MDT : Microsoft Deployment Toolkit

Présentation

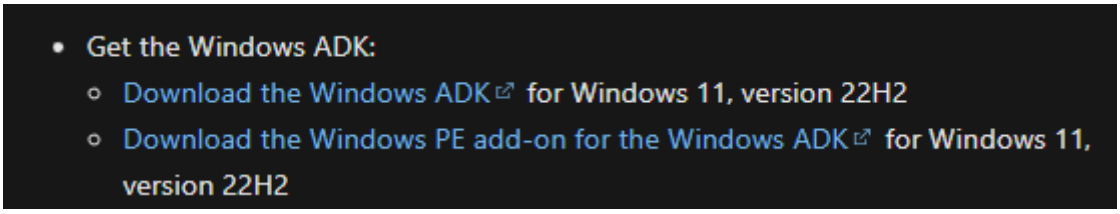
MDT pour Microsoft Deployment Toolkit est un outil pour préparer le déploiement de machines Windows. Il permet d'installer des logiciels, des pilotes, gérer les paramètres de l'ordinateur... le tout durant ou après l'installation par le réseau via le service WDS.

Installation

Prérequis

On télécharge et installe ADK et WinPE.

https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install



On exécute le setup en Admin, en laissant tout par défaut.

Installation de MDT

On va ensuite pouvoir télécharger et installer MDT.

https://www.microsoft.com/en-us/download/details.aspx?id=54259

Une fois installé, on télécharge la mise à jour.

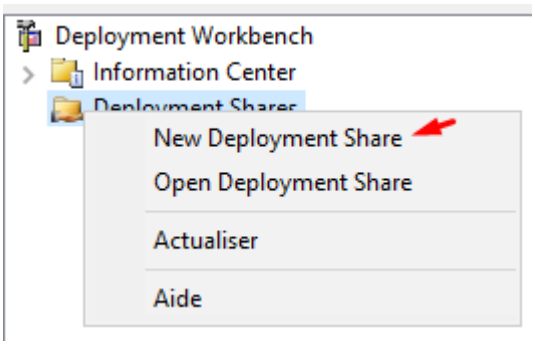
https://support.microsoft.com/en-us/topic/windows-10-deployments-fail-with-microsoft-deployment-toolkit-on-computers-with-bios-type-firmware-70557b0b-6be3-81d2-556f-b313e29e2cb7

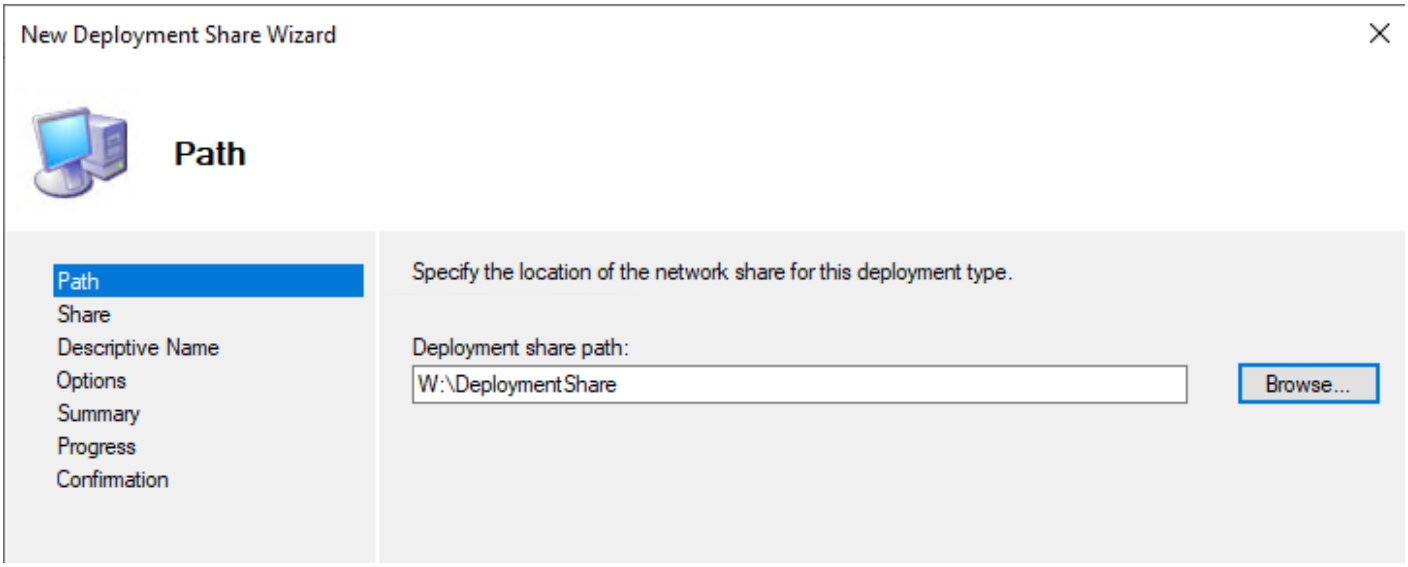
On exécute le .exe, et on copie les fichiers extraits dans %ProgramFiles%\Microsoft Deployment Toolkit\Templates\Distribution\Tools.

Création du partage de déploiement

On crée un nouveau dossier sur la partition du WDS, nommé DeploymentShare.

On ouvre ensuite la console Deployment Workbench et on crée notre partage.

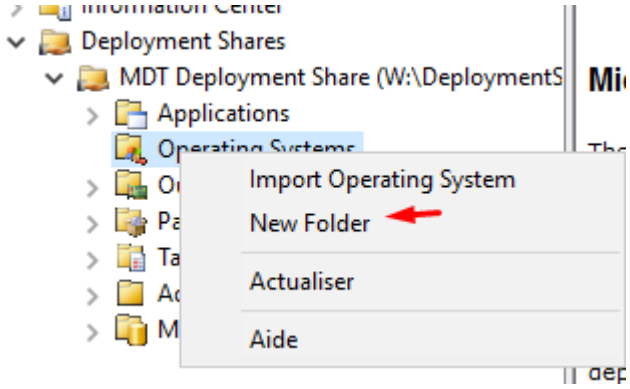


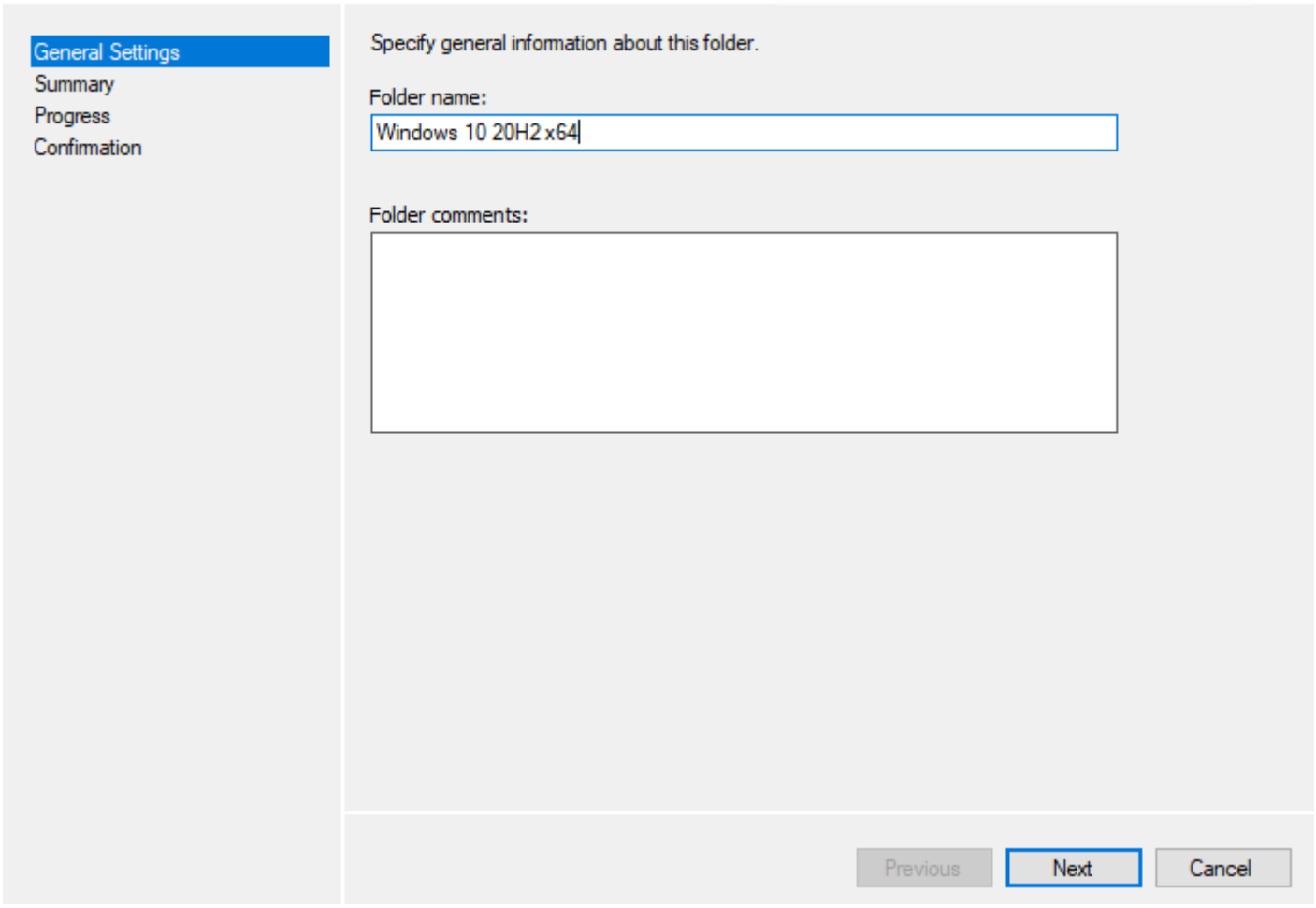


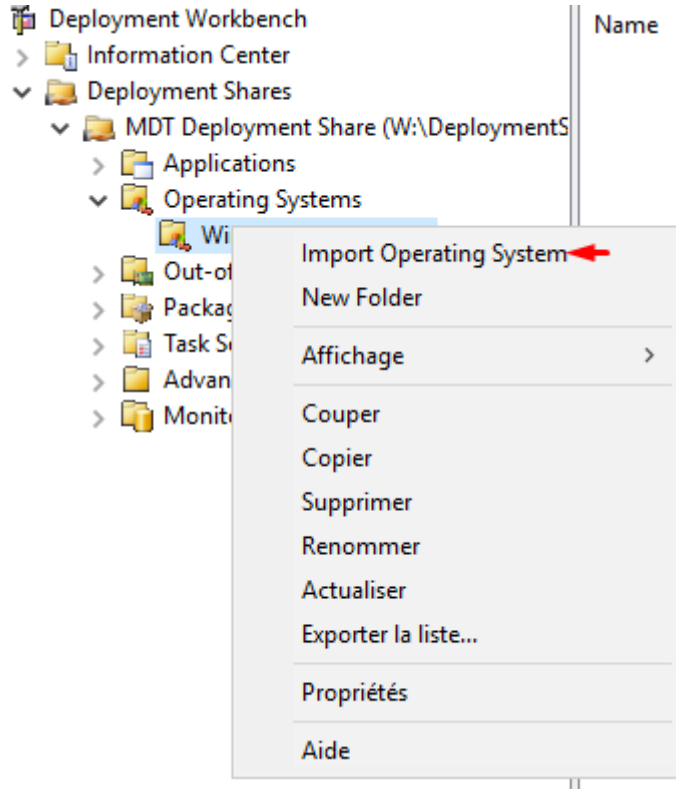
On laisse tout par défaut, on peut modifier les options plus tard.

Ajout du système d'exploitation

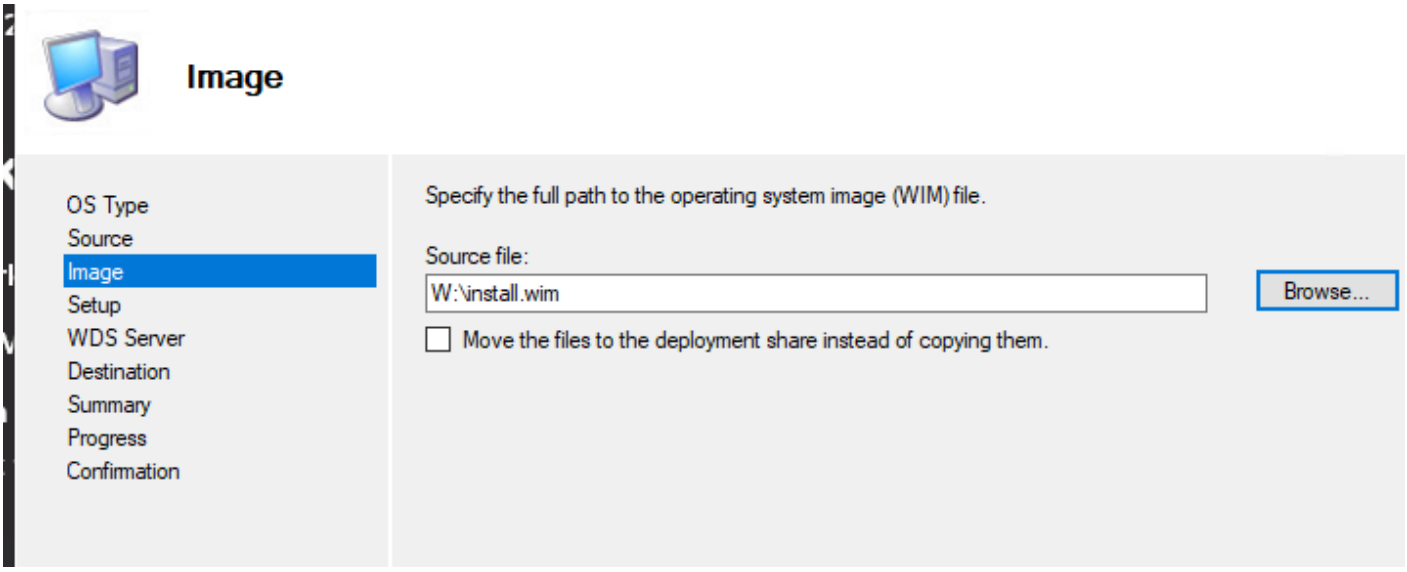
On crée un nouveau dossier nommé "Windows 10 Pro 20H2".

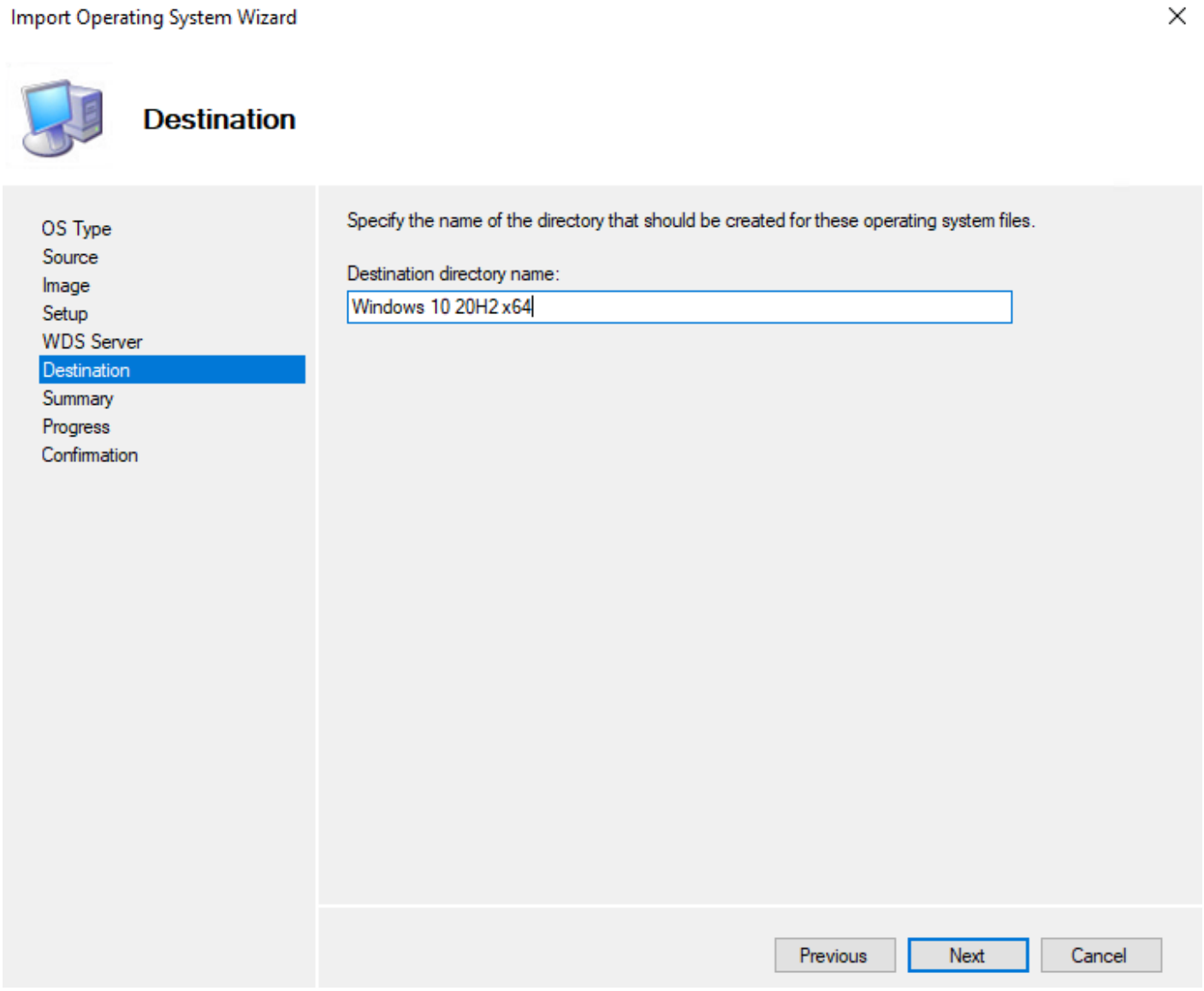

Deployment Shares
MDT Deployment Share (W:\DeploymentS
Applications
Import Operating System
New Folder
Actualiser
Aide

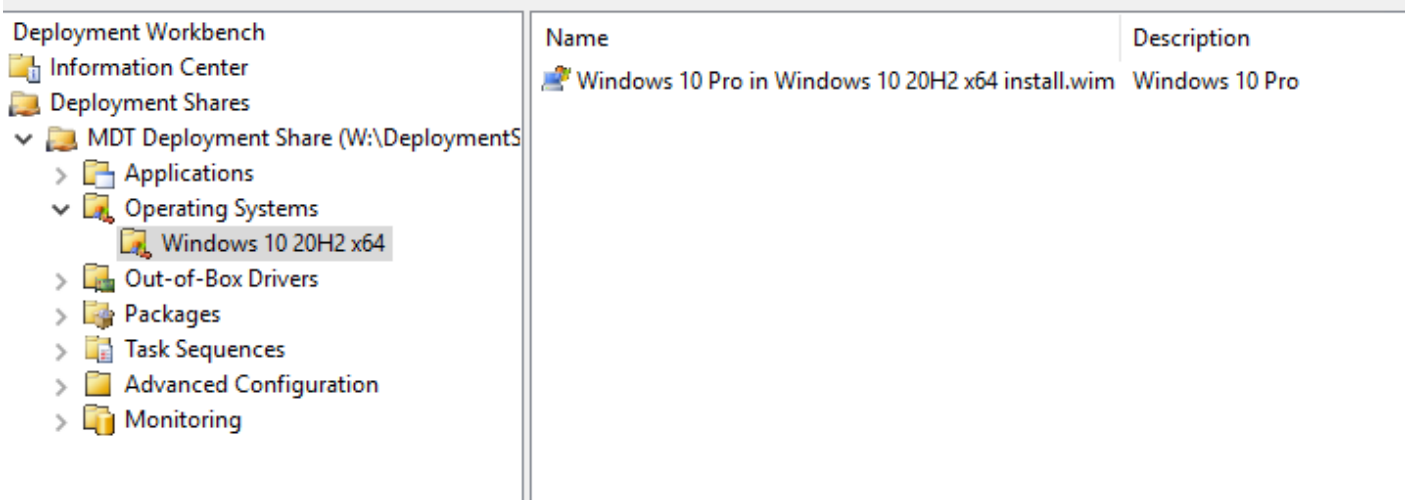

General Settings
Summary
Progress
Confirmation
Specify general information about this folder.
Folder name:
Windows 10 20H2 x64
Folder comments:
Previous
Next
Cancel



On monte le fichier .wim extrait auparavant.





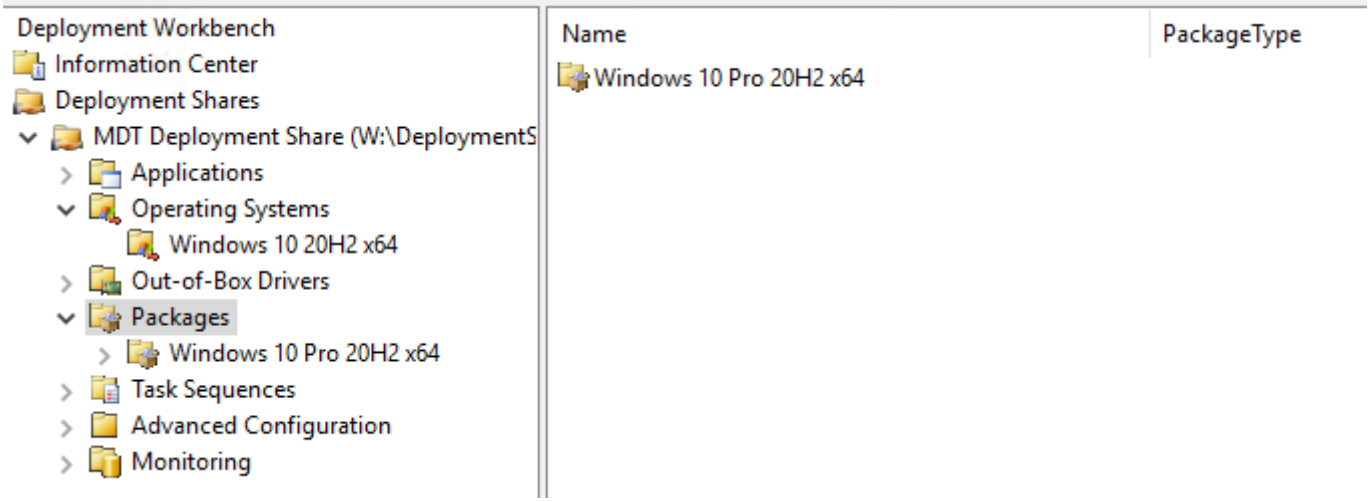


On le renomme.

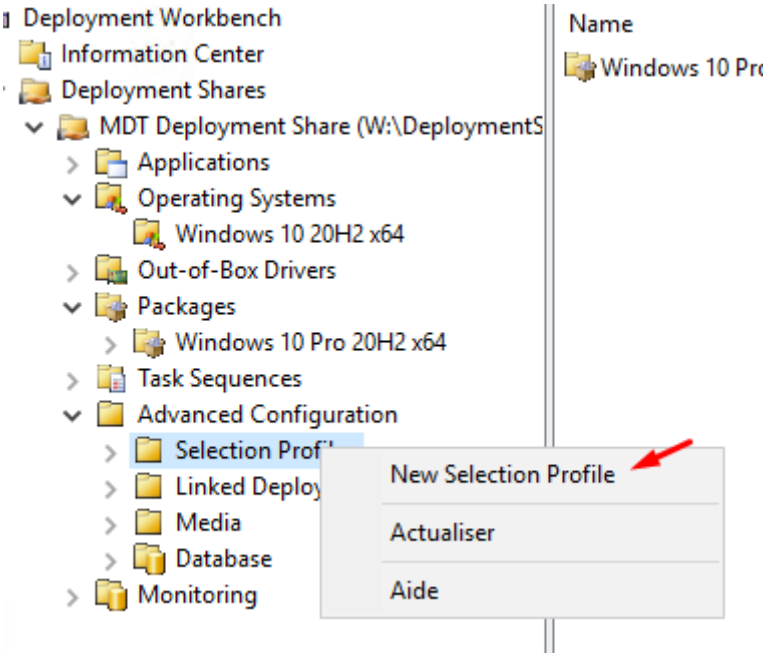


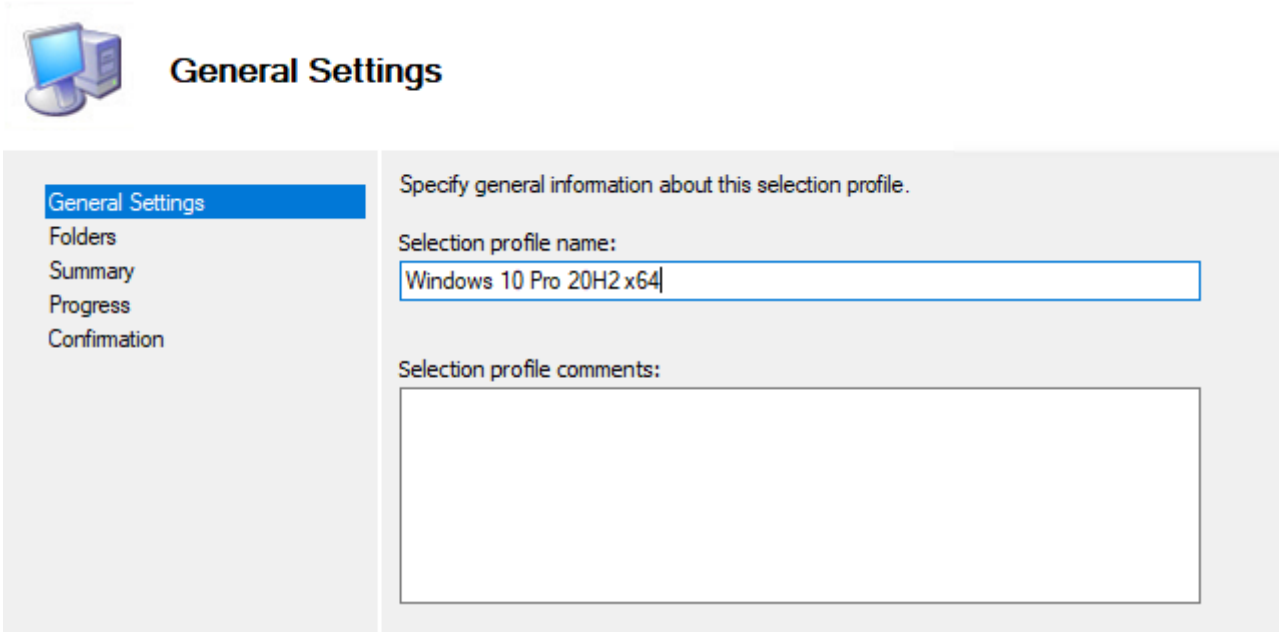
Création d'un dossier de packages

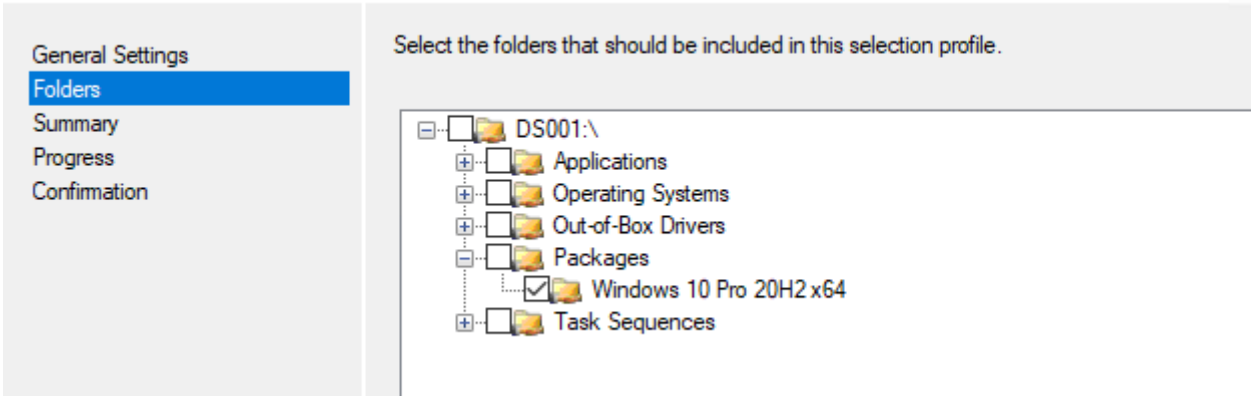
On crée un dossier dans "Packages" pour les mises à jour.



On crée ensuite un profil de sélection.

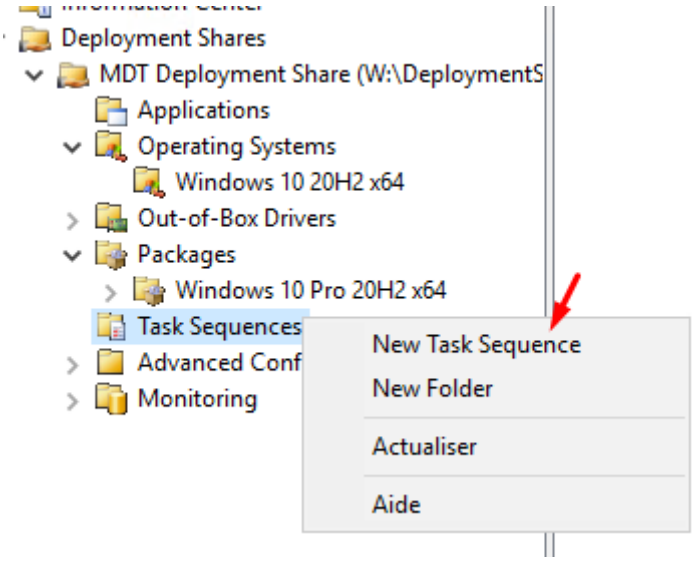


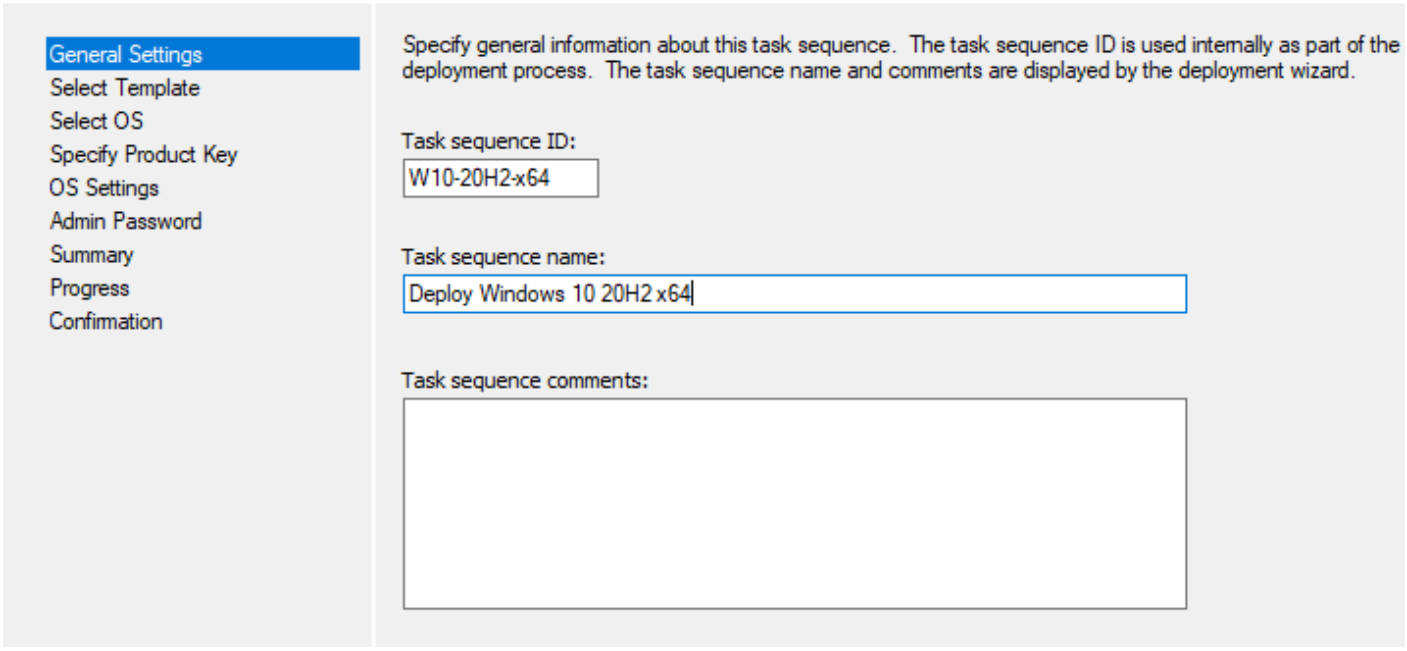


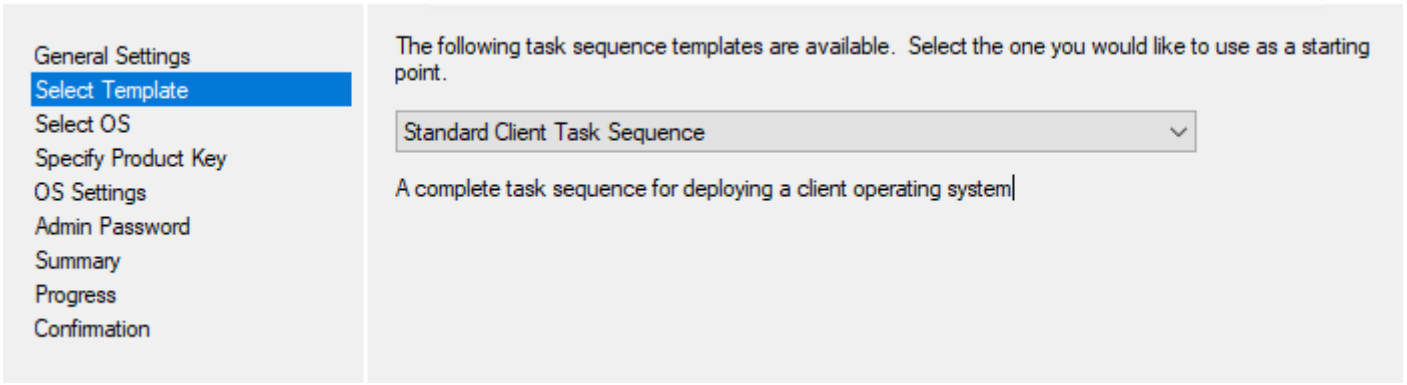


Création de la séquence de tâches

On crée ensuite une tâche.




General Settings
Select Template
Select OS
Specify Product Key
OS Settings
Admin Password
Summary
Progress
Confirmation
Specify general information about this task sequence. The task sequence ID is used internally as part of the deployment process. The task sequence name and comments are displayed by the deployment wizard.
Task sequence ID:
W10-20H2-x64
Task sequence name:
Deploy Windows 10 20H2 x64
Task sequence comments:


General Settings
Select Template
Select OS
Specify Product Key
OS Settings
Admin Password
Summary
Progress
Confirmation
The following task sequence templates are available. Select the one you would like to use as a starting point.
Standard Client Task Sequence
A complete task sequence for deploying a client operating system



Select OS

- General Settings
- Select Template
- Select OS
- Specify Product Key
- OS Settings
- Admin Password
- Summary
- Progress
- Confirmation

The following operating system images are available to be deployed with this task sequence. Select the one to use.

- Operating Systems
  - Windows 10 20H2 x64
    - Windows 10 Pro 20H2 x64

- General Settings
- Select Template
- Select OS
- Specify Product Key
- OS Settings
- Admin Password
- Summary
- Progress
- Confirmation

(●) Do not specify a product key at this time.

A product key is not required when deploying Windows 7, Windows Server 2008 R2, or later OS versions, or if the product key will be specified at deploy time using the wizard or a rule.

( ) Specify a multiple activation key (MAK key) for activating this operating system.

In order to activate, each computer deployed using this MAK key will need to contact the Microsoft activation service on the internet. This is only supported for Windows 7 and later operating systems when using volume license media.

MAK Product Key:

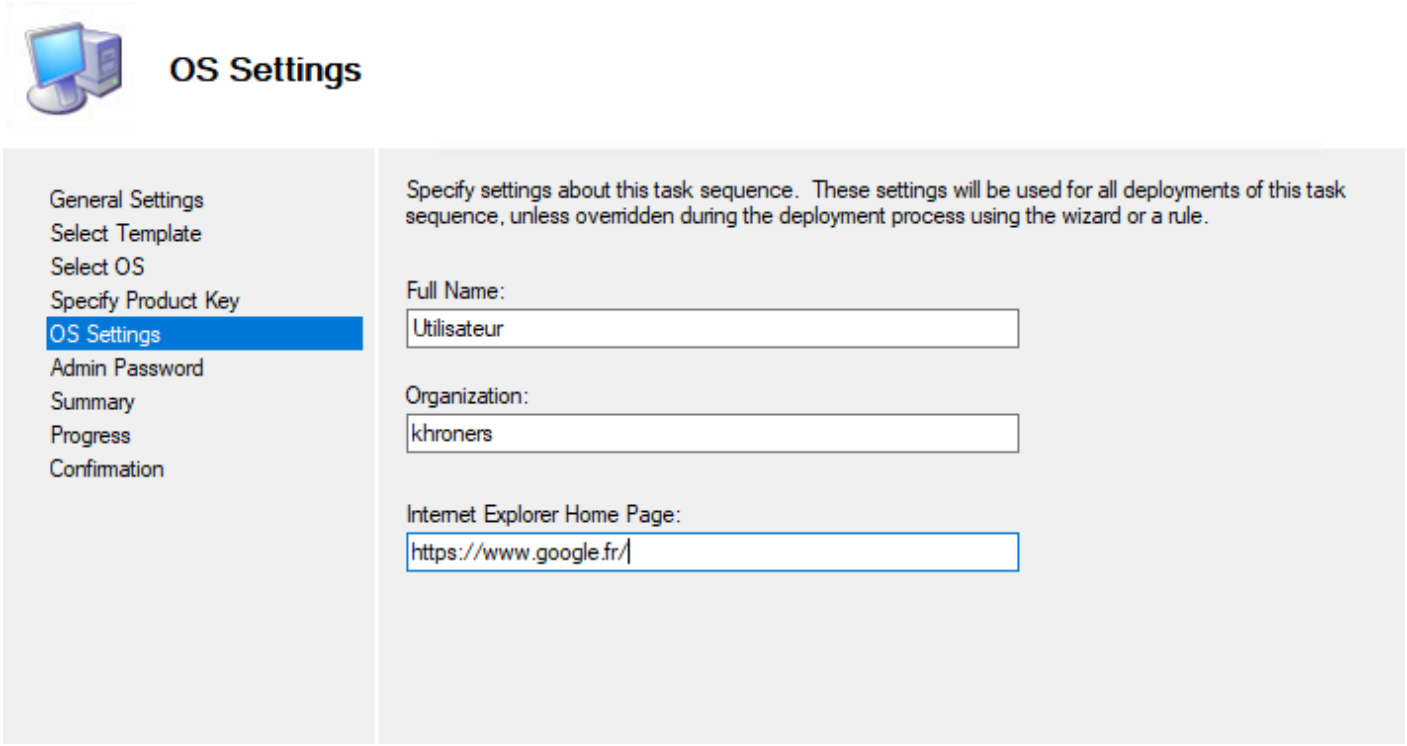
_____-_____-_____-_____-_____

( ) Specify the product key for this operating system.

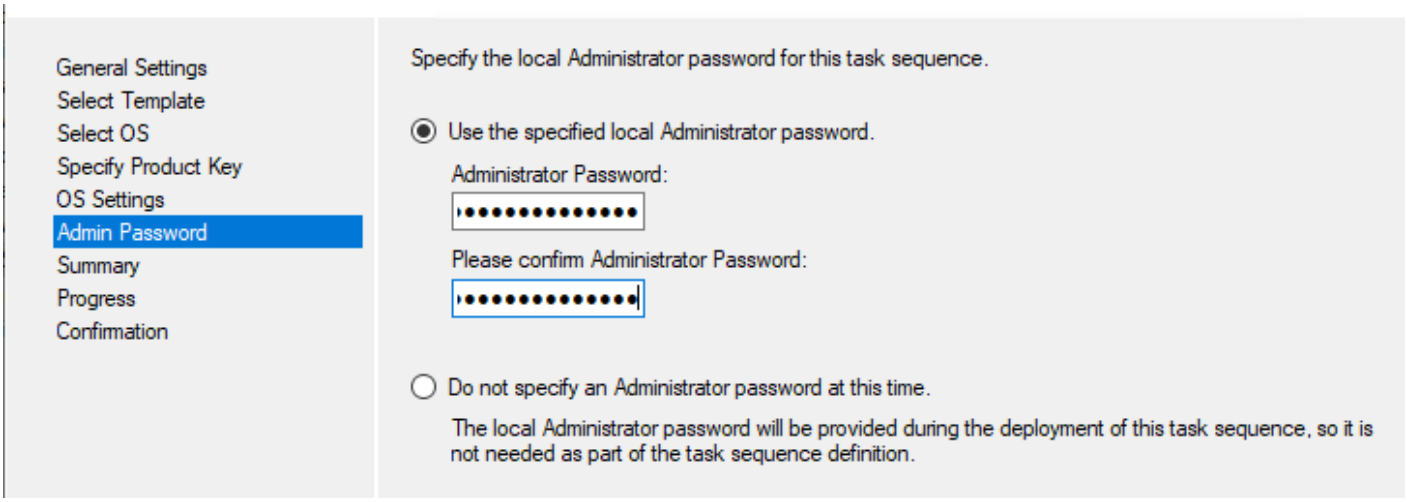
Specify a retail product key. (Note that retail keys can only be used to activate a single machine.)

Product Key:

_____-_____-_____-_____-_____

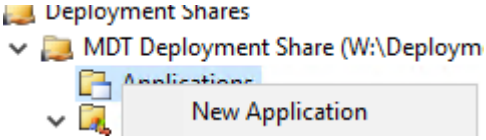


On entre un mot de passe administrateur local.



Ajouter des applications

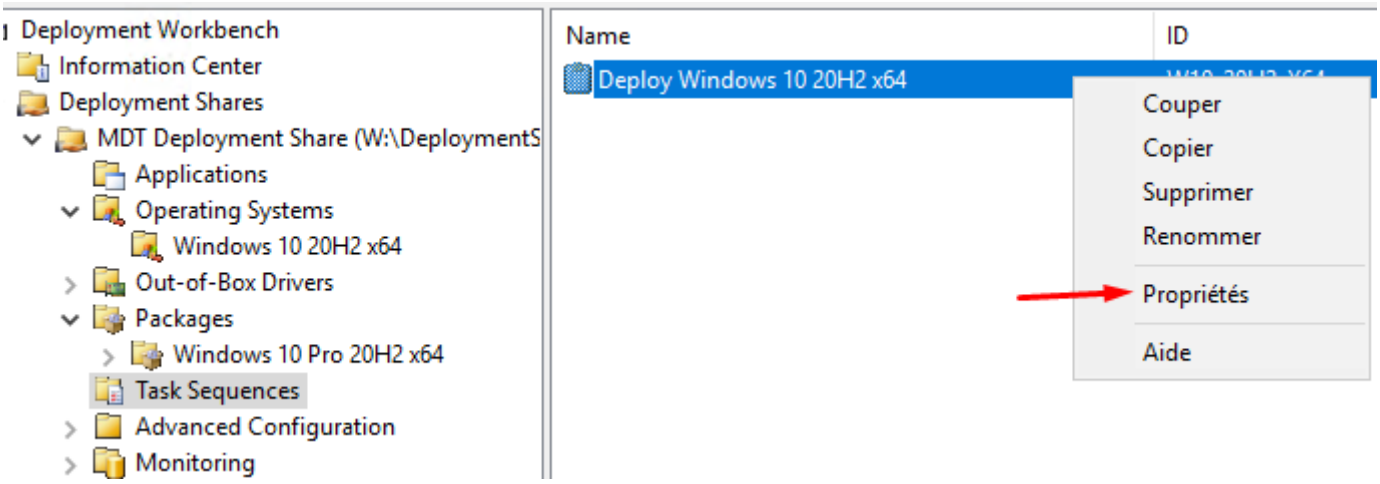
On clique droit sur Applications puis on ajoute.

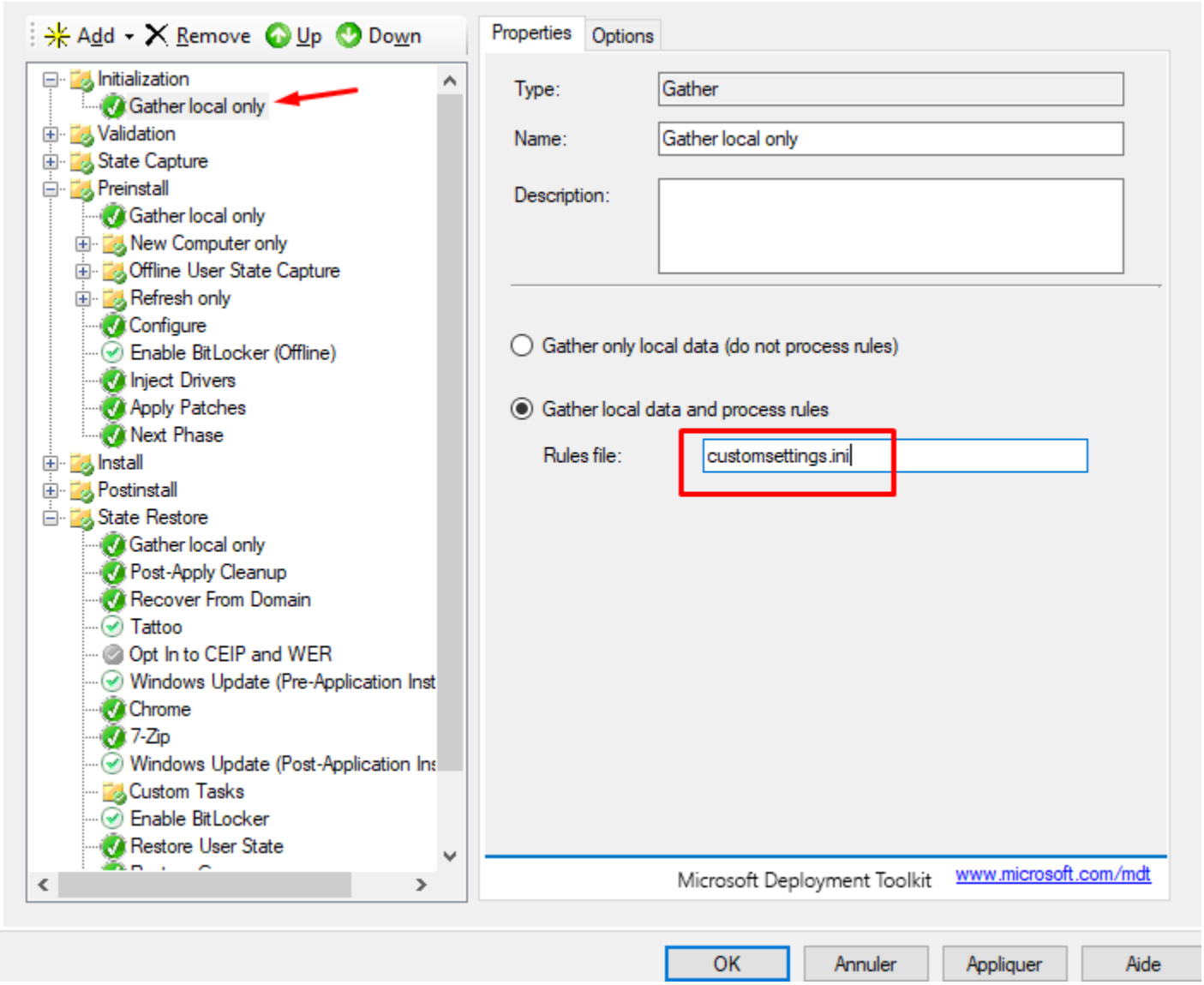


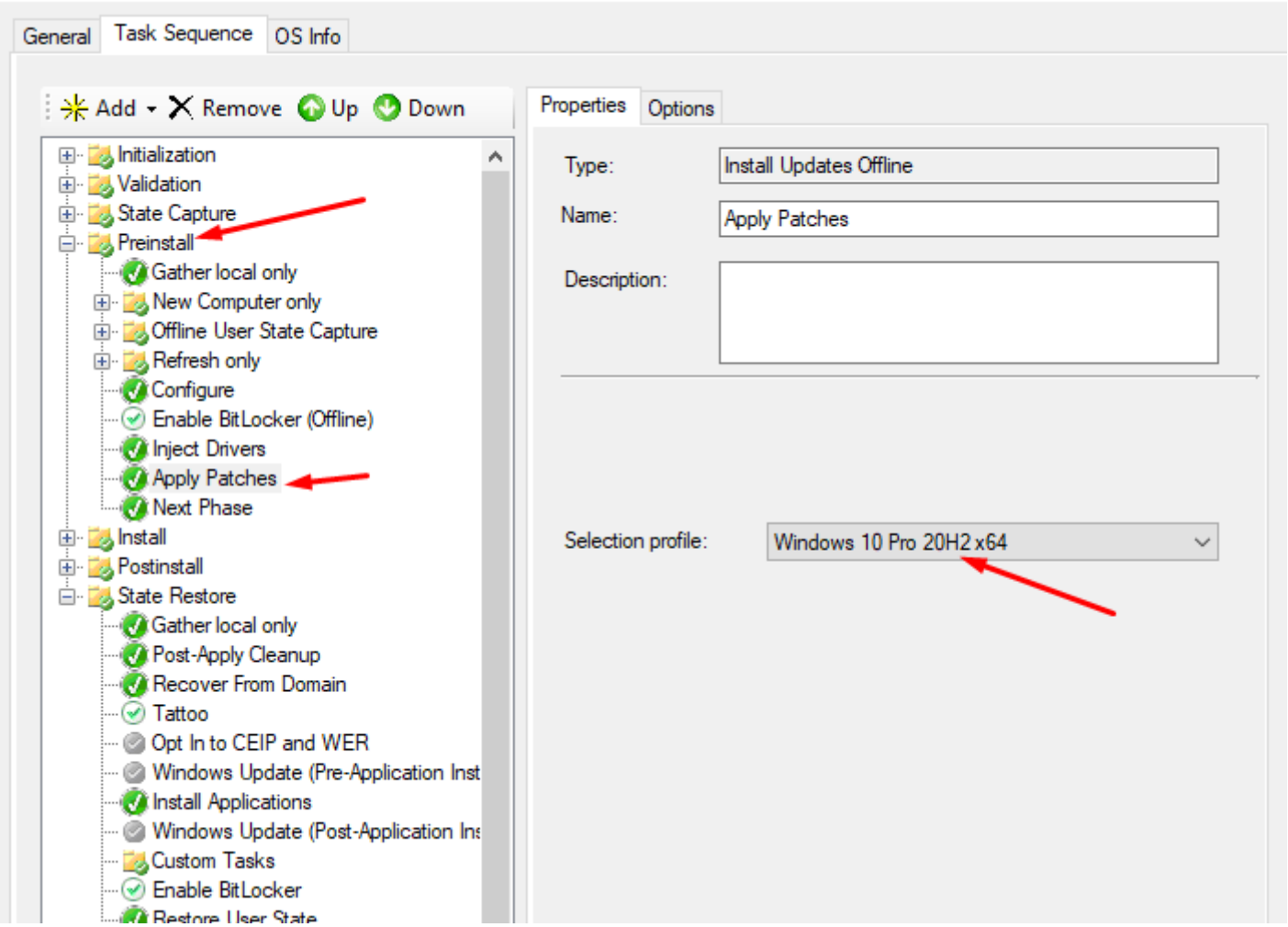
On choisit la première option, on choisit le chemin du dossier contenant le setup, la ligne de commande

```
msiexec /I googlechromestandaloneenterprise64.msi /qn
```

Edition de la séquence de tâches

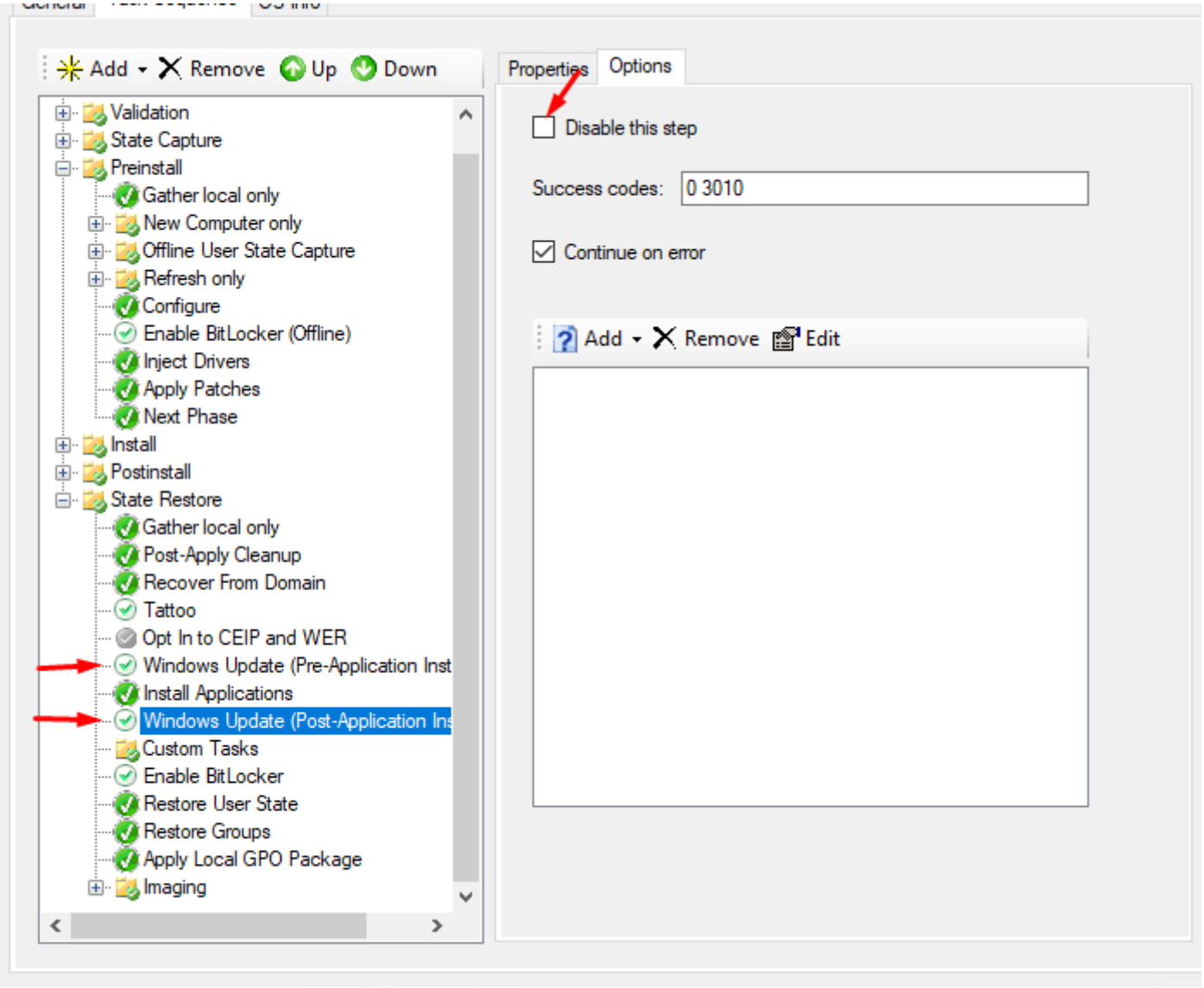




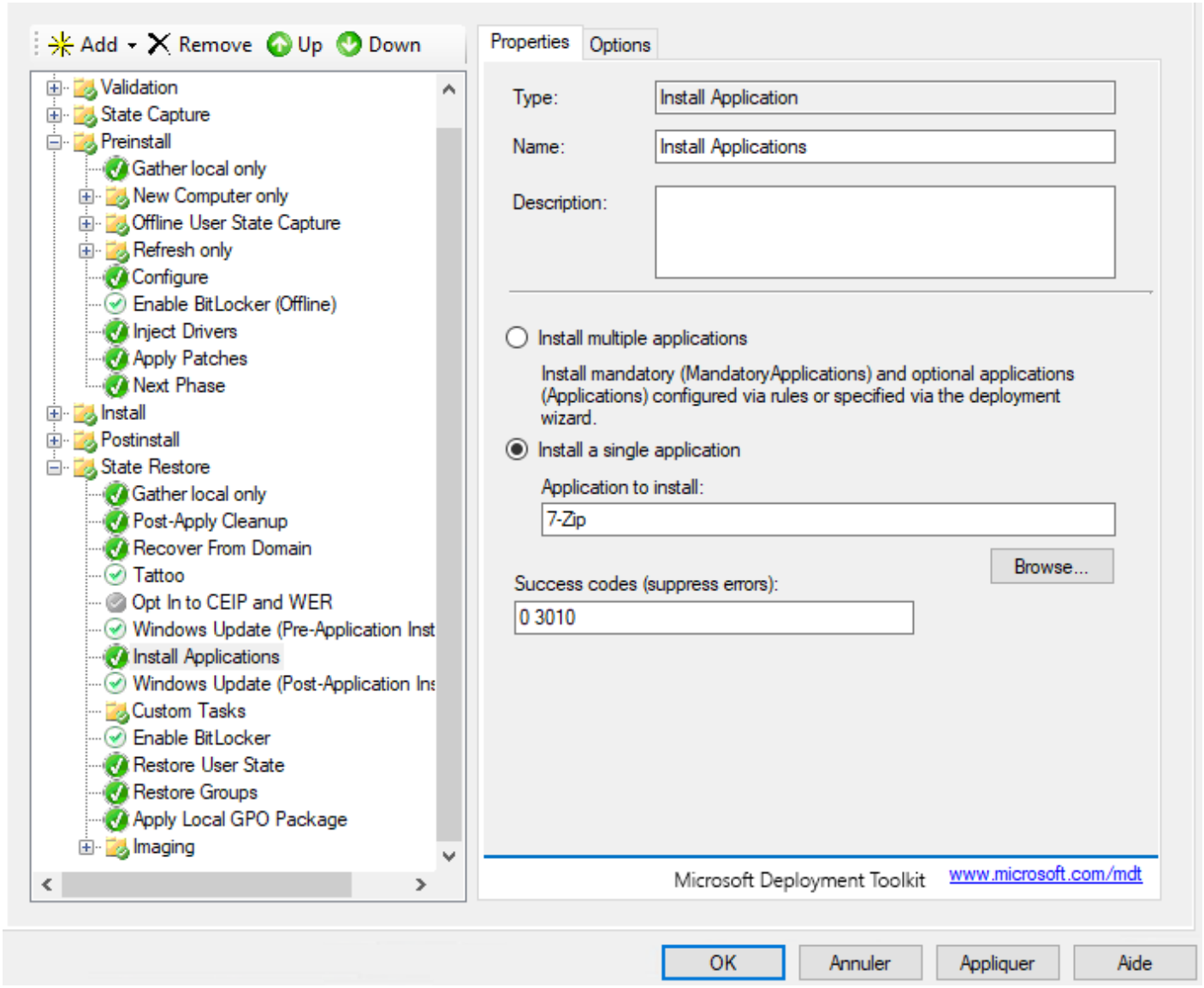


On a donc mis ici le profil de sélection pour les packages.

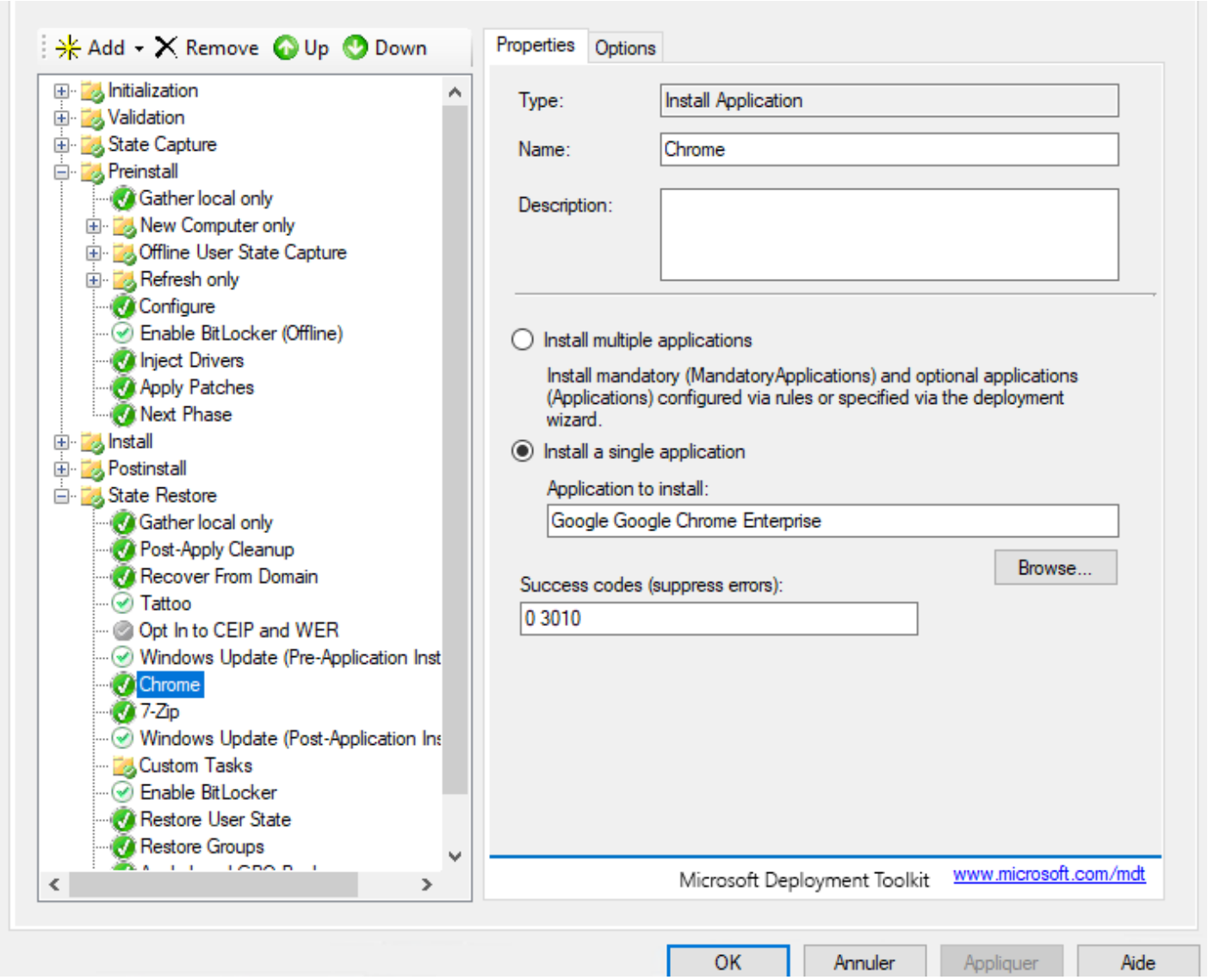
On active ces deux tâches.



On clique sur "Install Applications" et on coche la deuxième option, en renseignant l'application.



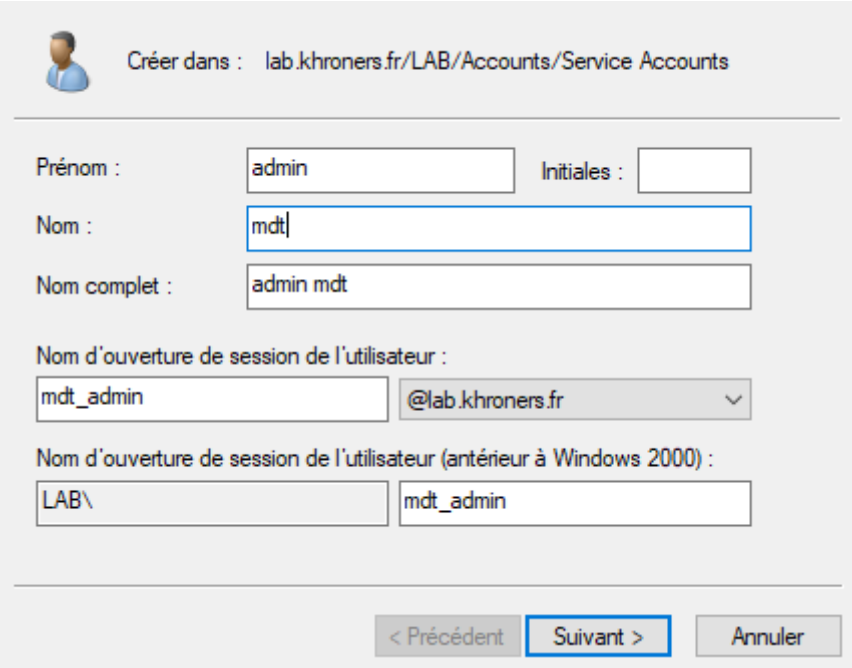
On peut ensuite copier coller pour ajouter autant d'applications que l'on veut (on les renomme).



> En laissant par défaut, le choix des applications se fait durant l'installation (cases à cocher).

Sécurisation du partage pour le déploiement

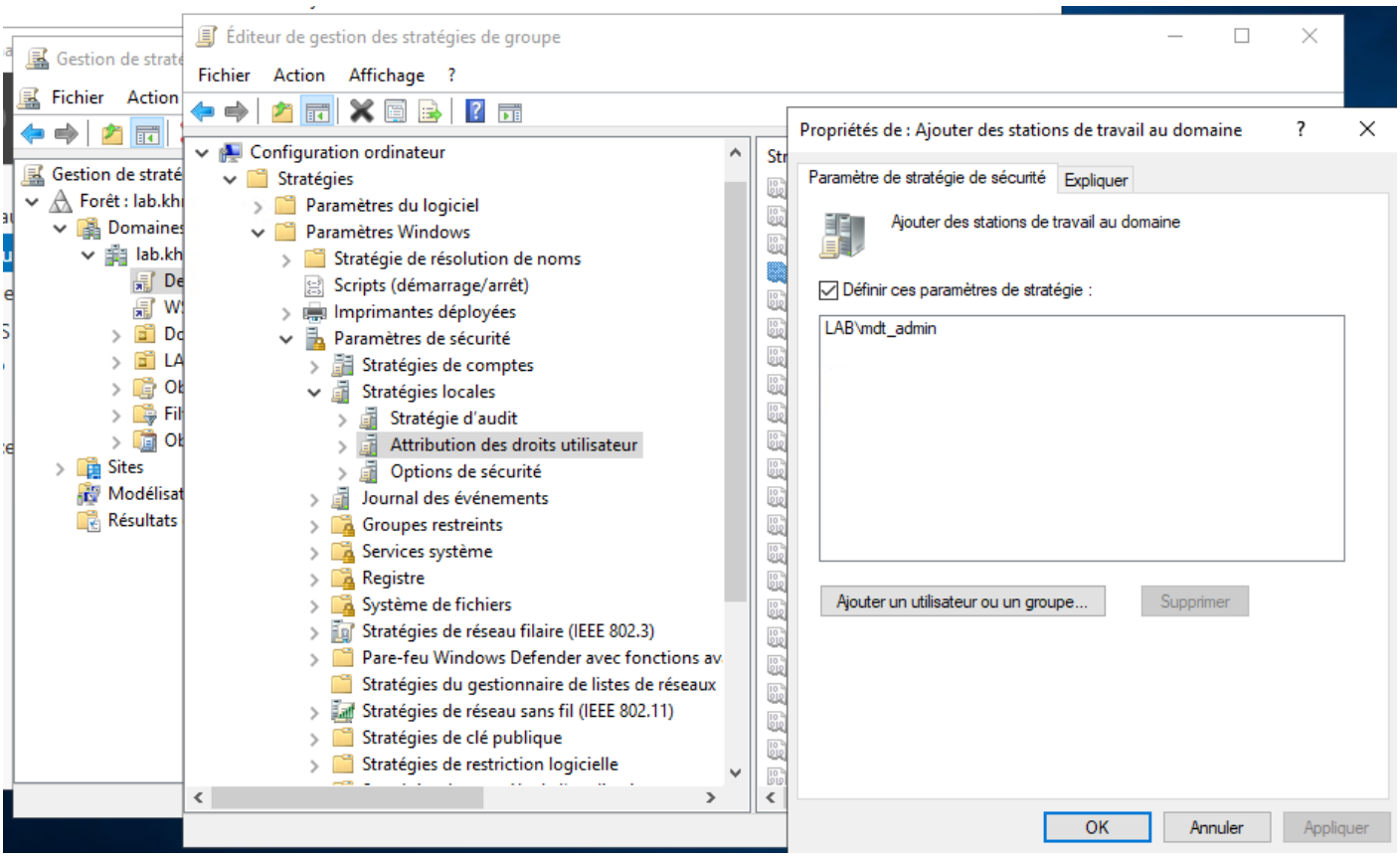
Créer un compte de service pour MDT dans l'Active Directory



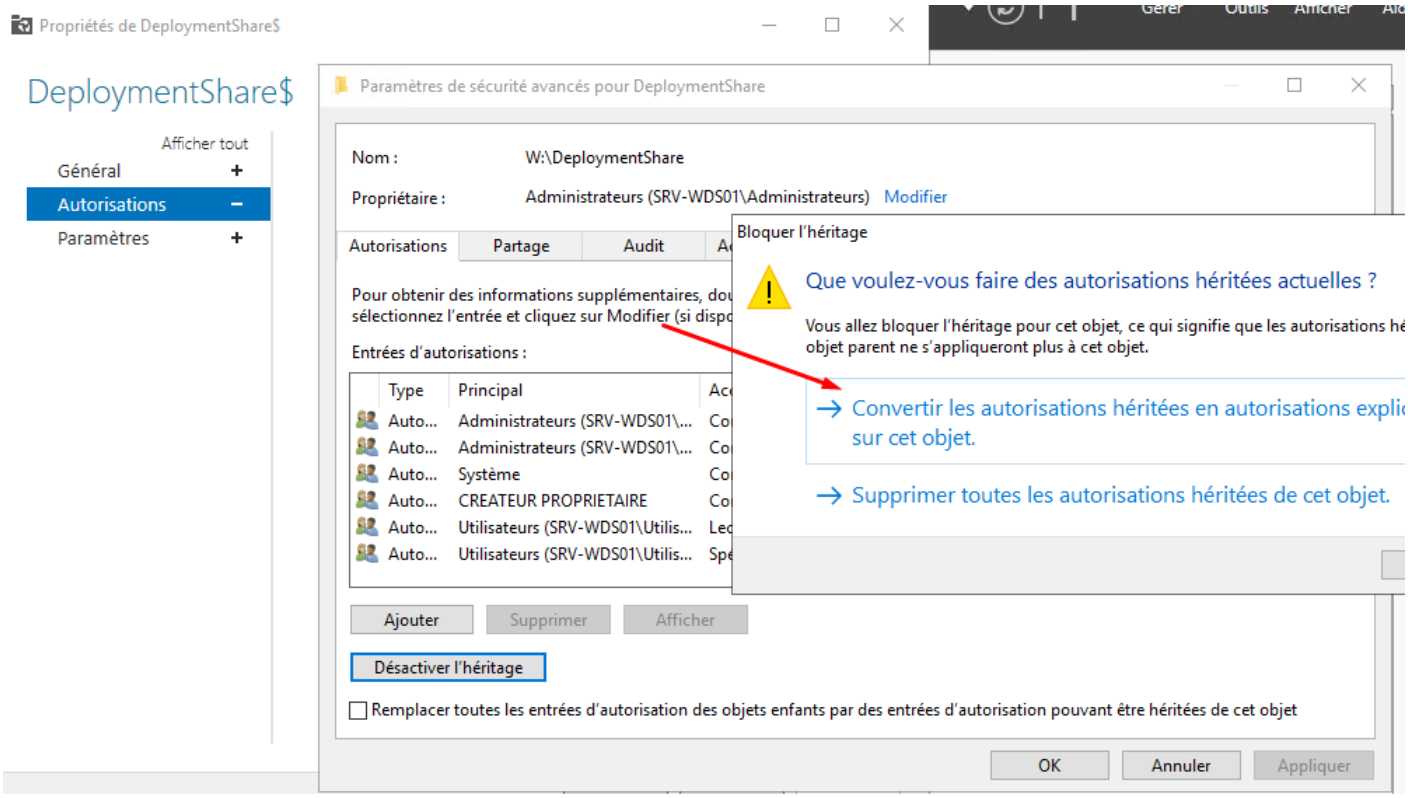
On lui attribue un mot de passe fort.

Permissions et partage

On lui donne la permission d'ajouter un ordinateur au domaine.



Sur le partage, on désactive l'héritage en convertissant les autorisations héritées.

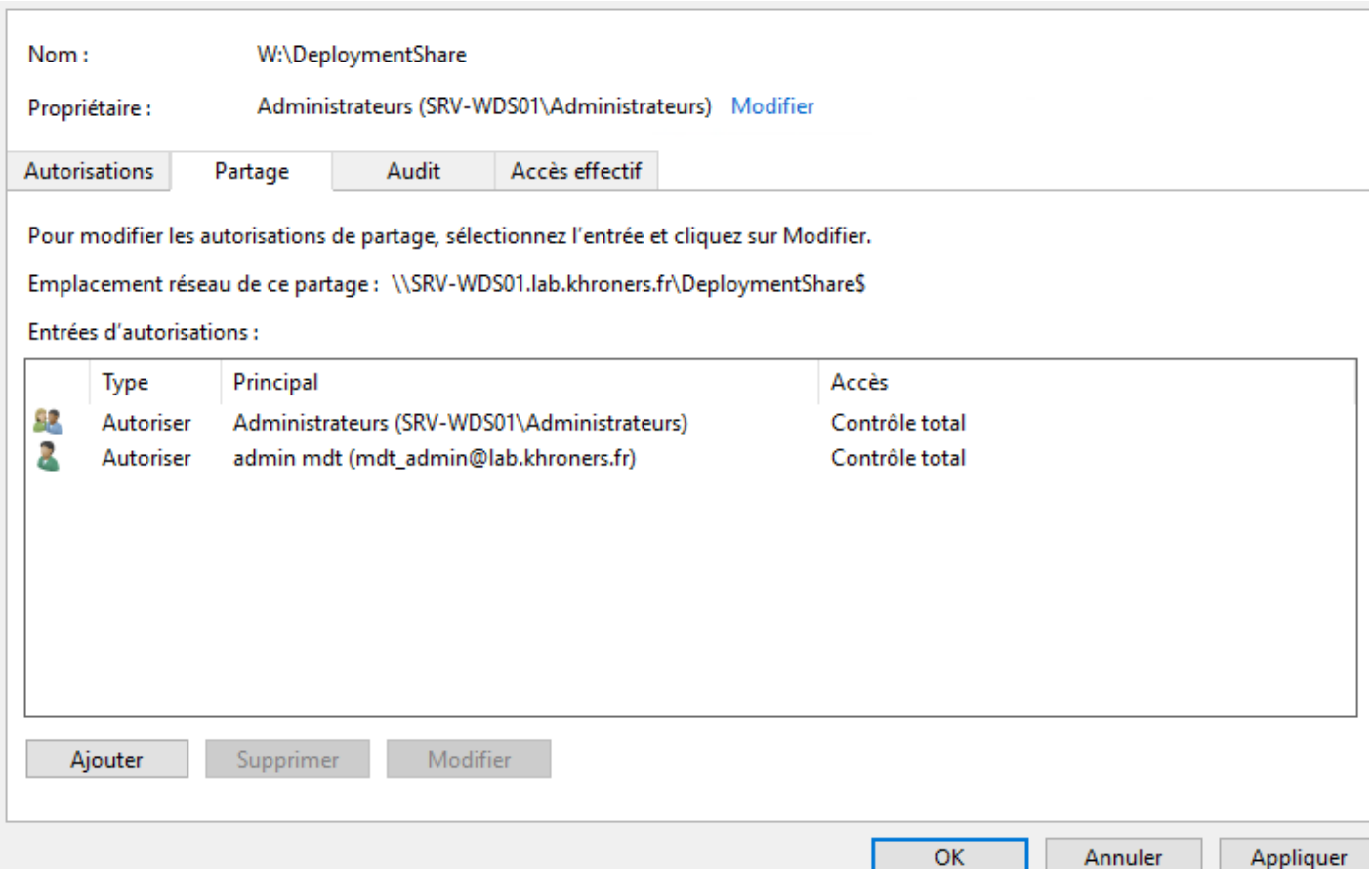


Autorisations | Partage | Audit | Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

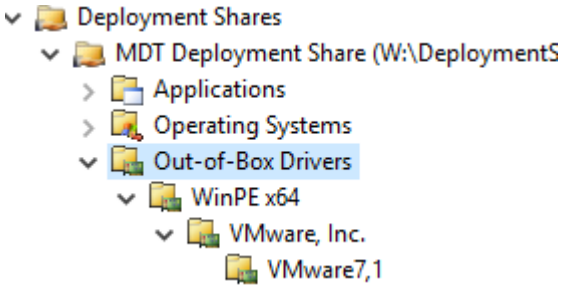
Entrées d'autorisations :

Type	Principal	Accès	Hérité de	S'applique à
Auto...	Administrateurs (SRV-WDS01\...	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers...
Auto...	admin mdt (mdt_admin@lab....	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...



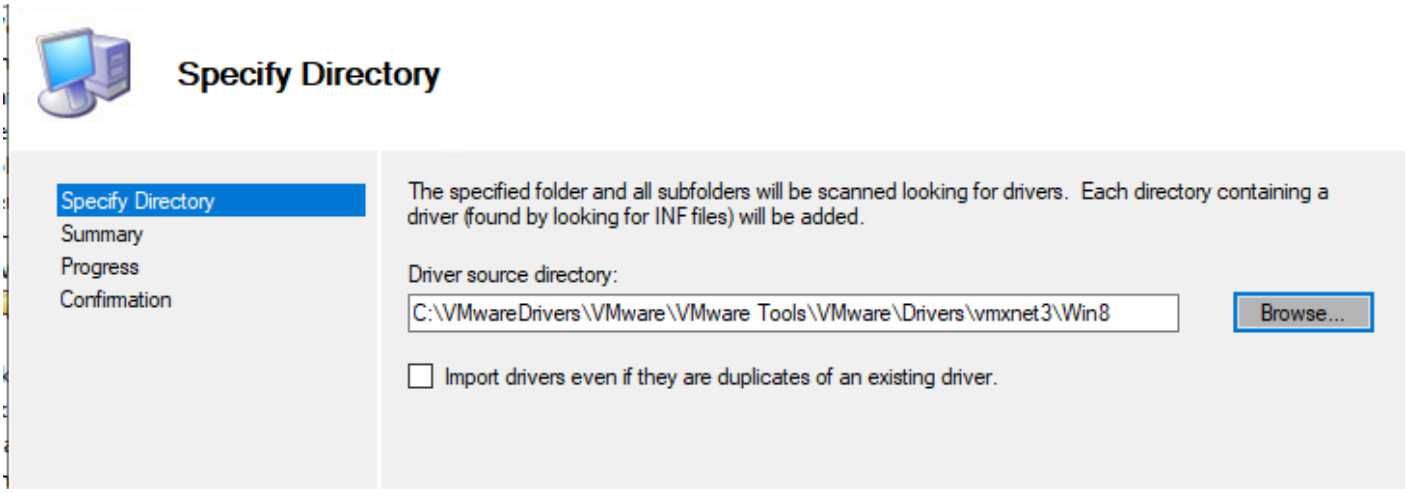
Ajouter un pilote dès le démarrage PXE

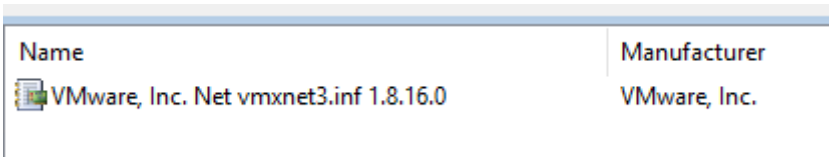
On créer les dossiers.



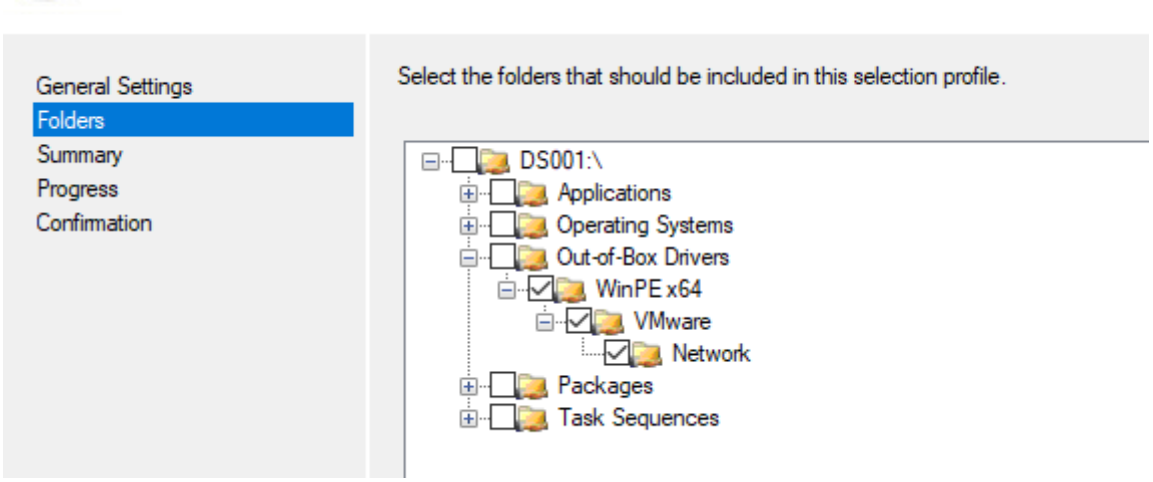
Ici, VMware, Inc. correspond au manufacturer (requête WMI, %Make%) et VMware7,1 au modèle (requête WMI, %Model%).

On clique droit sur "Network" (nom défini selon le pilote, ici on ajoute un pilote réseau) et on importe.

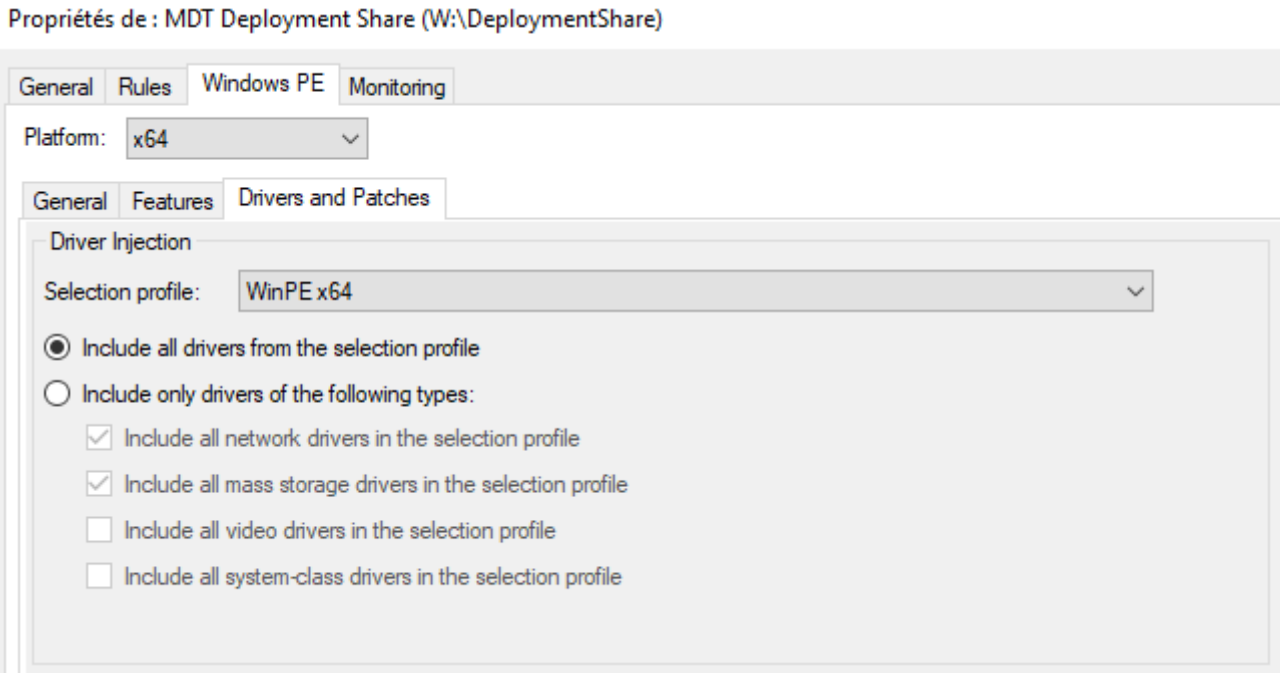




On crée un profil de sélection. (nommé WinPE x64)



Ensuite, clic droit sur le partage de déploiement, propriétés, puis on vérifie :



Ajouter les pilotes VMware Tools

Il suffit de créer une application comme pour 7zip ou Chrome. Il faut créer un dossier VMware Tools, y copier le contenu de l'iso à l'intérieur, puis créer l'application et choisir le dossier en source.

Pour la ligne de commandes :

```
setup64.exe /S /v /qn REBOOT=R
```

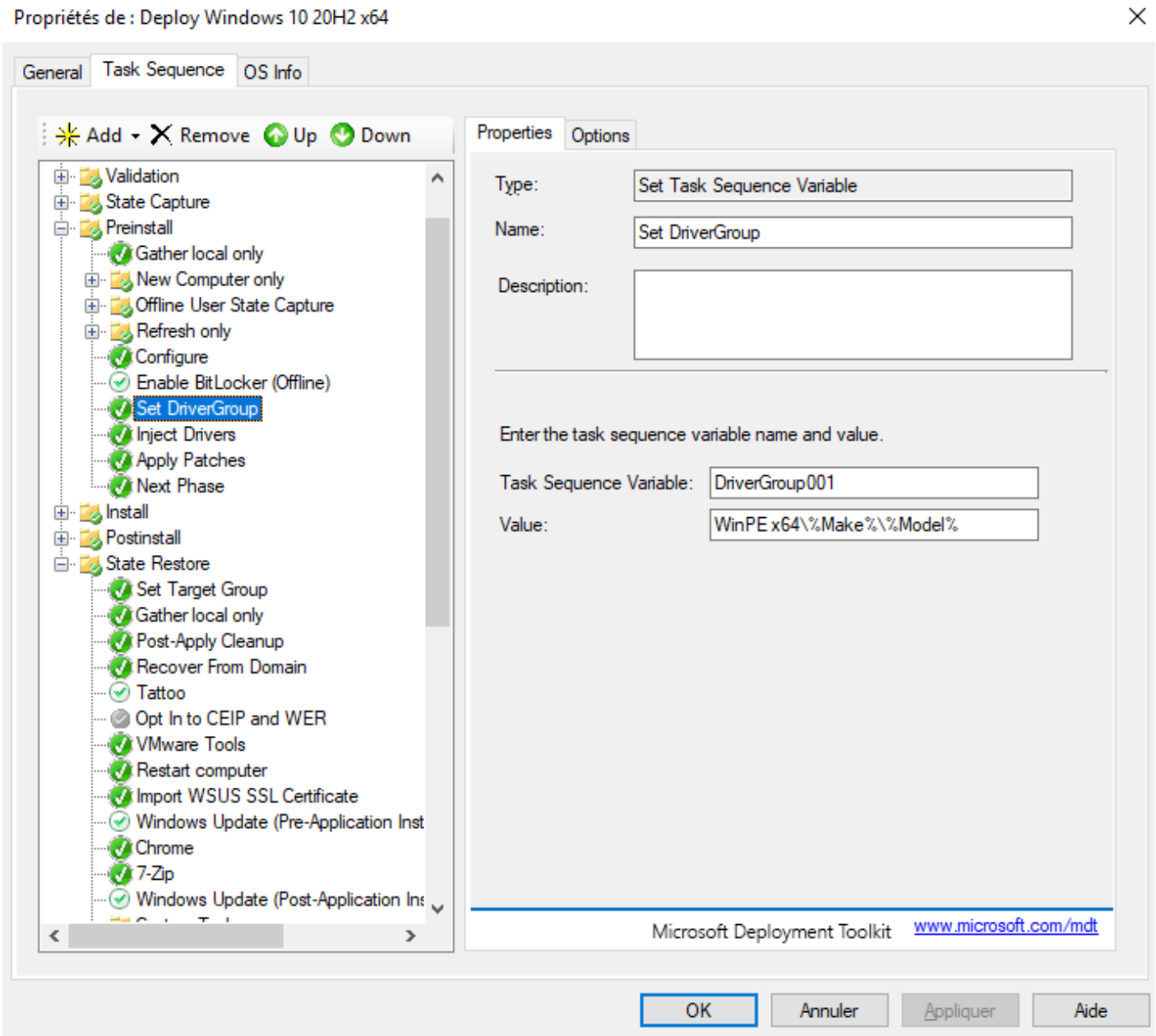
On rajoute une tâche après l'installation de VMware Tools : Restart Computer.

Ajouter d'autres pilotes

Pour installer d'autres pilotes, il est recommandé de créer des sous dossiers dans Windows 10 x64.

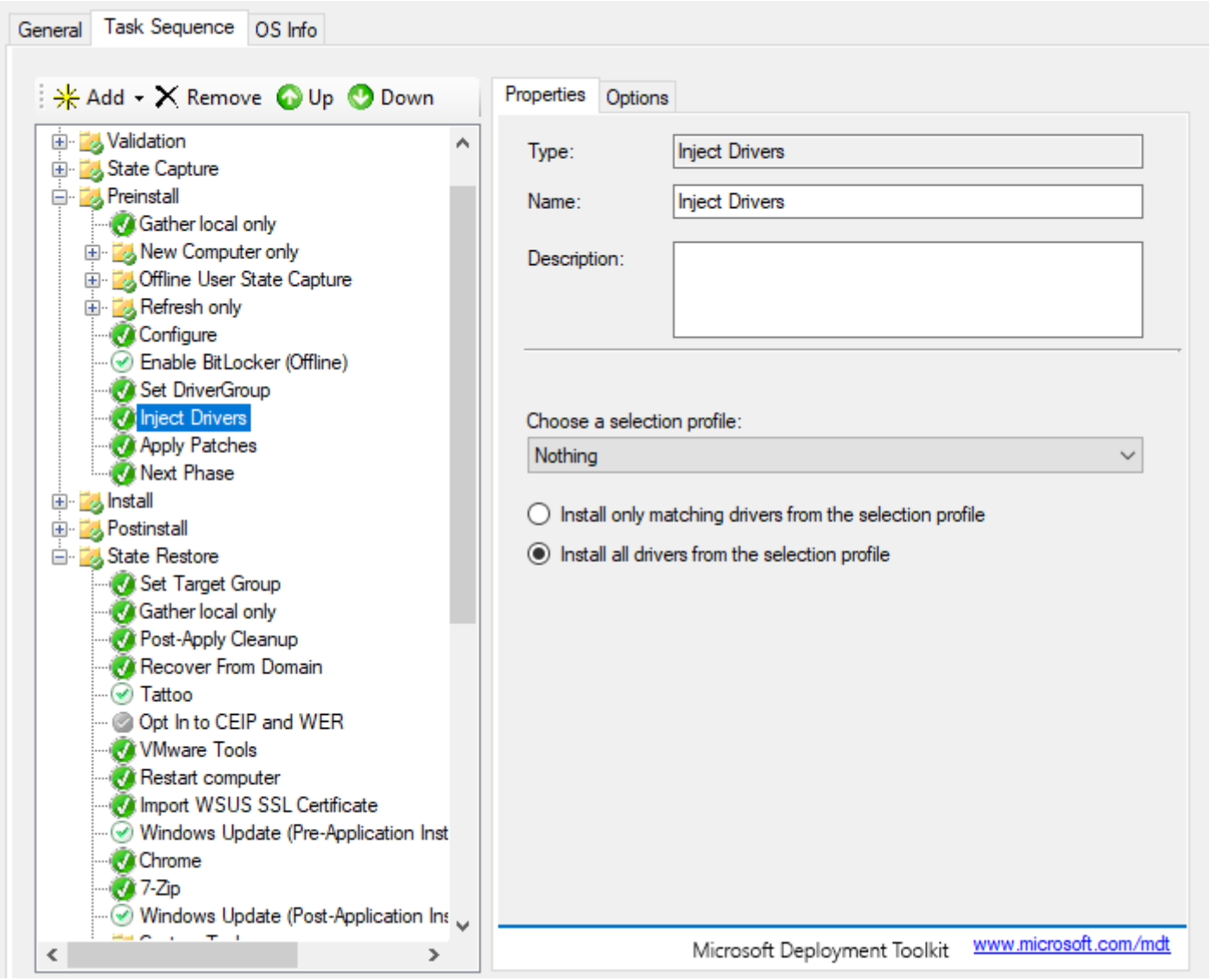
On crée d'abord un dossier pour la marque, et ensuite le modèle.

On ajoute ensuite un tâche qui va affecter une valeur à une variable. Cette valeur est "DriverGroup001".



> %Make% correspond au manufacturer (marque, comme Dell, HP, VMware, Lenovo, etc...
> %Model% correspond au modèle.

On définit le profil de sélection pour "Nothing" dans Inject Drivers.



Exemple pour chaque fichier .ini

Bootstrap.ini :

```
[Settings]
Priority=Default

[Default]
DeployRoot=\\SRV-WDS01\DeploymentShare$
UserDomain=lab.khroners.fr
UserID=mdt_admin
UserPassword=mdt_admin-password
SkipBDDWelcome=YES
```

Customsettings.ini :

```
[Settings]
Priority=Init, Model, Default, SetOSD
Properties=OSDPrefix, ComputerSerialNumber, TargetGroup

[Init]
ComputerSerialNumber=#Right(Replace(Replace(oEnvironment.Item("SerialNumber")," ",""),"-
","",6)#

[Default]
OSInstall=Y

;Computer Details
SkipComputerName=YES
SkipDomainMembership=YES
JoinDomain=lab.khroners.fr
DomainAdmin=mdt_admin
DomainAdminDomain=lab.khroners.fr
DomainAdminPassword=mdt_admin-password
MachineObjectOU=OU=Workstations,OU=Computers,OU=LAB,DC=lab,DC=khroners,DC=fr

;Skip Task Sequence
SkipTaskSequence=YES
TaskSequenceID=W10-20H2-X64

;User Data
SkipUserData=YES

;Computer Backup
SkipComputerBackup=YES

;Product Key
SkipProductKey=YES

;Language Packs
SkipPackageDisplay=YES

;Locale and Time
SkipLocaleSelection=YES
```

```
SkipTimeZone=YES
KeyboardLocale=040c:0000040c
KeyboardLocalePE=040c:0000040c
UserLocale=fr-FR
UILanguage=fr-FR
TimeZoneName=Romance Standard Time

;Roles and Features
SkipRoles=YES

;Applications
SkipApplications=NO

;Administrator Password
SkipAdminPassword=YES
AdminPassword=local-admin-password

;Local Administrators
SkipAdminAccounts=YES

;Capture Image
SkipCapture=YES

;Bitlocker
SkipBitLocker=YES

;Ready to begin
SkipSummary=YES

;Operating system deployment completed successfully
SkipFinalSummary=YES

FinishAction=SHUTDOWN
WSUSServer=https://srv-wsus01.lab.khroners.fr:8531
SLShare=\\SRV-WDS01\DeploymentShare$\Logs
EventService=http://SRV-WDS01:9800
OSDComputerName=%OSDPrefix%-%ComputerSerialNumber%

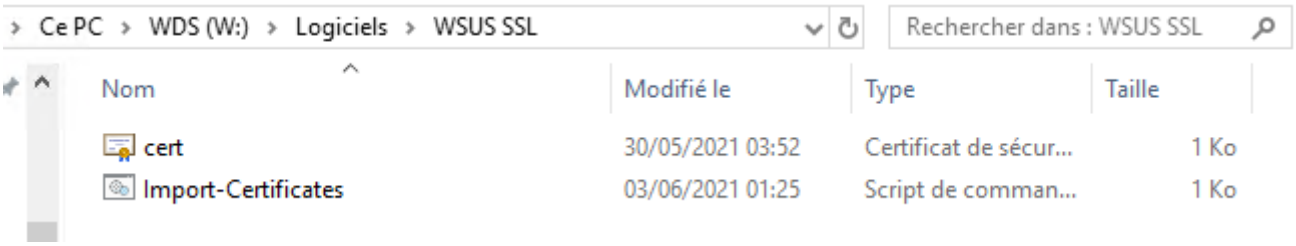
[VMware7,1]
```

```
OSDPrefix=VM
```

Déploiement MDT avec WSUS SSL

Suite à mon guide pour le WSUS en SSL, il faut avoir le certificat sur le poste pour rechercher des mises à jour. Pour cela, on le fait habituellement en GPO. Cependant, ces stratégies ne sont pas appliquées durant le déploiement. On va donc les importer.

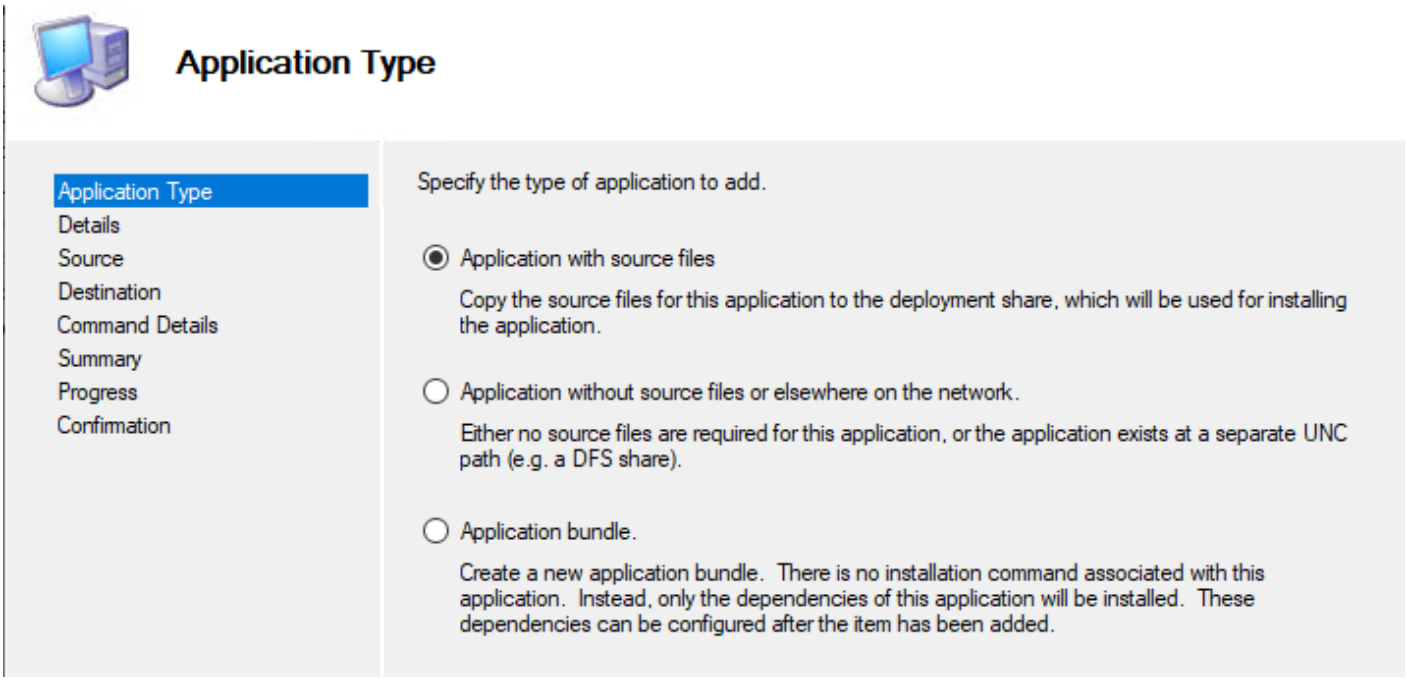
Pour cela, il faut créer un dossier sur le serveur MDT (pas dans le partage), avec le certificat (en .cer) et un fichier de commandes .cmd. Je vais créer ce dossier dans W:\Logiciels\.

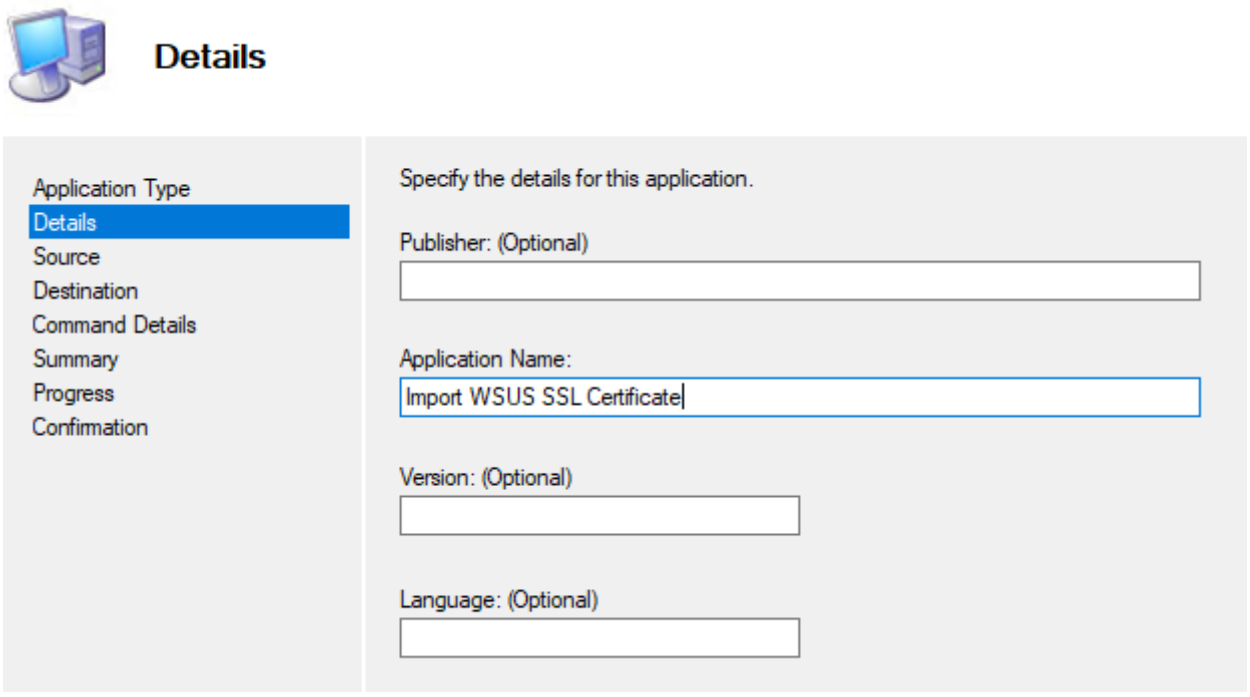


Le contenu du fichier Import-Certificates :

```
certutil -addstore -f  "Root" "cert.cer"
certutil -addstore -f "TrustedPublisher" "cert.cer"
```

On ajoute ensuite ce dossier en créant une application comme pour Google Chrome & 7Zip. En source, on choisit le dossier.

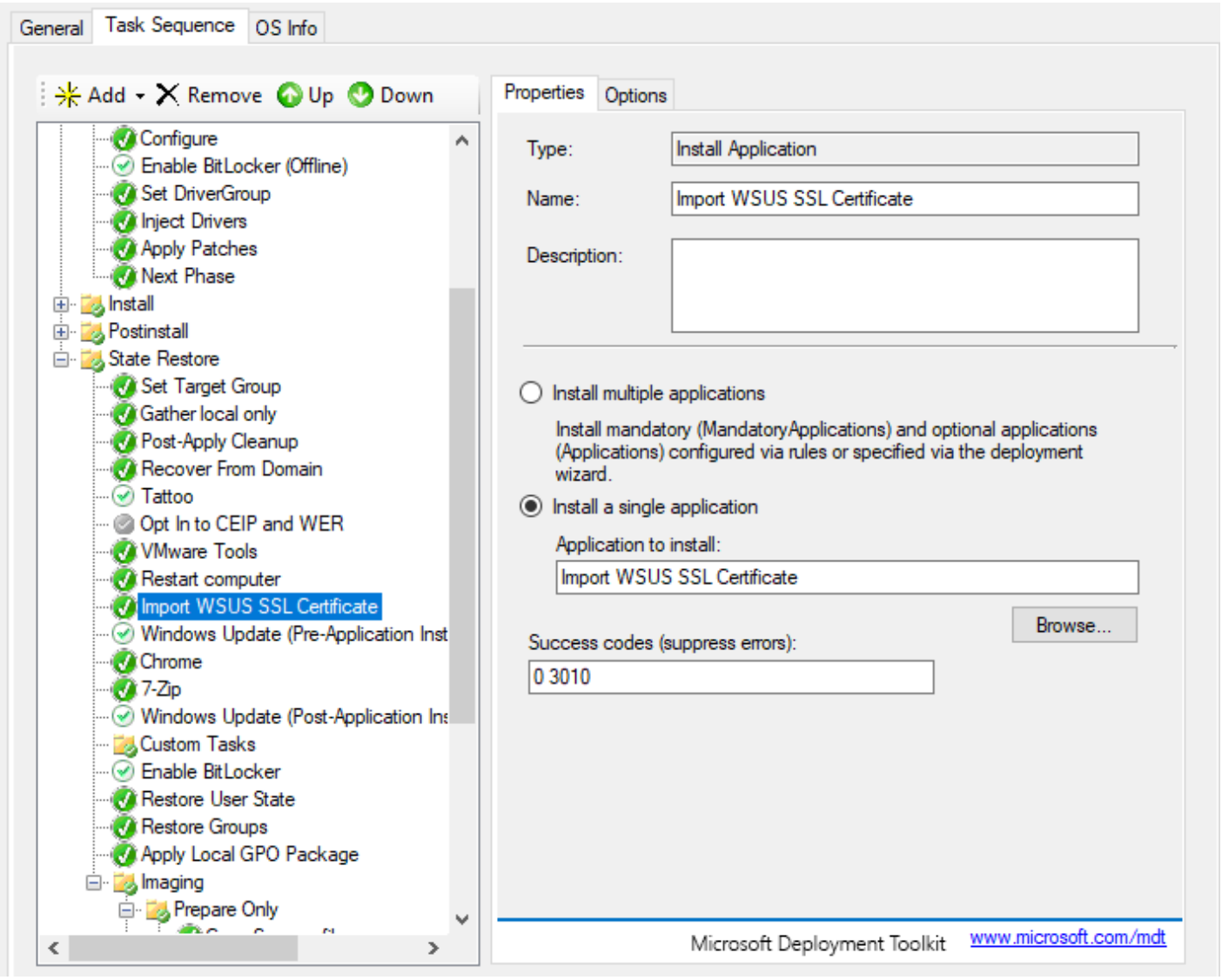




Pour la commande, on rentre le nom du fichier, c'est à dire : Import-Certificates.cmd

On ajoute ensuite une tâche dans la Task Sequence. (Pour cela, je copie colle "Chrome" par exemple, et on modifie le nom et l'application à installer)

> Faites en sorte de l'installer avant la tâche Windows Update. Dans mon cas, après VMware Tools.

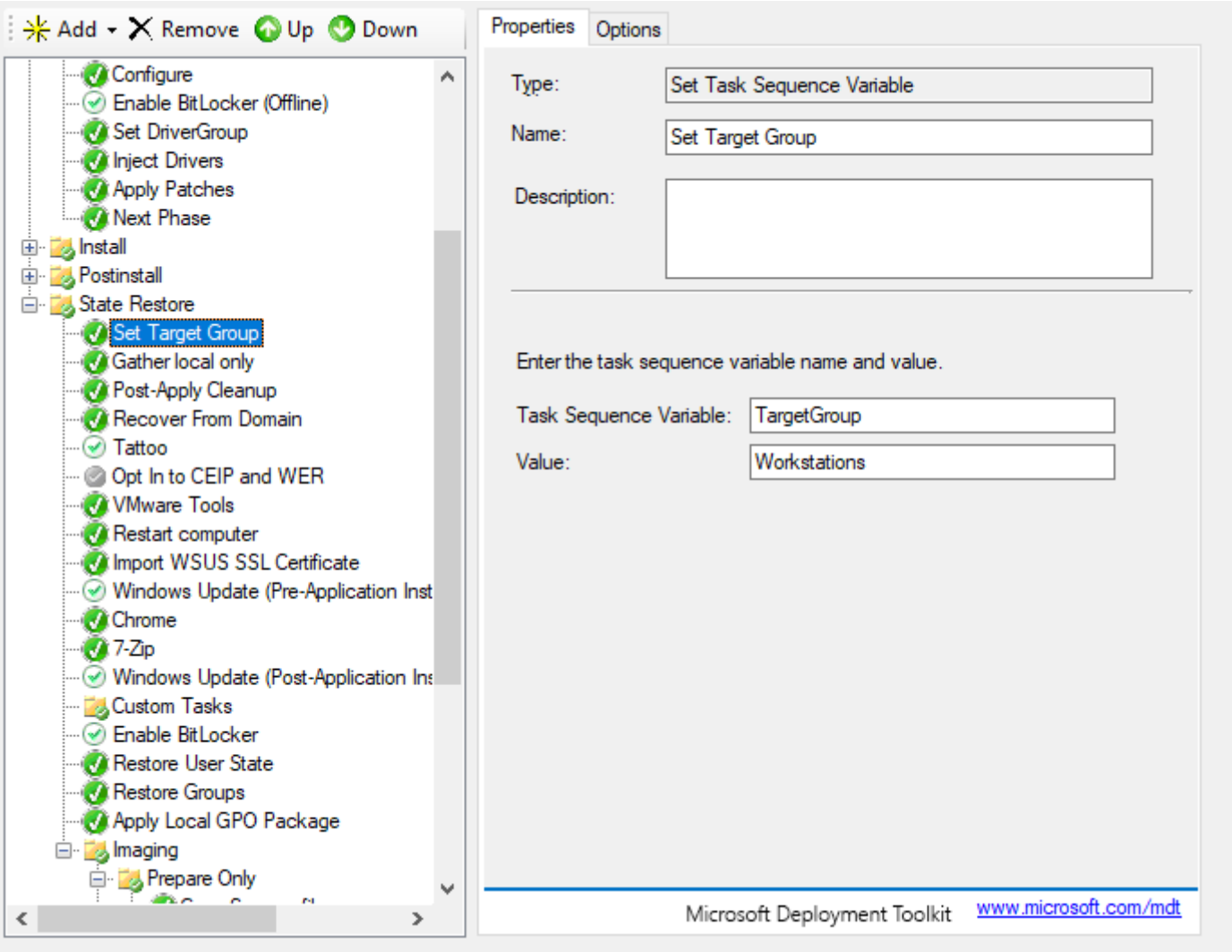


On modifie également la ligne dans le fichier customsettings.ini pour ajouter le https et le port.

> **Attention :** Il faut mettre le FQDN.

Ciblage côté client pour WSUS

Pour activer le ciblage pour le WSUS, on rajoute une tâche.



Activation du monitoring (supervision)

Dans les propriétés du partage du déploiement, on active le monitoring dans l'onglet "monitoring".

En se rendant sur cette URL, on devrait arriver sur la page.

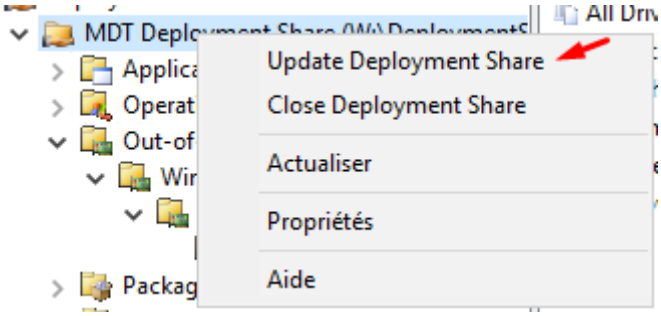
http//localhost:9800/MDTMonitorEvent/

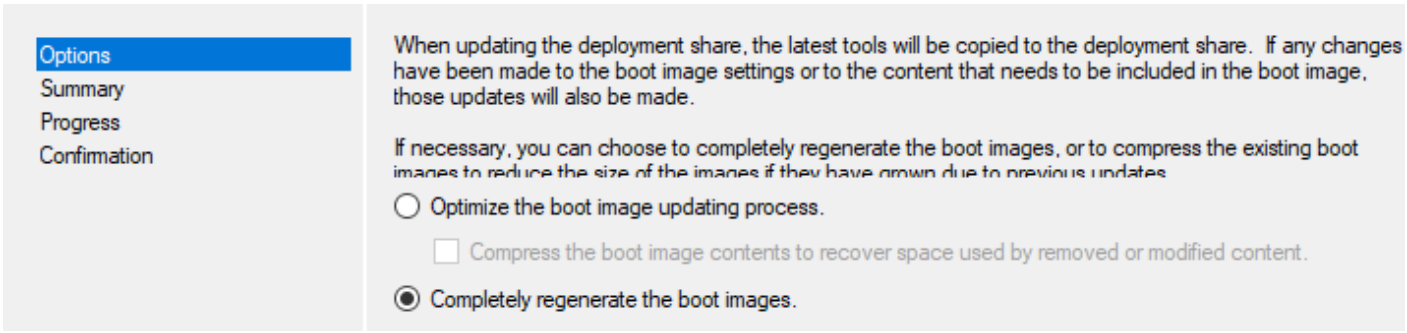
On ajoute ensuite dans le fichier customsettings.ini la ligne :

```
EventService=http://SRV-WDS01:9800
```

Génération de l'image

On clique droit sur le partage de déploiement et "Update..."

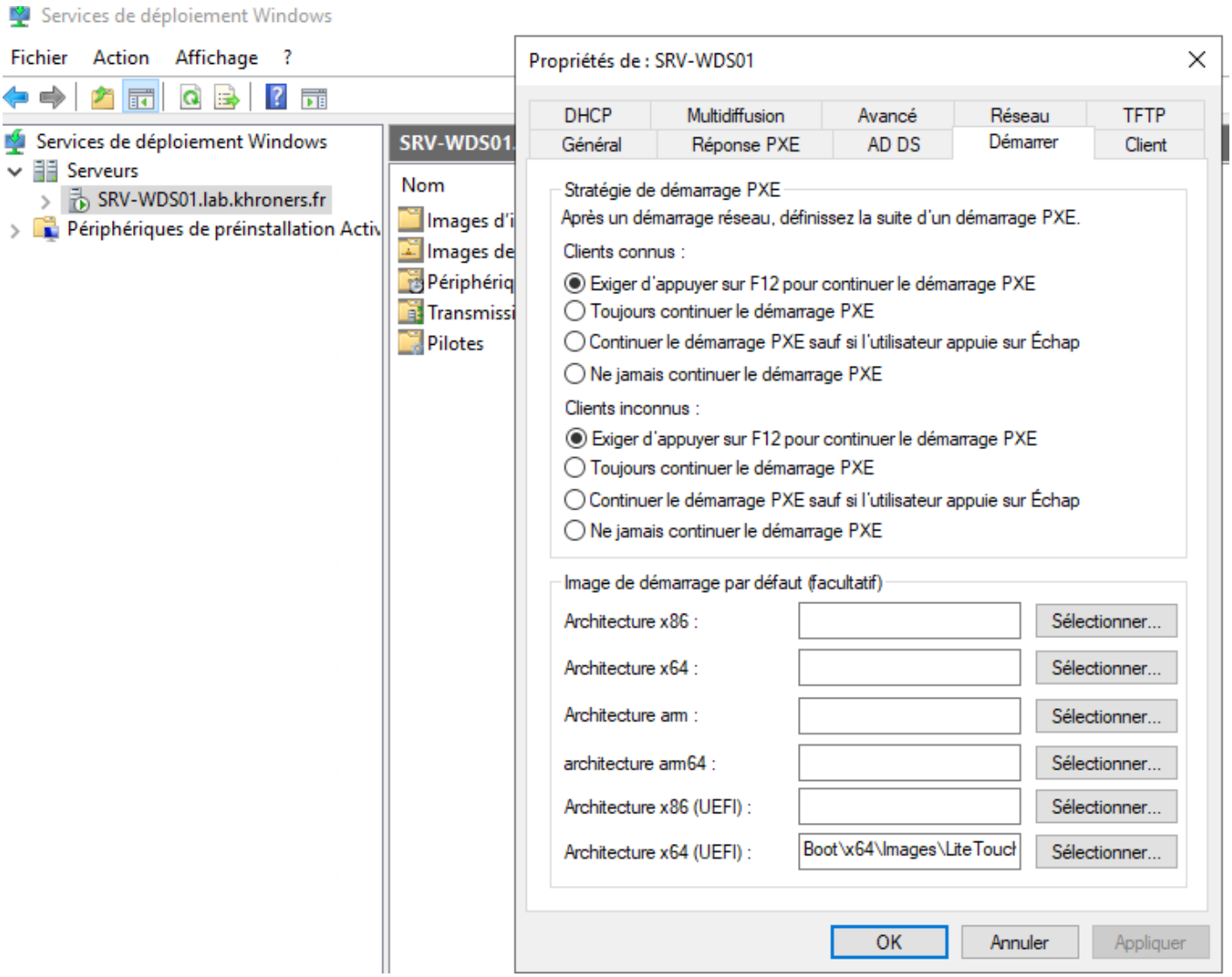




Ajout de l'image dans WDS

On ajoute l'image LiteTouchPE_x64.wim situé sur le partage dans le dossier boot dans Images de démarrage.

Dans les propriétés, on rajoute l'image.



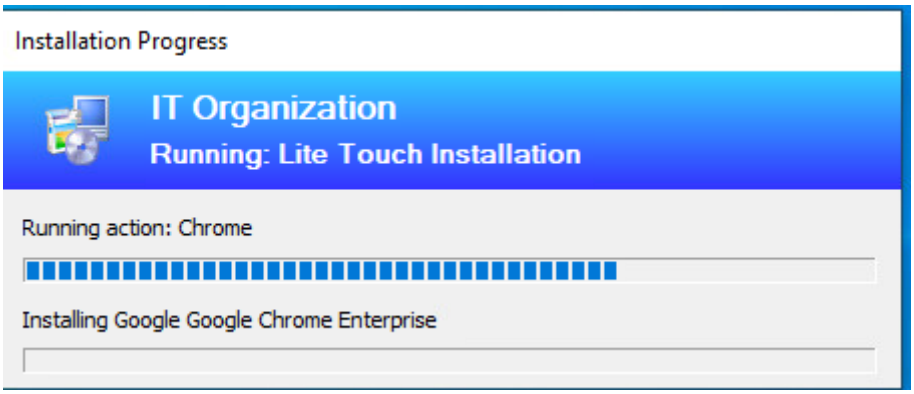
On clique droit sur le serveur, toutes les tâches puis redémarrer.

Tests



On pourra automatiser le choix de la séquence de tâches en ajoutant SkipTaskSequence=YES et TaskSequenceId=l'ID_de_notre_sequence_de_taches (dans mon cas, W10-20H2-X64).

Une fois l'installation faite :



Les applications rajoutées précédemment s'installent.

Déploiement inter-sites

Il est possible de répliquer un MDT sur différents sites.

Pour cela, il sera nécessaire de procéder à une réplication DFS ainsi que de modifier le fichier ini (customsettings).

Revision #17
Created 2021-05-06 15:08:44 UTC by Khroners
Updated 2022-11-01 11:00:58 UTC by Khroners