**

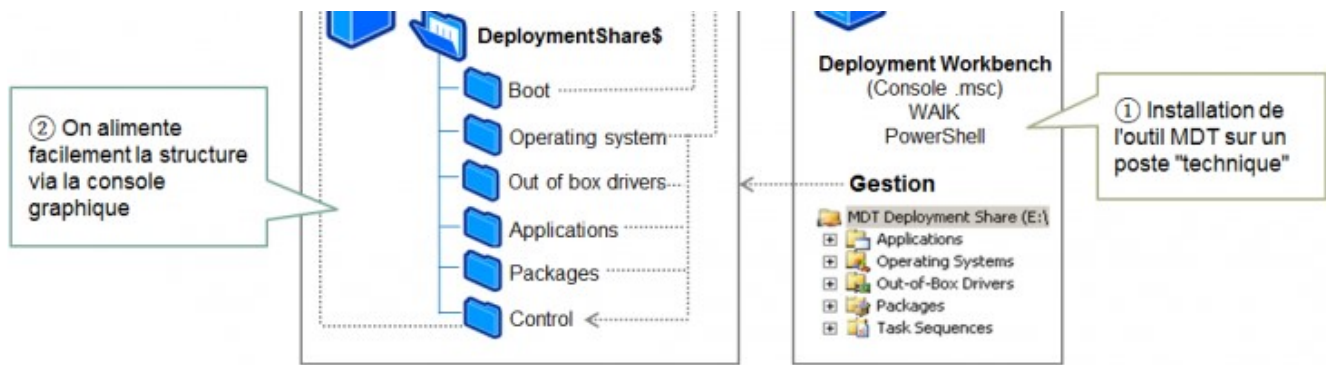
Le second avantage de WDS (depuis 2008R2) est d'offrir une capacité de flux multiples dits « multicast ». Le déploiement d'images identiques est alors réduit de façon significative dès lors que le nombre d'ordinateurs ciblés est important. (>5)

Notez cette subtilité très intéressante : Contrairement aux versions antérieures à Windows Server 2012R2, le serveur WDS n'a plus besoin d'appartenir impérativement à un domaine Active Directory. Autrement dit, dorénavant, vous pouvez installer un serveur WDS en mode « autonome », ce qui me semble un choix parfaitement adapté à des déploiements en mode « atelier ».

Si vous ne souhaitez pas utiliser WDS, alors MDT peut suffire. Il présentera l'énorme avantage de produire automatiquement les fichiers de réponse par défaut. Toutefois, WDS et MDT ne sont pas exclusifs l'un de l'autre. Au contraire, j'affirmerais même qu'ils sont complémentaires.

Comme on dit souvent qu'un schéma vaut mieux qu'un long discours, je vous propose un petit extrait d'une de mes présentations sur les principes MDT et WDS.





Cette illustration montre la complémentarité des différents composants utilisés dans une solution de déploiement Windows.

## B. Faut-il dédier un serveur pour MDT ?

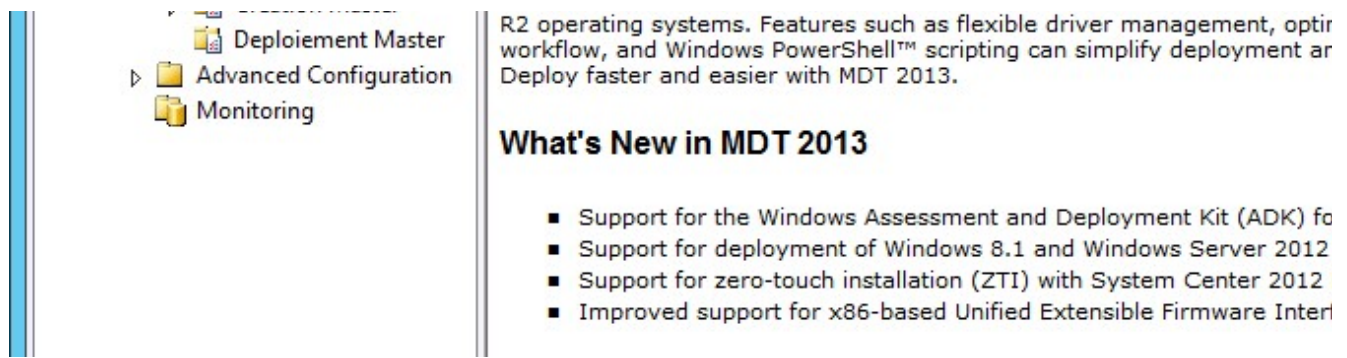
Non, en fait, si vous avez compris le schéma précédent, un poste MDT basé sur un système tel que Windows 7 32 ou 64 bits peut suffire. En fait, ce que l'on pourrait désigner par « le poste d'administration MDT », est un système Windows, poste de travail ou serveur, sur lequel sont installés le MDT et l'ADK.

**Note :** L'usage d'un système Windows Server peut être toutefois plus approprié afin de disposer d'une infrastructure de base plus efficace, et lui ajouter des rôles tels que WDS ou encore DHCP.

Le partage « *DeploymentShare\$* » du MDT, mentionné sur l'illustration ci-dessus, n'est pas nécessairement stocké sur un serveur de fichier Windows (Un NAS sur [Linux](#) Samba peut aussi faire l'affaire) et vous pouvez connecter la console « Deployment Workbench » vers un chemin UNC (sous réserve de fournir les bonnes identités « credentials »).

Pour vous faire une première idée de ce à quoi ressemble MDT, voici ci-après un aperçu de la console aussi appelée « **Deployment Workbench** », que l'on peut traduire littéralement par « Atelier de déploiement »





Console « *Déploiement Workbench* »

Notez qu'il est très facile, au grès des nouvelles versions de MDT, de mettre à jour un partage de déploiement, mais c'est une opération irréversible ! Donc, si vous installez des versions différentes de MDT, vous devrez vous astreindre à administrer des partages bien distincts.

**Je vous conseille également de réaliser toutes vos opérations de copie ou de déplacement de dossier et de fichiers au sein de la console MDT, et d'éviter les modifications directes de la structure MDT.**

Enfin, il est souvent conseillé d'avoir plusieurs MDT dédiés aux [tests](#) et développements, à la fabrication des images de référence (masters), puis aux déploiements dans l'environnement de production.. En effet, même si le MDT peut paraître « souple » et convivial, il n'en reste pas moins un enchevêtrement complexe de scripts, souvent délicat à dépanner.

Ultime conseil : Pensez à vider régulièrement le journal « Audit.log » situé à la racine du partage de déploiement. Ce fichier consigne toutes les actions/modifications réalisées sur le MDT et peut s'avérer volumineux (surtout lors de vos phases de test)

### C. Peut-on utiliser WinPE comme un « live-cd » ?

Non, bien qu'il soit issu du même noyau, Windows PE n'est pas un système d'exploitation d'utilisateur à proprement parler et à ce titre ne propose qu'une licence d'utilisation limitée. Officiellement, en termes de licence, voici un petit extrait de ce que vous pourrez lire en installant le kit Windows ADK :

[...]

1. **INSTALLATION ET DROITS D'UTILISATION.** Vous êtes autorisé à installer et utiliser un nombre quelconque de copies du logiciel sur vos dispositifs, uniquement dans le but de déployer, d'entretenir, d'évaluer la qualité du système et d'évaluer vos systèmes et dispositifs sous les systèmes d'exploitation Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista, Windows 7, Windows 8 ou Windows 8.1.

[...]

Autrement dit, tout produit, même gratuit tel que LibreOffice est proscrit. On peut en déduire que seul

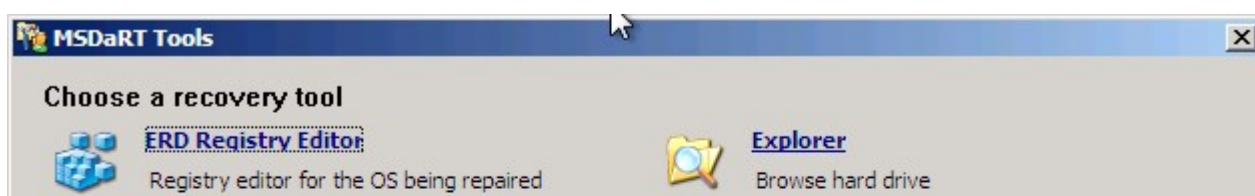
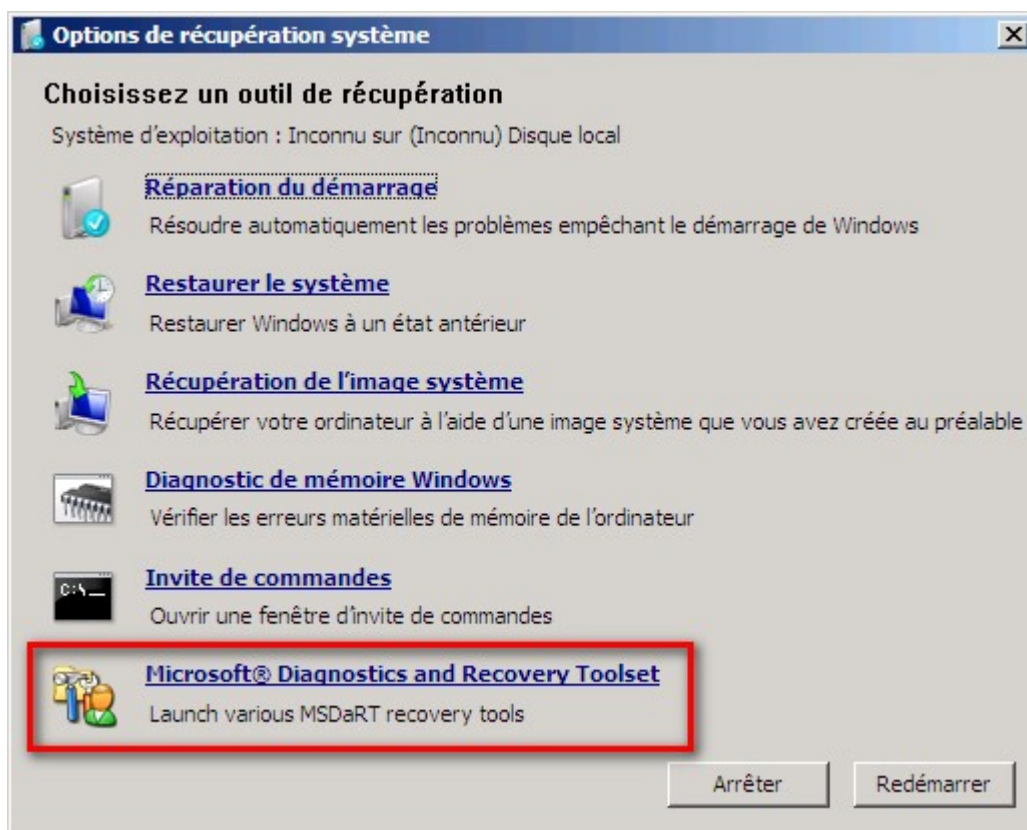
L'outillage au titre des déploiements ou réparations des systèmes Windows est toléré. Ainsi, je pense qu'on ne vous reprochera pas d'ajouter un explorateur de fichiers tel que « Explorer++ », mais l'ajout d'un navigateur « portable » tel que Firefox devient rapidement « borderline ».

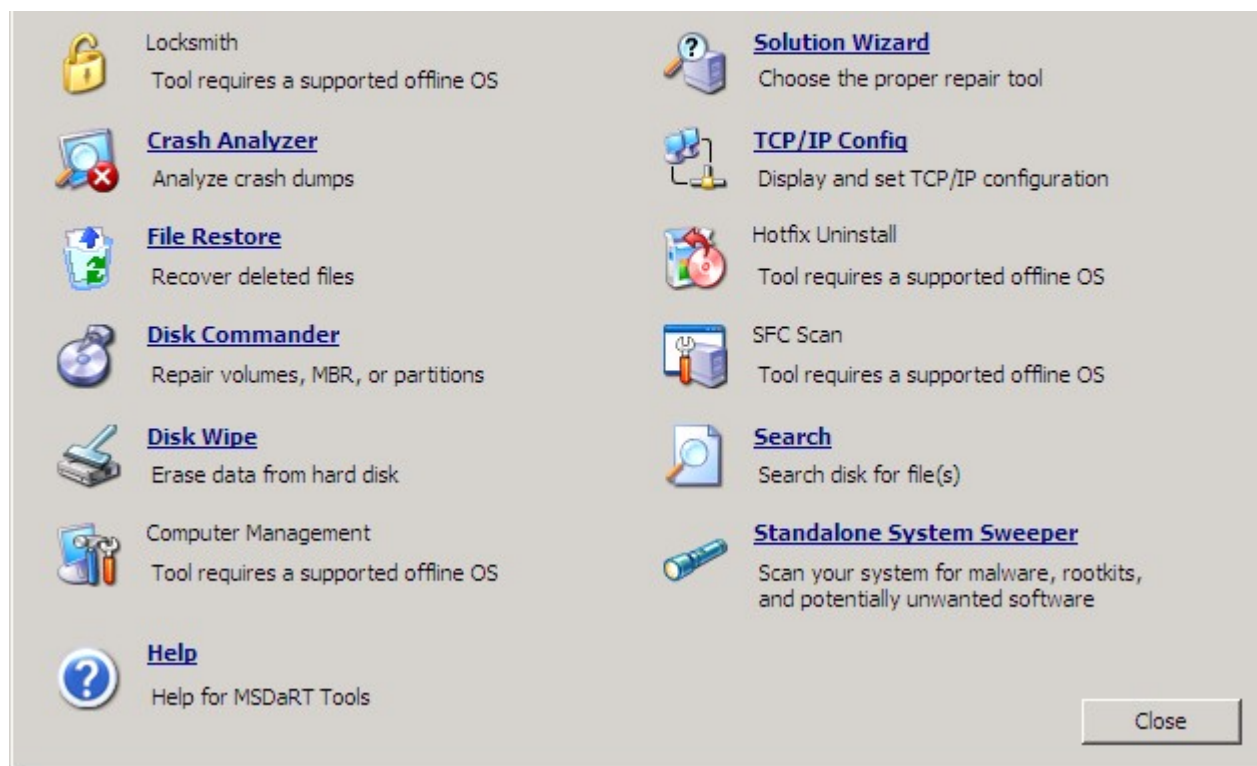
Quoi qu'il en soit, n'oubliez pas que WinPE est minimaliste, et qu'il ne supporte pas WoW (*Windows On Windows*). Autrement dit, sur un WinPEx64 ne tourneront que les binaires compilés 64 bits (beaucoup plus rares en freeware).

De plus, les services réseau tels qu'un accès à distance seront, comment dire ? problématiques... En effet, WinPE active un pare-feu par défaut, qu'il est possible d'inhiber, via l'outil spécifique « Wpeutil disablefirewall » ou bien encore via des commandes de type « netsh », mais Microsoft ne communique pas trop sur les limites d'usage.

En fait, le message subliminal que Microsoft veut faire passer, c'est que « *Windows PE* » est un système de type « client de déploiement », et pas un « Serveur » donc pas de connexions entrantes...

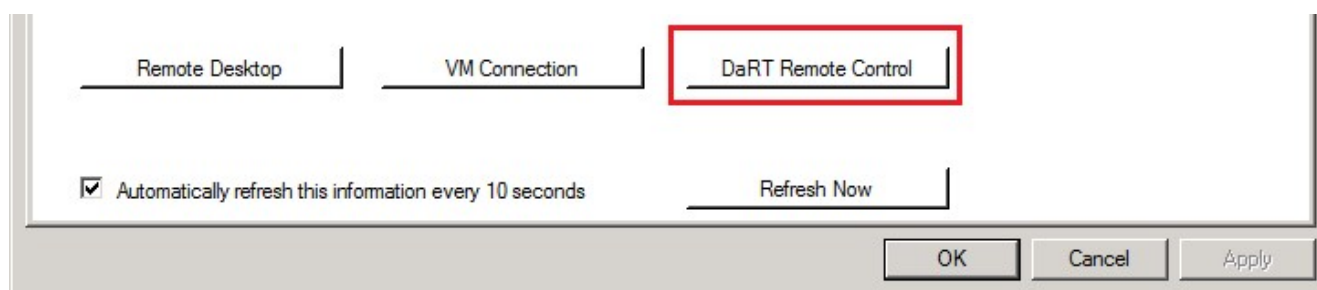
En toute franchise, j'aurais donc tendance à me limiter et m'inspirer de l'outillage offert par DaRT (*Diagnosis And Repair Toolkit*) fournit aux entreprises ayant souscrit un contrat Software Assurance MDOP (*Microsoft Desktop Optimisation Pack*).





À ce propos, depuis MDT 2012, via la fonction « **Monitoring** », Microsoft a prévu la possibilité d'effectuer des contrôles à distance vers les machines en cours de déploiement.

Ci-dessous : Aperçu des boutons de contrôle à distance, « potentiellement disponible » via les propriétés d'un poste en cours de déploiement via MDT :



Si cela vous intéresse, vous pouvez consulter une alternative possible VNC dans WinPE décrite dans le tutoriel dédié aux [personnalisations de WinPE...](#)

En conclusion, il est préférable de limiter ces adaptations à quelques outils propices aux opérations de maintenance, avec peut être un gestionnaire d'archives en plus, histoire d'ouvrir certains fichiers .zip, .7z, ou [autres](#) .rar... mais guère plus, afin de « rester dans les clous »...

#### D. Pourquoi ne faut-il pas cloner « directement » Windows ?

Ce sujet se prête souvent à des tergiversations selon les contextes ou les produits utilisés. Il est vrai qu'il sera plus facile de configurer une machine puis de cloner son état pour en faire des duplications, mais cela risque de vous exposer à des problèmes ou instabilités potentiels.

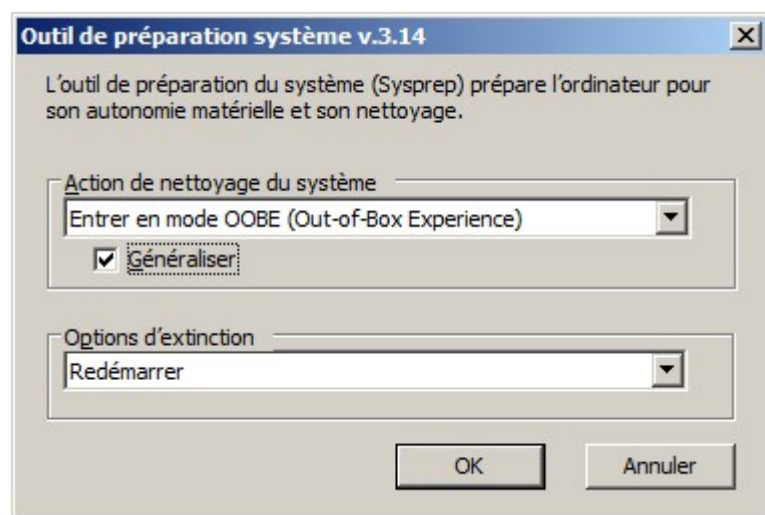
## 1. Utilisez impérativement « sysprep » avant une capture

Tout système Windows destiné à être dupliqué, typiquement les machines de référence (dit « Master ») doivent impérativement subir une préparation préalable, via l'outillage intégré « SYSPREP ». **L'usage de ce programme réalise un certain nombre de « dépersonnalisations » et remet la machine en condition de « réinstallation ».**

Parmi les plus importantes actions de sysprep, on peut relever :

- Nettoie les traces d'utilisation
- Supprime les pilotes tiers de périphériques
- Supprime la clé de licence et réarme le processus d'activation
- Régénère l'identifiant unique de sécurité local (SID) de l'ordinateur
- Passe le système en condition de « re-personnalisation » (OOBE – Out Of Box Experience)

Depuis Vista, l'outil « *sysprep.exe* » est systématiquement présent sous le dossier « %SystemRoot%\system32\sysprep » du système d'exploitation courant. Il peut être utilisé en ligne de commande ou graphiquement si vous n'indiquez aucun paramètre.

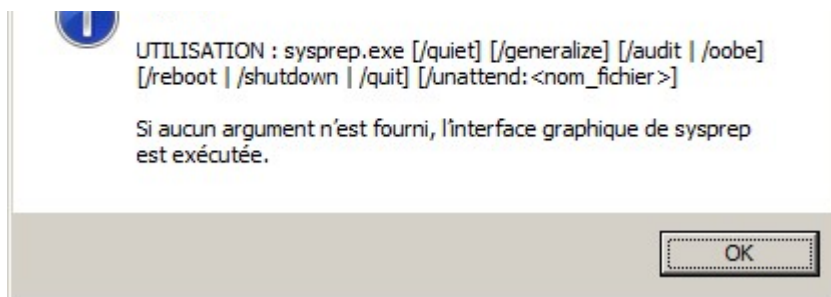


Préparer son système avec Sysprep

Les commutateurs sont obtenus par la commande « **sysprep /?** »







### Les commutateurs de SYSPREP

**Note :** Bien que cela ne soit pas imposé par l'outil lui-même, pour fabriquer un système de référence, il est fortement conseillé que la machine ne soit pas membre d'un domaine.

Autre recommandation : Si vous réalisez une machine de référence, prenez l'habitude de réactiver le compte administrateur intégré et éviter l'usage des autres comptes tels que celui de l'installation.

Il s'agissait ici de vous sensibiliser à cet outil fondamental, mais l'usage du MDT vous affranchira de cette contrainte et se chargera de la satisfaire à votre place.

Conseil : En matière de préparation d'un poste de référence, n'hésitez pas à exploiter des machines virtuelles et leur capacité de retour arrière, couramment appelé « Snapshots ». En effet, comme j'aurais pu le préciser précédemment, l'usage de l'outil « sysprep » supprime toutes les traces d'utilisation et, mais aussi les dépendances matérielles. Grâce à la virtualisation, vous pourrez donc reprendre la fabrication au point souhaité, tester l'efficacité du déploiement puis valider en dernier lieu le résultat sur une machine physique, en évitant de gaspiller un temps précieux lors de vos différents essais.

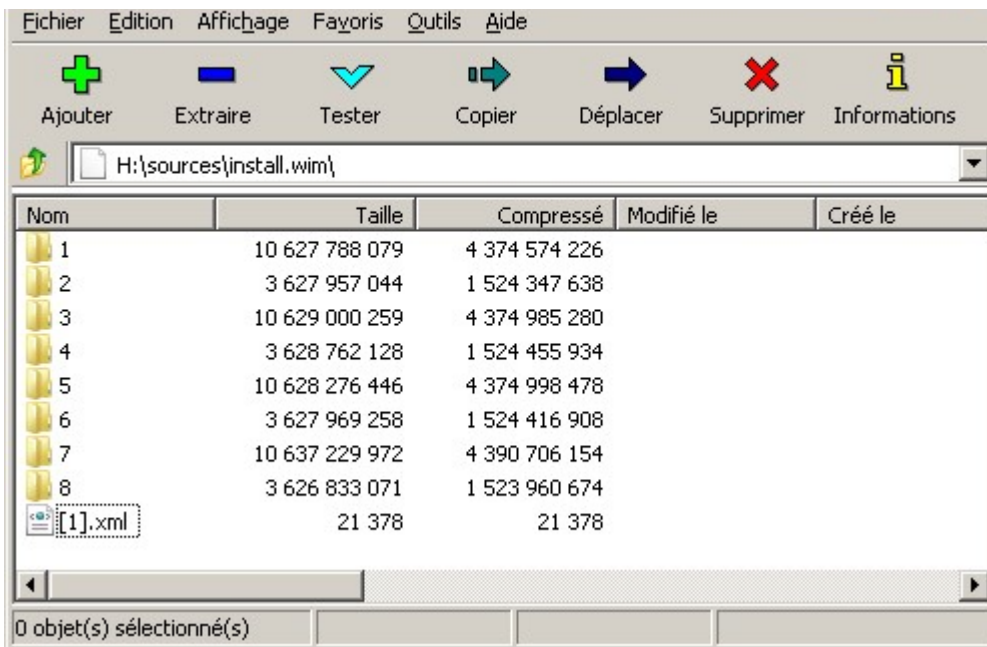
## 2. Les images .WIM, c'est quoi exactement ?

Comme vous pourrez le remarquer, **les fichiers .WIM sont au cœur des nouvelles technologies de déploiement Windows et la maîtrise de ces derniers est une clé essentielle en la matière.** Les fichiers .WIM sont des « conteneurs d'images », non au sens photographique, ni autres dessins d'artistes en herbe, mais une structure de fichiers et de dossiers (un peu comme un fichier archive de type .ZIP). À l'instar de ces archives, ils peuvent également bénéficier d'un mécanisme de compression, mais offrent d'autres avantages tels que l'instanciation unique des fichiers redondants, des métadonnées XML ...

**Note :** L'extension des fichiers WIM n'est pas prise en compte dans les interfaces graphiques Windows. Vous pouvez cependant recourir à l'utilitaire gratuit « 7-Zip » pour visualiser le contenu de ces fichiers. Dans le cas d'images multiples, chacune d'entre-elle apparaît sous forme d'un dossier représentant le numéro d'index alors que le fichier .xml à la racine contient les métadonnées.

Exemple d'ouverture d'un fichier .WIM contenant plusieurs images avec 7-Zip:

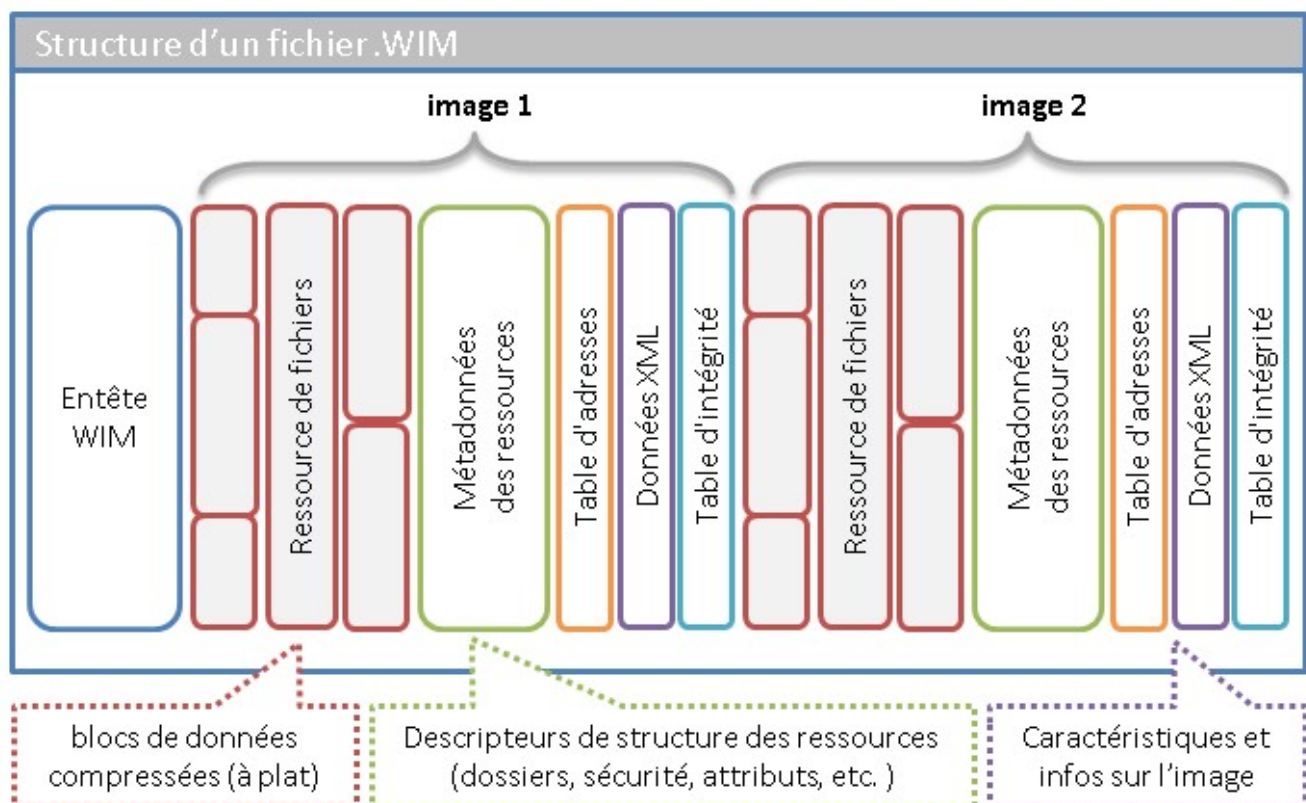




Structure d'un fichier WIM

Il faut toujours avoir à l'esprit qu'un fichier .WIM contient toujours une image au minimum. Chaque image étant identifiée par un index, il faut toujours stipuler ce numéro et ne pas oublier que les images sont indépendantes. Autrement dit, une modification apportée sur l'image donnée ne sera pas visible dans les autres images d'un même fichier. Toutefois, cette technique d'images multiples est essentiellement exploitée par les distributions Microsoft et plus rarement par les entreprises elles-mêmes.

La structure des fichiers .WIM :



Officiellement la manipulation des fichiers WIM s'effectue via les outils suivants :

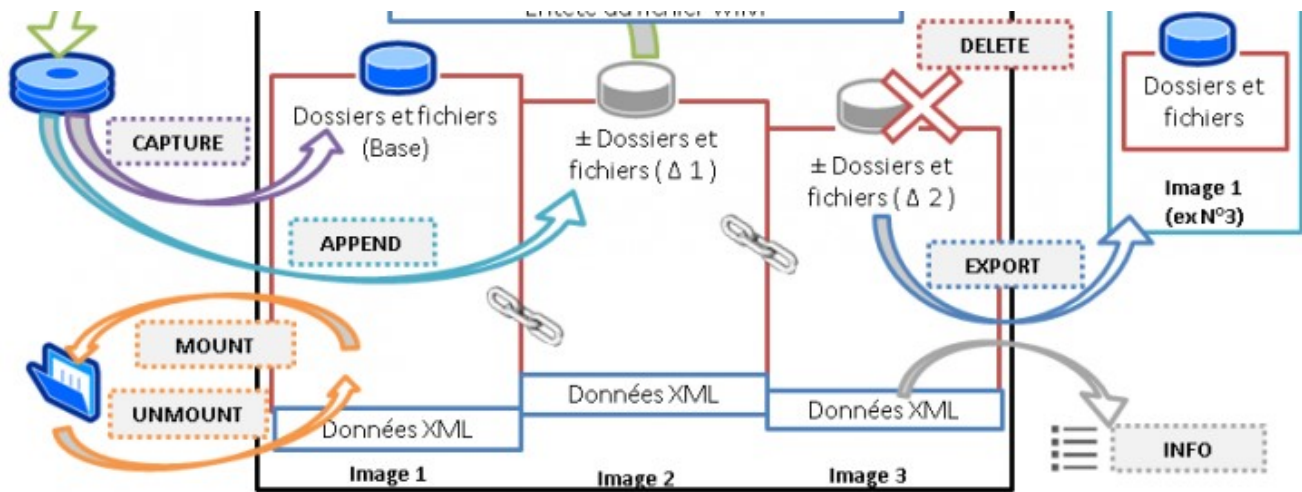
Outil	Description
<b>DISM</b>	C'est l'outil par excellence en matière de gestion des images .WIM en ligne de commande. Il permet de réaliser toute sorte d'action sur les fichiers WIM
<b>ImageX</b>	Cet outil en ligne de commande, initialement fournit au travers du kit WAIK puis ADK est en passe de disparaître totalement au profit de DISM. À l'origine, cet outil présentait l'avantage de pouvoir capture ou appliquer une image, mais les dernières versions de DISM le permettent également.
<b>GImageX</b>	Cet outil graphique réalisé via AutoIT est une alternative intéressante pour ceux qui n'affectionne pas la ligne de commande. Dérivé du programme officiel « ImageX », il propose les mêmes capacités.

Résumé des principales actions réalisables sur les fichiers WIM

Actions / Verbe	Description
<b>Capture</b>	Copie la structure de dossier et de fichier indiquée et génère un nouveau fichier .WIM résultant. Note : Vous pouvez également recourir à l'outil « WDS Capture », présent par défaut sur un DVD original, mais celui-ci vous imposera que le système soit préalablement préparé via sysprep.
<b>Append</b>	Similaire à la capture, mais ajoute le résultat en tant que nouvelle image dans un fichier .WIM existant
<b>Delete</b>	Supprime une image dans un fichier .WIM existant
<b>Apply</b>	Permet d'extraire la structure d'une image donnée à partir d'un fichier .WIM existant vers une destination préalablement formatée.
<b>Mount</b>	Réalise le montage de l'image indiquée dans un dossier existant. Il est possible de stipuler que le montage est en lecture seule.
<b>Unmount</b>	Effectue le démontage d'une image actuellement montée sur un dossier. Il est possible de valider les éventuelles modifications via l'option « /commit » ou les annuler « /discard »
<b>Export</b>	Permet d'extraire une image présente dans un fichier .WIM afin de générer un nouveau fichier .WIM contenant cette image.
<b>Info</b>	Permet d'afficher les métadonnées XML d'un fichier .WIM existant (Taille, nombre d'images, description...)
<b>Dir</b>	Rarement utilisée, cette action consiste à énumérer le contenu d'une image sans procéder au montage. En raison de la quantité importante des contenus, il est souvent préférable d'utiliser des outils tels que 7-Zip.

*Schéma de synthèse des actions*





Pour manipuler le contenu d'un fichier .WIM, il est nécessaire de procéder à un « montage ».

```
DISM /Mount-Wim /WimFile:.\DVD\Sources\install.wim /index:1 /MountDir:.\MNT
```

Pour effectuer ce montage, il est nécessaire que le dossier de destination (.MNT) existe au préalable et il est préconisé qu'il soit vide, bien que cela ne soit pas imposé par l'outil.

Pour enregistrer des modifications apportées dans une image .WIM montée, il faut valider les changements lors du démontage (/commit).

```
DISM /Unmount-Wim /MountDir:.\MNT /commit
```

En cas de difficulté de montage des images, vous pouvez recourir aux actions suivantes

Actions / Verbe	Description
<b>Remount</b>	Récupère un répertoire de montage WIM orphelin
<b>Cleanup</b>	Nettoie les références et ressources associées aux montages endommagés

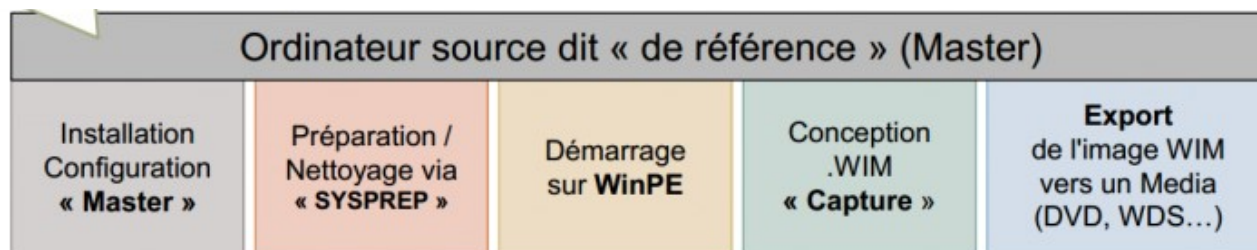
Pour terminer sur cette présentation des fichiers .WIM, j'ajouterais qu'il ne faut pas les confondre avec un système d'imagerie de disque par blocs (du genre .VHD, GHO...). Autrement dit, ils ne contiennent aucune notion de partition, ni de formatage, et il faut donc préparer le support de destination et ne pas oublier d'ajouter un mécanisme d'amorçage le cas échéant.

### 3. Les processus de fabrication et de déploiement

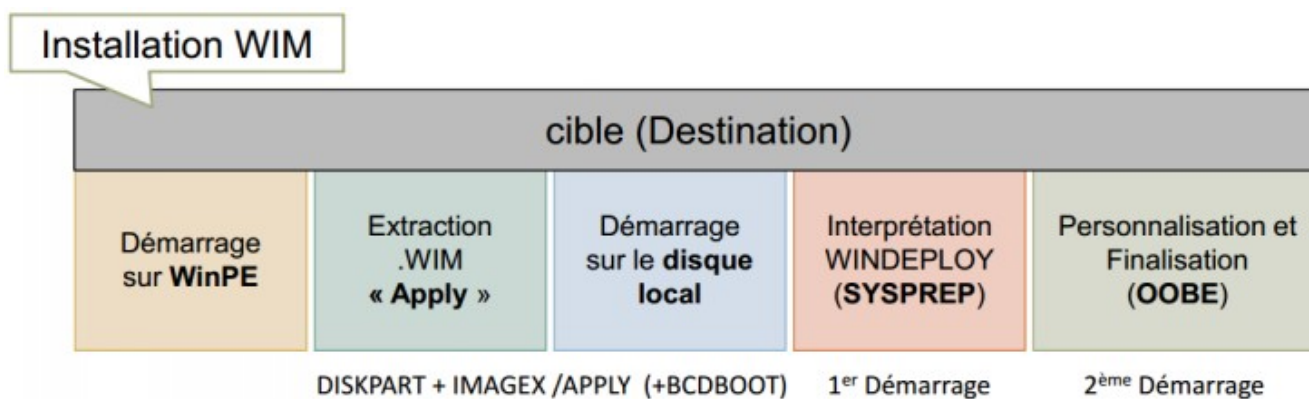
Schématiquement on pourrait résumer le processus de fabrication et de déploiement comme suit :

- Préparation de l'ordinateur de référence et génération de l'image WIM

Génération WIM



- Installation – Partitionnement des disques, configuration de l'amorçage et extraction (ou application) de l'image WIM



Je vous invite à continuer la lecture avec ce second article : [Débuter avec MDT 2013](#)