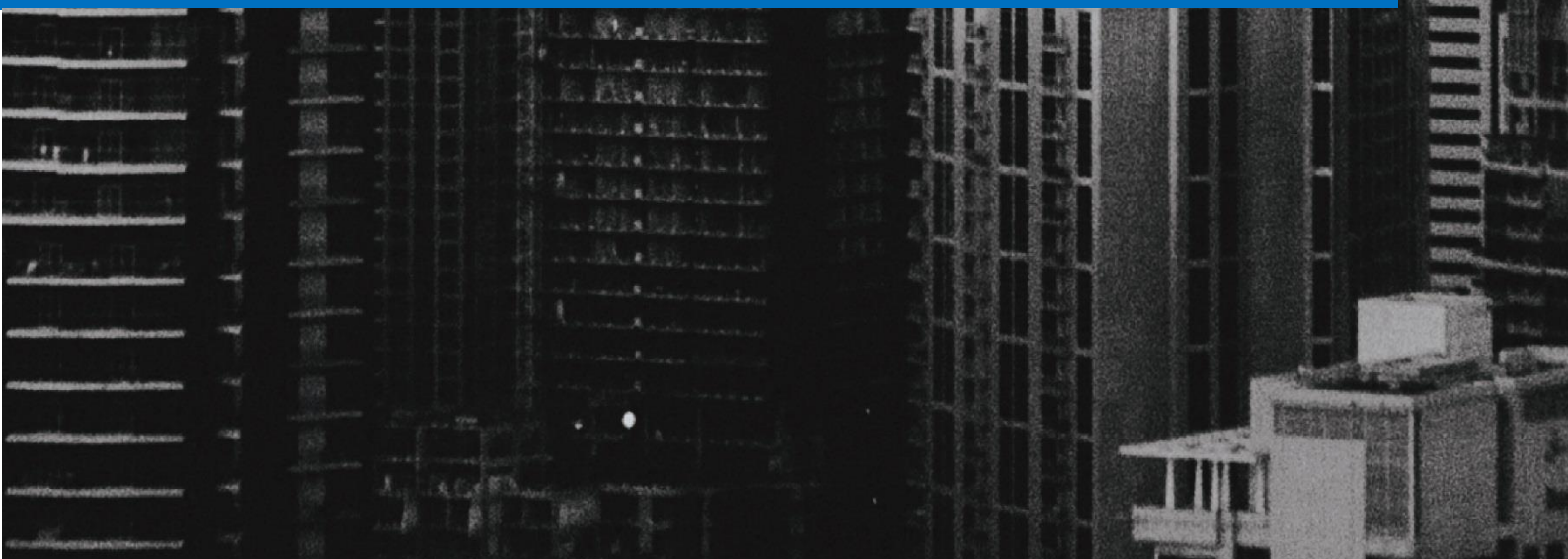
Procédure d'installation

Déploiement ASSURMER

ASSURMER

Montpellier, Occitanie, France

Kévin Boulier, Ezequiel-Junior Varela Montieiro, Maxence Martin-Parent / SISR 1B



Métadonnées

Version	Nom	Commentaires	Dernière modification	Destinataires	Diffusion du document
0.1	Maxence MARTIN-PARENT	Rédaction introduction	30/12/2023	DSI	Interne
0.2	Maxence MARTIN-PARENT	Rédaction étape 1	02/01/2024	DSI	Interne
0.3	Maxence MARTIN-PARENT	Rédaction étape 4	02/01/2024	DSI	Interne
0.4	Kevin BOULIER	Rédaction étape 3	07/01/2024	DSI	Interne
0.5	Maxence MARTIN-PARENT	Aide à la correction étape 3	07/01/2024	DSI	Interne
0.6	Ezequiel-Junior VARELA-MONTEIRO	Rédaction étape 2	07/01/2024	DSI	Interne
1	TOUS	Correction finale	07/01/2024	DSI	Interne

Table des matières

Introduction

Introduction de la procédure d'installation

RAPPEL : Dans le cadre de cet AP, nous admettons les faits suivants :

- La présence d'une infrastructure fonctionnelle au sein d'ASSURMER.
- La présence de plusieurs serveurs exécutant tous **Windows Server 2022**
- La présence des services *AD DS*[1]*, DNS*[2]*, et DHCP*[3]*,* sur un serveur **ASSURDC02**, tous déjà configurés et en état de fonctionnement. Le serveur est contrôleur du domaine *assurmer.local*.
- La fourniture d'un serveur **Windows Server 2022** déjà intégré au domaine *assurmer.local*, nommé **ASSURDEPLOY**.

De même, nous avons testé cette procédure sur l'hyperviseur VMWare Workstation Pro 17. Ces machines virtuelles sont toutes configurées sur le même réseau virtuel, séparées de la machine bare-métal qui est l'host.
Les configurations pourront donc varier selon l'environnement utilisé par la suite du déploiement sur l'infrastructure réelle d'ASSURMER.

[1] AD DS : Active Directory Domain Services, annuaire LDAP (protocole de centralisation de l'annuaire)
[2] DNS : Domain Name System, service qui traduit les noms/IP.
[3] DHCP : Dynamic Host Configuration Protocol, service qui distribue les informations réseaux (IP, DNS, etc…)

Etape 1 : Configurer le DHCP pour WDS

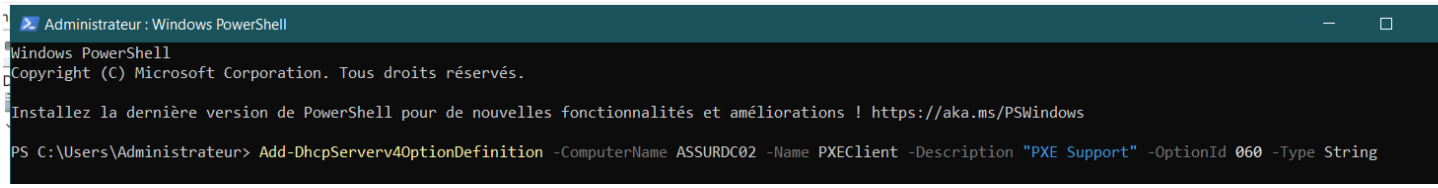
Essentiel au bon fonctionnement du boot PXE

Avant de commencer l'installation de **WDS** et de **MDT**, nous devons préparer des configurations nécessaires dans le **DHCP** du serveur **ASSURDC02**.
Ainsi, nous allons procéder à l'ajout d'options et de stratégies pour permettre le **boot PXE** sur notre infrastructure.
Informations importantes pour la suite :

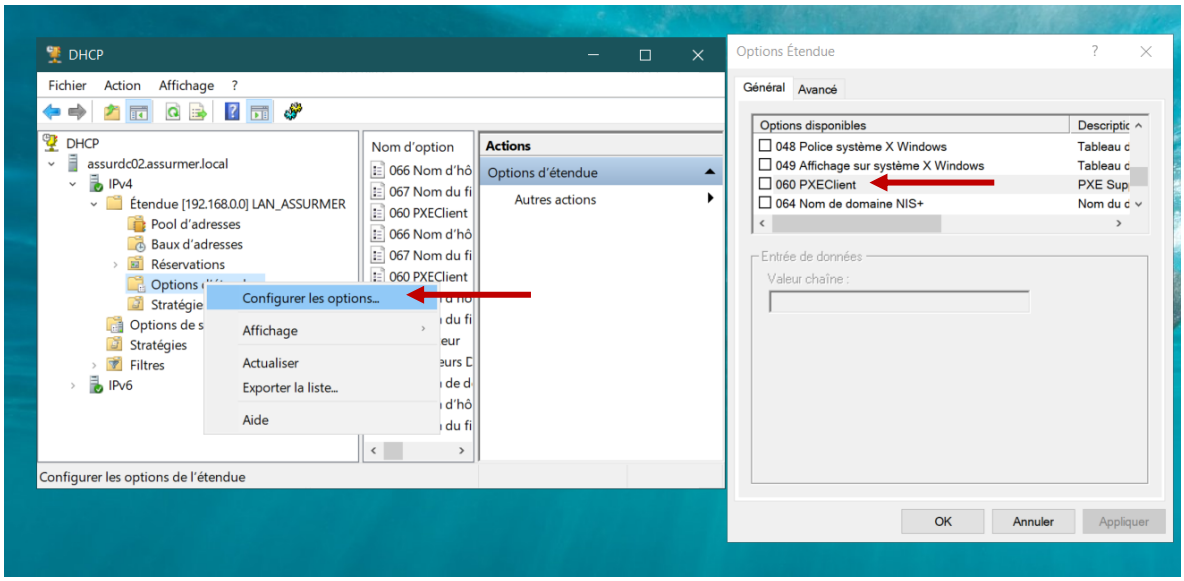
- **ASSURDC02** a comme adresse IP 192.168.0.1.
- **ASSURDEPLOY** a comme adresse IP 192.168.0.2.
- L'étendue **DHCP d'ASSURMER** est à l'adresse 192.168.0.0.

1. Se connecter au serveur **ASSURDC02** et démarrer la console **DHCP**.
2. Démarrer **PowerShell**, car nous allons procéder à la configuration à l'aide de scripts.
3. Insérer ceci dans la console, et appuyer sur la touche **Entrée** du clavier :

« Add-DhcpServerv4OptionDefinition -ComputerName ASSURDC02 -Name PXEClient -Description "PXE Support" -OptionId 060 -Type String »



4. On peut vérifier que la commande est bien effective en redémarrant la console DHCP, faire un clic droit sur les options de notre étendue DHCP, et chercher « 060 PXEClient » dans la liste.



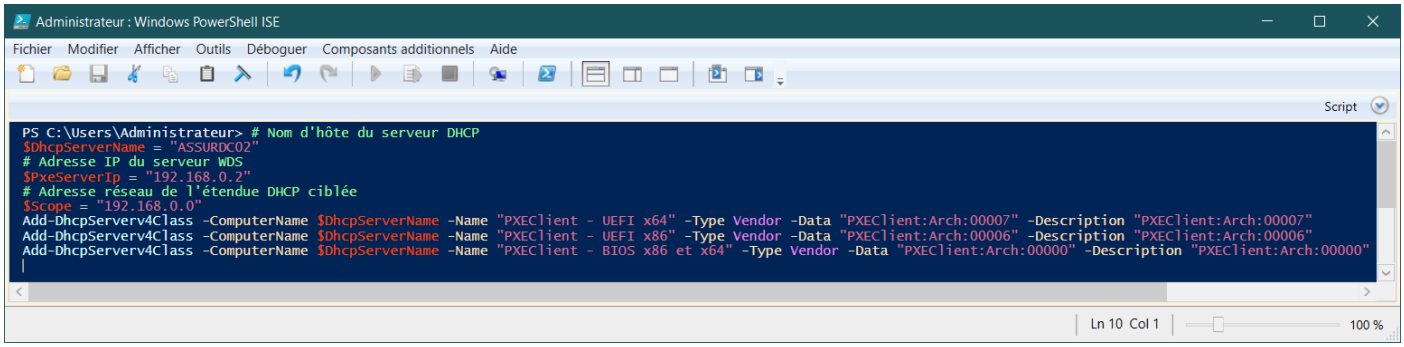
Pour éviter toute erreur, par la suite nous allons utiliser PowerShell ISE, qui permet d'effectuer plein de commandes à la suite et éviter toutes confusions et erreurs dans nos commandes.

5. Démarrer Powershell ISE, puis copier ces variables dans la fenêtre :

```
# Nom d'hôte du serveur DHCP
$DhcpServerName = "ASSURDC02"
# Adresse IP du serveur WDS
$PxeServerIp = "192.168.0.2"
# Adresse réseau de l'étendue DHCP ciblée
$Scope = "192.168.0.0"
```

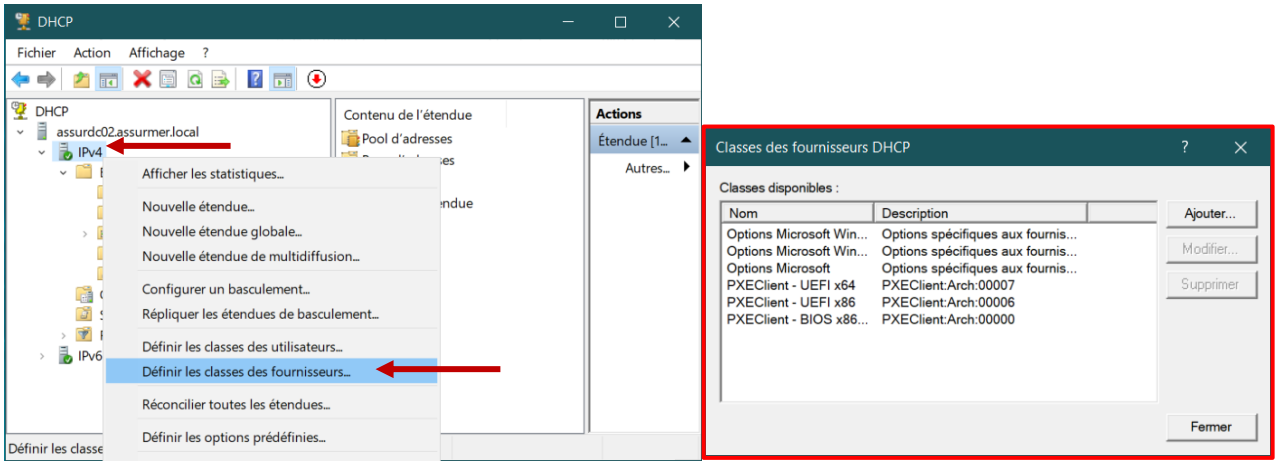
6. Appuyer sur entrée, puis coller ces commandes, et appuyer sur entrée :

```
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x64"
-Type Vendor -Data "PXEClient:Arch:00007" -Description "PXEClient:Arch:00007"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - UEFI x86"
-Type Vendor -Data "PXEClient:Arch:00006" -Description "PXEClient:Arch:00006"
Add-DhcpServerv4Class -ComputerName $DhcpServerName -Name "PXEClient - BIOS x86
et x64" -Type Vendor -Data "PXEClient:Arch:00000" -Description "PXEClient:Arch:00000"
```



Rendu de la commande dans l'ISE

7. Ne pas fermer l'ISE, puis se rendre sur la console DHCP (qu'on aura à nouveau redémarré), puis faire un clic droit sur « *IPv4* », puis « *Définir les classes des fournisseurs* », où on devrait obtenir :



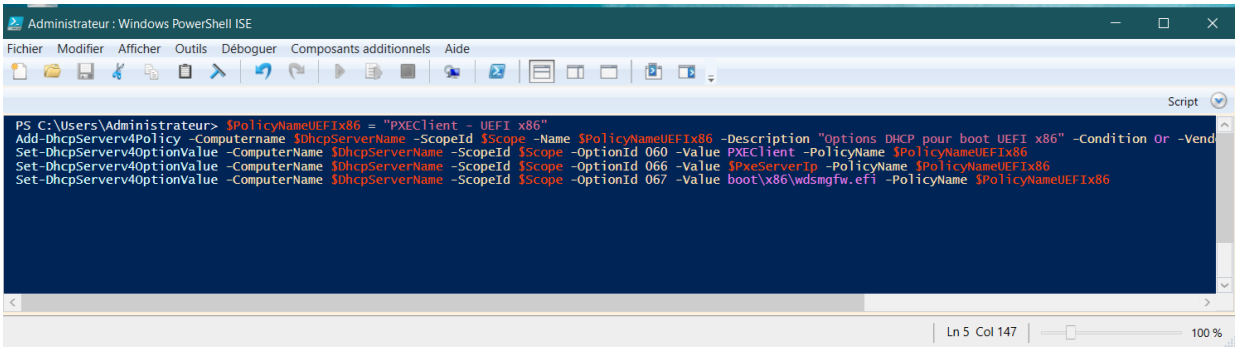
Enfin, nous allons avoir besoin de créer des **stratégies DHCP pour le boot PXE**.

8. Revenir sur l'ISE, et coller les successions de commandes suivantes, une par une :

```
$PolicyNameUEFIx64 = "PXEClient - UEFI x64"
Add-DhcpServerv4Policy -ComputerName $DhcpServerName -ScopeId $Scope -Name
$PolicyNameUEFIx64 -Description "Options DHCP pour boot UEFI x64" -Condition Or -
VendorClass EQ, "PXEClient - UEFI x64*"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx64
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx64
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 067 -Value boot\x64\wdsmgfw.efi -PolicyName $PolicyNameUEFIx64
```

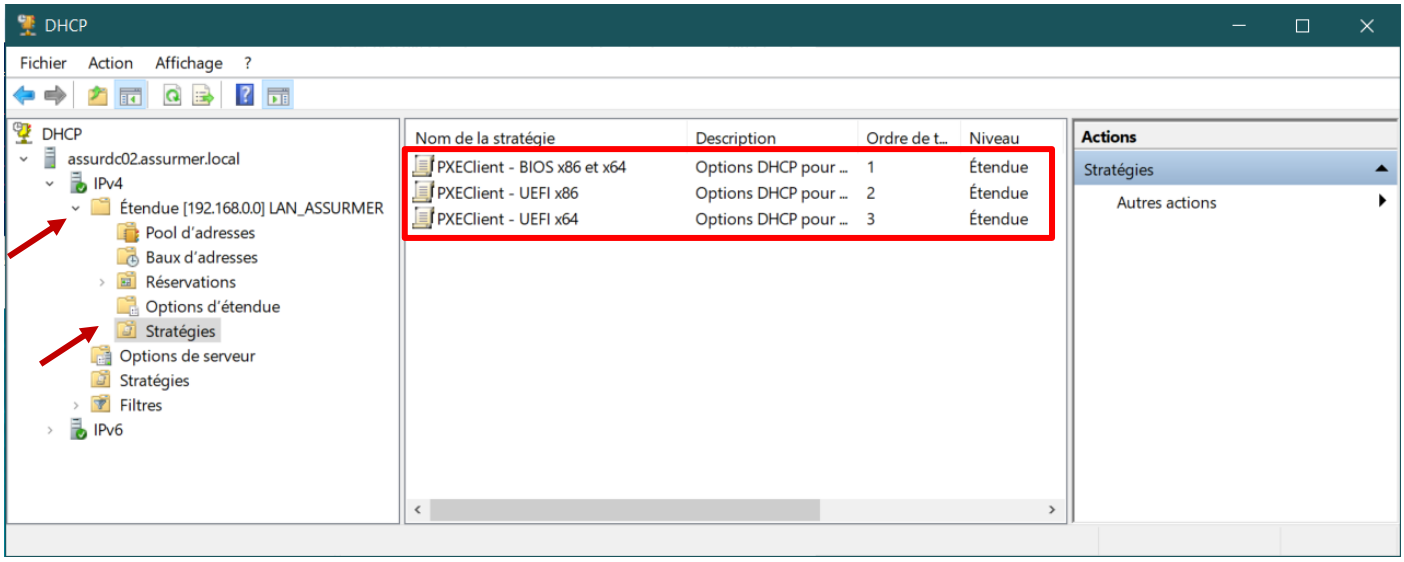
```
$PolicyNameUEFIx86 = "PXEClient - UEFI x86"
Add-DhcpServerv4Policy -ComputerName $DhcpServerName -ScopeId $Scope -Name
$PolicyNameUEFIx86 -Description "Options DHCP pour boot UEFI x86" -Condition Or -
VendorClass EQ, "PXEClient - UEFI x86*"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 060 -Value PXEClient -PolicyName $PolicyNameUEFIx86
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameUEFIx86
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -
OptionId 067 -Value boot\x86\wdsmgfw.efi -PolicyName $PolicyNameUEFIx86
```

```
$PolicyNameBIOS = "PXEClient - BIOS x86 et x64"
Add-DhcpServerv4Policy -ComputerName $DhcpServerName -ScopeId $Scope -Name $PolicyNameBIOS -Description "Options DHCP pour boot BIOS x86 et x64" -Condition Or -VendorClass EQ, "PXEClient - BIOS x86 et x64*"
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -OptionId 066 -Value $PxeServerIp -PolicyName $PolicyNameBIOS
Set-DhcpServerv4OptionValue -ComputerName $DhcpServerName -ScopeId $Scope -OptionId 067 -Value boot\x64\wdsnbp.com -PolicyName $PolicyNameBIOS
```



Exemple pour le x86 UEFI

9. Vérifier que la configuration est visible dans la console DHCP (après l'avoir redémarrée à nouveau) dans *IPv4*, *étendue*, *Stratégies*.

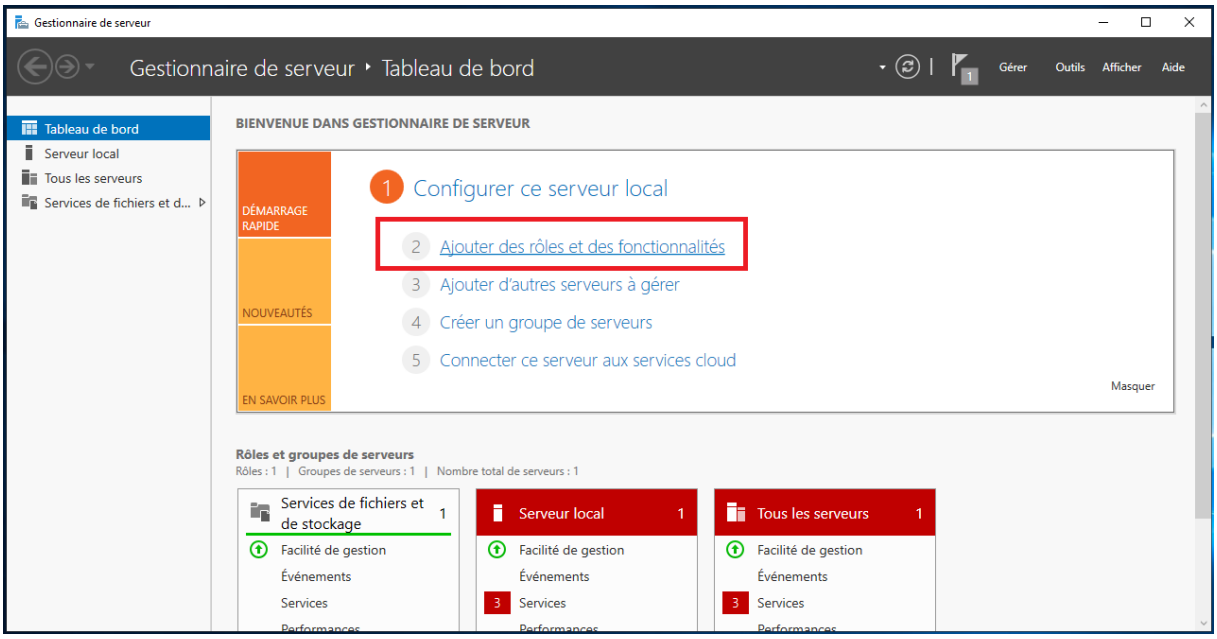


La configuration pour le boot PXE est maintenant terminée, et nous pouvons nous déconnecter d'**ASSURDC02** pour **ASSURDEPLOY**, et ainsi configurer WDS et MDT.

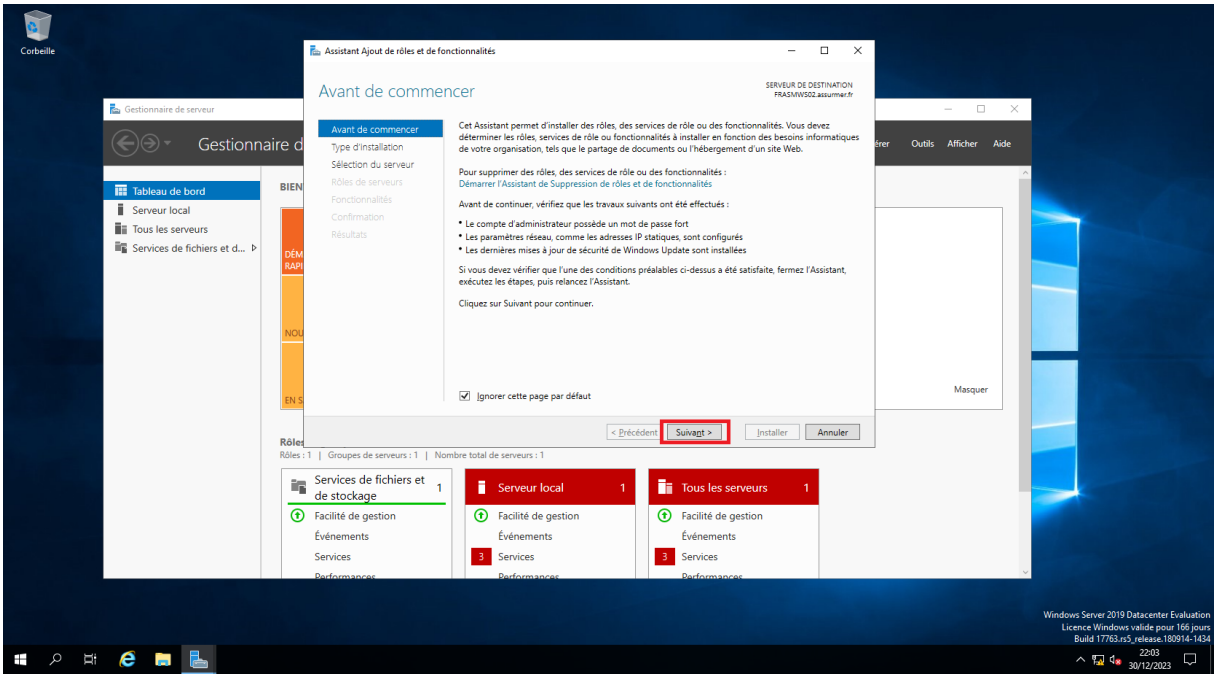
Etape 2 : Configurer WDS

Création de notre serveur de déploiement

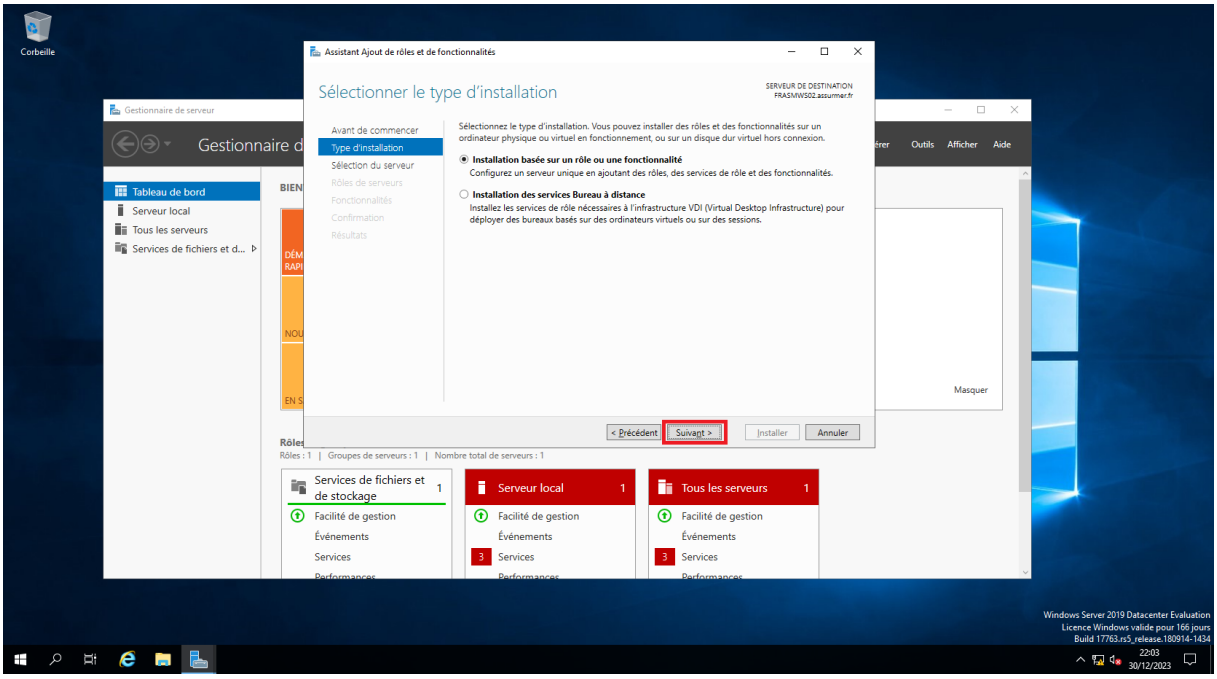
1. Sur le second serveur destiné à WDS et MDT, dans le Gestionnaire de serveur, sélectionner « Ajouter des rôles et des fonctionnalités ».



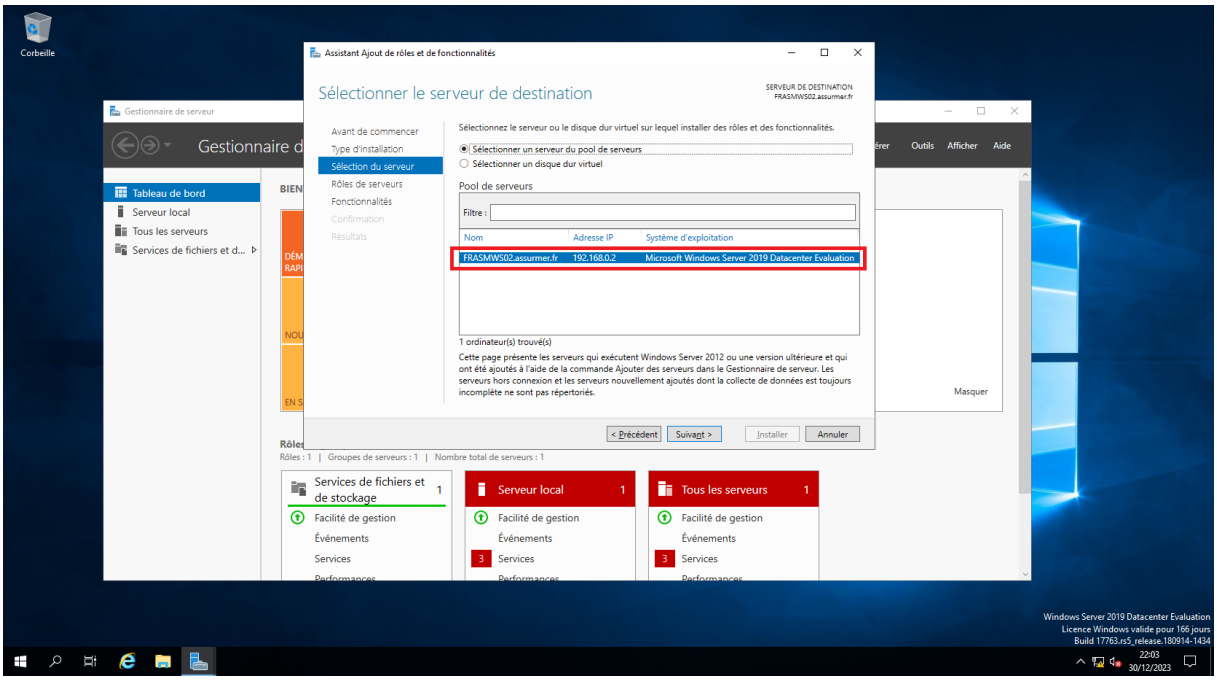
2. Cliquer sur « suivant ».



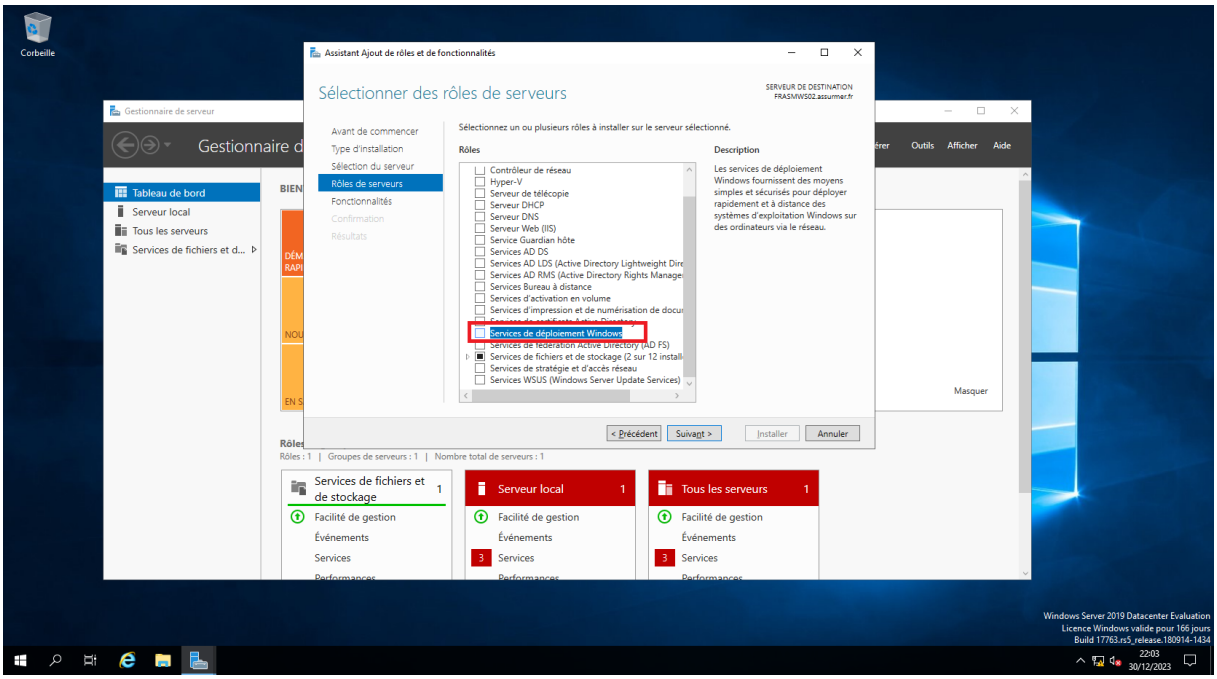
3. Cliquer sur « suivant ».



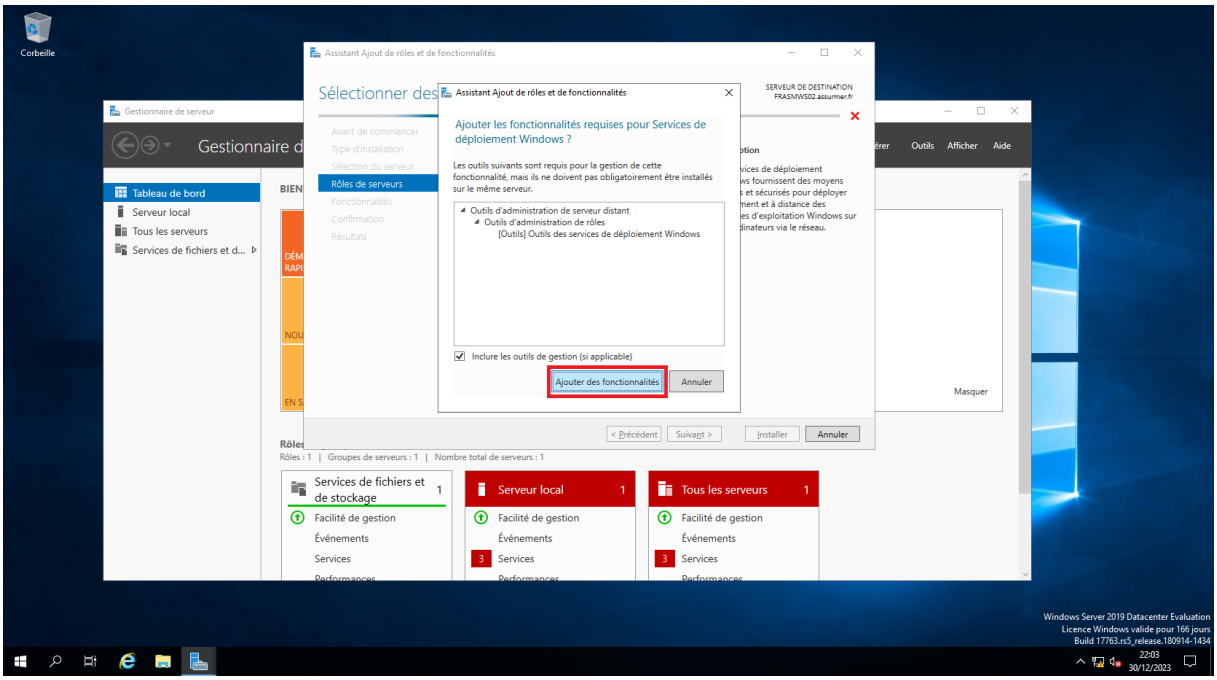
4. Sélectionner le serveur et cliquer sur « suivant ».



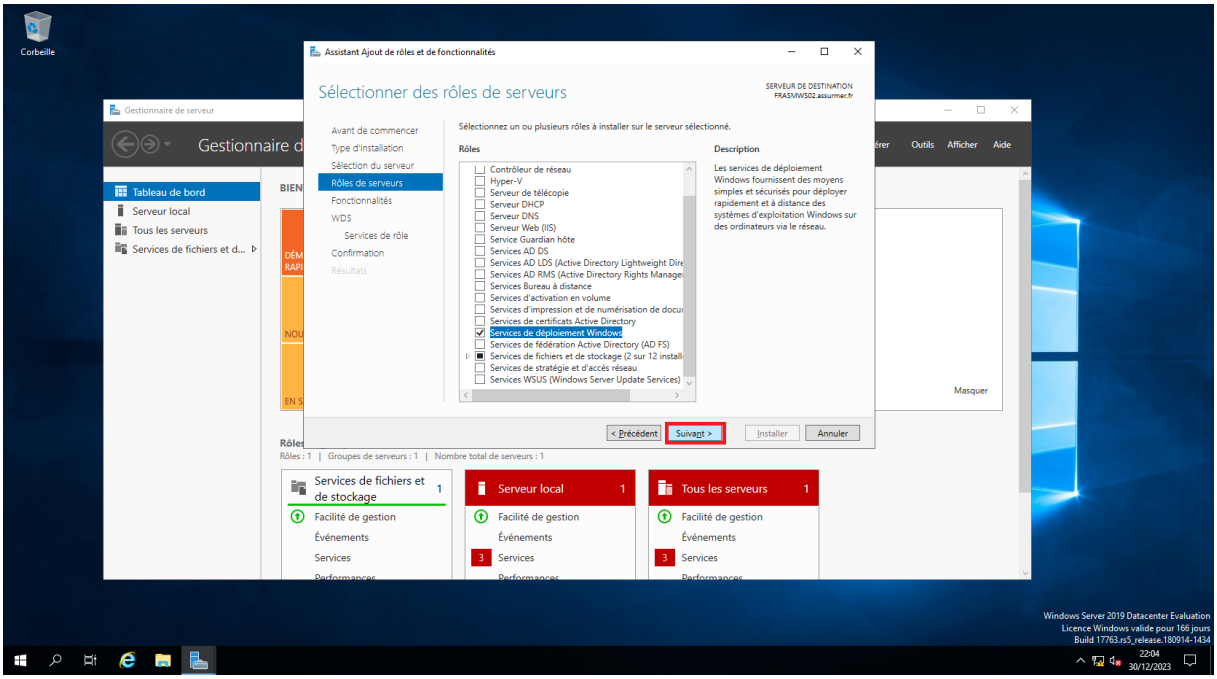
5. Sélectionner « Service de déploiement Windows » (WDS), une boîte de dialogue s'ouvrira alors.



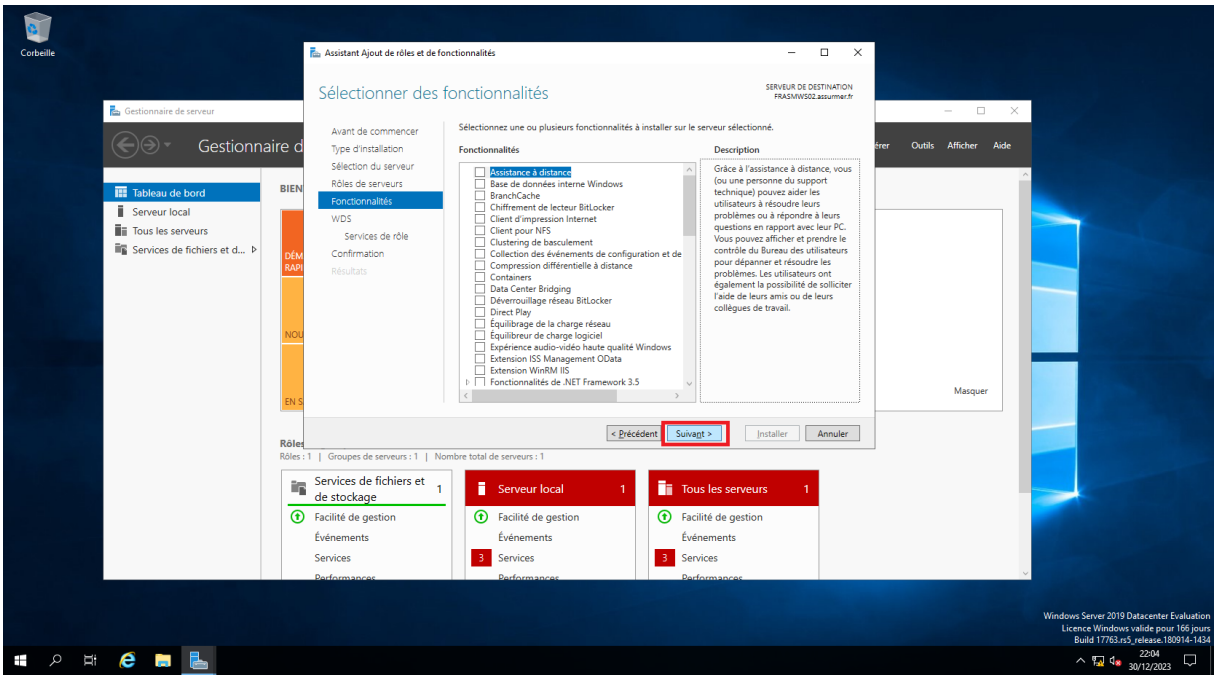
6. Cliquer sur « Ajouter des fonctionnalités ».



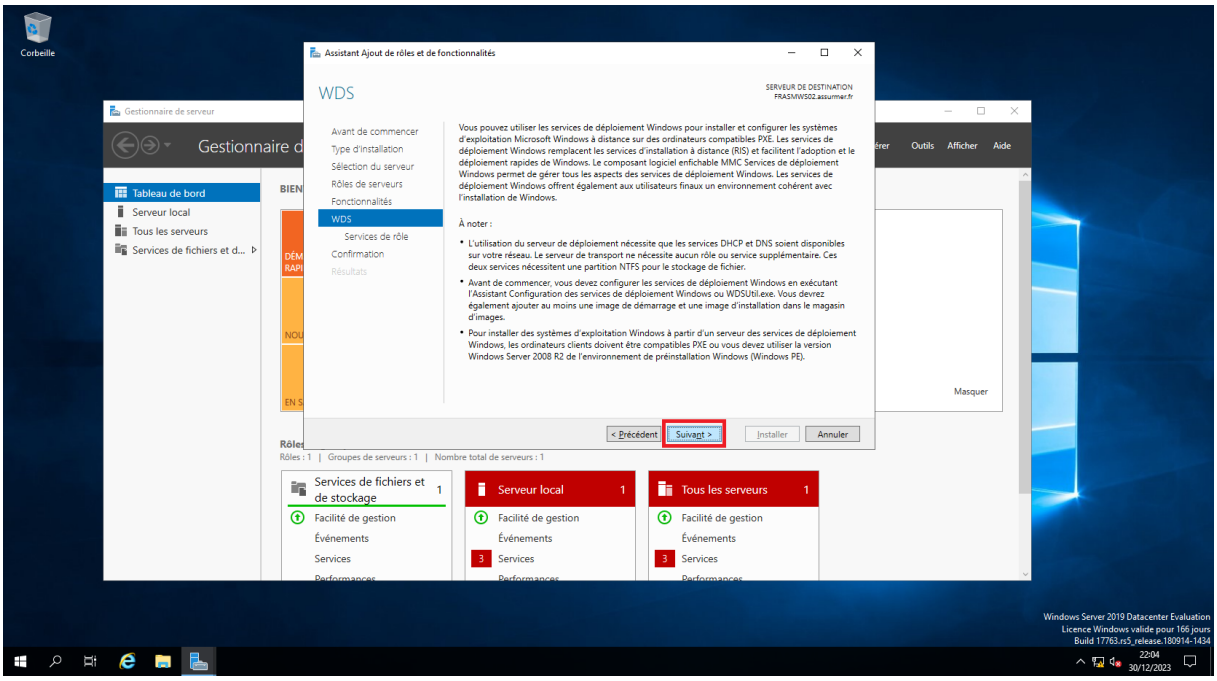
7. Cliquer sur « suivant ».



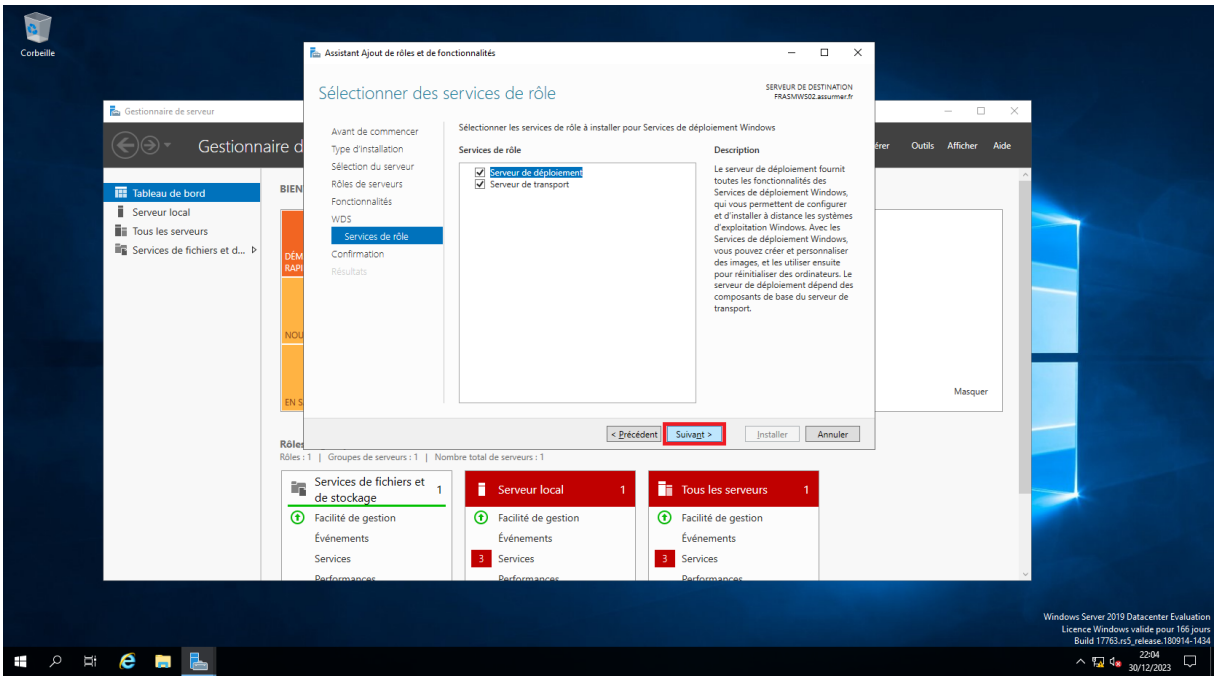
8. Cliquer sur « suivant ».



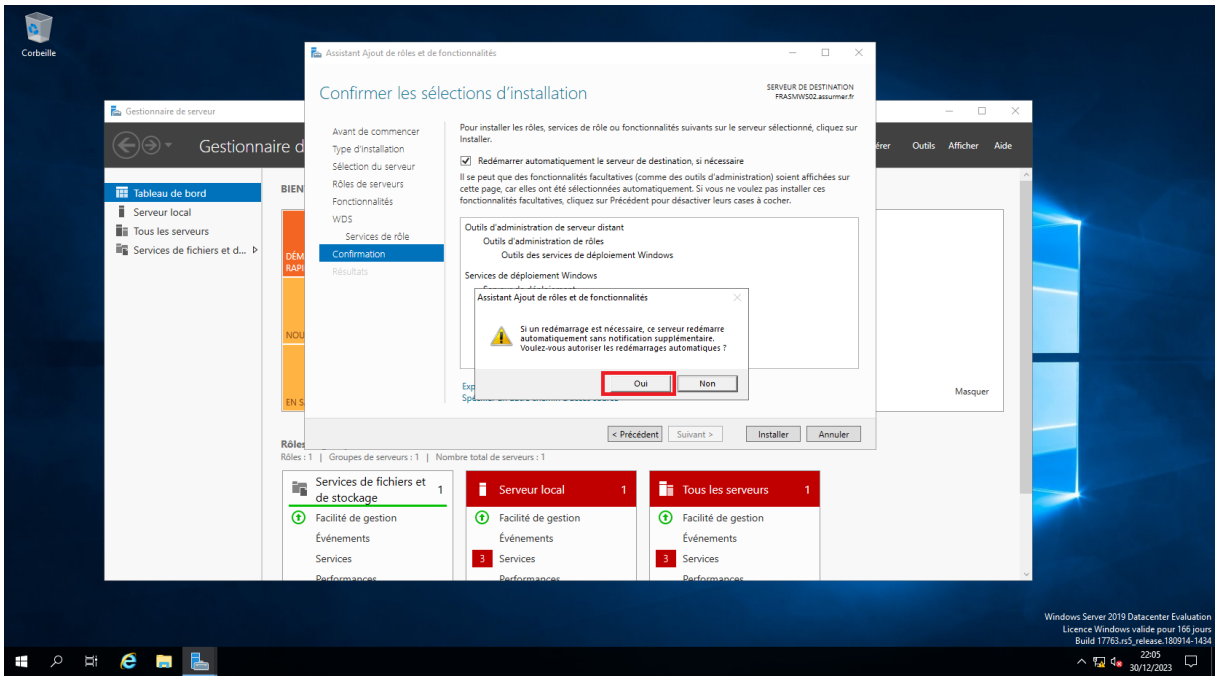
9. Cliquer sur « suivant ».



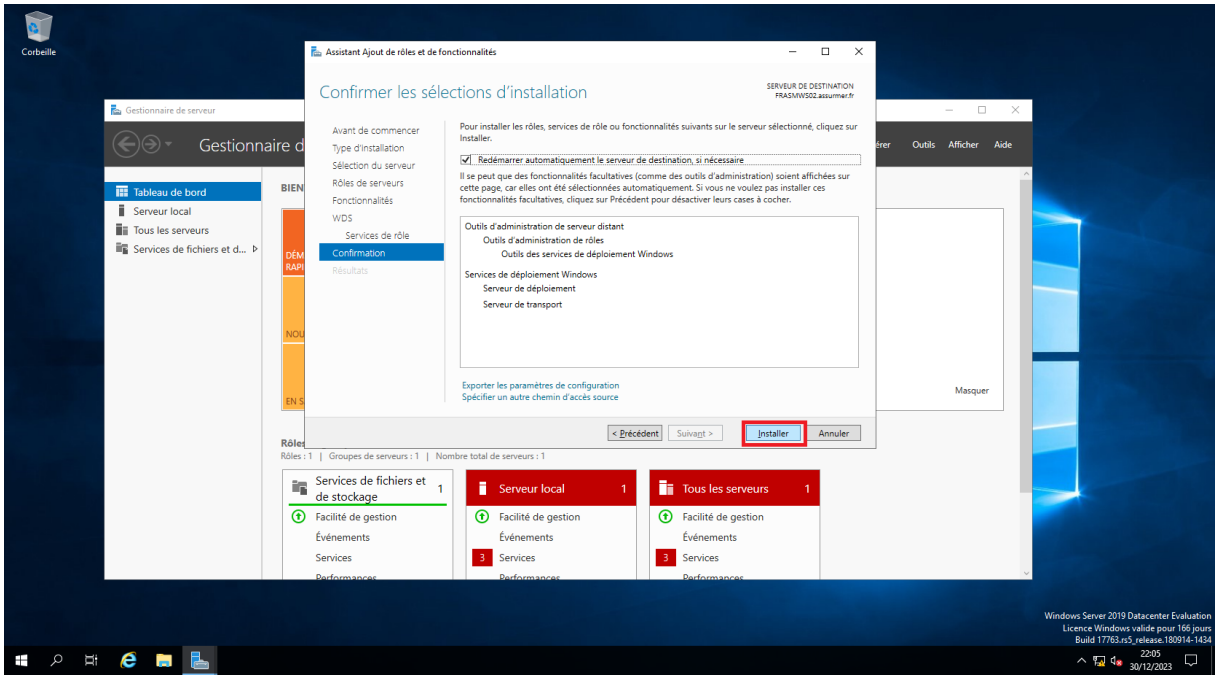
10. Cliquer sur « suivant ».



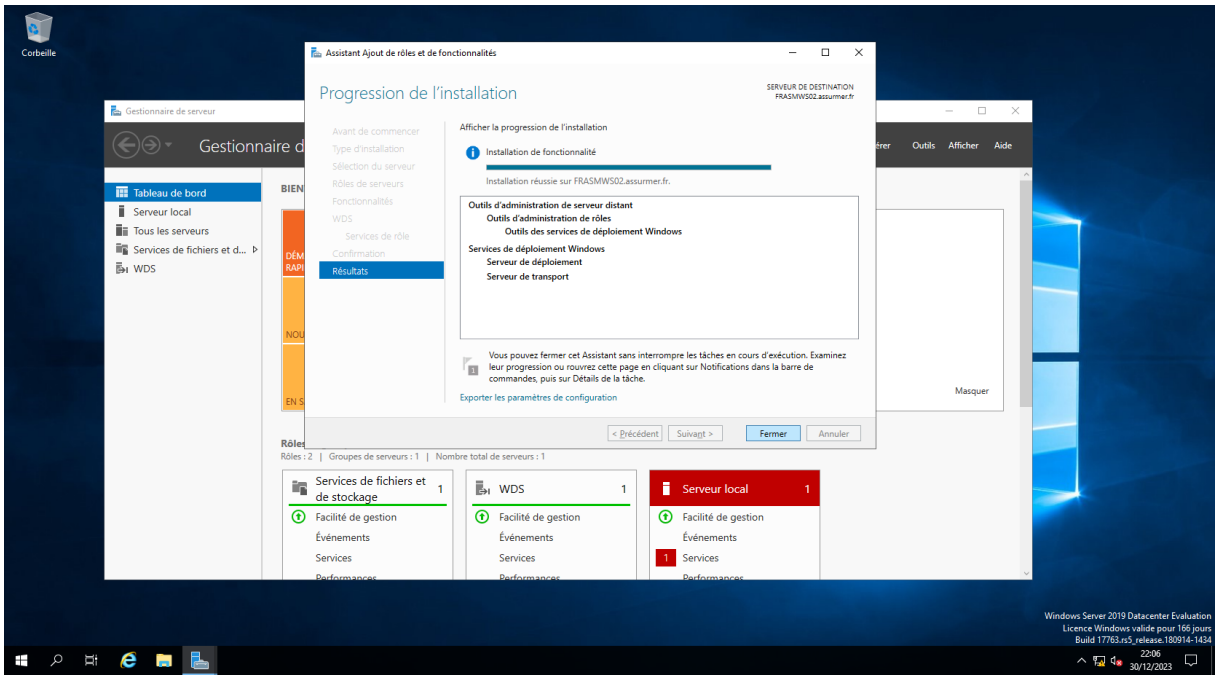
11. Cliquer sur « Oui ».



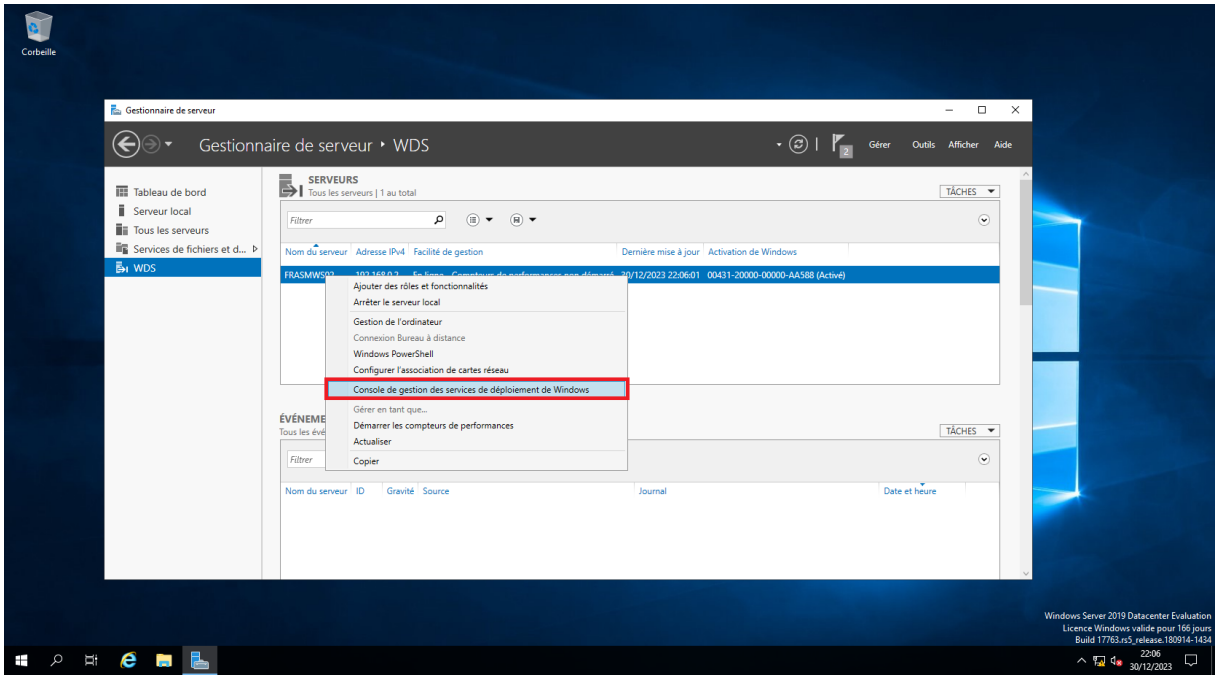
12. Cliquer sur « Installer ».



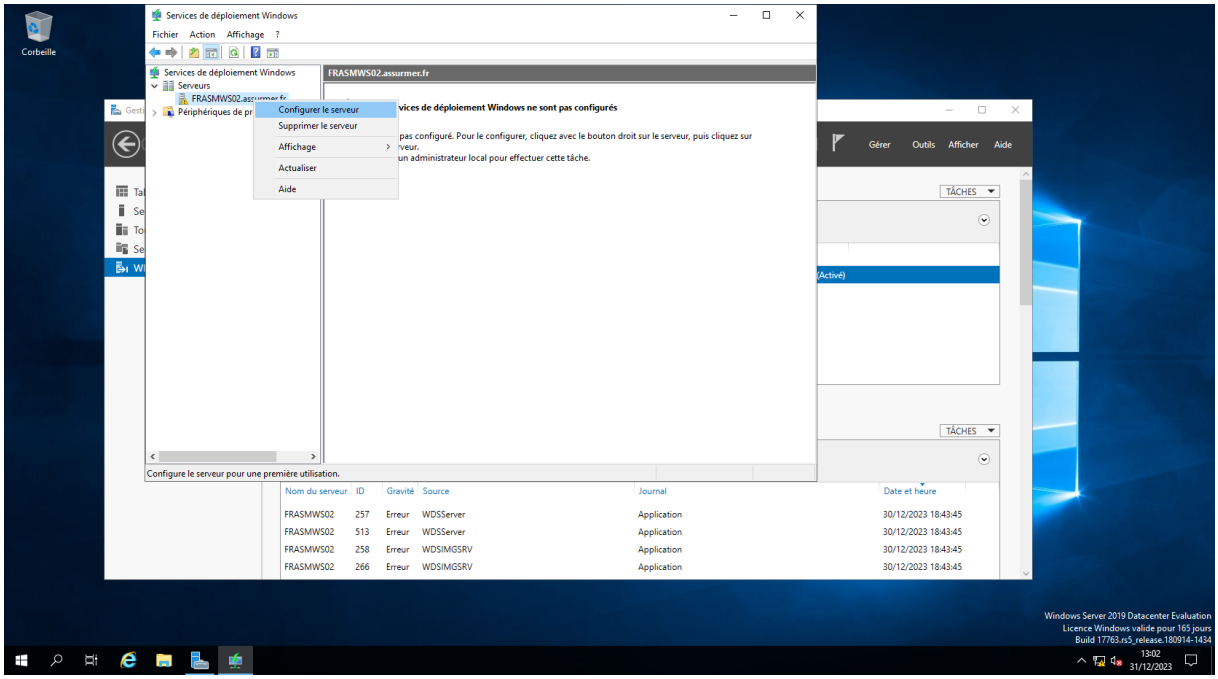
13. Cliquer sur « Fermer ».



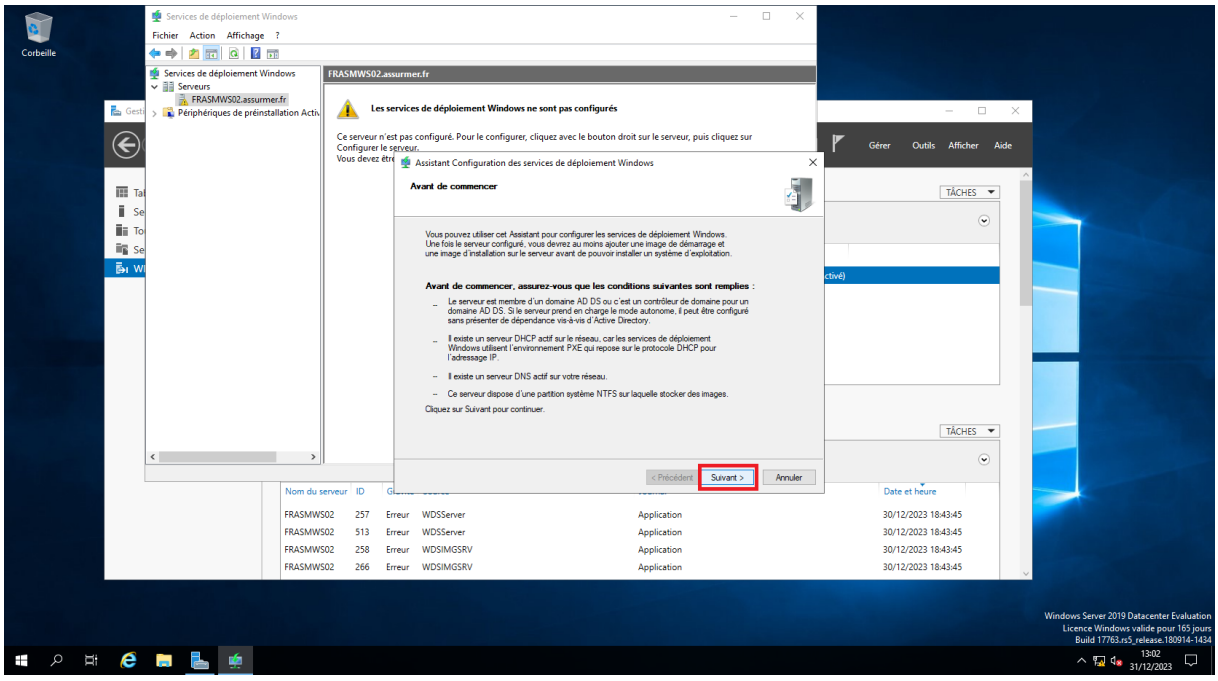
14. Sur l'onglet WDS sélectionner le serveur, et ouvrez la « Console de gestion des services de déploiements de Windows ».



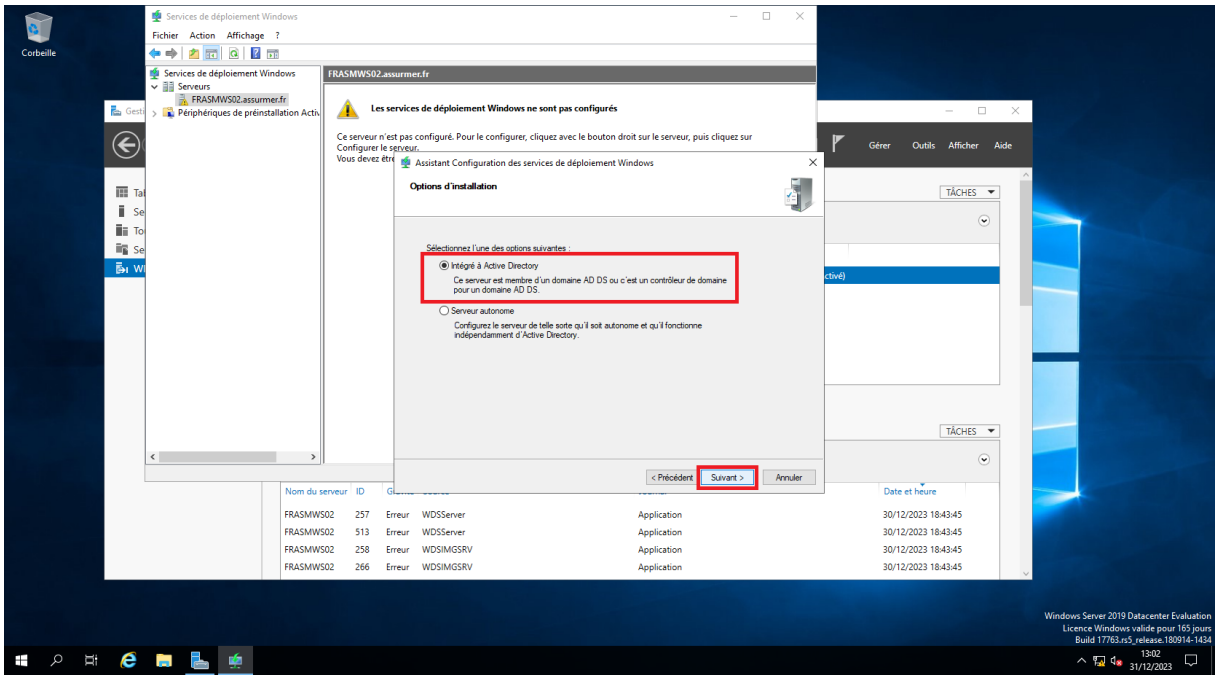
15. Sélectionner le serveur et cliquer sur « Configurer le serveur ».



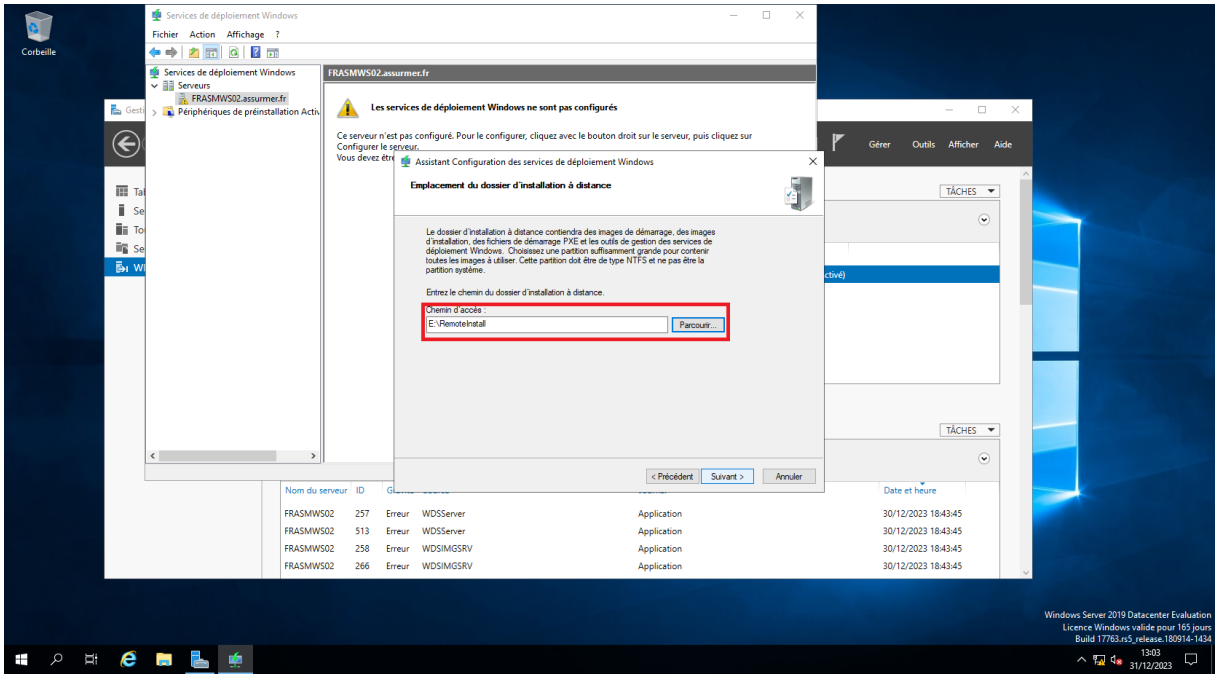
16. Cliquer sur « suivant ».



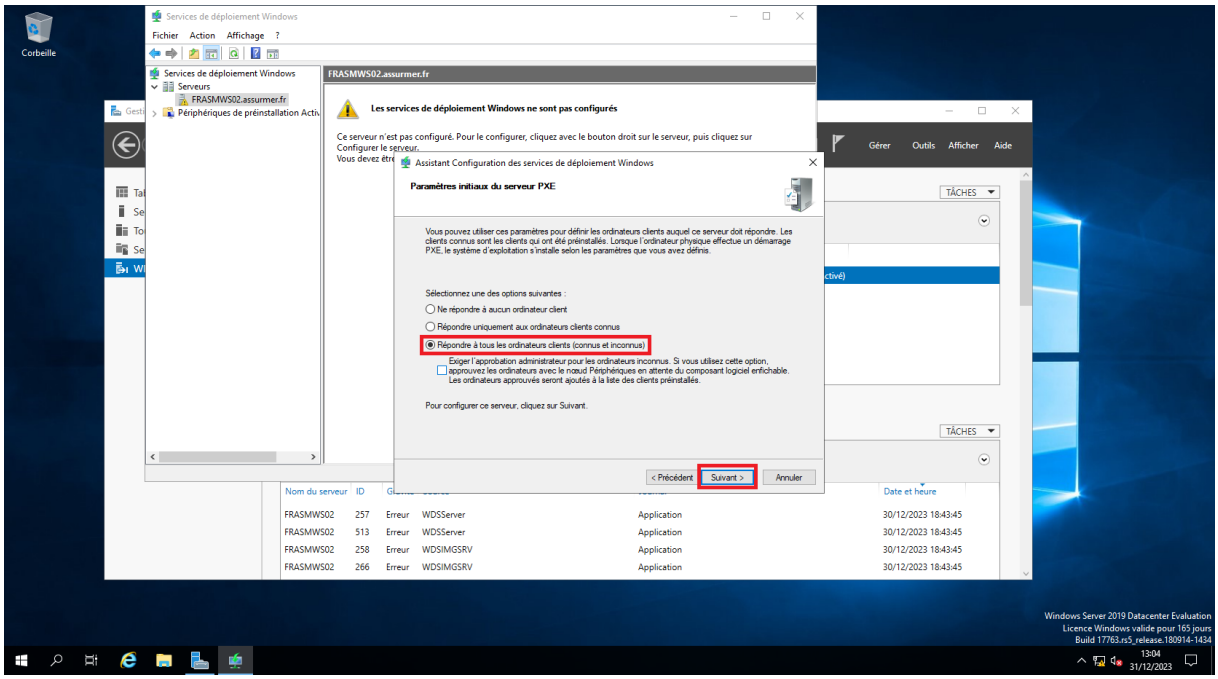
17. Veiller à ce que le serveur soit intégrer dans l'Active Directory et cliquer sur « suivant ».



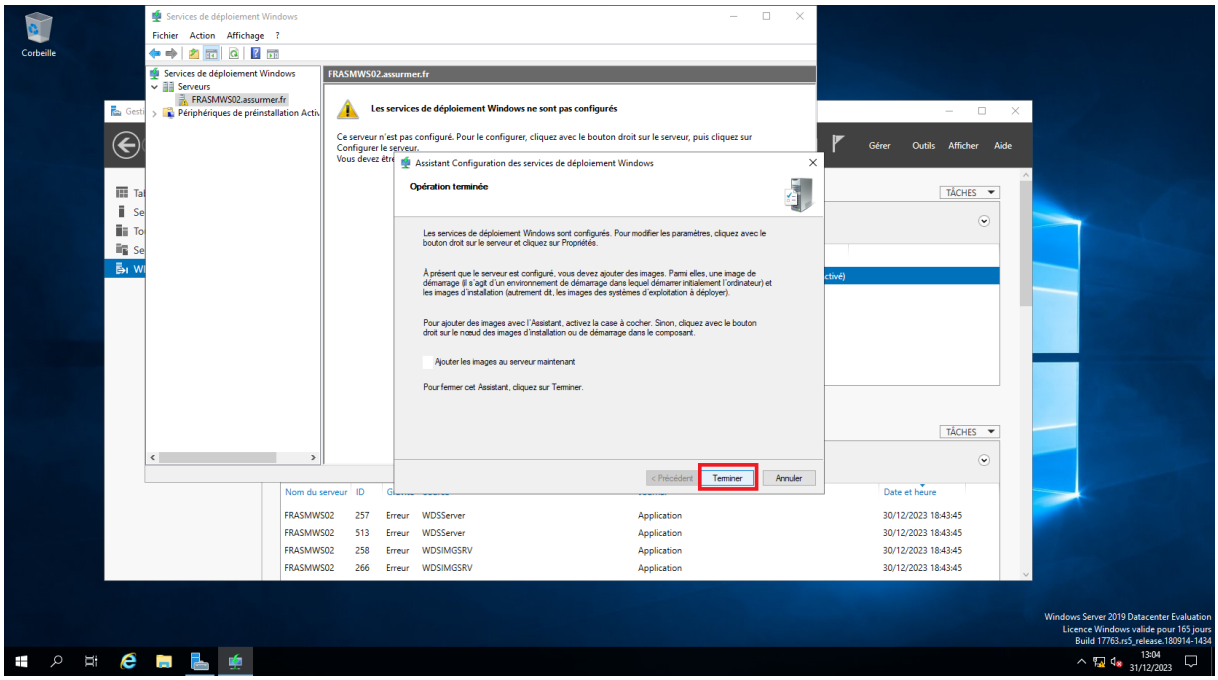
18. Ici entrer l'emplacement du dossier dans lequel se trouvera nos fichiers d'installation.



19. Sélectionner « Répondre à tous les ordinateurs clients », Ensuite cliquer sur « Suivant ».

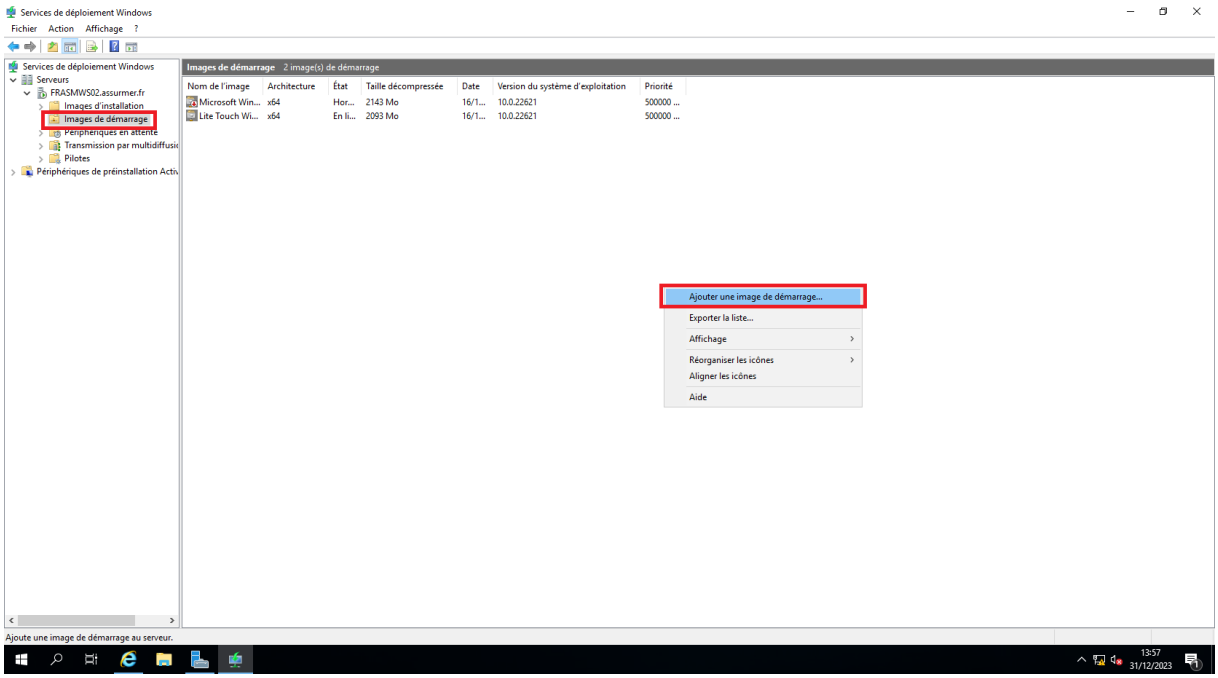


20. Décocher la case « Ajouter les images au serveur maintenant », et enfin cliquer sur « Terminer »

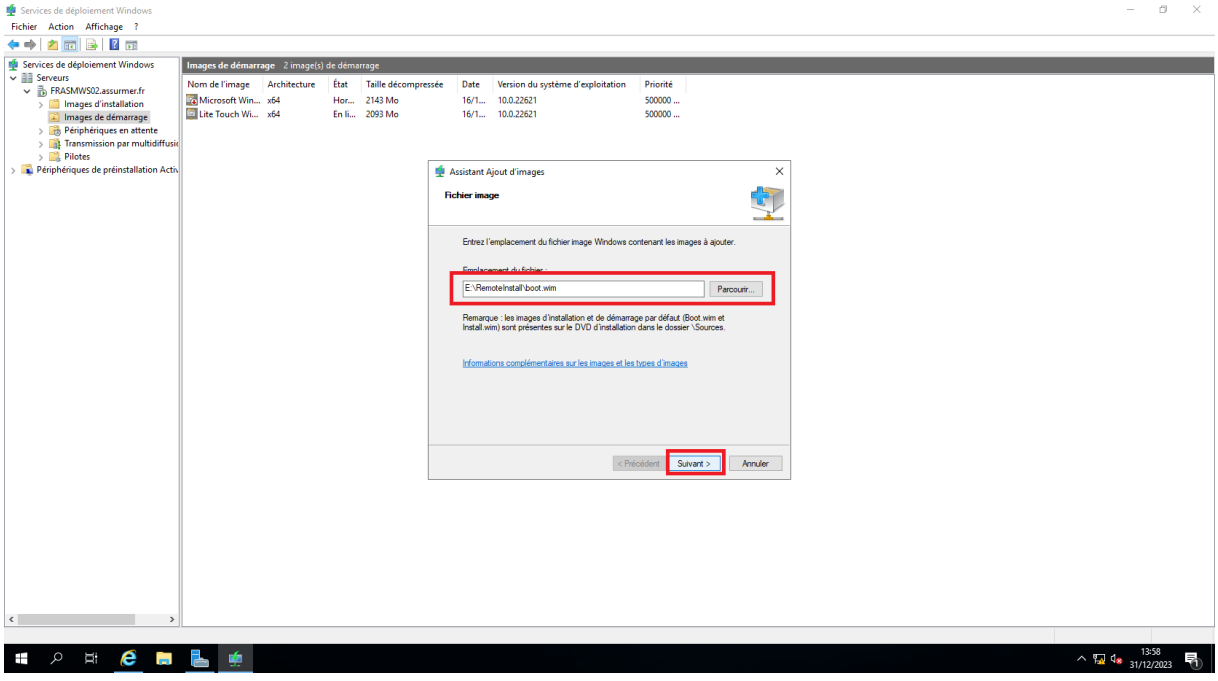


Ici notre serveur est configuré, et nous pouvons rajouter les images de démarrage et d'installation, comme le déploiement de Windows 11 via WDS uniquement ne fonctionne pas, nous allons ajouter des images Windows 10, en cas de nécessité d'un PC hors domaine ou en cas de nécessité de Windows 10 sur un PC particulier.

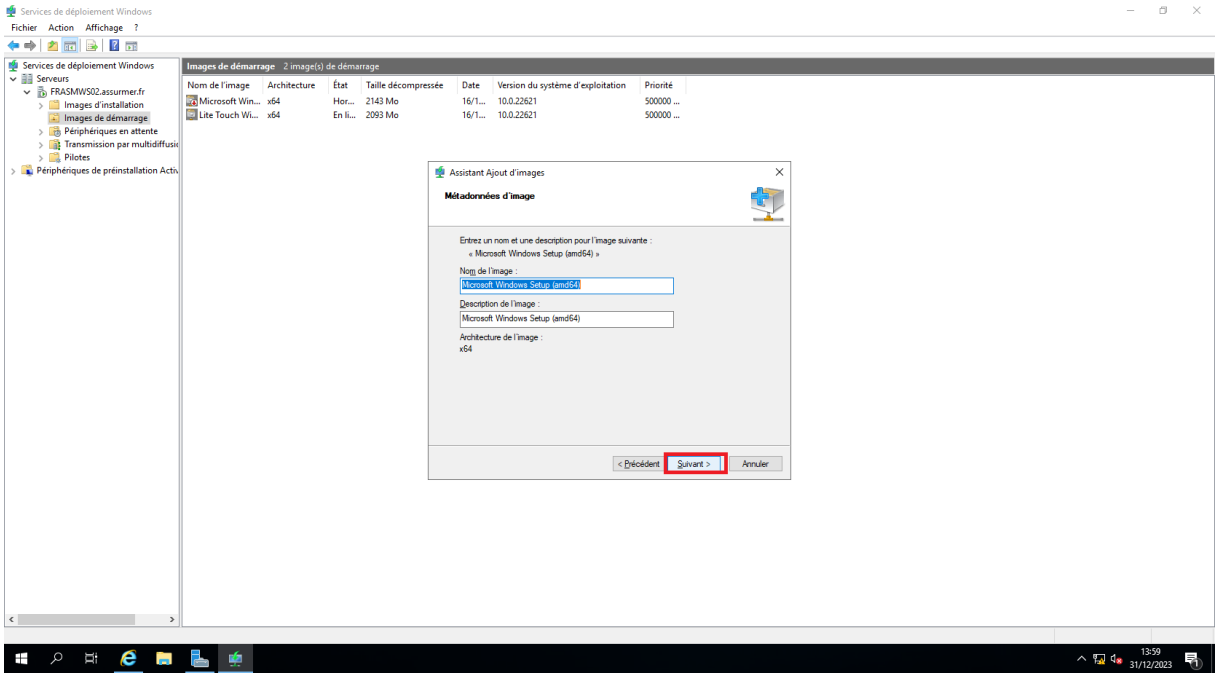
21. Dans l'onglet « images de démarrage », faire un clic droit et cliquer sur « Ajouter une image de démarrage »



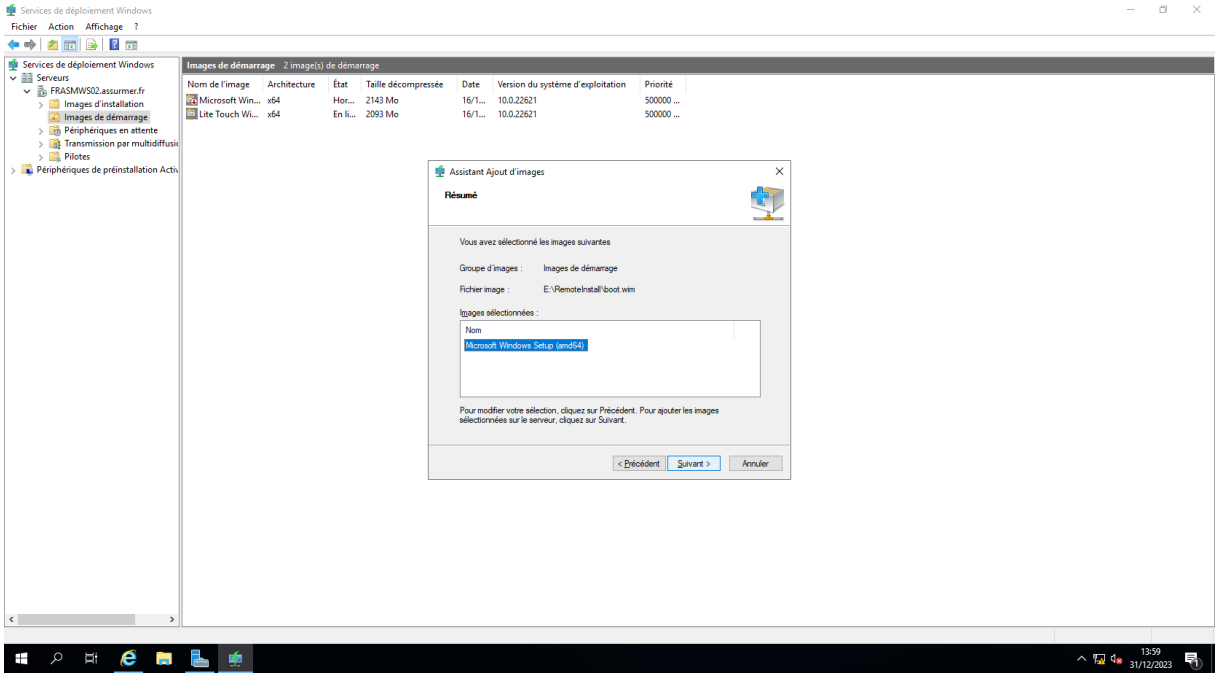
22. Sélectionner le fichier boot.wim de l'image que l'on souhaite installer.



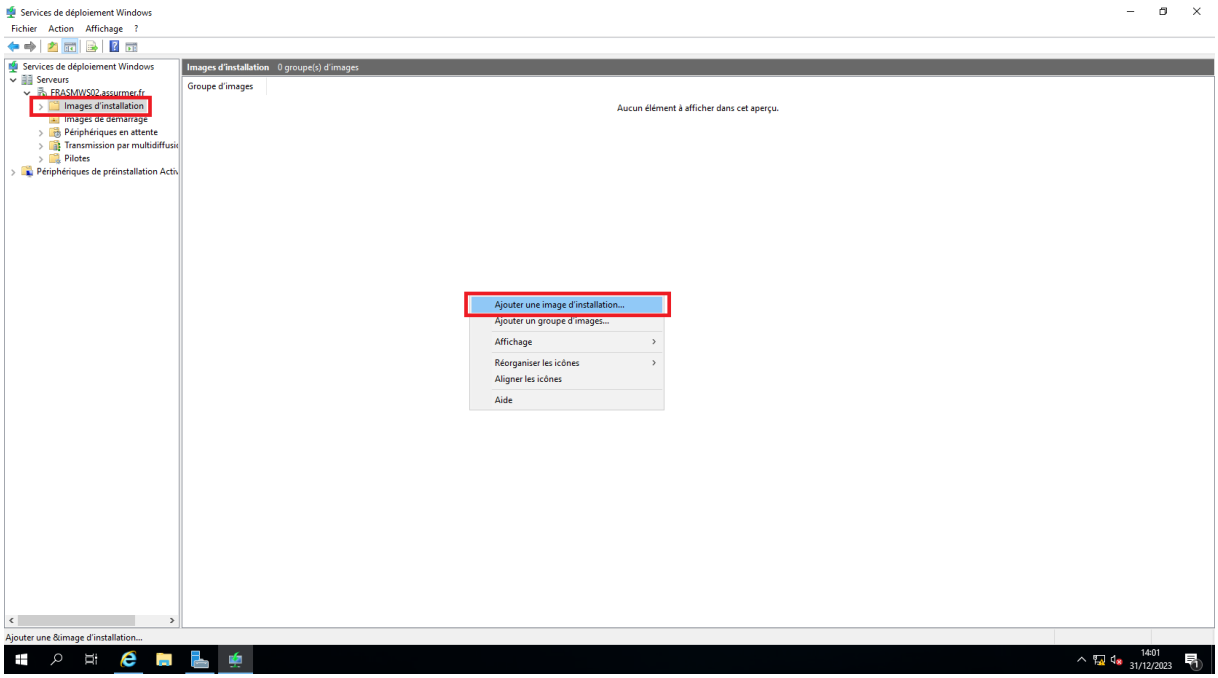
23. Renommer l'image ou non l'image à notre convenance, puis cliquer sur « Suivant »



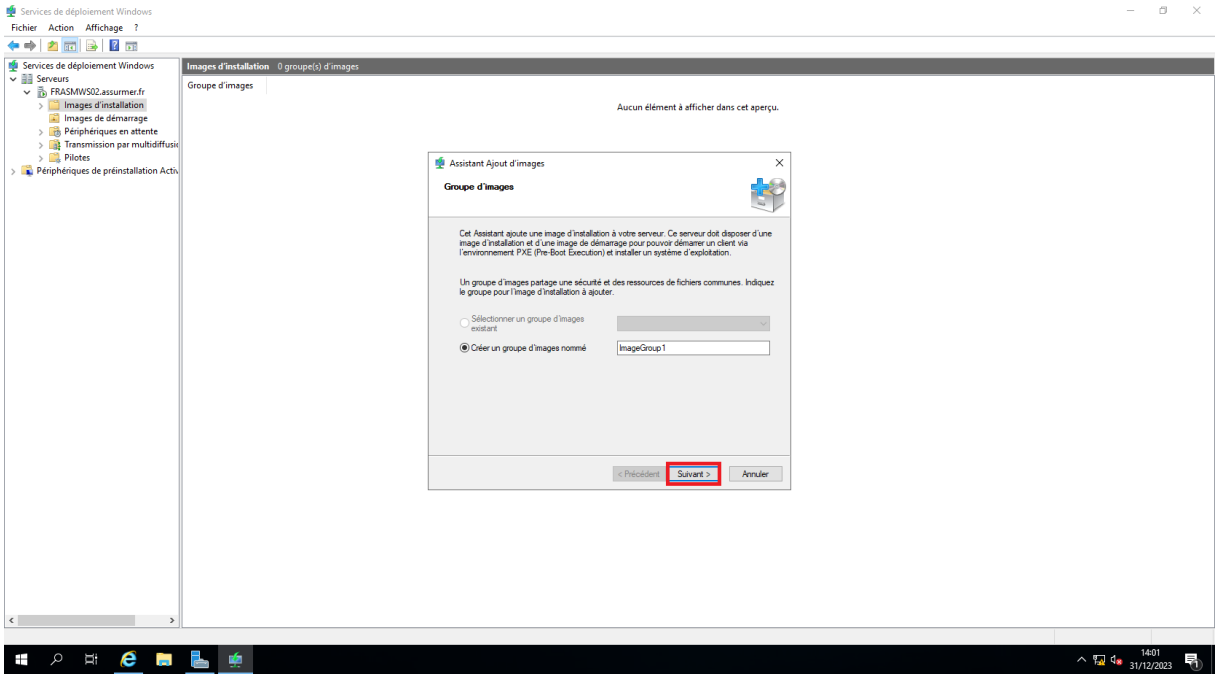
24. Cliquer sur « Suivant »



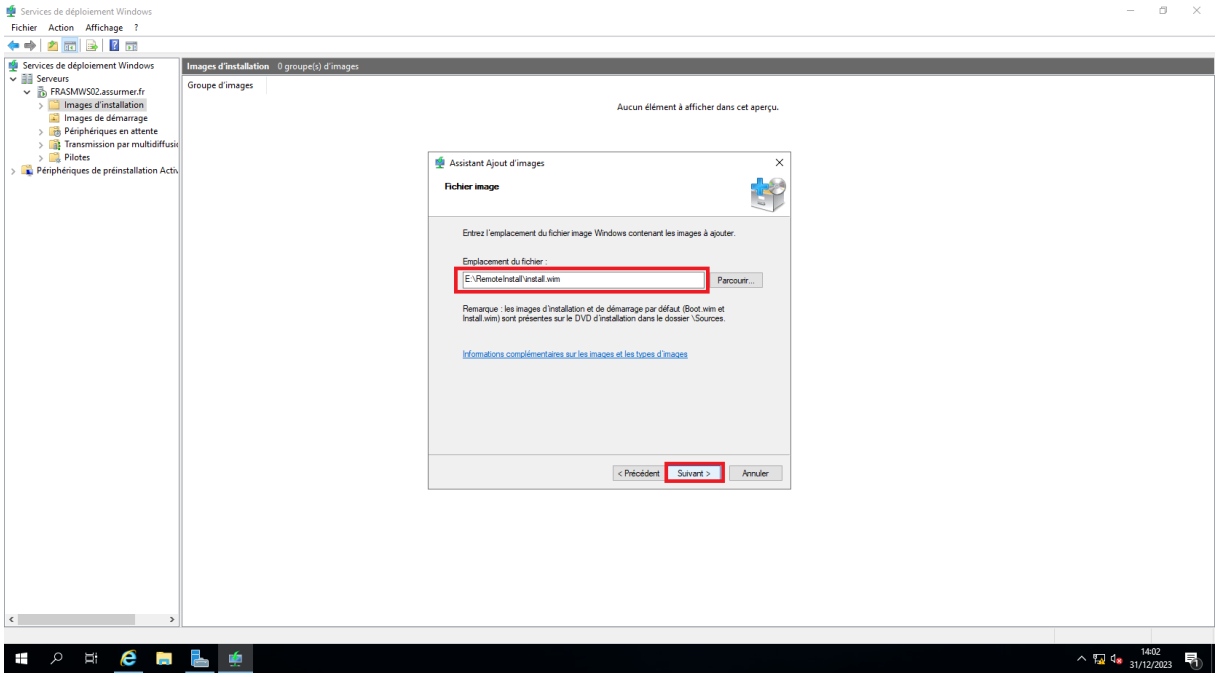
25. Dans l'onglet « images d'installation », faire un clic droit et cliquer sur « Ajouter une image d'installation »



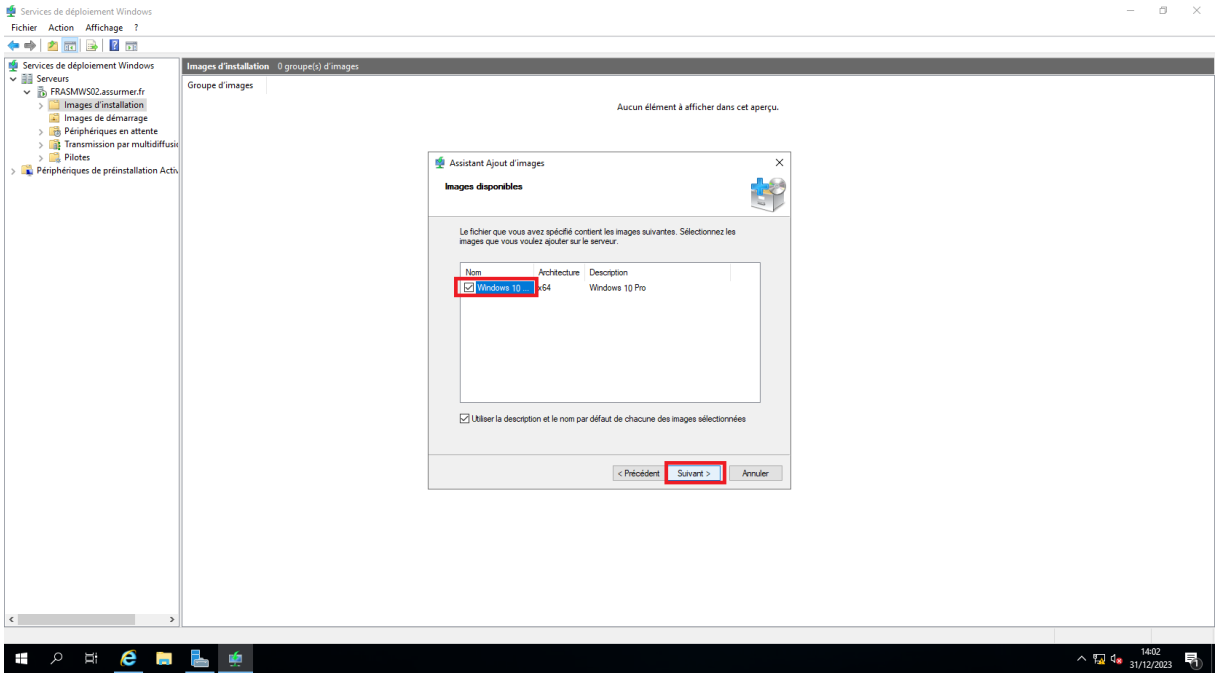
26. Nommer le groupe d'image à notre convenance et cliquer sur Suivant.



27. Sélectionner le fichier install.wim de l'image que l'on souhaite installer.



28. Sélectionner la version de l'image qui nous intéresse et cliquer sur « Suivant »



La configuration de WDS est finie, Nous pouvons maintenant démarrer un poste via le Boot PXE et ce dernier pourra bénéficier de l'image de Windows 10.

Cependant nous souhaitons installer Windows 11 et non Windows 10 et pour cela nous devrons configurer MDT.

Etape 3 : Installation et configuration de MDT

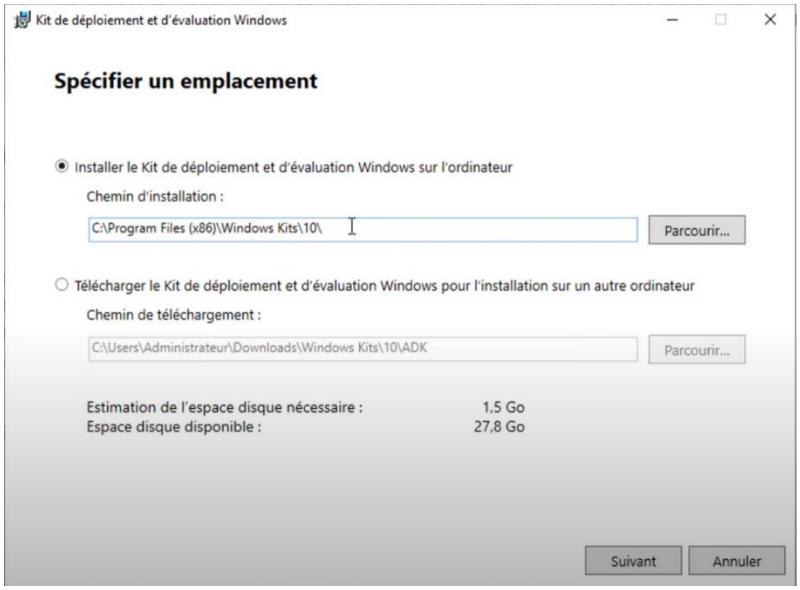
Création de notre image légère pour le déploiement des PC

Pour commencer l'installation de MDT, il nous faut **Windows ADK** et **Windows PE ADK** puis installer MDT, directement disponible sur le site de Microsoft.

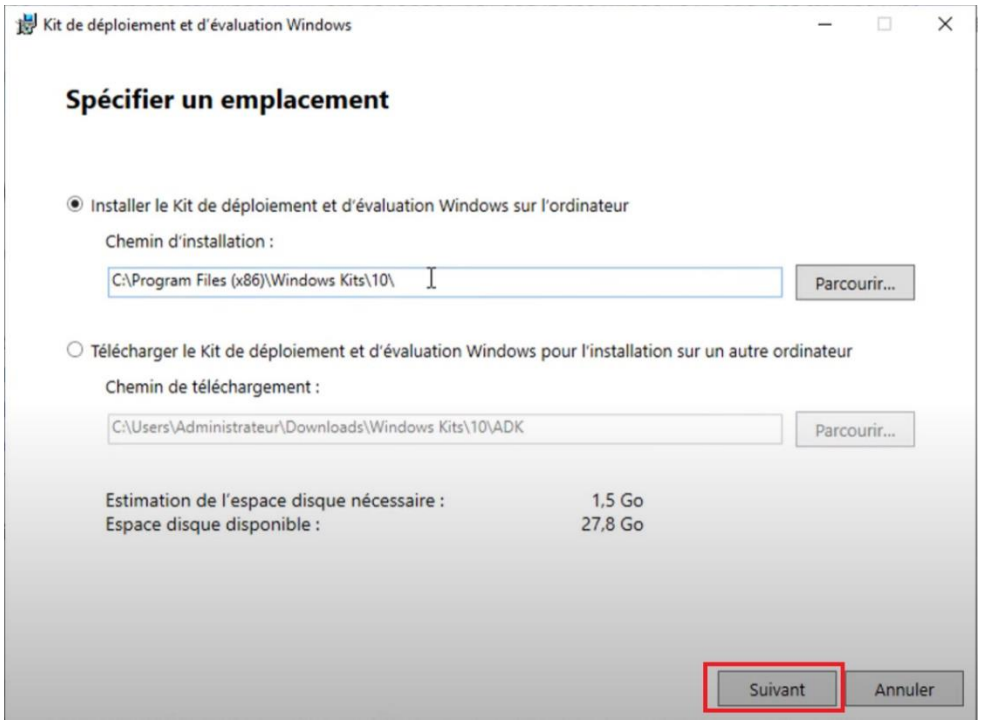
1. Il nous faut télécharger les addons nécessaires au bon fonctionnement de MDT

2. Exécuter adsetup.exe

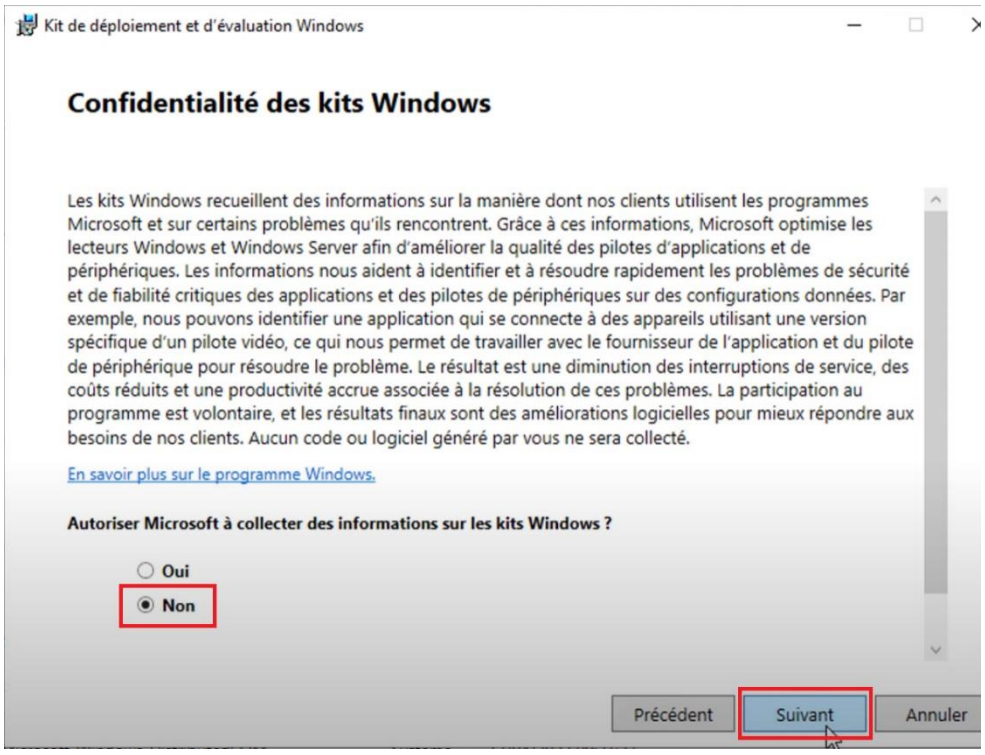
3. La fenêtre ci-dessous s'affiche



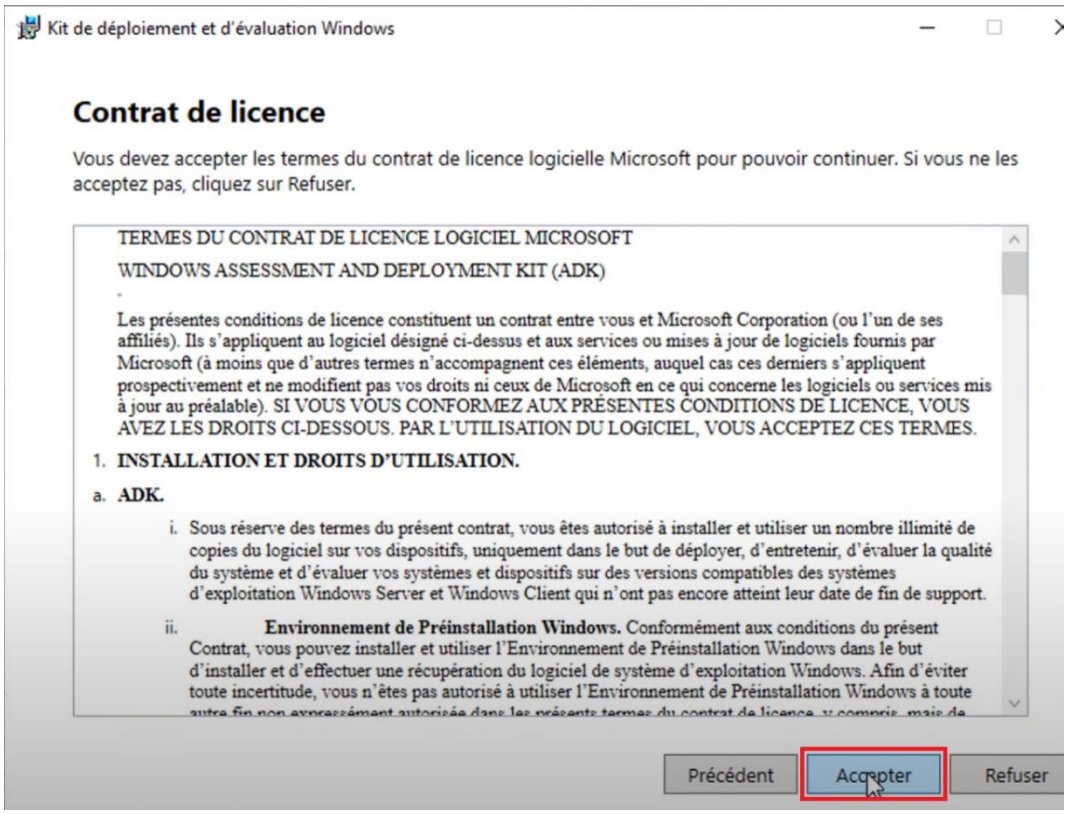
4. Cliquer sur Suivant



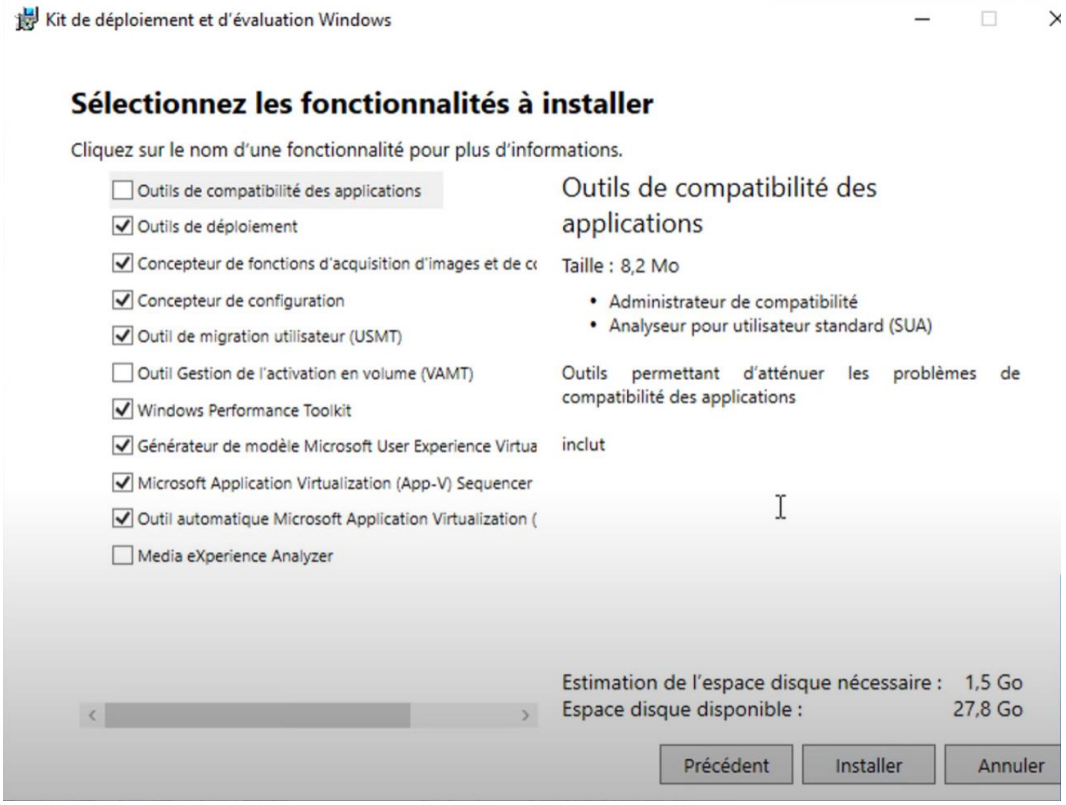
5. Cliquer sur « non » puis suivant



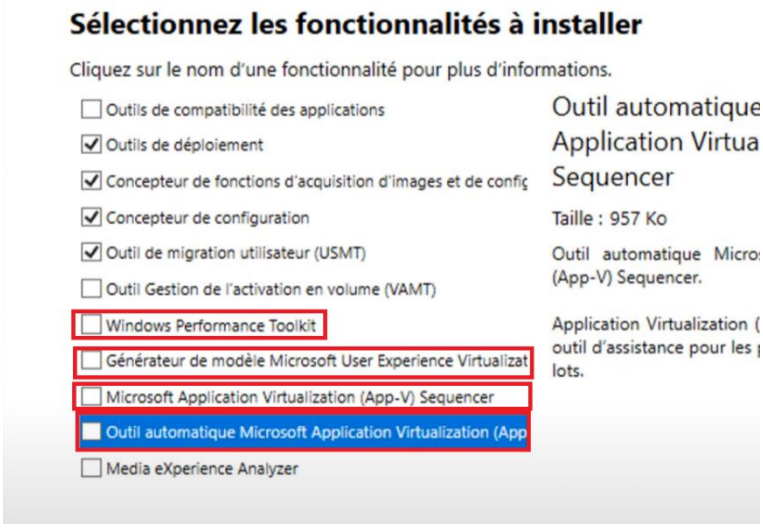
6. Accepter le contrat de licence



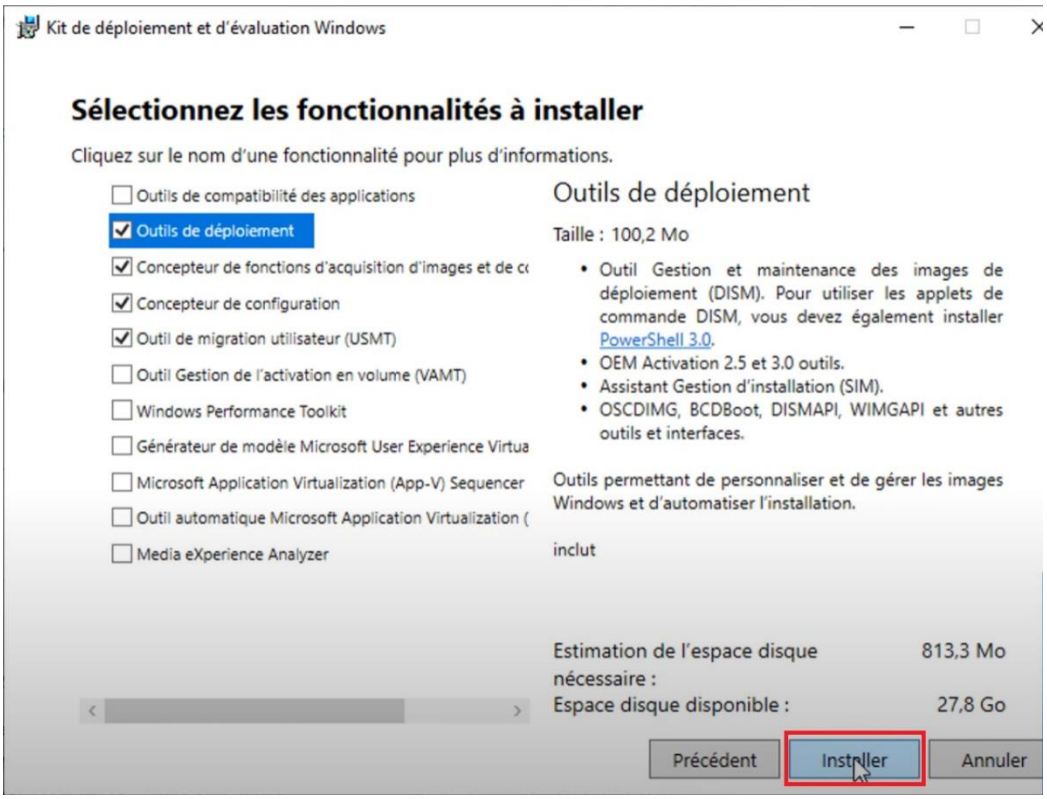
7. La fenêtre suivante sont les fonctionnalités que nous allons choisir d'activer.



8. On désactive les fonctionnalités encadrées

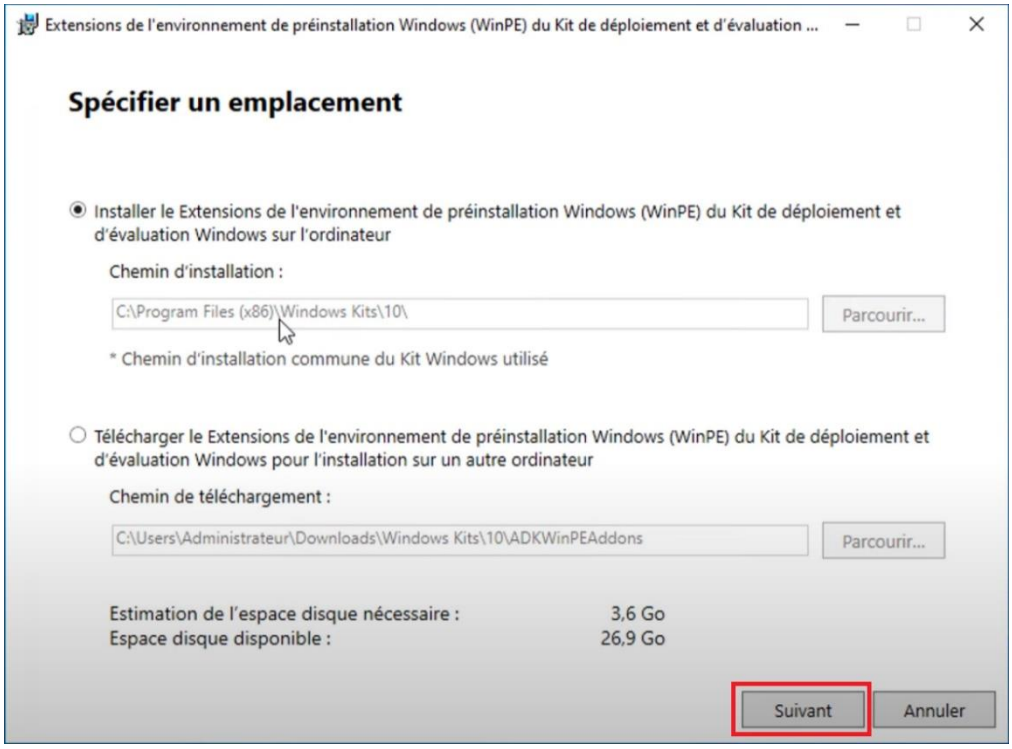


9. Cliquer sur installer, puis fermer quand l'installation se termine.

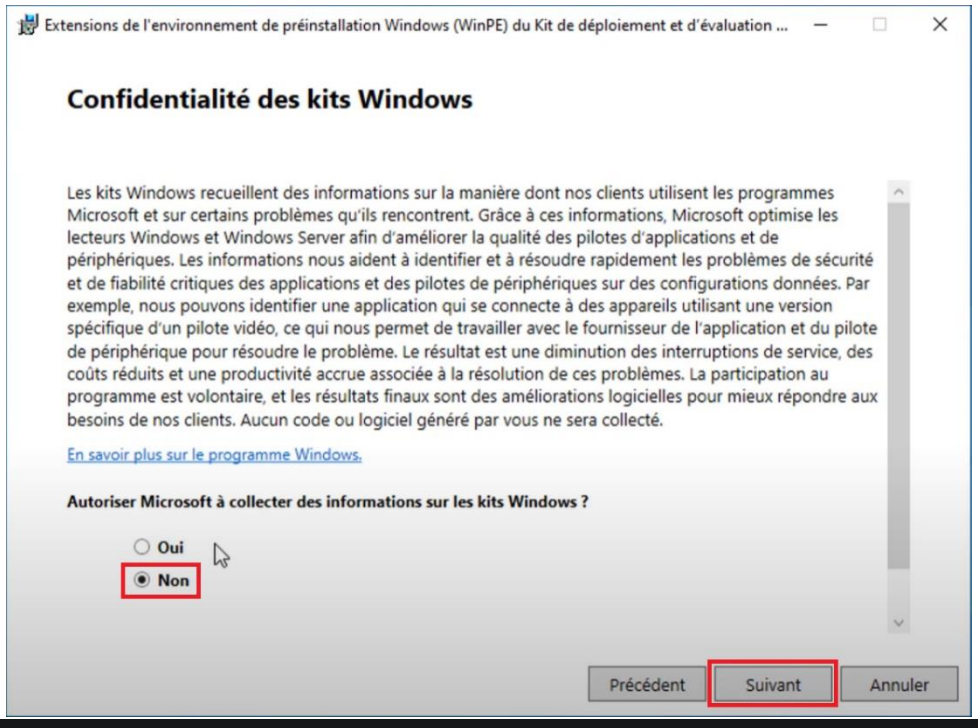


10. Exécuter ensuite adkwinpesetup.exe

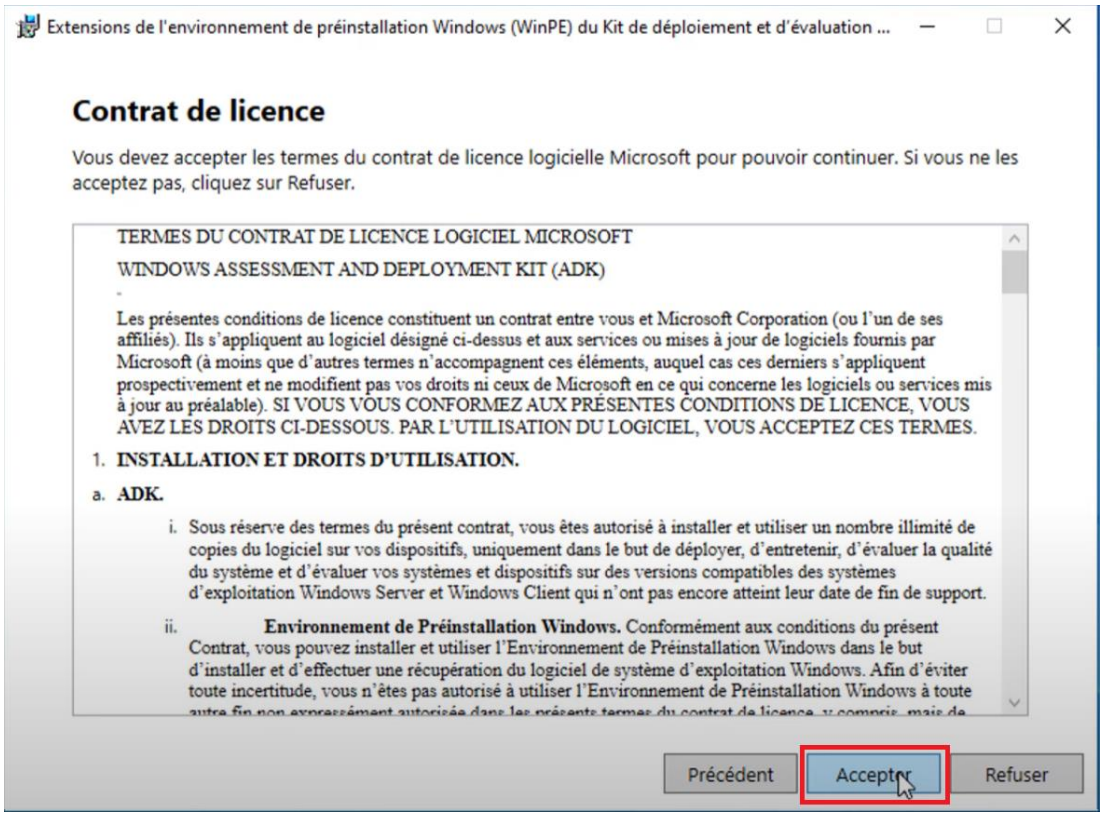
11. Cliquer sur « Suivant »



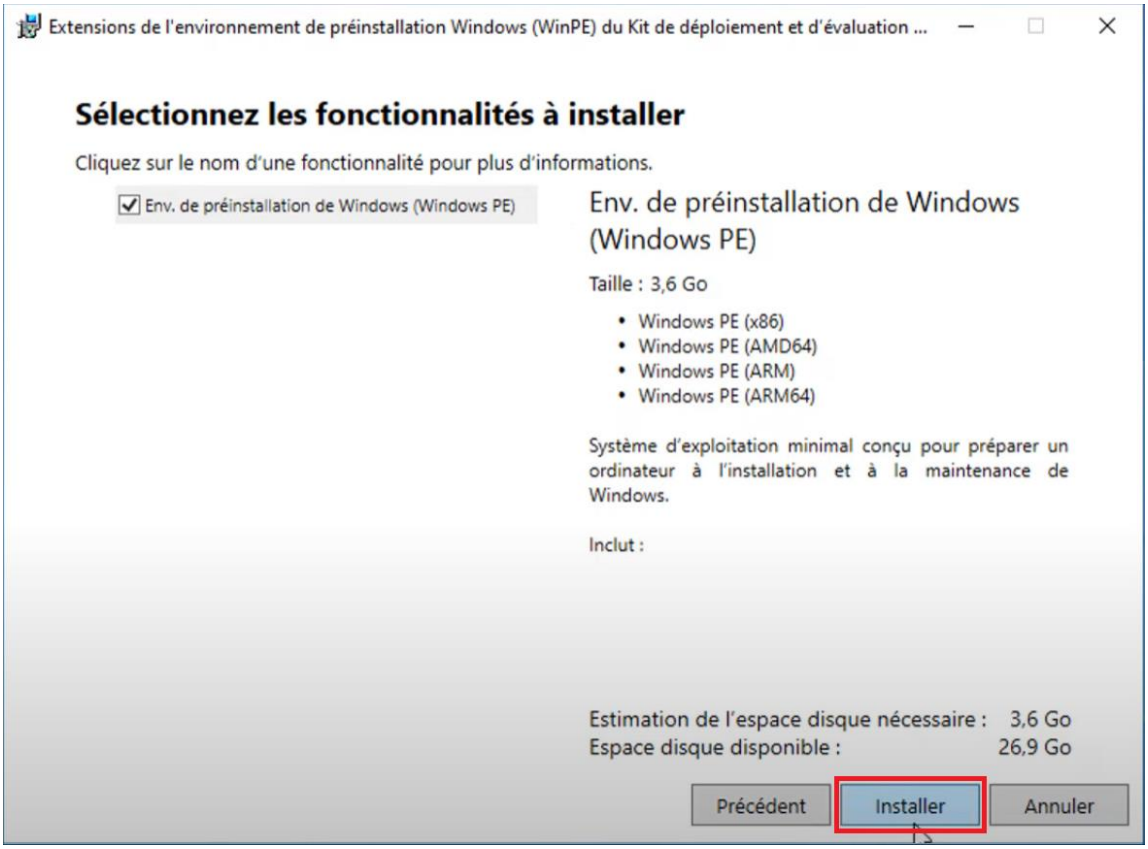
12. Cliquer sur « Non » et « Suivant »



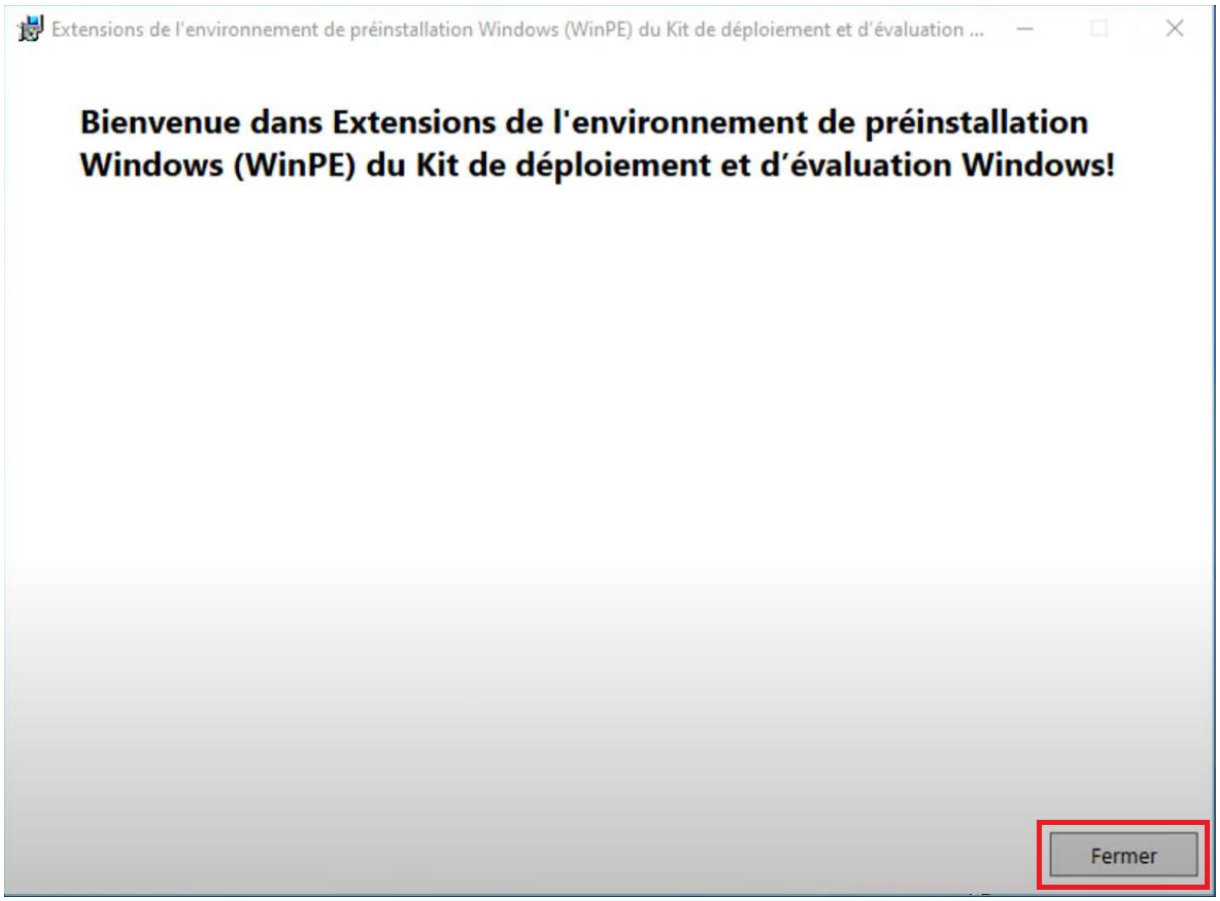
13. Accepter le contrat de licence



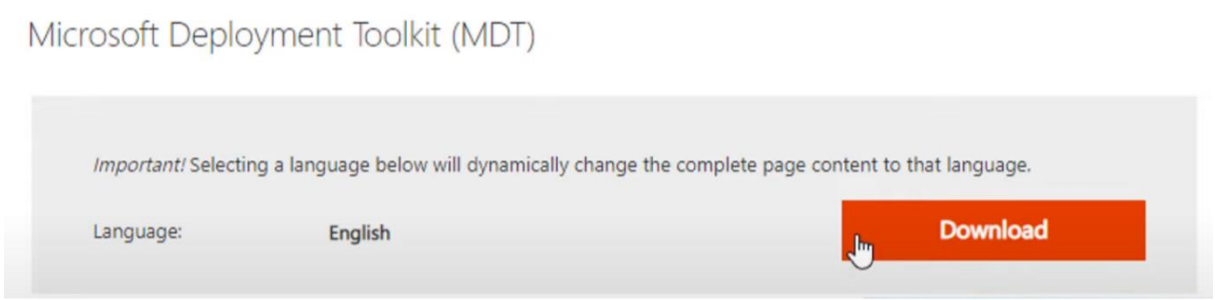
14. Puis cliquer sur installer



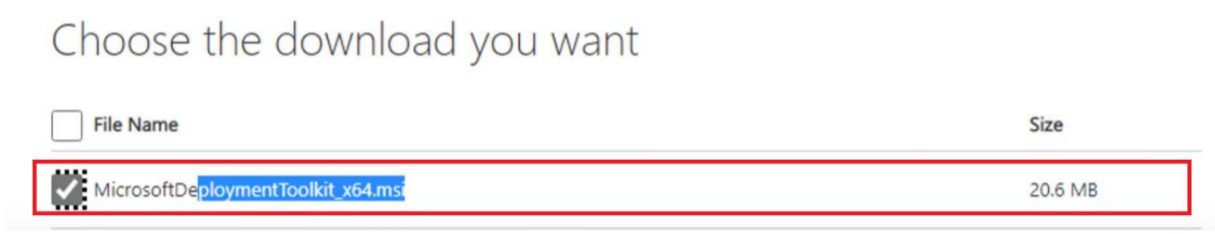
15. Une fois l'installation terminée, Cliquer sur Fermer



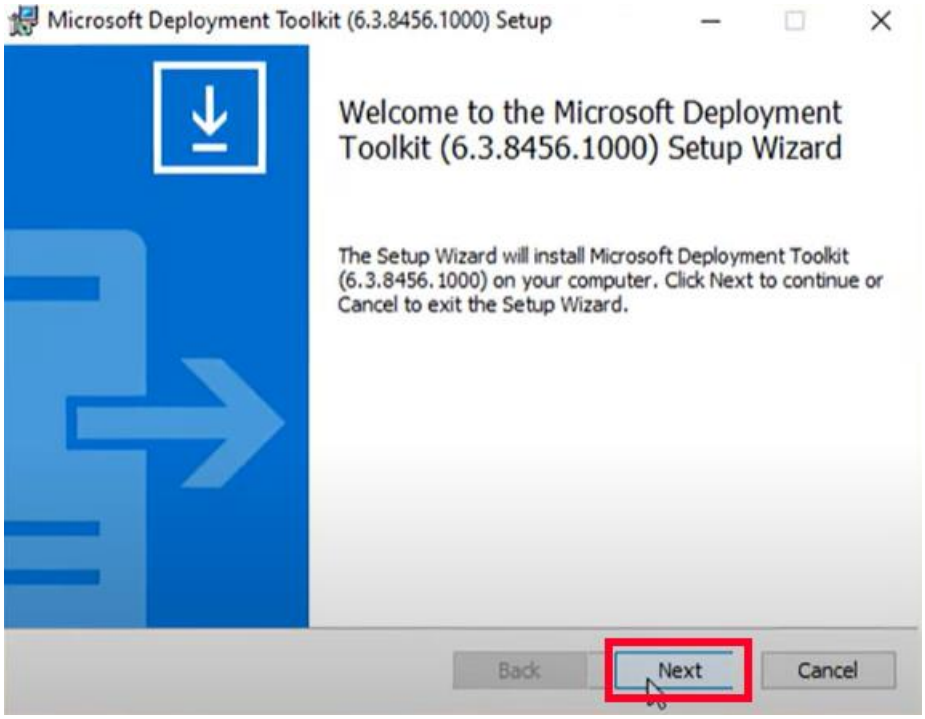
16. On va ensuite télécharger les fichiers nécessaires au MDT



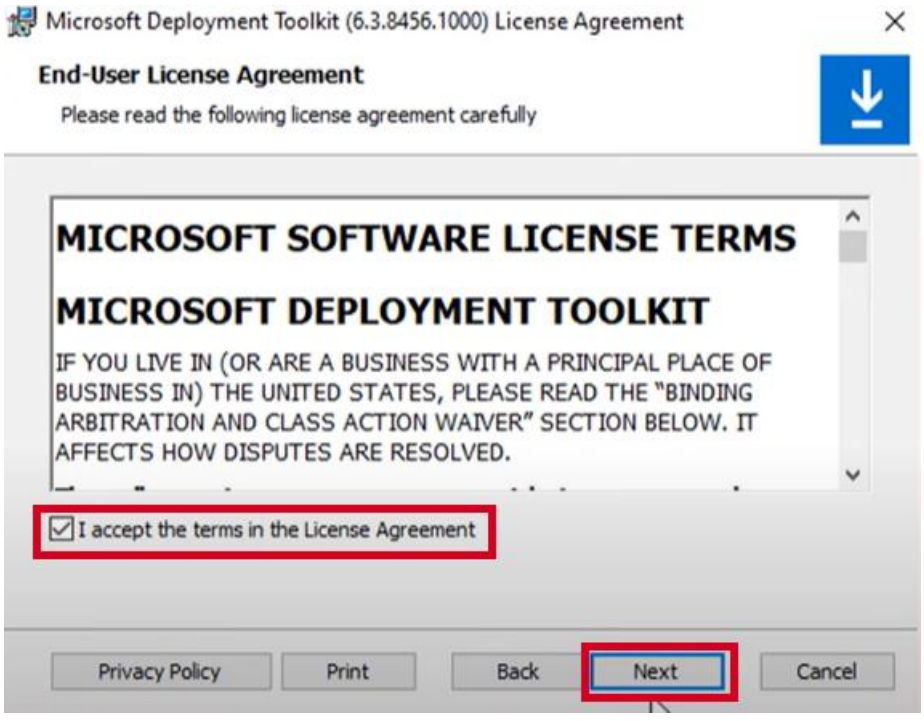
17. Bien choisir la version x64 et exécuter le .msi



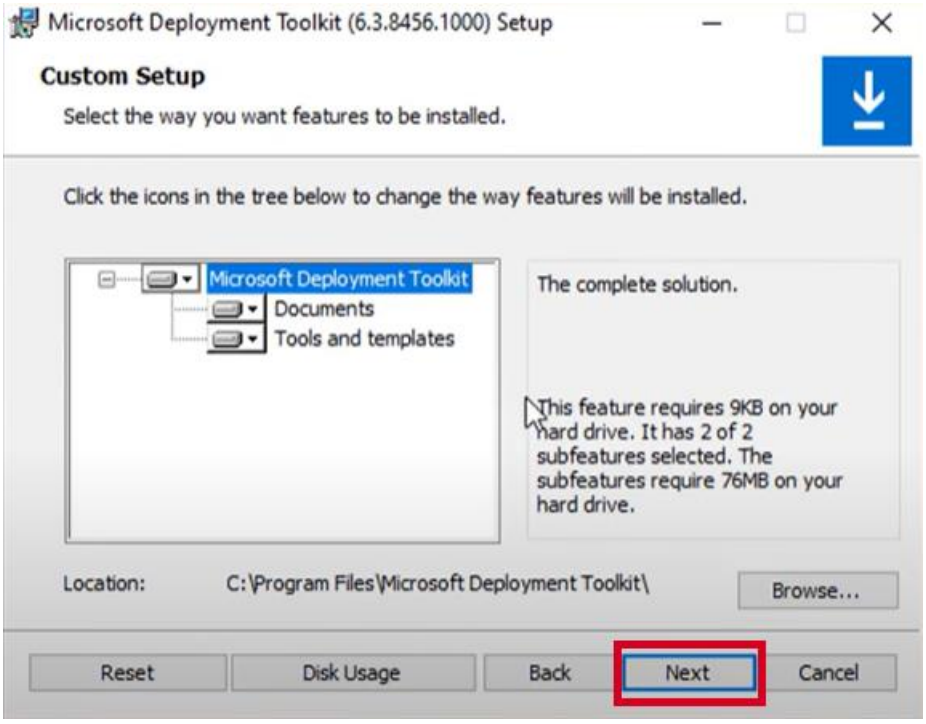
18. Cliquer sur « Next »



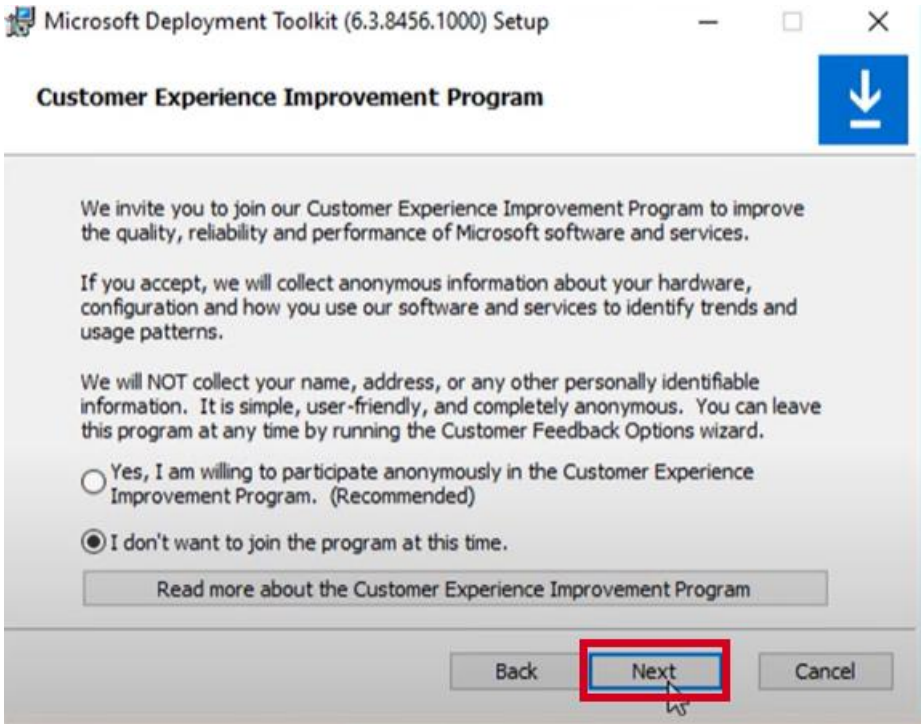
19. Accepter le contact de licence et Cliquer sur « Next »



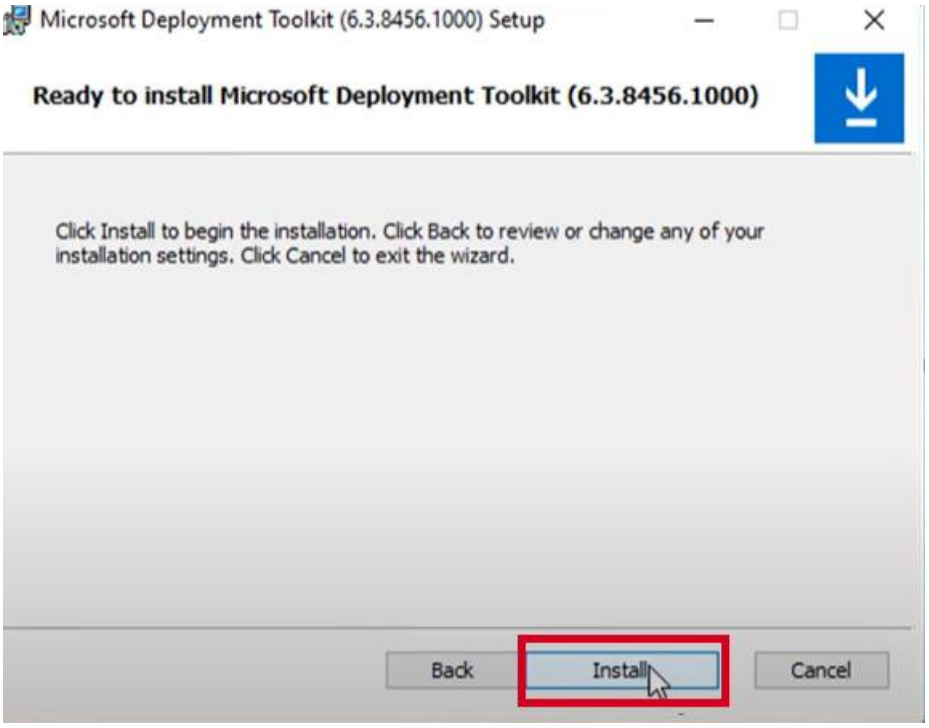
20. Cliquer sur Next



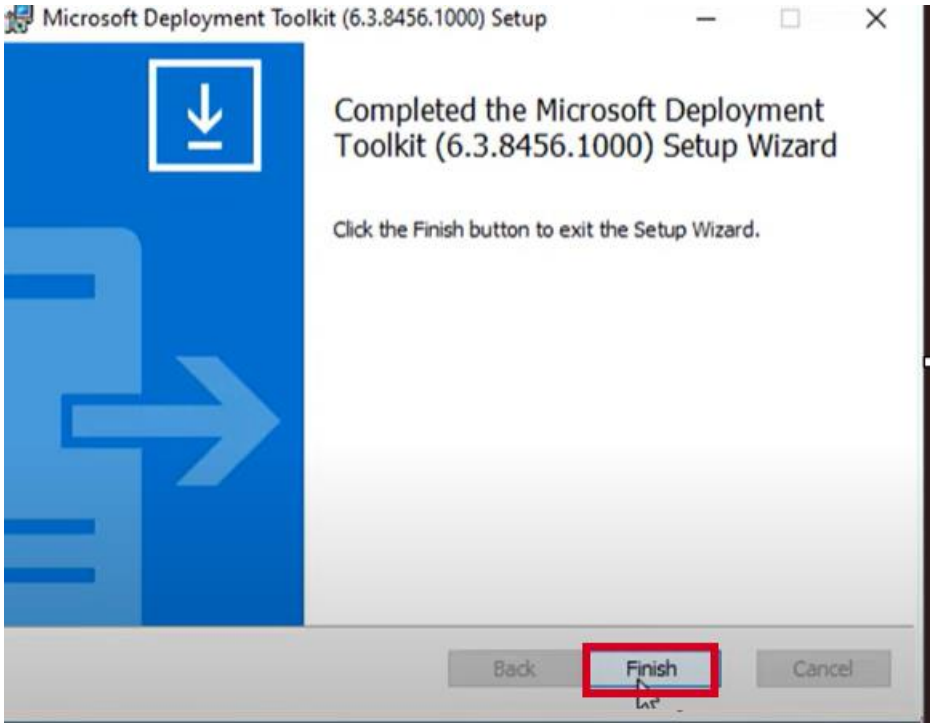
21. Cliquer sur Next



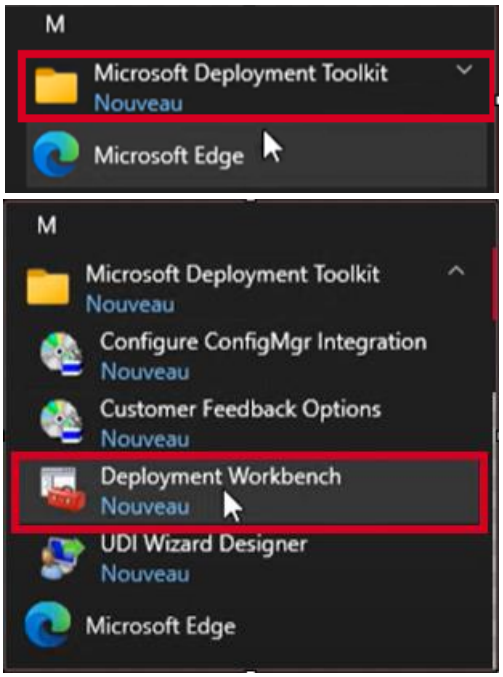
22. Puis « Install »



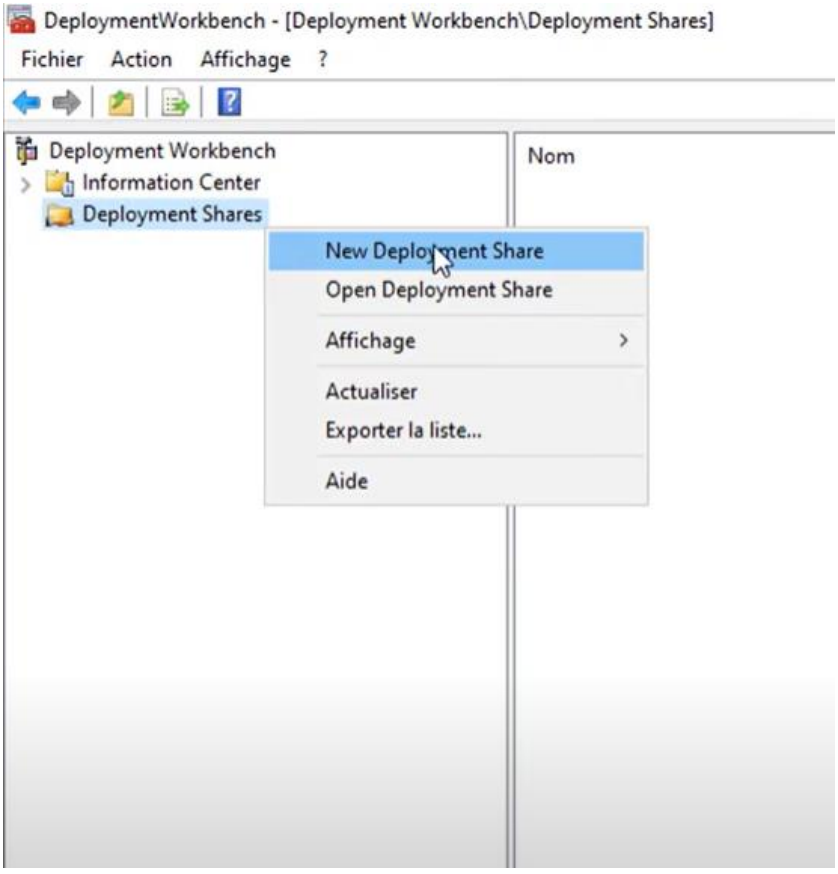
23. Enfin cliquer sur « Finish » pour finir l'installation



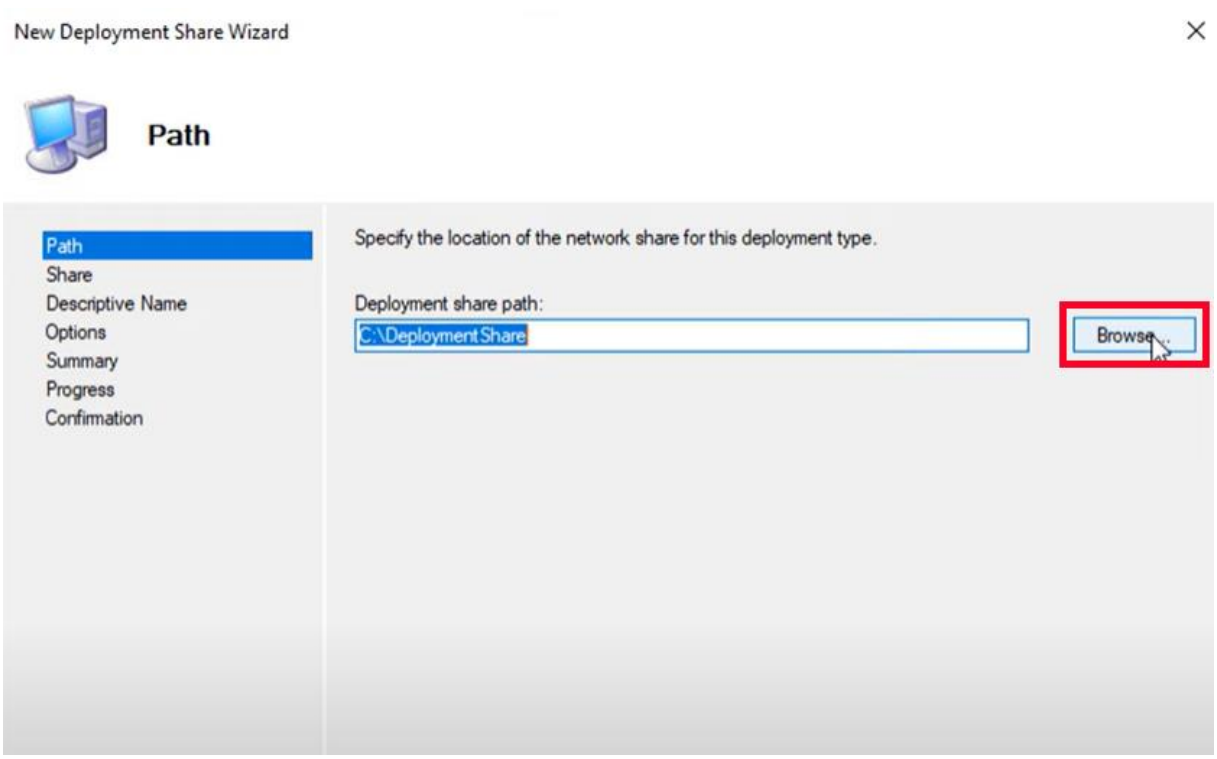
24. Dans le menu démarrer trouver le dossier « Microsoft Deployement Toolkit » puis ouvrir le Deployement Workbench, qui nous permettra de faire toute la configuration de MDT



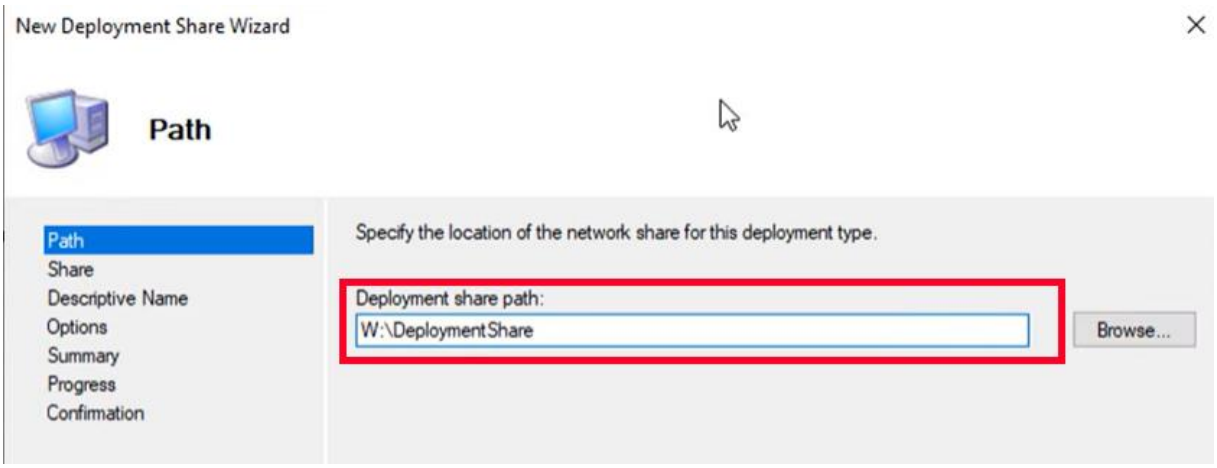
25. On crée un nouveau Deployement Share, c'est un dossier qui va contenir les éléments de notre image MDT et sera déployé sur les PC.



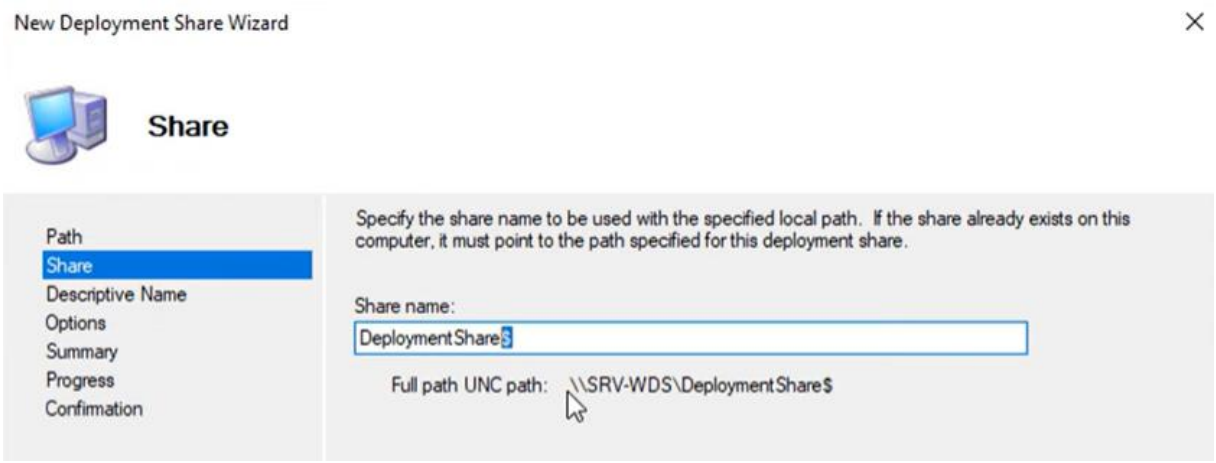
26. Il est recommandé de stocker les données sur une partition dédiée, on va choisir la même partition que celle où l'on stocke les fichiers de WDS.



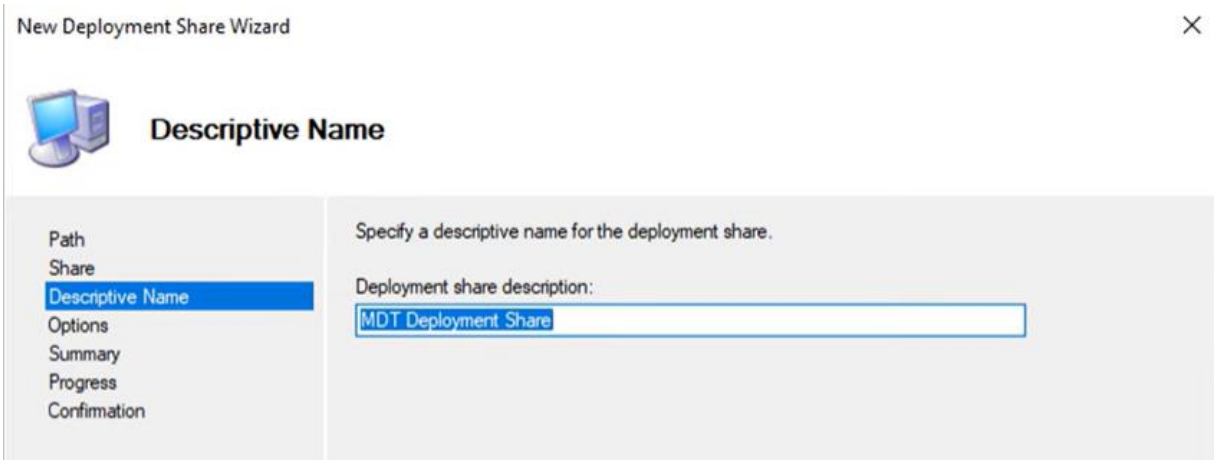
27. Puis on va donner un nom a notre dossier pour que tout ne soit pas à la racine et on Cliquer sur Next



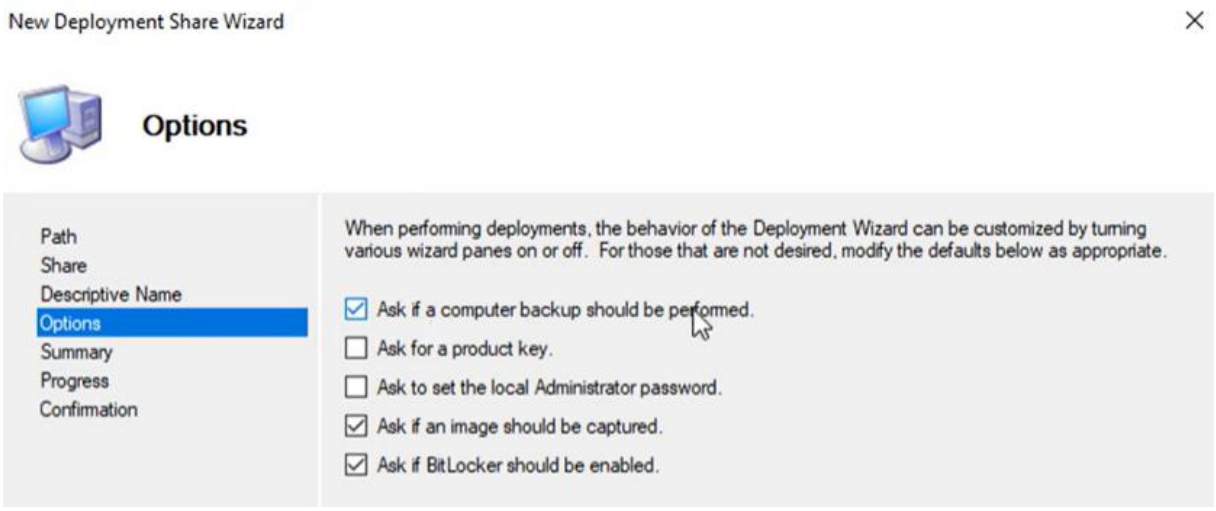
28. Ici on choisit le nom du chemin pour accéder au partage (le $ a la fin sert à le masquer sur le réseau) puis on clique sur « Next ».



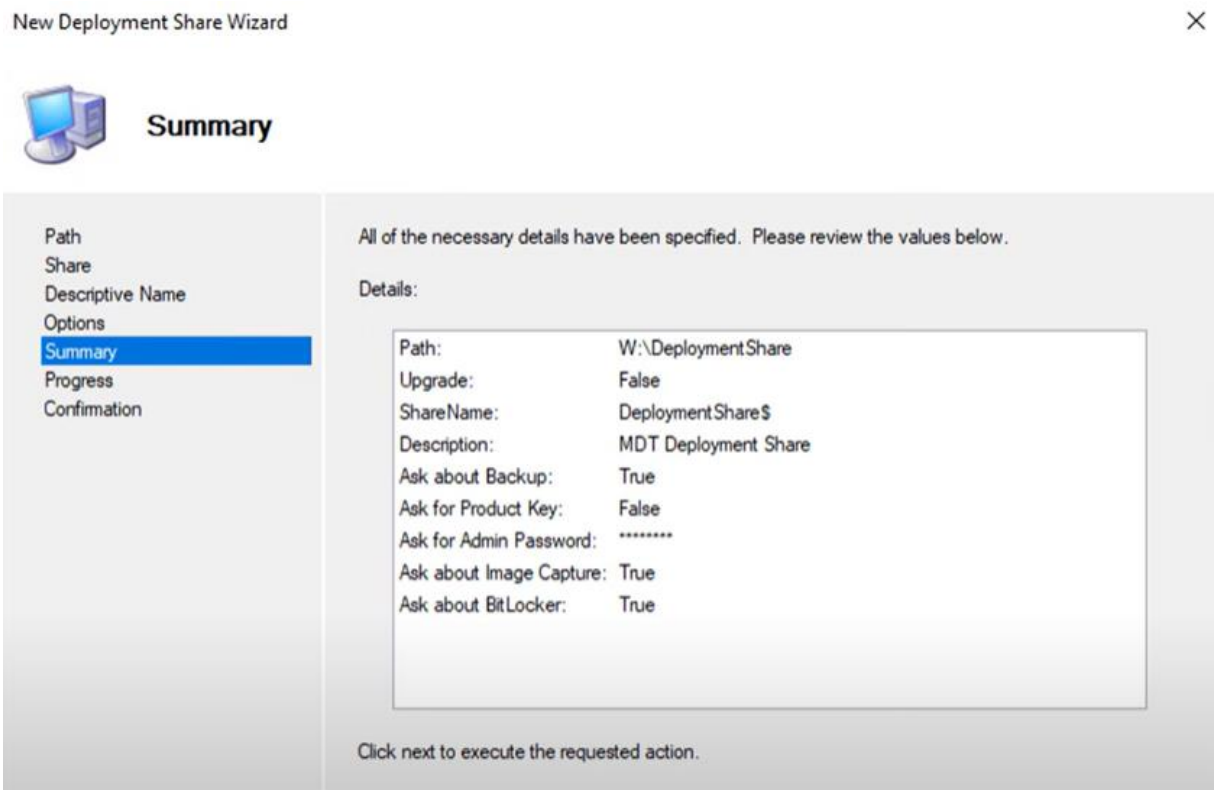
29. On peut changer la description, ici nous n'allons pas le faire.



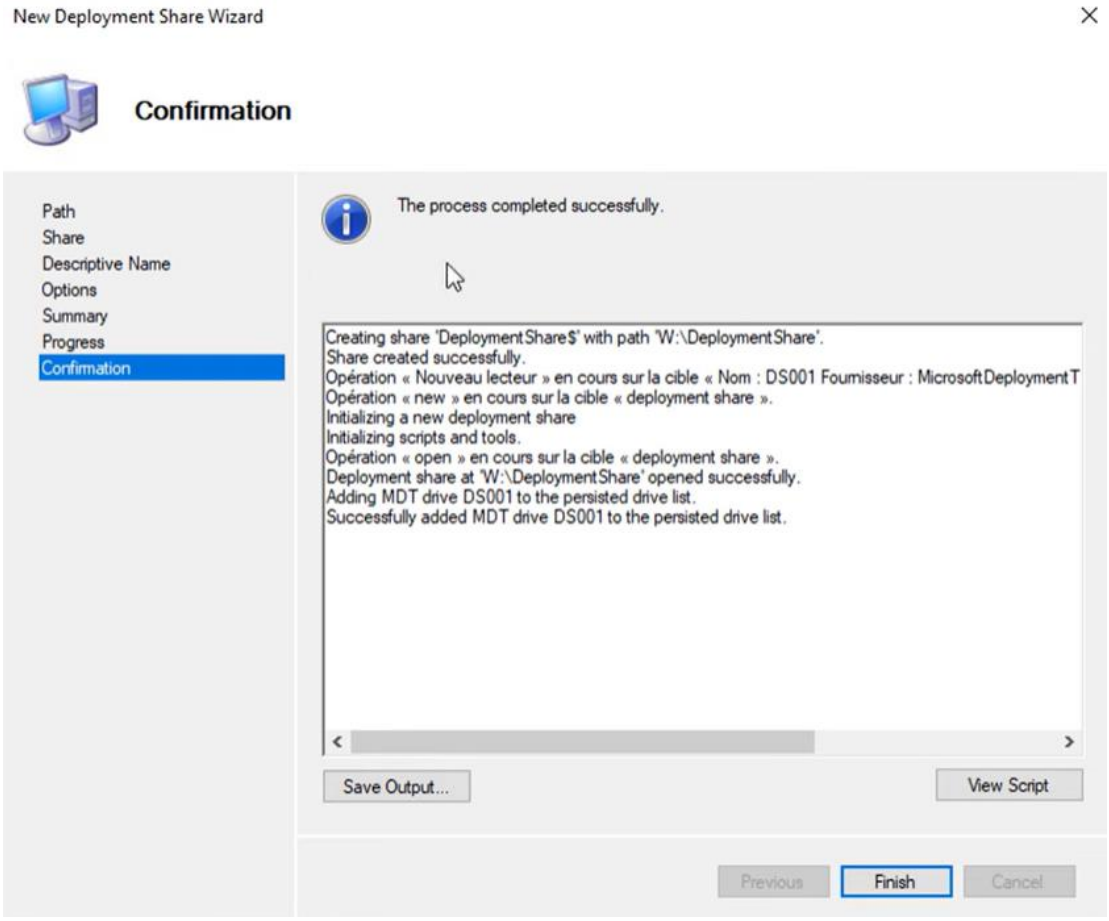
30. Ici on obtient des options pour compléter le déploiement on laisse par défaut. Cliquer sur Next (les options peuvent être changés par la suite).



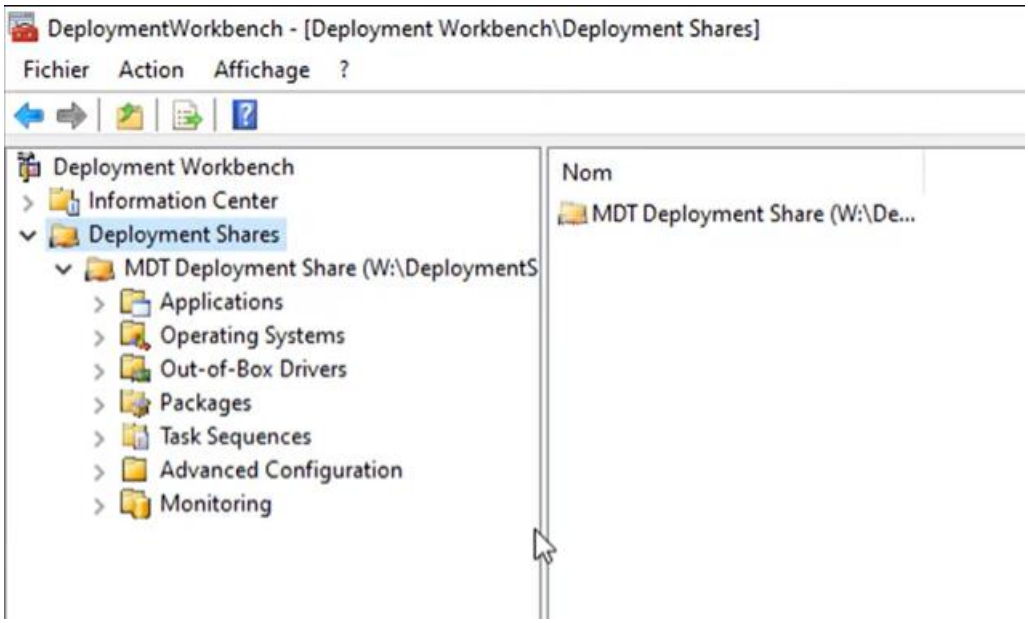
31. Ensuite un récapitulatif est fourni.



32. Une fois la configuration finie, on peut cliquer sur Finish

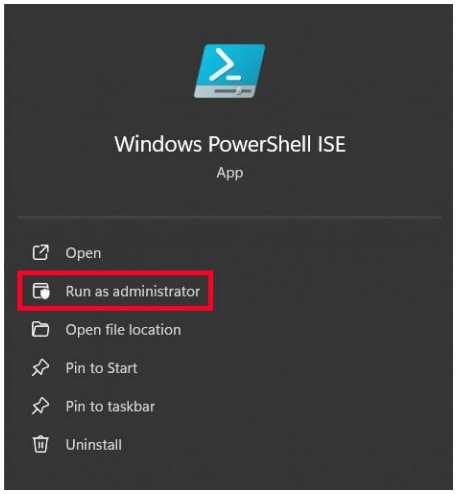


33. MDT Deployment Share apparaît maintenant.



On va maintenant créer un utilisateur qui aura les droits de lecture sur le Deployment Share.

34. Ouvrir un ISE PowerShell.



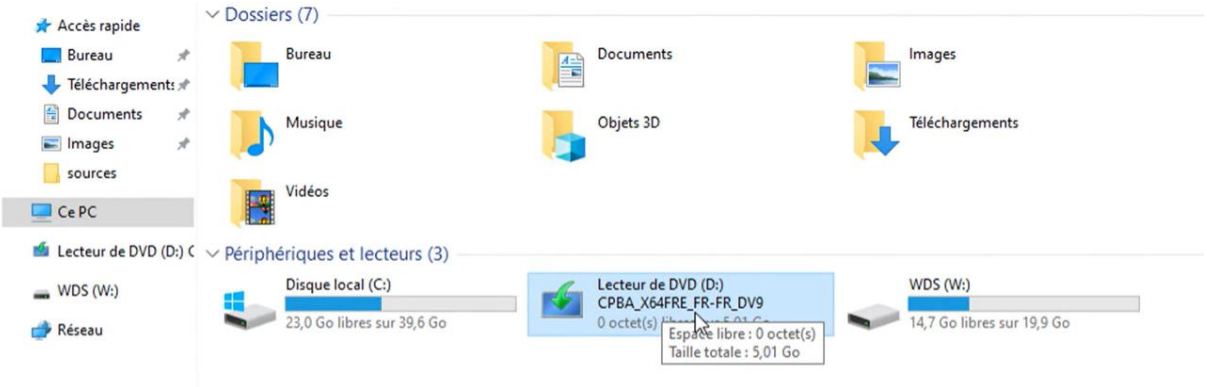
35. À la suite de l'exécution de ce script, l'utilisateur « Service_MDT » est bien créé.

```
# Spécifier le nom et le mot de passe du compte de service
$ServiceAccountName = "Service_MDT"
$ServiceAccountPassword = ConvertTo-SecureString "P@ssword123!" -AsPlainText -Force

# Créer le compte local
New-LocalUser $ServiceAccountName -Password $ServiceAccountPassword -FullName "MDT" -Description "Compte de service pour MDT"

# Ajouter les droits en lecture sur le partage
Grant-SmbShareAccess -Name "DeploymentShare$" -AccountName "Service_MDT" -AccessRight Read -Force

# Attribuer au compte de service les permissions nécessaires pour accéder aux fichiers de déploiement MDT
$MDTSharePath = "\\ASSURDEPLOY\DeploymentShare$"
$Acl = Get-Acl $MDTSharePath
$Rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Service_MDT","ReadAndExecute", "ContainerInherit, ObjectInherit", "None", "Allow")
$Acl.SetAccessRule($Rule)
Set-Acl $MDTSharePath $Acl
```

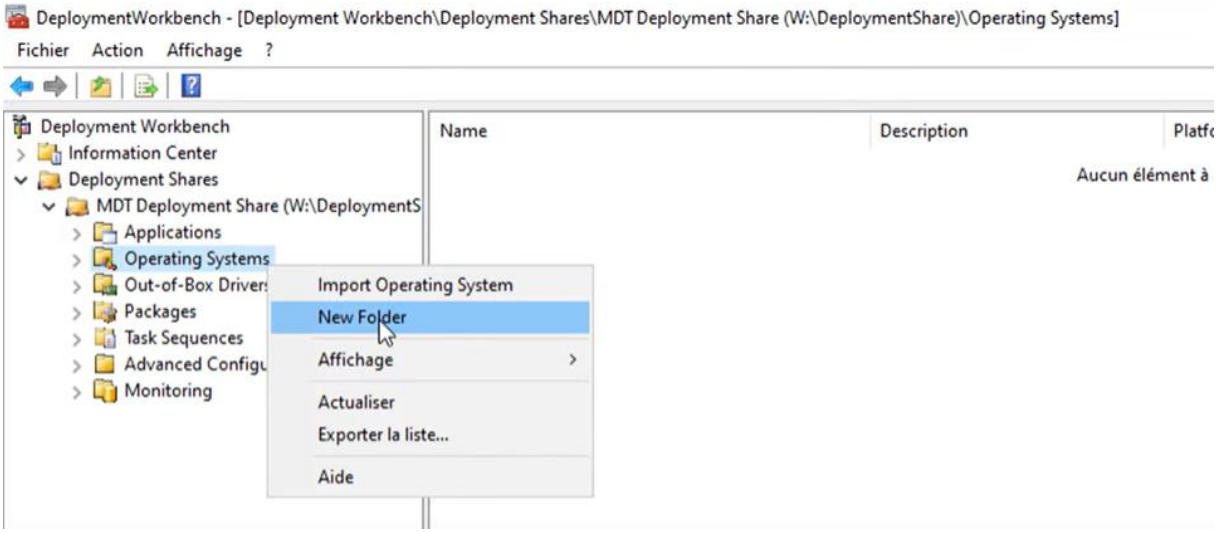
On va importer une image ISO Windows 11 dans le Deployement Share pour pouvoir la descendre sur nos machines par la suite.

36. Après avoir téléchargé une ISO Windows 11 on se rend à son emplacement dans nos fichiers, et on double clic dessus pour la monter comme un DVD.

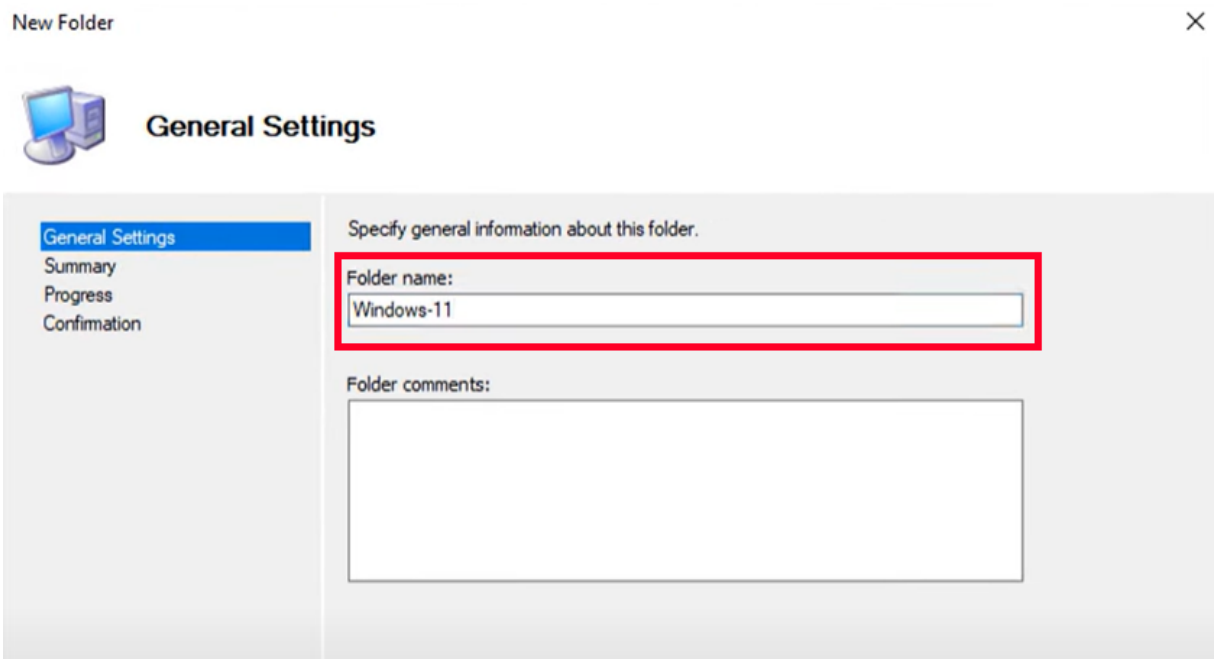
37. On retrouve le lecteur ou l'ISO est monté avec nos autres disques



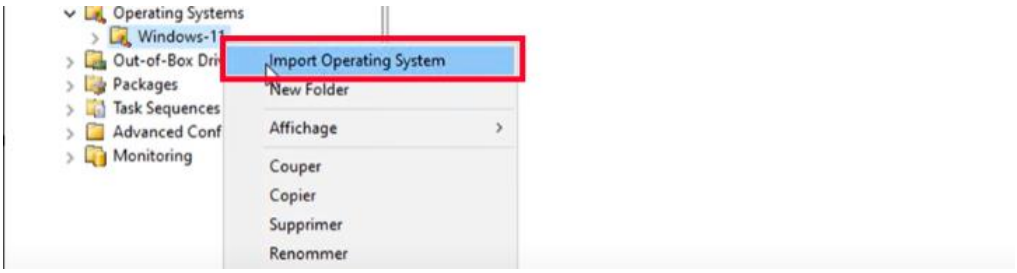
38. De retour sur le DeployementWorkbench on va créer un nouveau dossier pour organiser nos images.



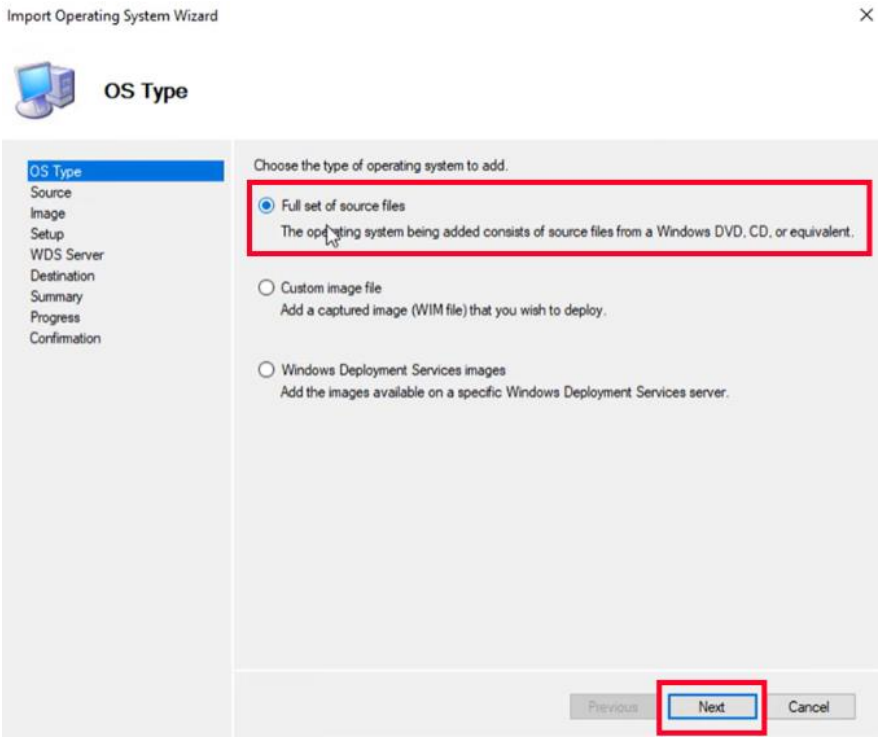
39. On lui donne comme nom Windows 11 et on finit la création du dossier.



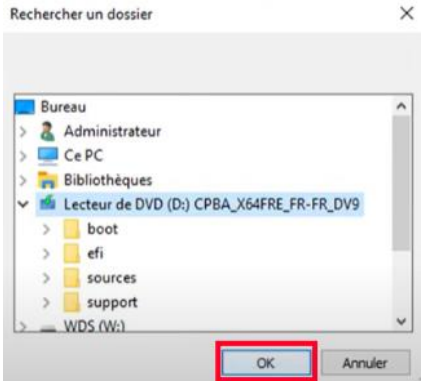
40. Dans le dossier maintenant crée on peut « Import Operating System »



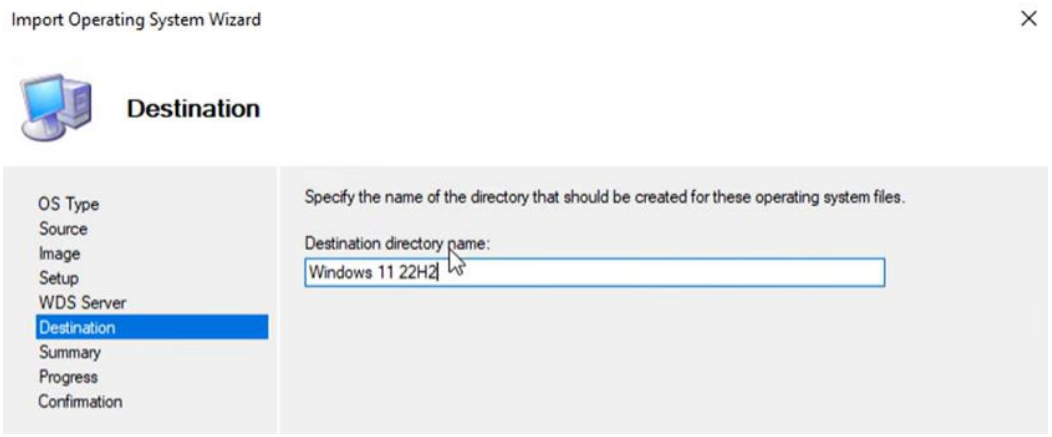
41. On choisit le premier car notre ISO est monté comme un CD\DVD…

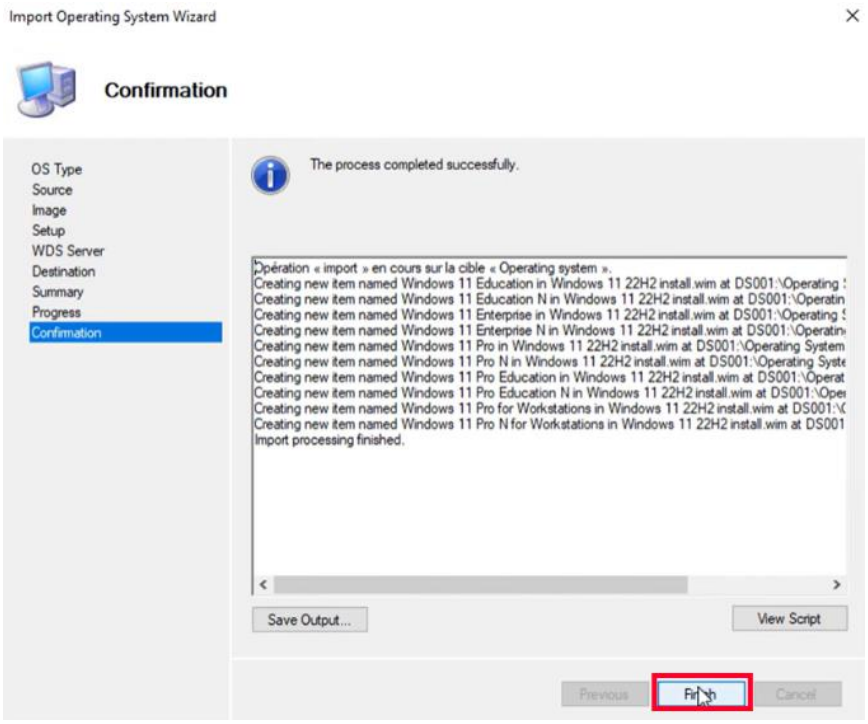


42. On choisit bien notre ISO, puis « OK ». Cliquer sur Next.

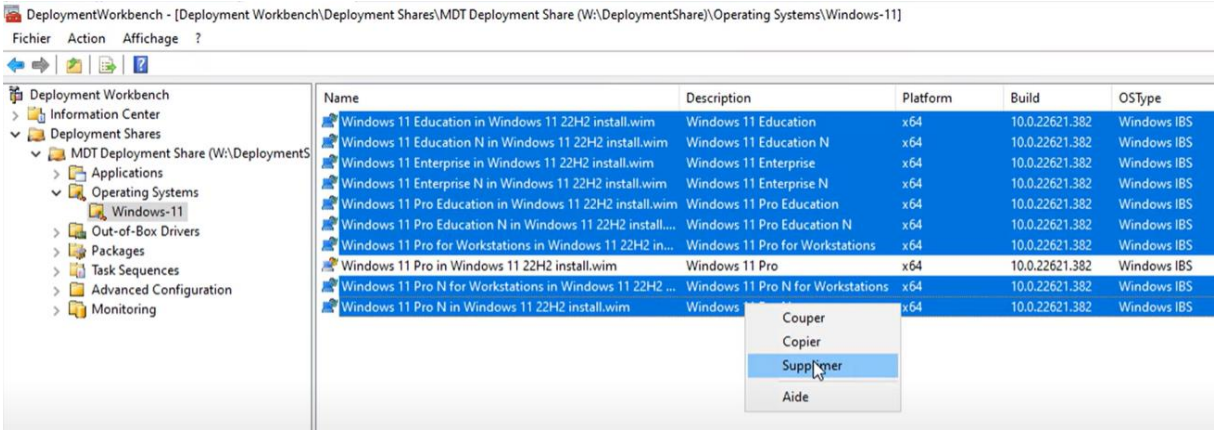


43. L'image détecté est bien du Windows 11. On la renomme Windows 11 22H2 puis on finit l'installation jusqu'à la fin.

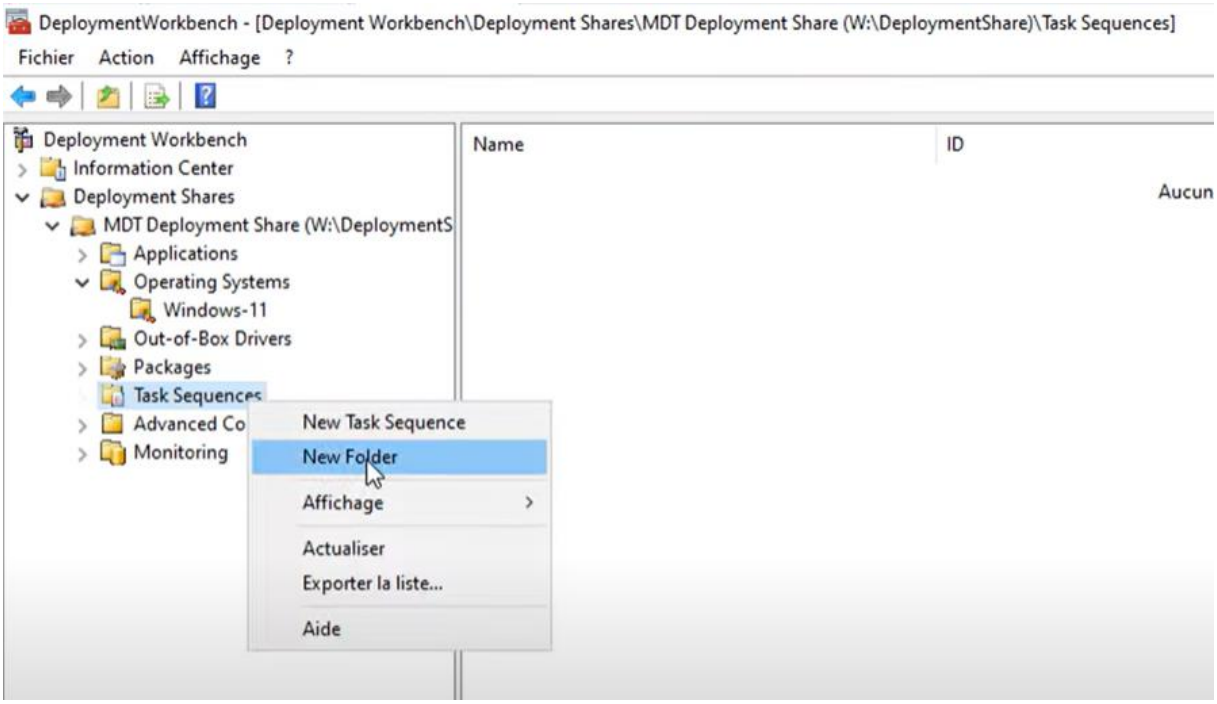




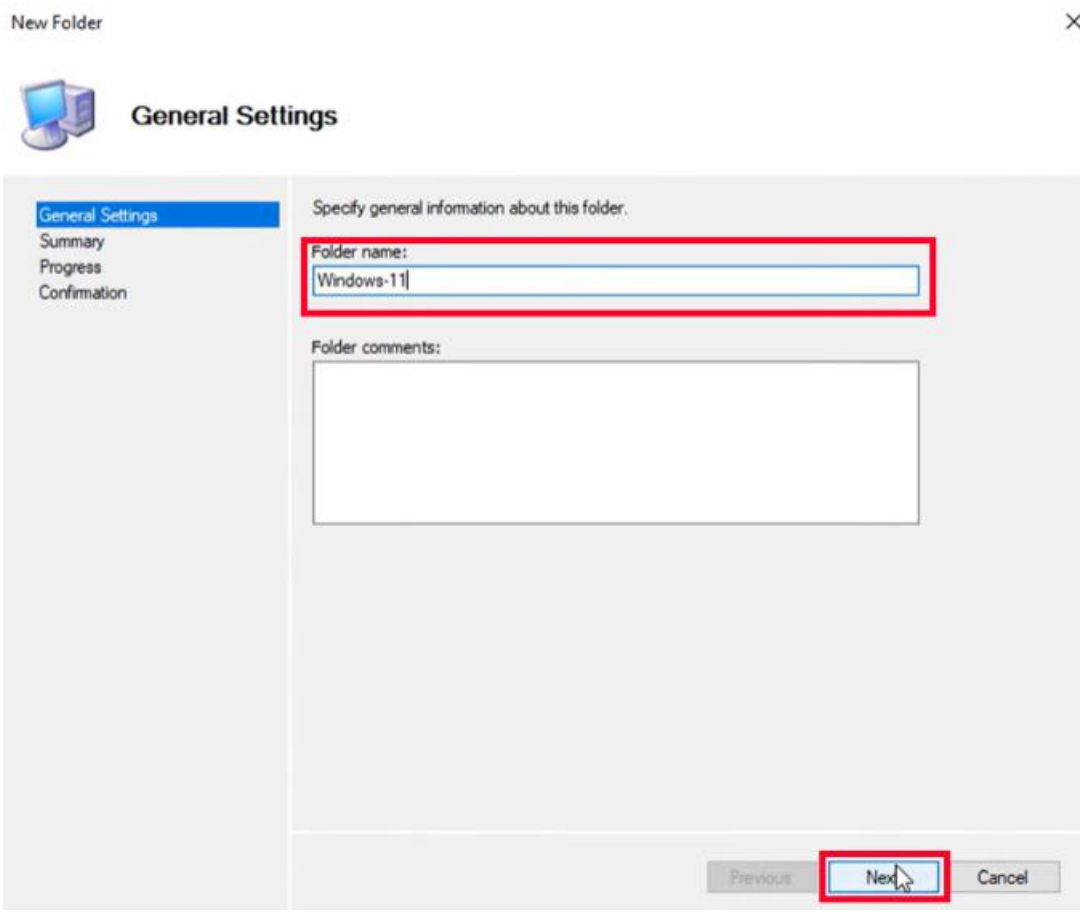
44. De retour sur le DeployementToolkit on peut voir que toutes les versions de Windows sont présentes. On supprime les inutiles.



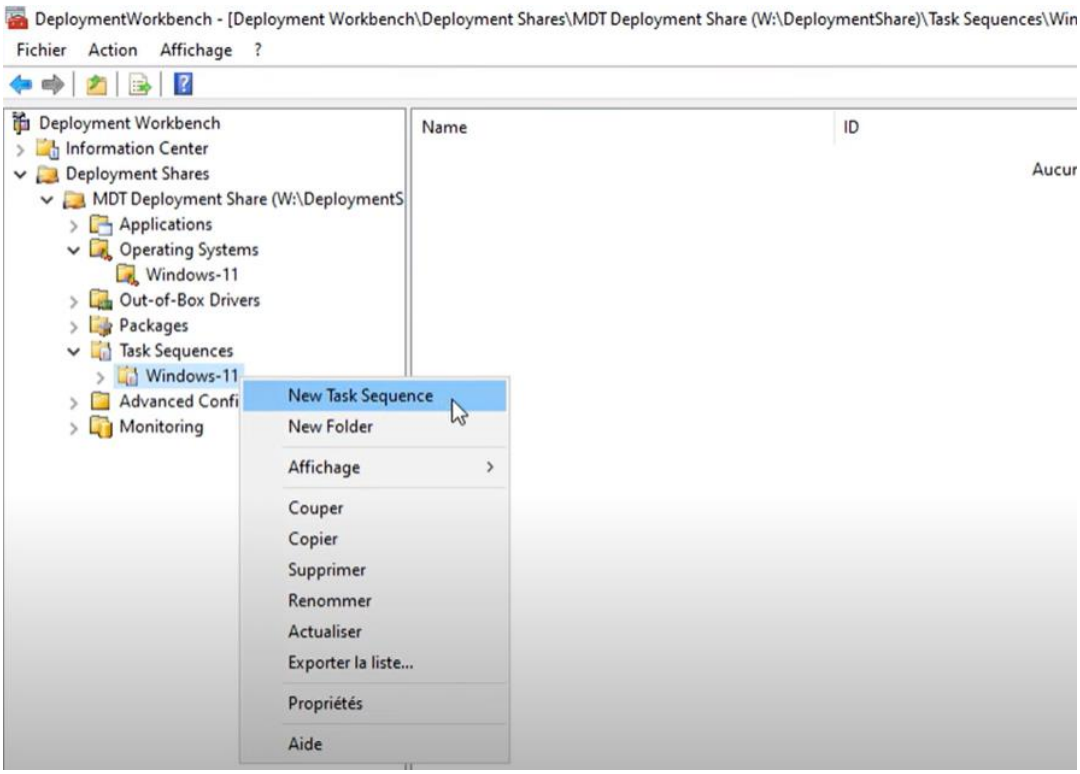
45. Dans Task Sequence on va créer un nouveau dossier de séquence de tâche qui permettra de faire plusieurs versions d'initialisation de déploiement (par exemple, une version de Windows précise en cas de besoin).



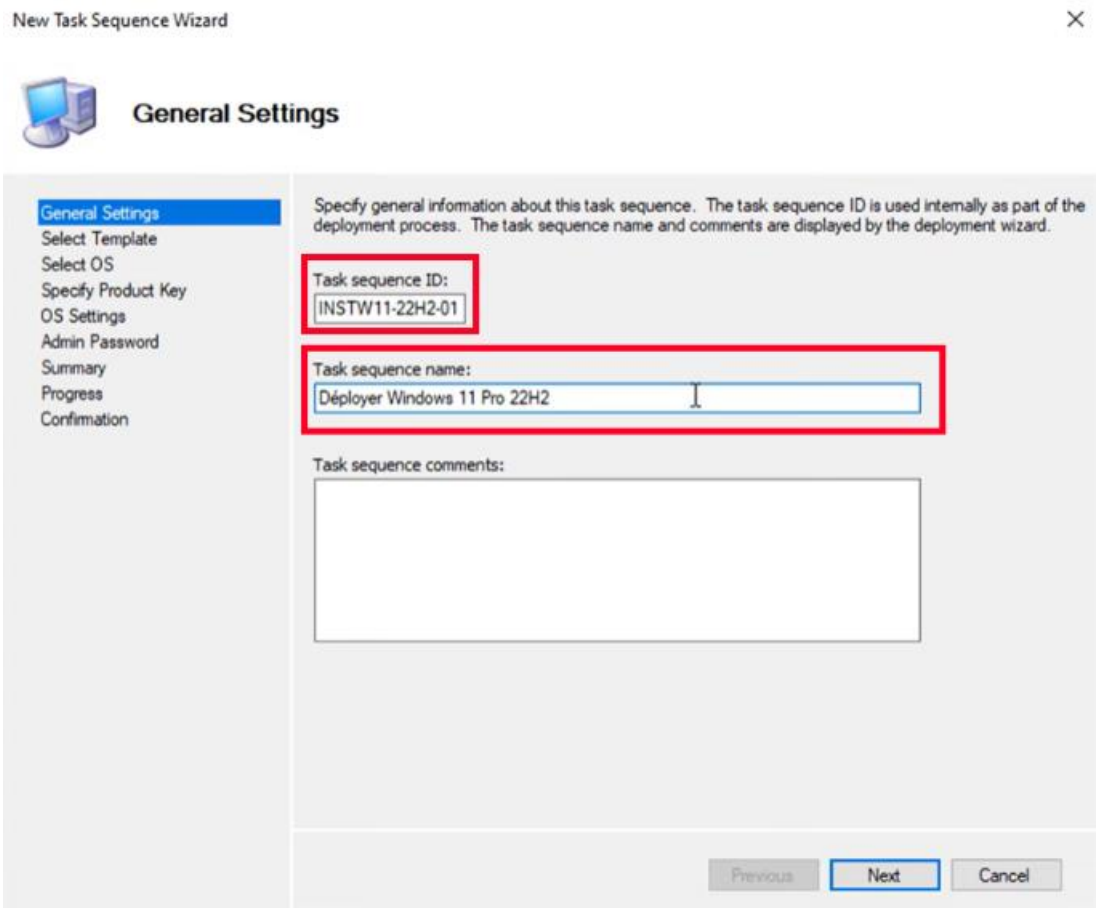
46. Après avoir donné le nom du dossier, Cliquer sur suivant jusqu'à créer celui-ci.



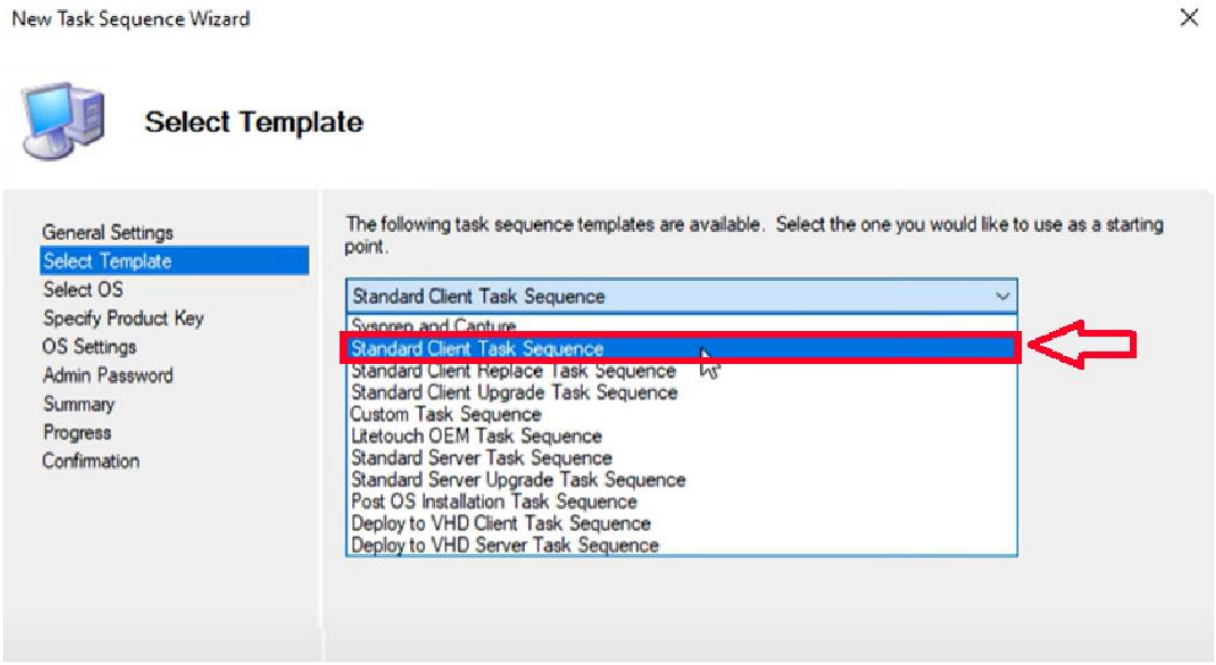
47. On fait un clic droit, et on fait notre nouvelle séquence de tâches



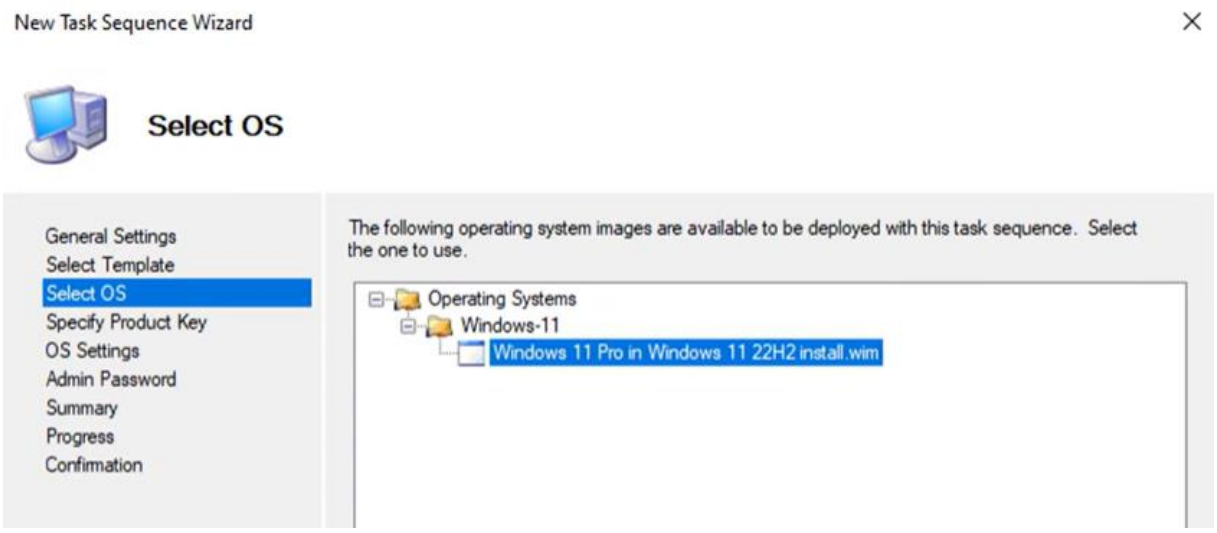
48. L'assistant apparait et on doit entrer un ID et un nom pour notre séquence ici INSTW11-22H2-01 (nom indiquant la version de Windows, sa version et la version de la Task Sequence (ici, 01)), et « Déployer Windows 11 Pro 22H2 » qui s'affichera dans le MDT.



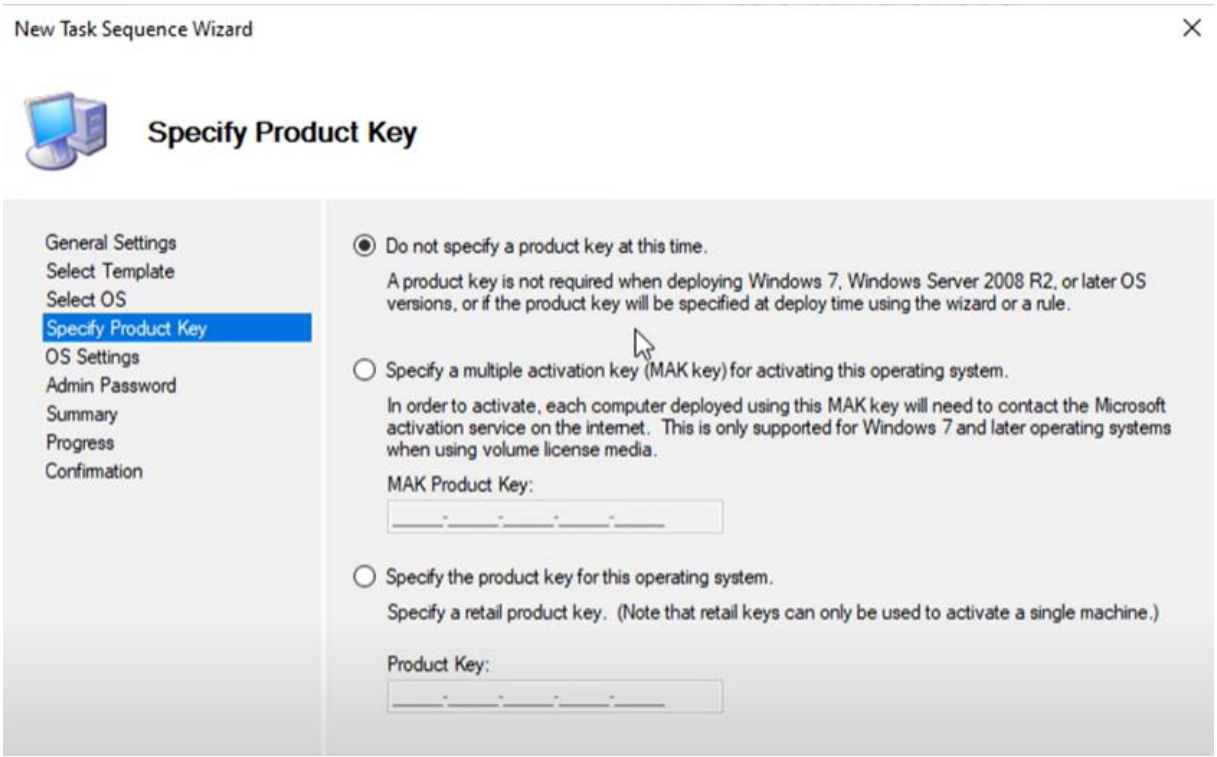
49. On choisit un template pour aider à la configuration, ici le standard.



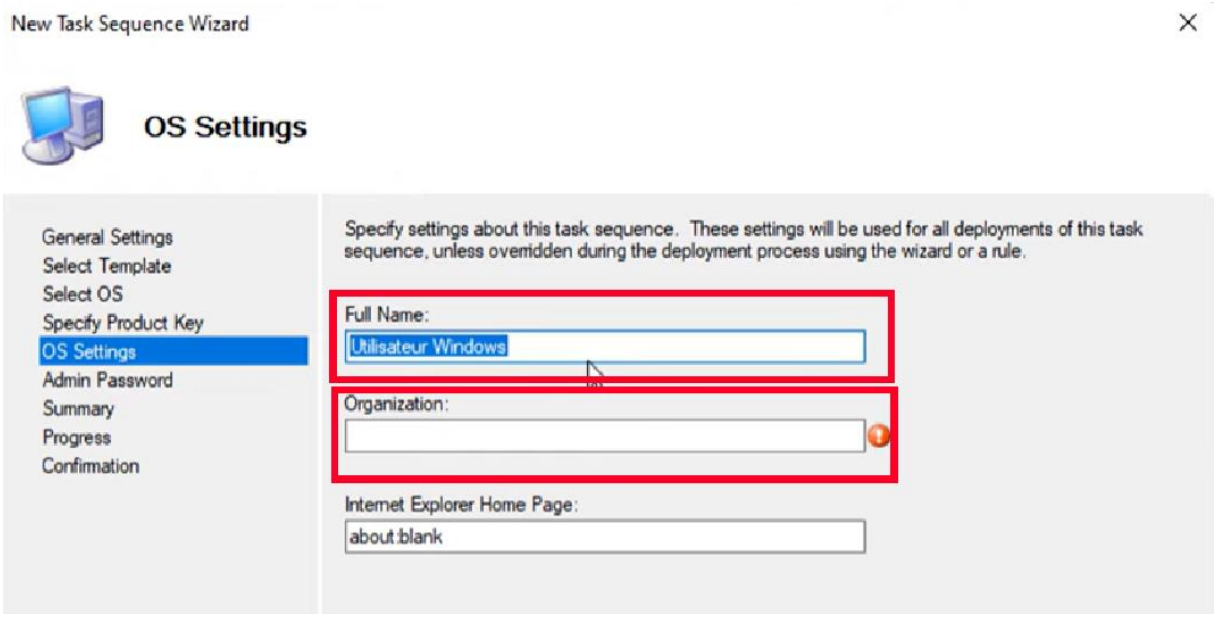
50. Ensuite on choisit l'image que l'on veut utiliser dans cette séquence puis on clique sur Next



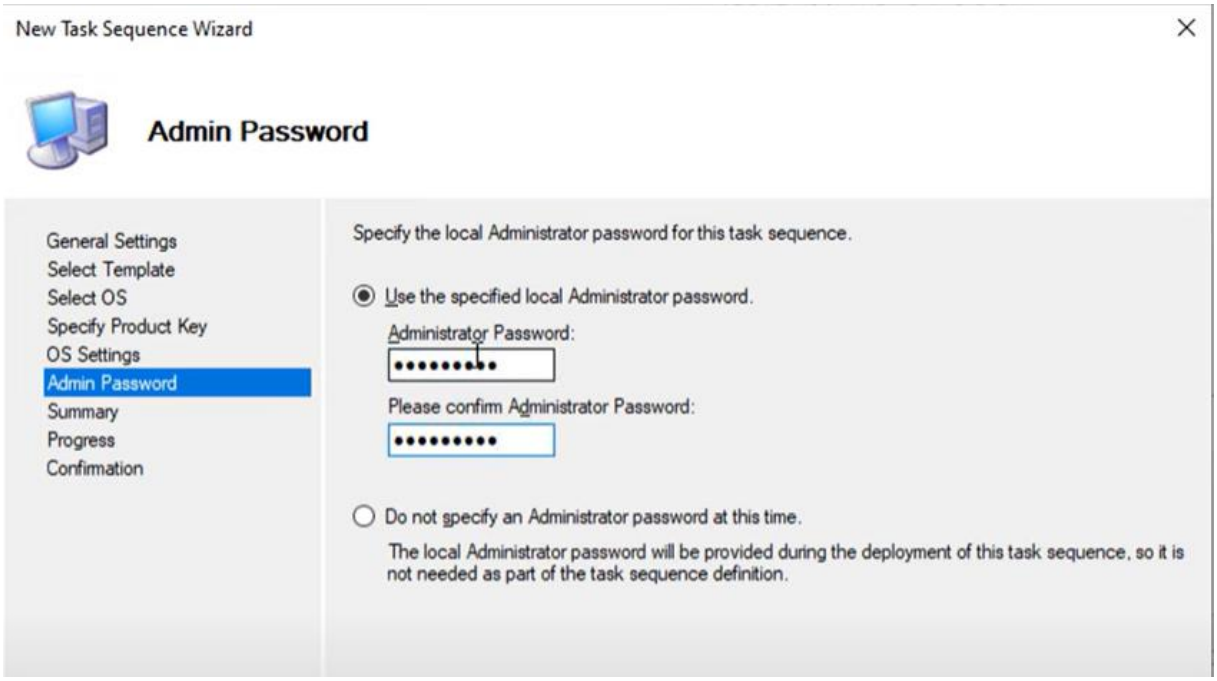
51. Ensuite on choisit si l'on veut déployer avec une clé d'activation ou pas dans notre cas, après la configuration initiale un technicien s'occuperas d'activer les Windows ***(Nous mettrons plus tard en place une clé produit de volume que l'on déploiera via Key Management Service),*** puis cliquer sur « Next ».



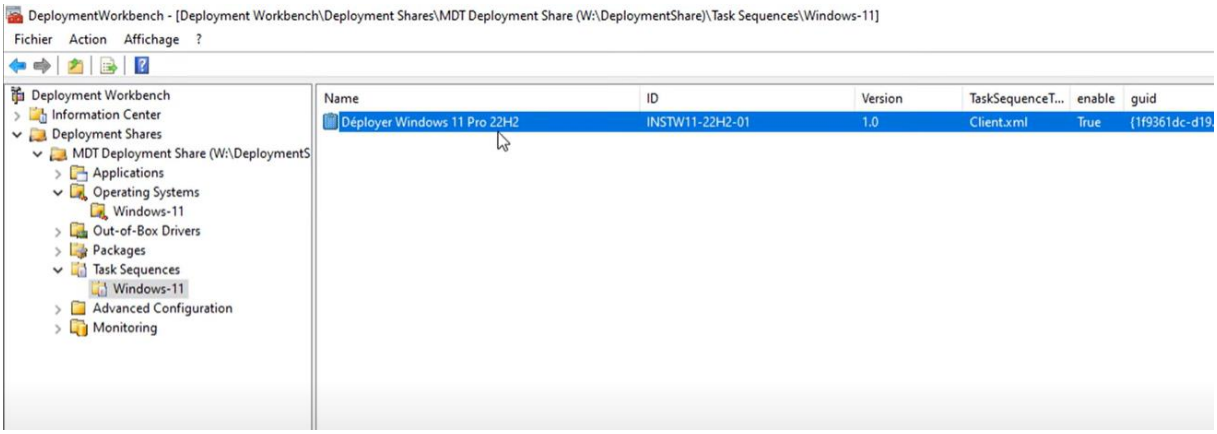
52. Dans la suite on rentre le nom de l'Utilisateur local que MDT va créer, ici on va entrer « Administrateur » et ASSURMER dans notre Organisation, ensuite on clique sur « Next »



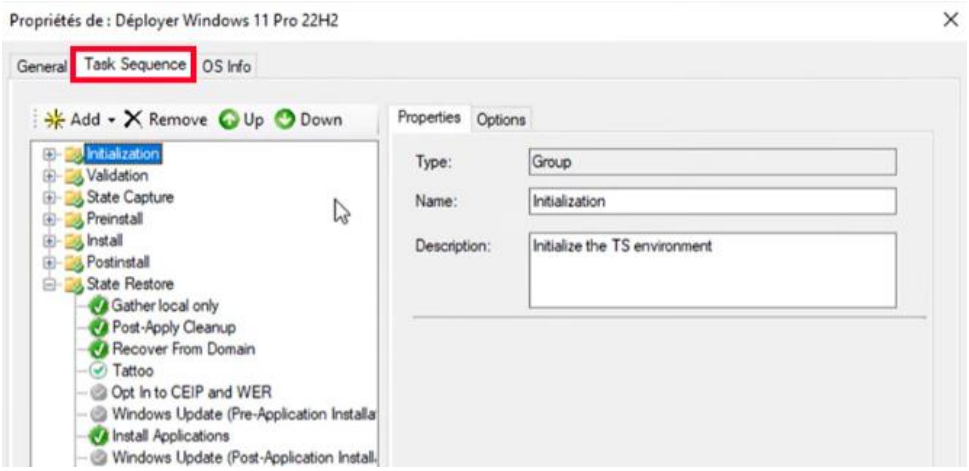
53. On entre le mot de passe de l'admin local, qui doit être robuste, puis on finit notre séquence de tâches.



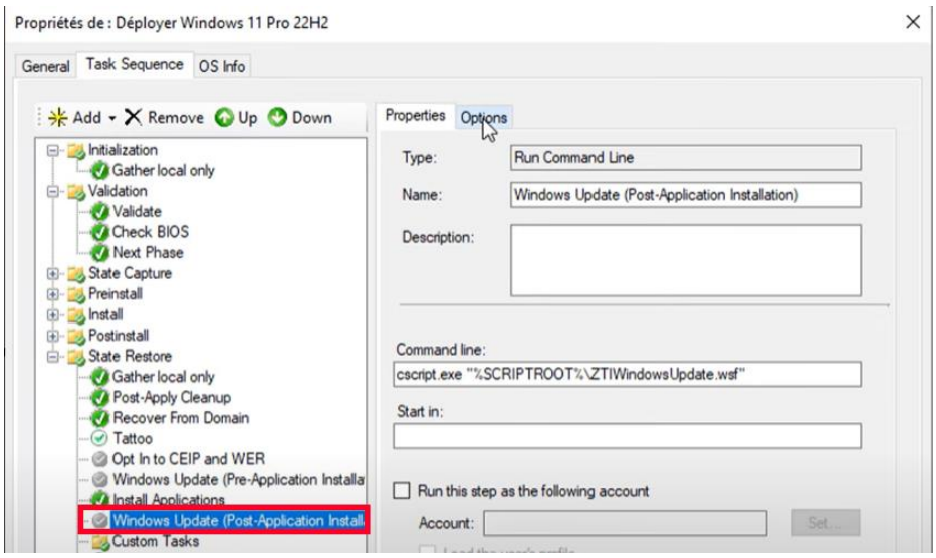
54. La tâche est bien créée.



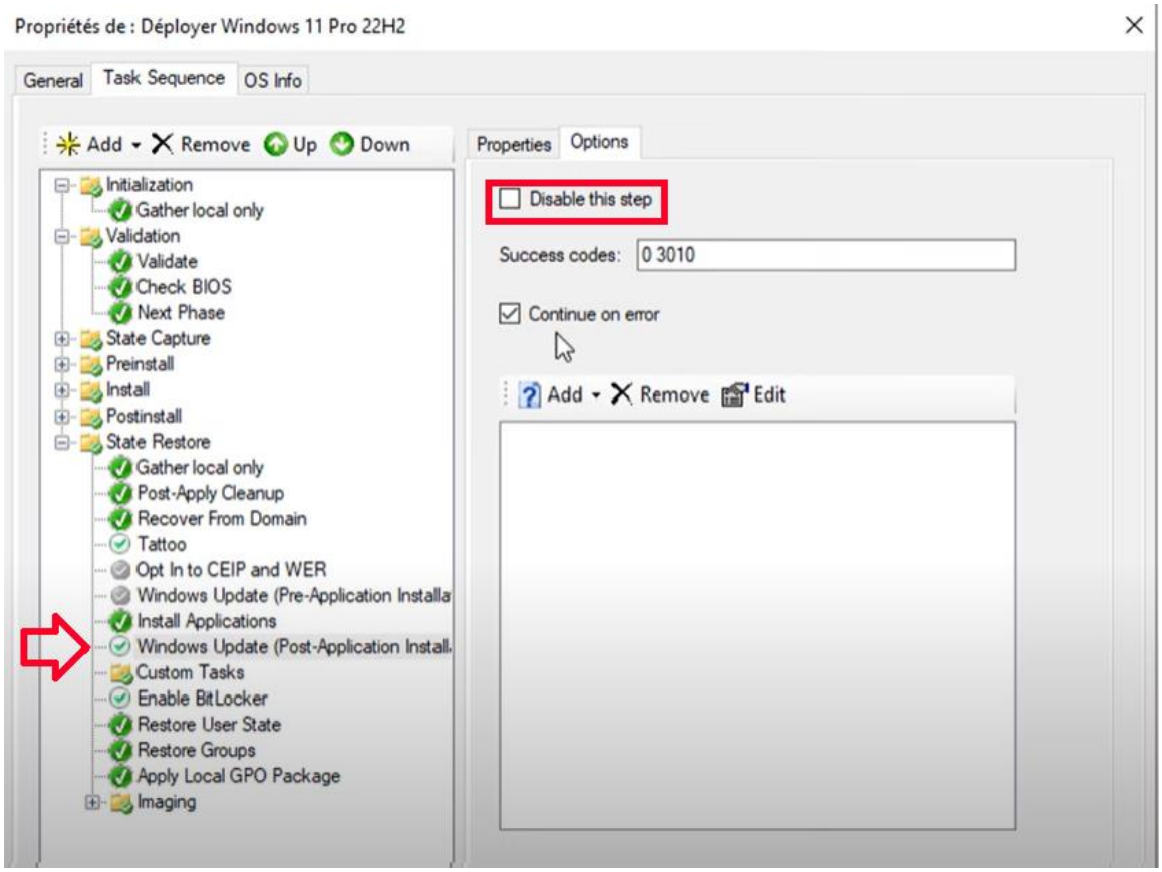
55. En faisant clic droit puis Propriétés et ensuite aller dans l'onglet « Task Sequence », on peut avoir accès à toutes les étapes de notre déploiement.



56. Il faut activer Windows Update. On clique dessus dans la liste, puis dans options.

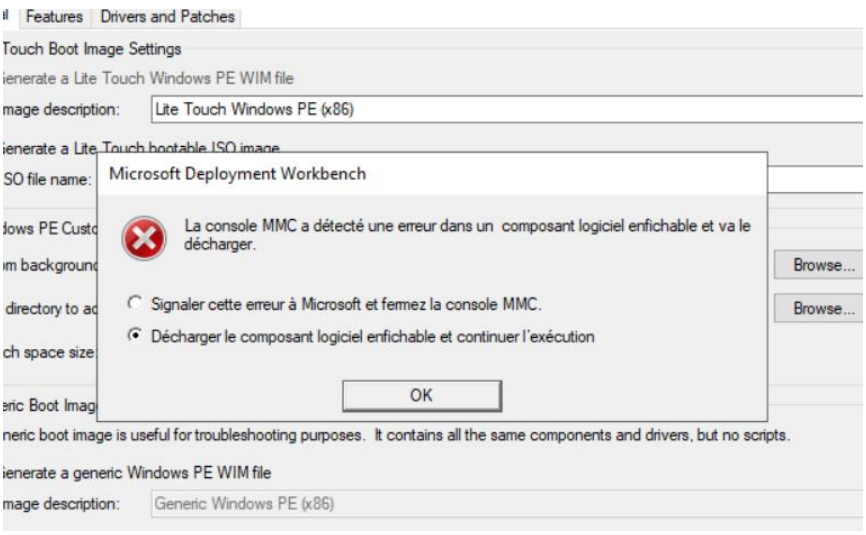


57. Décocher « Disable this step ». On voit bien que le Windows update n'est plus grisé et est maintenant vert, pour finir on fait « OK ».



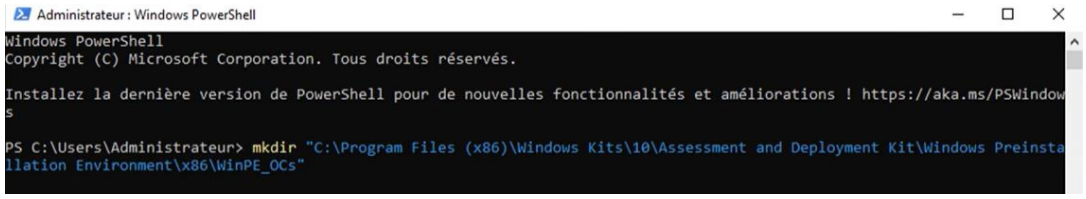
On va ensuite passer à une configuration spéciale pour Windows 11, afin d'éviter des bugs de déploiement.

Tout d'abord, lorsque l'on accède aux propriétés du Deployement Share (via un clic droit sur le Deployement Share) et que l'on clique sur l'onglet "Windows PE", on obtient cette erreur.

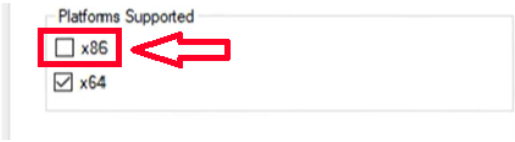


58. Pour résoudre cette erreur, il faut créer cette structure de dossiers vide, dans une fenêtre PowerShell on va exécuter cette commande :

mkdir "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs"

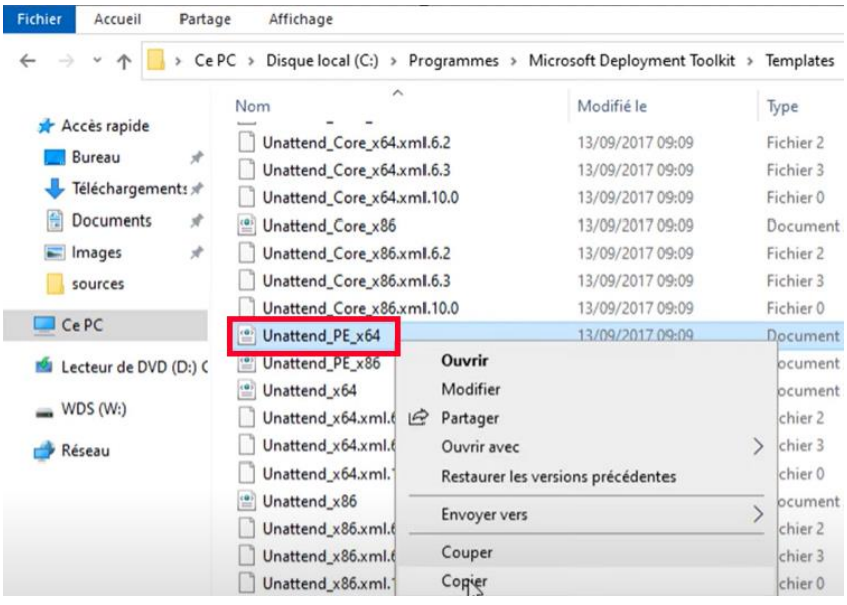


59. De retour dans le DeployementWorkbench, dans les propriétés du DeployementShare on va désactiver le x86 (32 Bits).



On va résoudre un autre problème qui a lieu lors du déploiement de type « script error… ».

60. A cet emplacement on cherche 'Unattend_PE_x64'



61. On fait une copie du fichier au cas où, et on l'ouvre puis on supprime son contenu pour le remplacer par ce code (lien) :

Pour finir, avant de générer une image, nous devons copier-coller quelques éléments dans le Deployment Share.

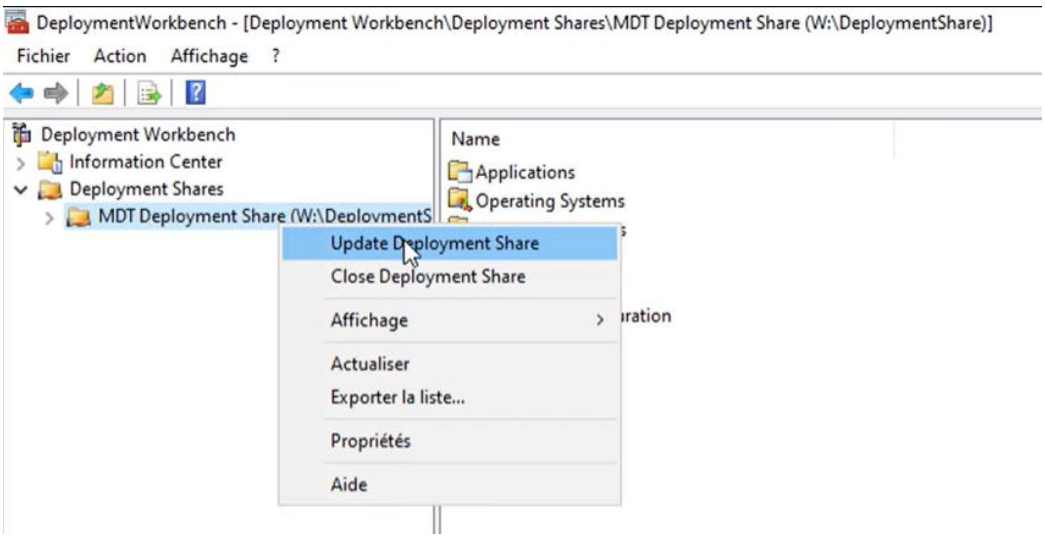
62. On va ouvrir les propriétés du Deployment Share, puis l'onglet « Rules », puis on clique sur « Edit Bootsrap.ini », où on copie ce qui suit :

```
[Settings]
Priority=Default

[Default]
DeployRoot=\\ASSURDEPLOY\DeploymentShare$
UserID=Service_MDT
UserPassword=P@ssword123!
UserDomain=ASSURDEPLOY
SkipBDDWelcome=YES
KeyboardLocalePE=040c:0000040c
```

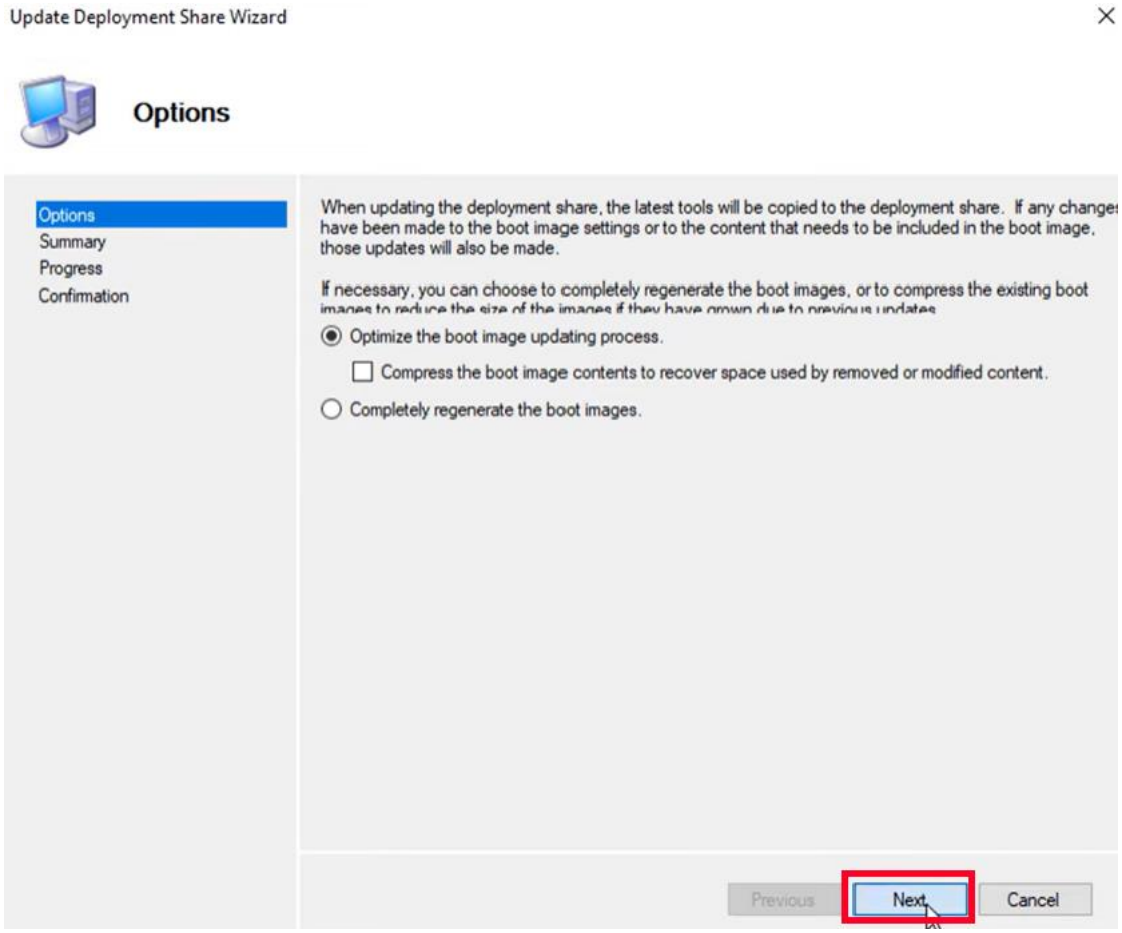
Cela correspond à l'utilisateur qu'on a créé précédemment, et on donne le nom d'utilisateur et le mot de passe à l'ordinateur qui se déploie pour qu'il accède au serveur de déploiement.

On peut maintenant générer une image LiteTouch dès maintenant.

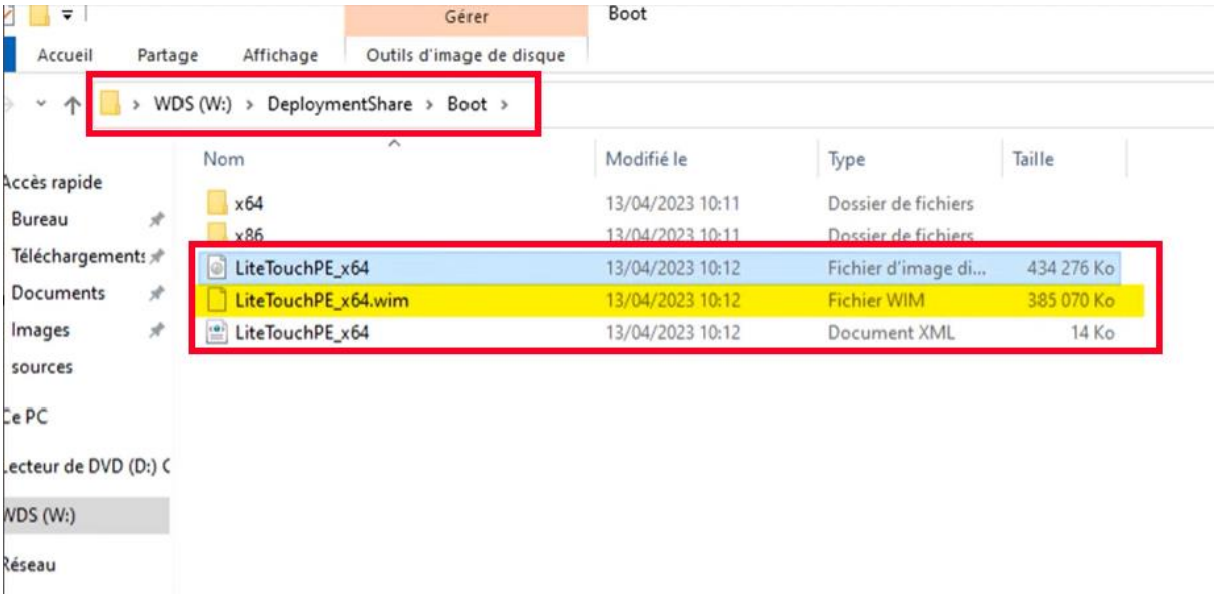
63. Sur le Deployement Share on fait un clic droit puis on sélectionne « Update Deployement Share ». Un assistant va apparaître.



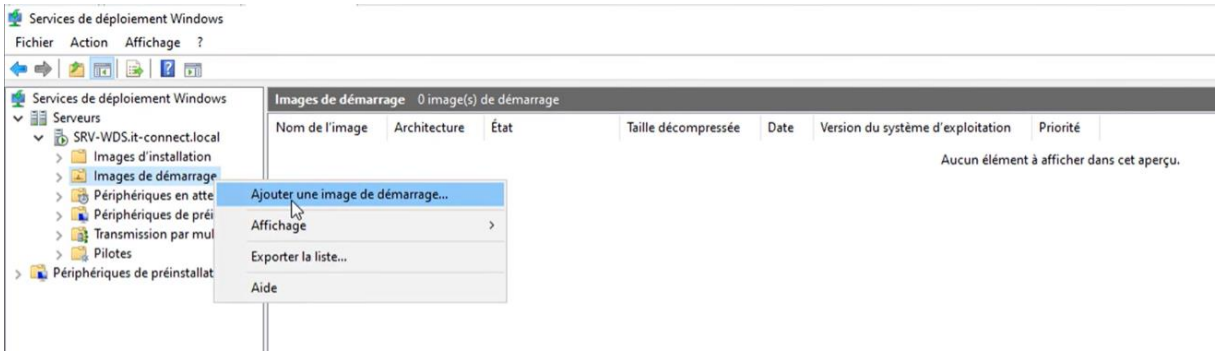
64. On ne change rien, et on appuie sur « Next » puis on finit la génération.



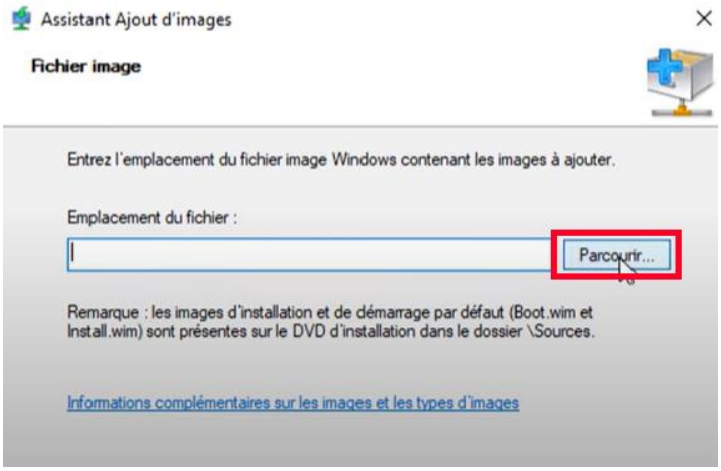
65. On vérifie que notre image est bien générée et est dans notre dossier Boot

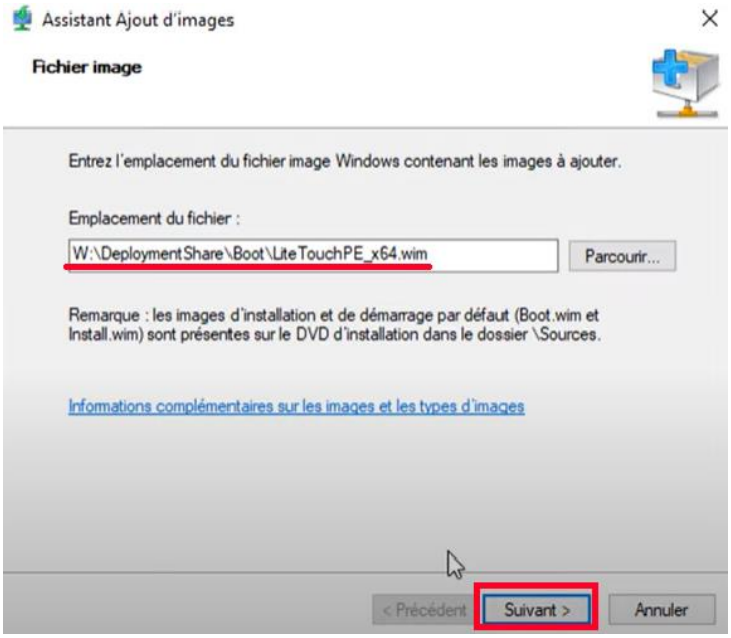


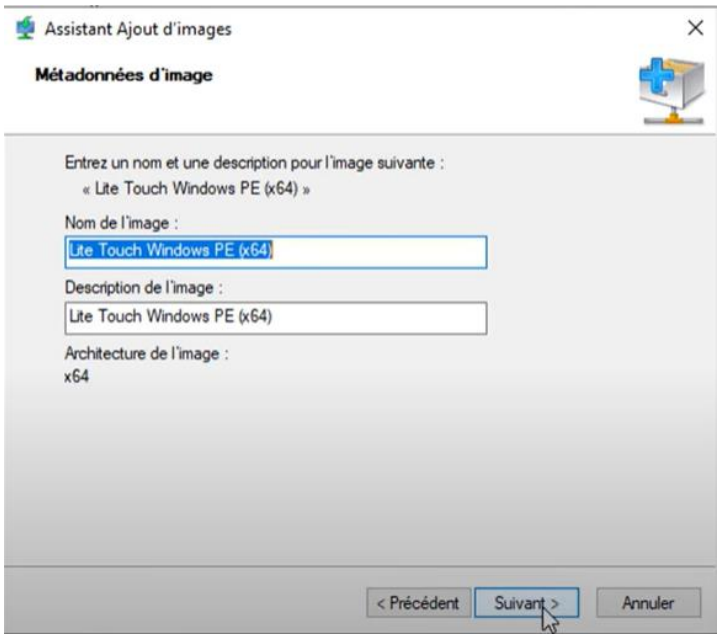
66. Au sein de notre console WDS, dans les images de démarrage, on fait un clic droit puis on fait « Ajouter une image de démarrage »



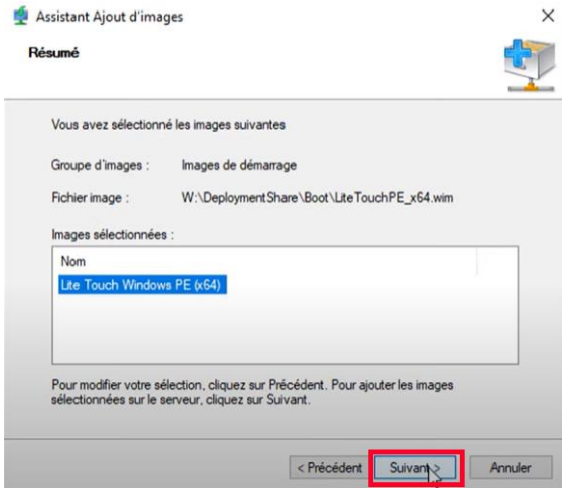
67. Un assistant apparait, on clique sur parcourir et on va retrouver notre image LiteTouch dans le dossier Boot. On peut changer son nom après, mais on ne va pas le faire.



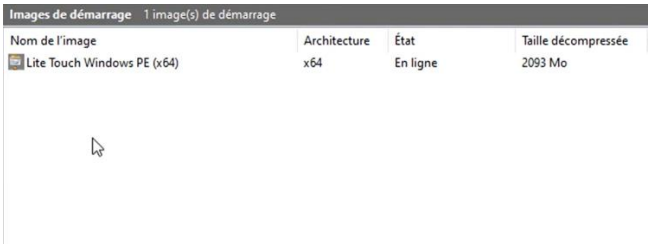




68. On clique sur suivant, puis Finir.

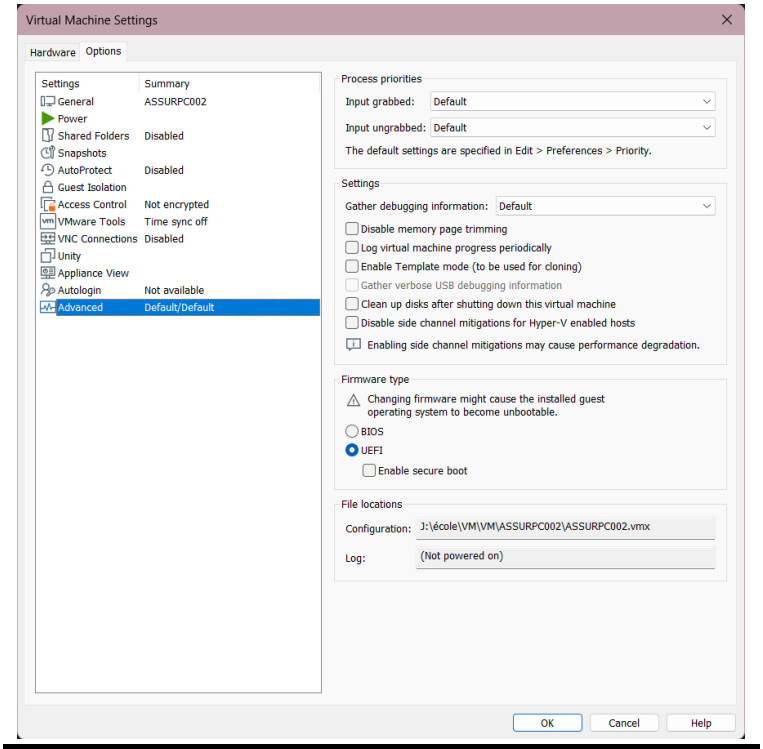


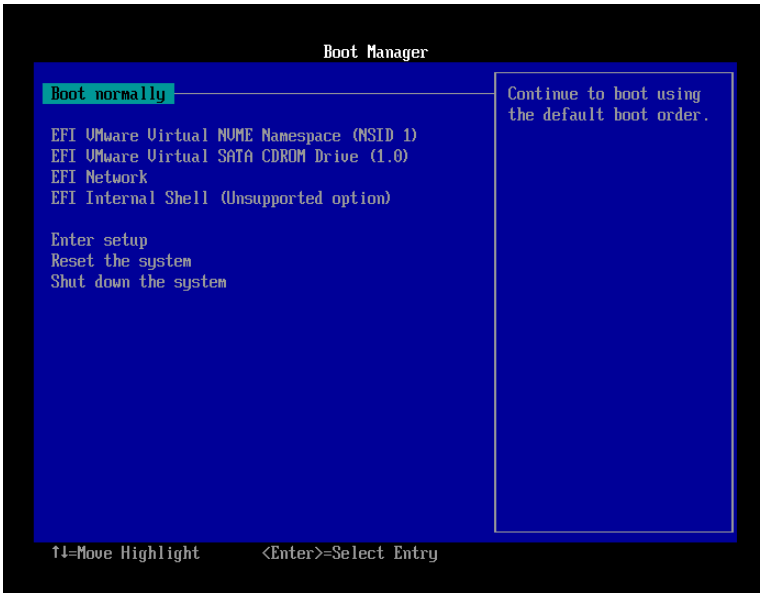
69. Notre image apparaît bien dans les images de démarrage.



On a donc fini la mise en place de l'image de démarrage MDT sur WDS. On va vérifier, ici à l'aide d'une machine virtuelle vide, si c'est fonctionnel.

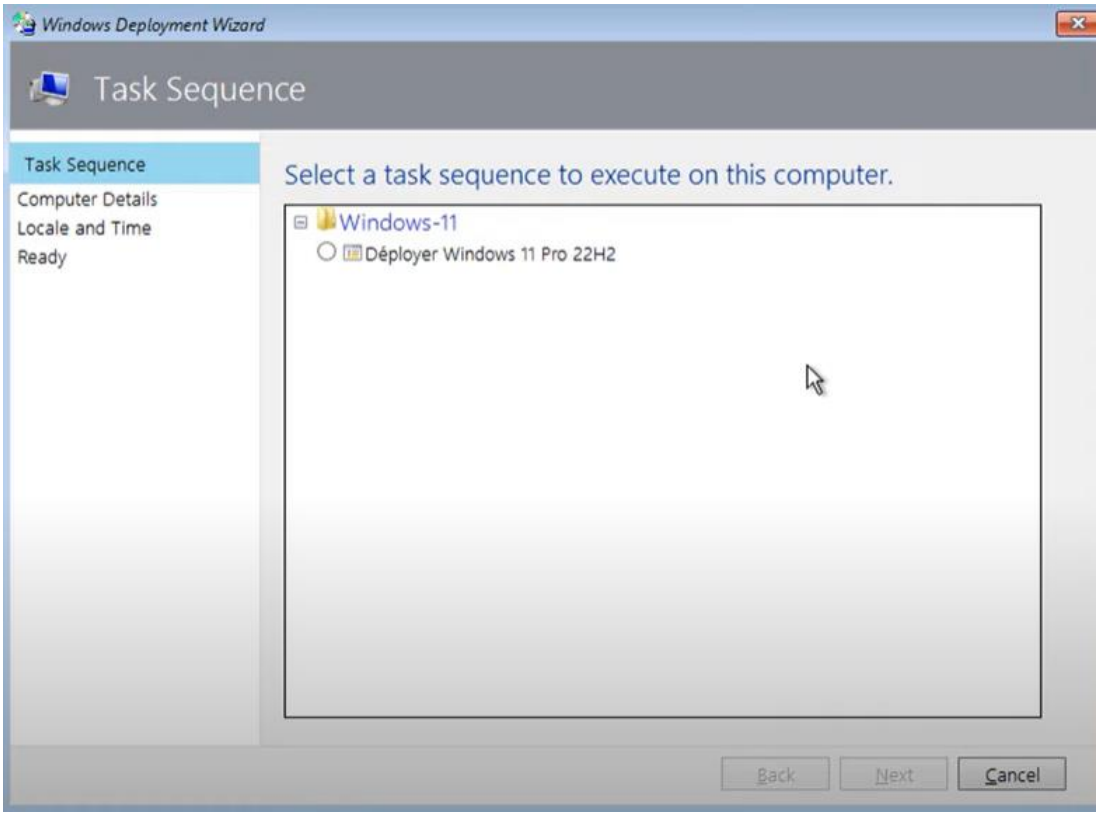
Dans les paramètres de celle-ci on vérifie que UEFI et le Secure Boot sont activés, puis on démarre notre VM, en sélectionnant « EFI Network »





Pendant le boot c'est bien notre image LiteTouch qui apparaît.

La fenêtre de déploiement MDT apparaît ensuite dans la VM, ce qui indique donc que MDT est fonctionnel sur notre infrastructure.



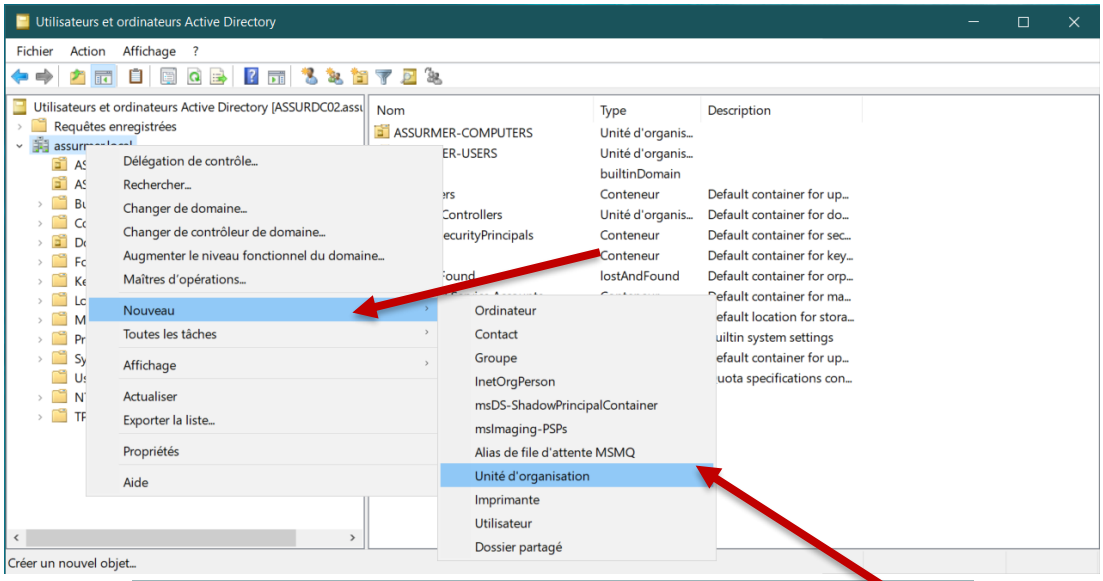
Etape 4 : Personnalisation de MDT

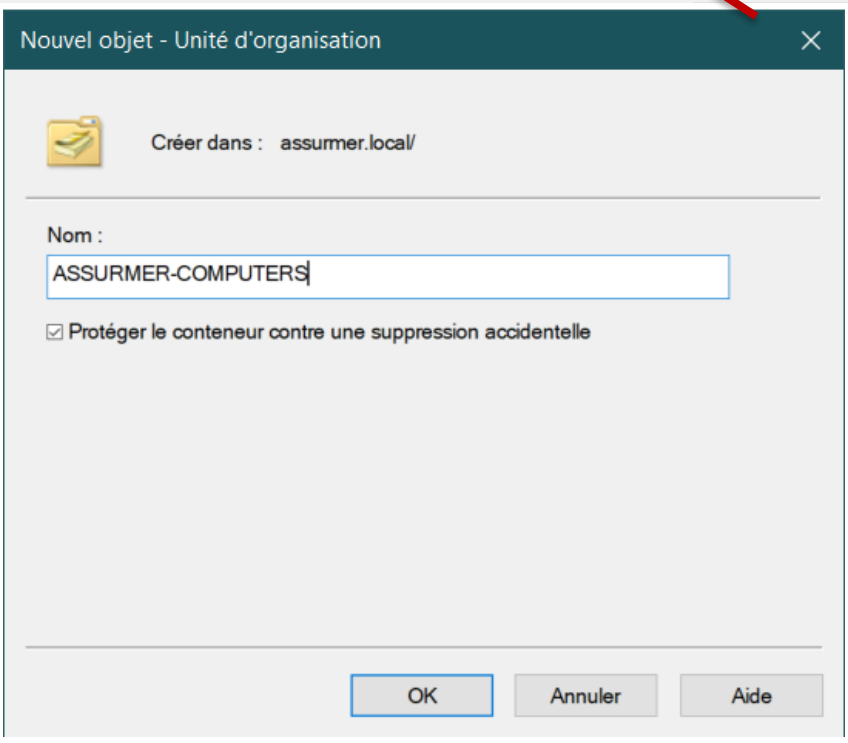
Pour faciliter le déploiement au technicien

Dans les faits, MDT est prêt, mais le PC déployé ne rejoindra pas ni le domaine ni l'AD d'ASSURMER automatiquement. On peut se permettre de rajouter ces options à l'image.

Nous devons donc créer un user AD, qui possèdera des droits d'accès à l'AD pour rajouter des ordinateurs au domaine et à l'AD.

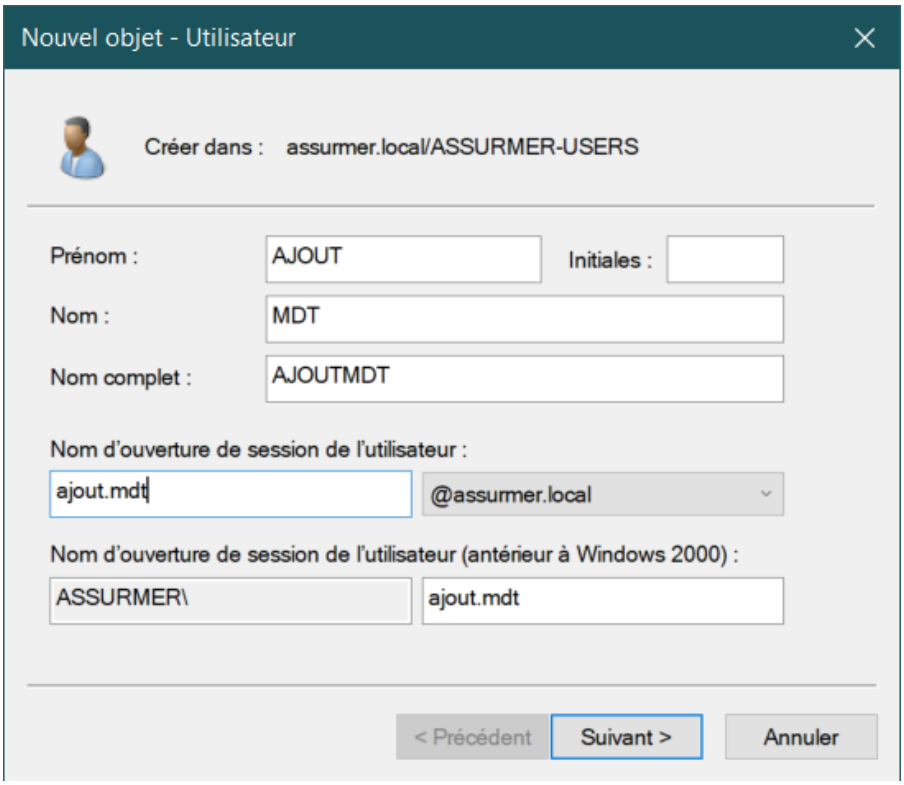
1. Retourner sur **ASSURDC02**, où se situe notre *Active Directory*.
2. Lancer l'annuaire *Active Directory*, puis créer deux OU[4] : **ASSUMER-COMPUTERS** et **ASSURMER-USERS**. Laisser la case cochée.



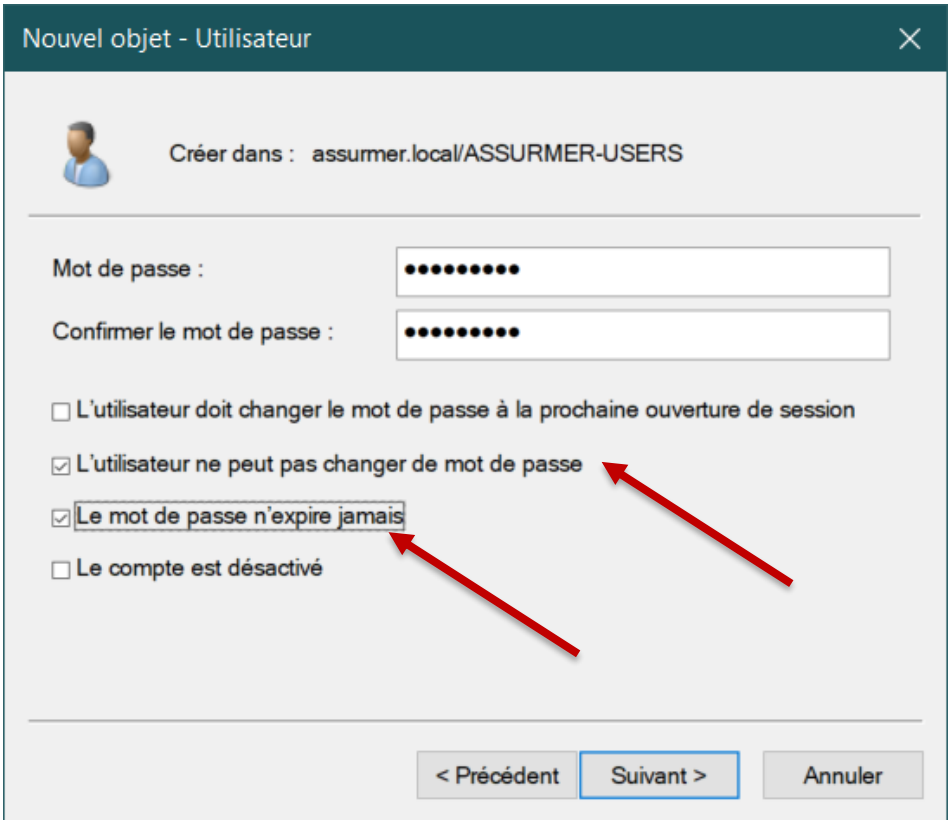


[4] OU : Unité d'organisation, ou dossier de l'Active Directory

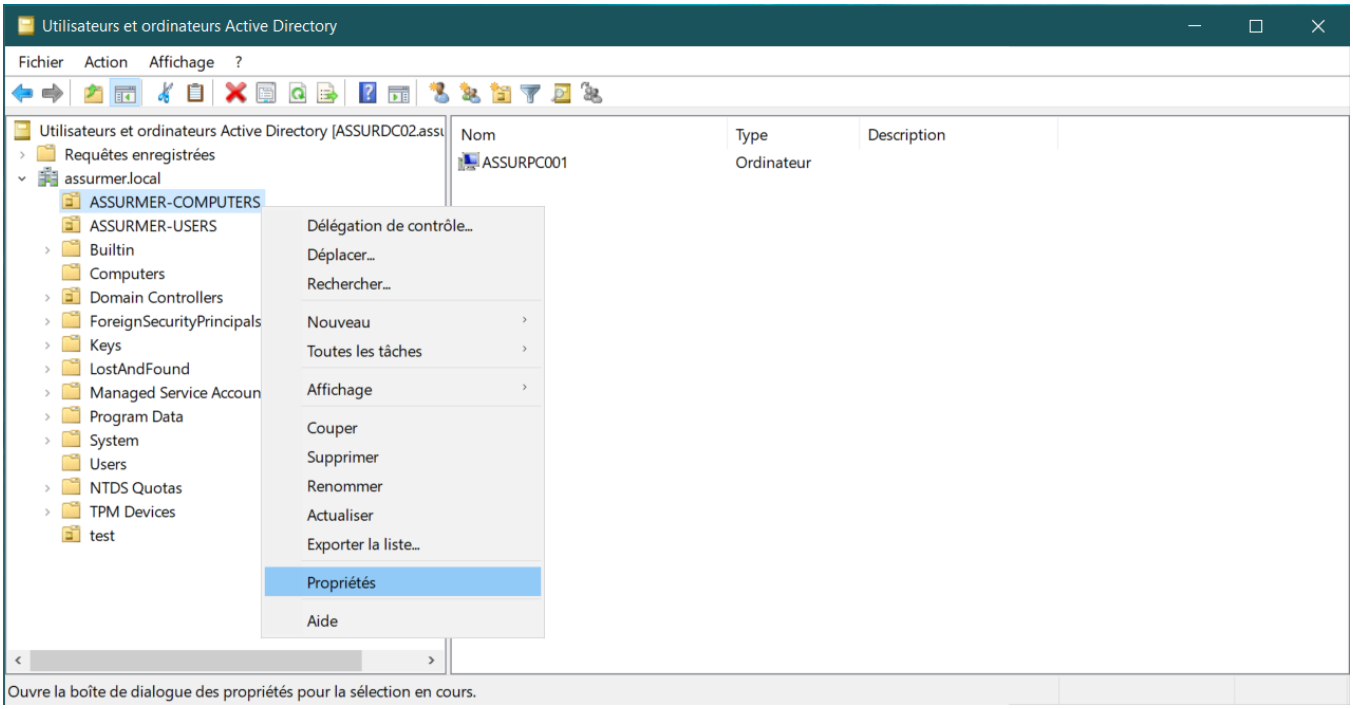
3. Dans l'OU **ASSURMER-USERS**, créer un nouvel utilisateur. Ici, on le nommera « **AJOUTMDT** », avec comme nom d'ouverture de session de l'utilisateur « **ajout.mdt** ».



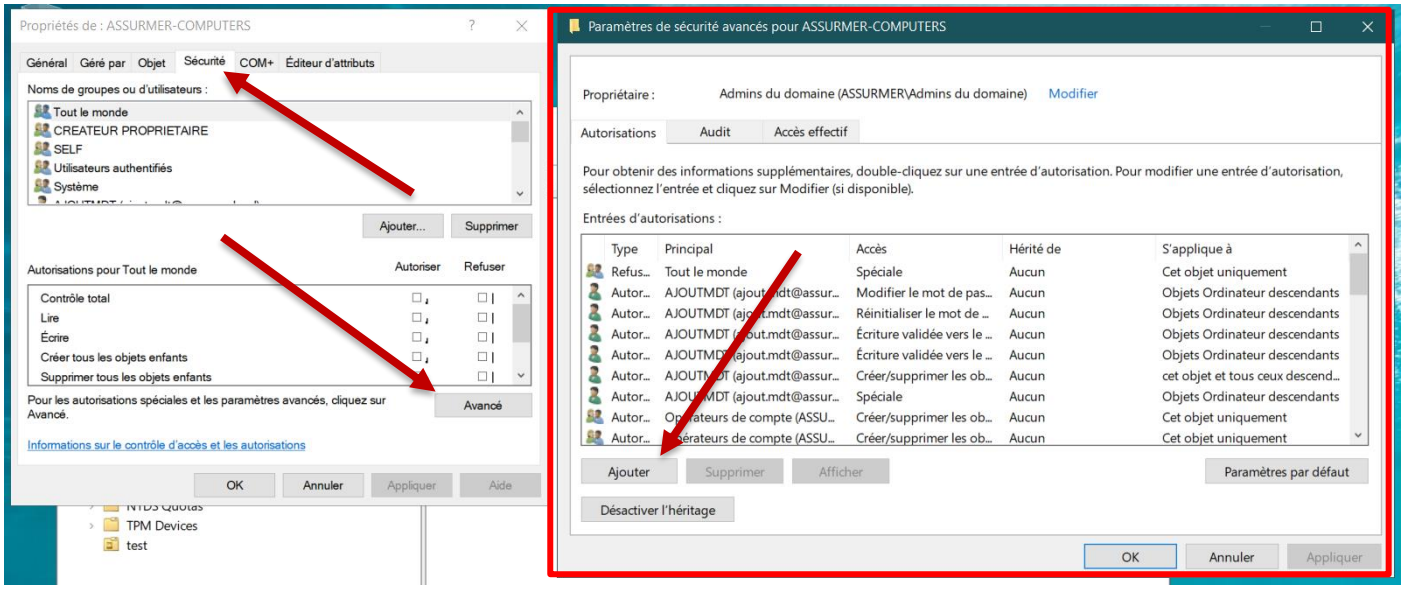
4. Indiquer un mot de passe, puis décocher la première case, et cocher la deuxième et la troisième. Au prochain écran, cliquer sur Terminer.



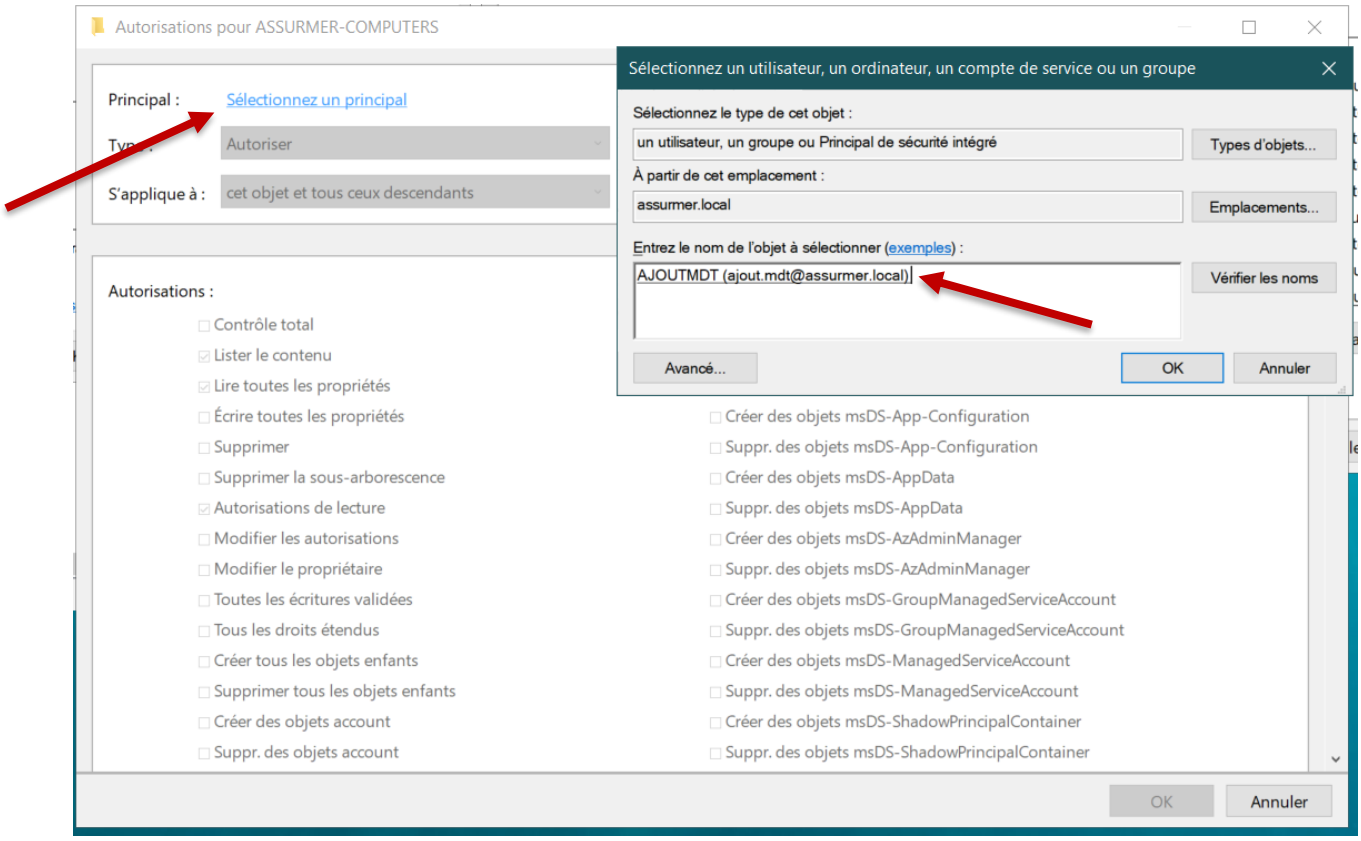
5. Continuer ensuite en visitant les propriétés de notre OU qui va contenir les ordinateurs du domaine : **ASSURMER-COMPUTERS.**



6. Cliquer ensuite sur l'onglet « Sécurité », puis « Avancé », ce qui ouvrira une nouvelle fenêtre. Cliquer sur Ajouter.



7. Une nouvelle fenêtre apparaît. Cliquer sur « *Sélectionnez un principal* », puis, dans la fenêtre qui s'ouvre, y sélectionner **AJOUTMDT**, et cliquer sur *OK*.



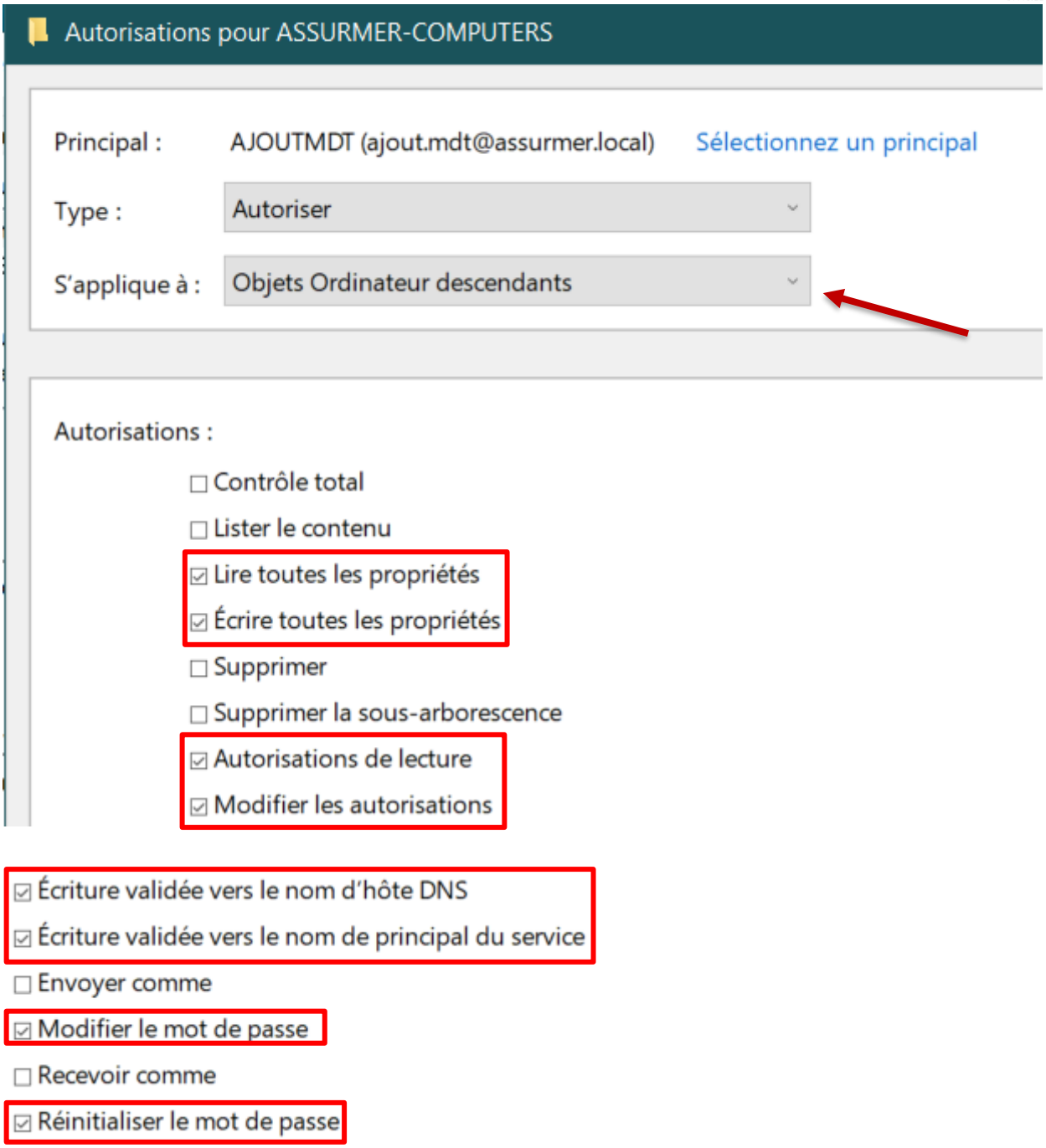
8. Sélectionner ensuite les permissions suivantes, puis cliquer sur OK.

☑ Créer des objets Ordinateur

☑ Suppr. des objets Ordinateur

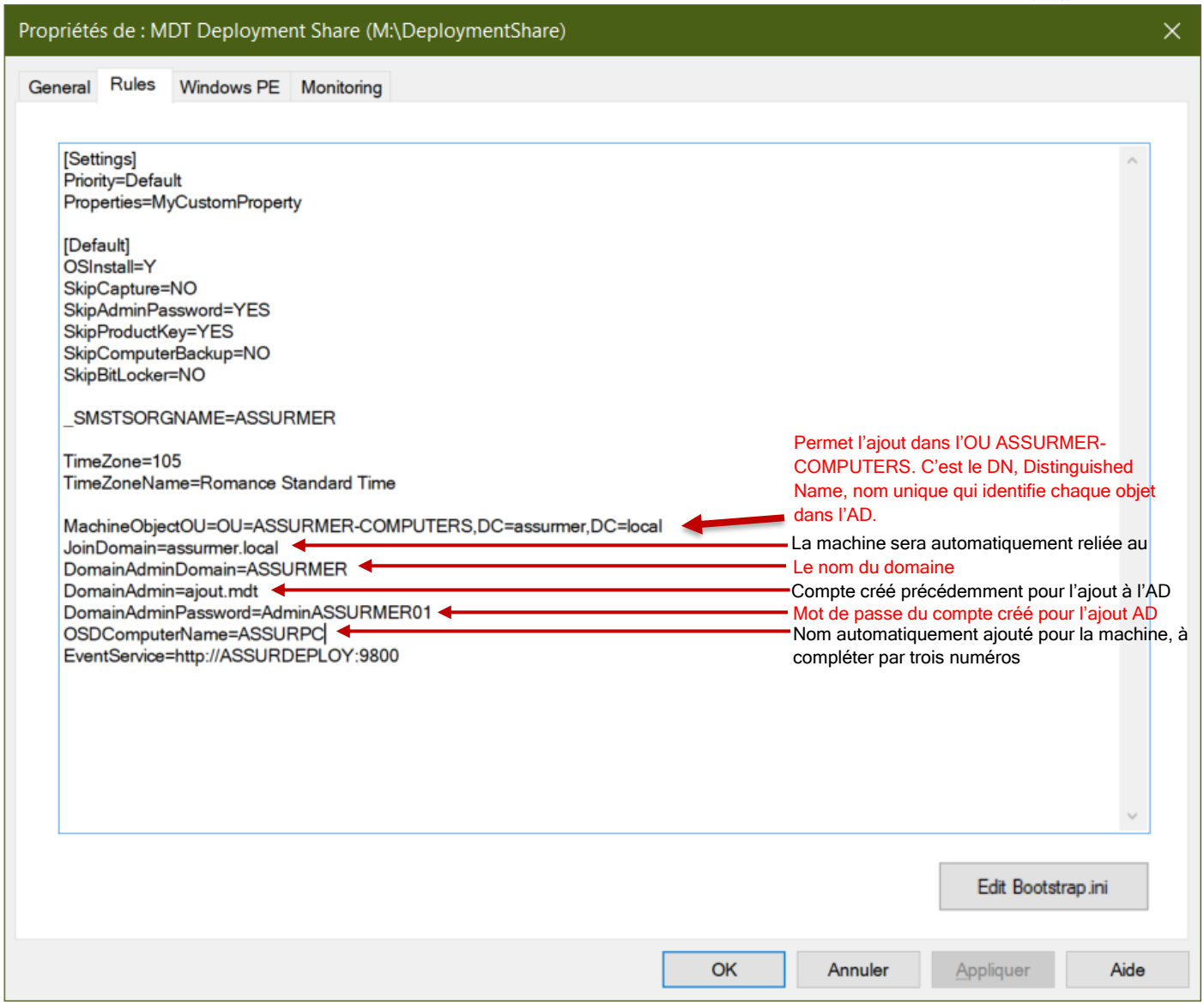
9. Renouveler l'opération depuis l'étape 7, en sélectionnant cette fois « *Objets Ordinateurs descendants* » au niveau de la liste déroulante « *S'applique à :* », puis sélectionner les autorisations :
   - **Lire toutes les propriétés**
   - **Écrire toutes les propriétés**
   - **Autorisations de lecture**
   - **Modifier les autorisations**
   - **Écriture validée vers le nom d'hôte DNS**
   - **Écriture validée vers le nom principal du service**
   - **Modifier le mot de passe**
   - **Réinitialiser le mot de passe**

   Décocher « **Lister le contenu** ».

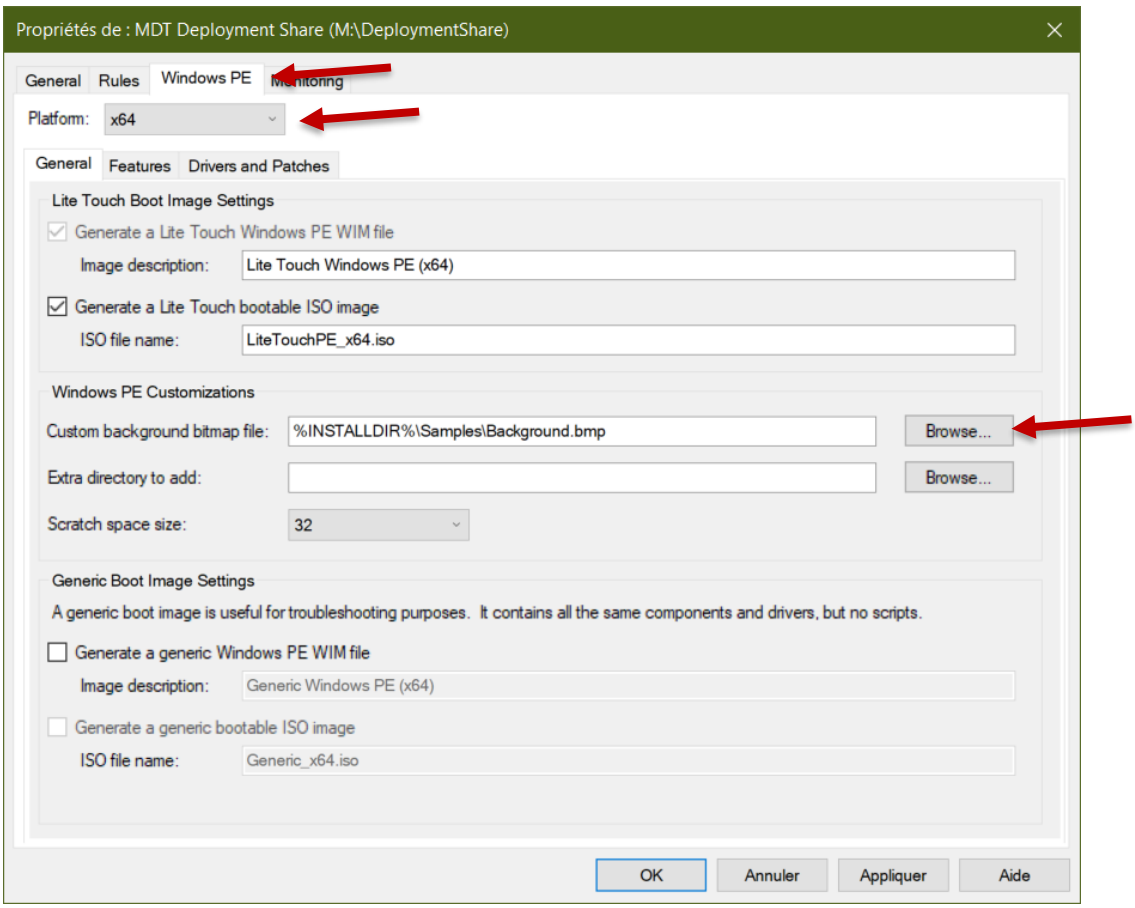


Cliquer ensuite sur OK, Appliquer, et enfin OK.
Nous en avons fini avec l'Active Directory, et pouvons repasser à **ASSURDEPLOY**.

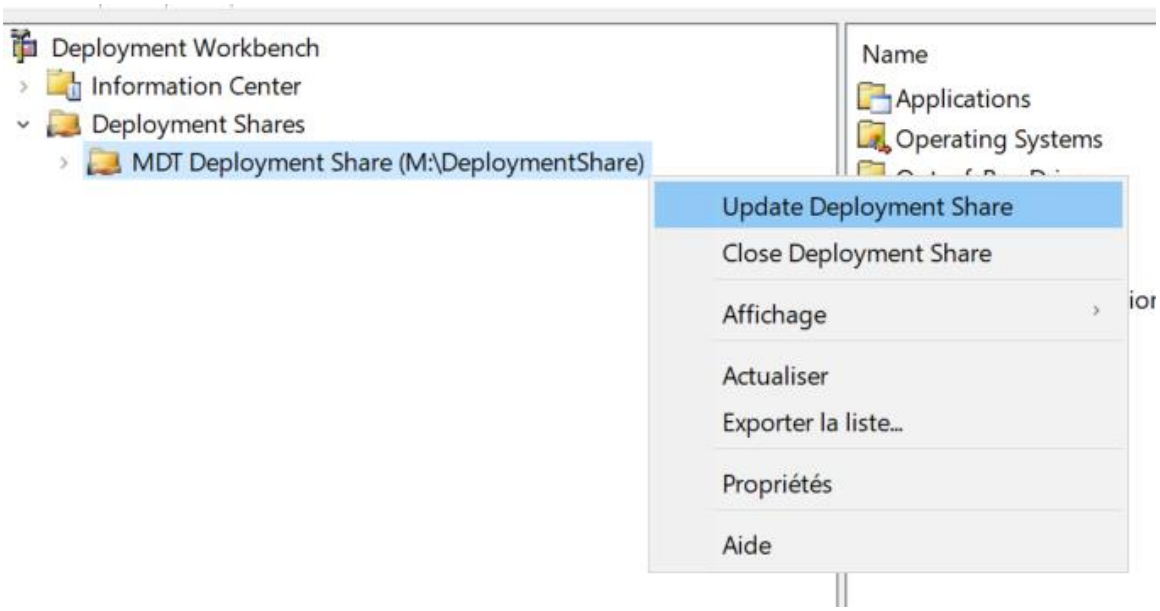
10. Ouvrir la *Deployement Workbench* sur **ASSURDEPLOY**. Faire un clic droit sur le MDT *Deployment Share*, et *Propriétés*, puis dans *Rules*, où on ajoutera à la suite quelques lignes d'instructions :

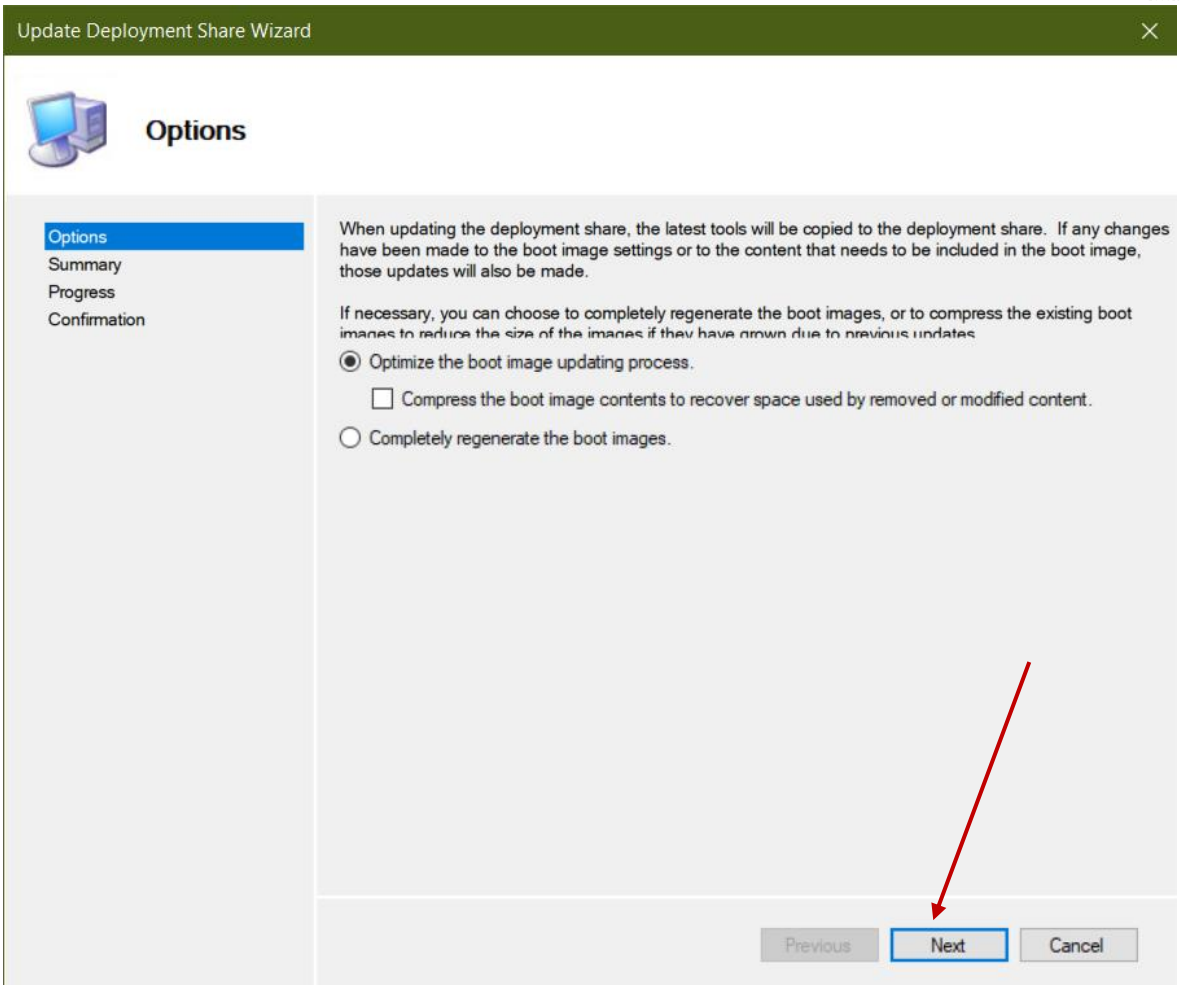

Propriétés de : MDT Deployment Share (M:\DeploymentShare)
General
Rules
Windows PE
Monitoring
[Settings]
Priority=Default
Properties=MyCustomProperty
[Default]
OSInstall=Y
SkipCapture=NO
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=NO
SkipBitLocker=NO
_SMSTSORGNAME=ASSURMER
TimeZone=105
TimeZoneName=Romance Standard Time
MachineObjectOU=OU=ASSURMER-COMPUTERS,DC=assurmer,DC=local
JoinDomain=assurmer.local
DomainAdminDomain=ASSURMER
DomainAdmin=ajout.mdt
DomainAdminPassword=AdminASSURMER01
OSDComputerName=ASSURPC
EventService=http://ASSURDEPLOY:9800
Permet l'ajout dans l'OU ASSURMER-COMPUTERS. C'est le DN, Distinguished Name, nom unique qui identifie chaque objet dans l'AD.
La machine sera automatiquement reliée au
Le nom du domaine
Compte créé précédemment pour l'ajout à l'AD
Mot de passe du compte créé pour l'ajout AD
Nom automatiquement ajouté pour la machine, à compléter par trois numéros
Edit Bootstrap.ini
OK
Annuler
Appliquer
Aide

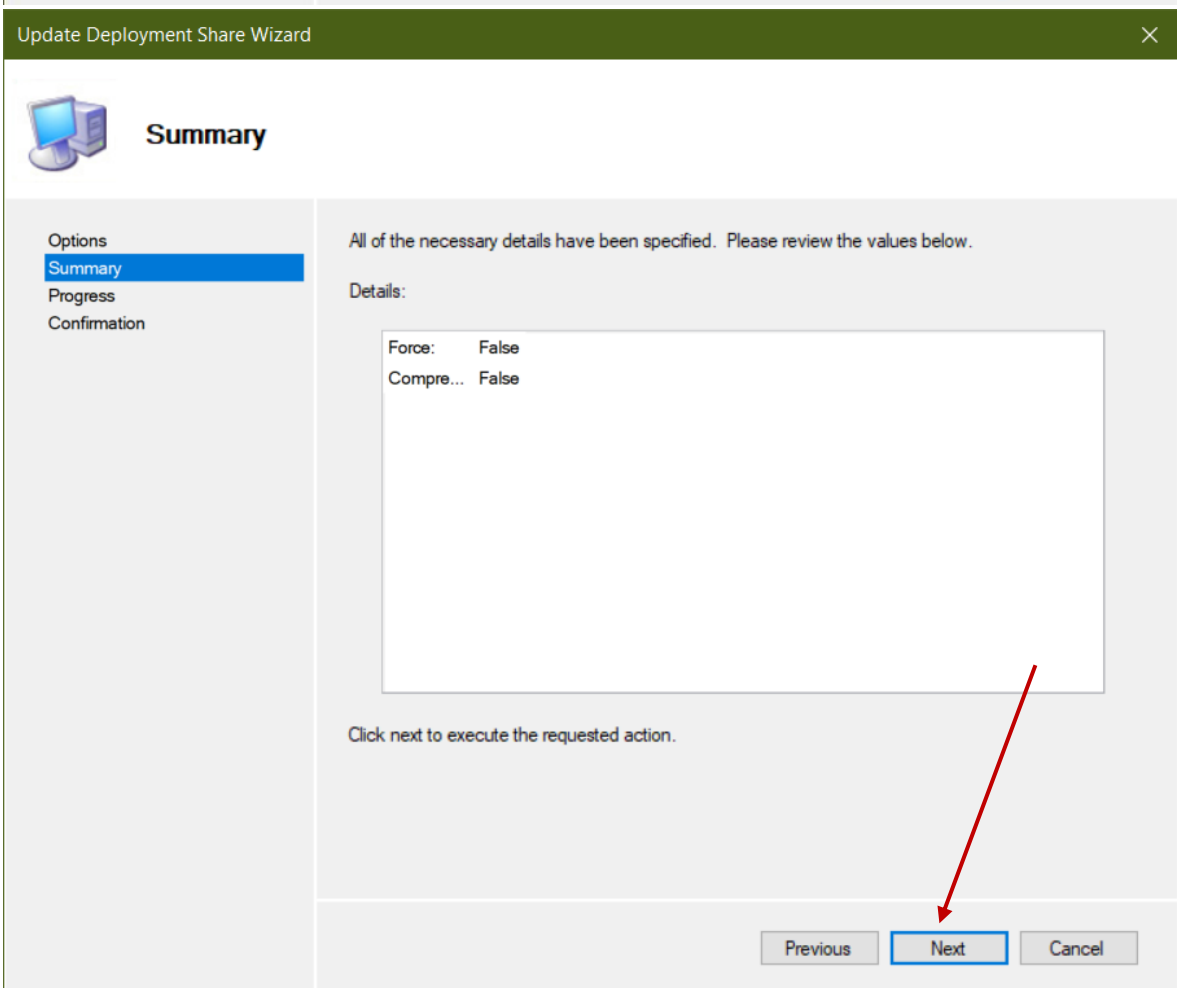
11. L'ajout à l'AD et au domaine de manière automatique est terminée. Pour faire coller l'outil à notre image, nous allons maintenant passer à la personnalisation du fond d'écran de MDT.
Pour se faire, se rendre dans l'onglet *Windows PE*, puis choisir dans « Platform » le choix *x64*.
Enfin, au niveau de *Custom Background bitmap file*, cliquer sur « Browze » pour aller choisir notre propre image.

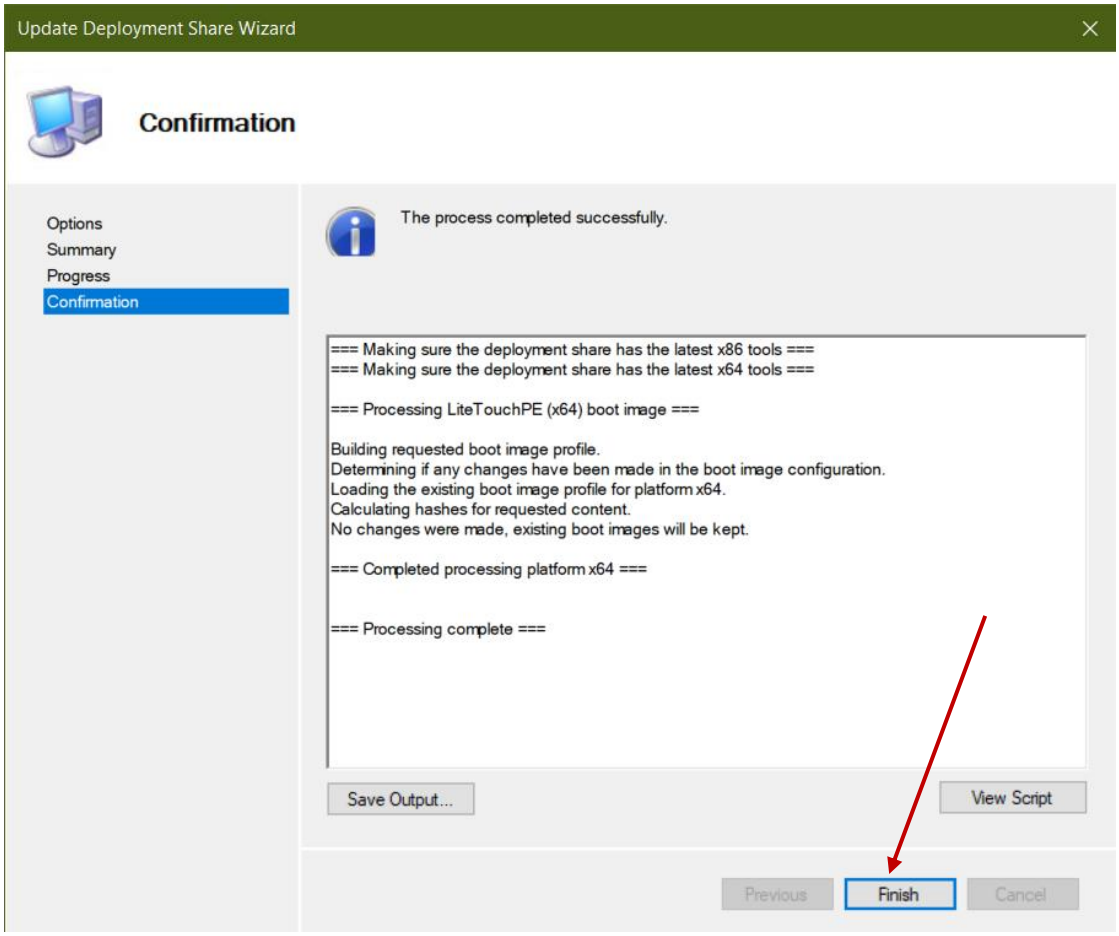


12. Enfin, il ne faut pas oublier de mettre à jour l'image MDT. Pour cela, il faut faire un clic droit sur le Deployment Share, Update Deployment Share, et cliquer sur Next deux fois, puis Finish à la fin.




Update Deployment Share Wizard
Options
Options
Summary
Progress
Confirmation
When updating the deployment share, the latest tools will be copied to the deployment share. If any changes have been made to the boot image settings or to the content that needs to be included in the boot image, those updates will also be made.
If necessary, you can choose to completely regenerate the boot images, or to compress the existing boot images to reduce the size of the images if they have grown due to previous updates
Optimize the boot image updating process.
Compress the boot image contents to recover space used by removed or modified content.
Completely regenerate the boot images.
Previous
Next
Cancel


Update Deployment Share Wizard
Summary
Options
Summary
Progress
Confirmation
All of the necessary details have been specified. Please review the values below.
Details:
Force: False
Compre... False
Click next to execute the requested action.
Previous
Next
Cancel



13. Après vérification, les modifications sont bien apportées, et MDT est prêt à être utilisé par les techniciens de la DSI.