Déploiement automatisé MS Windows (WDS + MDT)

En tant que administrateur Infrastructure Sécurisée, malgré l'introduction de InTune par Microsoft, nombres d'entreprises encore les solutions WDS et MDT pour le déploiement de postes de travail sous MS Windows 10 et 11. En tant qu'administrateur, vous devez maitriser cette opération d'automatisation et de personnalisation d'un modèle ou "master" du système d'exploitation. Et assurer la sécurité des masters.

Auteurs

Roblot Jean-Philippe - jroblot.simplon@proton.me
Drula Kevin - kdrula.roblot@proton.me

Version

15/05/2024 - V1R0

Stack technique

Powered by https://shields.io

Contexte

Sur la base d'un environnement de virtualisation de type VirtualBox ou VMware Workstation, vous devez mettre en oeuvre un environnement de déploiement de postes d'entreprise.

Votre environnement doit répondre au cahier des charges suivants :

L'environnement de déploiement est isolé du réseau d'entreprise

Le déploiement doit permettre l'installation de poste Windows 10 Pro intégré dans un domaine AD DS

L'environnement doit disposer d'un serveur Windows Server 2019 ou 2022 avec les rôles WDS et ADDS (DNS+DHCP)

La personnalisation des postes doit offrir les éléments suivants :

REQ01 = Système d'exploitation = MS Windows 10 Professionnel Build 1903 ou supérieur REQ02 = Partitionnement des disques = C:\ (SYSTEM) de 30 Go et D:\ (DATA) de 10 Go REQ03 = Intégration des postes dans le domaine d'entreprise (AD-DS) REQ04 = Installer VS Code REQ05 = Installer CCleaner SEC01 = Interdire l'installation de logiciel aux utilisateurs du domaine SEC02 = Désactiver/Interdire la connexion de supports de stockage externes SEC03 = Afficher un message à la connexion d'un utilisateur du domaine (Personnaliser votre message d'entreprise)

SEC04 = Interdire l'accès au "Panneau de Configuration" aux utilisateurs du domaine

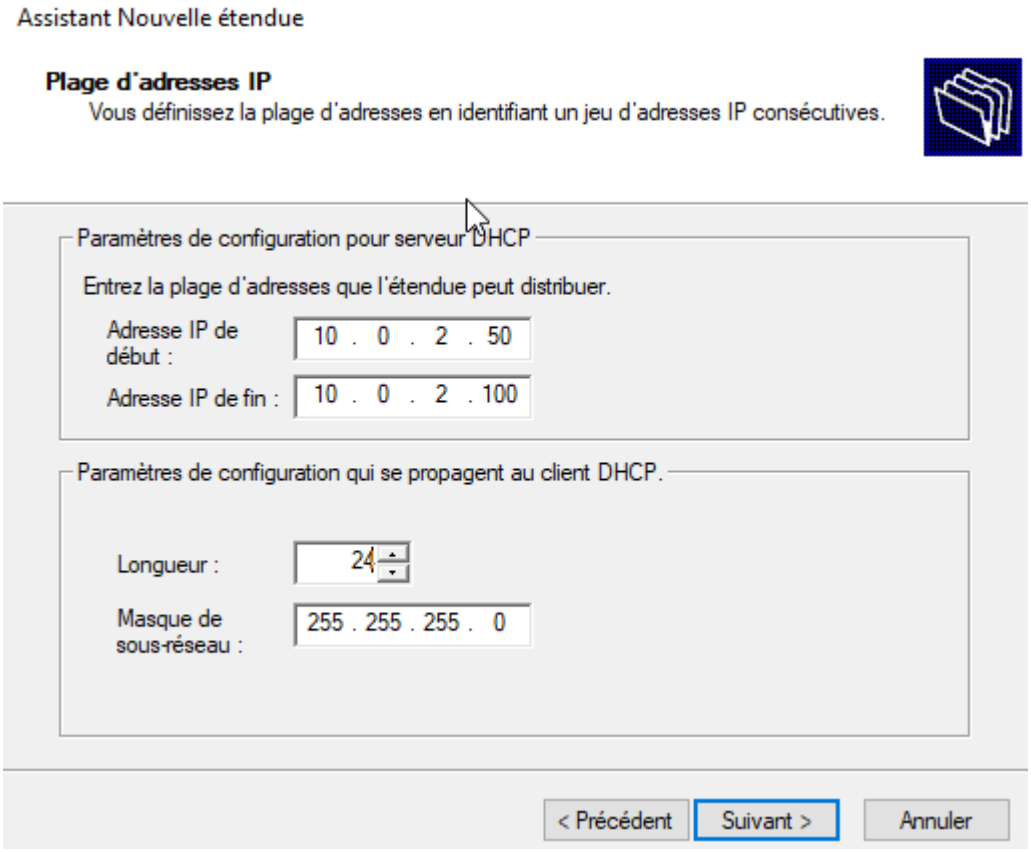
L'intégration de LAPS est obligatoire pour la gestion des comptes administrateurs locaux

Pré-requis

Un serveur Windows 2019 avec les rôles ADDS et DHCP Le rôle Service de déploiement Windows (WDS) Les outils ADK (Windows Assessment and Deployment Kit), MDT (Microsoft Deployment Toolkit) et Windows PE (Preinstallation Environment). Accès administrateur au serveur.

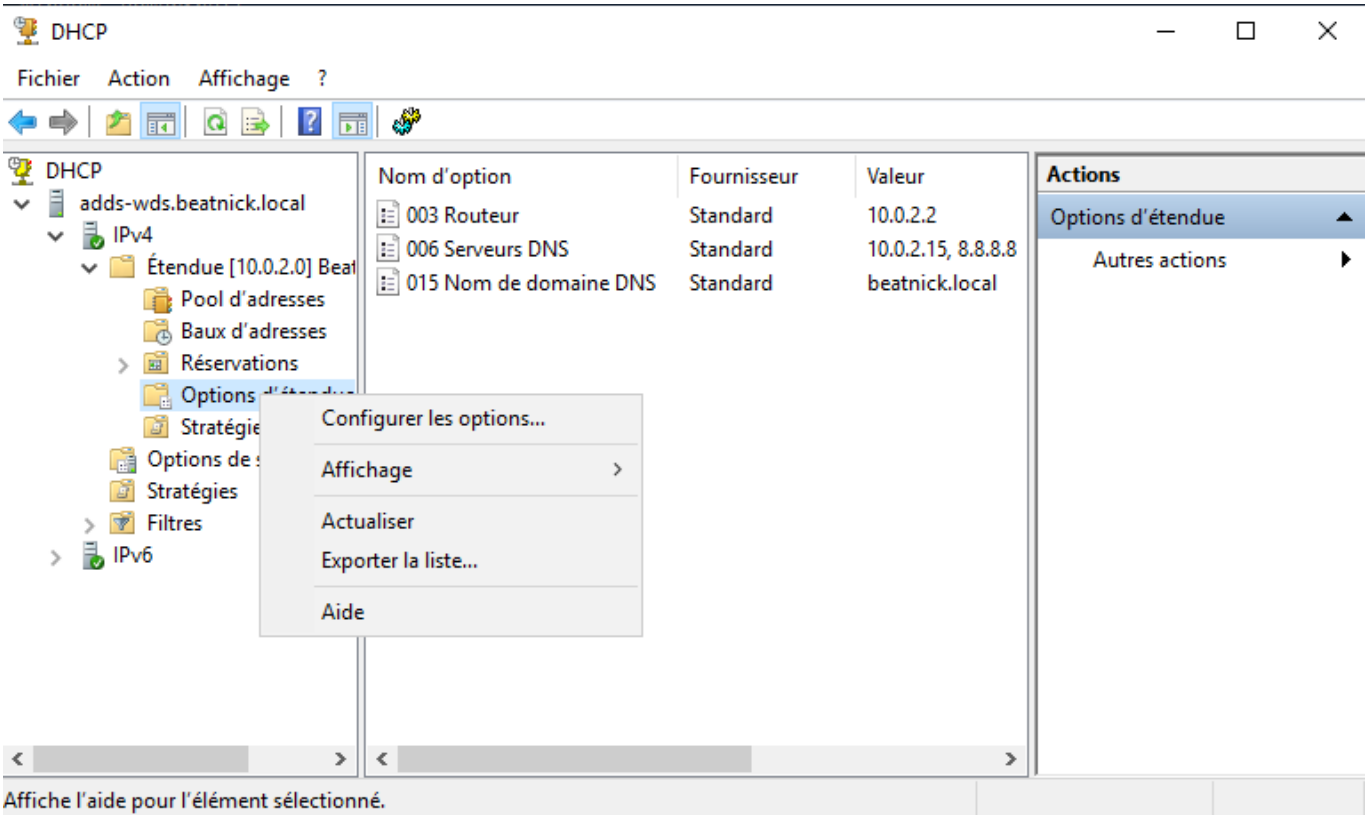
DHCP

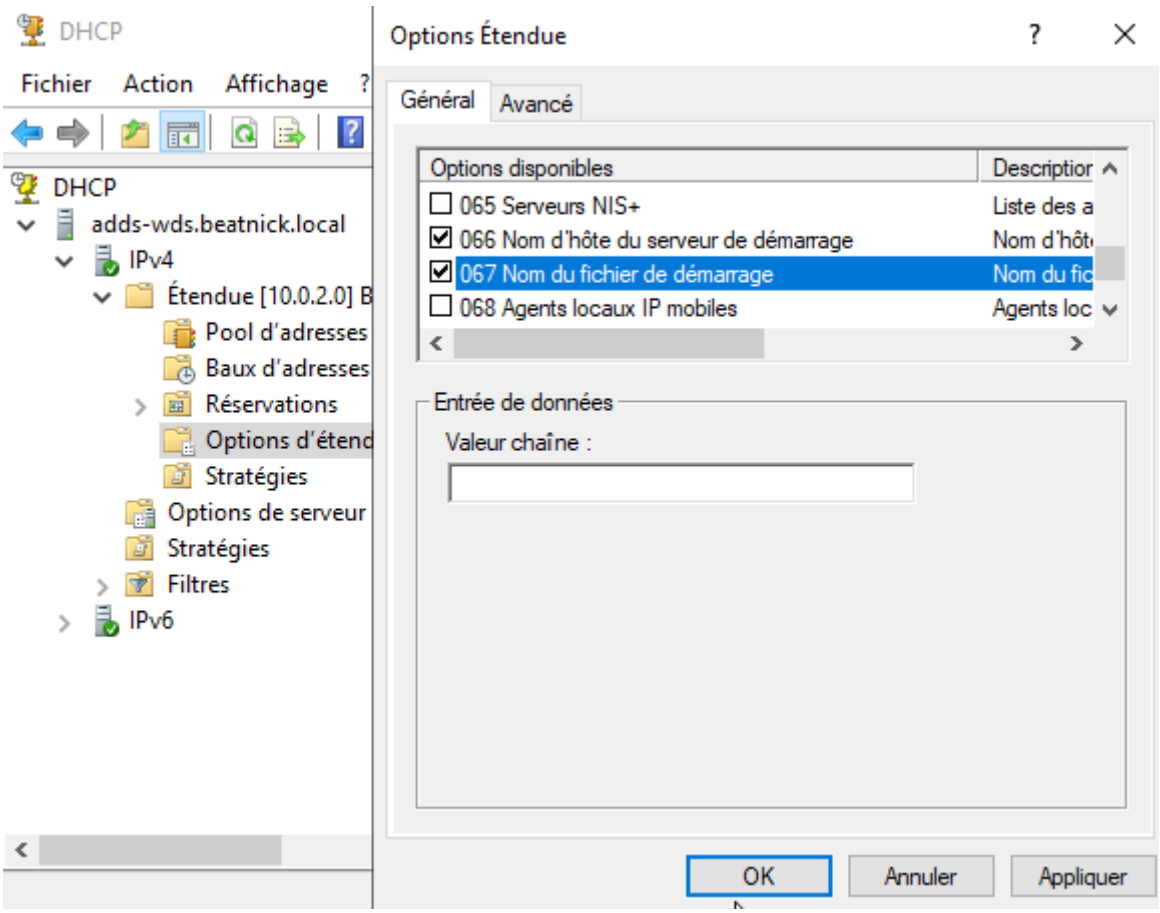
Ajouter le rôle DHCP et paramétrer une plage d'étendue



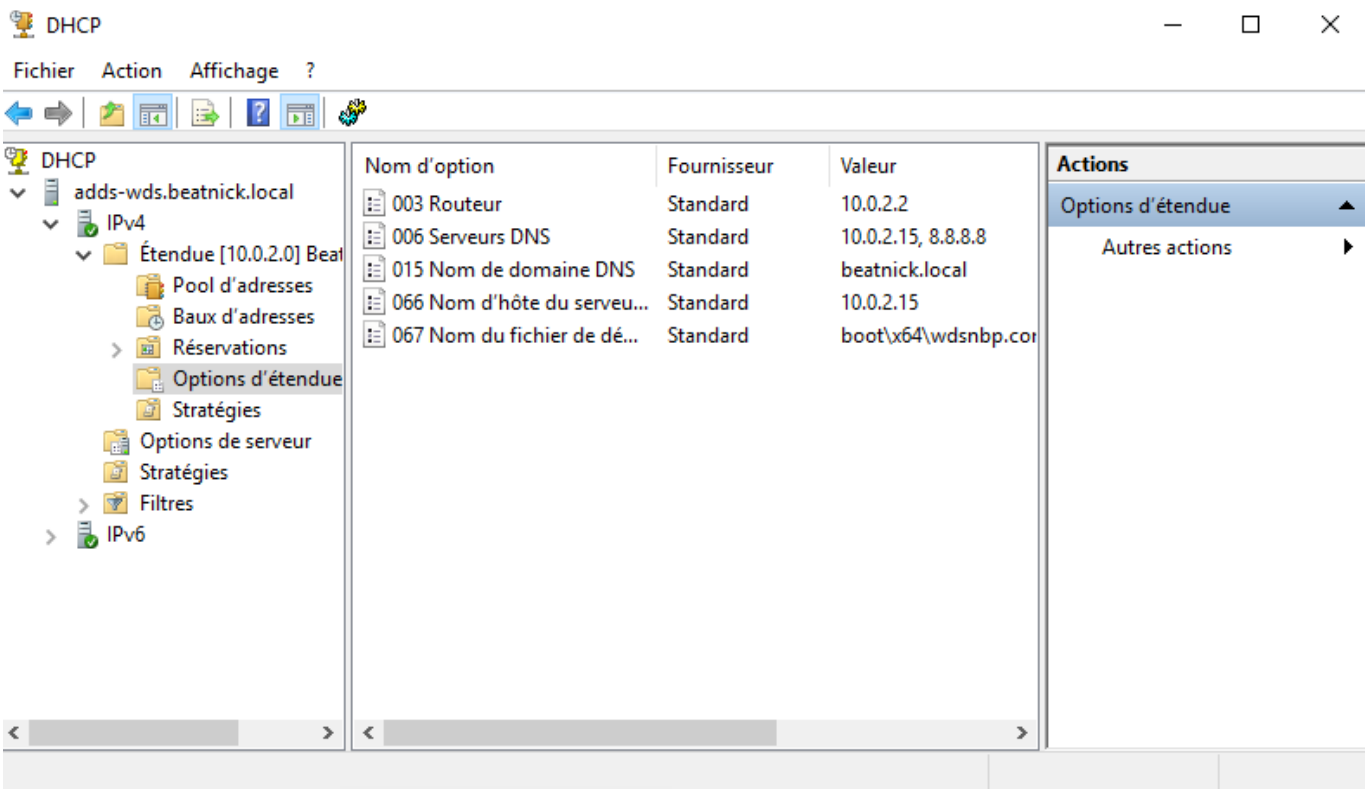
Paramétrer l'étendue pour WDS :

`Options d'étendue > Configurer les options`



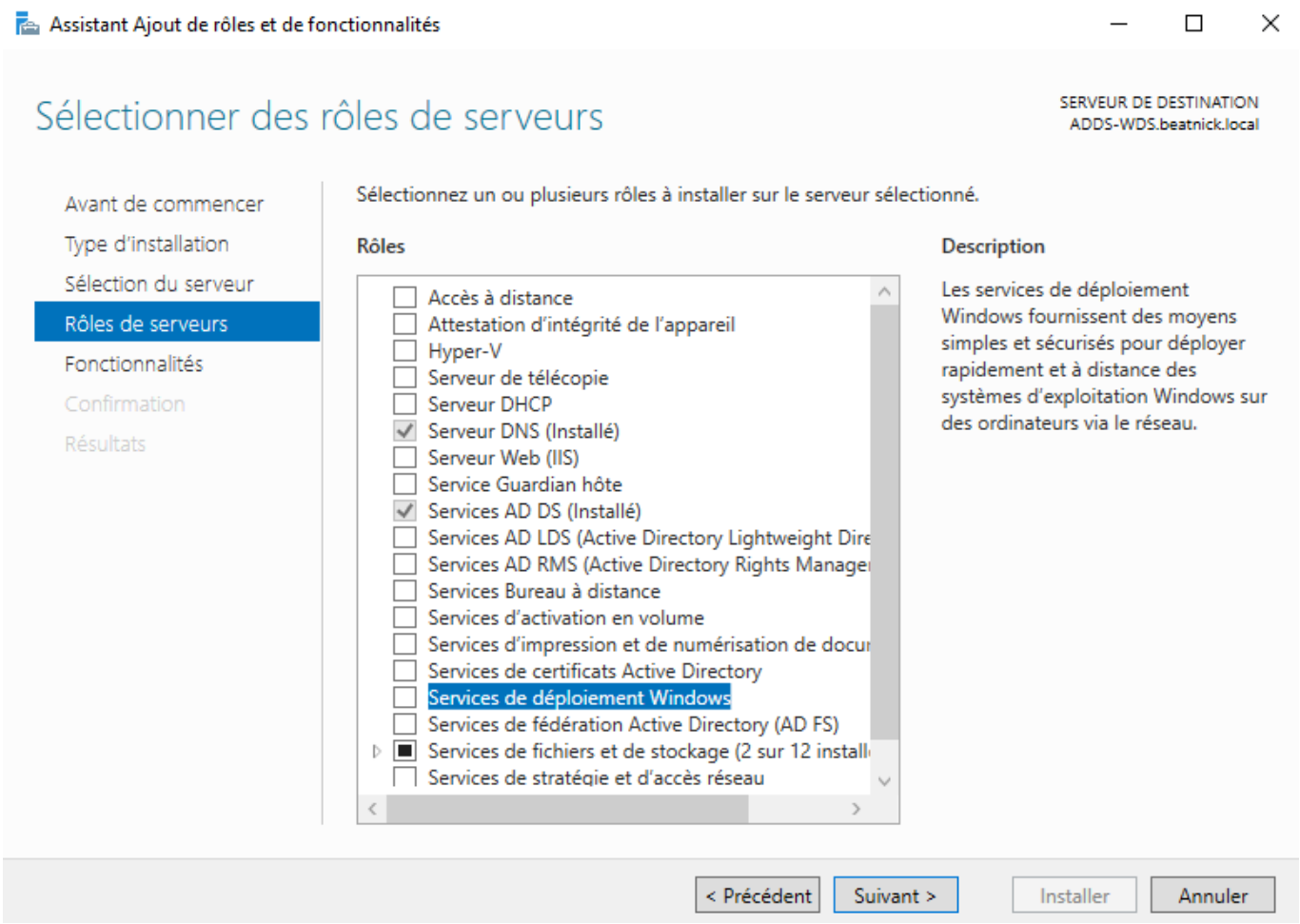


cocher les options 66 et 67



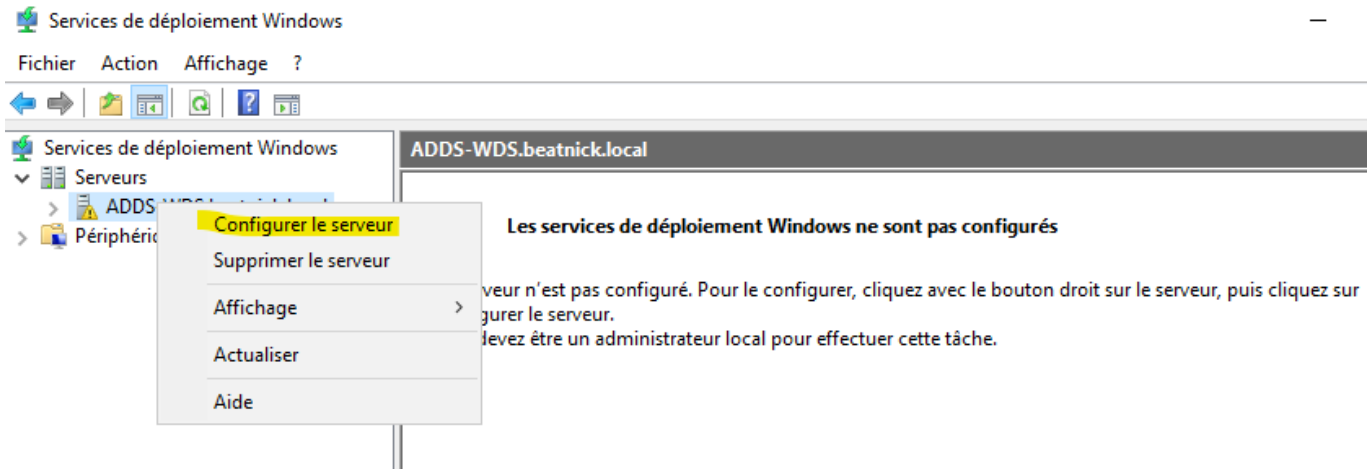
Ajout du rôle WDS

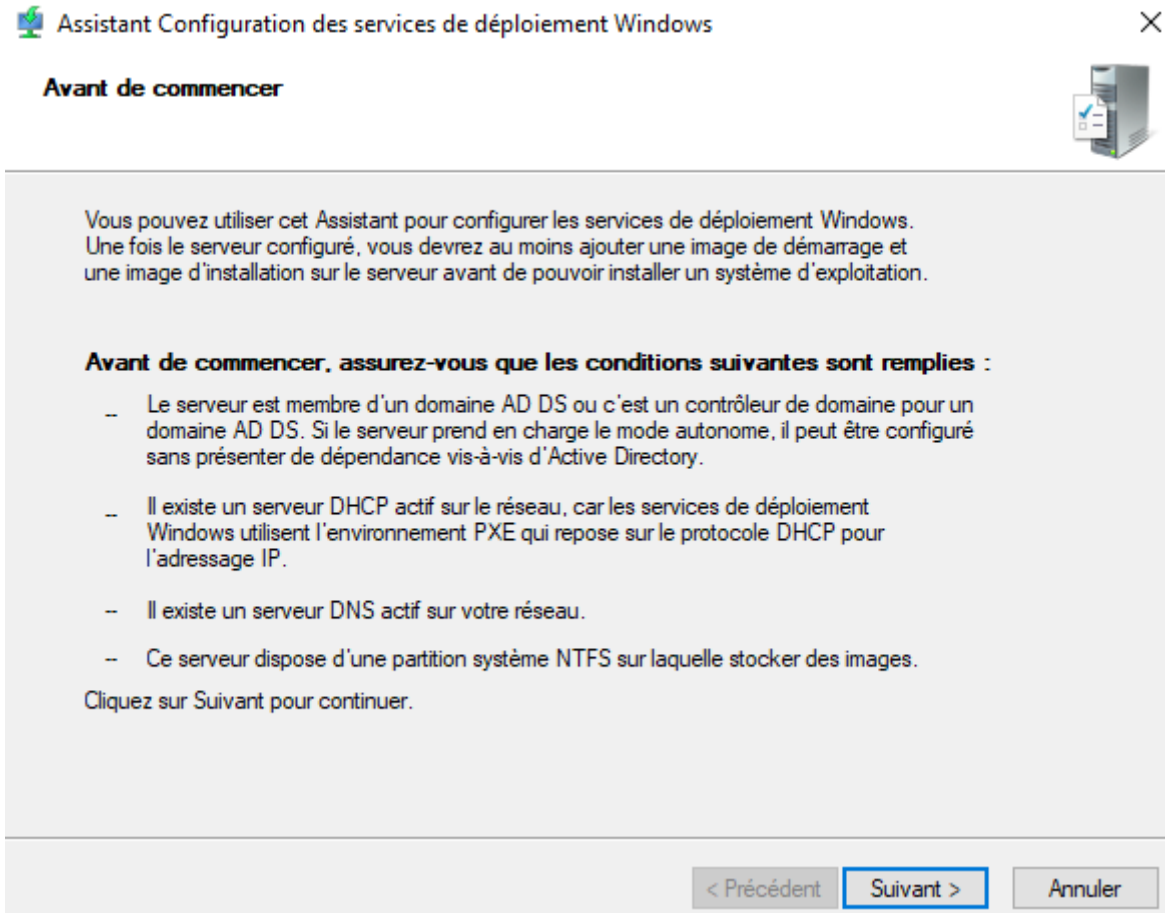
Sur votre serveur ADDS, ajouter le rôle `Service de déploiement Windows` et suivre les indication de l'assistant d'installation

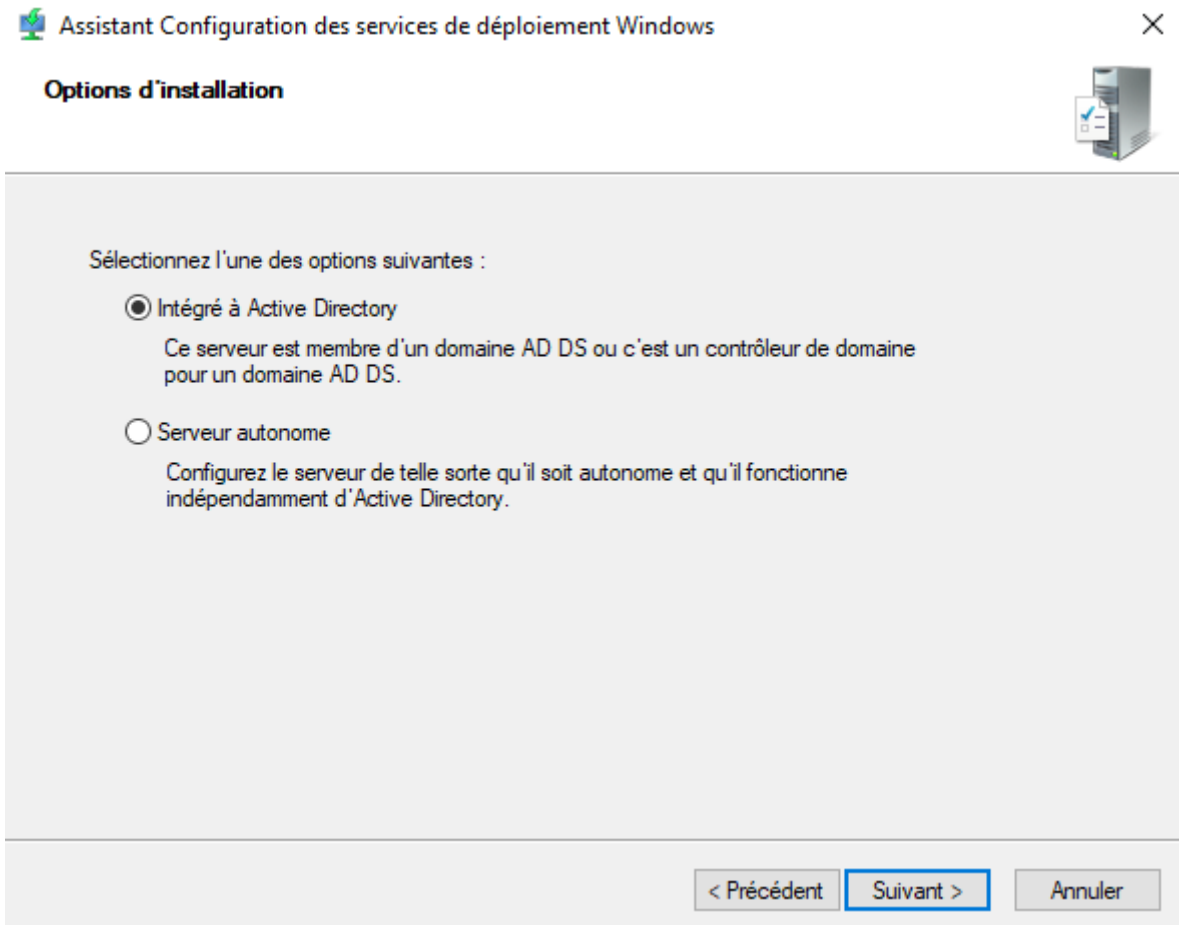


Paramétrer WDS :

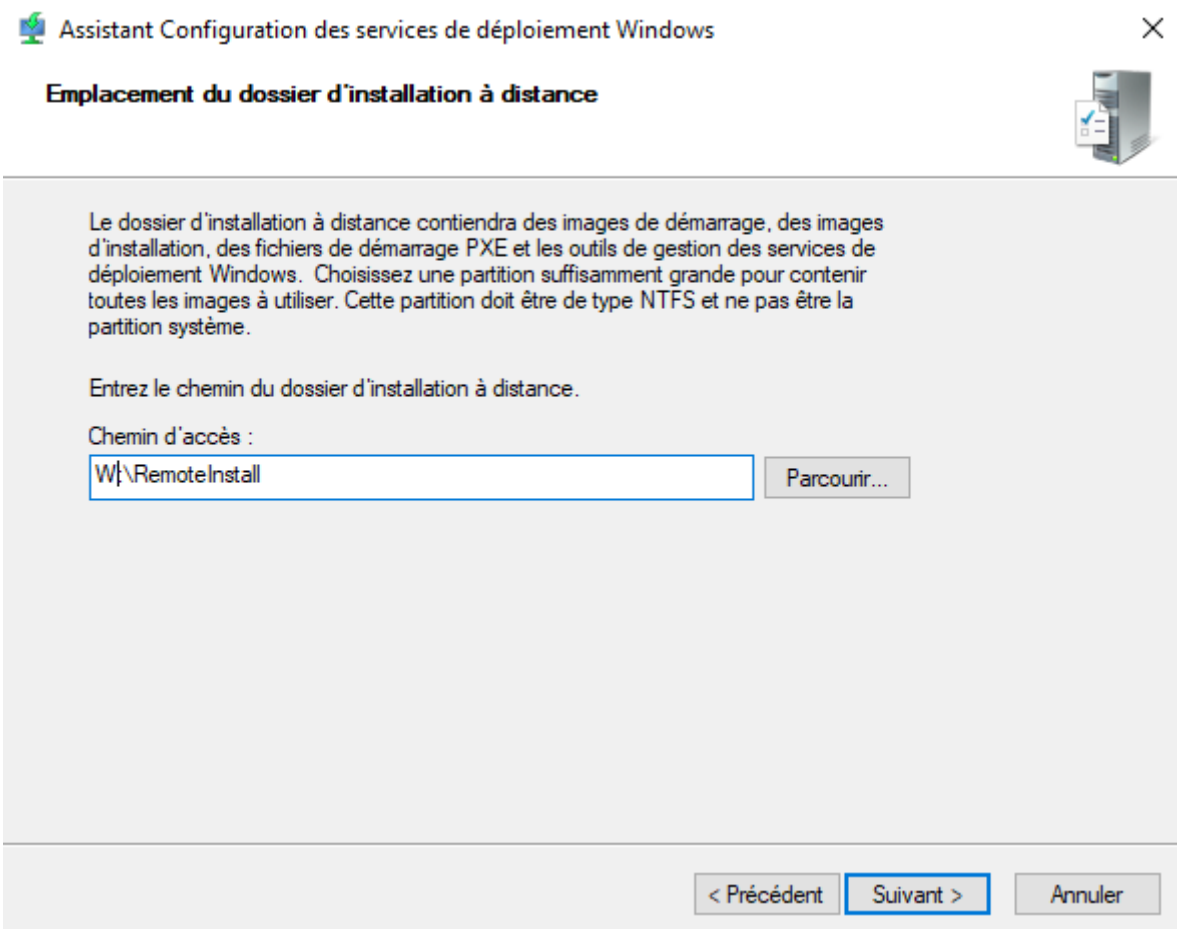
Outils > Services de déploiement Windows

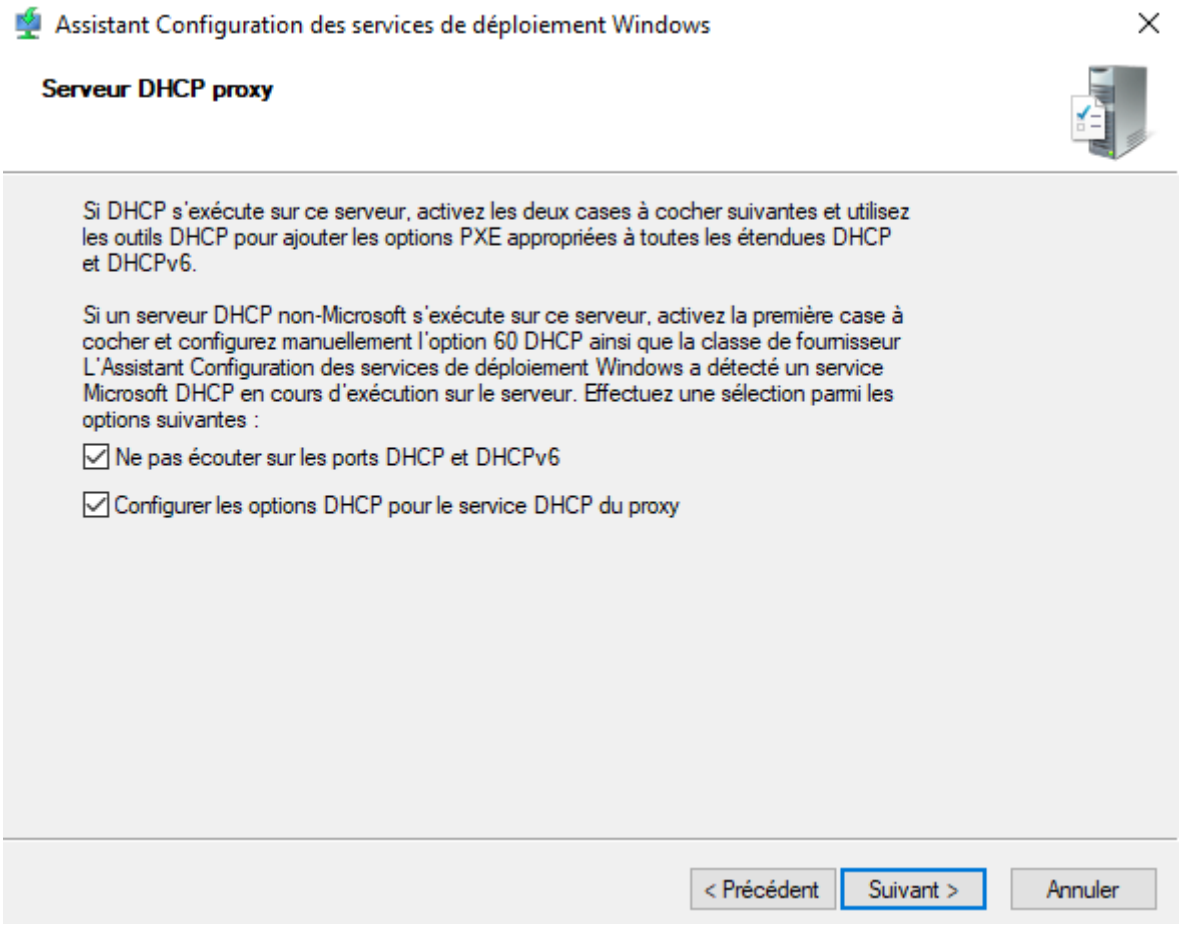


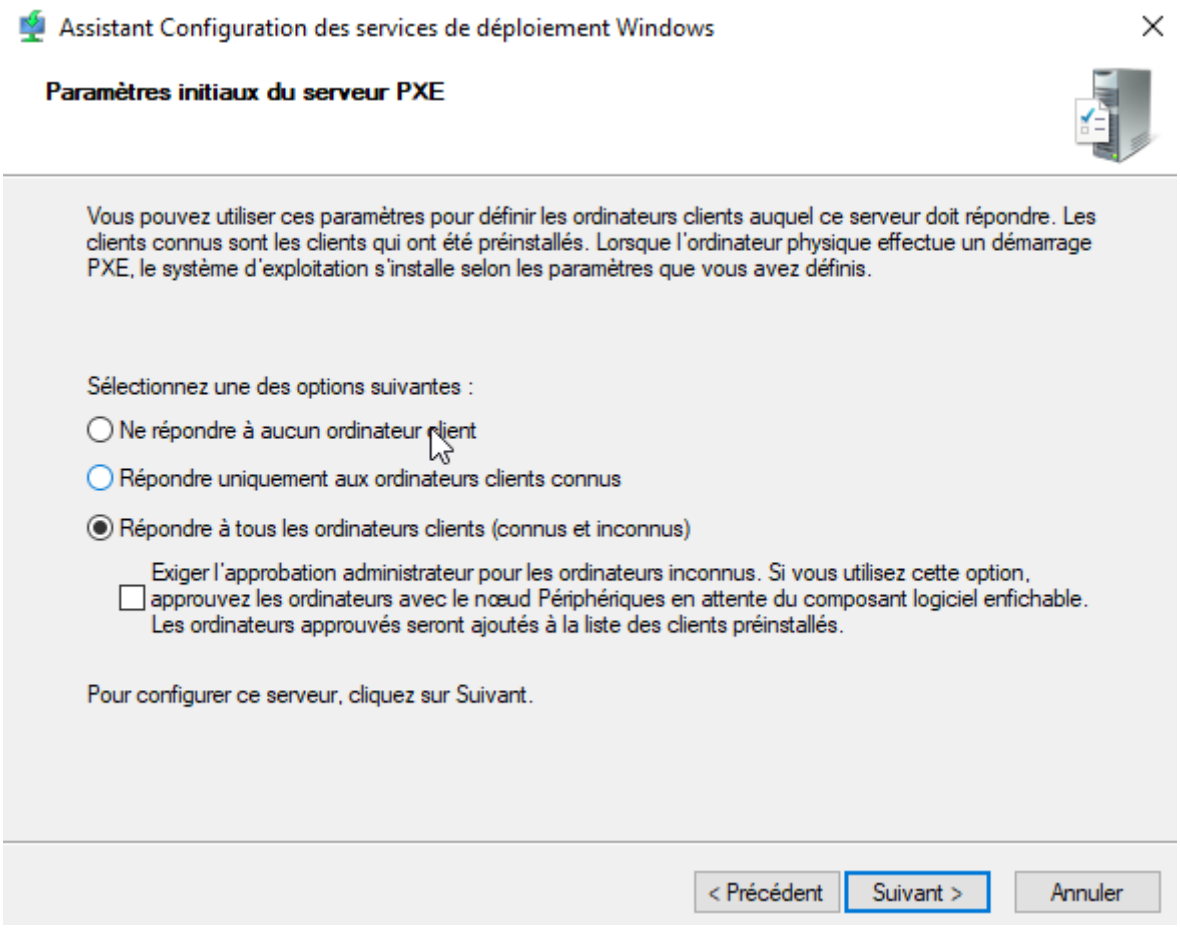




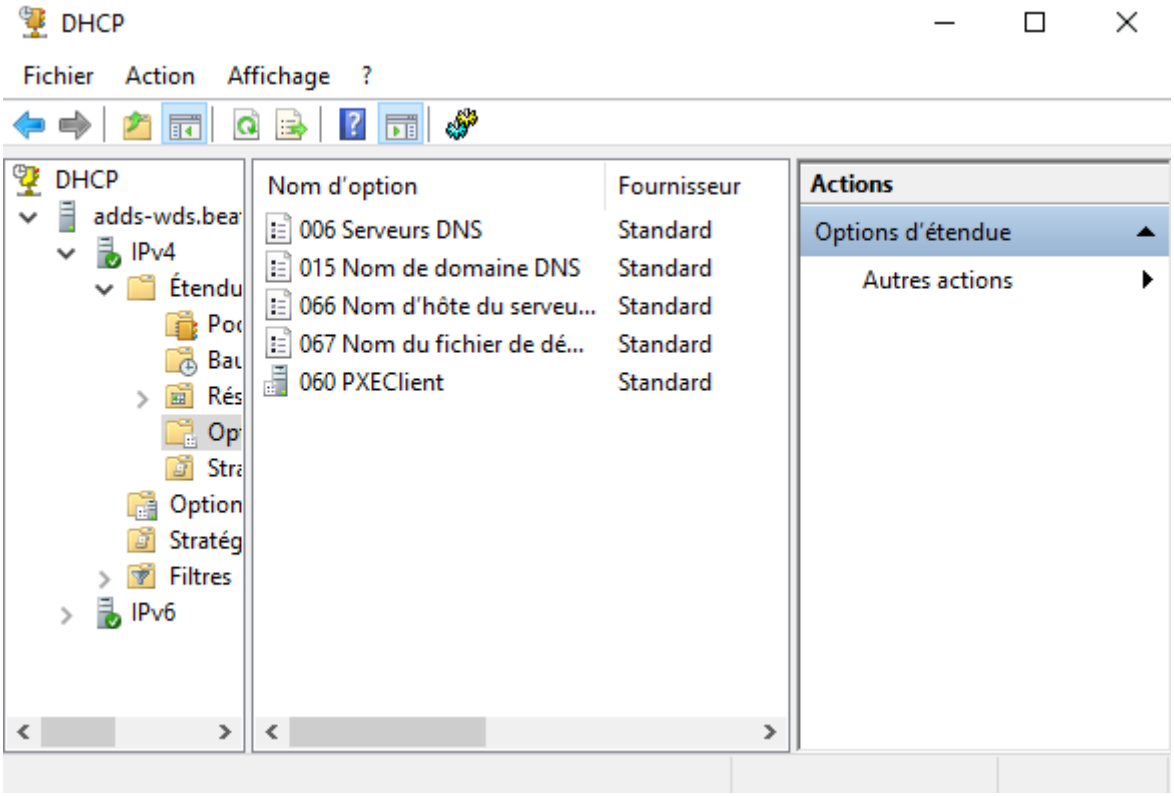
Spécifier le volume de stockage que vous souhaitez dédier à WDS


Assistant Configuration des services de déploiement Windows
Emplacement du dossier d'installation à distance
Le dossier d'installation à distance contiendra des images de démarrage, des images d'installation, des fichiers de démarrage PXE et les outils de gestion des services de déploiement Windows. Choisissez une partition suffisamment grande pour contenir toutes les images à utiliser. Cette partition doit être de type NTFS et ne pas être la partition système.
Entrez le chemin du dossier d'installation à distance.
Chemin d'accès :
W:\RemoteInstall
Parcourir...
< Précédent
Suivant >
Annuler

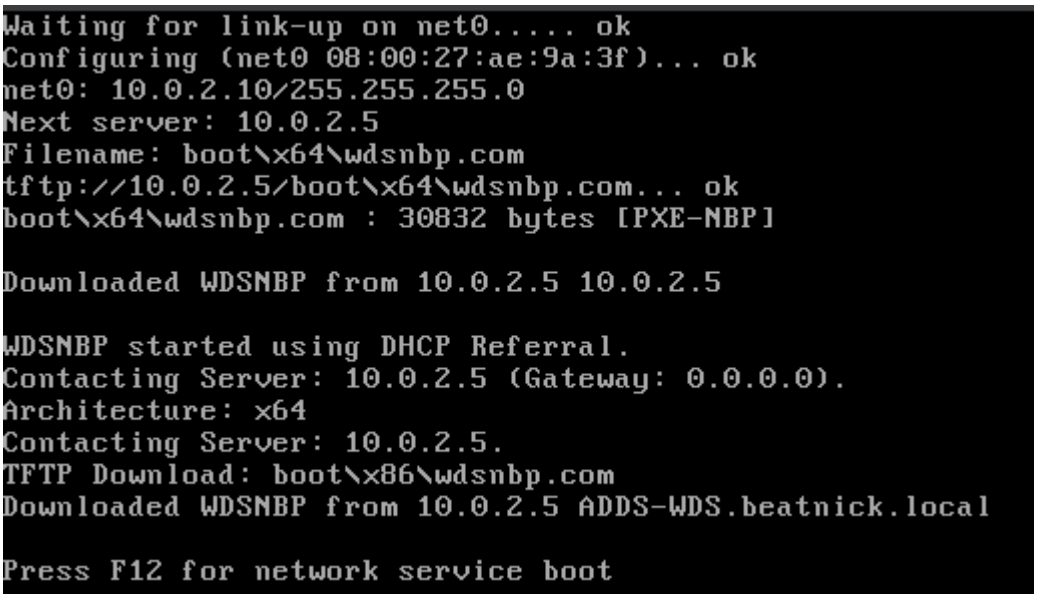

Assistant Configuration des services de déploiement Windows
Serveur DHCP proxy
Si DHCP s'exécute sur ce serveur, activez les deux cases à cocher suivantes et utilisez les outils DHCP pour ajouter les options PXE appropriées à toutes les étendues DHCP et DHCPv6.
Si un serveur DHCP non-Microsoft s'exécute sur ce serveur, activez la première case à cocher et configurez manuellement l'option 60 DHCP ainsi que la classe de fournisseur L'Assistant Configuration des services de déploiement Windows a détecté un service Microsoft DHCP en cours d'exécution sur le serveur. Effectuez une sélection parmi les options suivantes :
Ne pas écouter sur les ports DHCP et DHCPv6
Configurer les options DHCP pour le service DHCP du proxy
< Précédent
Suivant >
Annuler



Vous constatez suite à la configuration de WDS que l'option 60 s'est automatiquement ajoutée au DHCP

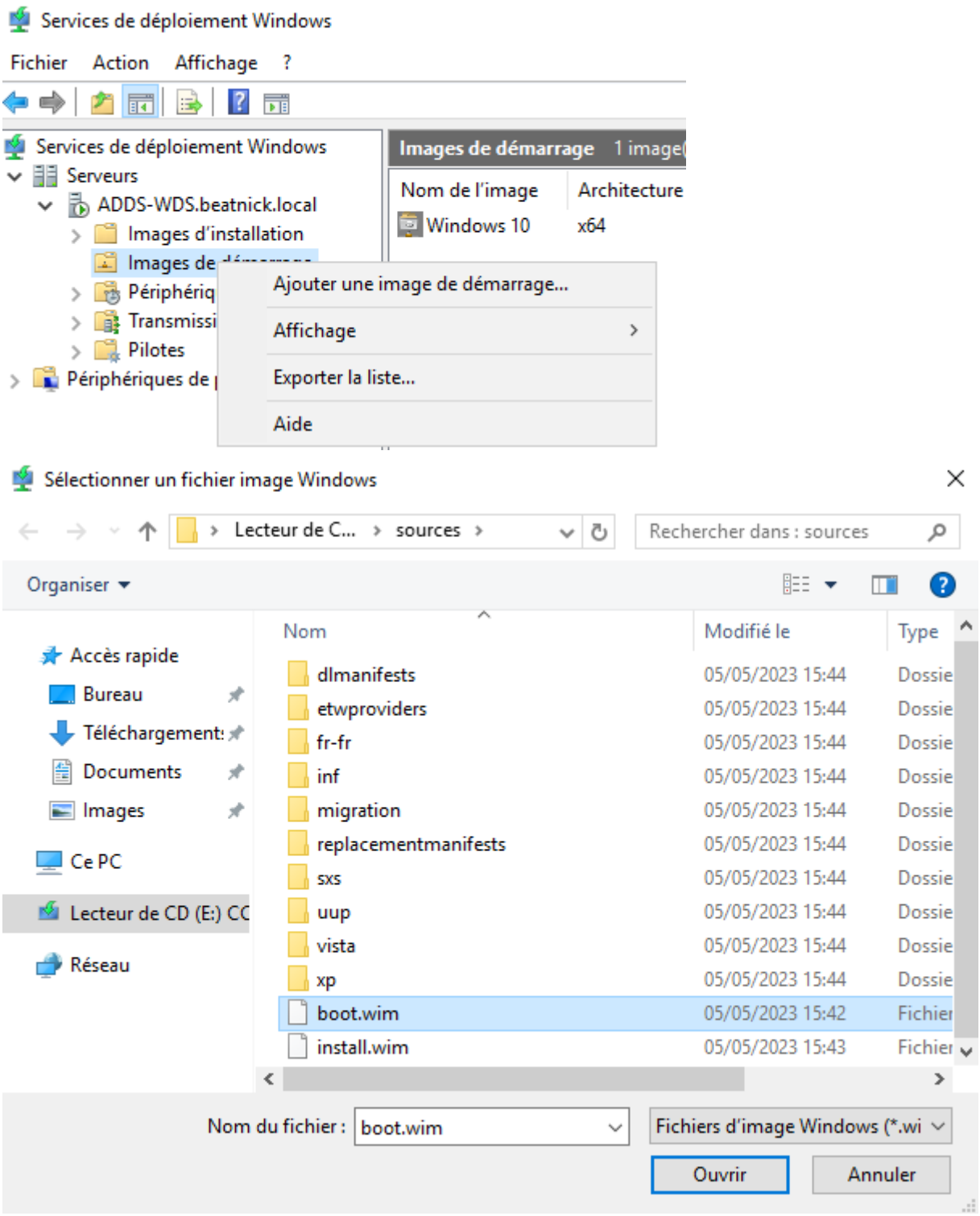


Pour tester le fonctionnement de notre WDS, lancer une machine cliente sans système d'exploitation, configurée pour démarrer sur le réseau. Si tout va bien, vous obtenez ceci :



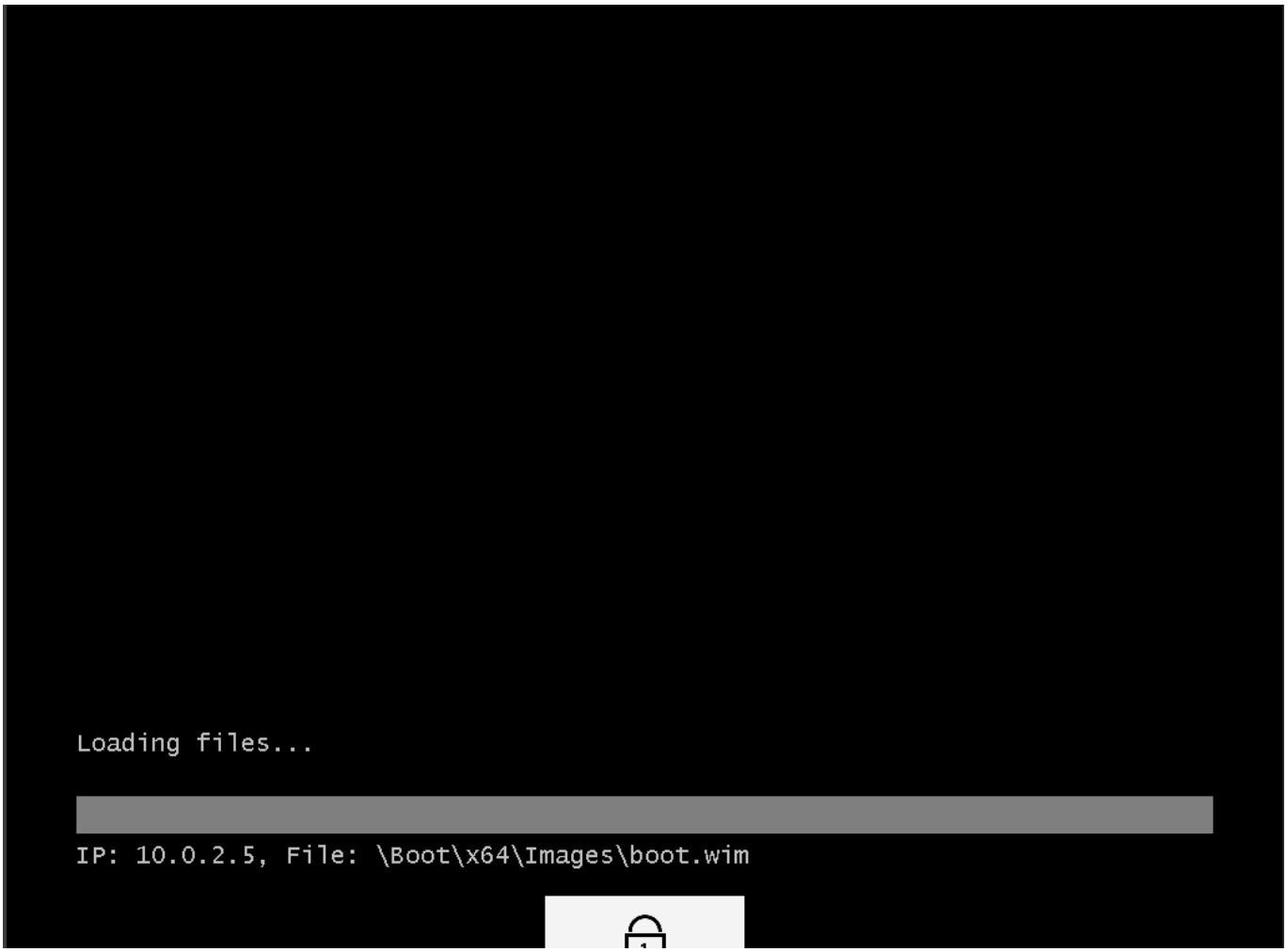
Maintenant que nous nous sommes assuré du bon fonctionnement, nous allons ajouter les images que nous voulons sur WDS

`Images de démarrage > Ajouter une image de démarrage > Parcourir`



Récupérer boot.wim depuis le cd d'installation de Win10 chargée dans le lecteur du serveur

De la même manière, charger `install.wim` dans le dossier `Images d'installation`

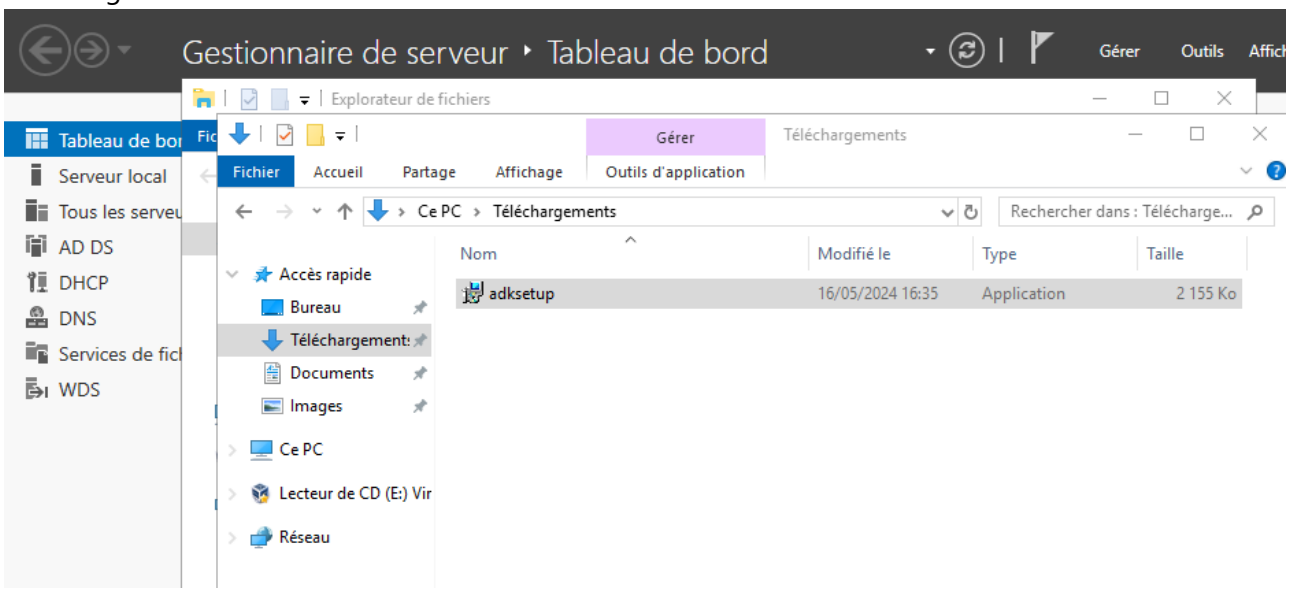


Notre poste client à maintenant une installation Windows Pro standard. Cependant, cette solution ne permet pas de personaliser l'installation. Pour cela, il va falloir passer par d'autres outils : Windows ADK et MDT.

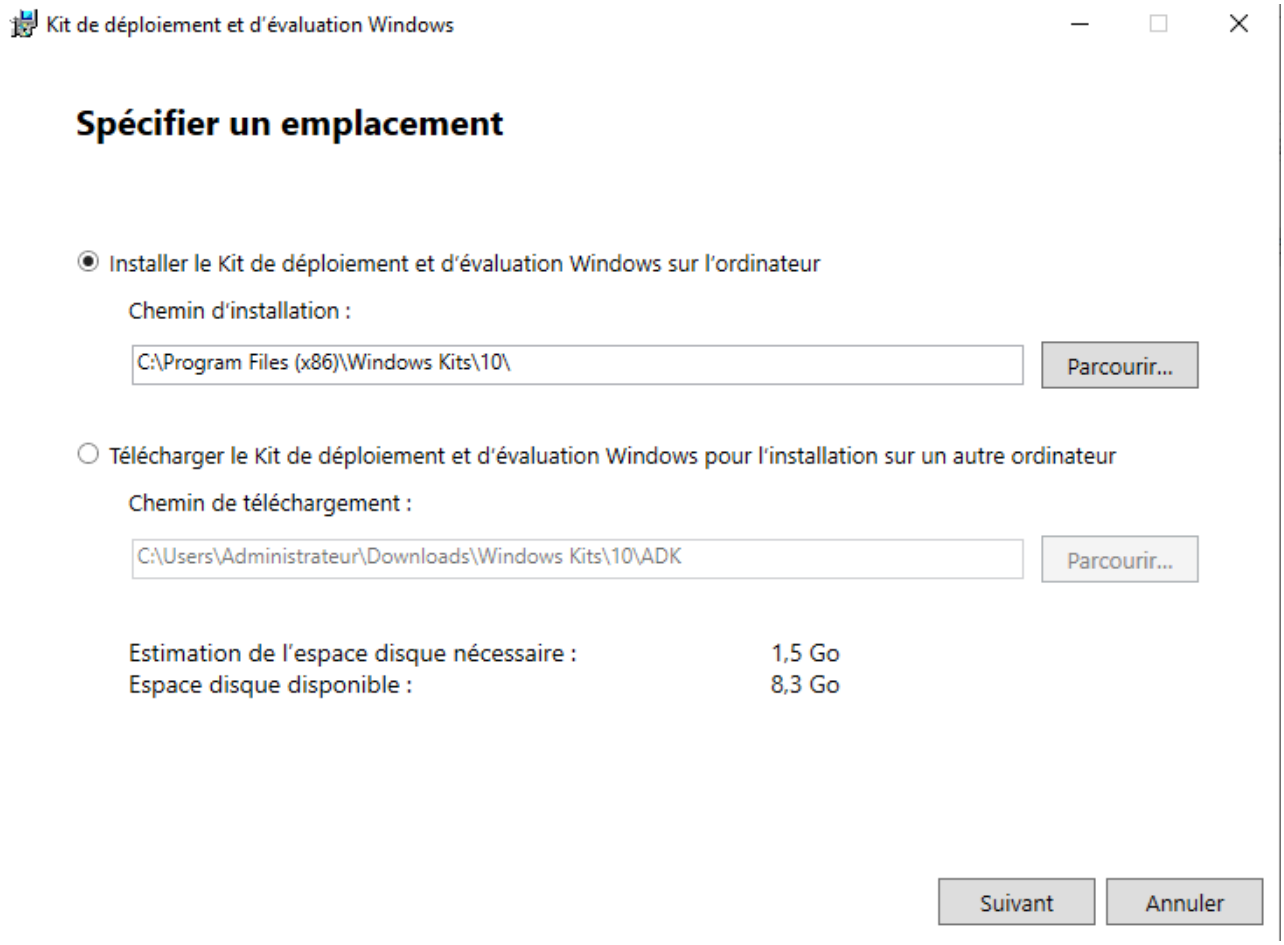
Paramétrer le DHCP pour prise en charge de l'UEFI

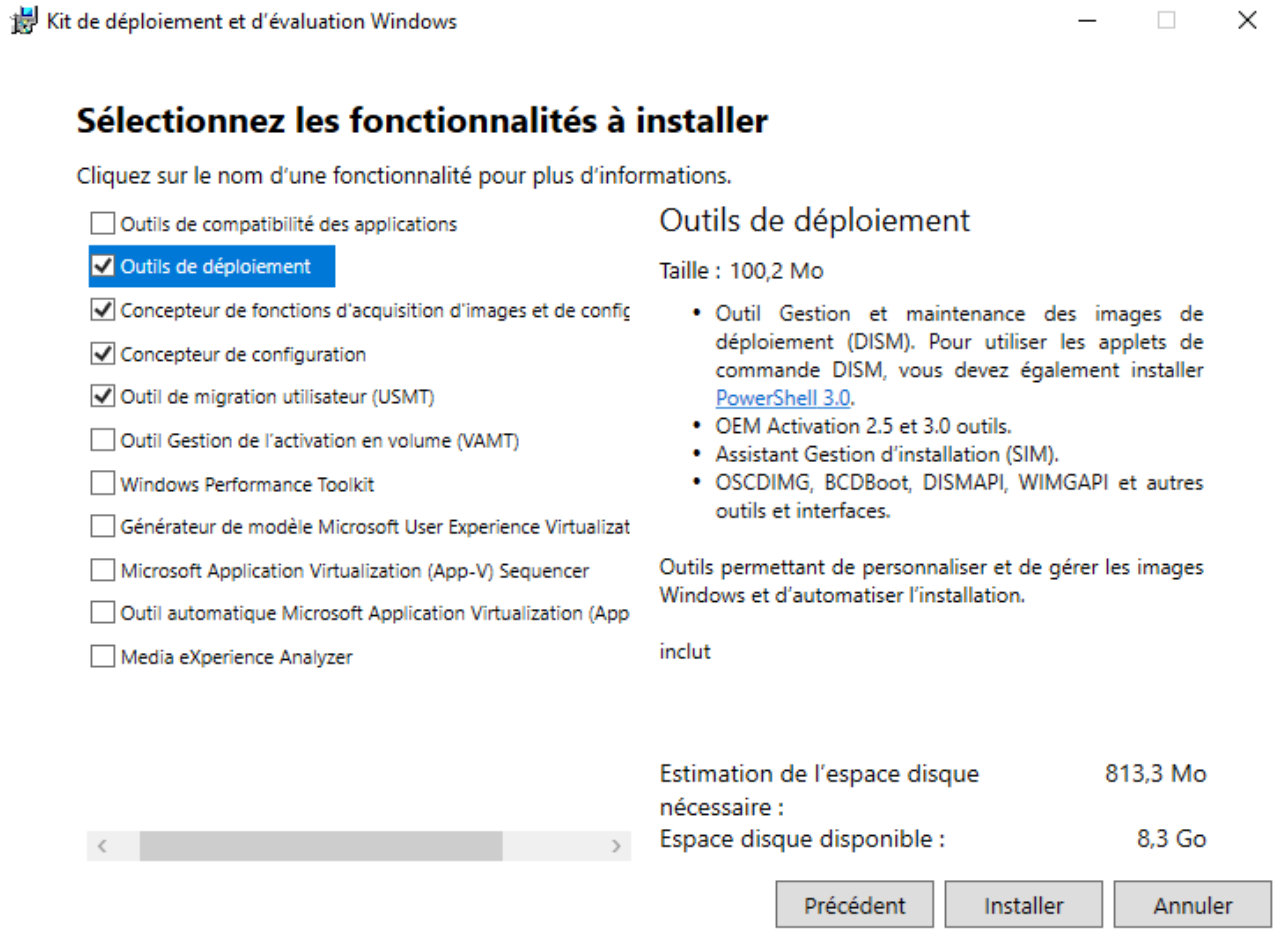
Installer Windows ADK

- Télécharger ADK

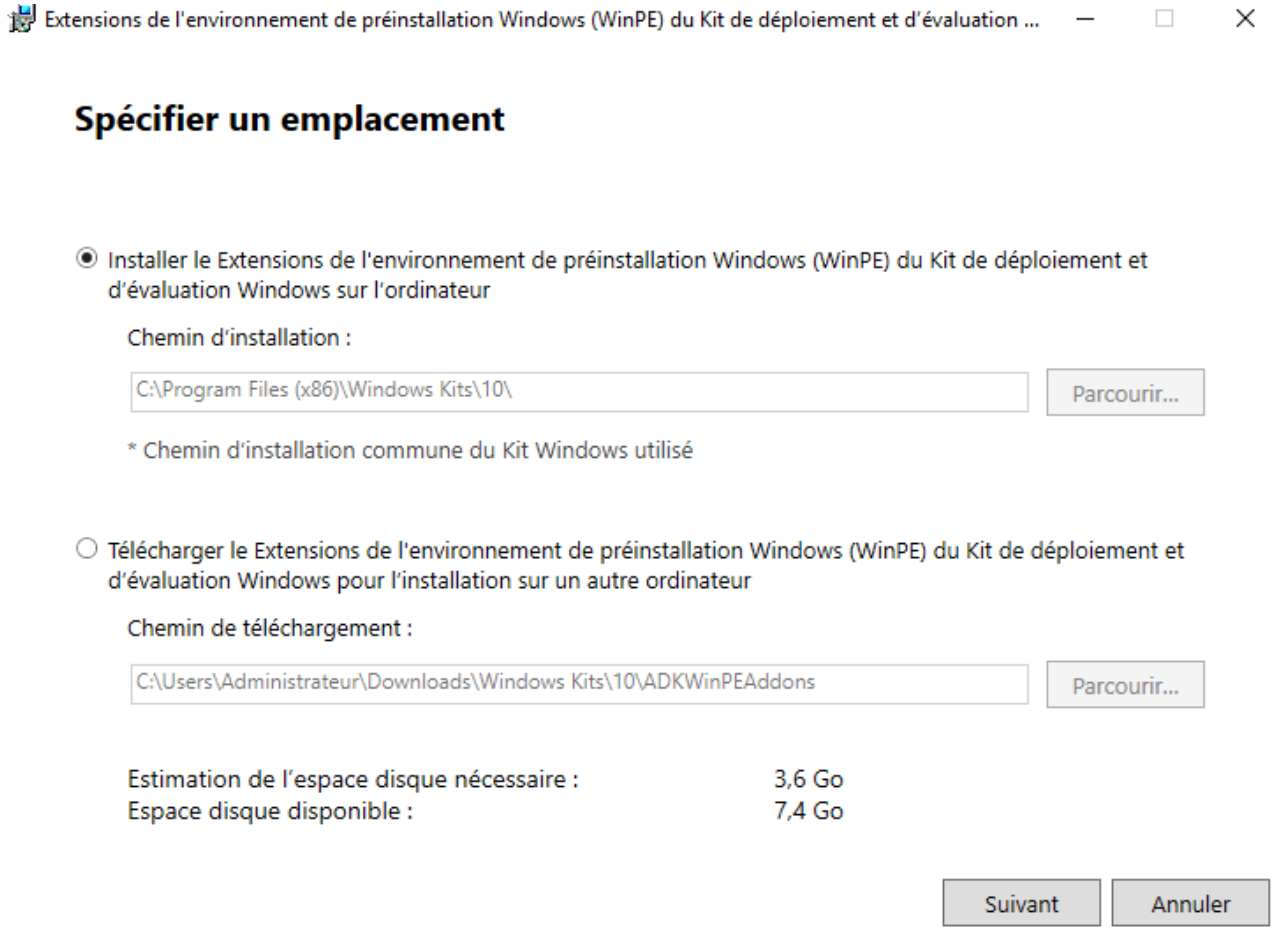


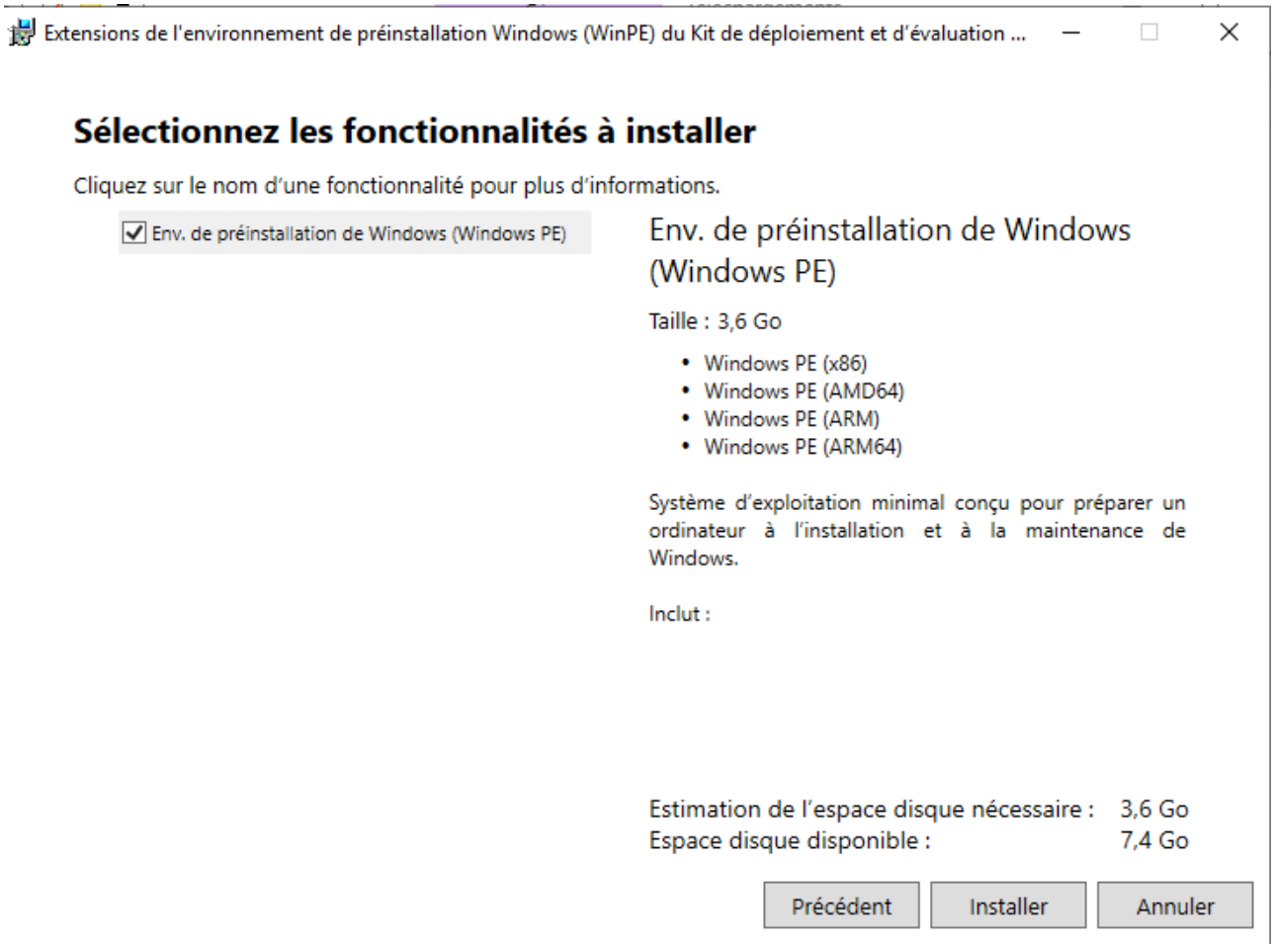
- Lancer l'assistant d'installation

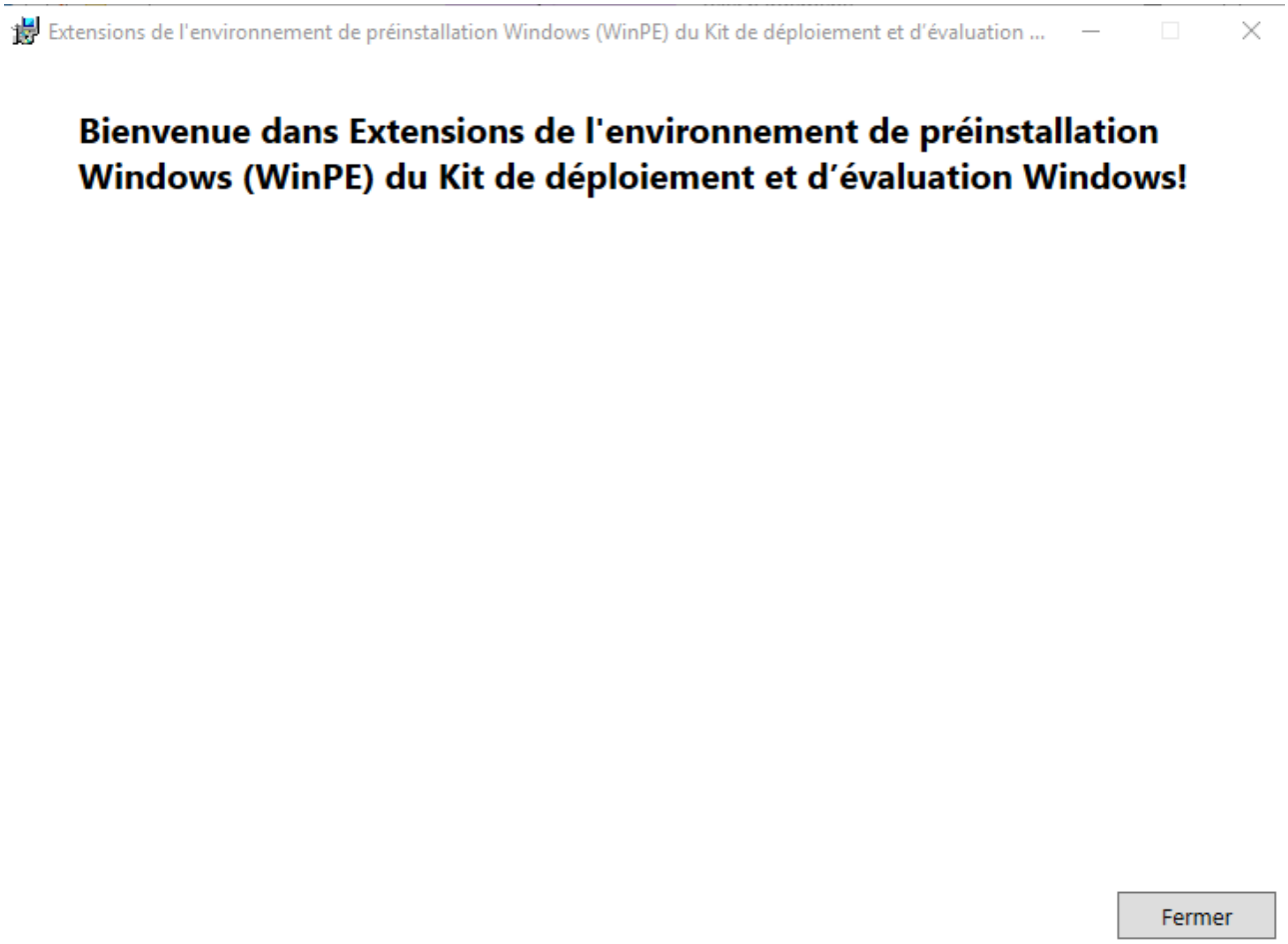




- Installer l'add-on Windows PE

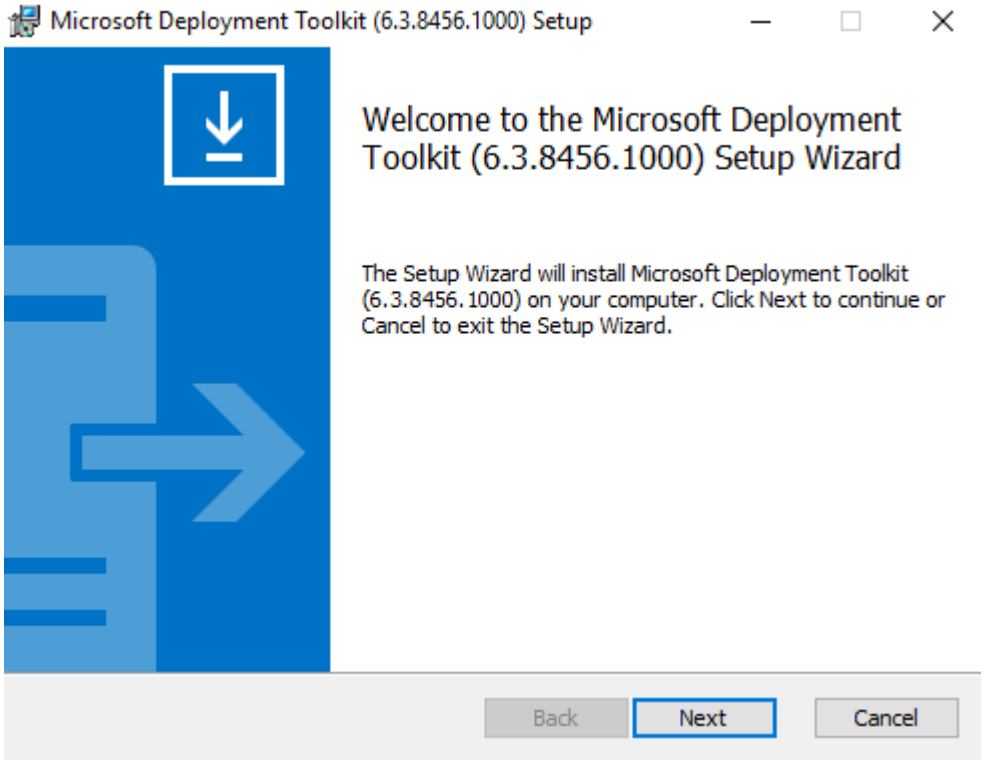


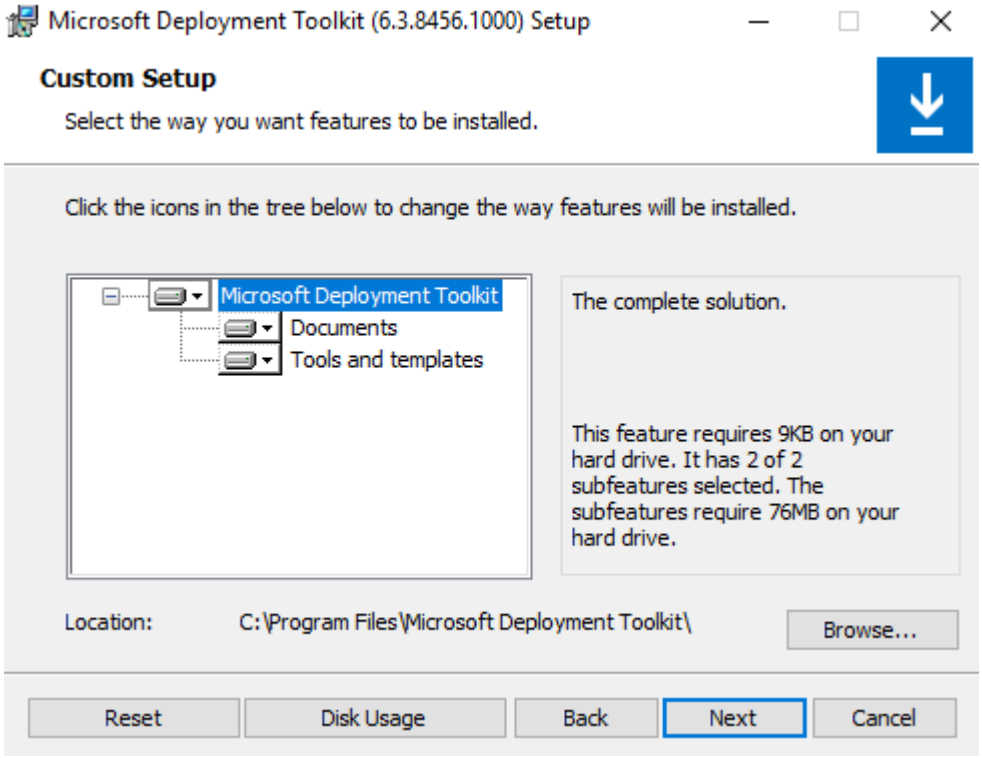


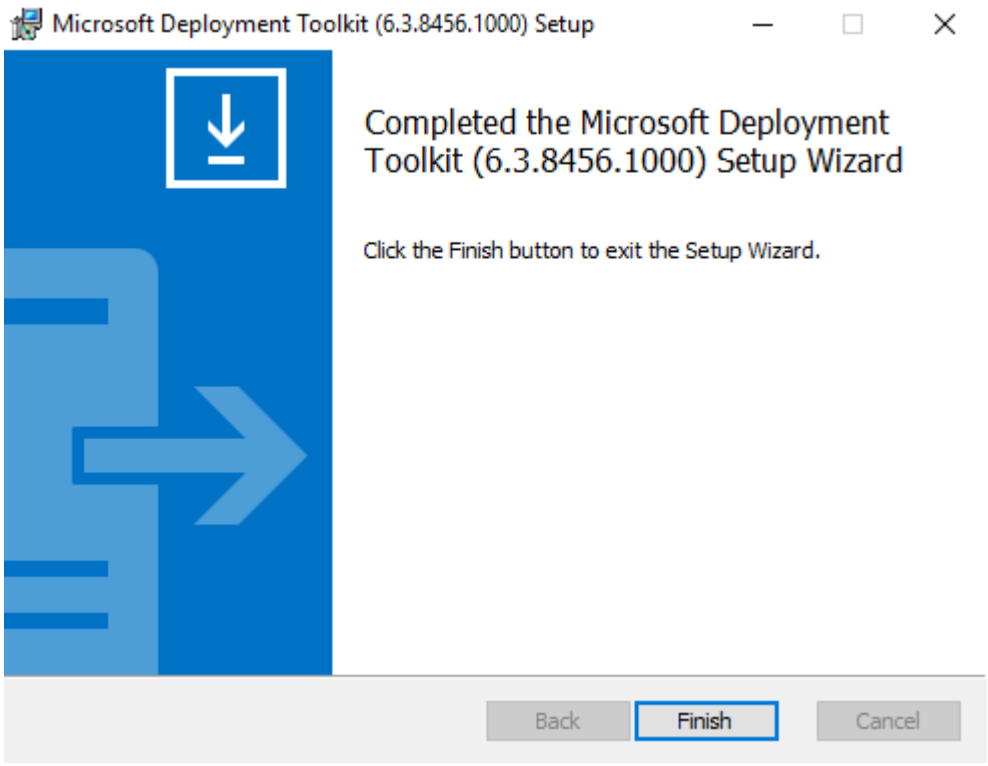


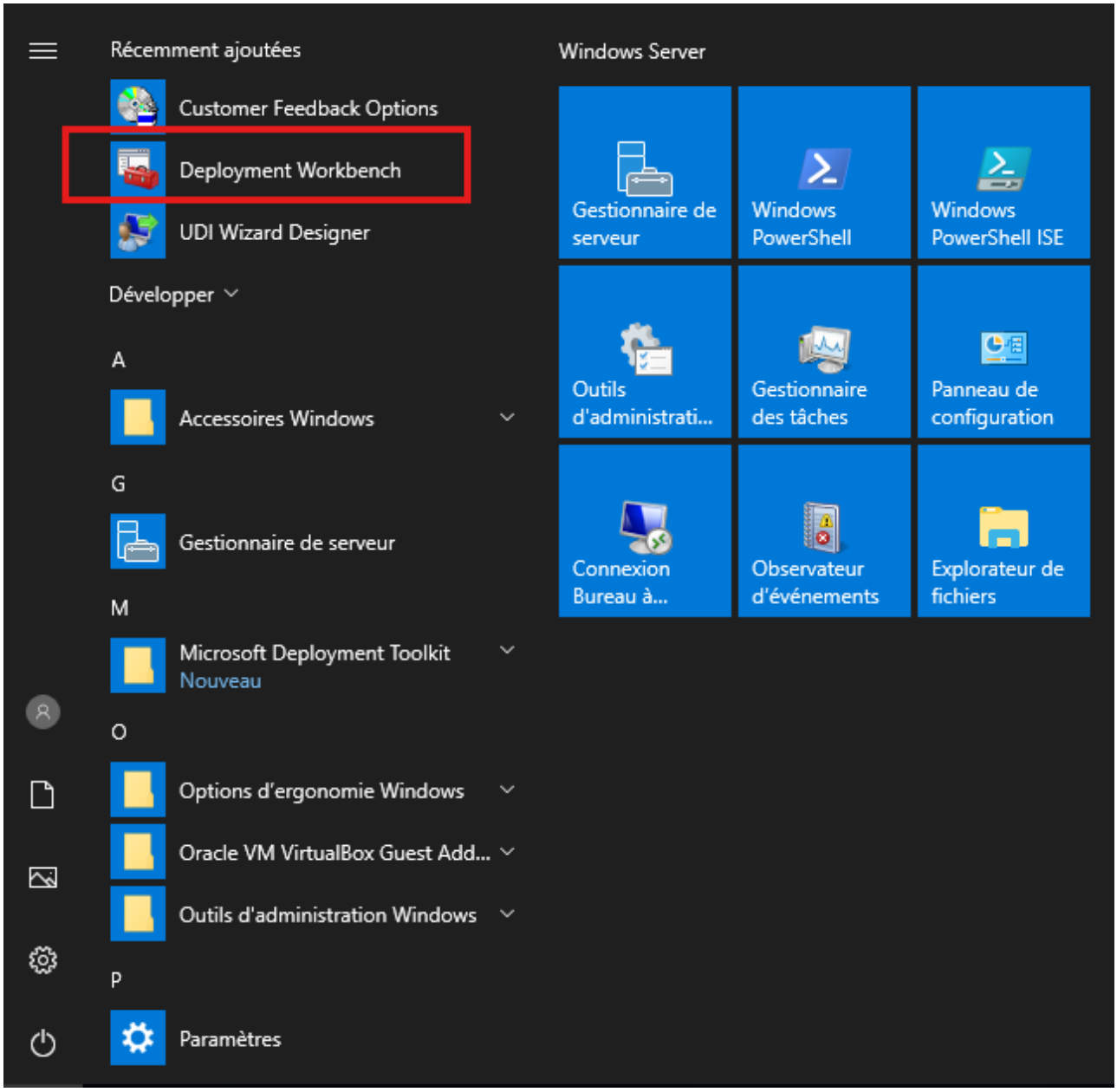
Installer MDT

- Télécharger MDT et lancer l'assistant

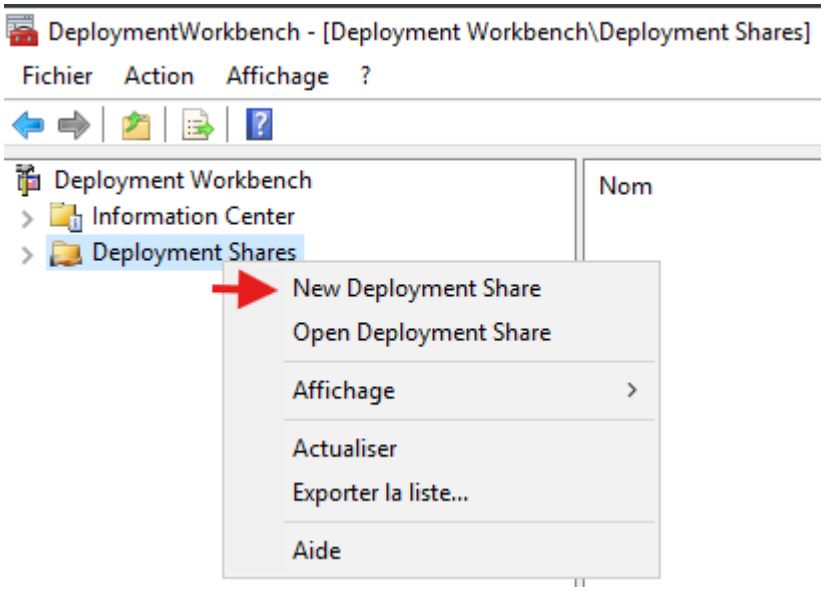


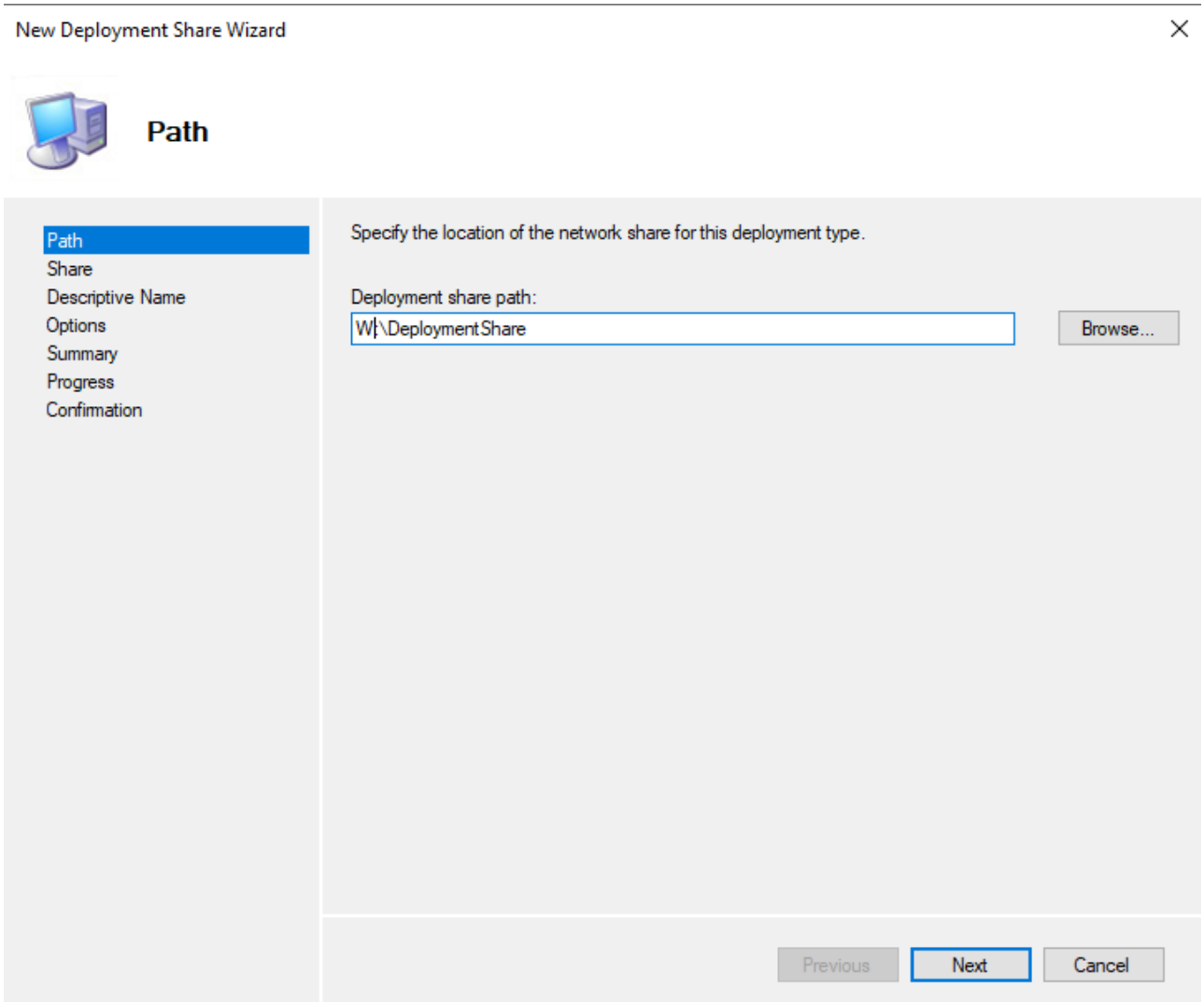


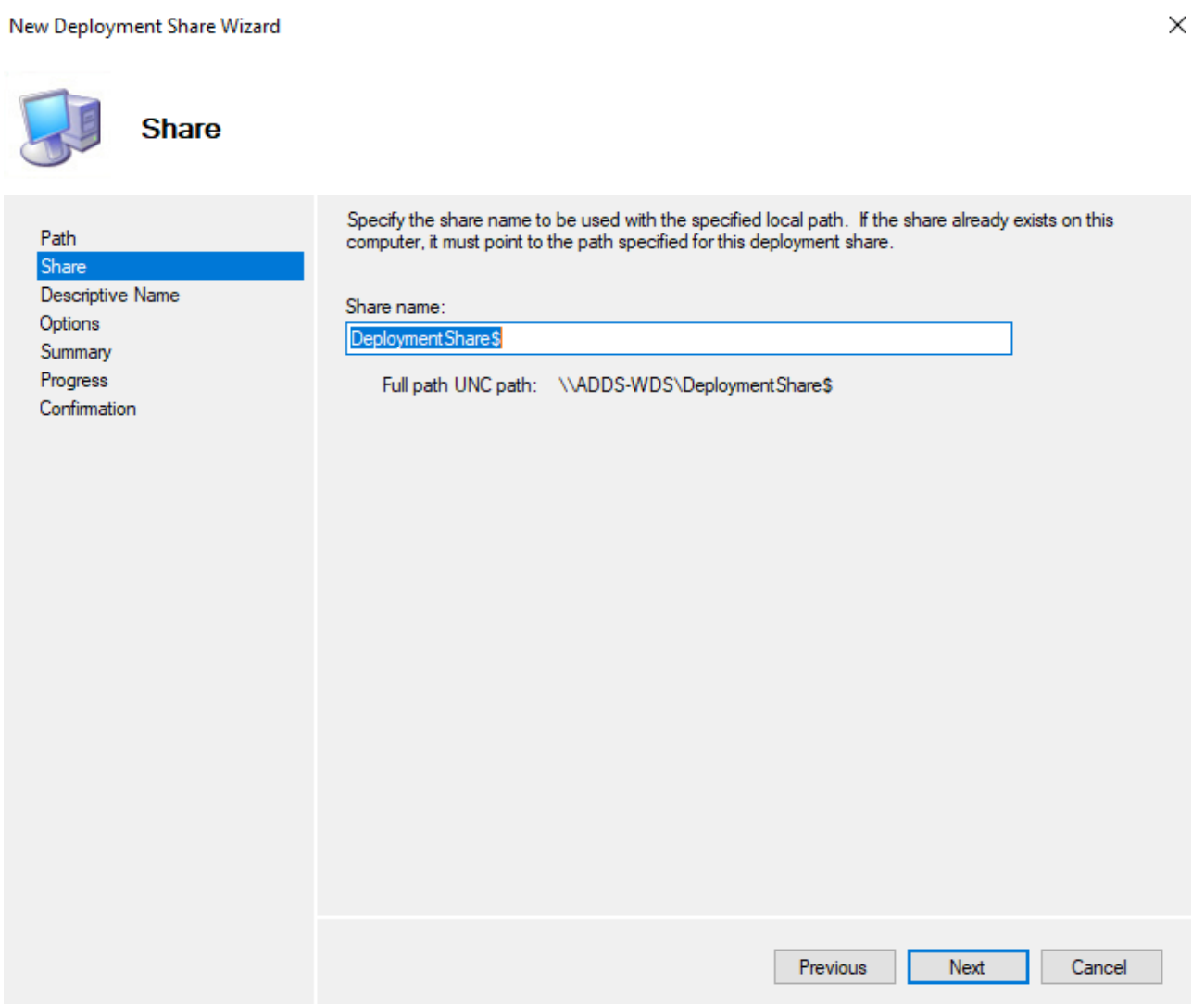

Microsoft Deployment Toolkit (6.3.8456.1000) Setup
Completed the Microsoft Deployment Toolkit (6.3.8456.1000) Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

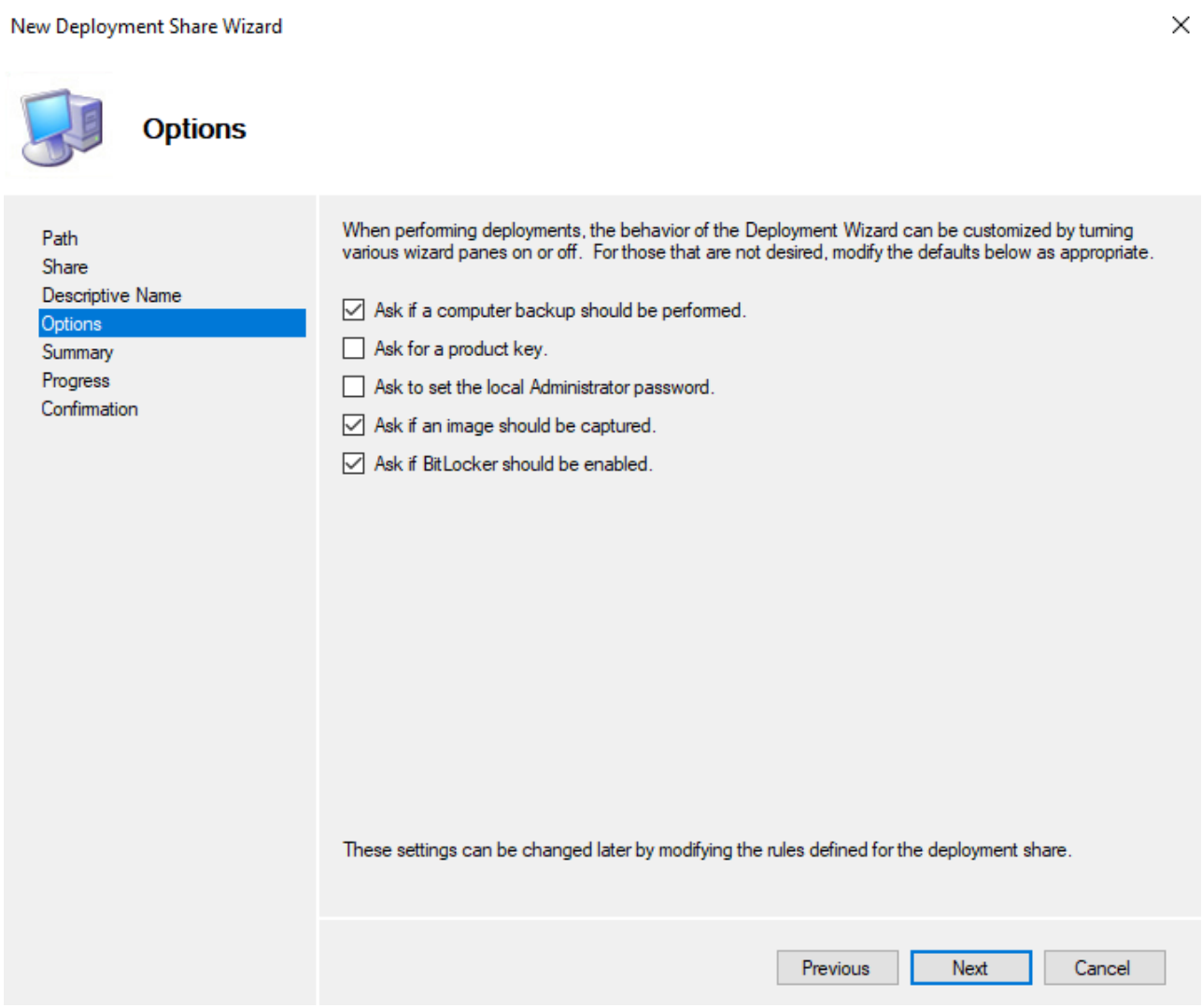

Récemment ajoutées
Customer Feedback Options
Deployment Workbench
UDI Wizard Designer
Développer
A
Accessoires Windows
G
Gestionnaire de serveur
M
Microsoft Deployment Toolkit
Nouveau
O
Options d'ergonomie Windows
Oracle VM VirtualBox Guest Add...
Outils d'administration Windows
P
Paramètres
Windows Server
Gestionnaire de serveur
Windows PowerShell
Windows PowerShell ISE
Outils d'administrati...
Gestionnaire des tâches
Panneau de configuration
Connexion Bureau à...
Observateur d'événements
Explorateur de fichiers

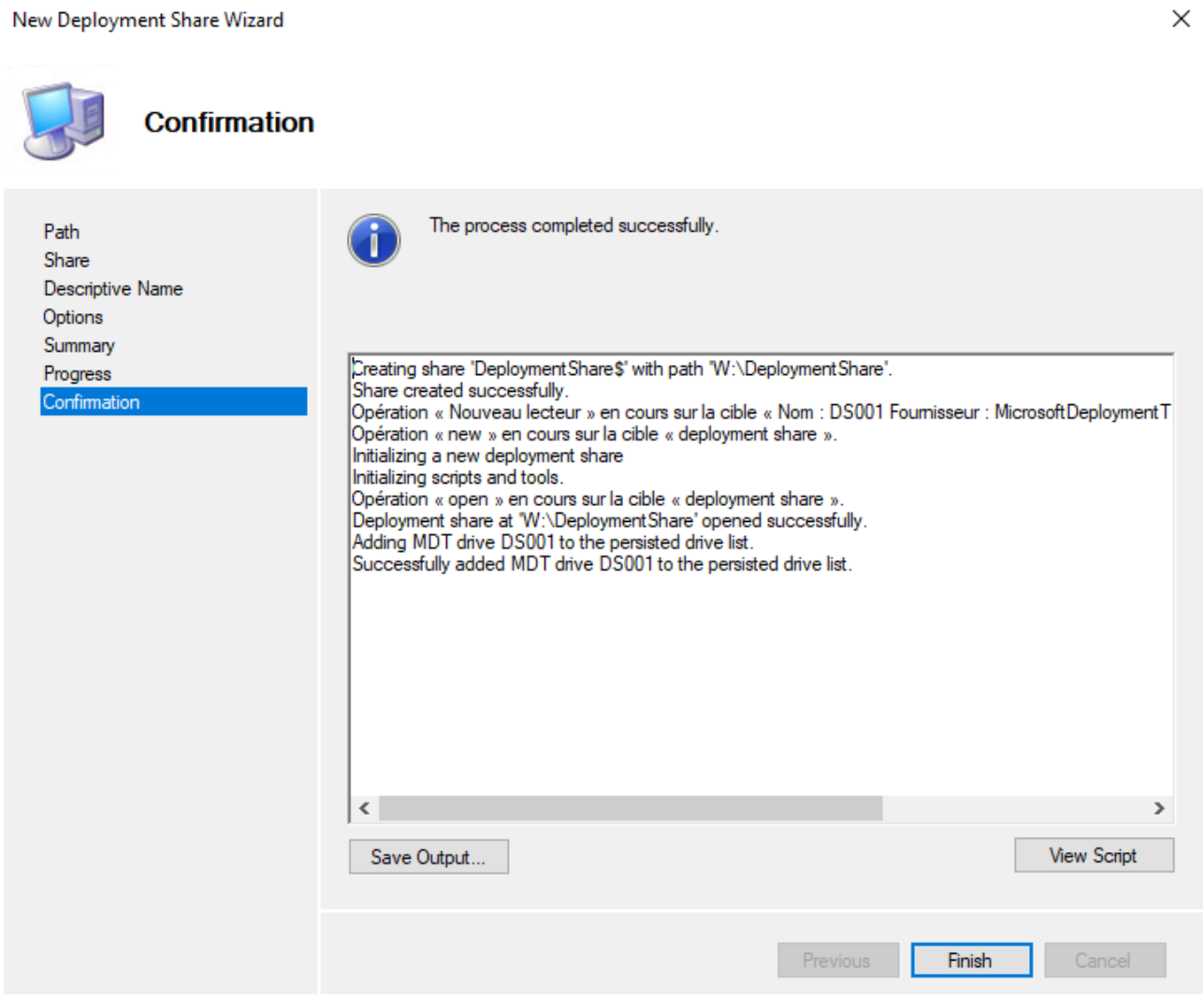
- Créer le deployment share via le Deployment Workbench



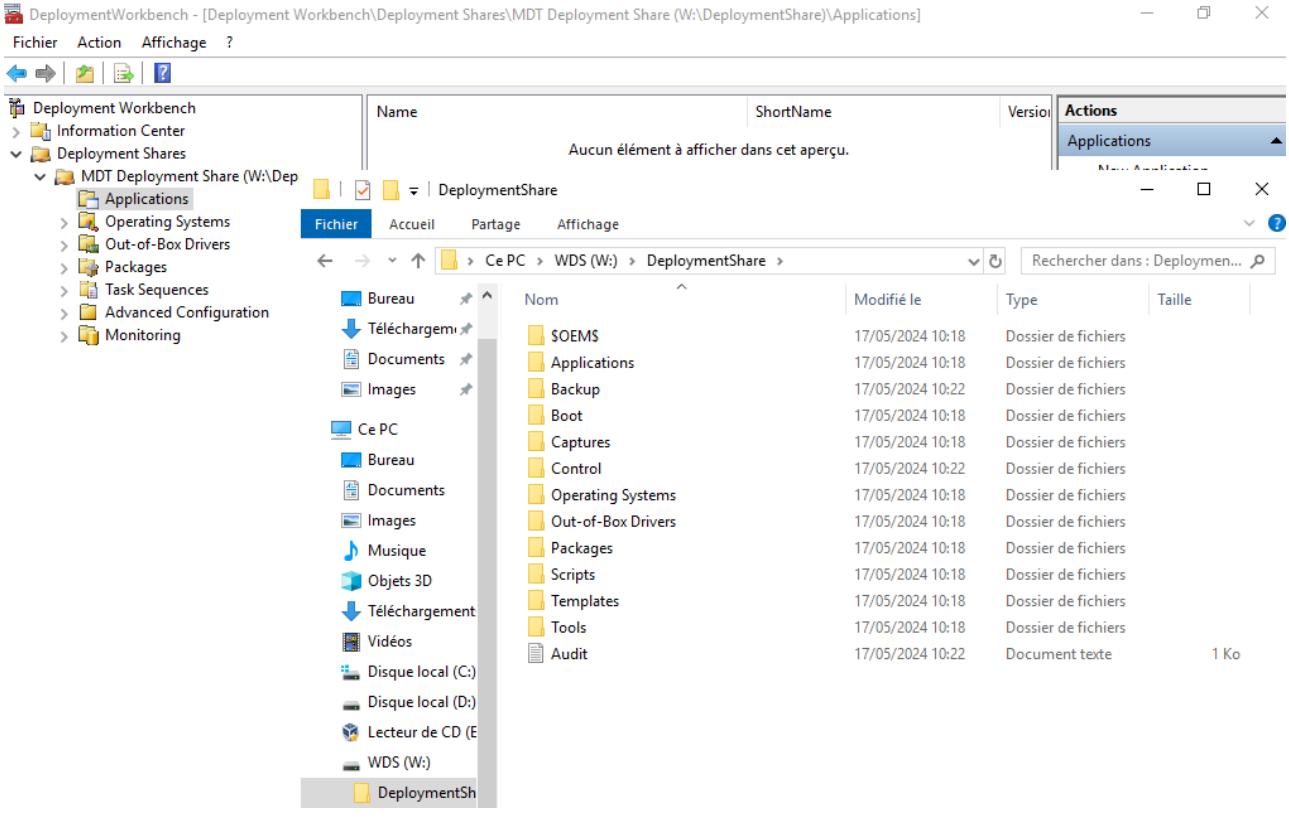



New Deployment Share Wizard
Share
Path
Share
Descriptive Name
Options
Summary
Progress
Confirmation
Specify the share name to be used with the specified local path. If the share already exists on this computer, it must point to the path specified for this deployment share.
Share name:
DeploymentShare$
Full path UNC path: \\ADDS-WDS\DeploymentShare$
Previous
Next
Cancel


New Deployment Share Wizard
Options
Path
Share
Descriptive Name
Options
Summary
Progress
Confirmation
When performing deployments, the behavior of the Deployment Wizard can be customized by turning various wizard panes on or off. For those that are not desired, modify the defaults below as appropriate.
Ask if a computer backup should be performed.
Ask for a product key.
Ask to set the local Administrator password.
Ask if an image should be captured.
Ask if BitLocker should be enabled.
These settings can be changed later by modifying the rules defined for the deployment share.
Previous
Next
Cancel



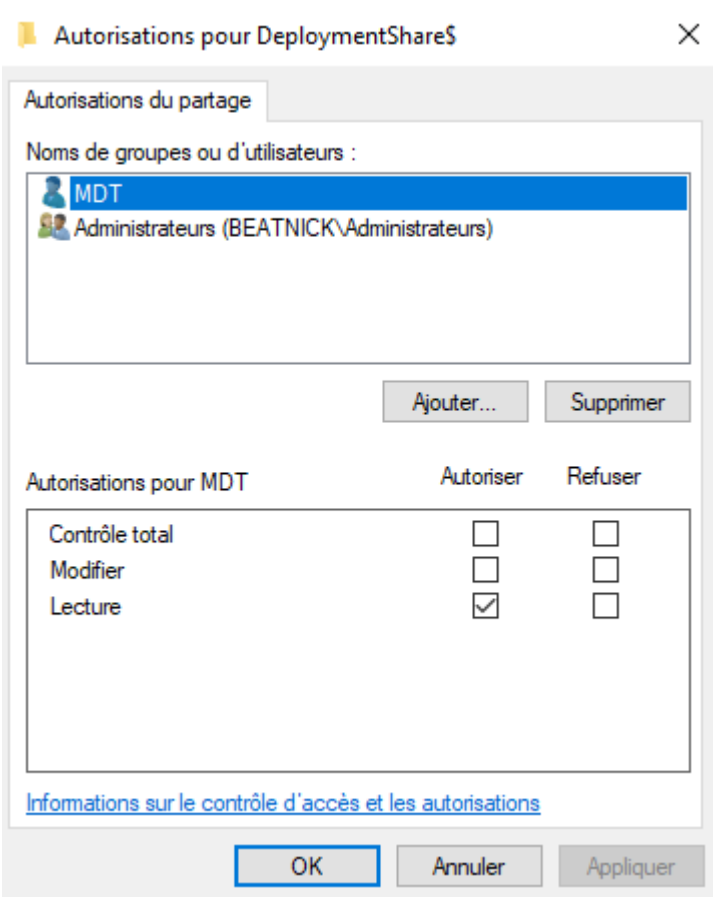
Une fois le partage configuré, vous obtenez ceci, côté Workbench et Explorateur de fichiers



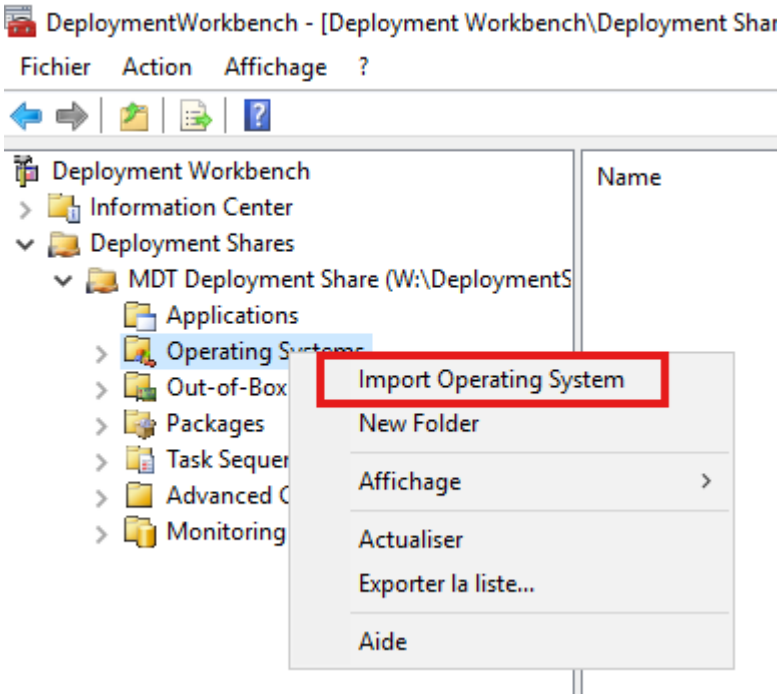
- Script PS de création d'utilisateur local dédié à MDT il est nécessaire, lors du démarage de la machine qui se connecte au partage, qu'elle puisse utiliser un compte utilisateur avec lres droit de lecture et d'exécution

```
  # Spécifier le nom et le mot de passe du compte de service
  $ServiceAccountName = "Service_MDT"
  $ServiceAccountPassword = ConvertTo-SecureString "V0treMDP!" -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
  $MDTSharePath = "\\$env:COMPUTERNAME\DeploymentShare$"
  $Acl = Get-Acl $MDTSharePath
  $Rule = New-Object
System.Security.AccessControl.FileSystemAccessRule("Service_MDT","ReadAndExe
cute", "ContainerInherit, ObjectInherit", "None", "Allow")
  $Acl.SetAccessRule($Rule)
  Set-Acl $MDTSharePath $Acl
```

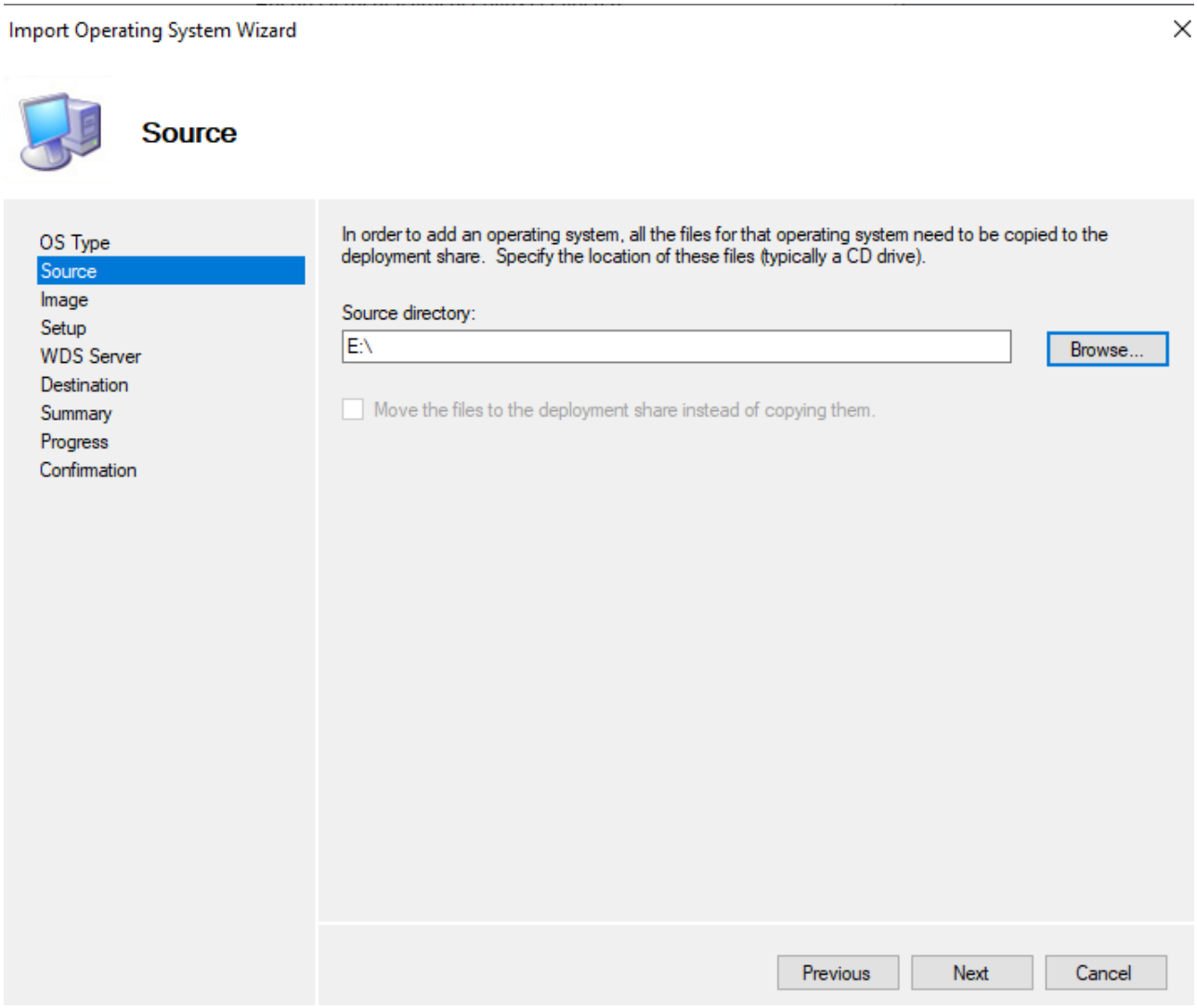
```
PS C:\Users\Administrateur\Documents> .\Service_MDT.ps1

Name        Enabled Description
----        ------- -----------
Service_MDT True    Compte de service pour MDT

AccessControlType : Allow
AccessRight       : Full
AccountName       : BUILTIN\Administrateurs
Name              : DeploymentShare$
ScopeName         : *
PSComputerName    :


AccessControlType : Allow
AccessRight       : Read
AccountName       : BEATNICK\Service_MDT
Name              : DeploymentShare$
ScopeName         : *
PSComputerName    :
```

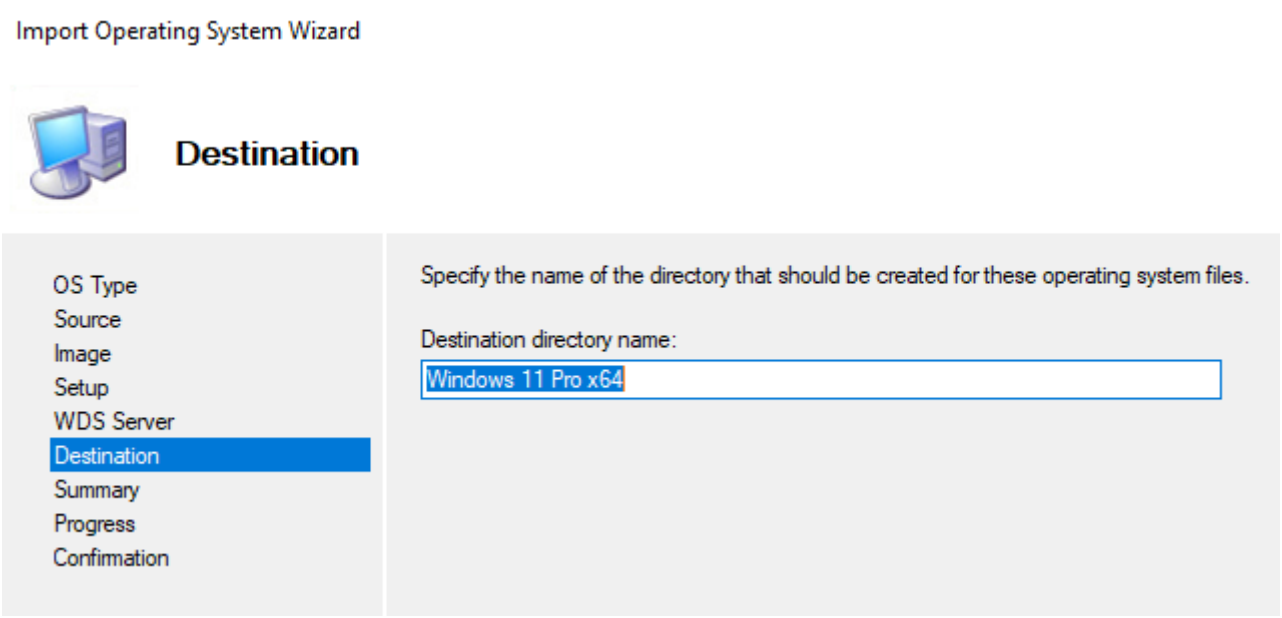


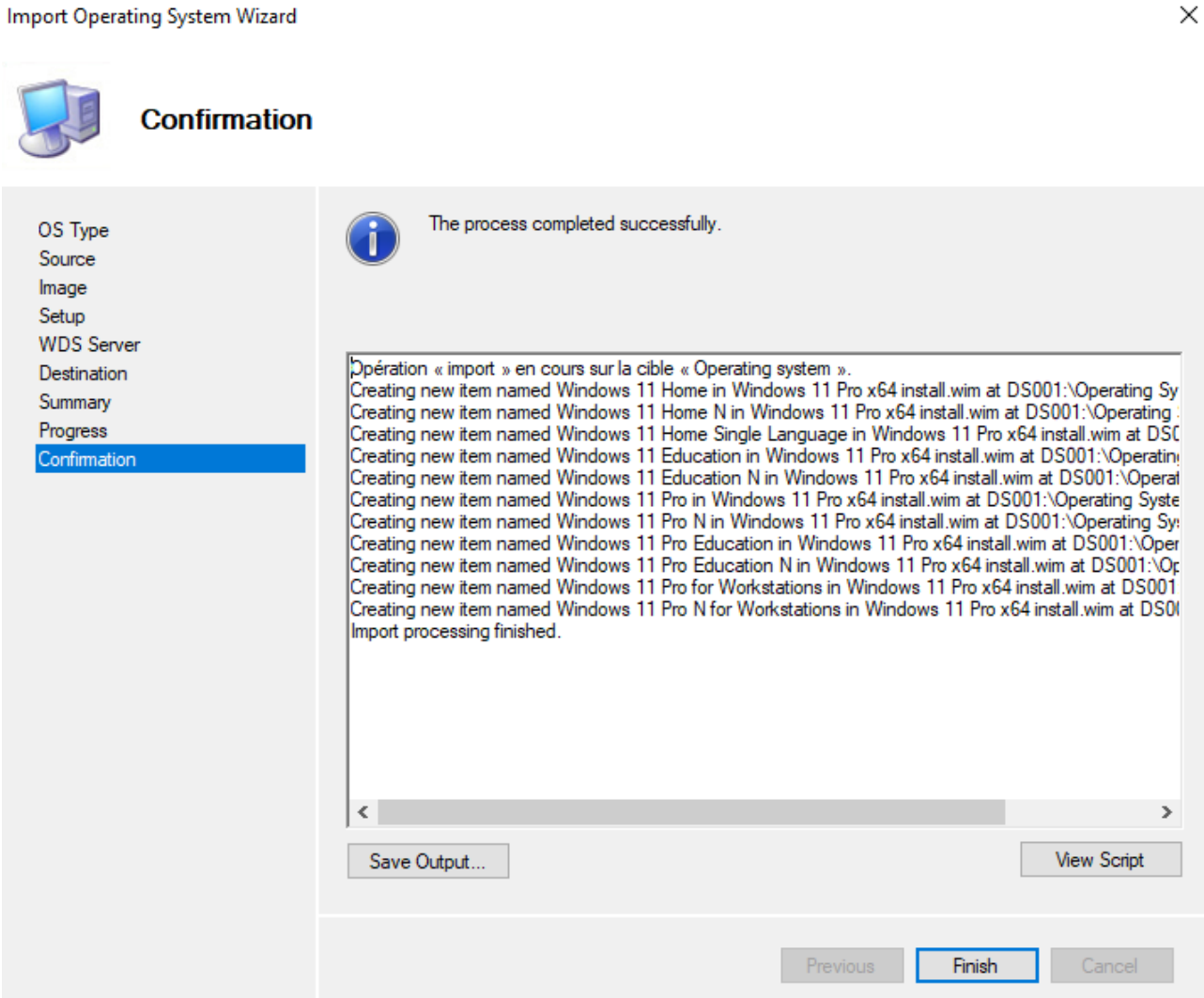
- Importer une image Windows 11



Importer l'image montée dans le lecteur, autrement, dans source, sélectionné votre lecteur optique



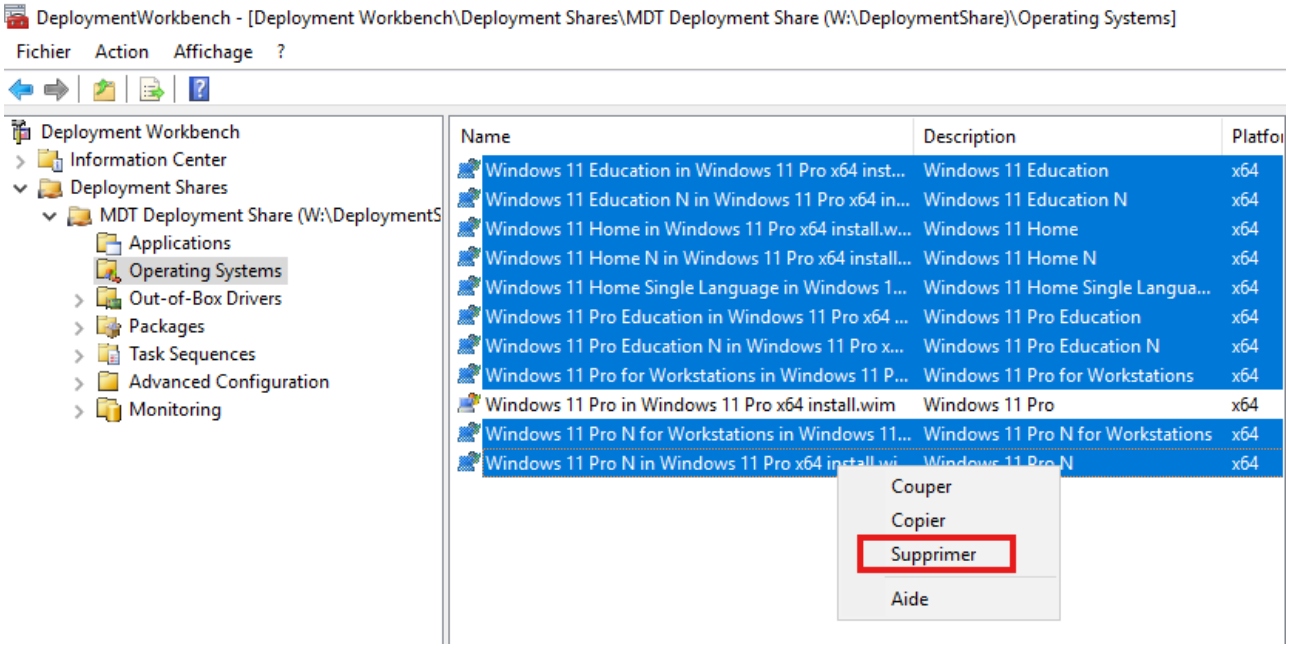




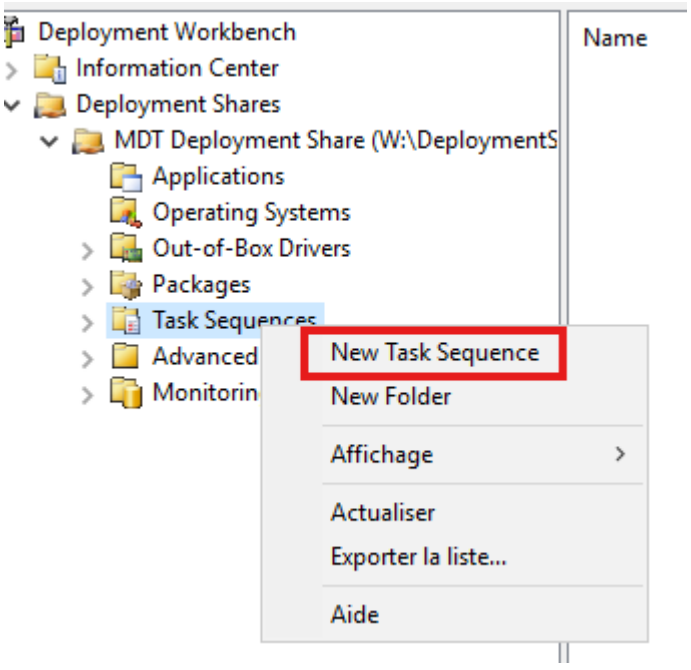
Le script

```
  Import-Module "C:\Program Files\Microsoft Deployment
Toolkit\bin\MicrosoftDeploymentToolkit.psd1"
  New-PSDrive -Name "DS001" -PSProvider MDTProvider -Root
"W:\DeploymentShare"
  import-mdtoperatingsystem -path "DS001:\Operating Systems" -SourcePath
"E:\" -DestinationFolder "Windows 11 Pro x64" -Verbose
```

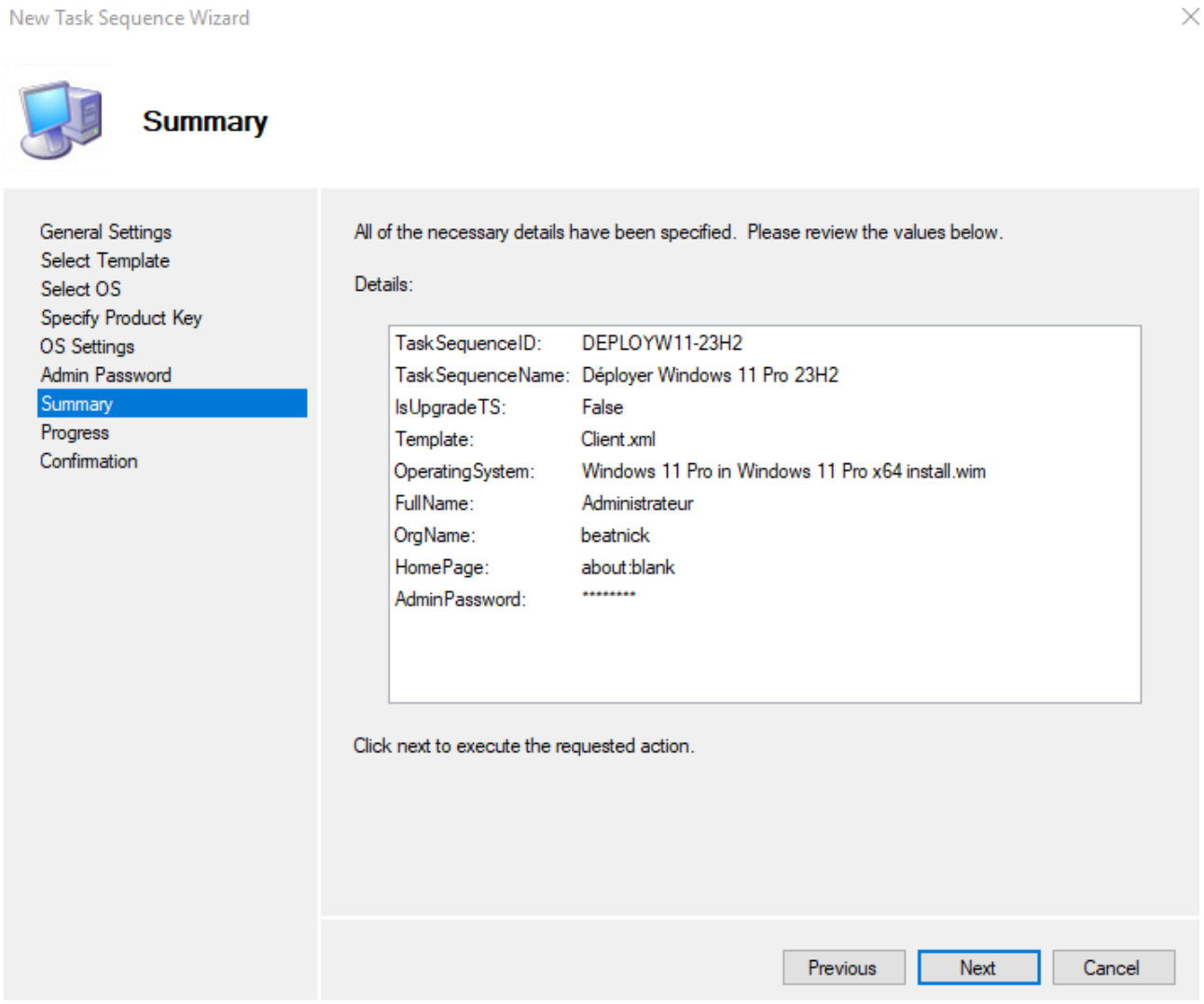
Dans 'Operating System', nous avons récupéré toutes les versions de l'OS présentent dans boot.wim. Nous allons supprimer les versions dont nous n'avons pas l'utilité

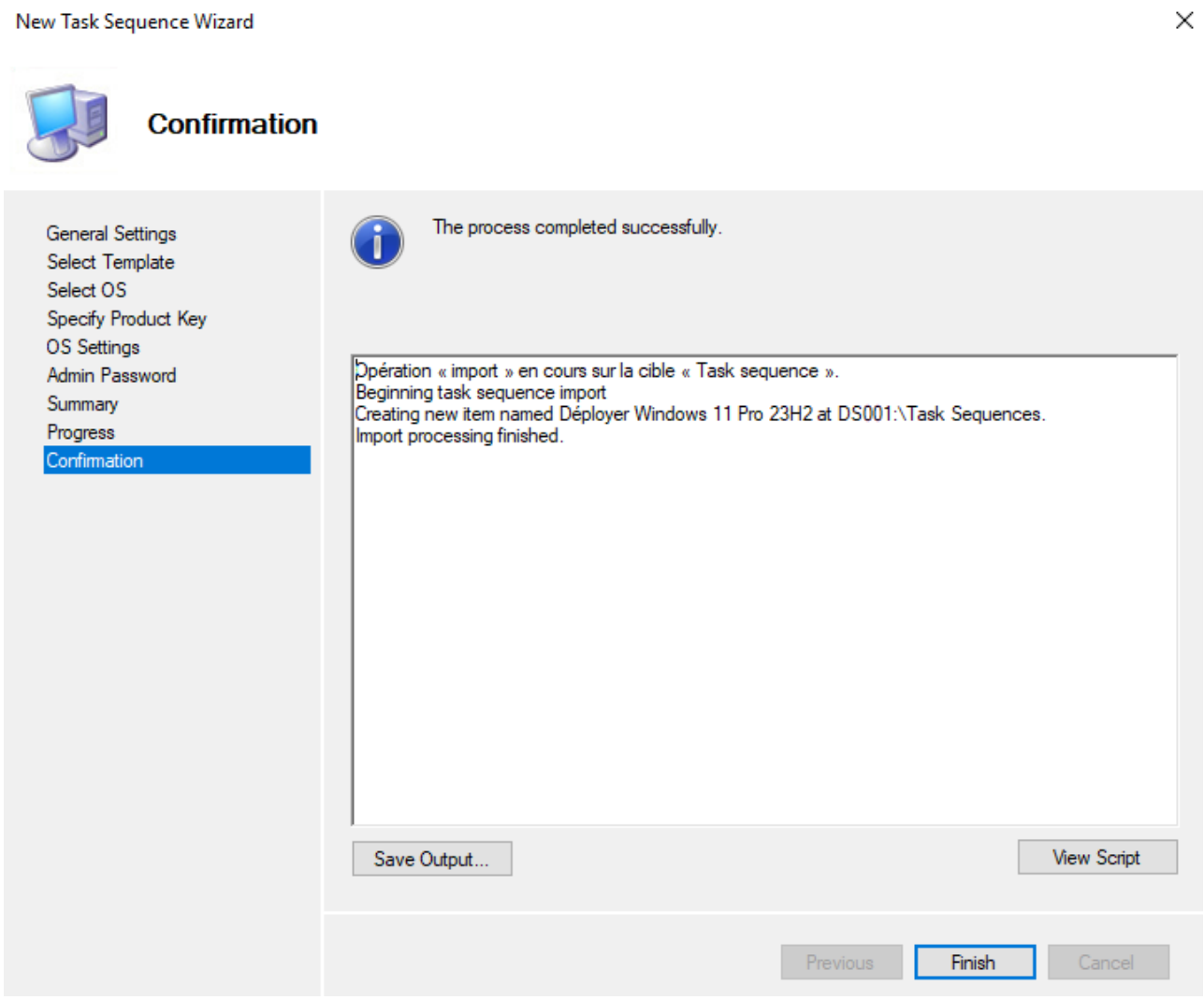


- Ajouter une séquence de tâches

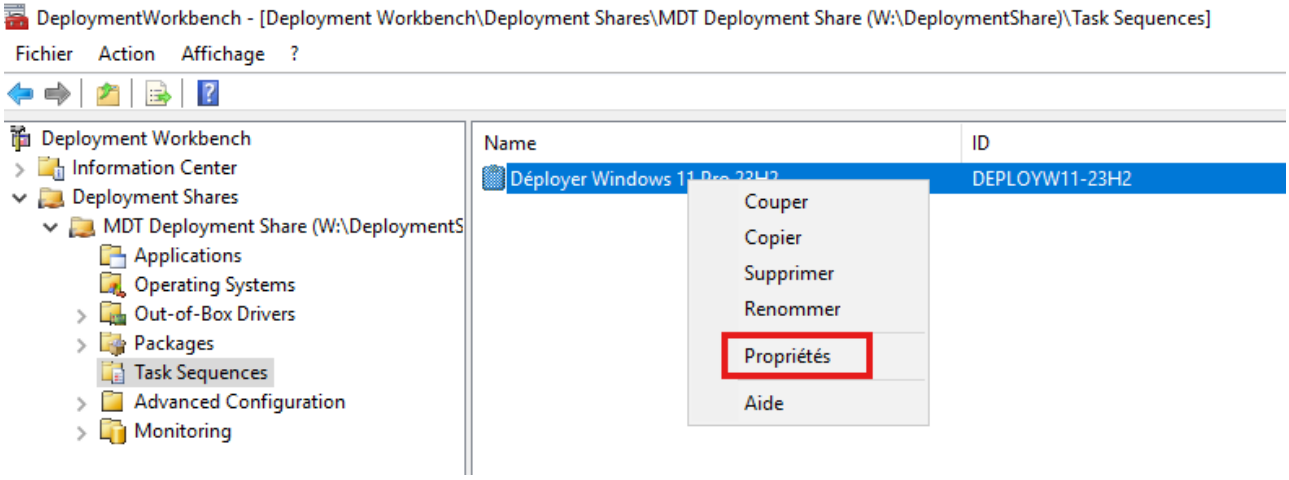


Suivez les étapes du wizard


New Task Sequence Wizard
Summary
General Settings
Select Template
Select OS
Specify Product Key
OS Settings
Admin Password
Summary
Progress
Confirmation
All of the necessary details have been specified. Please review the values below.
Details:
TaskSequenceID: DEPLOYW11-23H2
TaskSequenceName: Déployer Windows 11 Pro 23H2
IsUpgradeTS: False
Template: Client.xml
OperatingSystem: Windows 11 Pro in Windows 11 Pro x64 install.wim
FullName: Administrateur
OrgName: beatnick
HomePage: about:blank
AdminPassword: ********
Click next to execute the requested action.
Previous
Next
Cancel

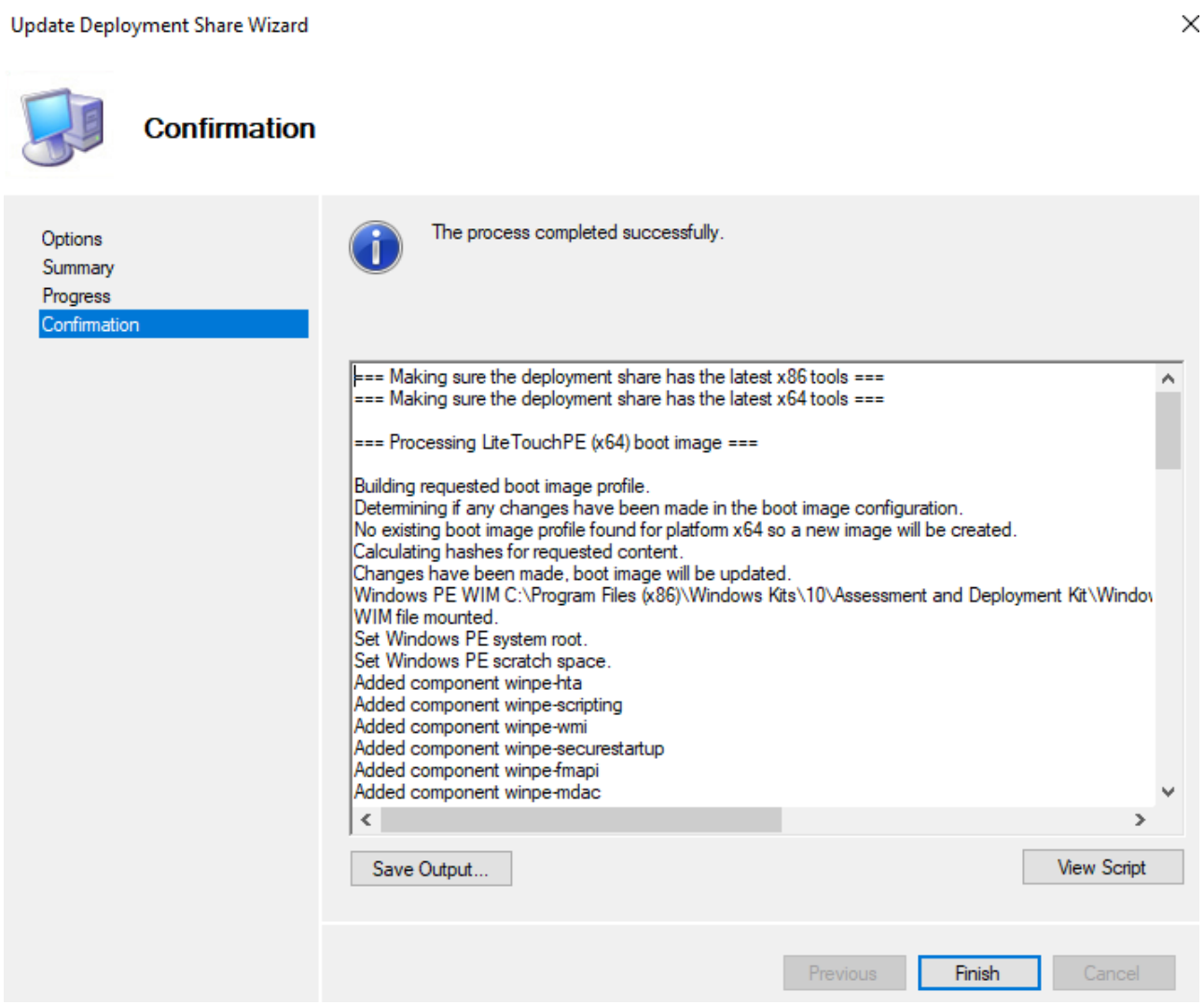


- Editer la séquence

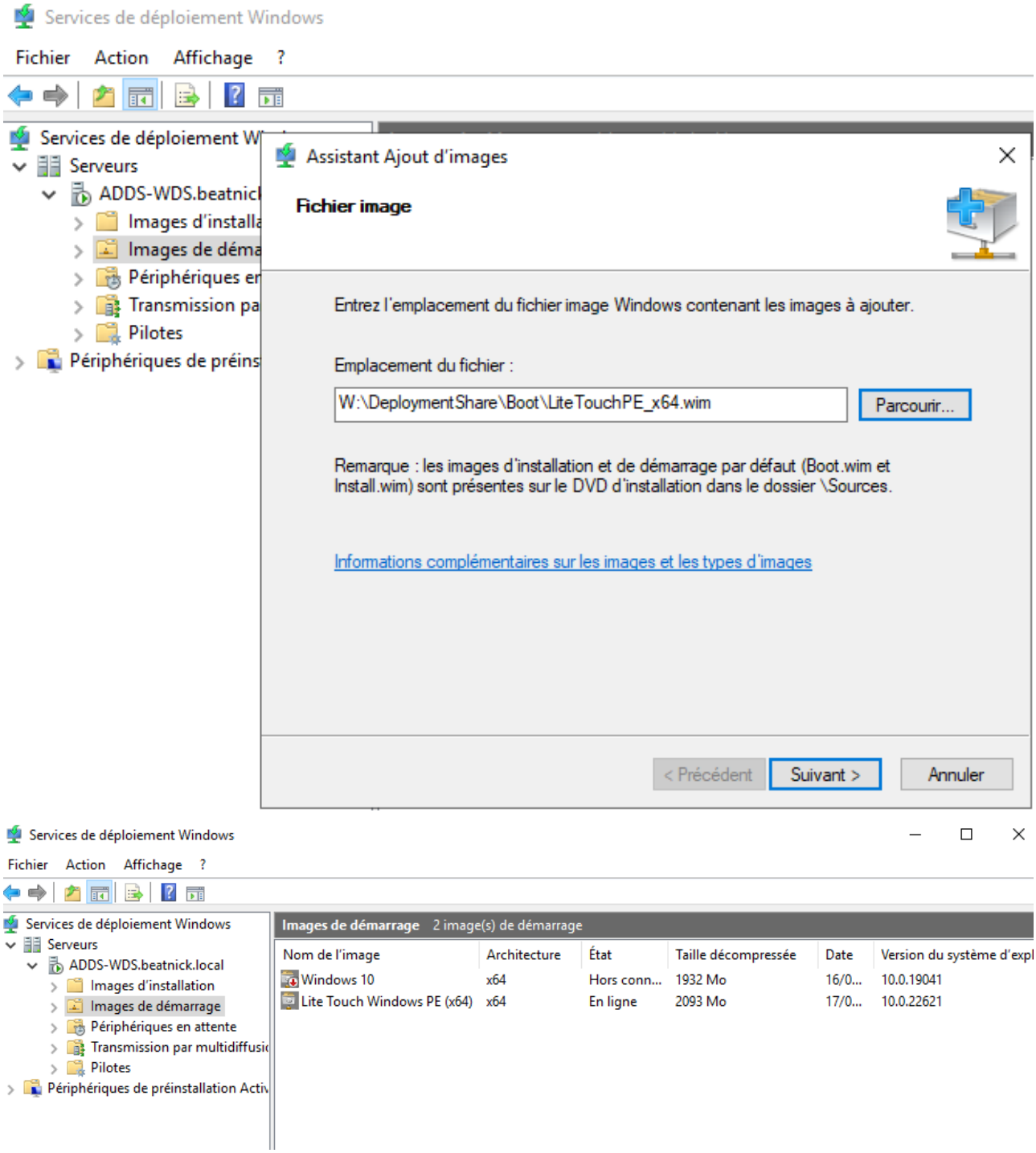


- Update Deployment Share

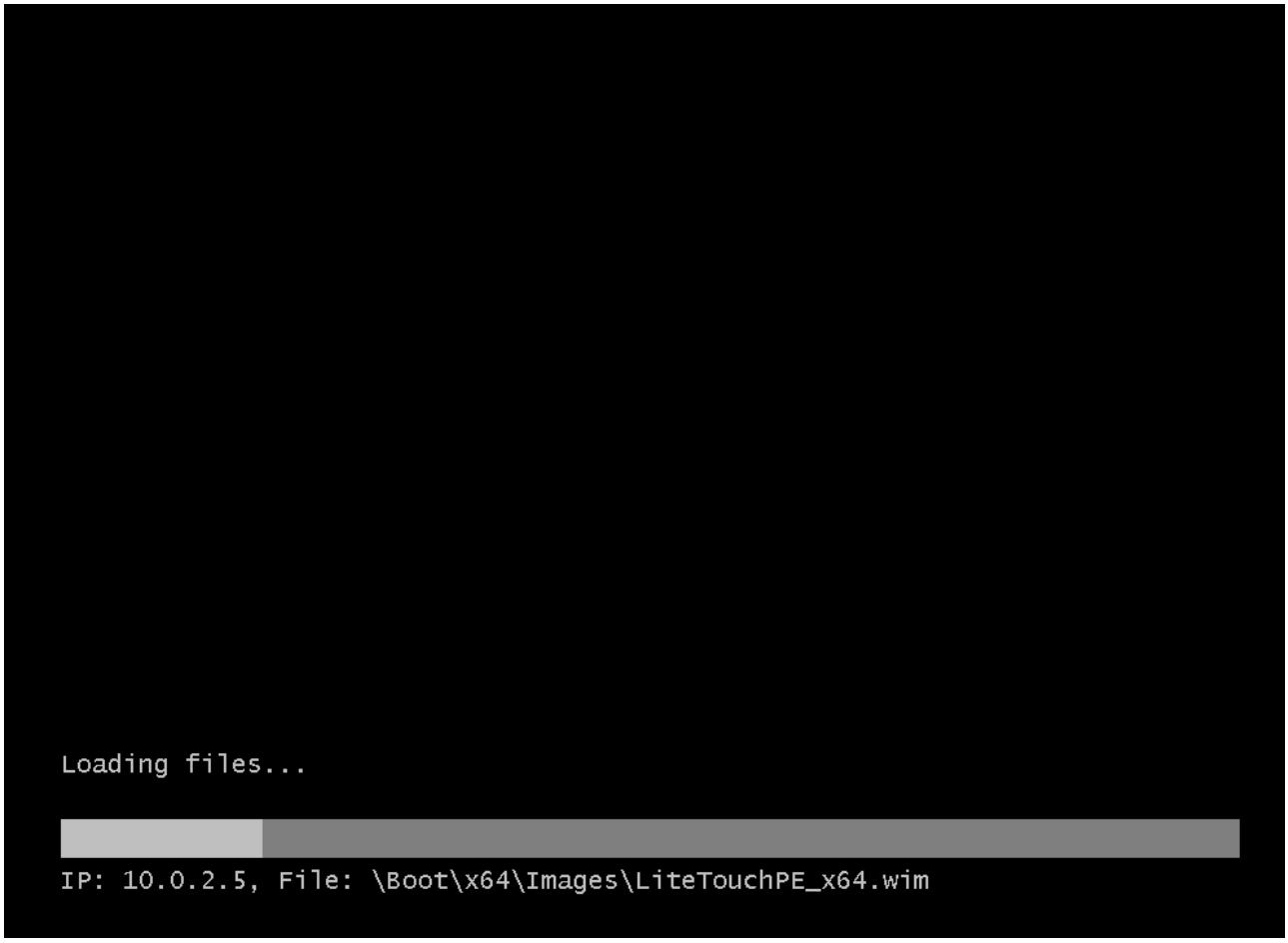
  `MDT Deplyment Share > clicl droit > Update`

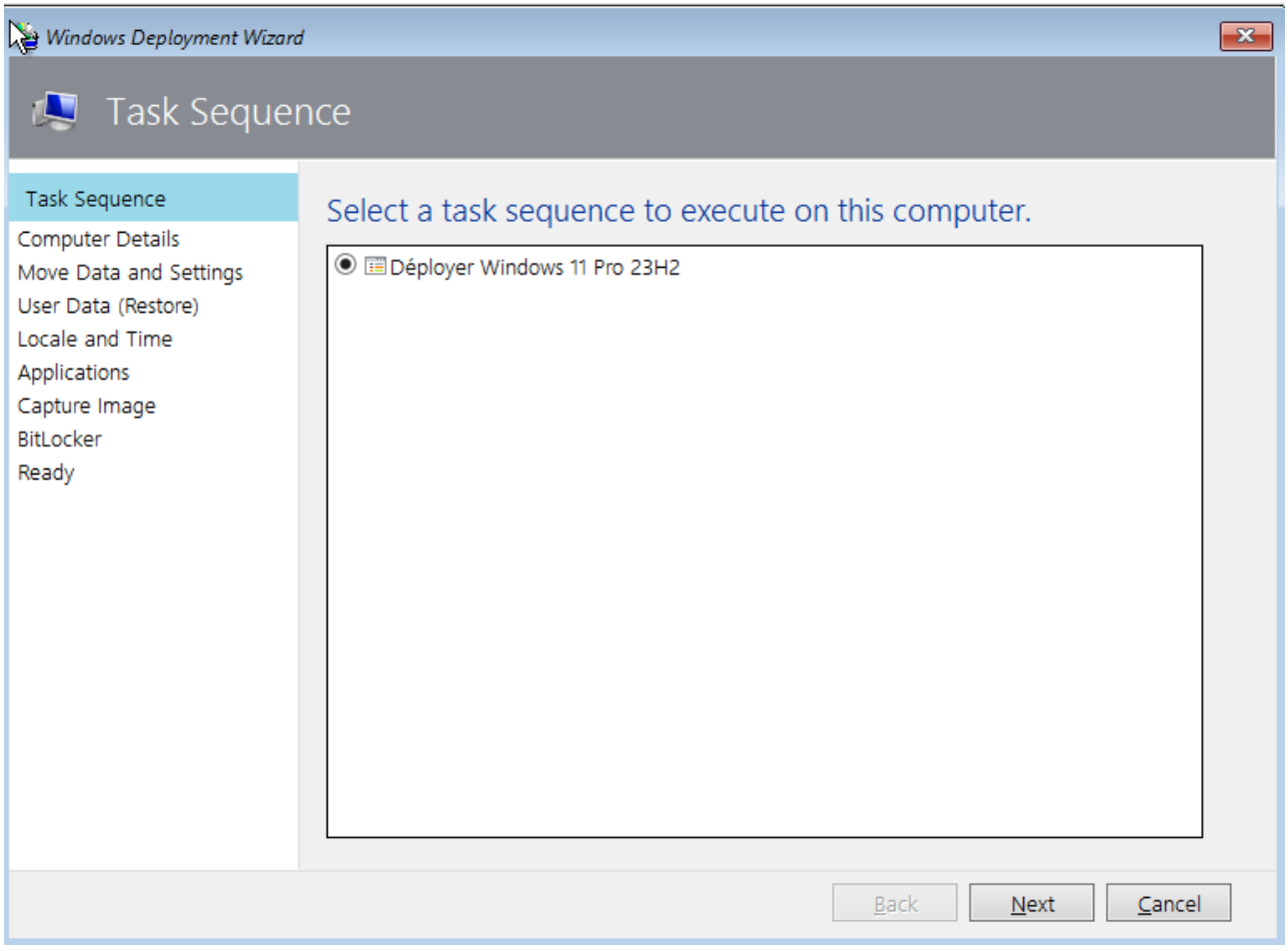

Update Deployment Share Wizard
Confirmation
Options
Summary
Progress
Confirmation
The process completed successfully.
=== Making sure the deployment share has the latest x86 tools ===
=== Making sure the deployment share has the latest x64 tools ===
=== Processing LiteTouchPE (x64) boot image ===
Building requested boot image profile.
Determining if any changes have been made in the boot image configuration.
No existing boot image profile found for platform x64 so a new image will be created.
Calculating hashes for requested content.
Changes have been made, boot image will be updated.
Windows PE WIM C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windo
WIM file mounted.
Set Windows PE system root.
Set Windows PE scratch space.
Added component winpe-hta
Added component winpe-scripting
Added component winpe-wmi
Added component winpe-securestartup
Added component winpe-fmapi
Added component winpe-mdac
Save Output...
View Script
Previous
Finish
Cancel

- Importer l'image Lite Touch Dans l'outil WDS

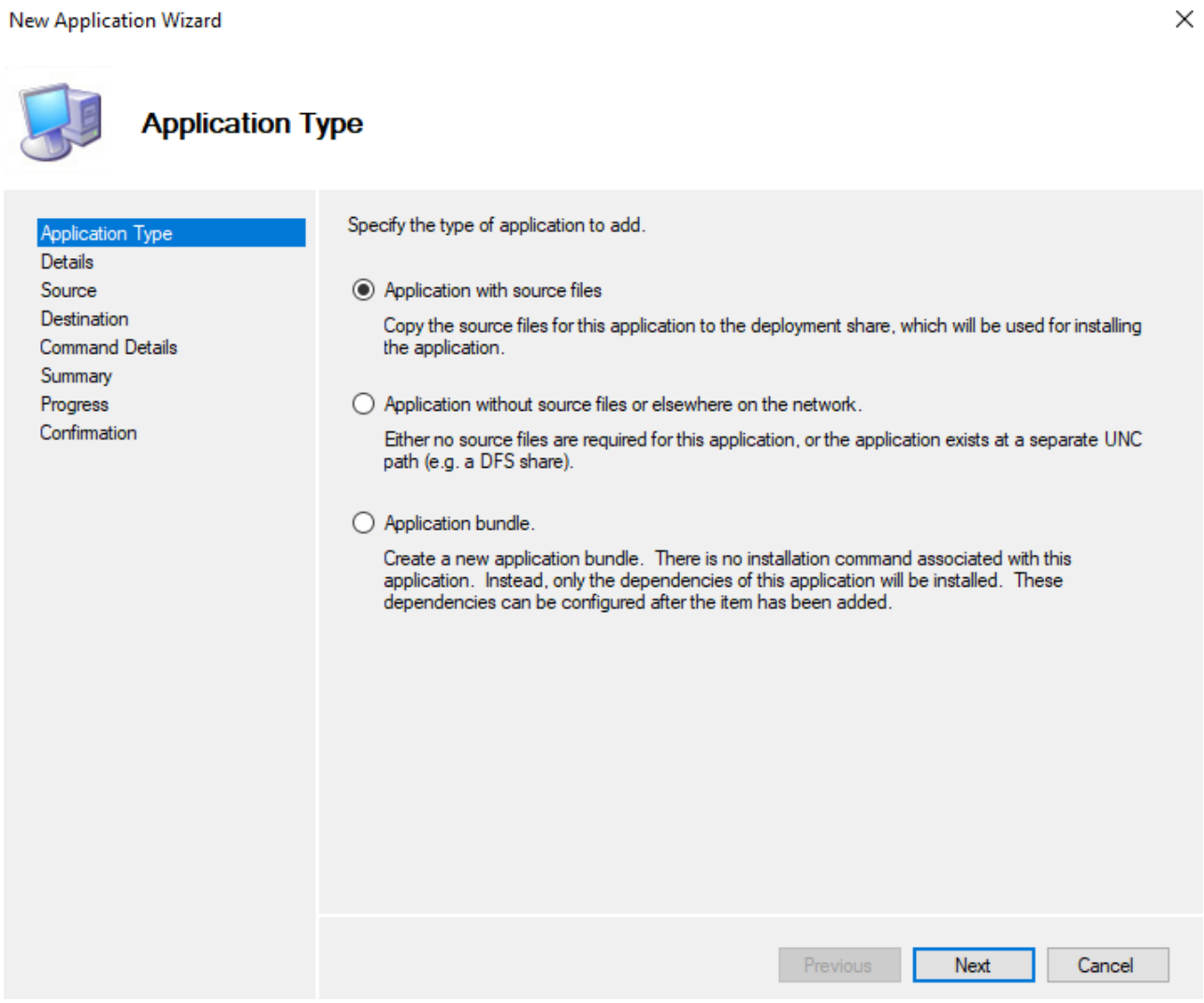


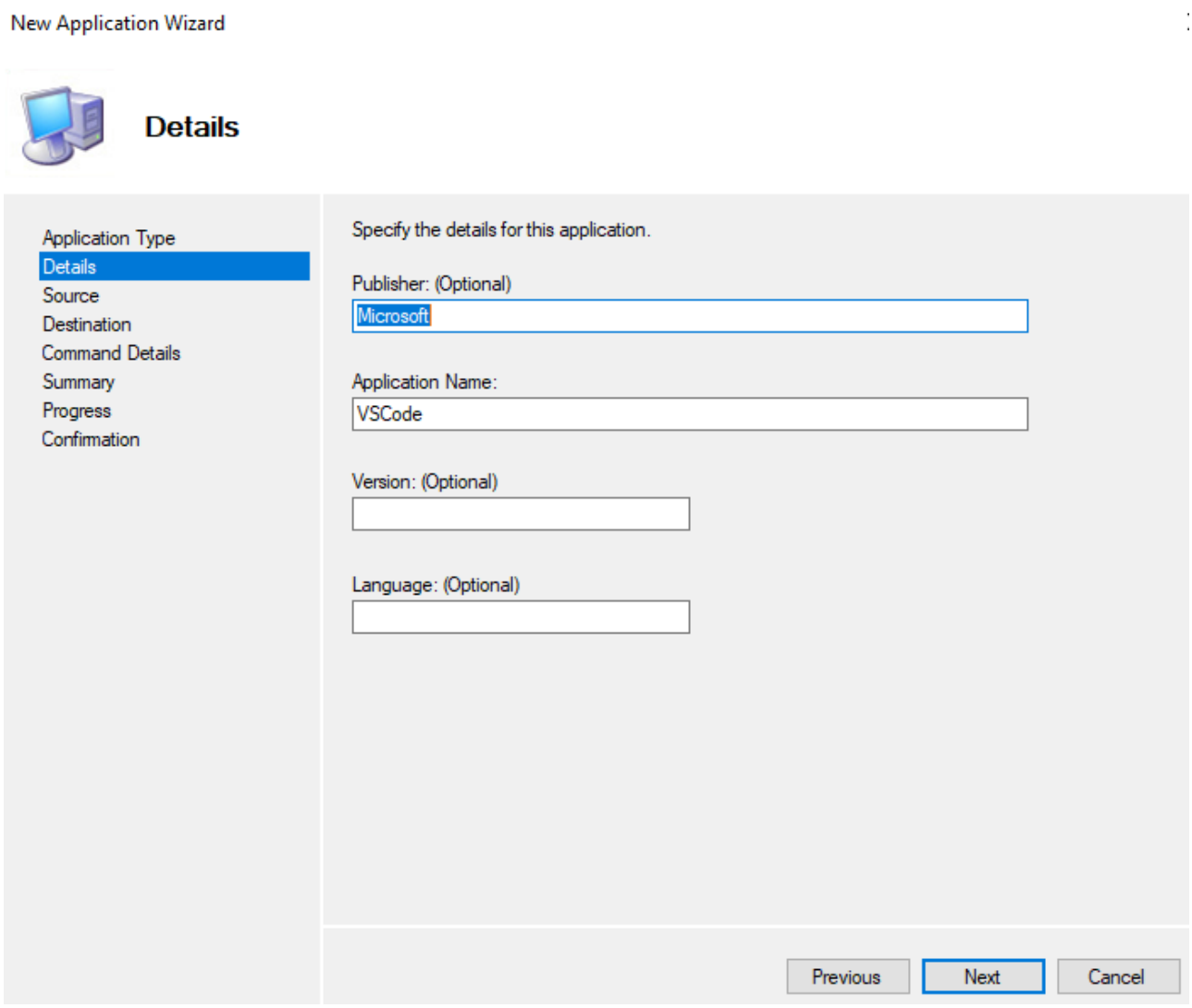
- Test de déploiement sur une machine vierge

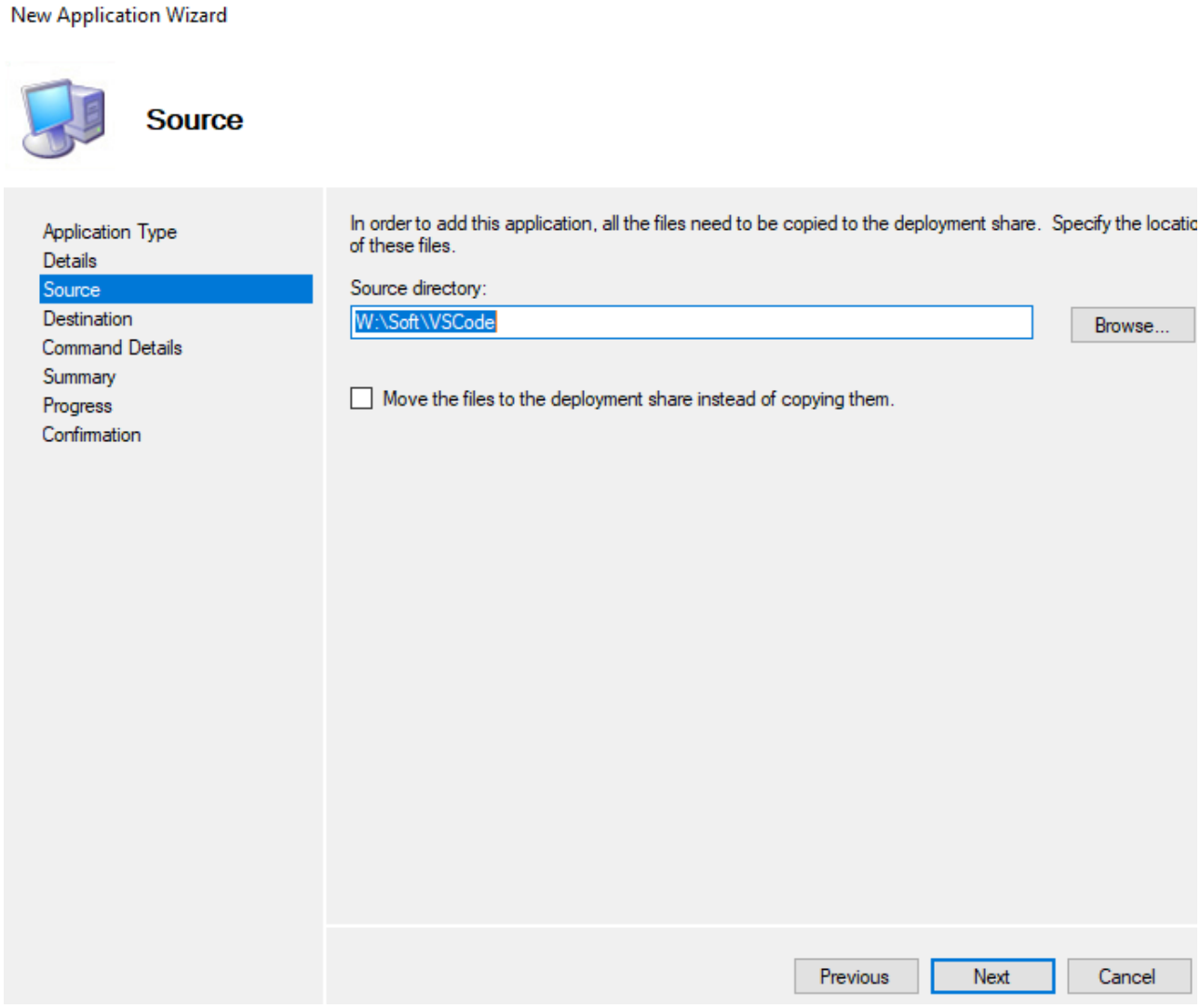


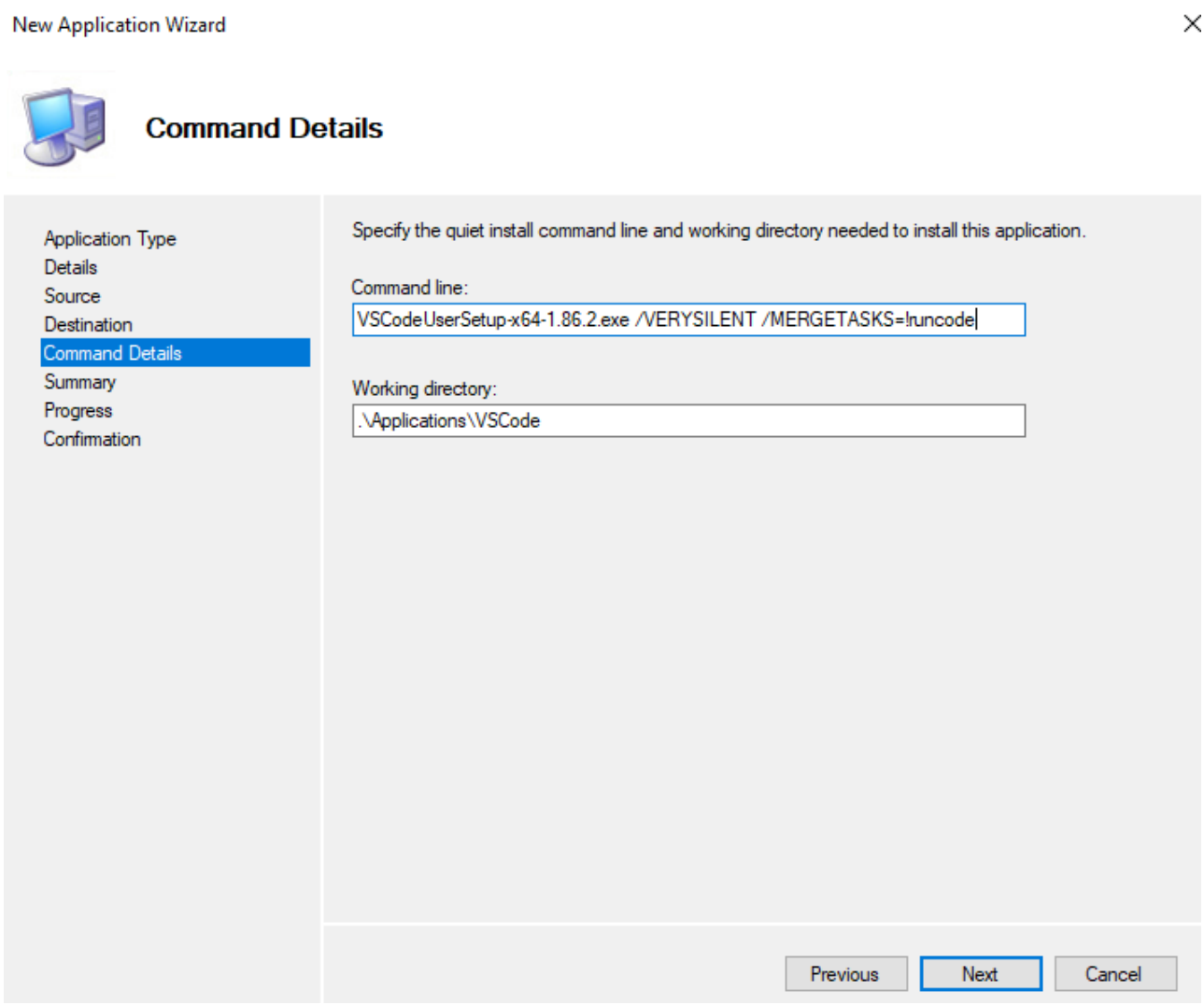


- Ajouter des programmes à l'installation (Exemple de VSCode)

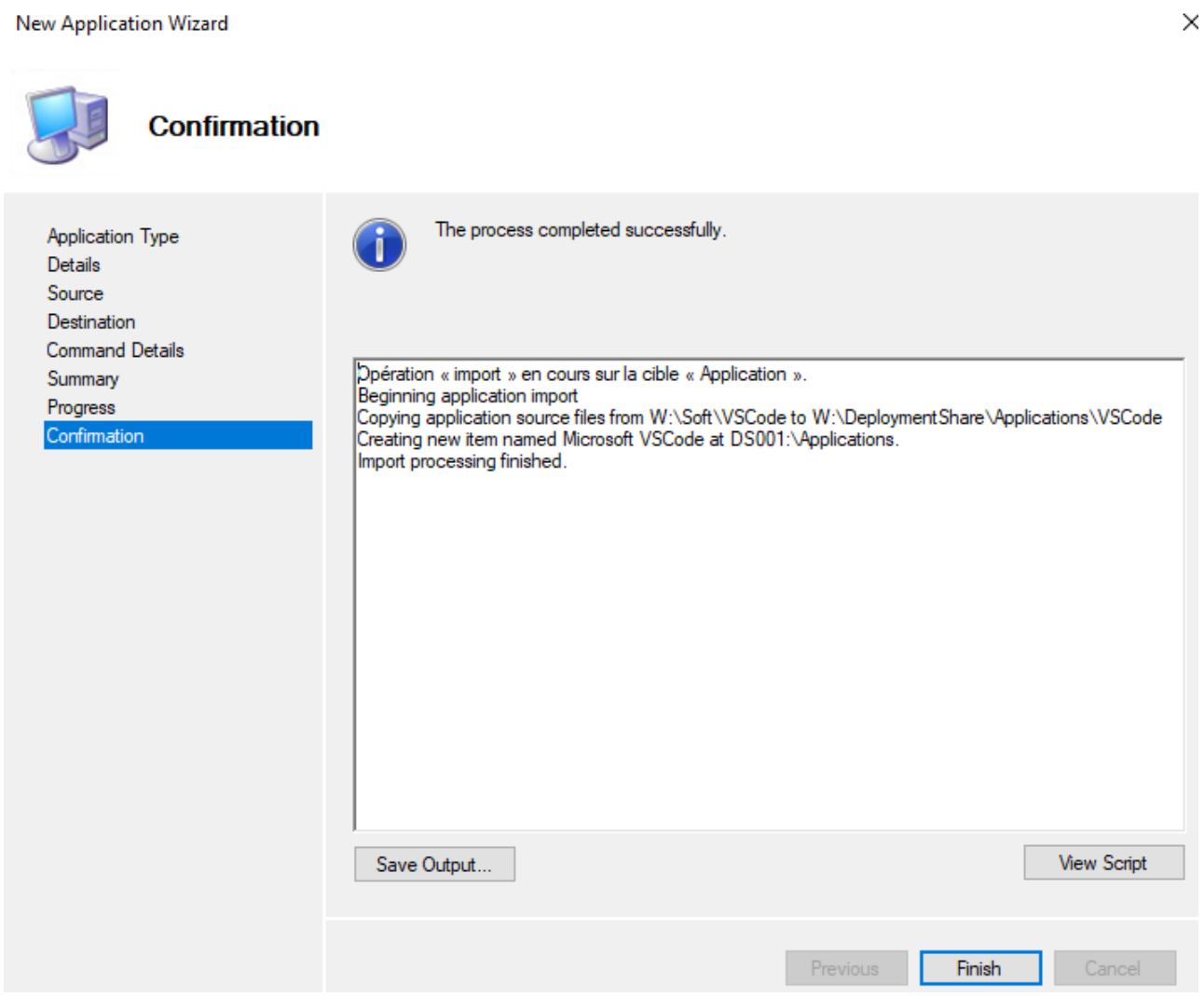



New Application Wizard
Details
Application Type
Details
Source
Destination
Command Details
Summary
Progress
Confirmation
Specify the details for this application.
Publisher: (Optional)
Microsoft
Application Name:
VSCode
Version: (Optional)
Language: (Optional)
Previous
Next
Cancel


New Application Wizard
Source
Application Type
Details
Source
Destination
Command Details
Summary
Progress
Confirmation
In order to add this application, all the files need to be copied to the deployment share. Specify the locatic
of these files.
Source directory:
W:\Soft\VSCode
Browse...
Move the files to the deployment share instead of copying them.
Previous
Next
Cancel



La commande d'installation dépend du logiciel, à trouver sur le site éditeur


New Application Wizard
Confirmation
Application Type
Details
Source
Destination
Command Details
Summary
Progress
Confirmation
The process completed successfully.
Opération « import » en cours sur la cible « Application ».
Beginning application import
Copying application source files from W:\Soft\VSCode to W:\DeploymentShare\Applications\VSCode
Creating new item named Microsoft VSCode at DS001:\Applications.
Import processing finished.
Save Output...
View Script
Previous
Finish
Cancel

- Partionner le disque

  Preinstall > New Computer only > Format and Partition Disk (UEFI)

  - **Supprimer** la partition « **Recovery**«