Renouvellement par masterisation des postes clients d'une PME

Introduction

Ce projet a été réalisé dans le cadre de mon BTS SIO (option SISR), il a pour objectif de répondre à un besoin concret de déploiement massif de postes de travail dans une entreprise fictive nommée EXPERTY. Cette entreprise souhaite renouveler son parc informatique, composé de 80 postes, en déployant Windows 11 avec un ensemble d'applications et de configurations spécifiques.

L'objectif principal est d'automatiser au maximum le processus de déploiement afin de gagner du temps, garantir l'uniformité des installations et assurer un haut niveau de sécurité. Pour cela, plusieurs outils seront testés et mis en œuvre : **NTLite** pour la création d'une image personnalisée, **FOG** pour le déploiement réseau en environnement Linux, et **WDS** dans un environnement Windows.

Ce rapport présente la démarche adoptée, les outils utilisés, les procédures détaillées pour chaque solution ainsi que les bonnes pratiques de sécurité appliquées, en se basant notamment sur les recommandations de l'ANSSI et de Microsoft.

SOMMAIRE

Cahier des charges

Le projet consiste à concevoir une procédure complète permettant de déployer 80 postes clients Windows 11 dans l'entreprise EXPERTY. Ce déploiement devra inclure :

- La création d'une image Windows 11 personnalisée avec **NTLite**
- Le test d'un déploiement par **clé USB**
- Le test d'un déploiement par le réseau à l'aide de **FOG**
- Le test d'un déploiement réseau avec **WDS**
- L'intégration des logiciels suivants dans l'image :
  - OpenOffice
  - Adobe Reader
  - 7zip
  - Google Chrome (version entreprise)
- La configuration automatique de l'ouverture de **Google Chrome** sur l'URL "www.intranet.local"
- La mise en œuvre des **bonnes pratiques de sécurité** recommandées par l'**ANSSI** et **Microsoft**
- La rédaction d'un **rapport détaillé**, comprenant toutes les procédures avec captures d'écran

Le tout devra être testé dans une **maquette virtuelle**, afin de valider le bon fonctionnement des différentes méthodes de déploiement.

Liste des Ressources pour ce Projet

Lien de téléchargement :

- NLite
- Rufus
- FOG
- Windows 11 iso
- Windows Server 2022 iso
- Debian 12 iso

- Chrome Entreprise
- Adobe Reader
- OpenOffice
- 7zip

- Microsoft Deployment Toolkit (MDT)
- Windows ADK (DL direct)
- Windows PE (DL direct)

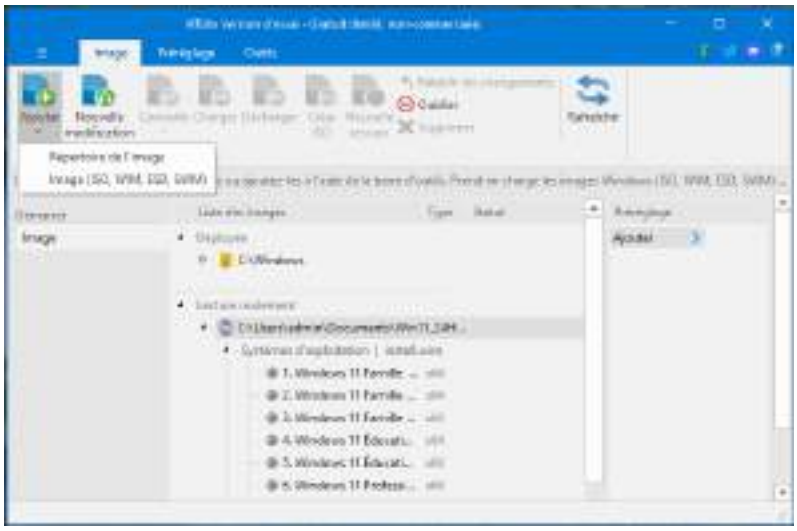
Bypass Connexion Windows 11 :
Il faut désactiver la connexion internet en amont.
Sur l'écran connexion à un réseau :

Shift + F10
CMD : *OOBE\BYPASSNRO*

Création Image personnalisé avec NLite

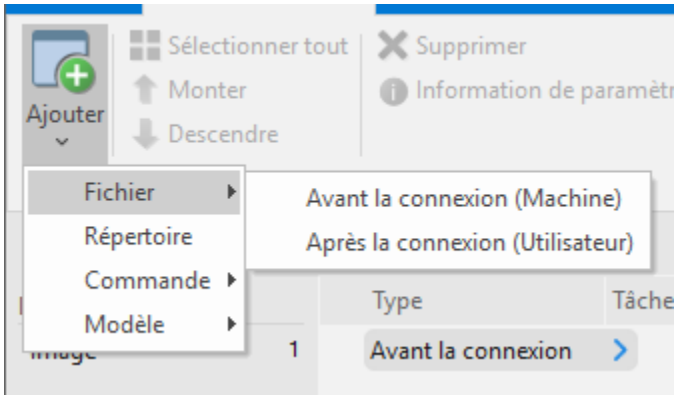
En amont, télécharger les logiciels en .exe souhaités.
/!\ Prendre les versions entreprises pour l'installation offline

Ajouter > **Image** > **Selection Windows 11 Pro** dans la liste puis **Charger**

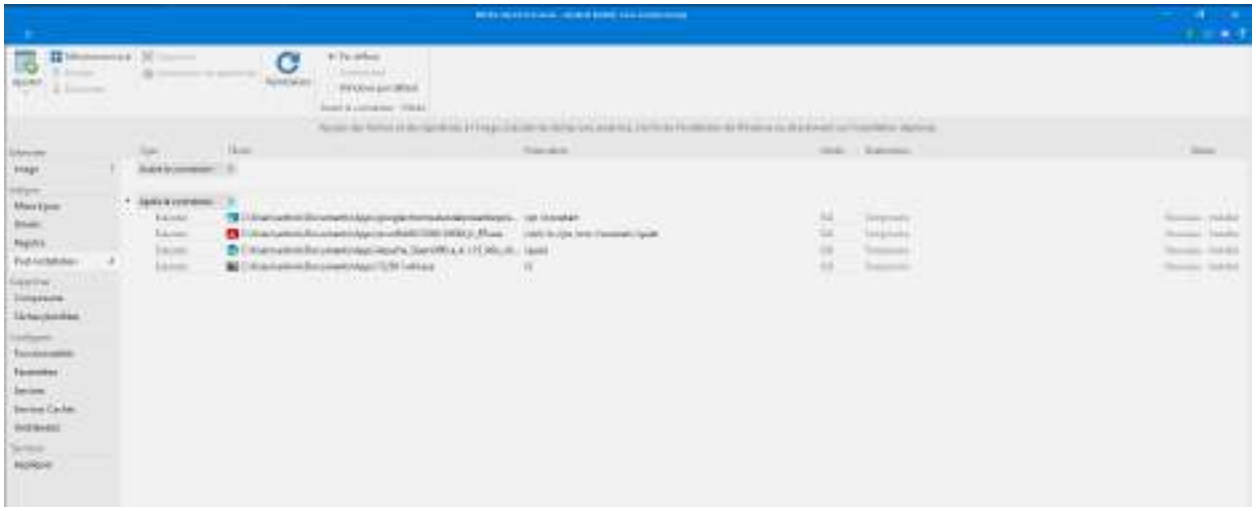


1. Pour ajouter des Logiciels

Post-Installation > **Ajouter** > **Fichier** > **Après la connexion** (car besoin environnement Windows) puis sélectionner les .exe et .msi nécessaires



/! Les paramètres (commandes silencieuses) servent à automatiser l'installation, ils sont **essentiels** pour éviter les interventions utilisateur ou redémarrage.

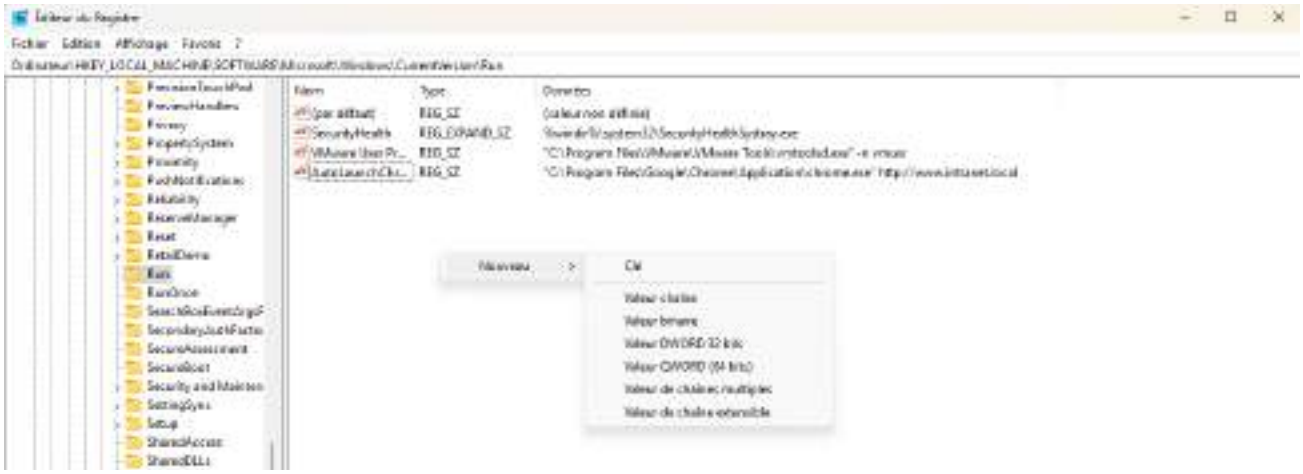


Chrome Entreprise ➔ /qn /norestart
Adobe Reader ➔ /sAll /rs /rps /msi /norestart /quiet
OpenOffice ➔ /quiet ou /S (selon la release)
7zip ➔ /S

2. Pour le lancement automatique d'une page internet :

NLite en version limitée : onglet **Registre**
Clique droit sur **Machine - SOFTWARE** puis **Modifier**

Naviguer vers :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Pour ajouter la valeur dans Run :
Clic droit > **Nouveau** > **Valeur chaîne** (REG_SZ)
Nom : AutoLaunchChrome
Données : *"C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.intranet.local*



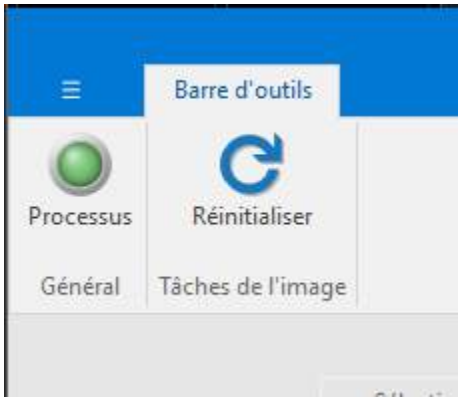
Si ne fonctionne pas car version gratuite ou autre :
Créer un fichier .reg avec les paramètres souhaités

Puis dans NLite, **Ajouter** > **Fichier** / **Commande** > **Après la connexion**
Pour la commande : *regedit.exe /s launch_chrome.reg* (pour exécuter le programme)

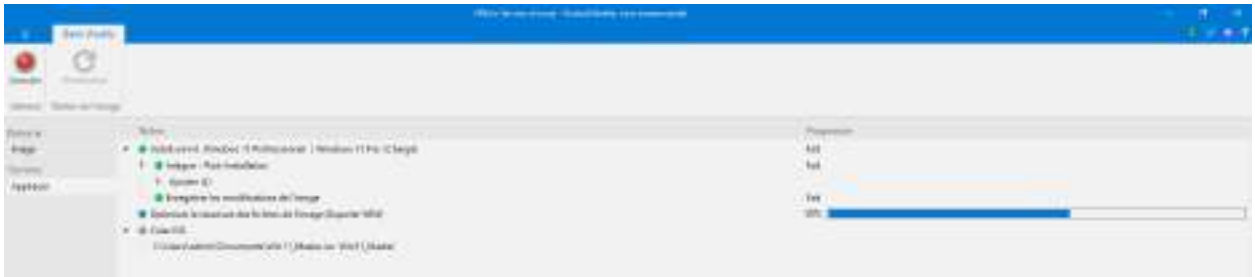
3. Pour créer L'ISO :

Sur le menu de gauche > **Appliquer** > **Créer ISO**

Donner un nom puis cliquer sur le bouton vert **Processus**

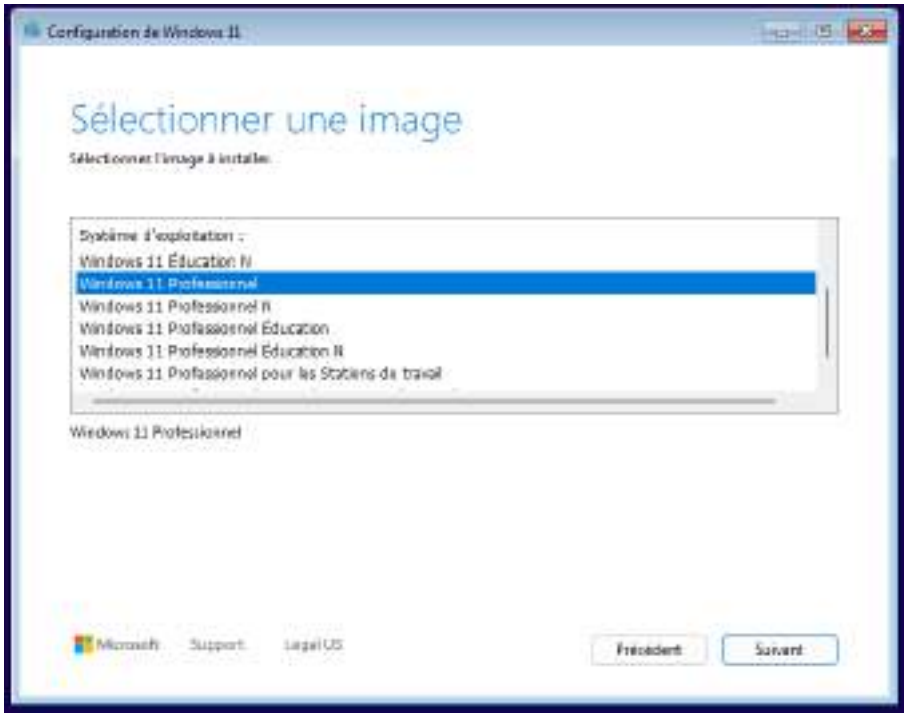


L'ISO se crée au fur et à mesure et se retrouve dans le dossier de destination choisi.

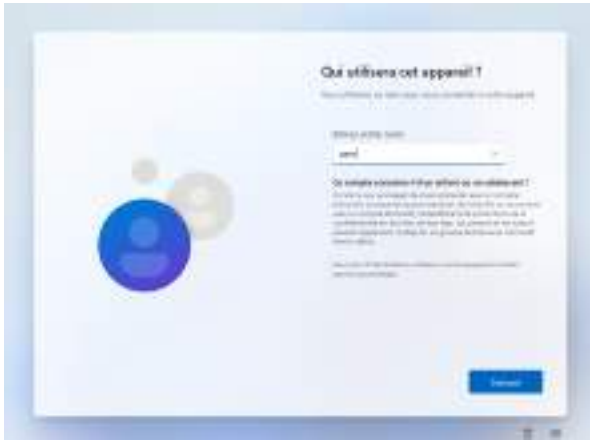


Test Image NLite

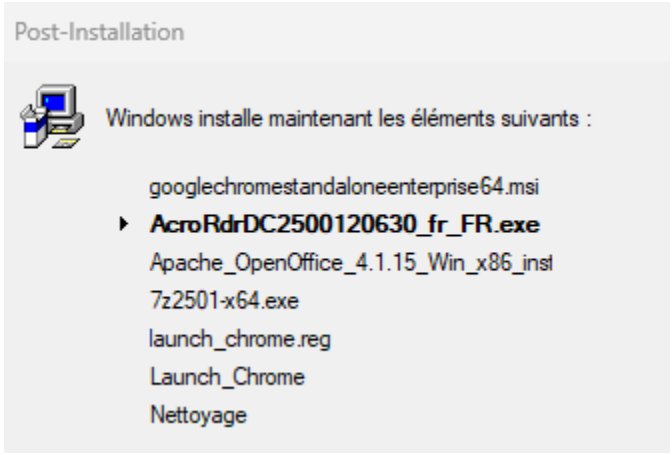
Lorsque je teste mon ISO je fais bien attention à choisir l'image précédemment modifiée, ici Windows 11 Professionnel.



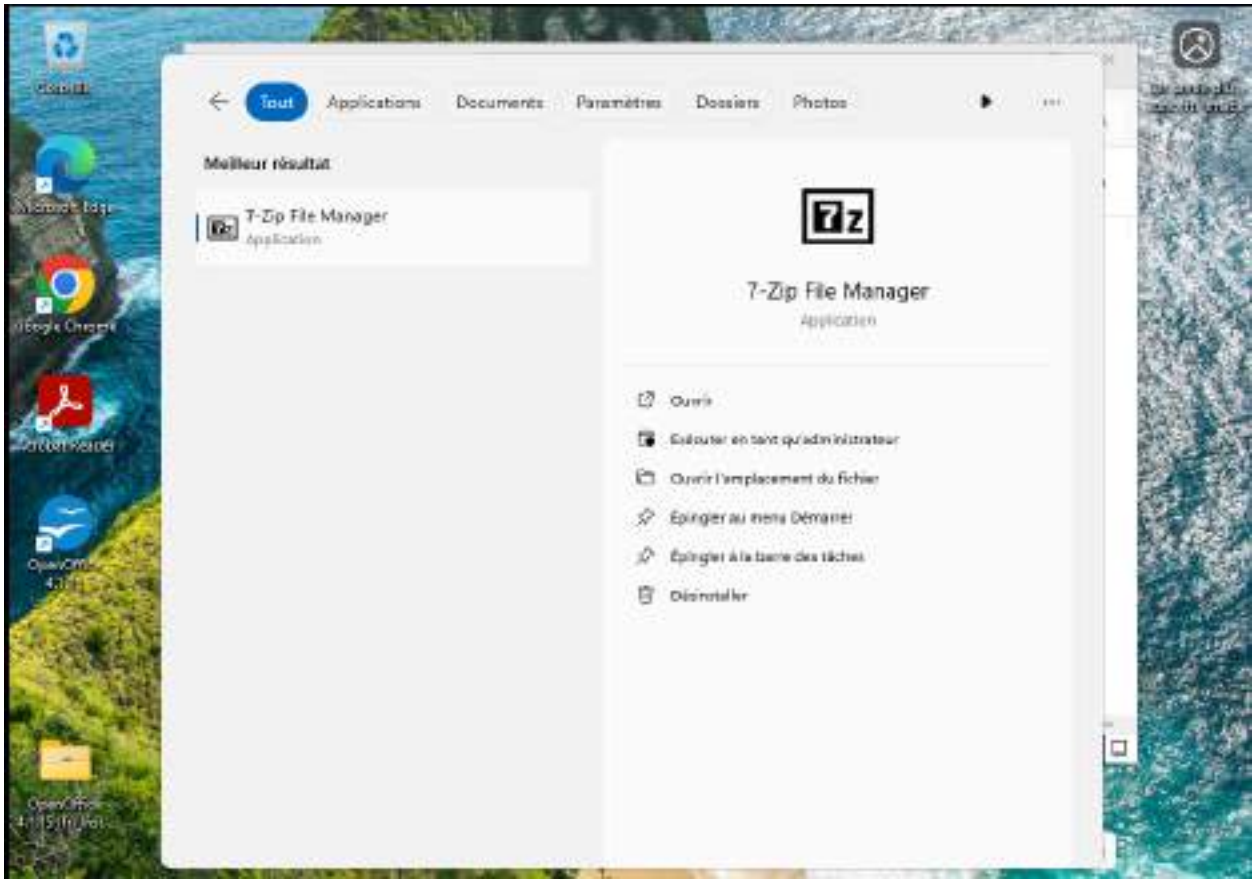
Je crée ensuite mon compte utilisateur



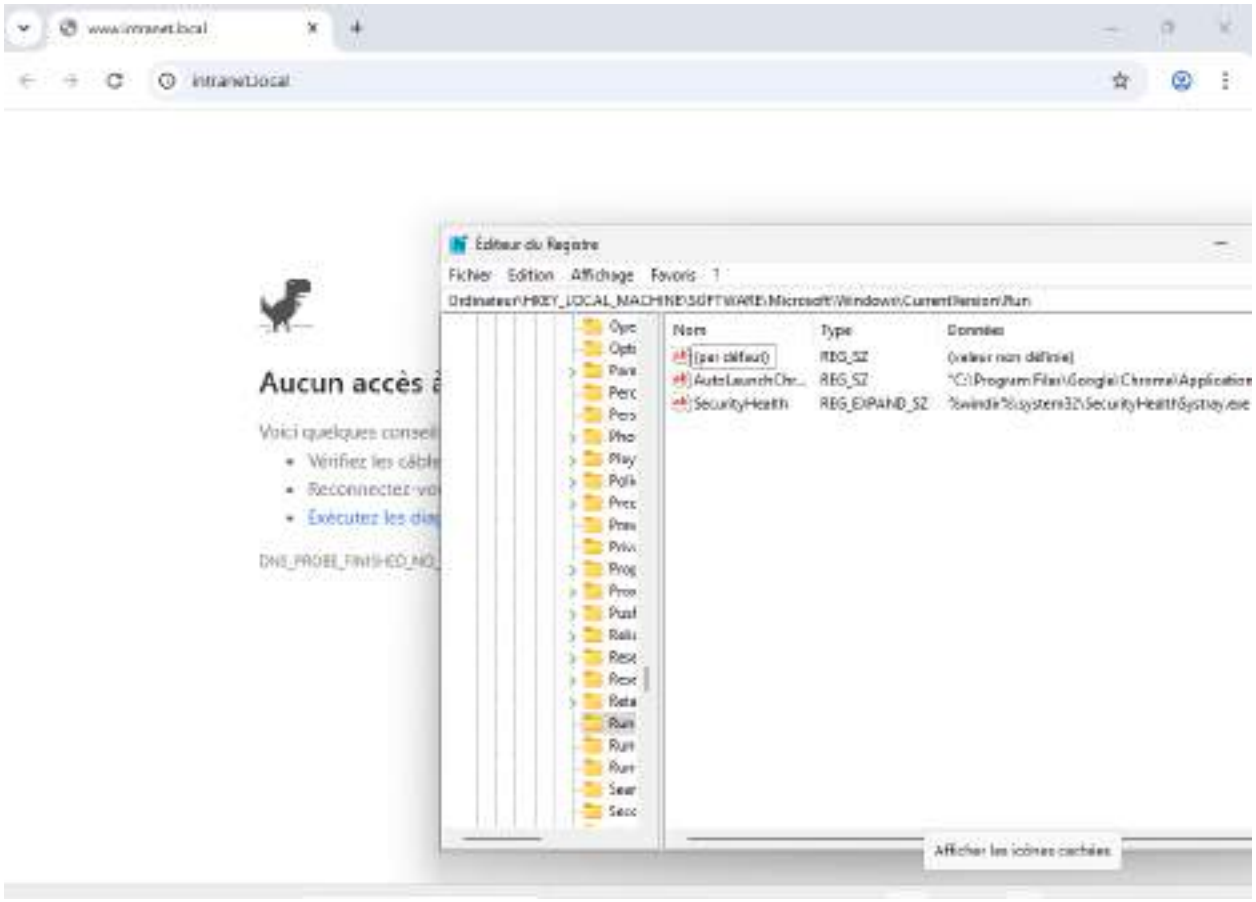
Ensuite on peut voir que Windows installe bien les applications demandées :



On peut ensuite voir que toutes les logiciels sont bien installés :



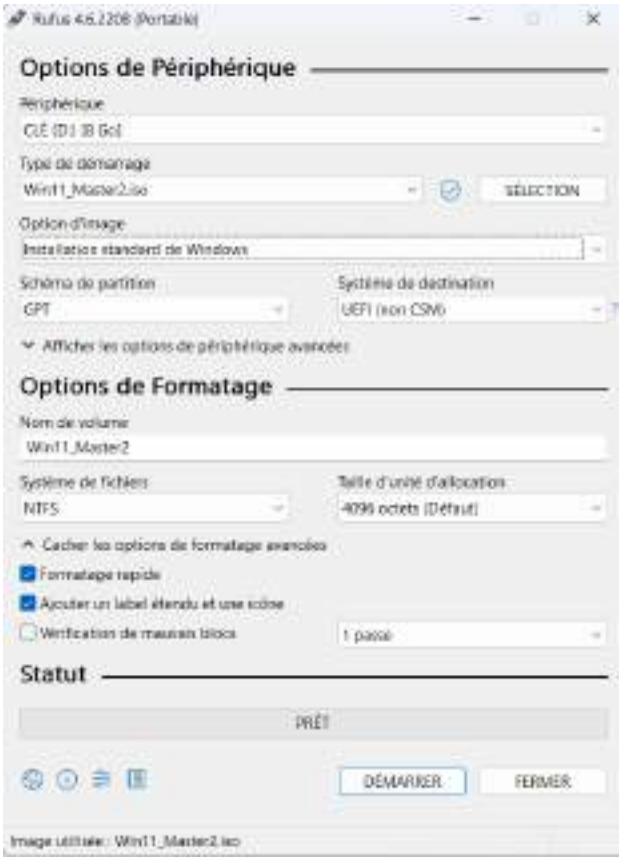
Également quand on relance la machine, chrome démarre automatiquement sur la page intranet.local



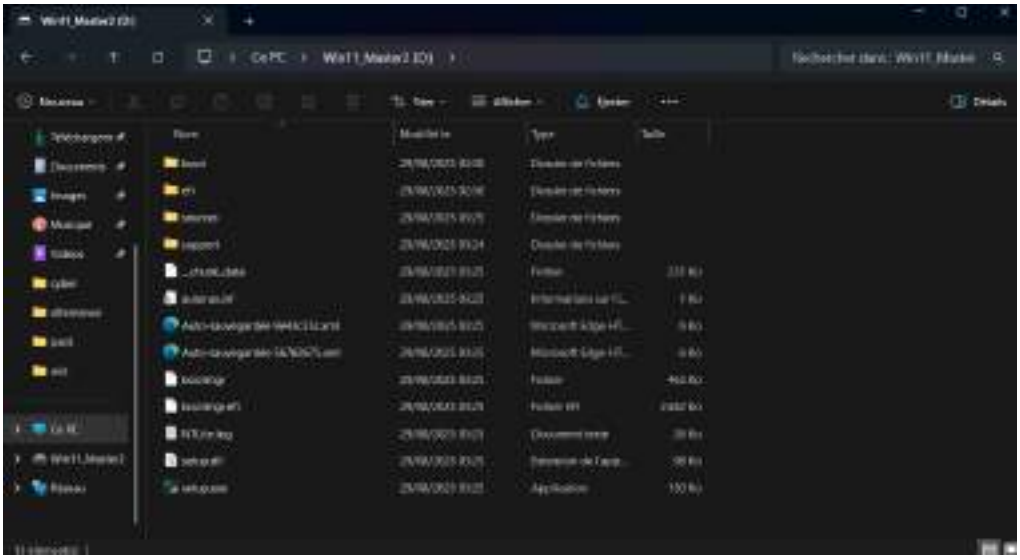
Avec une clé USB

On utilise le logiciel **Rufus** :

Périphérique : Clé USB
Type de démarrage : Sélectionner l'ISO
Schéma de partition : GPT (plus récent)



Une fois le chargement fini la clé est prête à être utilisé :



Installation du serveur FOG

Sur la VM Debian :

- Carte réseau : NAT (accès internet) + Host-only (réseau interne FOG (PXE + DHCP)
- IP fixe : Ici 192.168.158.1 pour rediriger correctement les clients PXE

Configuration de l'IP fixe :

- Repérer la carte réseau host-only avec *ip a*

```
root@fog-server:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0d:9b:06 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.158.130/24 brd 192.168.158.255 scope global dynamic ens33
       valid_lft 1529sec preferred_lft 1529sec
    inet6 fe80::20c:29ff:fe0d:9b06/64 scope link
       valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:0d:9b:10 brd ff:ff:ff:ff:ff:ff
    altname enp2s4
root@fog-server:~#
```

Ici ens33 car config VMware 192.168.158.0

- Modifier le fichier config des interfaces avec *vim /etc/network/interfaces*

```
#Interface Host-only
auto ens36
iface ens36 inet static
        address 192.168.158.1
        netmask 255.255.255.0
~
```

Téléchargement de FOG :

On met d'abord à jour les paquets : *apt update && apt upgrade -y*
On installe git pour récupérer les paquets nécessaires : *apt install -y git*
On récupère les paquets FOG : *git clone https://github.com/FOGProject/fogproject.git*
On lance l'installateur FOG : *cd fogproject/bin* puis *./installfog.sh*

Les choix pendant l'installation :

On choisit le bon système ici 2

```
What version of Linux would you like to run the installation for?

        1) Redhat Based Linux (Redhat, Alma, Rocky, CentOS, Mageia)
        2) Debian Based Linux (Debian, Ubuntu, Kubuntu, Edubuntu)
        3) Arch Linux

Choice: [2]
```

On choisit une installation normale

```
What type of installation would you like to do? [N/s (Normal/Storage)] N
```

On sélectionne la bonne carte réseau

```
We found the following interfaces on your system:
    * ens36 - 192.168.108.139/24
    * ens33 - 192.168.56.1/24

Would you like to change the default network interface from ens36?
If you are not sure, select No. [y/N] y
What network interface would you like to use? ens33
```

On n'a pas de routeur dans notre cas et on renseigne le DNS de Google par défaut

```
Would you like to setup a router address for the DHCP server? [Y/n] n

Would you like DHCP to handle DNS? [Y/n] y
What DNS address should DHCP allow? [192.168.108.2] 8.8.8.8
```

On indique bien que notre serveur FOG sert de DHCP et nous n'avons pas besoin d'activer HTTPS sur notre réseau privé.

```
Would you like to use the FOG server for DHCP service? [y/N] y

This version of FOG has internationalization support, would
you like to install the additional language packs? [y/N] N

Using encrypted connections is state of the art on the web and we
encourage you to enable this for your FOG server. But using HTTPS
has some implications within FOG, PXE and fog-client and you want
to read https://wiki.fogproject.org/HTTPS before you decide!
Would you like to enable secure HTTPS on your FOG server? [y/N] n_
```

On a ensuite le récap de nos paramètres avant finalisation :

```
* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Debian GNU/Linux
* Interface: ens33
* Server IP Address: 192.168.56.1
* Server Subnet Mask: 255.255.255.0
* Hostname: fog-server
* Installation Type: Normal Server
* Internationalization: No
* Image Storage Location: /images
* Using FOG DHCP: Yes
* DHCP router Address:
* Send OS Name, OS Version, and FOG Version: No
```

On finalise l'installation en accédant à l'interface web de FOG depuis une autre VM ayant une carte réseau Host-only dans le même réseau

```
* You still need to install/update your database schema.
* This can be done by opening a web browser and going to:

  http://192.168.56.1/fog/management

* Press [Enter] key when database is updated/installed.
```

On utilise l'URL affichée par FOG et on clique sur "Install/Update Now"

On peut ensuite se connecter avec les identifiants par défaut :

Login : fog
Password : password

On revient sur la Debian et on peut faire entrée pour enregistrer les paramètres

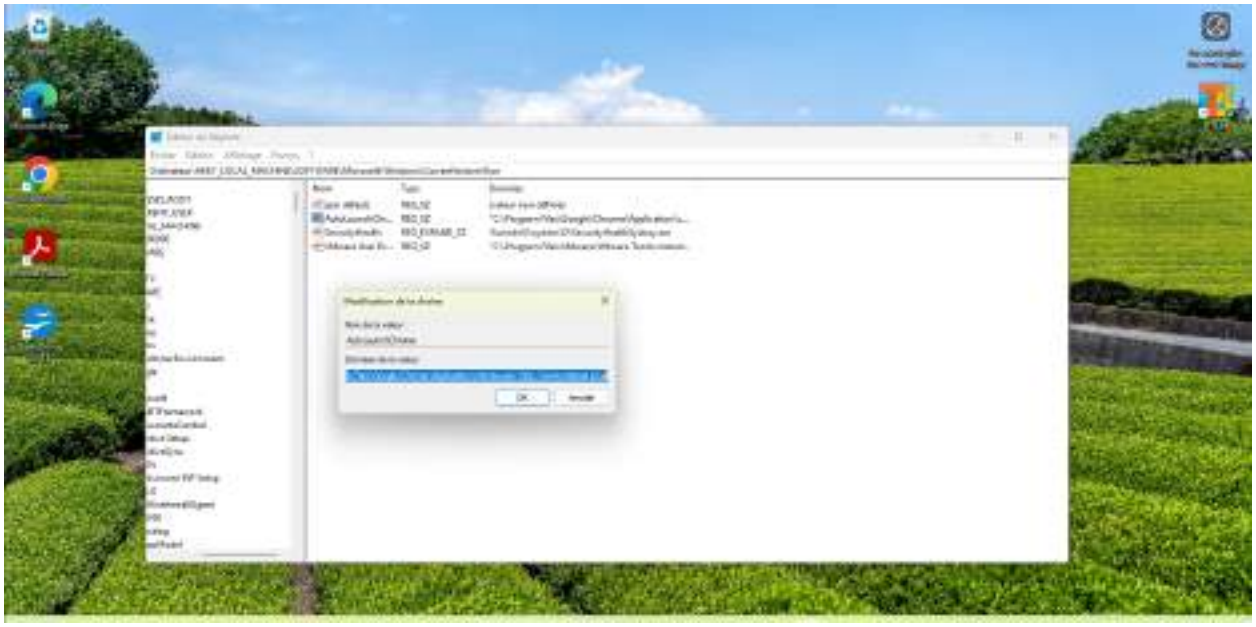
```
 * Setup complete

   You can now login to the FOG Management Portal using
   the information listed below.  The login information
   is only if this is the first install.

   This can be done by opening a web browser and going to:

   http://192.168.56.1/fog/management

   Default User Information
   Username: fog
   Password: password

 * Changed configurations:

   The FOG installer changed configuration files and created the
   following backup files from your original files:
   * /etc/dhcp/dhcpd.conf <=> /etc/dhcp/dhcpd.conf.1756656445
   * /etc/vsftpd.conf <=> /etc/vsftpd.conf.1756656445
   * /etc/exports <=> /etc/exports.1756656445

root@fog-server:~/fogproject/bin# _
```

Capture d’une Image avec FOG

1. Préparation de l’image

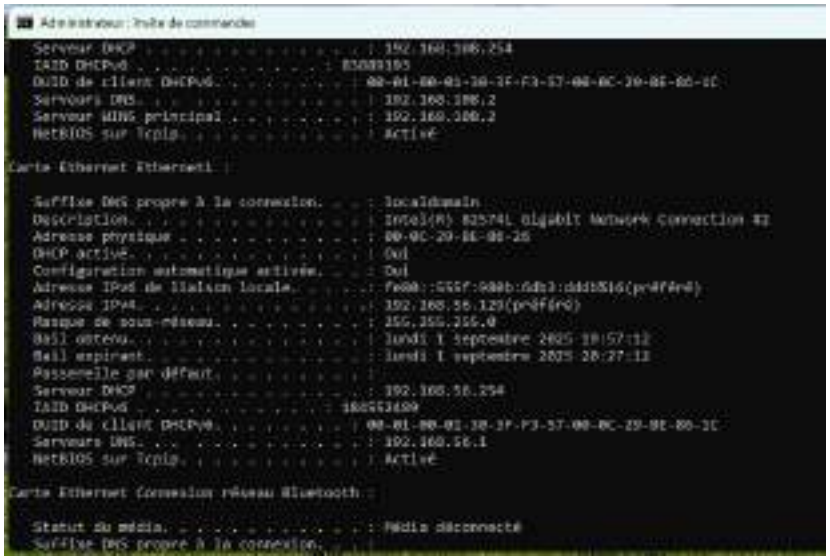
On prépare notre VM Win11-Base pour la capture :

- On installe OpenOffice - Adobe Reader - 7zip - Chrome Entreprise
- On configure le lancement auto de Chrome sur http://www.intranet.local
- On nettoie la machine avec cleanmgr



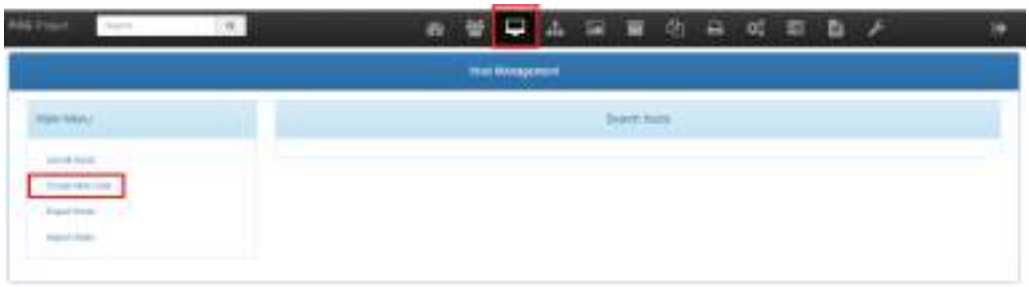
Pour le lancement de Chrome :
Win + R > **regedit**
Naviguer vers :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Pour ajouter la valeur dans Run :
Clic droit > **Nouveau** > **Valeur chaîne** (REG_SZ)
Nom : AutoLaunchChrome
Données : *"C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.intranet.local*

Ensuite, on prépare le Host dans l’interface FOG
Il nous faut d’abord l’adresse MAC de la machine donc depuis le cmd on tape la commande *ipconfig /all*
On repère ensuite la carte réseau Host-Only et on récupère l’adresse physique (ici **00-0C-29-BE-86-26**)



Après, on se rend sur l'interface FOG pour créer le Host.

"Host" > "Create New Host"

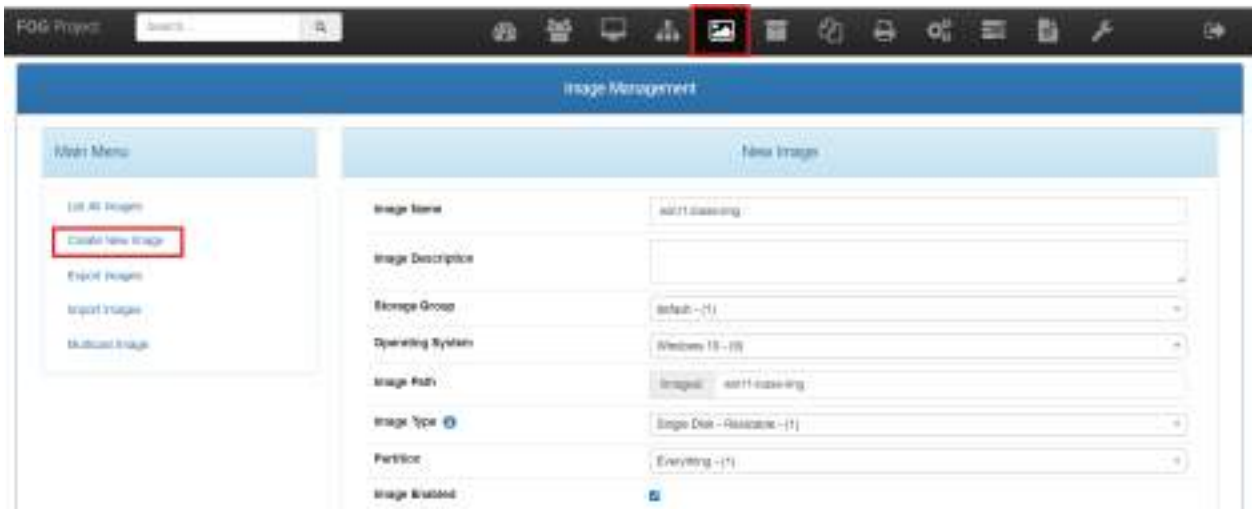


On remplit ensuite les deux premiers champs obligatoires et on peut sauvegarder.

On peut ensuite vérifier dans List All Hosts

Il faut aussi créer la **tâche de capture** :

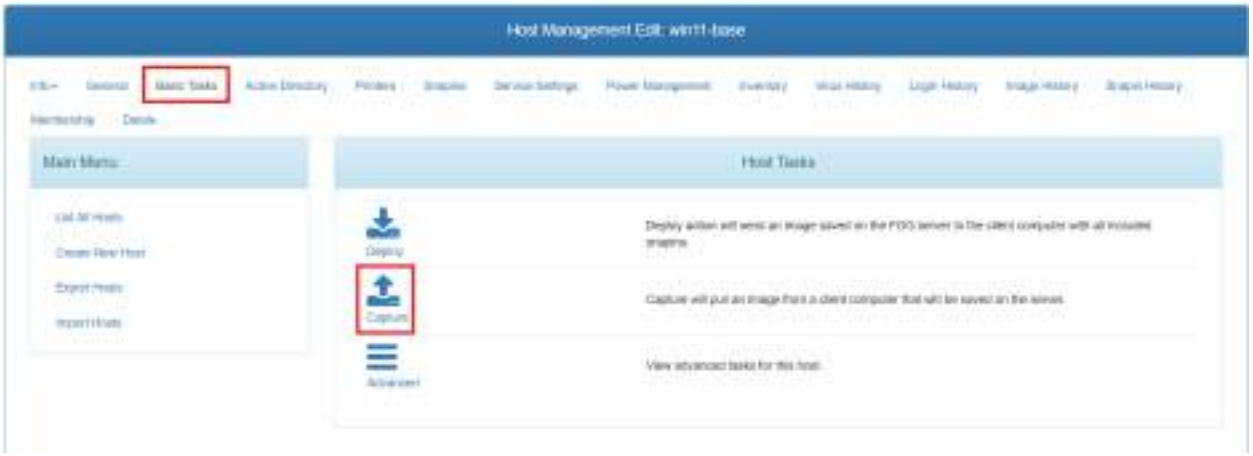
On doit créer une image pour l'ajouter à notre Host.
On donne un nom et on laisse les paramètres par défaut, on fait ensuite add



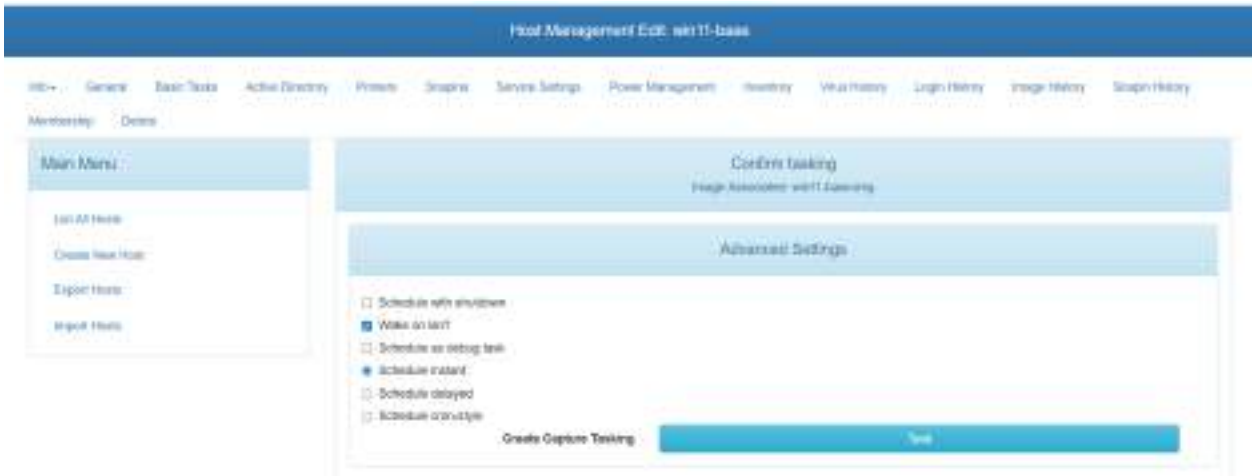
On retourne sur notre **Host** créé

On associe l'image créée

On se rend dans le menu **Basic Tasks** puis dans **Capture**

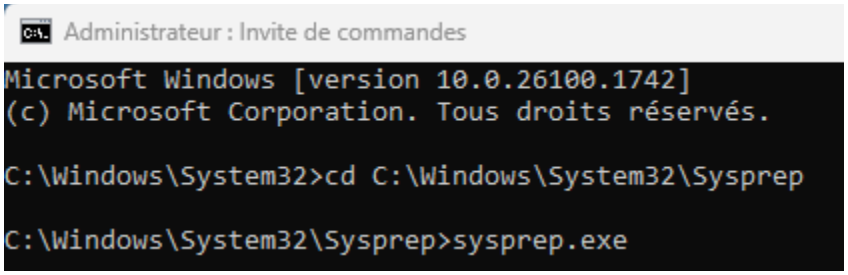


On clique simplement sur le bouton **Task** et FOG mettra la tâche en attente.

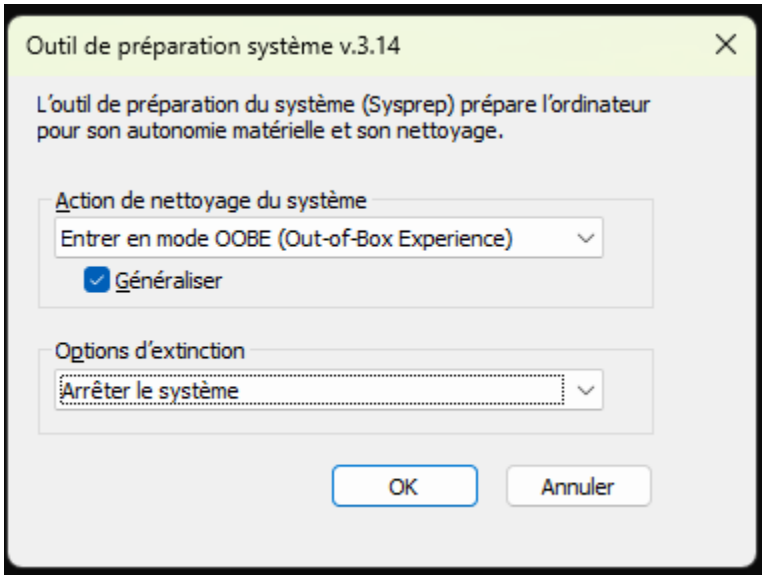


2. Capture avec Sysprep

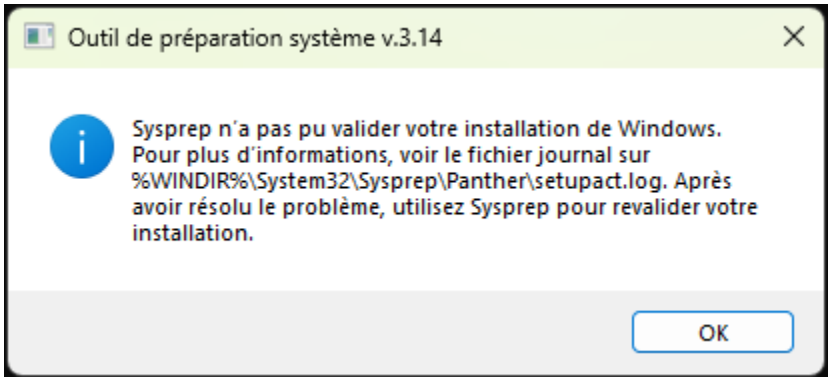
On ouvre un cmd en admin pour lancer Sysprep
cd C:\Windows\System32\Sysprep
sysprep.exe



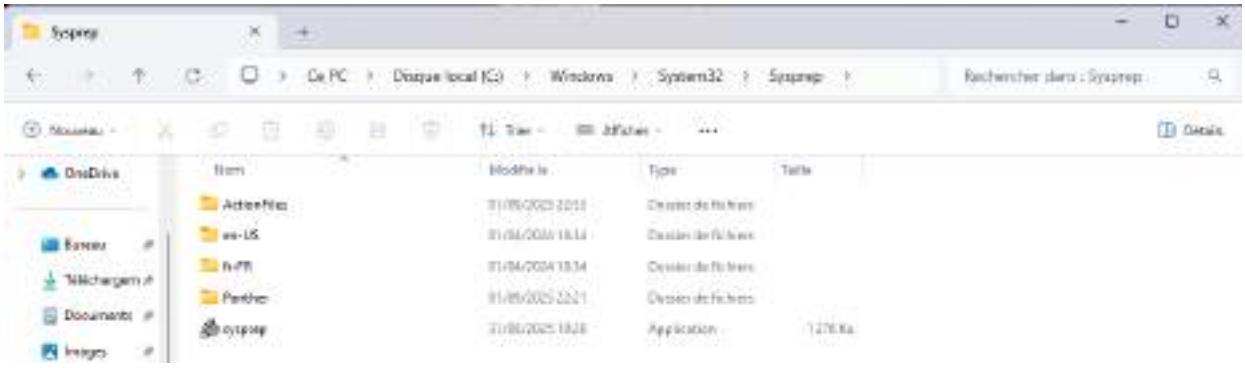
Options à choisir :
Action de nettoyage du système : *Entrer en mode OOBE*
Généraliser : *Coché* (Utile pour faire une image neutre sans nom, cache réseau, etc)
Option d'extinction : *Arrêter le système*



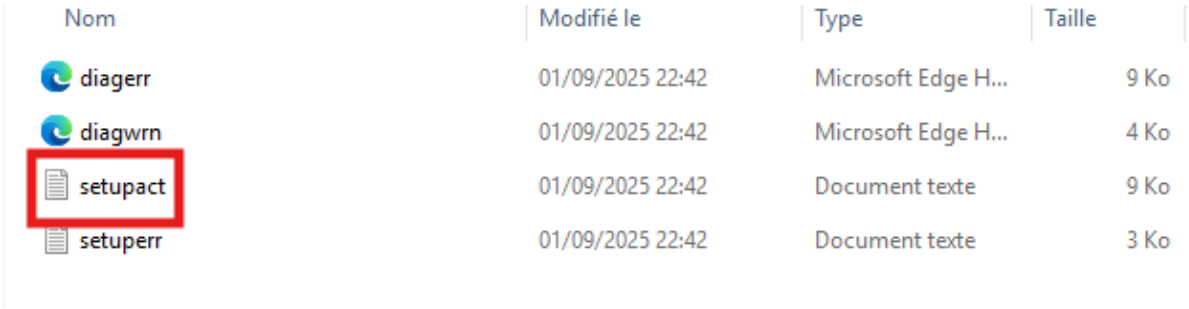
Si cette erreur apparaît



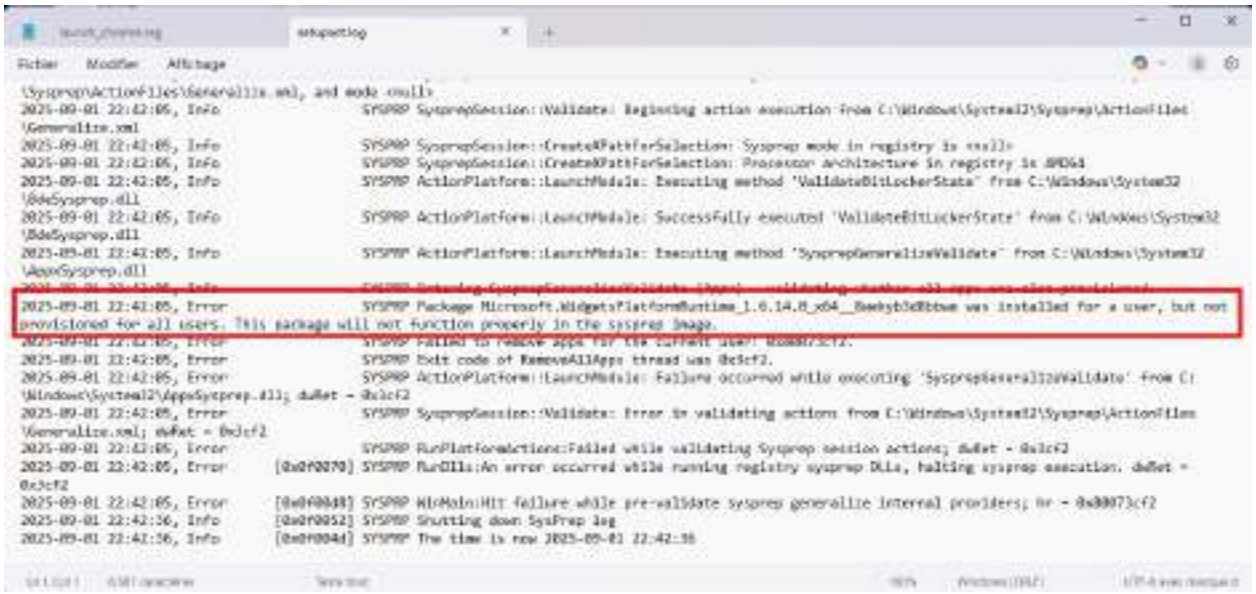
Rendez-vous dans le dossier sysprep : *C:\Windows\System32\Sysprep*



Puis dans aller voir les logs : **Panther** > **setupact**



Repérer ensuite la ligne qui empêche le lancement de la capture (situé vers la fin)



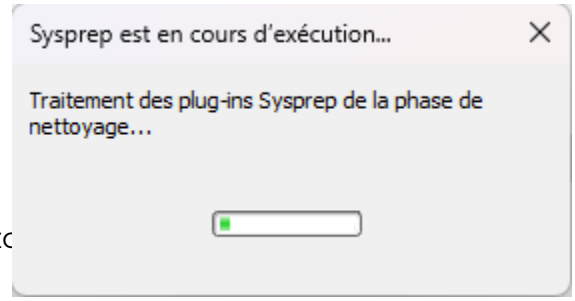
On copie le nom du paquet : *Microsoft.WidgetsPlatformRuntime*

Pour le supprimer, on se rend dans un Powershell en admin et on rentre ces 2 commandes :

Get-AppxPackage -AllUsers Microsoft.WidgetsPlatformRuntime | Remove-AppxPackage

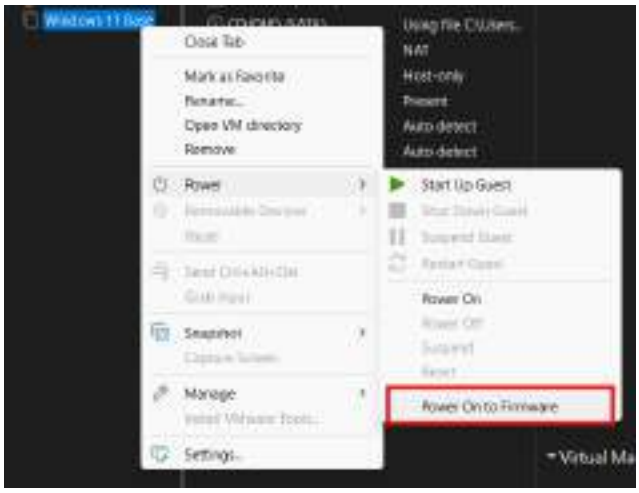
*Get-AppxProvisionedPackage -Online | Where-Object DisplayName -like "*Microsoft.WidgetsPlatformRuntime*" | Remove-AppxProvisionedPackage -Online*

Après ca Sysprep devrait se lancer correctement

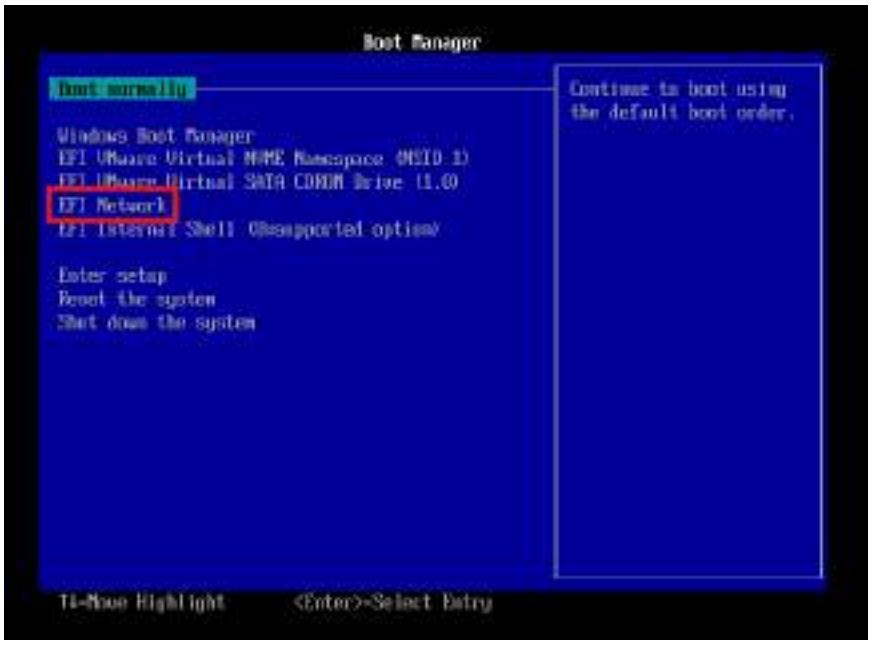


Enzo

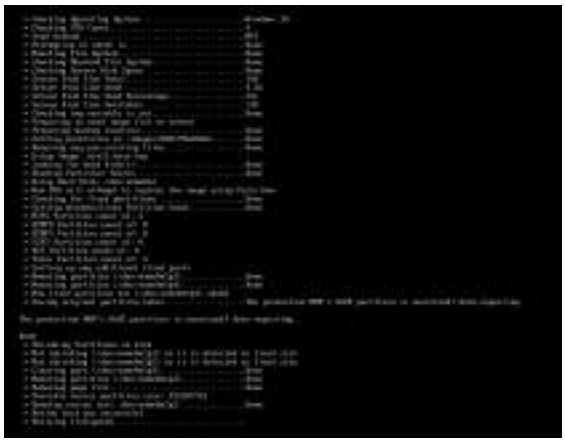
Quand la machine s’est éteinte :
Désactiver la carte NAT sur VMware (pour éviter un conflit)
Lancer la VM sur le BIOS

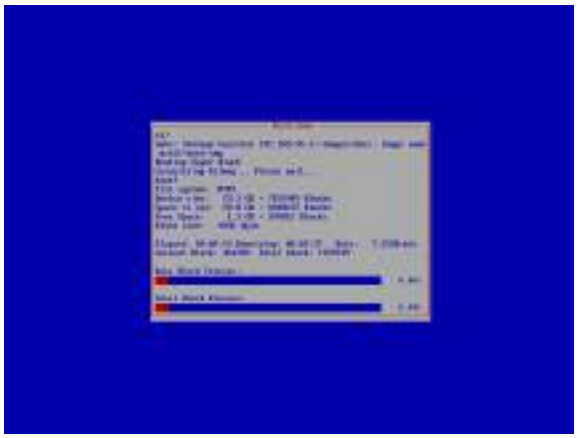


On choisit EFI Network qui correspond à la carte Host-Only

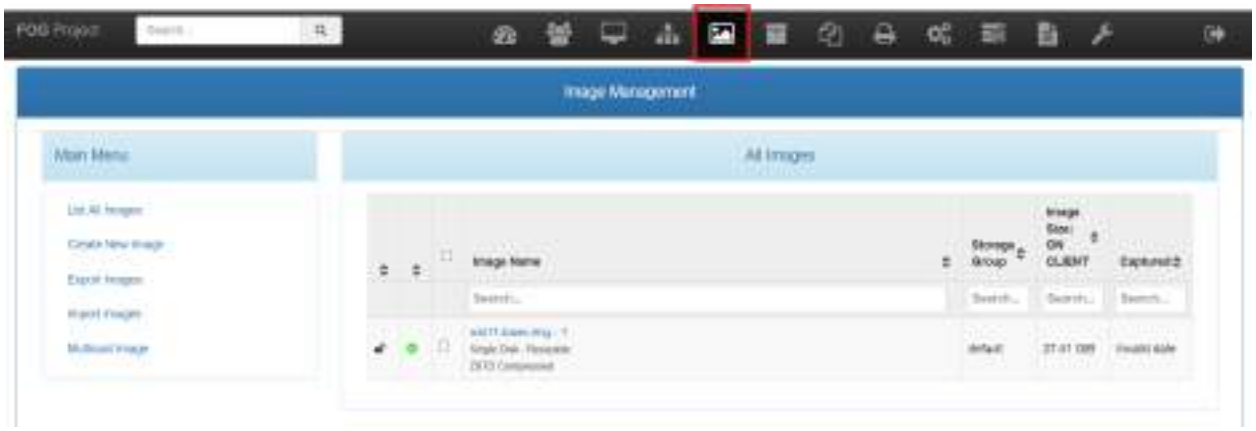


Ensuite la capture se lance automatiquement





Une fois fini, on peut voir dans l'onglet Images notre capture bien enregistré

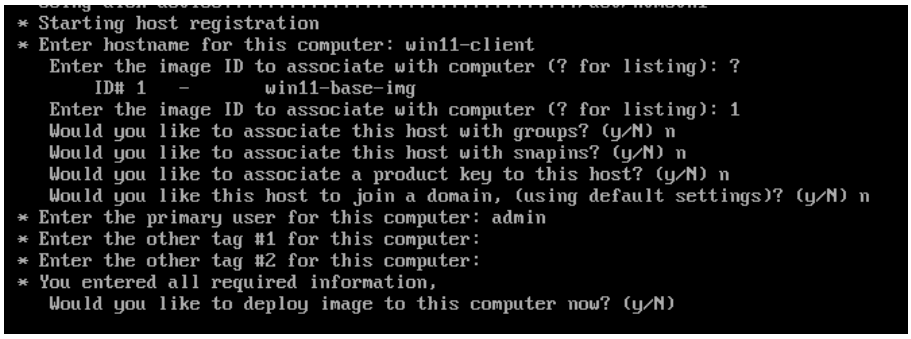


Déploiement de l’image par le réseau via FOG

On recrée une VM vierge avec une carte Host-Only & NAT puis on lance la VM et on boot en PXE.
Quand on lance pour la première fois, on nous indique que ‘Host is NOT registered!’

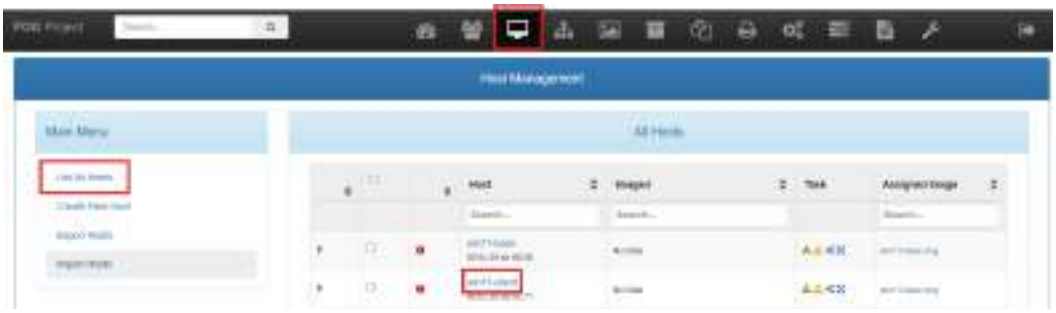
Pour l’enregistrer, on sélectionne **Perform Full Host Registration and Inventory**

On nous demande un nom et l’image qu’on souhaite utiliser ainsi que divers paramètres qui ne sont pas utiles dans notre cas

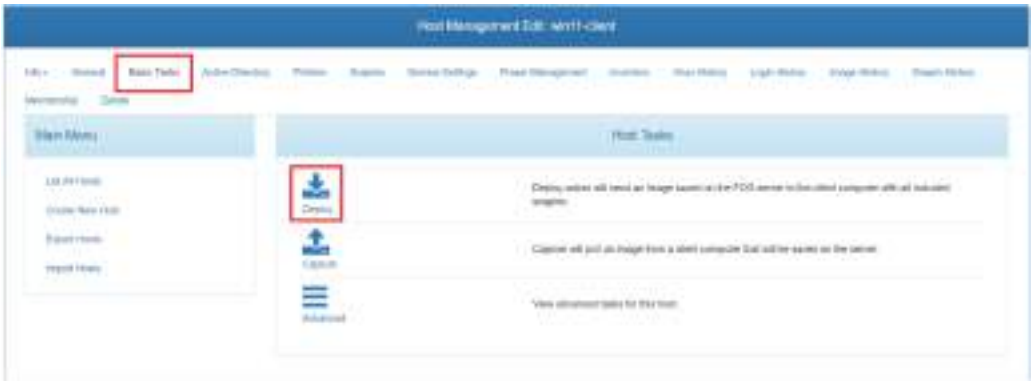


A la fin on nous demande si on veut déployer l’image immédiatement, on répond N pour le faire plus tard avec l’interface FOG.

Sur l’interface rendez-vous dans List All Hosts pour vérifier l’image associé à notre machine



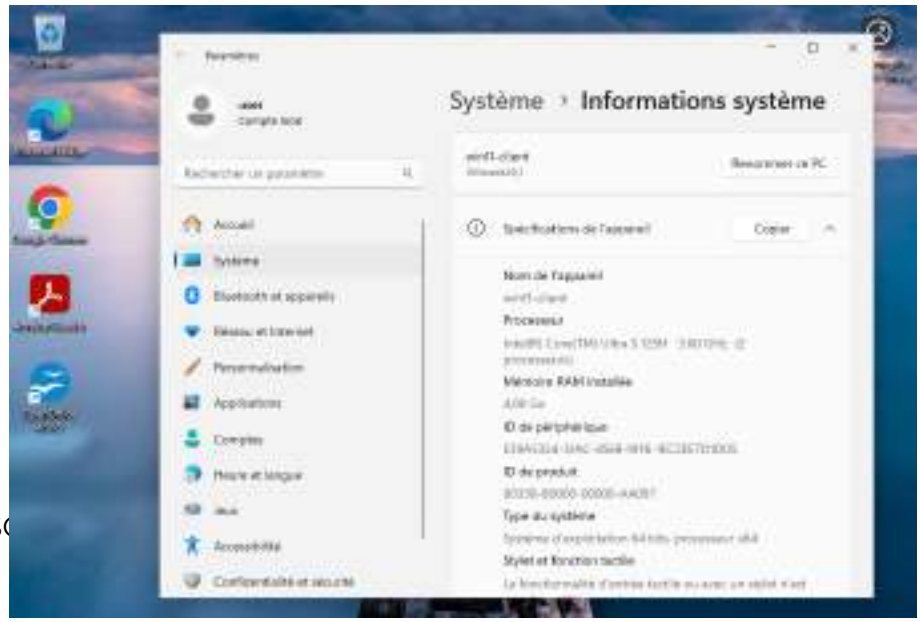
Ensuite dans **Basic Tasks** on fait **Deploy**



Sur la page de confirmation on coche “Wake on lan” si le PC est éteint sinon on décoche s'il est allumé. Et on planifie la tâche instantanée pour notre cas.

Un fois ça, on redémarre la VM et le boot en PXE va détecter une tâche de déploiement automatiquement et lancer le processus.
On fait ensuite la configuration classique pays/langue/clavier puis etc..

Une fois terminé, tous les logiciels sont présent, la page intranet.local se lance automatiquement et on peut voir que le PC a bien récupéré le nom donné dans l’interface FOG



Déploiement d'Images avec WDS

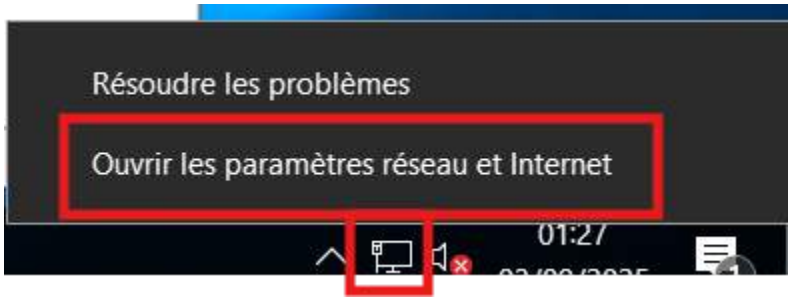
Le rôle WDS (Windows Deployment Services) permet de :

- Stocker des images Windows sur un serveur
- Les diffuser via PXE à des machines clientes
- Installer automatiquement Windows sur plusieurs postes

1. Préparer le réseau

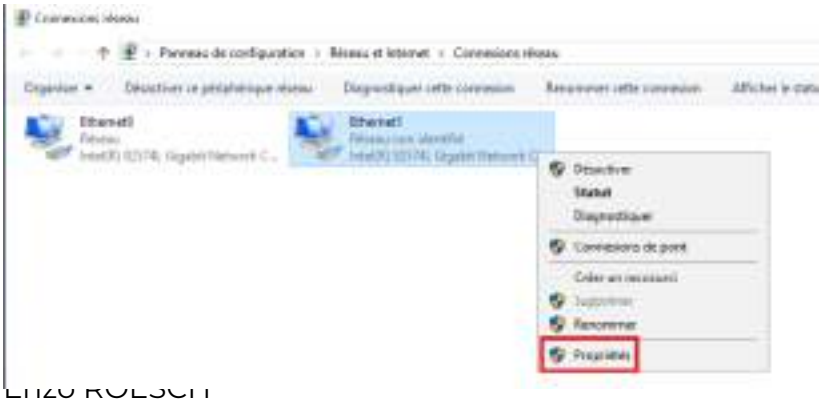
Il faut d'abord penser à attribuer une IP fixe pour que les clients puissent retrouver correctement le serveur PXE.

Clique droit sur l'**icône réseau** > **Ouvrir les paramètres réseau et Internet**

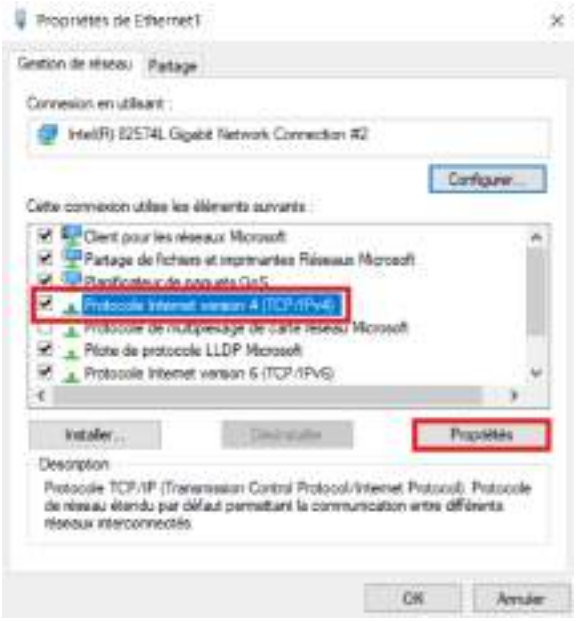


Modifier les options d'adaptateur

On sélectionne l'interface Host-only → **Clique droit** > **Propriétés**



IPv4 > **Propriétés**



Cocher **Utilise l'adresse IP suivante** puis remplir avec une adresse choisie

On peut ensuite vérifier dans le **cmd** avec **ipconfig**

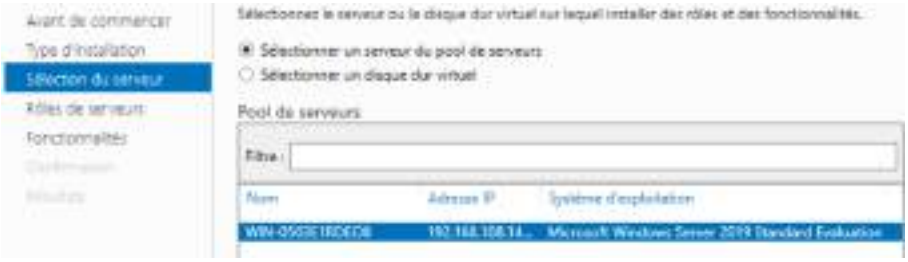
2. Installation & Configuration WDS Windows Server 2022

Ce rôle WDS permet de répondre à un boot réseau (PXE) et de diffuser des images d'installation Windows.

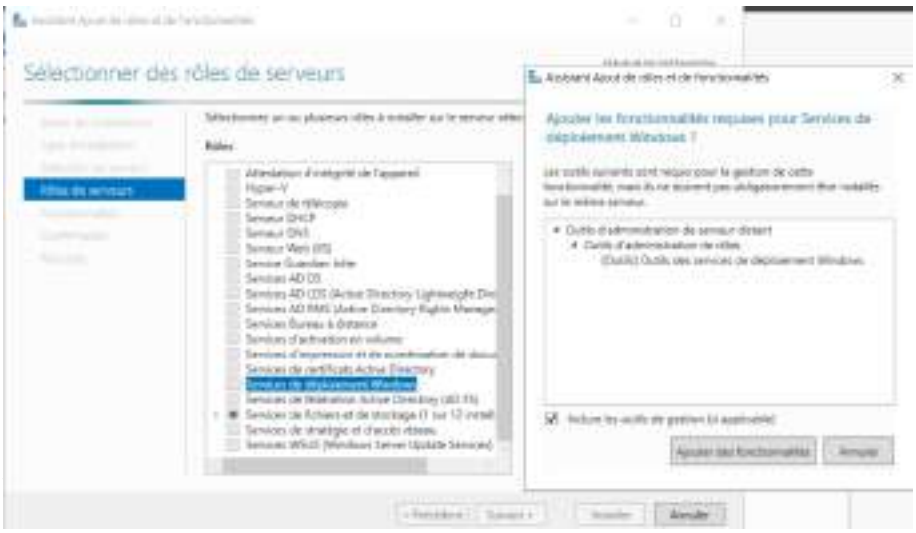
Ouvrir "**Gestionnaire de serveur**"
Cliquer "**Ajouter des rôles et fonctionnalités**"

Type d'installation : **Installation basée sur un rôle ou une fonctionnalité**

Sélection du serveur : Notre serveur local

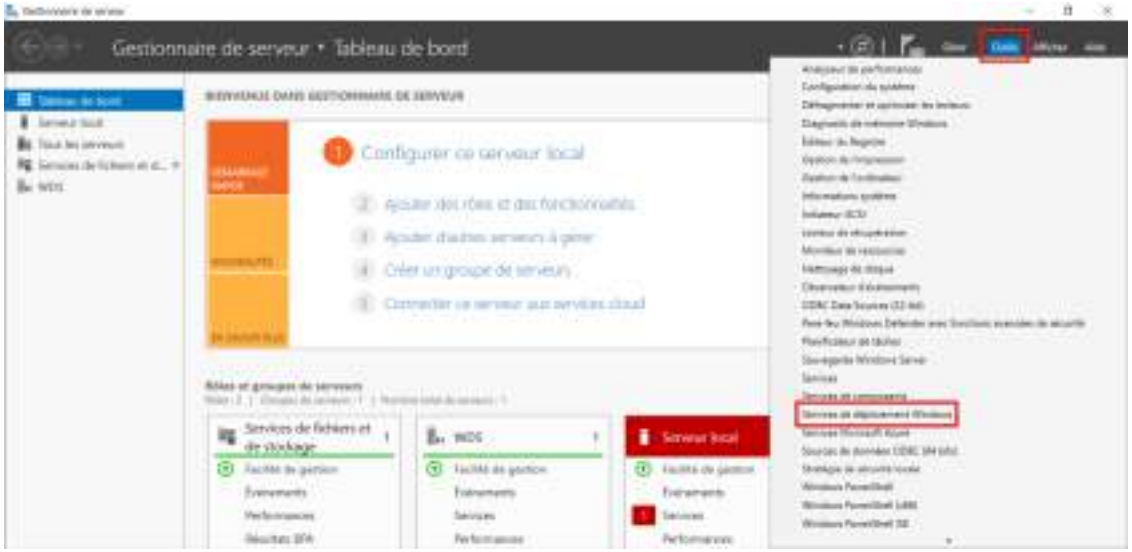


Rôles : Cocher "**Services de déploiement Windows**"

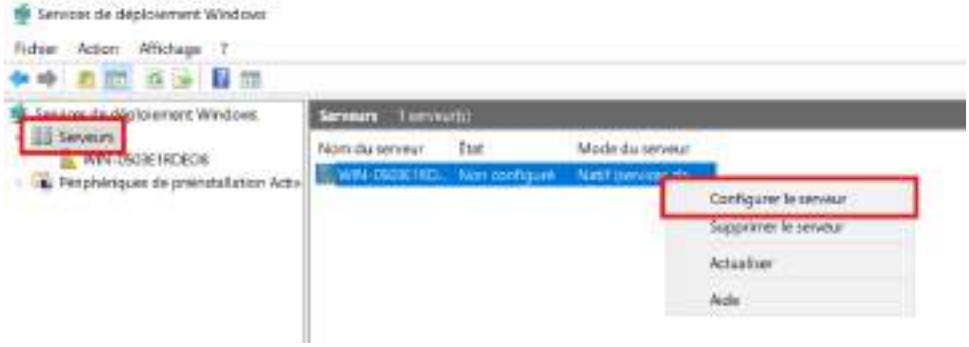


Fonctionnalités : Pas utile dans notre cas
Confirmation : On clique simplement sur **Installer**

Ouvrir **Outils** > **Services de déploiement Windows**



Serveurs > **Configurer le serveur**

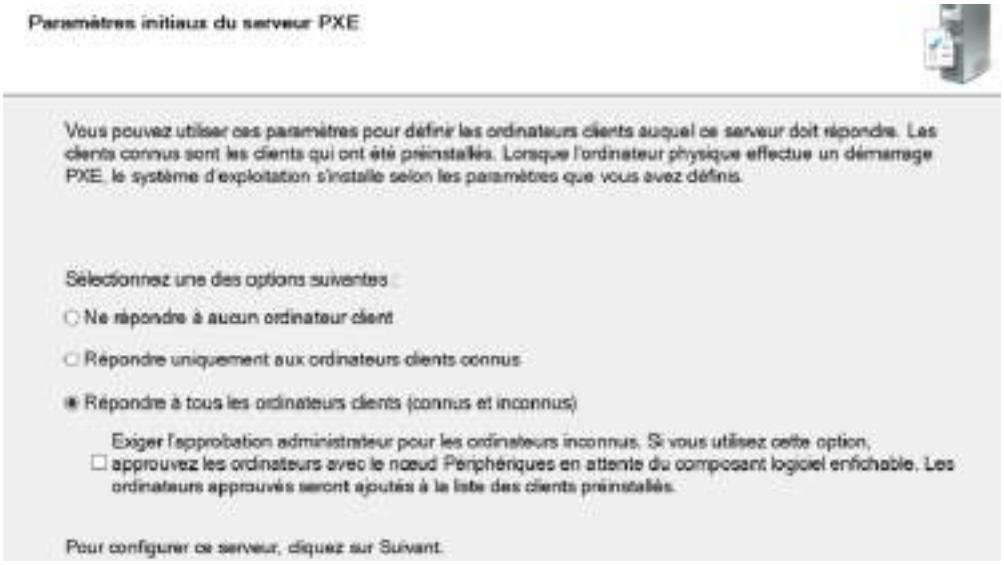


Options :

Serveur autonome (Pour les déploiement locaux)

Emplacement : *C:\RemoteInstall*
Dossier ou seront stockés les fichiers WDS

Paramètres serveur PXE : **Répondre à tous les ordinateurs clients**
Pour que n'importe quel client PXE puisse être servi automatiquement.



3. Ajouter & Déployer des images pour Windows 10

CETTE MÉTHODE NE FONCTIONNE QUE POUR WINDOWS 10
Nous utiliserons l'image modifiée avec NLite pour cet exemple.

Pour que WDS fonctionne, il a besoin de deux types d'images :
→ boot.wim (permet au client de démarrer via le réseau)
→ install.wim (contient l'image de windows qu'on installe)

Ces fichiers se situe dans l'ISO de Windows, pour les récupérer :

Clique droit > **Monter**

Sur le Gestionnaire de serveur :
Outils > **Services de déploiements Windows**
Serveurs > **Notre serveur** > Clique droit **Images de démarrage** > **Ajouter une image de démarrage**

Emplacement du fichier :
Notre lecteur monté > E:\sources\boot.wim

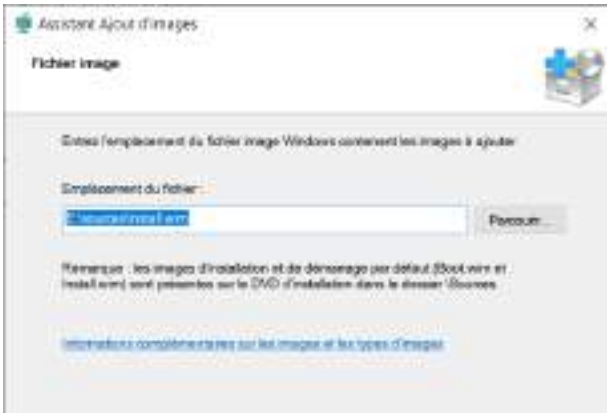
Donner un nom puis **Terminer**

Enzo ROESCH
32

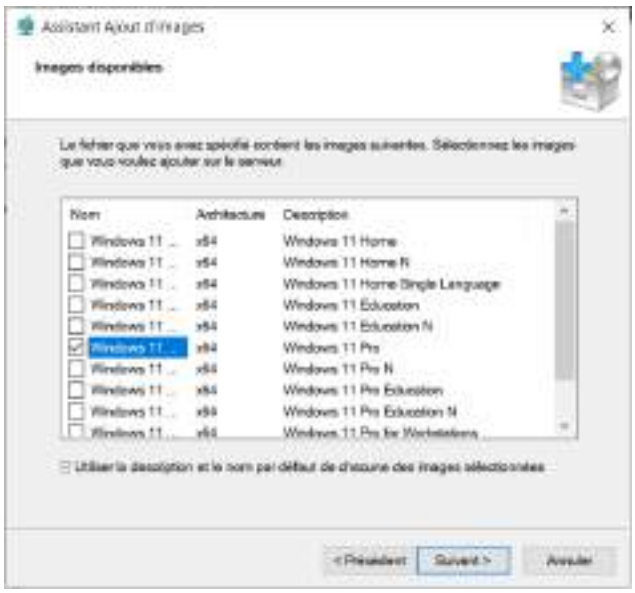
Même manipulation pour l'image d'installation :
Clique droit sur **Images d'installation** > **Ajouter une image d'installation**

Créer un groupe d'image
(ex : Windows11) → Suivant

Emplacement du fichier :
Notre lecteur monté > E:\sources\install.wim



Images disponibles :
On laisse cocher uniquement l'image que nous avons modifié précédemment ici Windows 11 Pro

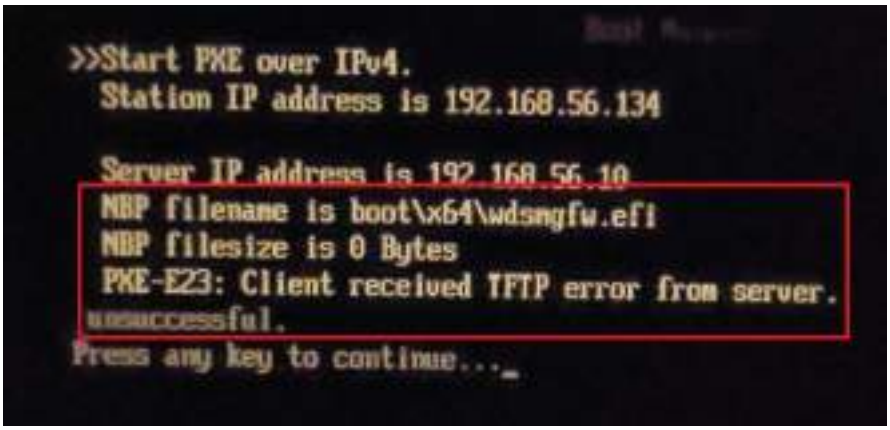


Un fois terminé on retrouve bien notre fichier chargé

Déployer l'image sur un poste client WIN10

On crée une VM cliente, disque vierge et avec une carte Host-only.
On lance la VM cliente sur le bios et on sélectionne le boot PXE

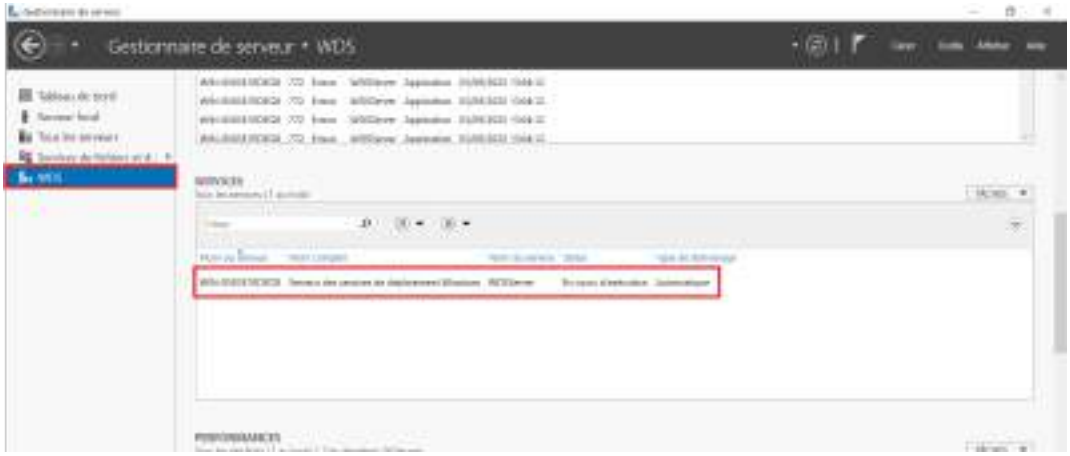
Si le boot sur PXE affiche l'erreur ci-dessous :



Le client reçoit une adresse IP via PXE (donc DHCP fonctionne).
Le client contacte bien le serveur WDS à l'adresse 192.168.56.10.

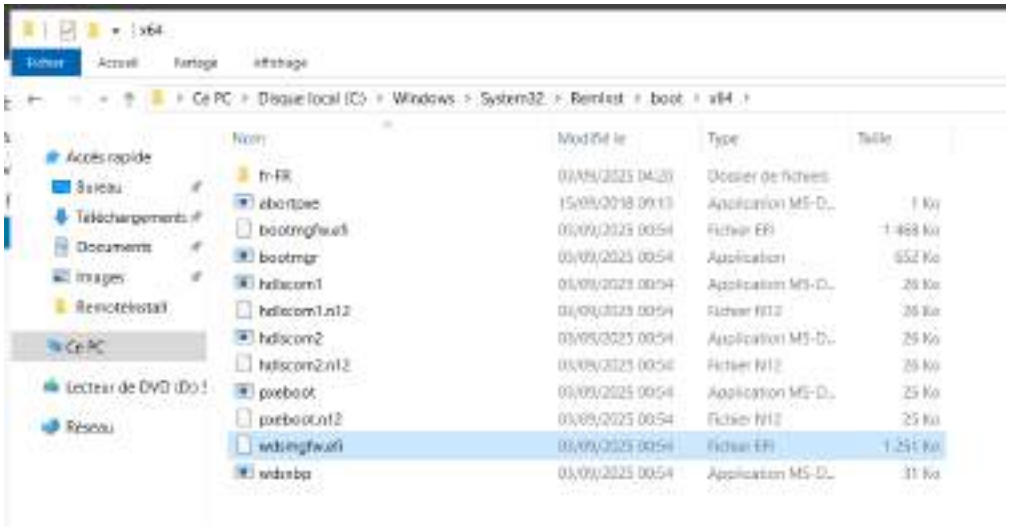
Le message "NBP filename is boot\x64\wdsmgfw.efi" & "NBP filesize is 0 Bytes" correspond au fait que le fichier de démarrage wdsmgfw.efi n'est pas trouvable ou que le service TFTP ne répond pas.

On peut vérifier que le rôle WDS est bien démarré :
On va dans **WDS** > **Catégorie Services**



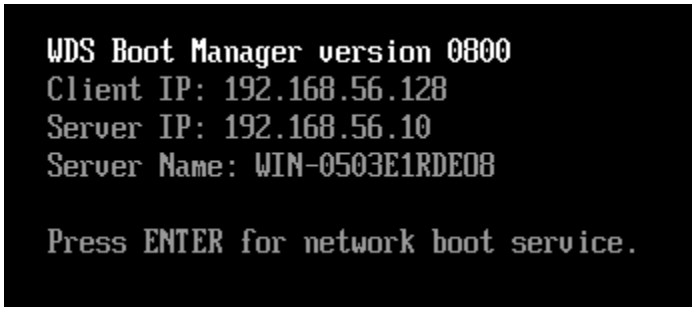
Si le statut n'est pas en cours d'exécution, Clique droit **Démarrer les services**.

Si le service est déjà lancé, on peut aller vérifier l'emplacement du fichier wdsmgfw.efi
Dans le dossier : *C:\RemoteInstall\Boot\x64*
Si le fichier est manquant, on peut aller le chercher dans le dossier *C:\Windows\System32\RemInst\boot\x64* pour le copier dans le précédent.

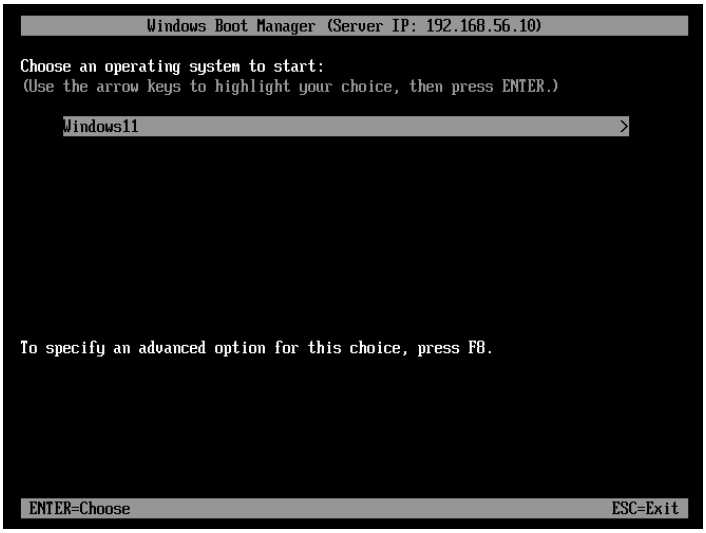


Après ça on peut redémarrer WDS pour s'assurer du bon fonctionnement.

Quand on relance la VM client, on arrive sur cette interface, tout est bon on fait juste **ENTER**



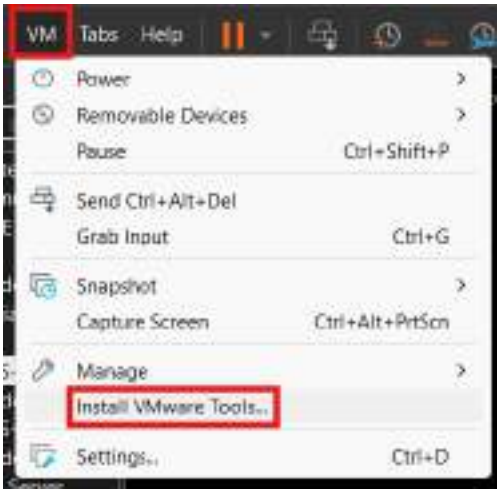
On nous demande de choisir le système qu'on veut, on prend celui qu'on a créé précédemment.



La VM télécharge boot.wim depuis le serveur WDS

Si la configuration bloque sur l'installation de driver, cela vient probablement de VMware

Arrivé sur l'écran ci-dessus, on installe les outils VMware : **VM** > **Install VMware Tools**

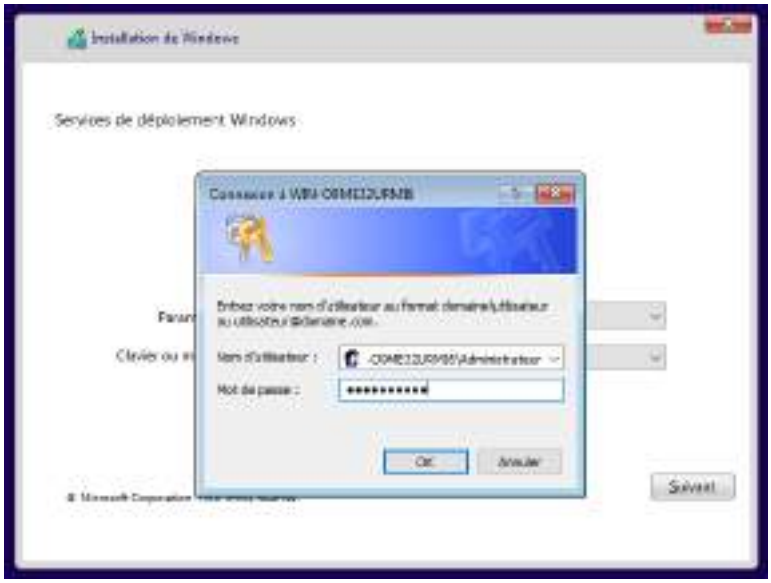


On pense d'abord à décocher "**Masquer les pilotes qui ne sont pas compatibles avec le matériel de cet ordinateur**"

Ensuite dans **Parcourir** > *D:\Program Files\VMware\Drivers\pvscsi\Win10\amd64*
A savoir que les pilotes Win10 sont compatibles avec Win11

Puis on fait **Installer**

Si l'installation se lance correctement, on atterrit sur une page de connexion on doit rentrer les identifiants du serveur WDS ici :
Nom d'utilisateur : WIN-O9ME32URMI6\Administrateur
Mot de passe : Admin@2025



On a sélectionne ensuite notre image et on procède à l'installation classique.

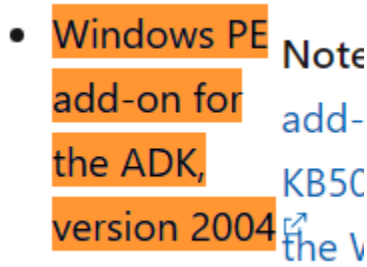
4. Ajouter des images pour Windows 11 avec MDT

MDT est un outil gratuit de Microsoft qui permet de centraliser les sources d'installation, les applications, les scripts et les règles d'automatisation dans un **Deployment Share**.

Sur un serveur Windows Server 2022, nous avons installé :

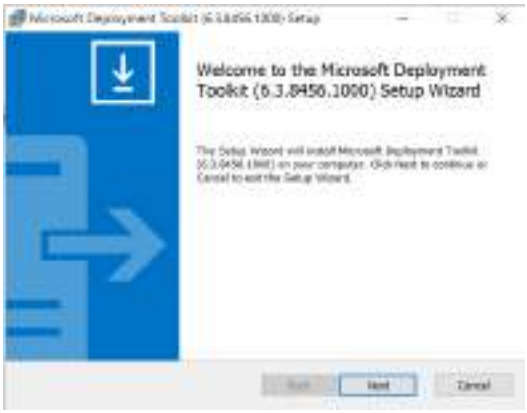
- **Microsoft Deployment Toolkit** (MDT)
- **Windows ADK** (Windows Assessment and Deployment Kit)
- **Windows PE Add-on** (module complémentaire WinPE)

Ces outils permettent de créer et gérer les images d'installation, et de générer des environnements de démarrage LiteTouch (ISO/WIM).



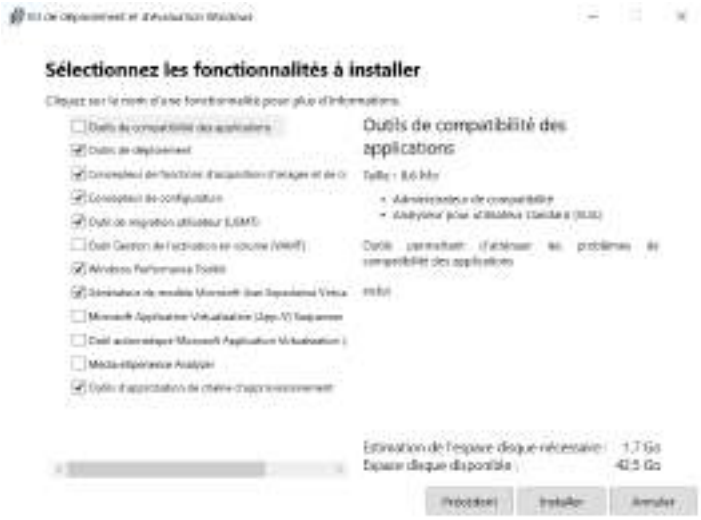
Prendre WinPE version 2004 car MDT à besoin d'une version 32 bits pour fonctionner

Installation de MDT :



Paramètres par défaut

Installation de Windows ADK :



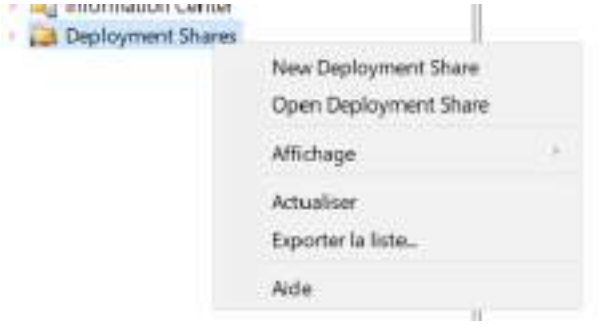
Paramètres par défaut

Installation de Windows PE Add-on :

Paramètres par défaut

Ensuite, on peut ouvrir l'application **Deployment Workbench**

Créer un nouveau Deployment Share :
Clique droit > **New Deployment Share**



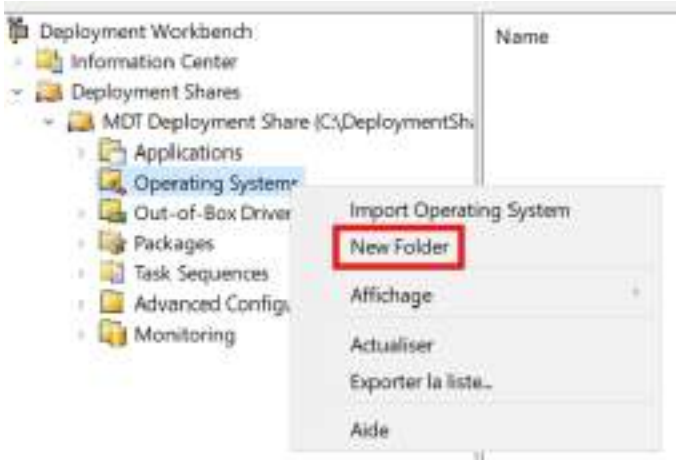
Ce dossier partagé avec le serveur WDS contient :

- les sources d'installation de Windows 11 Pro,
- les applications à installer automatiquement,
- les fichiers de configuration (Bootstrap.ini et CustomSettings.ini).

Pour les parties Share, Descriptive Name, Options, Summary, Confirmation on peut tout laisser par défaut dans notre cas.

On peut maintenant ajouter notre ISO, il faut d'abord le Monter :
Clique droit > **Monter**

Operating Systems **Clique droit** > **New Folder**



On donne un nom puis on confirme **Finish**

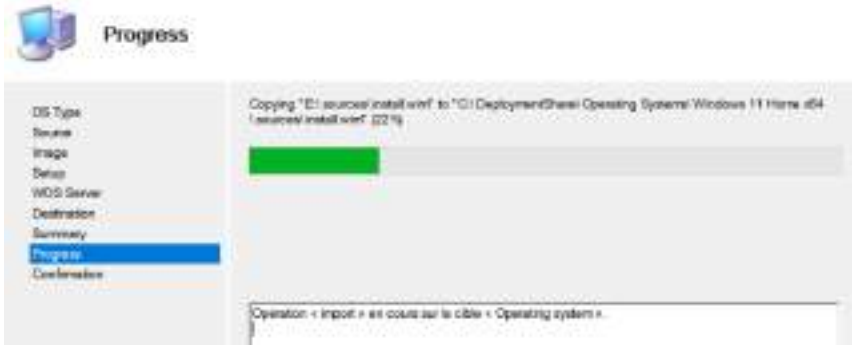
Windows 11 **Clique droit** > **Import Operating System**

On sélectionne **Full set of source files**

Enzo ROESCH
42

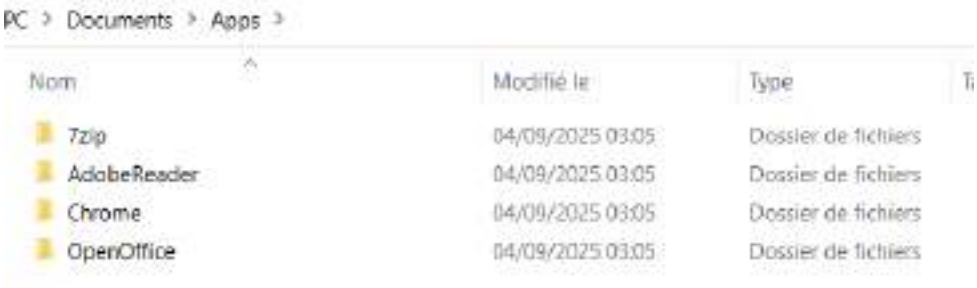
On cherche l’iso monter qui est maintenant un Lecteur

Le reste peut rester par défaut, on fait **Finish** pour importer



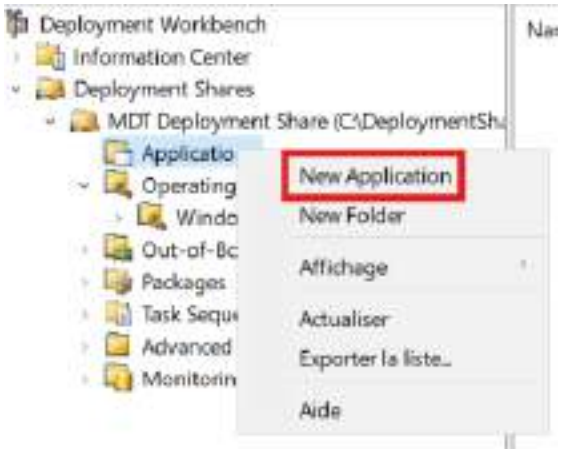
5. Configuration d’Image avec MDT

Pour ajouter des applications :
On prépare en amont un dossier pour y mettre le .exe ou .msi de chaque application.



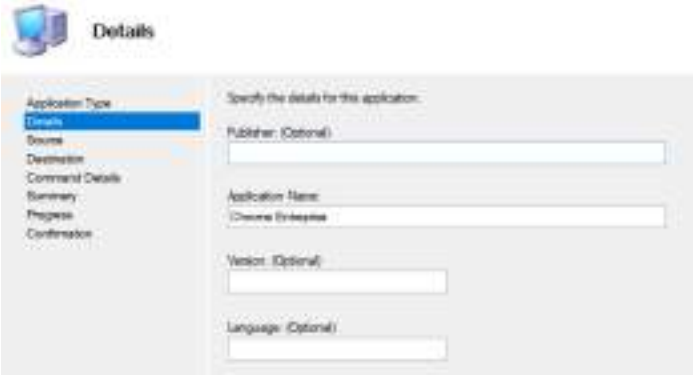
Sur MDT :

Application **Clique droit** > **New Application**



Selectionner **Application with source files**

On renseigne un nom



On renseigne le dossier source

On ajoute les commande pour automatiser l'installation

Puis on peut confirmer avec **Finish**

Commande Line pour chaque appli :

- **Chrome Entreprise** : *msiexec /i GoogleChromeStandaloneEnterprise64.msi /quiet /norestart*
- **7-Zip** : *7z2501-x64.exe /S*
- **Adobe Reader** : *AcroRdrDC2500120630_fr_FR.exe /sAll /rs /rps /msi /norestart /quiet*
- **OpenOffice** : *Apache_OpenOffice_4.1.15_Win_x86_install_fr.exe /quiet*

Pour le lancement automatique d'une page internet :

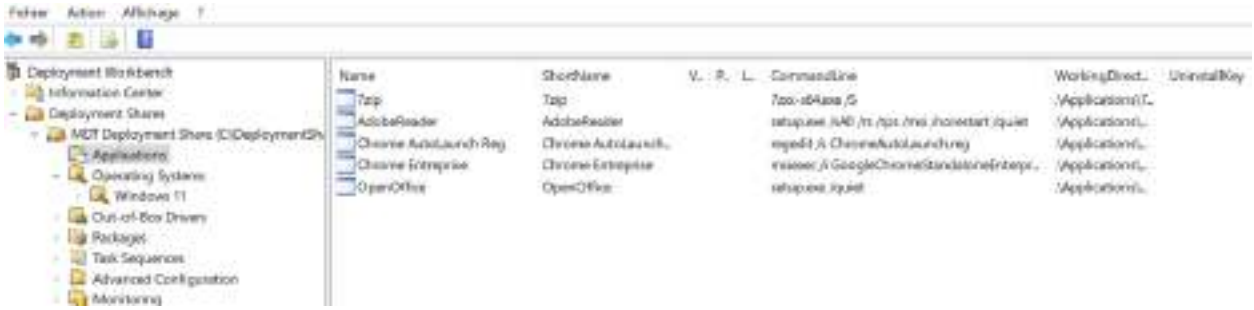
Créer un fichier .reg avec les paramètres souhaités

On met le fichier dans un dossier comme pour les autres applications, puis on ajoute le dossier comme avant.

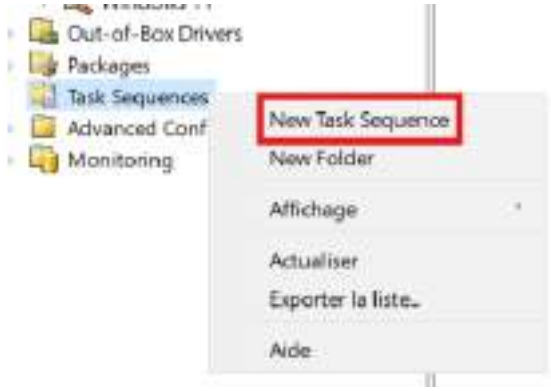
Application **Clique droit** > **New Application**
Selectionner **Application without source files**
On renseigne un nom
On renseigne le dossier source
On renseigne les commandes pour le lancement :

- *regedit /s ChromeAutoLaunch.reg*

On peut voir la liste de tout ce qu'on a ajouté :



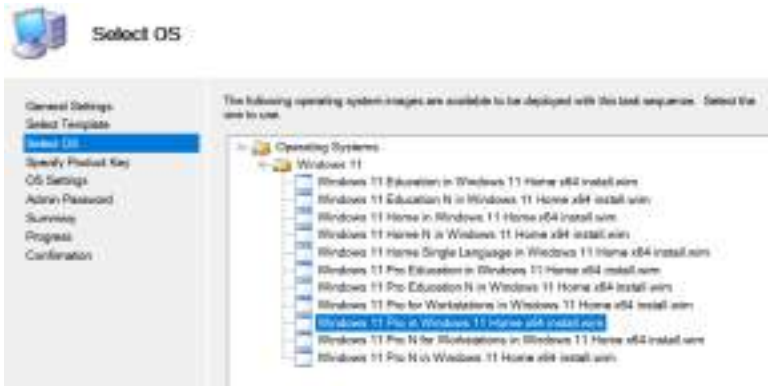
On doit maintenant créer une "Task Sequence" pour déployer le système ajouté.
Task Sequences **Clique droit** > **New Task Sequence**



General Settings : On donne ID et un Nom

Select Template : **Standard Client Task Sequence**

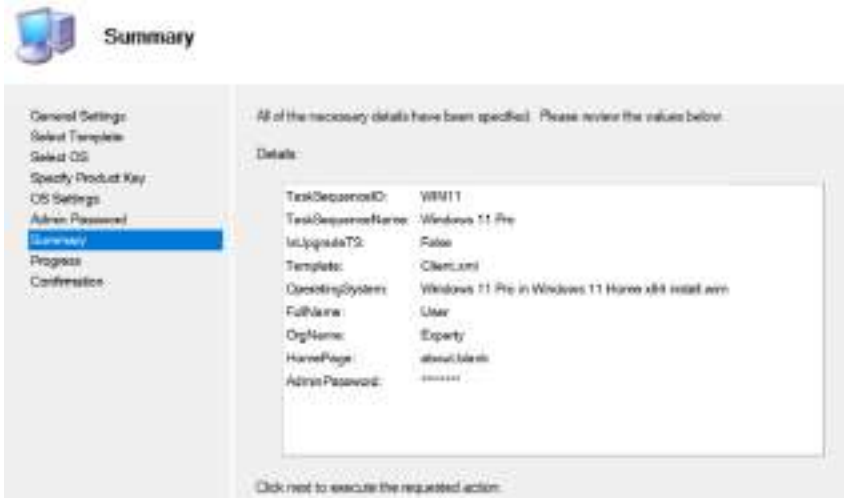
Select OS : On choisit l'image qu'on souhaite utiliser



Specify Product Key : Si on a une clé produit
OS Settings : On renseigne un nom/organisation

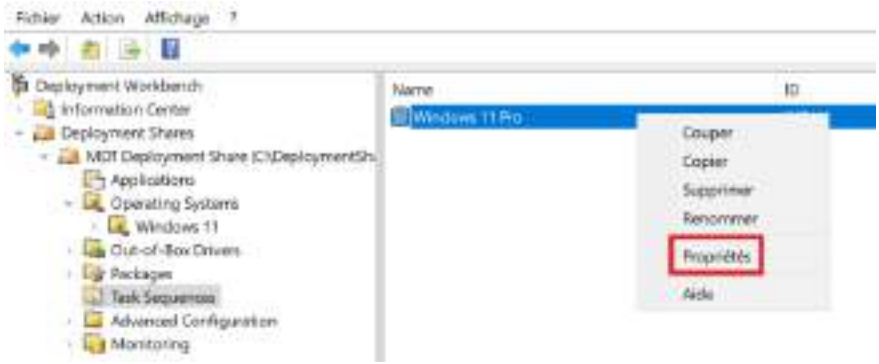
Admin Password : On peut déjà renseigner un mot de passe pour le compte administrateur (bonne pratique de sécurité)

Après on a le résumer et on peut confirmer avec Finish

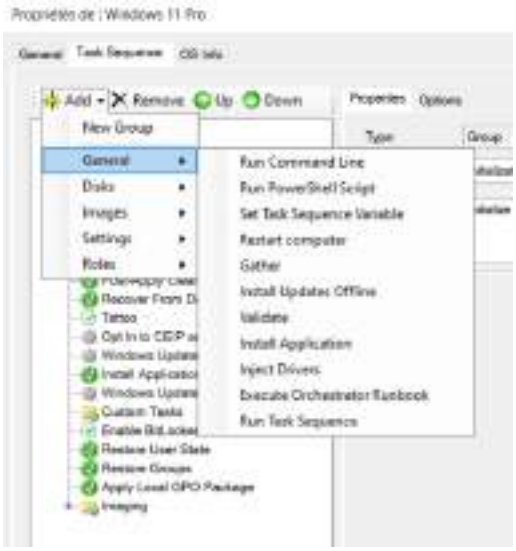


Il faut maintenant prévoir l'installation de Chrome avant que la clé de registre soit appliquée.

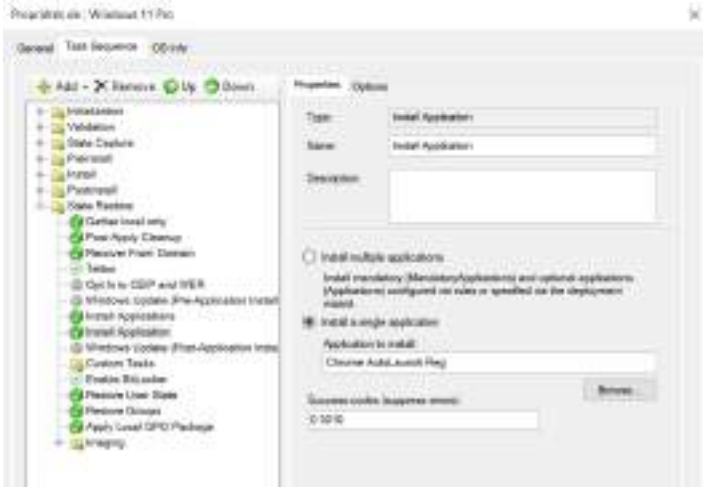
Task Sequences > Windows 11 Pro **Clique droit** > **Propriétés**



Onglet **Task Sequence** > **Add** > **General** > **Install Application** > On sélectionne AutoLaunchChrome

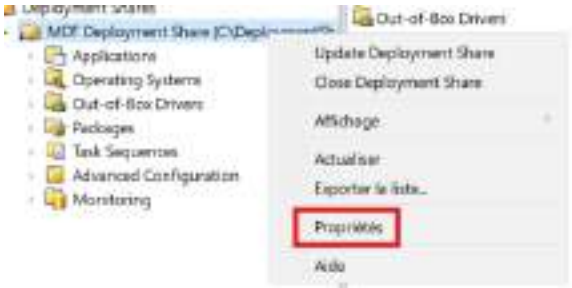


On place la Task juste après la Install Applications, sur la notre on sélectionne **Install a single application** et on donne un nom

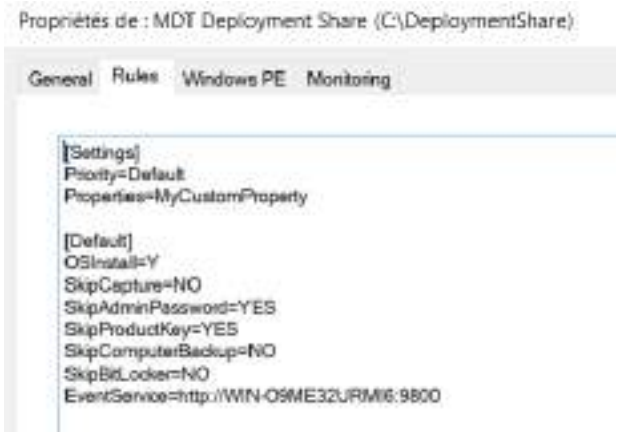


A savoir on peut **modifier les règles de lancements** pour passer les menus afin d'optimiser la mise en place du déploiement.
On peut ajouter ces règles dans les propriétés MDT :

Sur **MDT Clique droit** > **Propriétés**



Onglet **Rules**



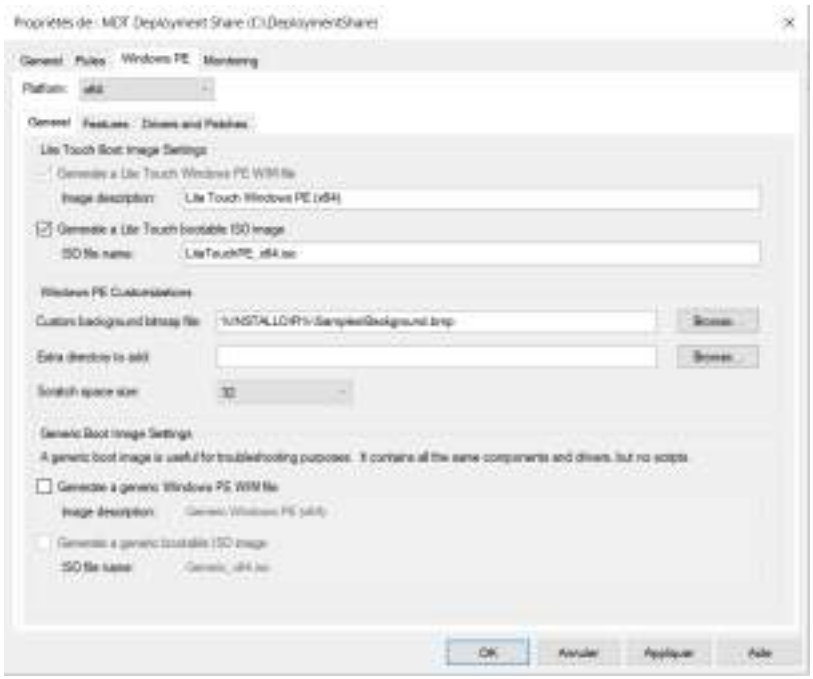
Par exemple :

SkipTimeZone=YES
SkipLocaleSelection=YES

KeyboardLocale=fr-FR
UserLocale=fr-FR
TimeZoneName=GMT Standard Time

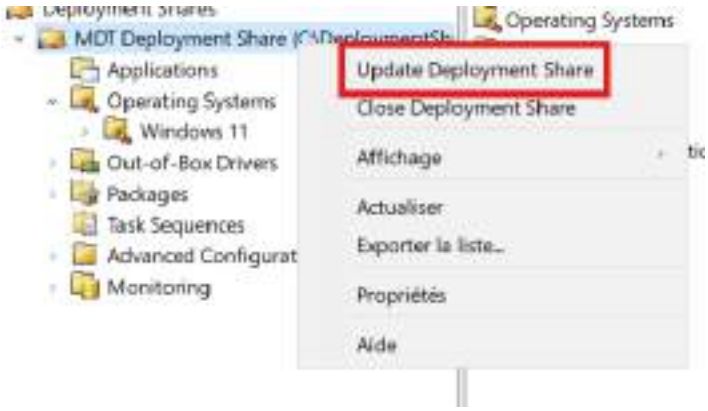
Pour passer et configurer la time zone en avance ou pour passer et configurer le choix de langue/clavier

Onglet **Windows PE**
Platform : **x64** (plus adapté pour Windows 11)



Onglet Monitoring
Si on coche Enable monitoring for this deployment share, on peut voir un tableau de bord centralisé qui montre en direct l'état de tous les déploiements des différentes machines.

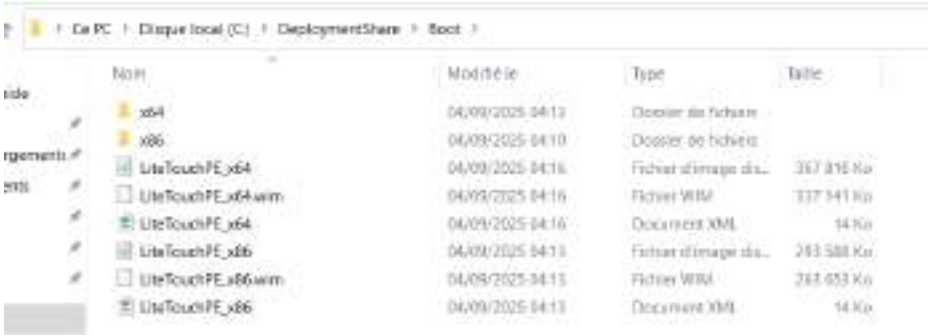
On doit maintenant mettre à jour le Deployment Share :
MDT **Clique droit** > **Update Deployment Share**



Options : **Completely regenerate the boot images** (comme c'est la première fois)

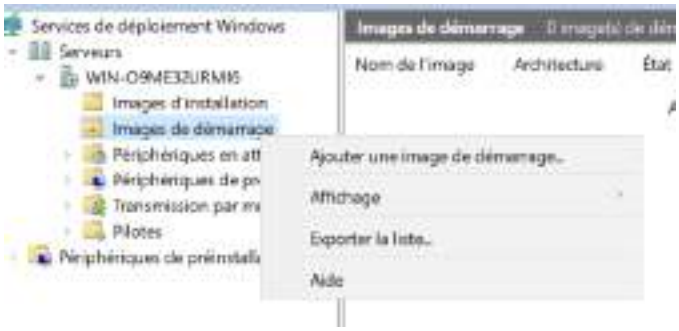
On peut faire **Next** > **Next** > Le deployment share va commencer à se générer les fichier .iso et .wim

On retrouve ce dossier sous *C:\DeploymentShare\Boot*

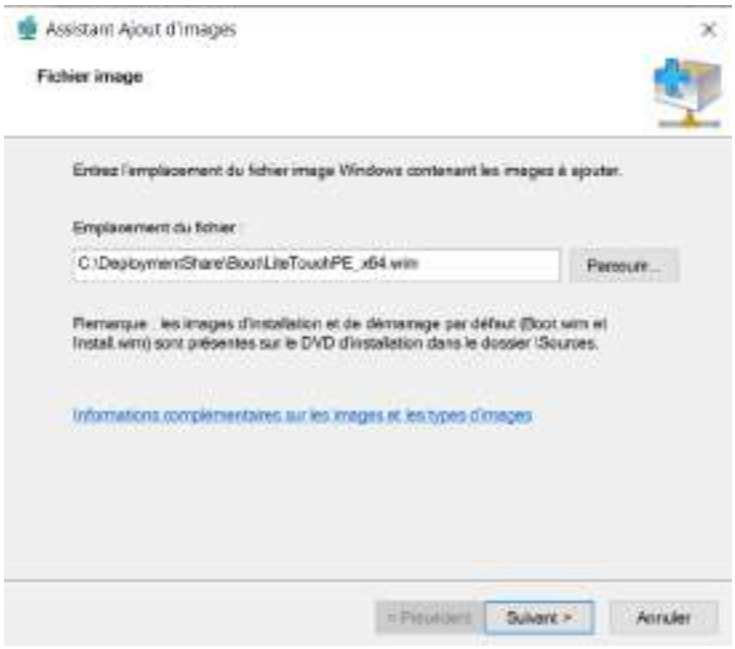


6. Déploiement d'Image Windows 11 avec MDT

On retourne sur WDS dans les **Services de déploiement Windows Serveurs** > **Notre Serveur** > Images de démarrage **Clique droit** > **Ajouter une image de démarrage**

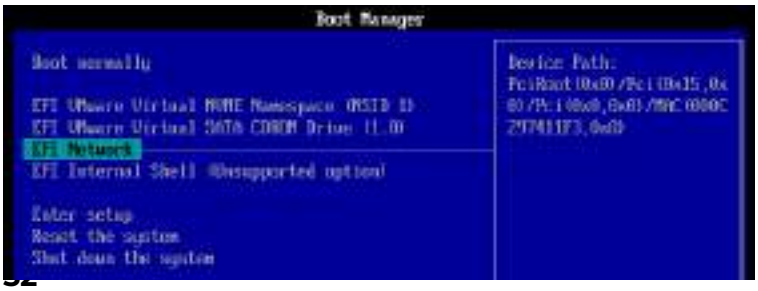


Dans **Parcourir** on cherche le fichier .wim qui vient d'être créé : *C:\DeploymentShare\Boot\LiteTouchePE_x64.wim*

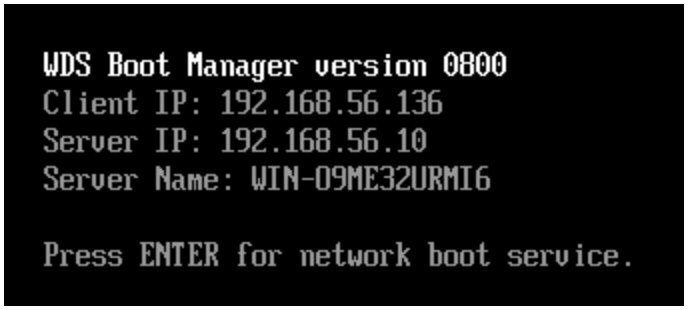


On ajoute cette image de démarrage.

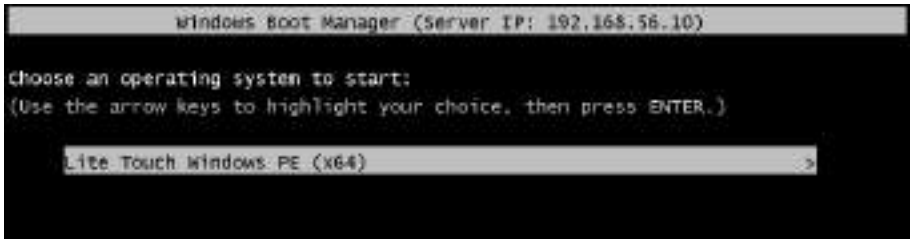
On prépare maintenant une VM vierge avec une carte Host-Only et on lance sur le bios pour sélectionner le boot PXE, ici EFI Network



Si tout fonctionne, on obtient une adresse et la connexion au serveur WDS. On fait **ENTER**

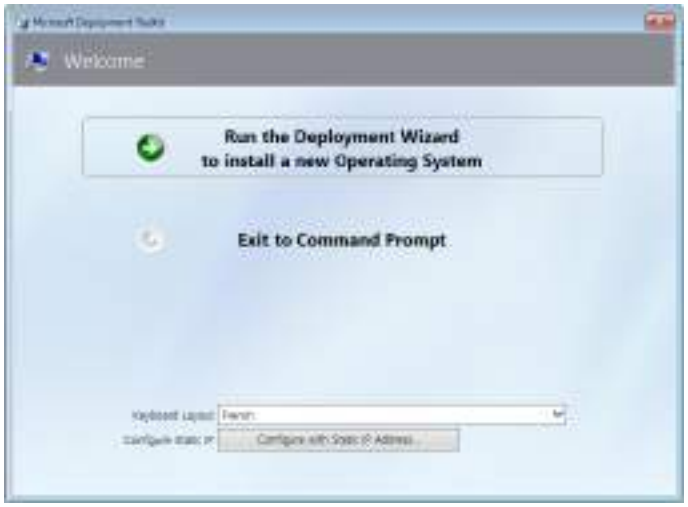


On choisit ensuite notre image de démarrage



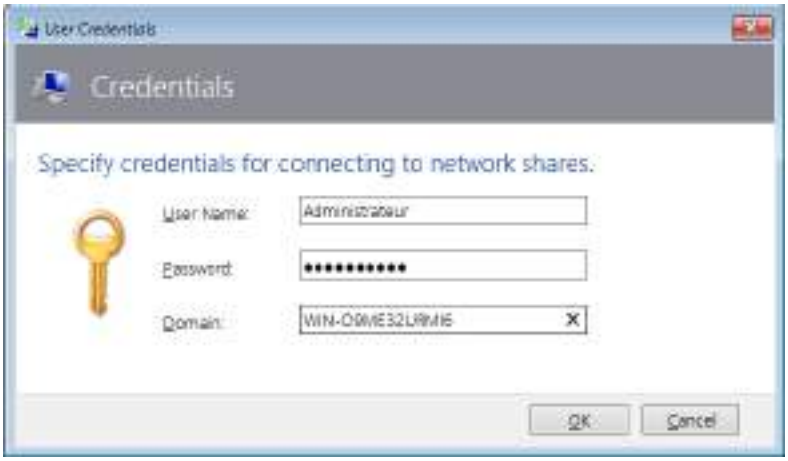
La VM charge les fichiers

Microsoft Deployment Toolkit (**WinPE**) se lance pour procéder à l'installation, on fait **Run the Deployment Wizard to install a new Operating System**



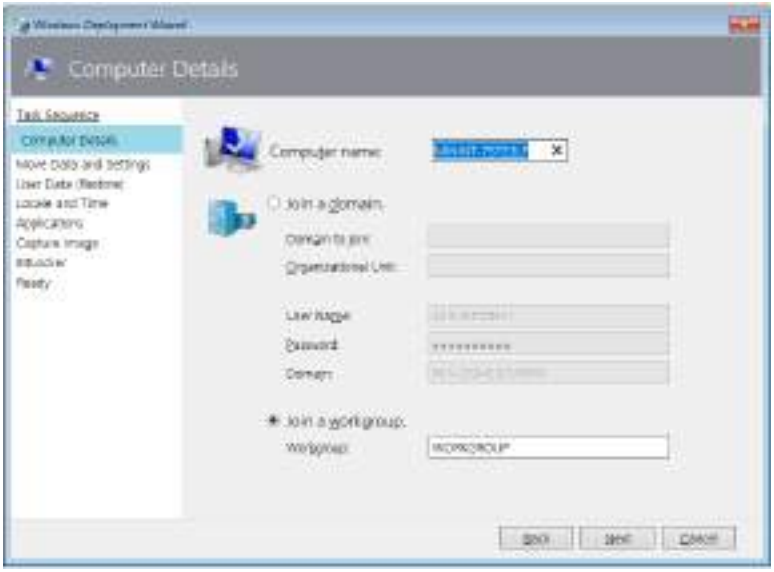
Pensez à prendre une disposition du clavier adapté

Ici, WinPE demande les identifiants pour accéder au partage réseau MDT (pour le Domain on utilise le nom de serveur dans notre cas car pas d'AD).
A savoir, cette tâche peut être automatisée dans les Rules MDT avec le fichier Bootstrap.ini.



On choisit la Task Sequence qu'on souhaite exécuter

On peut donner un nom au PC, et choisir soit un domaine soit un workgroup



Move Data and Settings : **Do not move user data and settings** (par défaut)
User Data : **Do not restore user data and settings** (par défaut)

Locale and Time : On choisit la langue, le clavier, la time zone

Applications : On choisit les applications à installer sur la machine

Capture Image : **Do not capture an image of this computer** (par défaut)
Ready : **Begin**

L'installation se lance

Sur le bureau, les applications sont installés

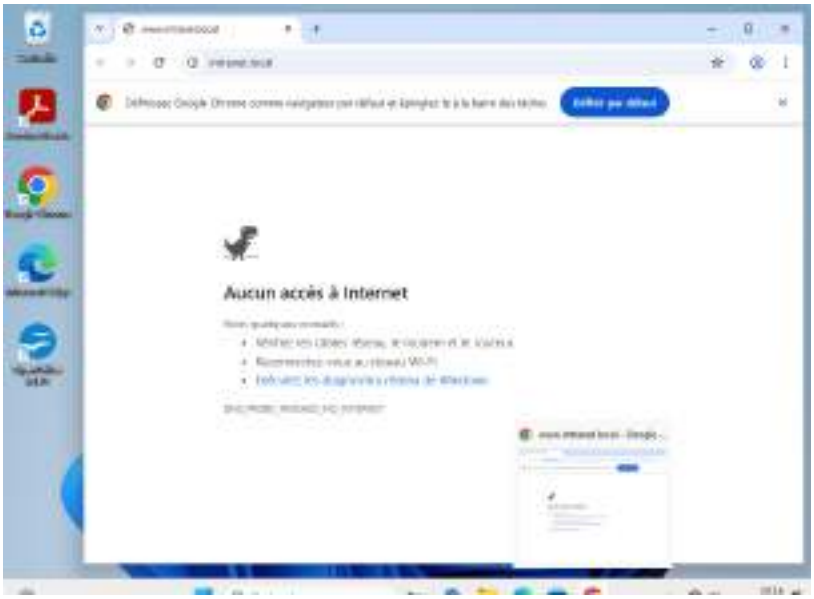
Si cette erreur apparaît à la fin de l'installation vérifier les CommandLine des applications

Exemple :

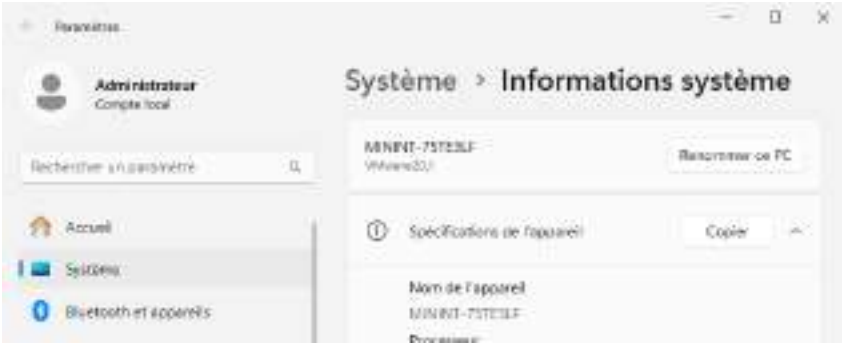
Name	ShortName	CommandLine
7zip	7zip	7zxx-x64.exe /S

La CommandLine n'a pas le bon nom.exe

Si tout fonctionne, les applications s'installent automatiquement, et la page internet intranet.local se lance toute seule.



On peut aussi voir dans les Informations système le nom qu'on a donnée précédemment à la machine.



Sécurisation des postes déployés

Dans le cadre du projet de renouvellement du parc informatique de l'entreprise EXPERTY, la sécurisation des postes clients représente un enjeu majeur. En effet, la simple installation d'un système d'exploitation et de logiciels applicatifs ne suffit pas : les postes doivent être configurés selon les bonnes pratiques de cybersécurité afin de limiter les risques de compromission, de fuite de données ou d'attaque par logiciel malveillant.

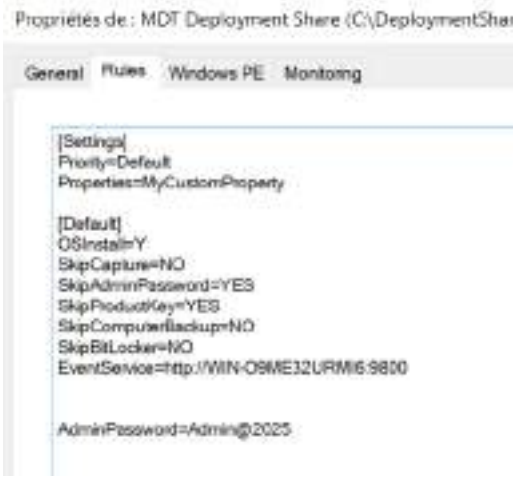
Pour ce projet, les recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et de Microsoft ont été prises en compte. Ces guides de référence fournissent un cadre permettant de définir des règles de sécurité robustes, applicables aussi bien lors du déploiement initial que dans la phase d'exploitation.

1. Mesures de sécurité intégrées au déploiement (via MDT)

Certaines mesures ont été directement intégrées à la Task Sequence MDT afin que chaque poste soit sécurisé dès la fin de l'installation :

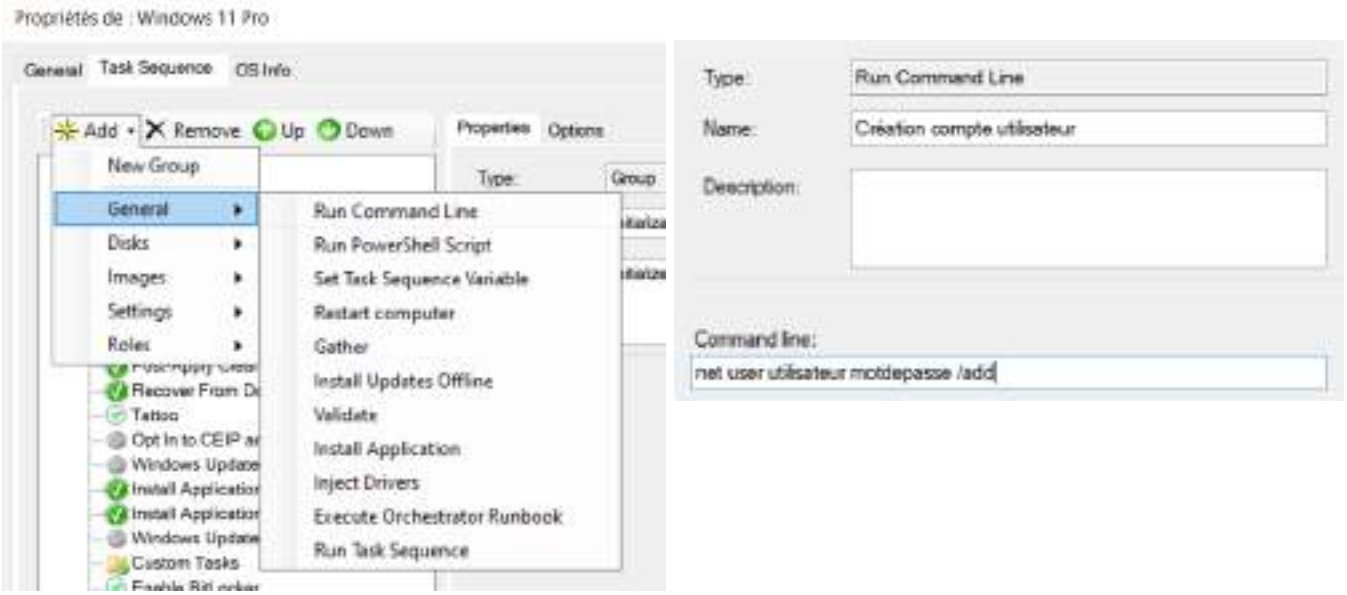
Mot de passe Administrateur local
Le mot de passe du compte administrateur local est défini et renforcé dès l'installation. Cela évite que le compte soit activé sans protection ou avec un mot de passe faible.

Exemple : Peut être configuré lors de la config d'une "**New Task Sequence**" ou après dans les **Rules MDT** : **Clique droit MDT Deployment** > **Propriétés** > **Rules** puis AdminPassword=MotDePasse



Création d'un compte standard pour les utilisateurs
Conformément au principe du moindre privilège, les utilisateurs finaux ne doivent pas disposer de droits administrateurs. Cela limite les risques d'installation non autorisée de logiciels ou de modification de la configuration système.

Exemple : Dans **Task Sequences** sur notre tâche Windows 11 créé, clique droit **Propriétés** > **Task Sequence** > **Add** > **General** > **Run Command Line**



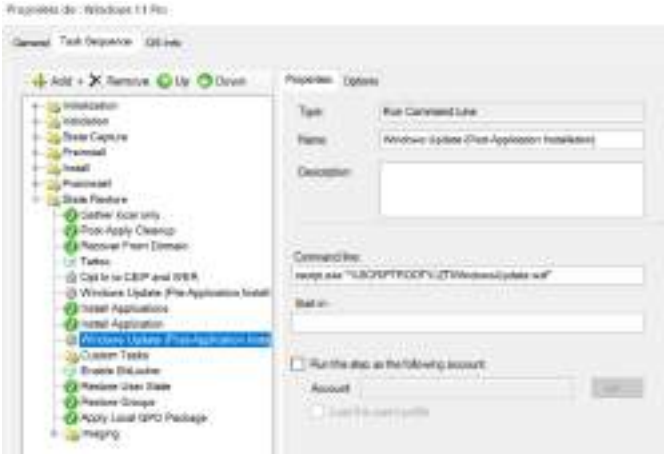
Commandes : *net user utilisateur motdepasse /add*
net localgroup Users utilisateur /add

Installation automatisée des applications nécessaires
Les logiciels requis (OpenOffice, Adobe Reader, 7-Zip, Google Chrome Enterprise) sont installés automatiquement via MDT. Cette approche garantit que chaque poste dispose des mêmes versions et limite les risques liés aux installations manuelles.

Configuration automatique du navigateur Chrome
À l'ouverture de session, Chrome démarre automatiquement et pointe vers l'intranet local (www.intranet.local). Cette configuration est appliquée via une clé de registre importée lors du déploiement.

Mises à jour Windows
Une étape de la Task Sequence permet de lancer Windows Update immédiatement après l'installation, garantissant que les postes sont patchés avec les dernières mises à jour de sécurité.

Exemple :
Toujours dans la **Task Sequence** vérifier ou ajouter une étape Windows Update après l'installation des logiciels. Les mises à jour de sécurité seront appliquées automatiquement.



Pare-feu Windows Defender
Le pare-feu est activé par défaut sur tous les profils (domaine, privé, public). Cela réduit les risques d'exposition à des services non protégés.

Quand le poste est déployé, ouvrir PowerShell pour vérifier que les 3 profils sont sur **True**

```
PS C:\windows\system32> Get-NetFirewallProfile | Format-Table Name, Enabled

Name    Enabled
----    -------
Domain     True
Private    True
Public     True
```

Commande : *Get-NetFirewallProfile | Format-Table Name, Enabled*

BitLocker (chiffrement des disques)
Une étape optionnelle dans MDT permet d'activer BitLocker. Le chiffrement des disques protège les données en cas de vol ou de perte d'un poste.

2. Mesures de sécurité post-déploiement (via GPO et supervision)

Certaines mesures doivent être mises en place après le déploiement, car elles relèvent de la gestion quotidienne et de la politique de sécurité de l'entreprise. Elles sont généralement appliquées par Active Directory et les Stratégies de Groupe (GPO) :

Politique de mots de passe
Mise en place de règles de complexité : longueur minimale de 12 caractères, présence de majuscules, minuscules, chiffres et caractères spéciaux. Rotation régulière des mots de passe et interdiction de réutiliser les anciens mots de passe.
Référence : ANSSI – Recommandations sur les mots de passe (2017).

Verrouillage automatique des sessions
Mise en veille ou verrouillage après une période d'inactivité (par exemple 10 minutes). Cela évite qu'un poste reste accessible sans surveillance.
Référence : Microsoft – Security Baseline for Windows 11.

Gestion centralisée des mises à jour
Utilisation de WSUS (Windows Server Update Services) ou de Windows Update for Business afin de s'assurer que tous les postes reçoivent régulièrement les mises à jour critiques.

Supervision et journalisation
Activation et collecte centralisée des journaux Windows (via l'Event Viewer ou une solution SIEM). Cela permet de détecter rapidement les tentatives de connexion suspectes, les erreurs systèmes ou les activités anormales.

Mises à jour des logiciels tiers
Les applications installées (Adobe Reader, Chrome, 7-Zip, OpenOffice) doivent être maintenues à jour. Une procédure de suivi ou un outil de gestion des correctifs (Patch Management) doit être mis en place.

3. Références officielles

ANSSI – Hygiène informatique : 42 règles
https://cyber.gouv.fr/sites/default/files/2017/01/guide_hygiene_informatique_anssi.pdf

ANSSI – Recommandations sur les mots de passe
https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

Microsoft – Security
https://learn.microsoft.com/en-us/windows/security/

Il faut retenir que la sécurisation des postes clients ne repose pas uniquement sur l'installation d'un système d'exploitation et de logiciels métiers. Grâce à l'utilisation de MDT, il est possible d'intégrer directement un grand nombre de mesures de sécurité dès le déploiement (mot de passe administrateur, installation normalisée des applications, configuration du pare-feu, chiffrement, mise à jour).

Ces mesures techniques doivent être complétées par des politiques organisationnelles appliquées via Active Directory et GPO : gestion des mots de passe, verrouillage automatique des sessions, supervision et mises à jour continues.