

Déploiement de postes de travail Windows.

Présentation LASER du 21/05/2024

Olivier FLOUCAT – AI CNRS – UMR 5506 LIRMM

- Environnement du LIRMM
- Windows
- Microsoft Deployment Toolkit (MDT)
- La solution mise en place au LIRMM pour déployer Windows
- Récupérer et installer les éléments de fabrication
- Préparation de l'image d'installation Windows
- Infrastructure
- WinPE – Préparation de WinPE
- WinPE – script startnet.cmd
- WinPE – personnalisation de Startnet.cmd
- install.cmd - Menu
- Install.cmd - Exécution de l'installation
- Unattend.xml
- Unattend.xml – Phase 1.windowsPE
- Unattend.xml – Phase 7.oobeSystem SetupComplete.cmd
- Unattend.xml – Phase 7.oobeSystem SynchronousCommands
- Localisation des scripts et paramètres
- Et ensuite...

- REMARQUES (suite à la présentation)
- Mon mail

environnement du LIRMM

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
Campus St Priest - 161 rue Ada, Montpellier

- 3 départements de recherche : Informatique, Robotique, Microélectronique
- Effectif de l'unité : 416
- Équipe INDEX : 6 agents dont 1 CDD pour le Système d'information et 1 Ingénieur dédié au support Web.
- 1 domaine Microsoft Active Directory (3 serveurs et 2 CD)
- Postes sous Windows : 250
- Environ 50 installations par an.

Windows

- Oct. 2022 : Sortie de Windows 10 22H2
- Oct. 2023 : Sortie de Windows 11 23H2
- La version finale de Windows 10 est la version 22H2, qui prendra fin à la maintenance le 14 octobre 2025.

Microsoft Deployment Toolkit (MDT)

citations Microsoft

- **"MDT ne prend pas en charge** Windows 10 appareils ARM64, **Windows 11** et systèmes d'exploitation Windows Server 2022."
- **"MDT n'est pas pris en charge avec Windows 11.** Tous les problèmes connus répertoriés pour Windows 11 ou ADK pour Windows 11 sont fournis à titre d'information uniquement et n'impliquent pas de prise en charge."
- **"Mises à jour de configuration prises en charge (dernière build : 8456 du 9/30/2020)**
 - Windows ADK pour Windows 10, version 1809 (**octobre 2018 update**)
 - Windows 10, version 1809
 - Configuration Manager, version 1810"

La solution mise en place au LIRMM pour le déploiement de Windows.

- Construction de la solution entre février et avril 2024
- Solution présentée : basée principalement sur des documentations Microsoft datés de septembre et juin 2023.

Récupérer et installer les éléments de fabrication.

Télécharger les sources de même version : (rien de nouveau...)

- Le Kit de déploiement et d'évaluation Windows (ADK)
- Le module complémentaire Windows PE pour ADK (WinPE)
- L'image iso de Windows (*ne garder que l'image de Windows Pro*).

Préparation de l'image d'installation Windows

On ne garde que l'image de Windows Pro.

1. Extraire le contenu de l'iso et placer son contenu sur partage réseau.
2. Install.esd : extraction de l'image correspondant à la version Windows Pro (*utiliser l'outil DISM de ADK*). Cela allégera l'installation.

DISM : Deployment Image Servicing and Management

Exemple d'une des commandes à exécuter :

```
dism /export-image /SourceImageFile:W:\w11\sources\install.esd /SourceIndex:1  
/DestinationImageFile:W:\w11\sources\install.wim /Compress:max  
/CheckIntegrity
```

3. Remplacement de install.esd par install.wim

infrastructure

Déploiement par le réseau (là aussi rien ne change...).

Brève description :

1. Le client_(UEFI, secure boot) démarre en boot PXE.
2. Il obtient son IP(DHCP) et le chemin d'accès au fichier de démarrage réseau du Service de Déploiement Windows (WDS).
3. WDS lui propose de charger notre image personnalisée WinPE.
4. Une fois chargé en mémoire, WinPE permet l'installation de Windows, dont le contenu de l'image iso se trouve sur un partage réseau.

WinPE - Préparation de WinPE

Le Kit Windows (ADK) fourni :

- l'outil DISM pour modifier l'image boot.wim.
(DISM : Deployment Image Servicing and Management)
- les capacités de boot à ajouter à l'image :
 - [bootmgr.efi](#) (*BIOS Hérité*)
 - [bootmgfw.efi](#) (*BIOS UEFI*)
- les composants **indispensables pour Windows 11**, à ajouter dans l'ordre à l'image :
 1. [WinPE-WMI.cab](#)
 2. [WinPE-SecureStartup.cab](#)

WinPE – script startnet.cmd

- **Permet d'ajouter des scripts de ligne de commande personnalisés dans Windows PE.**
- Localisation :
`%SYSTEMROOT%\System32\startnet.cmd`
- Démarre Wpeinit.exe
 - gère les éléments Plug-and-Play
 - traite les paramètres Unattend.xml (*si présent à la racine de WinPE*)
 - charge les ressources réseau.

WinPE - Personnalisation de Startnet.cmd

Le choix est fait de garder le minimum de code dans startnet.cmd et d'externaliser le reste sur le partage réseau (install.cmd, nom du script arbitraire).

- Monte le partage réseau (*Une identification sera demandée*).

```
net use N: \\mon-serveur.domaine\partage$
```

- Exécute le script distant « install.cmd » qui affiche un menu interactif et exécute le reste du code.

```
N:\dossier\install.cmd
```

A ce stade, on peut mettre à disposition WinPE dans WDS.

install.cmd - Menu

```
Administrateur: X:\windows\system32\cmd.exe - N:\AnswerFiles\install.cmd
==== INSTALLATION version 29/03/2024:01 ====
-----
Configuration :
(N) hostname: TEST01
(P) ajout pilotes = NON
(R) enregistrement dans le DOMAINE = OUI
    REMARQUE: si hors domaine, machine non chiffree.
.
Installation :
(1) 10V22H2 / (2) 11V23H2
.
(T) Instal. TEST / (0) Sortir du script
(H) Afficher Aide / (D) Lister les Disques
-----
:
-
Microsoft DiskPart version 10.0.25398.1
Copyright (C) Microsoft Corporation.
Sur l'ordinateur : MININT-TJGIQK5

N° disque  Statut          Taille  Libre  Dyn  GPT
-----
Disque 0   En ligne             80 G octets  80 G octets
(Votre choix) :N
(choisir le nom de la machine):TOT001_
```

Choix de l'installation.

Zone d'information et de saisie.

Configuration

Enregistre certains paramètres choisis dans l'image à installer :

- Le nom de la machine,
- La déclaration dans le domaine : *Oui ou Non*,
- Le nom du domaine (*non modifiable par le menu*)

Installation

Exécution de l'installation du Windows choisi.

- 10 version 22H2
- 11 version 23H2

Option : Ajout de pilotes (*pas encore testé...*)

Install.cmd - Exécution de l'installation

Exemple :

« N: » correspond au montage réseau

```
set setup=N:\install\11V23H2\setup.exe
```

```
set unattend=N:\answerfiles\unattend-11V23H2.xml
```

```
%setup% /unattend:%unattend%
```

Unattend.xml

Seulement 2 phases de configuration sur les 7 sont utilisées :

- Phase 1 windowsPE
- Phase 7 oobeSystem

Windows System Image Manager (Assistant Gestion d'installation)

- Outil du Kit de déploiement et d'évaluation Windows (ADK)
- Aide à fabriquer le fichier de réponses unattend.xml
- Utilise l'image install.wim dont on va générer un catalogue de références (*fichier.clg*).

Unattend.xml – Phase 1.windowsPE

- RunSynchronousCommand

Exécute une commande et attend qu'elle soit fini avant de passer à la suivante.

```
cmd.exe /c `` instruction à exécuter ``
```

Préparation des volumes avant installation ([diskpart](#)).

REMARQUES :

Avec MDT, la phase 3.specialize était utilisée.

Autre méthode pour pouvoir choisir le disque d'installation ? ...

Unattend.xml – Phase 7.oobeSystem SetupComplete.cmd

- Après la phase oobe, exécution possible d'un script SetupComplete.cmd
- Un script cmd peut exécuter un script powershell (PS1).
- Dans cette phase d'installation les scripts PS1 sont exécutés avec élévation de privilèges.
- Si on a besoin de redémarrer, impossible de faire un AutoLogOn et reprendre le même script. L'installation passera à la ligne suivante SynchronousCommands suivant son numéro d'ordre.
- Après le nombre max atteint d'AutoLogOn, au prochain redémarrage on verra l'invite de session.

Unattend.xml – Phase 7.oobeSystem SynchronousCommands

FirstLogonCommands - SynchronousCommands :

1. SetupComplete.cmd

- Suppression du chiffrement
- Enregistrement de la licence OEM (script PS1)
- Changer le nom de la machine (script PS1)
 - Paramètre d'entrée : name.txt
 - Seulement pour Windows 10 : RESTART / AutoLogON

2. DomainAdd.cmd (script PS1)

- Paramètre d'entrée : domainname.txt ; domain.txt (Oui/Non)
- RESTART / AutoLogON

3. BitLockerEnableAndBackup.cmd (script PS1)

4. Seulement pour Windows 10 : VerifUpdateAndInstall.cmd (script PS1)

Localisation des scripts et paramètres enregistrés

Dans le dossier contenant l'image, sur le partage réseau.

Il faut ajouter au dossier « sources » de l'image ces dossiers :

`OEM\$$\setup\scripts`

Une fois l'OS installé, cela correspondra à :

`%windir%\setup\scripts\ (c:\windows\setup\scripts\)`

On y ajoute les scripts et paramètres de configuration qu'on aura besoin quand le système s'installera.

Et ensuite...

Limites / Améliorations...

- Avec cette solution il faut que j'attende que winPE ait fini et redémarre la première machine en cours d'installation, avant de valider par le menu la configuration de la deuxième machine... Soit un intervalle de moins de 10mn.
- Pour une installation groupée de plusieurs machines, il est envisageable de définir une liste de (clé, valeur) soit (MAC@, nom de machine). Cela peut permettre à un script PS1 de sélectionner le nom correspondant à la machine en cours d'installation et de ne plus avoir à attendre les 10mn entre chaque installation...
- Installation de l'OS limité au disque « 0 » (diskpart). Autre solution ?...

REMARQUES (suite à la présentation)

- **Pour que cela fonctionne** il faut compléter unattend.xml avec d'autres paramètres non abordés, mais qui seront facile à trouver. j'ai choisi de me focaliser sur des points de configuration précis qui me permettent de me défaire de MDT.
- Enregistrement dans le domaine : j'ai décidé de ne pas utiliser unattend.xml car cela oblige à y inscrire un compte ayant les droits que je trouve trop critique (même si le psw dans ce fichier peut être chiffré). Donc je passe par un script PS1 qui demande de s'identifier. Total : 2 identifications demandés, 1 pour que winPE accède au partage réseau et 1 pour déclarer la machine dans le domaine.
- **Durée d'installation pour Win11 23H2 et Win10 22H2 en moins de 20mn avant la première connexion AutoLogON.** Pour Win10 il faudra quand-même lancer les mises à jours pour que tous les périphériques soient enfin reconnus. Pour Win11 il s'en occupe tout seul... **Au final l'installation + mises à jours : Win11 -30mn et Win10 -50mn.**
- Je n'ai pas eu besoin de télécharger et installer de pilotes additionnels et je n'ai pas eu à utiliser les logiciels DELL et HP pour la détection et l'installation de pilotes. Ceci dit pour le moment je n'ai testé que des portables DELL et HP du marché (Latitude 5490, Precision 7740 et 3530, EliteBook840, ...) et pas de station de travail avec carte additionnelles...

Mon mail

Merci d'avance pour vos remarques.

Je reste à votre disposition pour répondre à vos questions et partager mes scripts et configurations.

Cordialement,

olivier.floucat@lirmm.fr