

Serveur Pxe

Sommaire

1/ Installer et configurer Windows Serveur

2/ Installer et configurer le service DNS et ADK

3/ Installer et configurer le serveur TFTP (WDS ?)

4/ Création des Images Windows PE, (Debian?) avec imagex.exe et envois sur le serveur avec WDS

5/ Boot Machine Virtuelle depuis le serveur PXE

6/ Automatisation de l'installation grâce a AD et a un script PowerShell

7/ Sécurisation d'Image et du serveur

8/ Crédit à la fin de l'ensemble

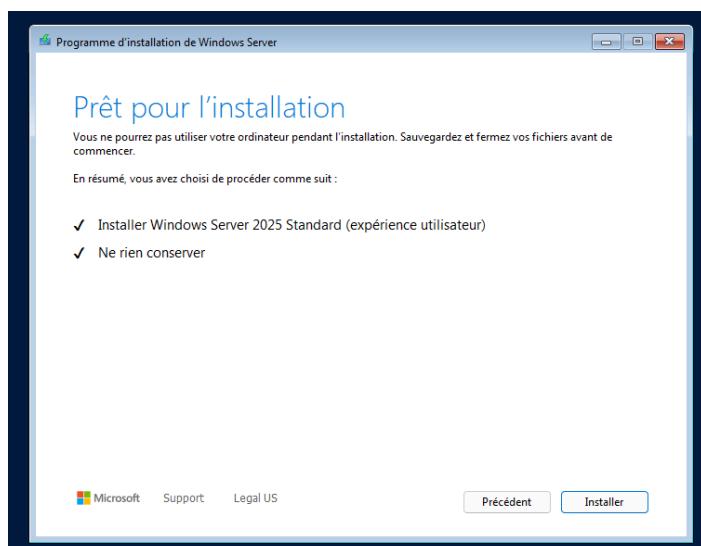
Job 1 : Installation et Configuration du Serveur de Base

1/ Installer et configurer Windows Serveur

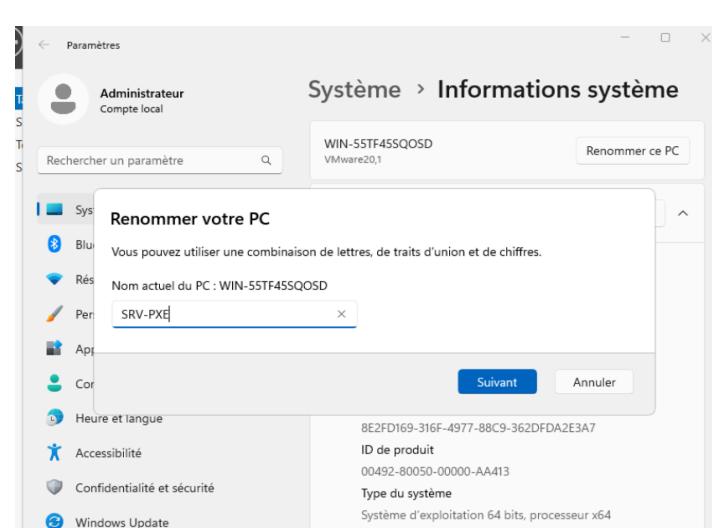
Étapes :

1. Installer Windows Server

- Créer une VM (Hyper-V, VMware, VirtualBox) avec :
 - 4+ Go RAM, 2+ CPU, 50+ Go de disque.
 - Sélectionner Windows Server (Desktop Experience) pour l'interface graphique.



- Configurer une IP statique (ex: 192.168.1.10/24) via :
 - powershell
 - Copy
 - Download
 - New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.20.133 -PrefixLength 24 -DefaultGateway 192.168.20.2
 - Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 192.168.20.133
- Renommer le serveur (SRV-PXE) et redémarrer.



2. Promouvoir en Contrôleur de Domaine (AD DS)

- Via Gestionnaire de serveur > Ajouter des rôles :
 - Sélectionner Active Directory Domain Services.
 - Promouvoir le serveur en DC et créer un nouveau domaine (ex: pxe.local).

The image contains three screenshots from Windows Server 2025:

- Screenshot 1: Assistant Ajout de rôles et de fonctionnalités**

This window shows the "Progression de l'installation" (Installation progress) for adding roles and features. The "Résultats" tab is selected, showing the successful addition of the "Outils AD DS et AD LDS" role. A note at the bottom indicates that the server can be closed while installations are running.
- Screenshot 2: Assistant Configuration des services de domaine Active Directory**

This window shows the "Examiner les options" (Review options) step. It displays configuration details for the new domain: "Nom NetBIOS du domaine : PXE", "Niveau fonctionnel de la forêt : Windows Server 2025", and "Niveau fonctionnel du domaine : Windows Server 2025". It also shows that "Catalogue global : Oui" and "Serveur DNS : Oui" are selected. Buttons for "Précédent", "Suivant >", "Installer", and "Annuler" are visible.
- Screenshot 3: Gestionnaire de serveur**

This screenshot shows the "Gestionnaire de serveur" interface with the "AD DS" role selected in the navigation pane. The main pane displays the "SERVEURS" list, which includes "SRV-PXE" with IP "192.168.20.133". The "ÉVÉNEMENTS" pane shows log entries for the newly promoted domain controller.

| Nom du serveur | ID | Gravité | Source | Journal |
|----------------|------|---------------|---|-------------------|
| SRV-PXE | 6016 | Avertissement | DFSR | Réplication DFS |
| SRV-PXE | 1844 | Avertissement | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service |
| SRV-PXE | 1844 | Avertissement | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service |

2/ Installer et configurer le service DNS et ADK

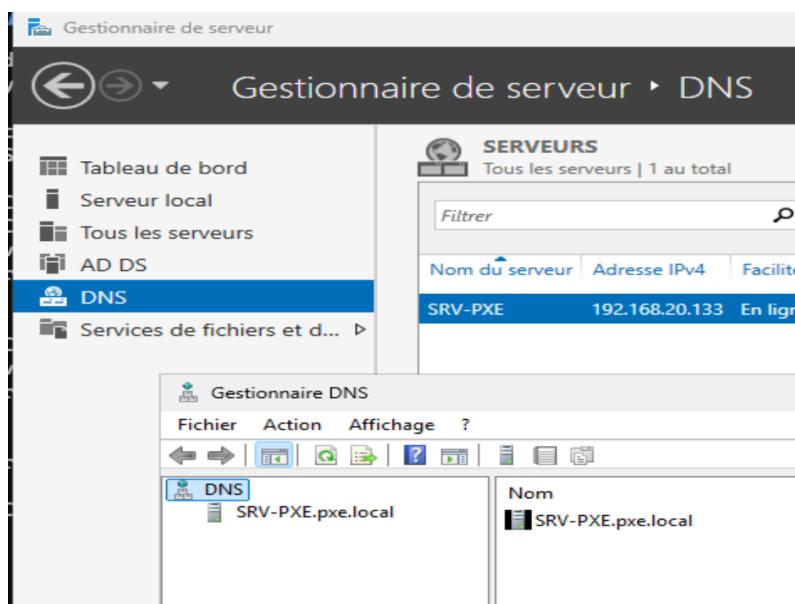
Services DNS

1. Dans Gestionnaire de serveur > Outils > DNS :

- Créer une zone directe (pxe.local).
- Activer les mises à jour dynamiques pour les clients PXE.

Installer le DNS (s'installe avec AD DS)

- Le DNS est automatiquement installé avec Active Directory



- Vérifie son fonctionnement :
 - Lance nslookup
 - Teste la résolution : nslookup olderpeople.local

```
PS C:\Users\Administrateur> nslookup pxe.local
Serveur :   localhost
Address:  ::1

Nom :      pxe.local
Address:  192.168.20.133
```

Kit de Déploiement ADK (Assessment & Deployment Kit)

Télécharger l'ADK

1. Téléchargement :

- Rendez-vous sur le site officiel Microsoft :
→ [Lien de téléchargement ADK](#)
- Choisissez la version compatible avec votre Windows Server (ex: ADK pour Windows 11 si vous utilisez WS 2022).

2. Options d'installation :

- Téléchargez :
 - adksetup.exe (programme d'installation principal).
 - ADK PE Add-on (optionnel, nécessaire pour WinPE).
 -

Installation de l'ADK

1. Lancer l'installation :

- Exécutez adksetup.exe en tant qu'administrateur.
- Cliquez sur Next et acceptez les termes du contrat.

2. Sélection des composants :

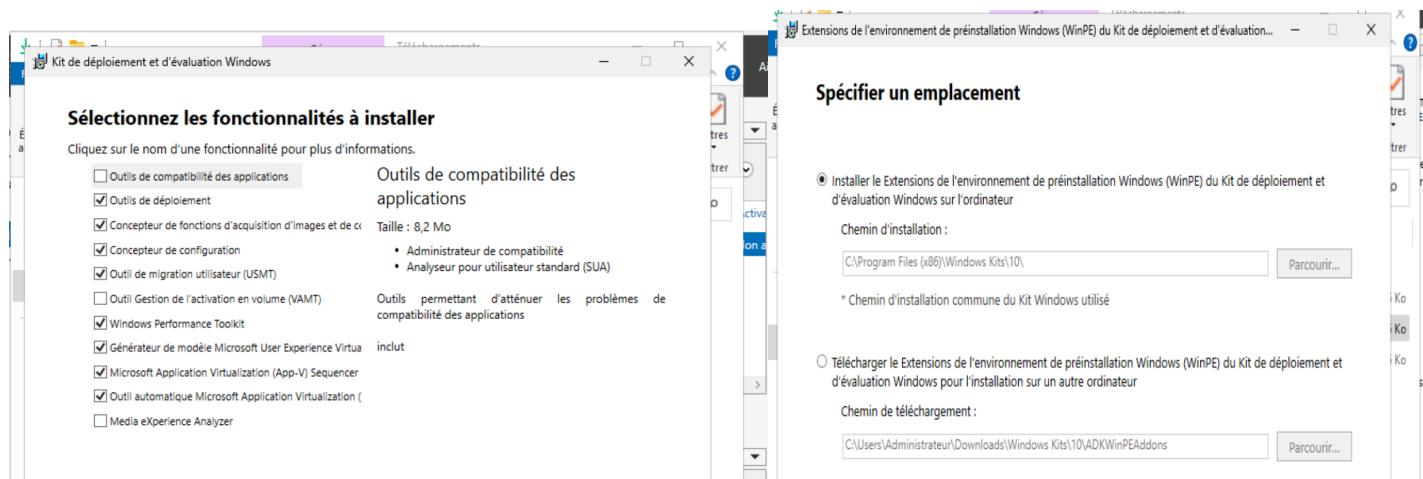
- Cochez au minimum :
 - Deployment Tools (pour imagex.exe, dism, oscdimg).
 - Windows Preinstallation Environment (Windows PE) (pour créer des images WinPE).
- (Optionnel) :
 - User State Migration Tool (USMT) (pour migrer des profils utilisateurs).

3. Emplacement d'installation :

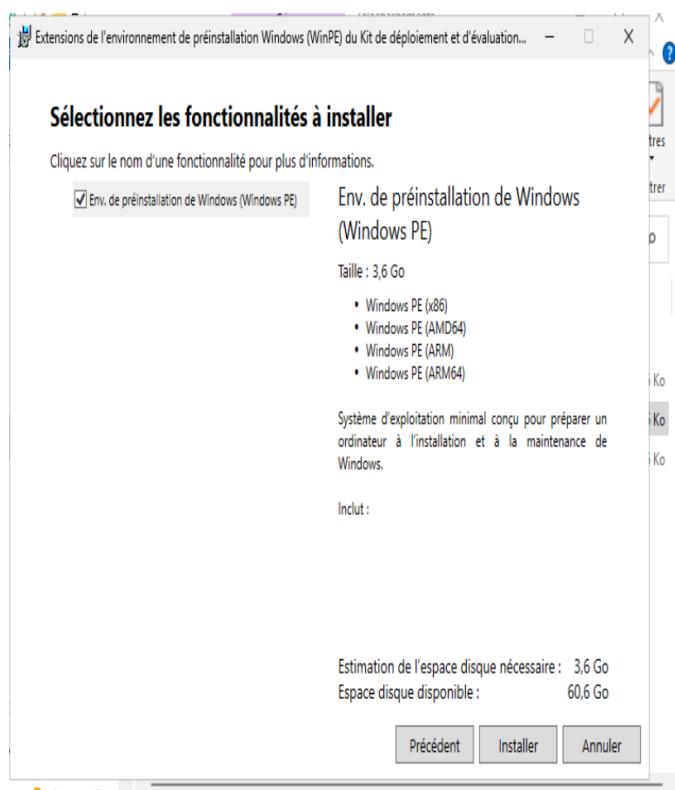
- Laissez par défaut (C:\Program Files (x86)\Windows Kits\10\ADK).

4. Finaliser l'installation :

- Cliquez sur Install et attendez la fin (5-10 min).



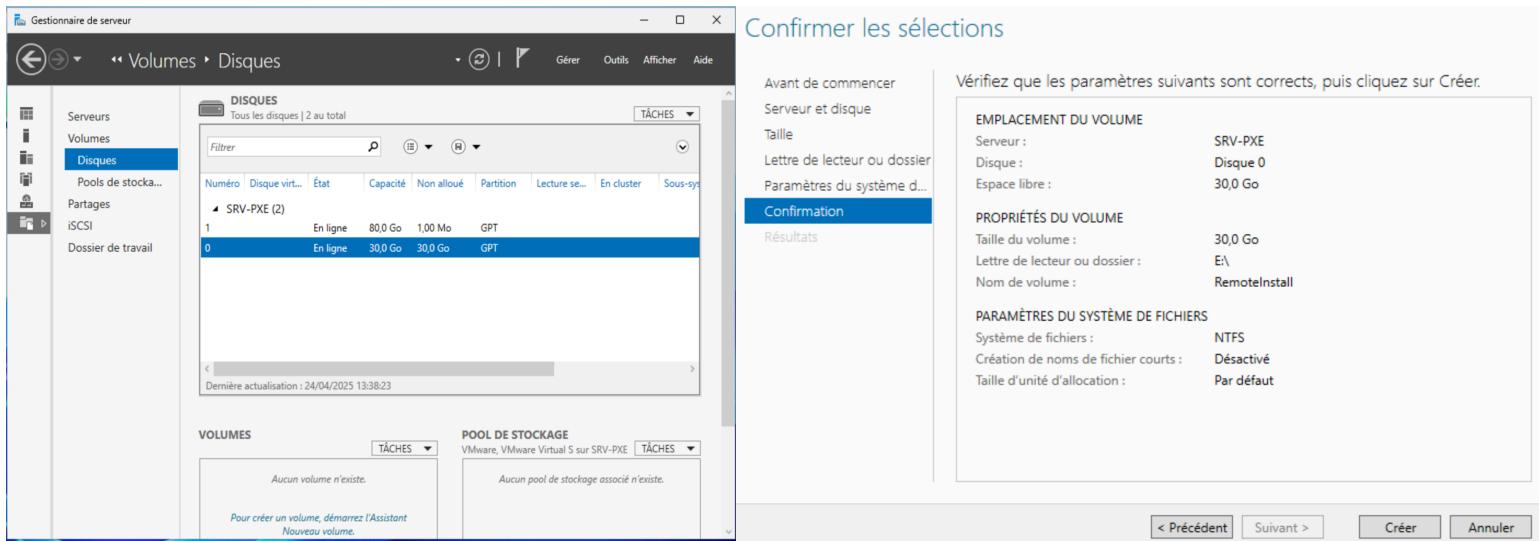
Installation du kit Windows PE



Il est possible d'installer le fichier avec PE directement normalement il installe les deux.

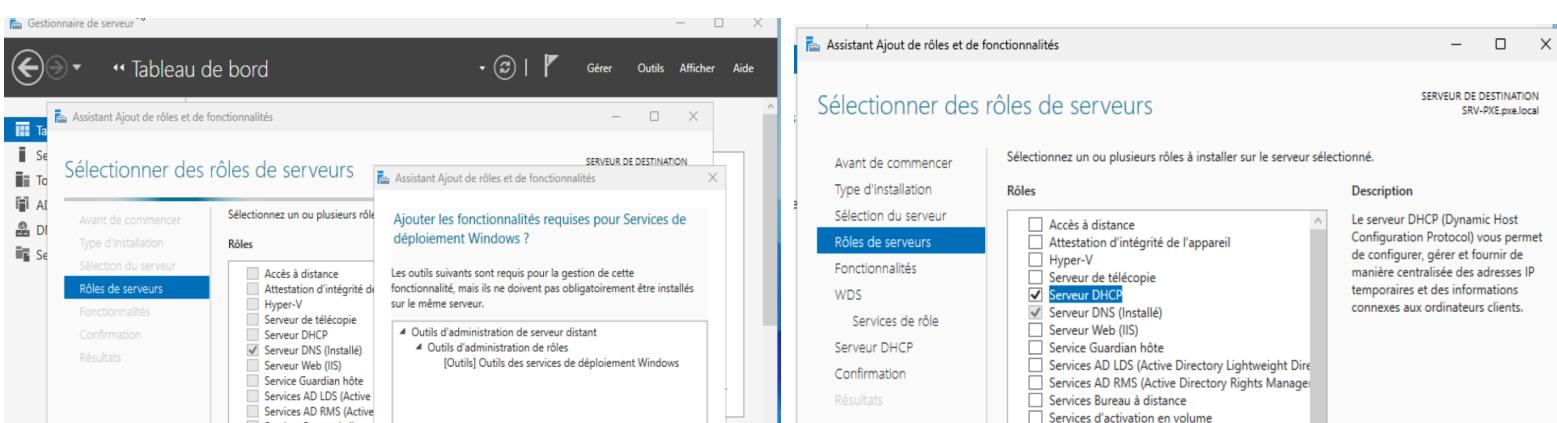
3/ Installer et configurer le serveur TFTP (WDS ?)

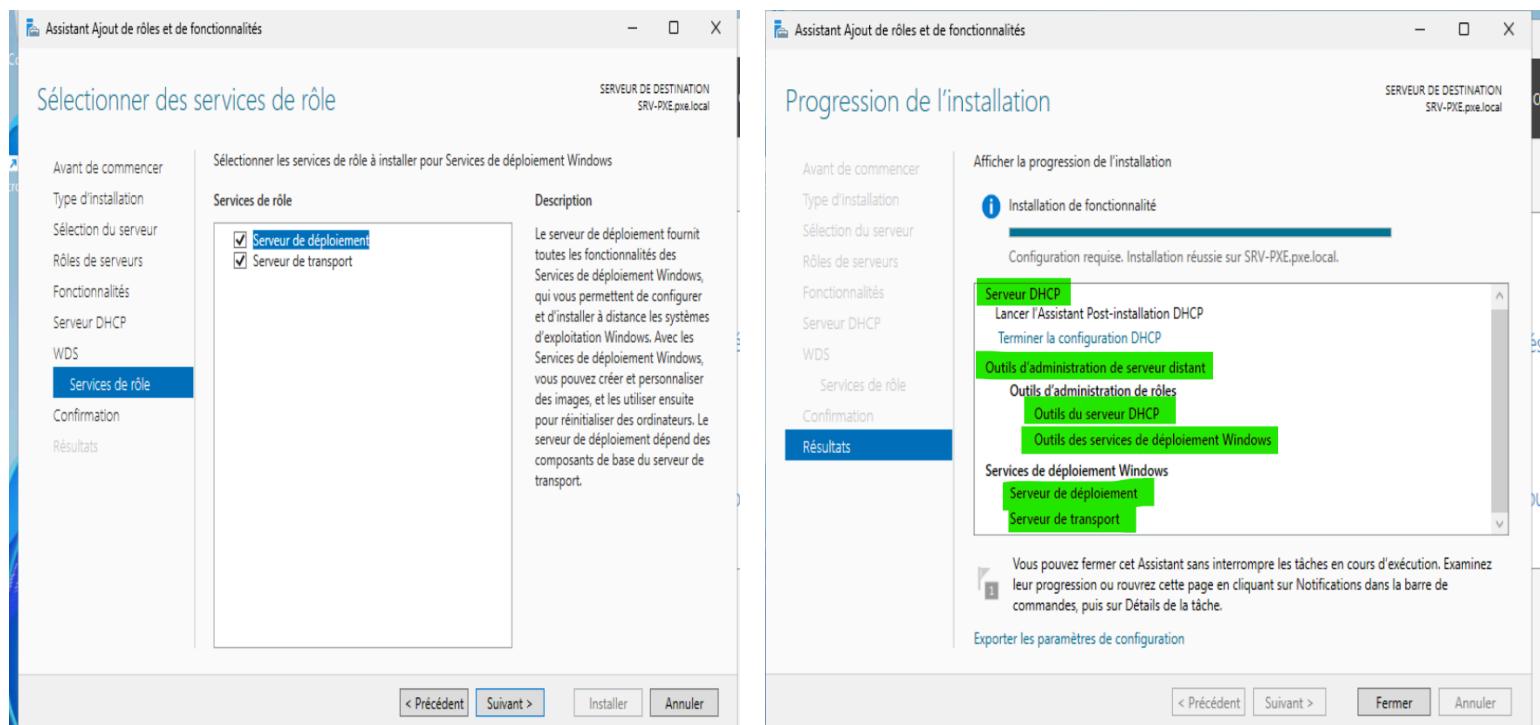
J'ajoute un Disque pour Installer les RemoteInstall dessus



Installer les services de déploiement Windows (WDS)

- Ouvre **Gestionnaire de serveur > Ajouter des rôles**
- Ajoute **Services de déploiement Windows**
- Pendant la configuration :
 - Choisis **Intégré à Active Directory**
 - Cocher **Serveur de transport (TFTP)** et **Serveur de déploiement**.
 - Choisis un **chemin de stockage d'image** (ex. : E:\RemoteInstall)
- Active le **démarrage automatique** de WDS

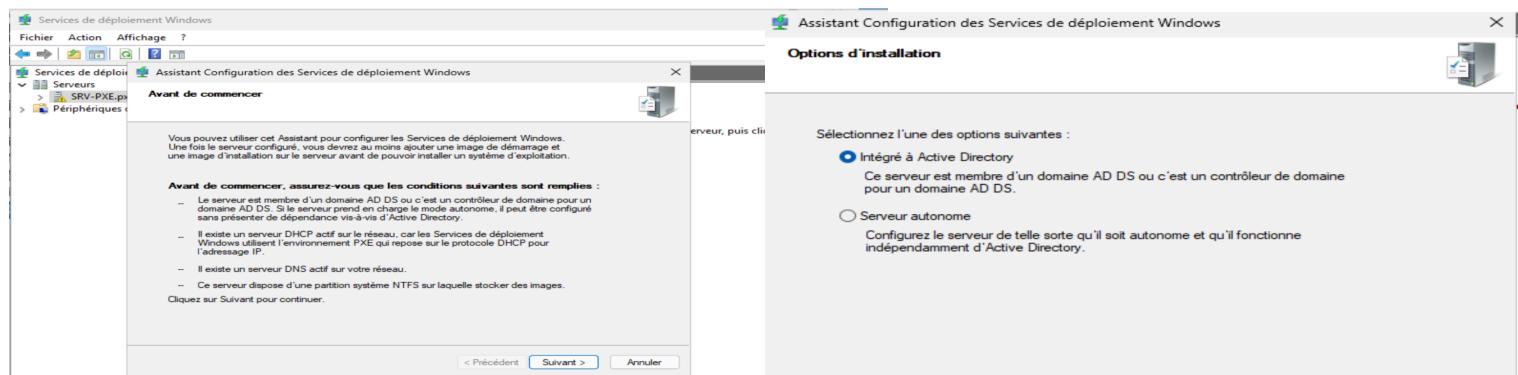




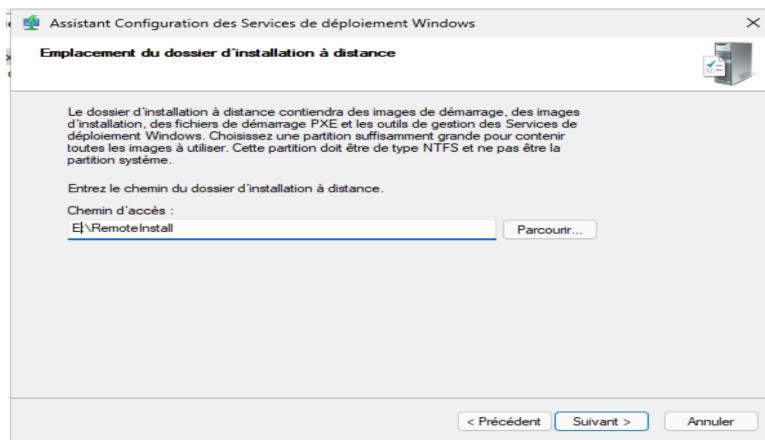
Configurer WDS et TFTP & PXE (via WDS)

- Ouvrir Windows Deployment Services (Administration).
 - Clic droit sur le **serveur** > Configurer
 - Choisir **Répondre aux clients PXE**
 - Choisir "**Integrated with DHCP**" si **DHCP est sur le même serveur**.
 - Spécifier le dossier **E:\RemoteInstall**.
 - Autoriser les clients anonymes (**test**) ou restreindre par MAC plus tard.

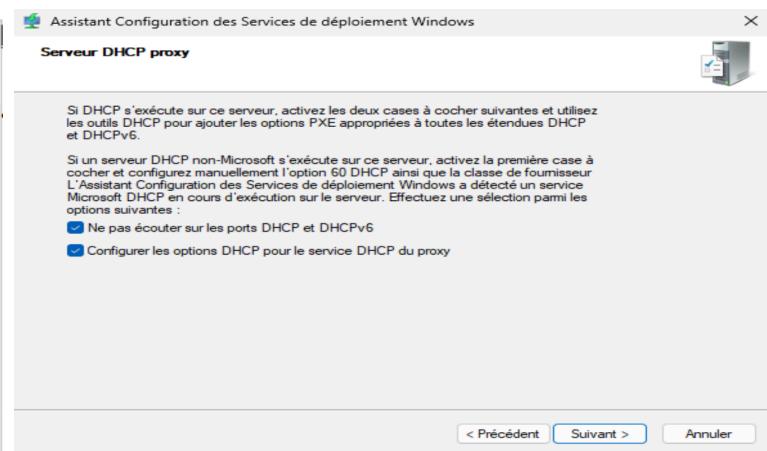
- Le service **TFTP** est activé automatiquement avec **WDS**



Je choisis mon dossier :

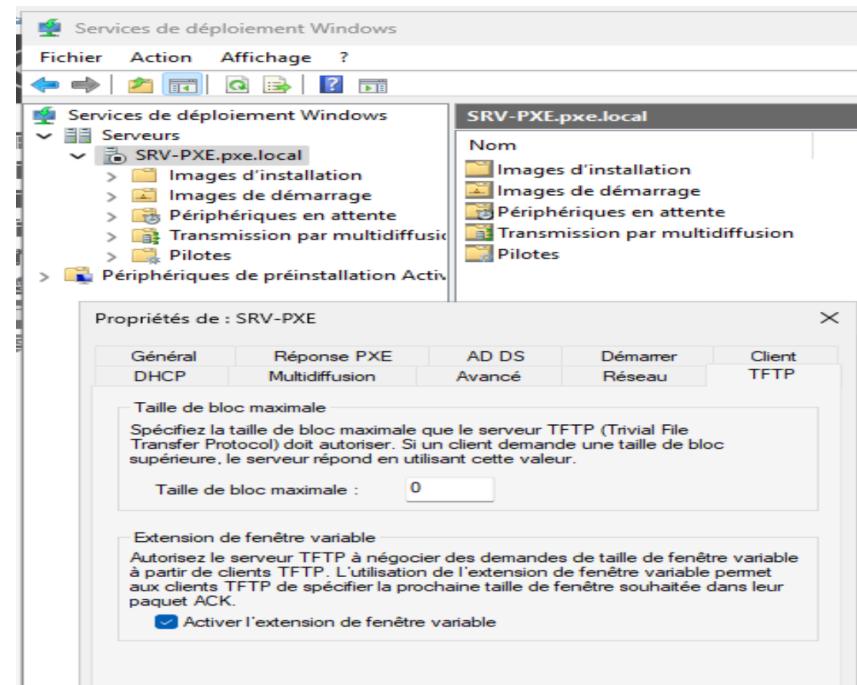
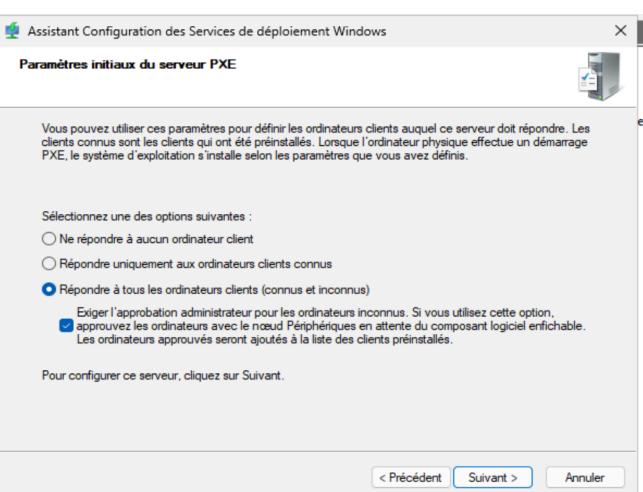


Je coche les 2 cases :



Paramètre du PXE, j'autorise toute connexion,

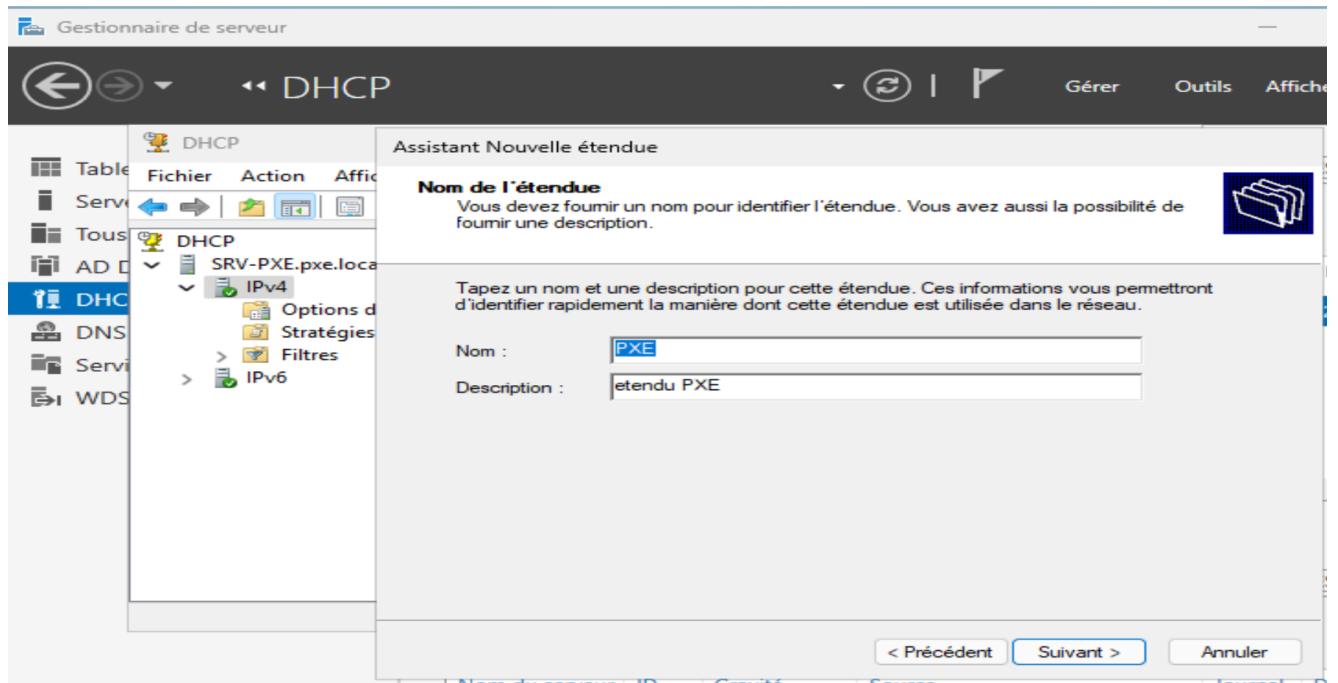
mais avec approbation de l'administrateur:



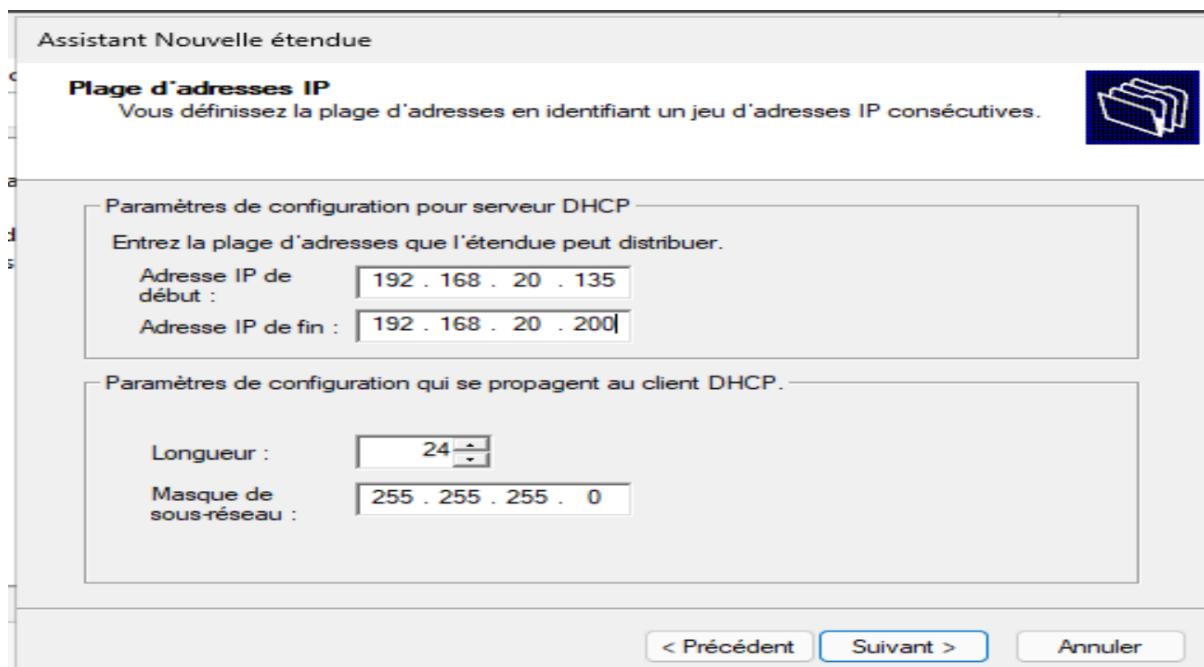
J'ai fini de déployé mon serveur, mon TFTP c'est installer en même temps que WDS. Je peux commencer a crée mes images.

Je configure mon DHCP:

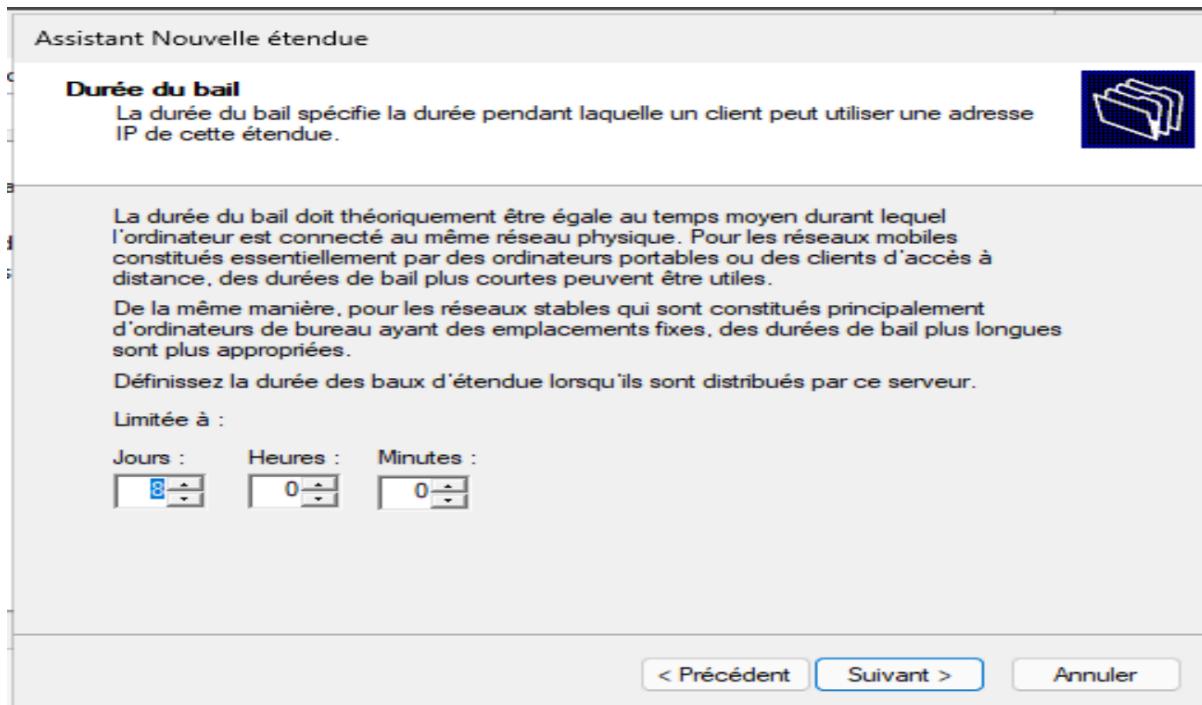
- Je crée une nouvelle étendue
serveur DHCP > configurer le serveur > clic droit ipv4 > crée une nouvelle étendue



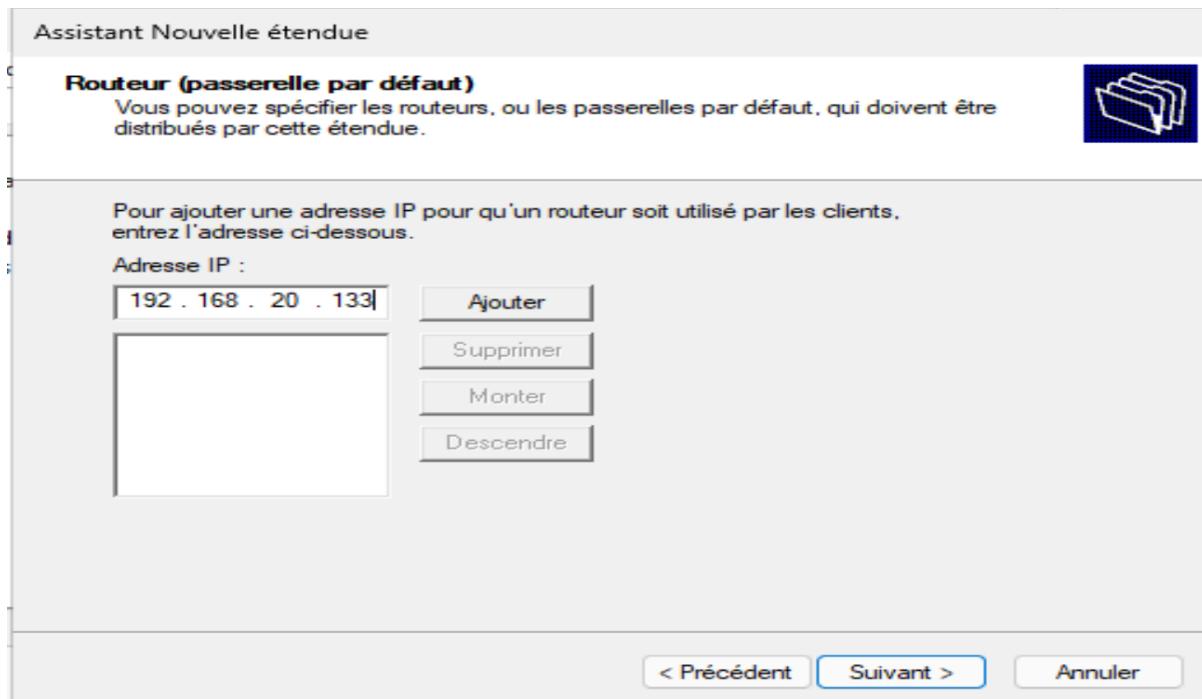
- Je règles les la plage



- Je règles les la durée du bail

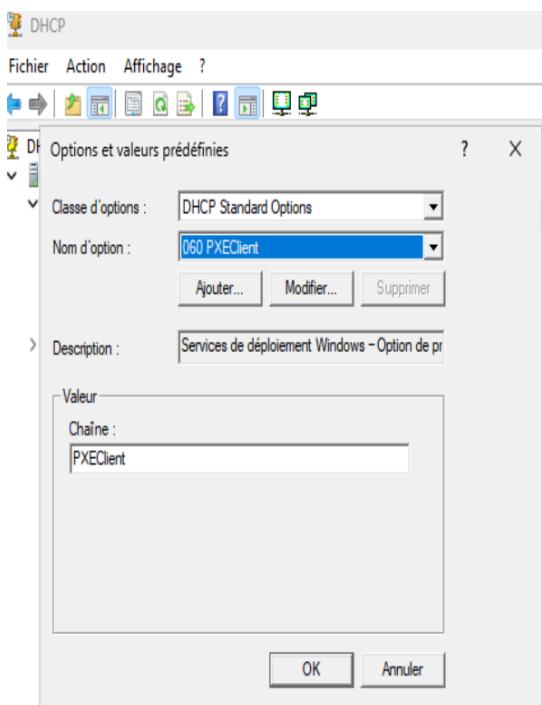


- je remet l'adresse de mon serveur



J'ajoute les options d'étendue :

dans le gestionnaire DHCP > IPV4 > option d'étendu > clic droit > configurer les options



Je rajoute les option 060

| Nom d'option | Fournisseur | Valeur |
|----------------------------------|-------------|----------------|
| 006 Serveurs DNS | Standard | 192.168.20.133 |
| 015 Nom de domaine DNS | Standard | pxe.local |
| 067 Nom du fichier de démarrage | Standard | boot.wim |
| 060 PXEClient | Standard | PXEClient |
| 066 Nom d'hôte du serveur de ... | Standard | 192.168.20.133 |

066 et 067 si le serveur DHCP est pas sur le même serveur

Mettre le nom de mon hotes pour l'option 066

Mettre le nom du fichier de démarrage pour option 067 "boot.win"

Je continue jusqu'à la fin et je redémarre le serveur.

Configurer le Pare-feu

J'ajoute des règles et j'ouvre les ports nécessaires du Pare-Feux pour TFTP et WDS

powershell

```
netsh advfirewall firewall add rule name="TFTP (PXE)" dir=in action=allow  
protocol=UDP localport=69
```

```
netsh advfirewall firewall add rule name="WDS (PXE)" dir=in action=allow  
protocol=UDP localport=4011
```

```
PS C:\Users\Administrateur> netsh advfirewall firewall add rule  
name="TFTP (PXE)" dir=in action=allow protocol=UDP localport  
=69  
Ok.  
  
PS C:\Users\Administrateur> netsh advfirewall firewall add rule  
name="WDS (PXE)" dir=in action=allow protocol=UDP localport=  
4011  
Ok.  
  
PS C:\Users\Administrateur>
```

Configurer le boot programme suivant l'architecture:

Configurer le profil de démarrage

powershell

```
WDSUTIL /Set-Server /BootProgram:"boot\x86\pxeboot.com" /Architecture:x86
WDSUTIL /Set-Server /BootProgram:"boot\x64\pxeboot.com" /Architecture:x64
```

```
La commande s'est terminée correctement.
PS C:\Users\Administrateur> WDSUTIL /Set-Server /BootProgram:"boot\x86\pxe.local" /Architecture:x86
Utilitaire de gestion des Services de déploiement Windows [Version 10.0.26100.1150]
© Microsoft Corporation. Tous droits réservés.

La commande s'est terminée correctement.
PS C:\Users\Administrateur> WDSUTIL /Set-Server /BootProgram:"boot\x64\pxe.local" /Architecture:x64
Utilitaire de gestion des Services de déploiement Windows [Version 10.0.26100.1150]
© Microsoft Corporation. Tous droits réservés.

La commande s'est terminée correctement.
```

```
# Autoriser tous les clients
```

powershell

```
WDSUTIL /Set-Server /PxePromptPolicy /New:NoPrompt /Known:Yes
/NewMachine:PreStaged
```

Le téléchargement TFTP du client suivant ne s'est pas effectué correctement :

```
# Vérifier l'intégrité du fichier spécifique
```

```
$bootFile = "E:\RemoteInstall\Boot\x64\bootmgr.exe"
```

```
Get-Item $bootFile | Select-Object FullName, Length, LastWriteTime
```

```
# Comparer avec la taille attendue (791984 octets)
```

```
if ((Get-Item $bootFile).Length -ne 791984) {
```

```
    Write-Warning "Fichier corrompu - Télécharger une version valide depuis les sources Windows"
```

```
    # Remplacer depuis l'ISO originale
```

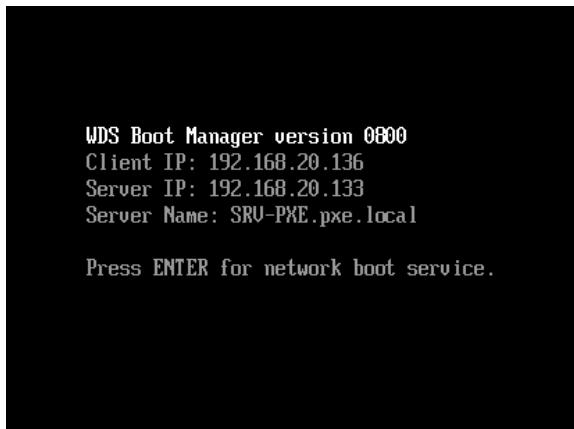
```
    Copy-Item "X:\sources\bootmgr.exe" $bootFile -Force
```

```
}
```

Tests pour s'assurer que l'installation est correcte :

1. Test PXE (Depuis un Client)

- Créer une VM sans disque
- Démarrer en réseau (PXE) → Doit afficher le menu WDS



2. Test DNS

Depuis un client joint au domaine :

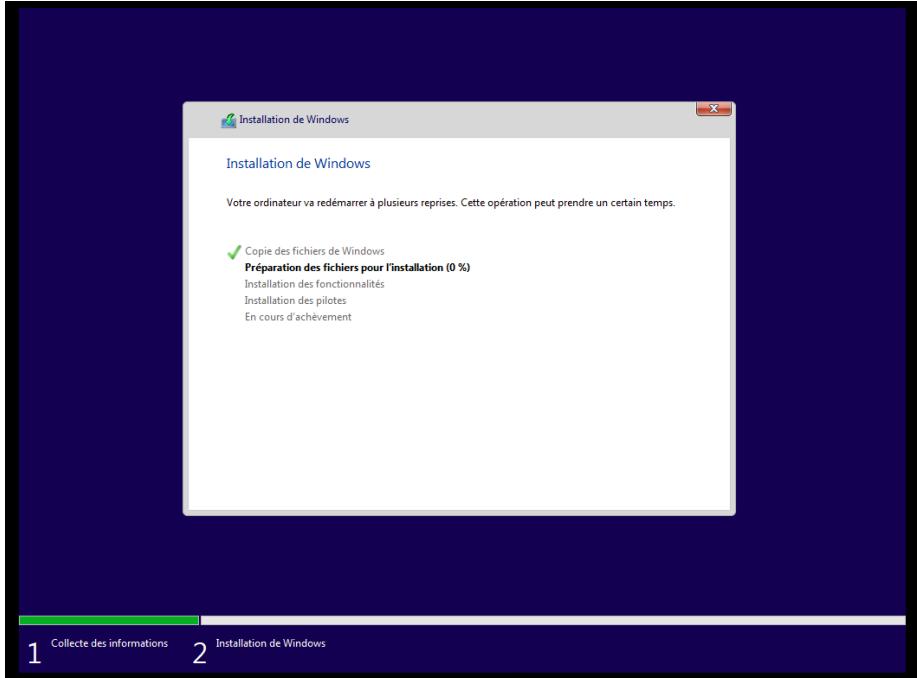
```
powershell
nslookup pxe.local

PS C:\Users\Administrateur> nslookup pxe.local
Serveur : localhost
Address: 127.0.0.1

Nom : pxe.local
Address: 192.168.20.133
```

3. Test TFTP

Depuis une autre machine, si le téléchargement des images s'effectue, mon TFTP est bien configuré :



4. Test WDS

powershell

WDSUTIL /Get-Server /Show:Config

```
INFORMATIONS DE CONFIGURATION POUR LE SERVEUR
[

Autorisation de serveur :
    État de l'autorisation : Autorisé

Stratégie de réponse :
    Répondre aux clients : Oui
    Répondre uniquement aux clients connus : Non
    Délai de réponse : 0 secondes

Stratégie d'utilisation Active Directory :
    Contrôleur de domaine préféré :
        Catalogue global préféré :
            Péphériques de préinstallation à l'aide de MAC : Non
            Stratégie de nommage des nouveaux ordinateurs : %61Username%#
            Ordre de recherche de domaine : Catalogue global uniquement
            Domaine de jointure des nouveaux ordinateurs : Oui

Unité d'organisation Nouvel ordinateur :
    Type d'unité d'organisation : Server Domain
    Unité d'organisation : CN=Computers,DC=pxe,DC=local

Configuration DHCP :
    État du service DHCP : En cours d'exécution
    Option DHCP 60 configurée : Oui
```

Vérifier "PXE Response = Respond to all clients"

Job 2 : Création et Déploiement des Images

<https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-create-usb-bootable-drive?view=windows-11>

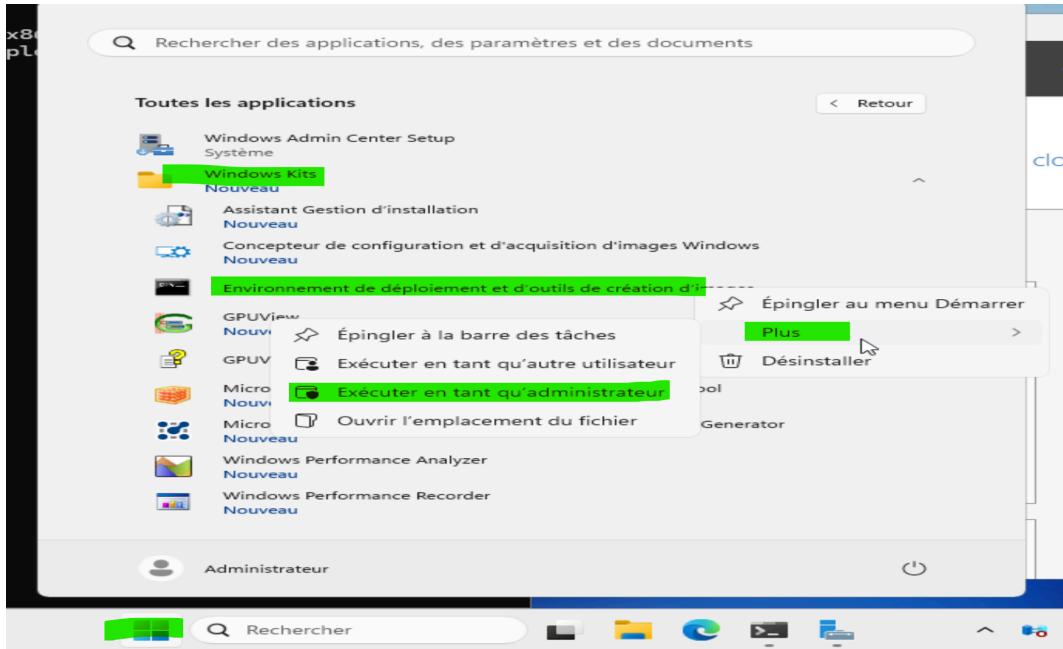
<https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-install-on-a-hard-drive--flat-boot-or-non-ram?view=windows-11>

<https://learn.microsoft.com/fr-fr/windows-hardware/manufacture/desktop/winpe-mount-and-customize?view=windows-11>

4/ Crédit des Images Windows PE, avec imagex.exe et envois sur le serveur avec WDS

Ouvrir l'invite de commande en tant qu'administrateur en passant par :

Logo Windows > tous les programmes > Windows kits > environnement de déploiement et outils de création d'image > plus > exécuté en tant qu'administrateur :



Crée une ISO de démarrage personnalisé WindowsPE

1. Générer une image personnalisé WinPE :

```
powershell
```

```
copype.cmd amd64 C:\winpe64
```

```
C:\>copype.cmd amd64 c:\winpe64  
=====  
Creating Windows PE customization working directory  
c:\winpe64  
=====  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\bootmgr  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\bootmgr.efi  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\bg-bg\bootmgr.efi.mui  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\Boot\BCD  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\Boot\BCDTemplate  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\Boot\boot.sdi  
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstalation Environment\amd64\Media\Boot\bootfix.bin
```

Activer Windows

2. Monter l'image

powershell

```
dism /mount-image /imagefile:c:\winpe64\media\sources\boot.wim  
/mountdir:c:\winpe64\mount /index:1
```

```
C:\>dism /mount-image /imagefile:c:\winpe64\media\sources\boot.wim /mountdir:c:\winpe64\mount /index:1
```

Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

Montage de l'image
[=====100.0%=====]
L'opération a réussi.

Activer Windows

```
dism /mount-image /imagefile:c:\winpe64\media\sources\install.wim /mountdir:c:\winpe64\mount  
/index:1
```

3. Nous allons ajouter les package

powershell

```
C:\>dism /image:c:\winpe64\mount /add-package /packagepath:"C:\Program Files (x86)\Windows  
Kits\10\Assessment and Deployment Kit\Windows Preinstallation  
Environment\amd64\WinPE_OCs\fr-fr\ip.cab"
```

```
C:\>dism /image:c:\winpe64\mount /add-package /packagepath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_0 Cs\fr-fr\lp.cab"
```

Outil Gestion et maintenance des images de déploiement

Version : 10.0.22621.1

Version de l'image : 10.0.22621.1

Processing 1 of 1 - Adding package Microsoft-Windows-WinPE-LanguagePack-Package~31bf3856ad364e35~amd64~fr-FR~10.0.22621.1

[=====100.0%=====]

L'opération a réussi.

Activer Windows

Accédez aux paramètres pour Windows

Je regarde les langues du fichier :

```
powershell  
dism /image:c:\winpe64\mount /get-intl
```

```
C:\>dism /image:c:\winpe64\mount /get-intl
```

Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

Version de l'image : 10.0.22621.1

Reporting offline international settings.

Default system UI language : en-US
System locale : en-US
Default time zone : Pacific Standard Time
User locale for default user : en-US
Location : États-Unis (GEOID = 244)
Active keyboard(s) : 0409:00000409
Keyboard layered driver : PC/AT Enhanced Keyboard (101/102-Key)

Installed language(s): en-US
Type : Fully localized language.
Installed language(s): fr-FR
Type : Partially localized language, MUI type.
Fallback Languages en-US

L'opération a réussi.

Activer

Je vois qu'elle sont encore en anglais donc je fait la commande :

```
powershell  
dism /image:c:\winpe64\mount /set-allIntl:fr-FR
```

```
C:\>dism /image:c:\winpe64\mount /set-allintl:fr-FR
```

```
Outil Gestion et maintenance des images de déploiement  
Version : 10.0.22621.1
```

```
Version de l'image : 10.0.22621.1
```

```
Input locale has been set to: fr-FR  
System locale has been set to: fr-FR  
User locale has been set to: fr-FR  
UI language has been set to: fr-FR  
L'opération a réussi.
```

```
C:\>
```

je refait la commande pour voir les langues de l'image :

```
powershell  
dism /image:c:\winpe64\mount /get-intl  
Je peux voir que les langues ont bien été changé
```

```
C:\>dism /image:c:\winpe64\mount /get-intl  
Outil Gestion et maintenance des images de déploiement  
Version : 10.0.22621.1  
Version de l'image : 10.0.22621.1  
Reporting offline international settings.  
Default system UI language : fr-FR  
The UI language fallback is : en-US  
System locale : fr-FR  
Default time zone : Pacific Standard Time  
User locale for default user : fr-FR  
Location : France (GEOID = 84)  
Active keyboard(s) : 040c:0000040c  
Keyboard layered driver : PC/AT Enhanced Keyboard (101/102-Key)  
Installed language(s): en-US  
Type : Fully localized language.  
Installed language(s): fr-FR  
Type : Partially localized language, MUI type.  
Fallback Languages en-US  
L'opération a réussi.
```

je vérifie les packages qui sont installés :

```
powershell
```

```
dism /image:c:\winpe64\mount /get-packages
```

```
C:\>dism /image:c:\winpe64\mount /get-packages
Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

Version de l'image : 10.0.22621.1

Packages listing:

Package Identity : Microsoft-Windows-WinPE-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~10.0.22621.1
State : Installed
Release Type : Language Pack
Install Time : 07/05/2022 05:35

Package Identity : Microsoft-Windows-WinPE-LanguagePack-Package~31bf3856ad364e35~amd64~fr-FR~10.0.22621.1
State : Installed
Release Type : Language Pack
Install Time : 25/04/2025 13:14

Package Identity : Microsoft-Windows-WinPE-Package~31bf3856ad364e35~amd64~~10.0.22621.1
State : Installed
Release Type : Foundation
Install Time : 07/05/2022 05:29
```

4. Je peux désormais démonter mon fichier WinPe

Attention toute les fenêtres doivent être fermée!!!

```
powershell
```

```
dism /unmount-image /mountdir:c:\winpe64\mount /commit
```

```
C:\>dism /unmount-image /mountdir:c:\winpe64\mount /commit
Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

Enregistrement de l'image
[=====100.0%=====]
Démontage de l'image
[=====100.0%=====]

Erreur : 5

Accès refusé.

Le fichier journal DISM se trouve à l'emplacement C:\WINDOWS\Logs\DISM\dism.log
```

Pour voir pourquoi il y a une erreur:

```
powershell
dism /Get-MountedWimInfo
dism /cleanup-wim
```

```
C:\>dism /Get-MountedWimInfo
Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

Images montées :

Aucune image montée n'a été trouvée.

L'opération a réussi.

C:\>dism /cleanup-wim
Outil Gestion et maintenance des images de déploiement
Version : 10.0.22621.1

L'entrée de montage périmée vers C:\mount a été supprimée.
L'entrée de montage périmée vers c:\winpe64\mount a été supprimée.
Analyse du lecteur C à la recherche de fichiers périmés
Analyse du lecteur E à la recherche de fichiers périmés
L'opération a réussi.
```

5. Je peux désormais créer mon fichier ISO :

powershell

```
makewinpemedia /ISO c:\winpe64 c:\winpe64\ISOwinPEpxe1.iso
```

```
C:\>makewinpemedia /ISO c:\winpe64 c:\winpe64\ISOwinPEpxe1.iso
Creating c:\winpe64\ISOwinPEpxe1.iso...
```

```
100% complete
```

```
Success
```

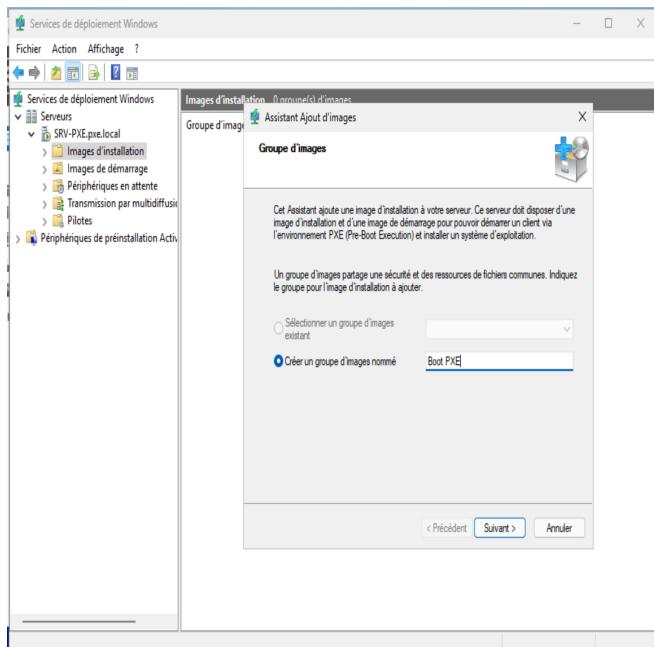
Mon ISO est bien était créé :

| Nom | Modifié le | Type | Taille |
|--------------|------------------|-----------------------|------------|
| fwfiles | 25/04/2025 14:34 | Dossier de fichiers | |
| media | 25/04/2025 14:34 | Dossier de fichiers | |
| mount | 25/04/2025 15:38 | Dossier de fichiers | |
| ISOwinPEpxe1 | 25/04/2025 15:51 | Fichier d'image di... | 363 684 Ko |

6. Ajouter l'image à WDS :

dans :

Outils > services de déploiement > serveur > clic droit sur image d'installation > ajouté une image

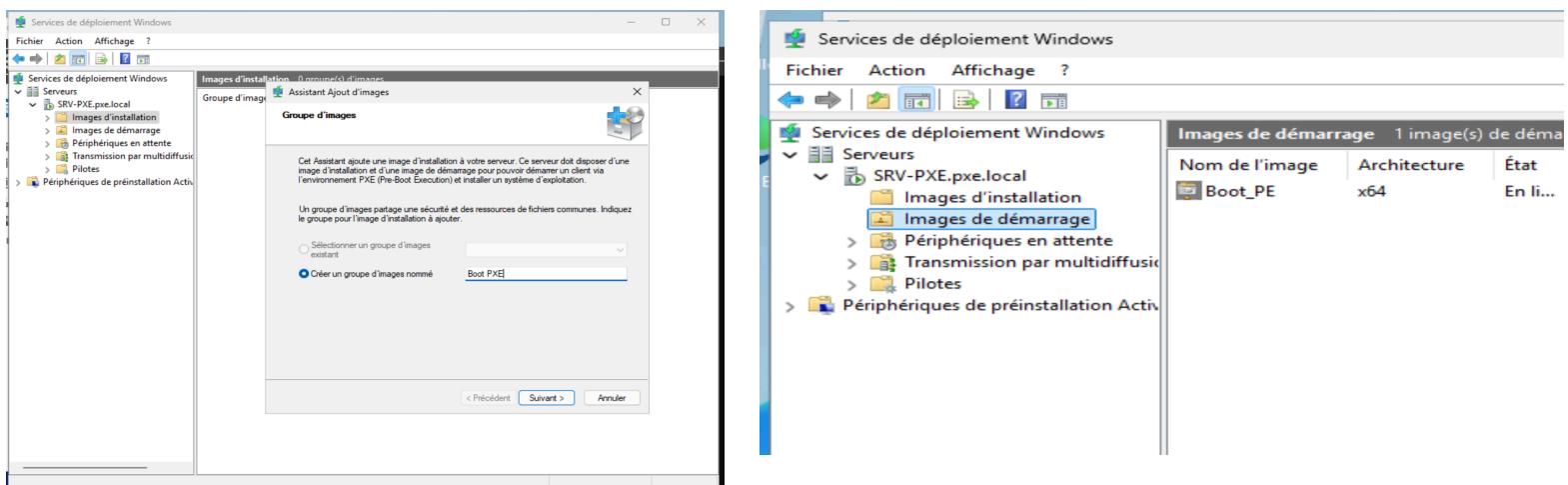


Ajouter une image d'un windows 10 :

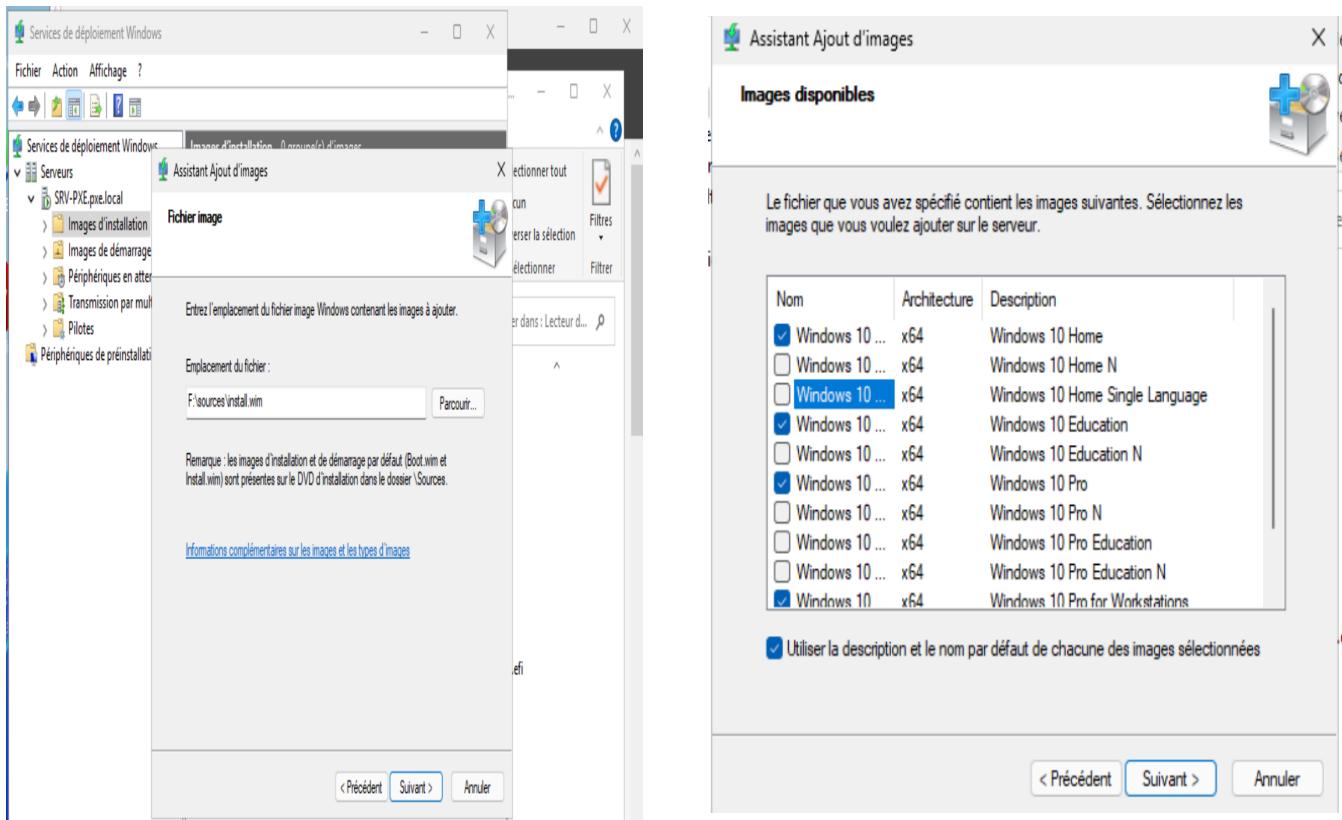
je prends Iso de windows 10 > clic droit > monter

ensuite, il me reste plus qu'à rajouter mes deux images dans mes services de déploiement Windows.

boot.win dans: Images de démarrages



install.wim dans: Images d'installations



J'ai rajouté plusieurs versions de Windows 10

The screenshot shows the 'Services de déploiement Windows' management console. On the left, the navigation pane shows 'SRV-PXE.pxe.local' expanded, with 'Images d'installation' selected. A sub-menu under 'Images d'installation' shows a folder named 'windows10' highlighted. On the right, a detailed view titled 'windows10 4 image(s) d'installation' lists four installed images. The table has columns for 'Nom de l'image' (Image Name), 'Architecture', 'État' (Status), 'Taille décompressée' (Uncompressed Size), 'Date' (Date), and 'V' (Version). The four entries are:

| Nom de l'image | Architecture | État | Taille décompressée | Date | V |
|-----------------|--------------|----------|---------------------|---------|---|
| Windows 10 E... | x64 | En li... | 14778 Mo | 29/0... | 1 |
| Windows 10 Pro | x64 | En li... | 14792 Mo | 29/0... | 1 |
| Windows 10 P... | x64 | En li... | 14778 Mo | 29/0... | 1 |
| Windows 10 H... | x64 | En li... | 14476 Mo | 29/0... | 1 |

Job 3 : Test et Automatisation

5/ Boot Machine Virtuelle depuis le serveur PXE

1. Créer une VM sans disque dur.
2. Configurer le boot réseau (PXE).
3. Démarrer : le menu WDS doit proposer WinPE

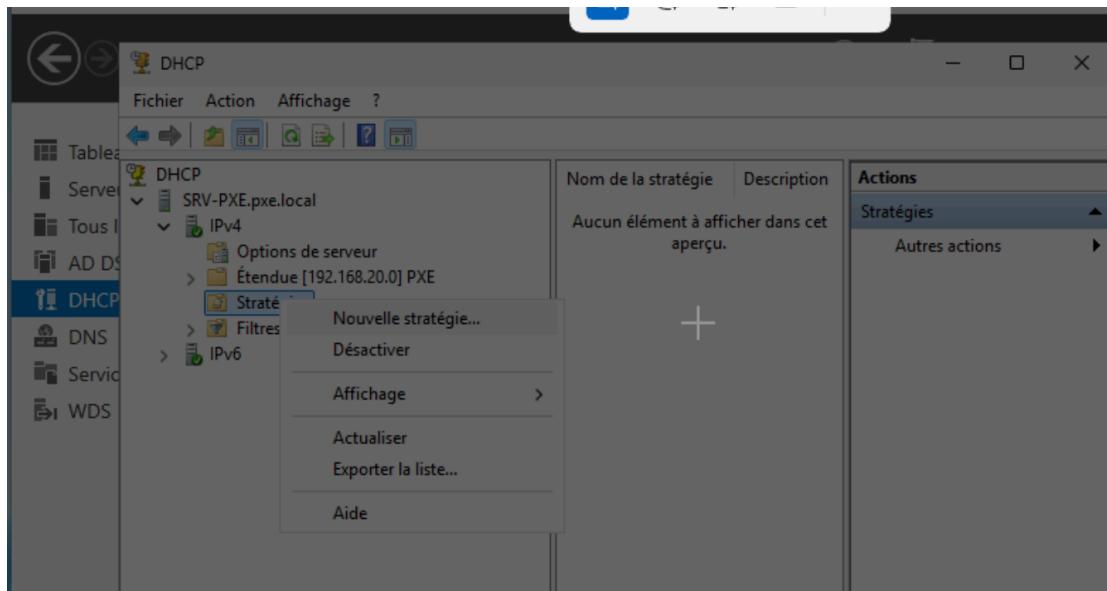
Problèmes courants :

- **PXE-E32: TFTP Timeout** → Vérifier le pare-feu (autoriser UDP 69).
- **Pas de réponse DHCP** → Vérifier que WDS est lié au DHCP (option 60).

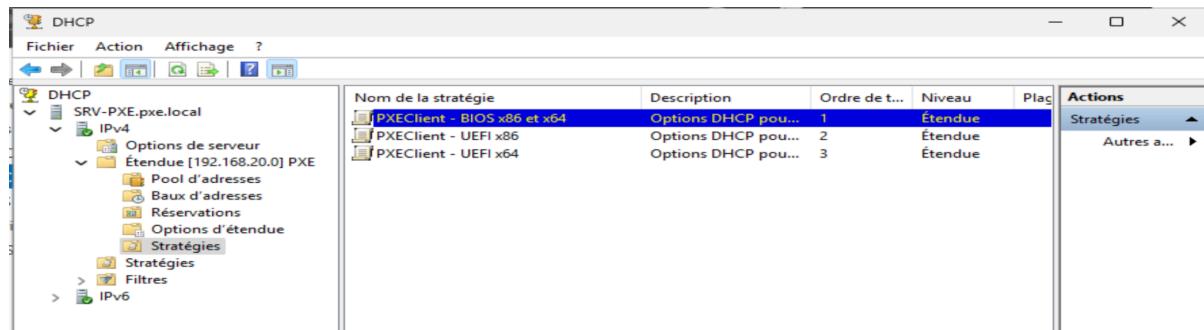
Suivant le mode de démarrage, il faut régler le DHCP de manière différente.

| Mode | Option 60 | Option 66 | Option 67 |
|------|-----------|-------------------|----------------------|
| BIOS | - | Adresse IP du WDS | boot\x64\wdsnbp.com |
| UEFI | PXEClient | Adresse IP du WDS | boot\x64\wdsmgfw.efi |

Nous pouvons créer des stratégies de démarrage pour que le DHCP réponde suivant la configuration de machine (Bios ou UEFI)

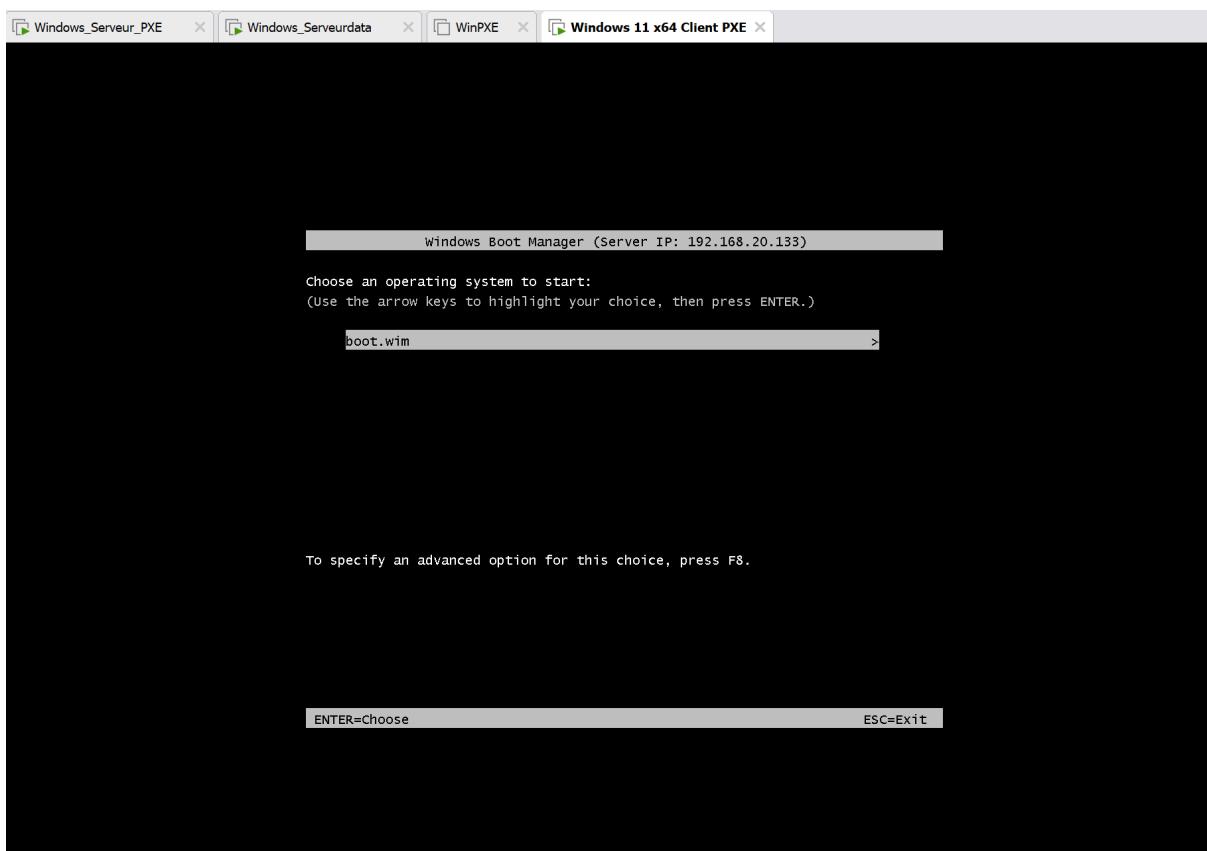
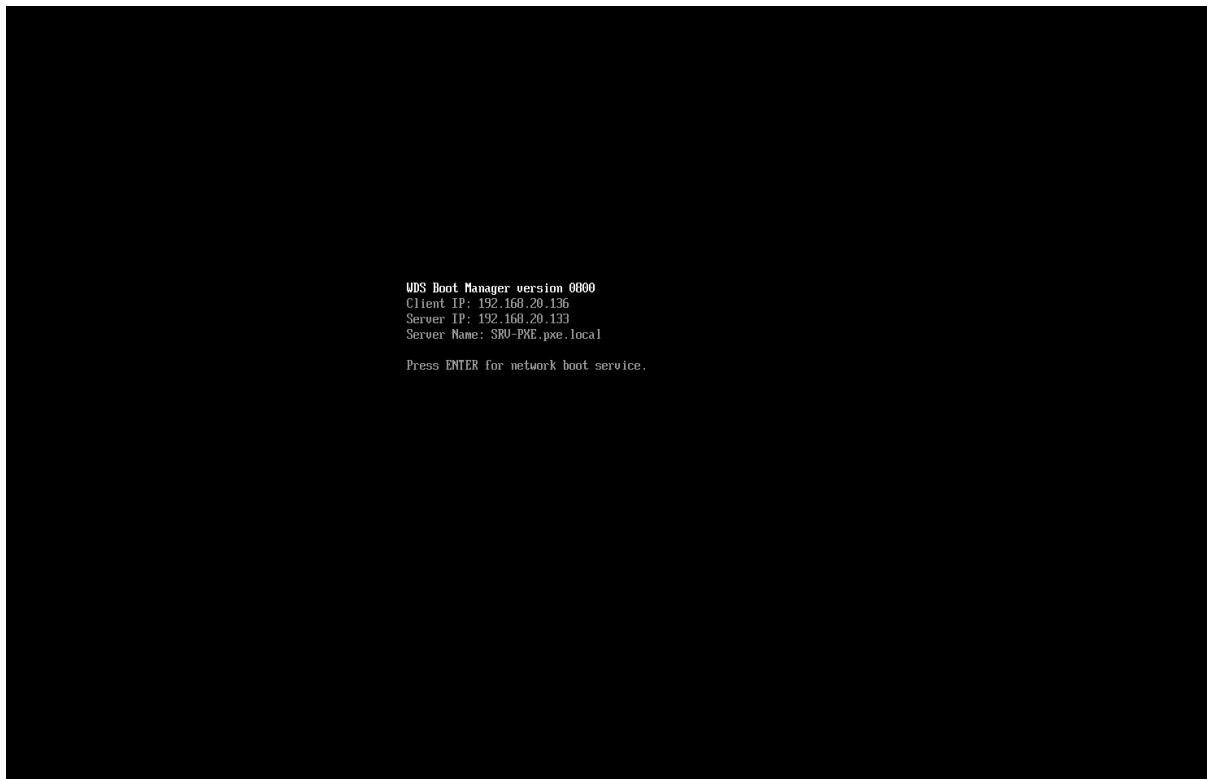


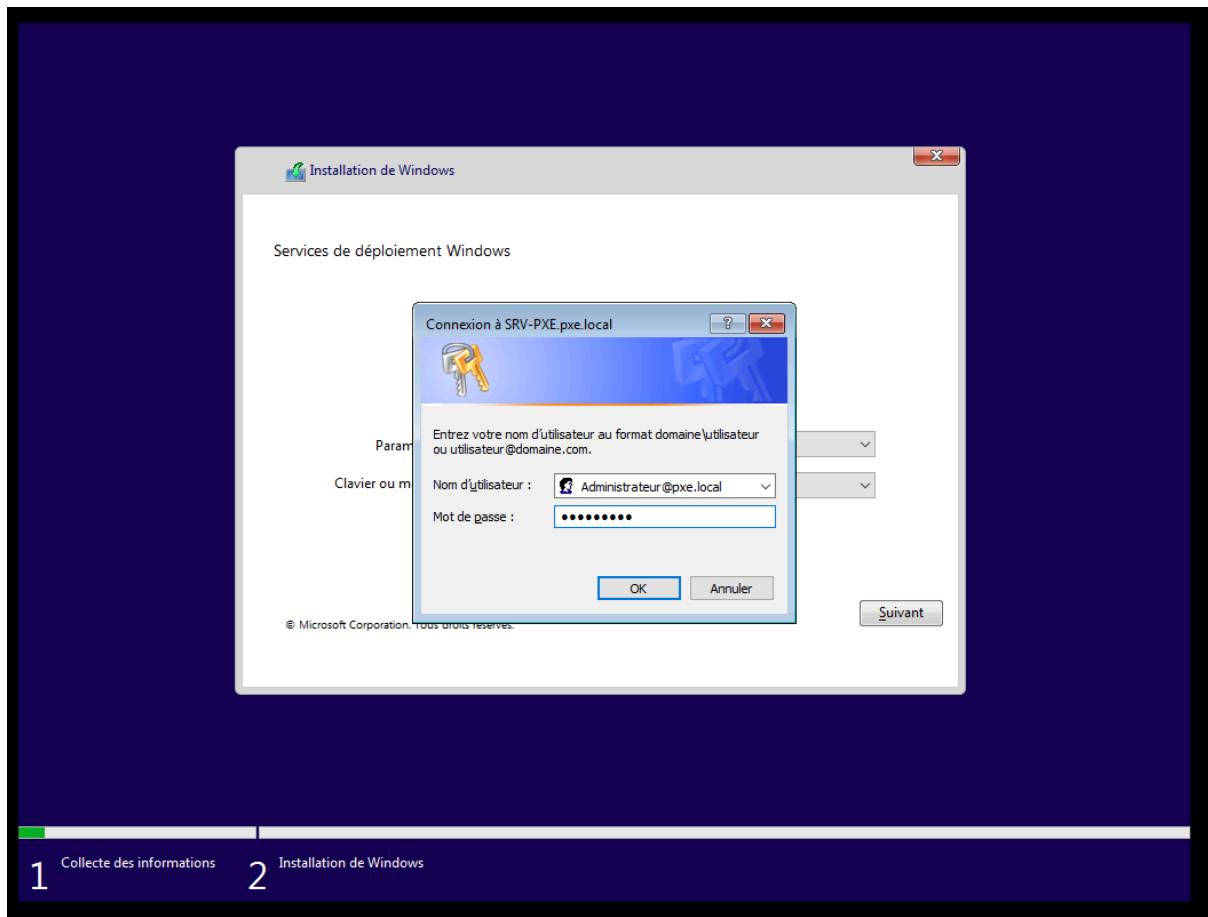
Nous allons créer 3 profils différents UEFI x64, UEFI x86 et BIOS X64 et X86

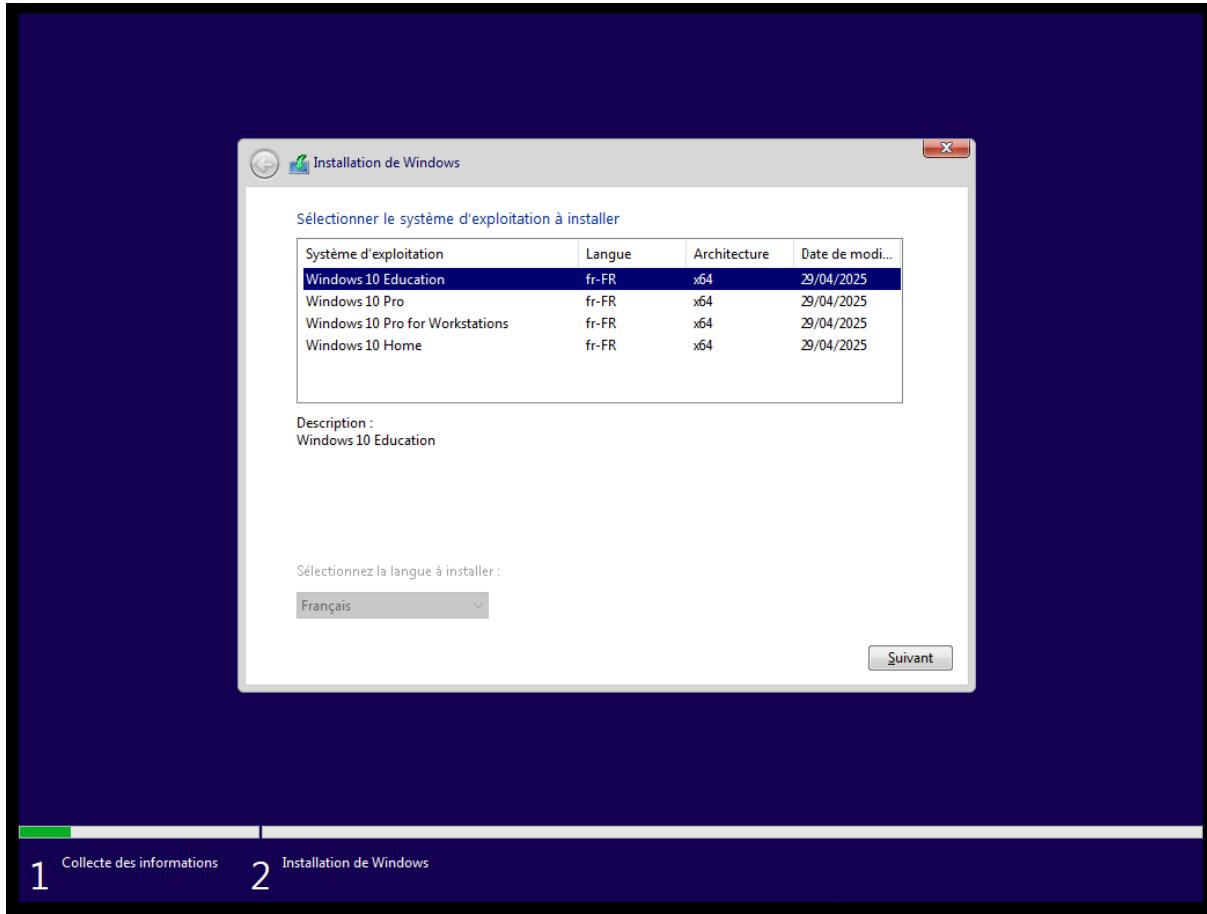


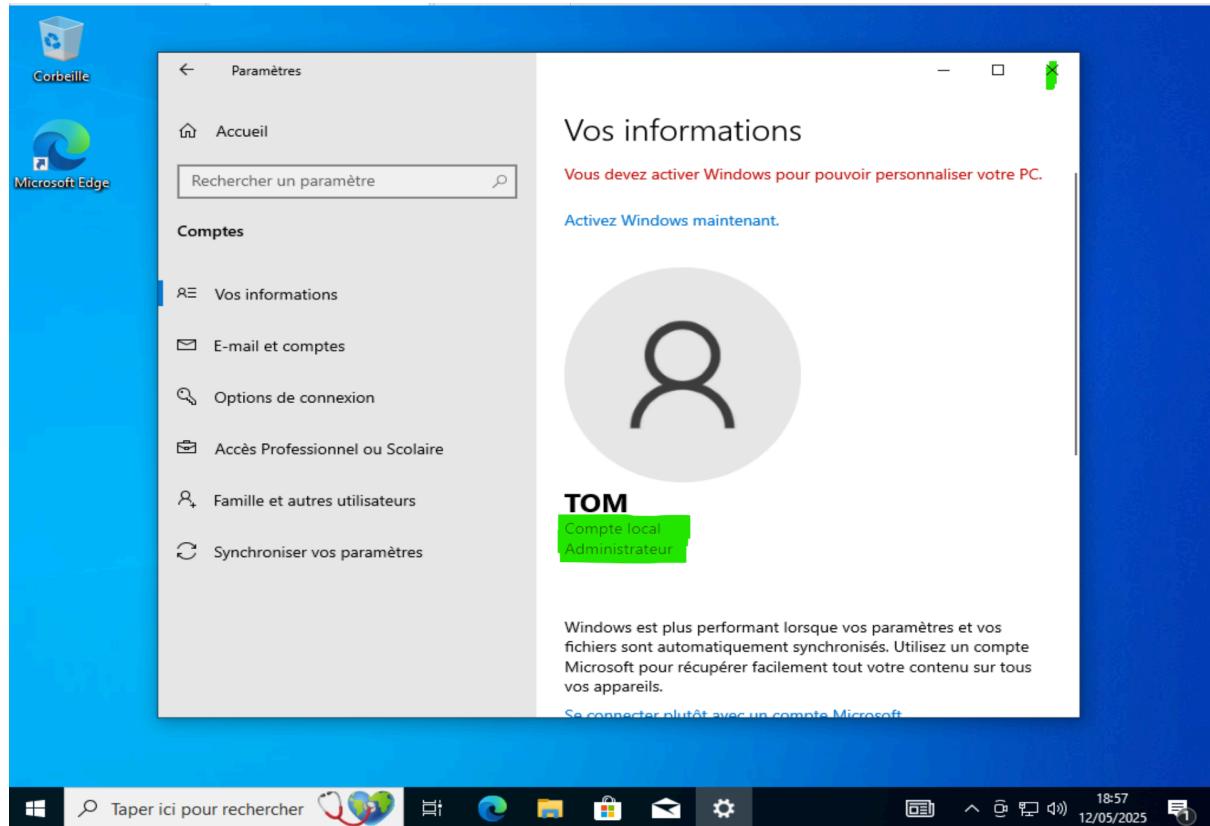
Pour faciliter la création, j'utilise un Script (Voir Script sur Github)

Je démarre donc ma machine clients qui as été crée sans os ni disque dur pour démarrer en PXE et déployer mon Os depuis mon serveur local









6/ Automatisation de l'installation grâce à AD et à un script PowerShell

1. Création de la GPO pour l'intégration automatique au domaine

a. Créer un compte de service dédié

```
powershell

# Dans AD (exécuter sur le DC)
$userParams = @{
    Name          = "SVC_JoinDomain"
    SamAccountName = "SVC_JoinDomain"
    UserPrincipalName = "SVC_JoinDomain@pxe.local"
    Path          = "OU=Service Accounts,DC=pxe,DC=local"
    Description    = "Compte pour jonction automatique au domaine"
    AccountPassword = (ConvertTo-SecureString "P@ssw0rdComplexe!")
-AsPlainText -Force)
    Enabled        = $true
    PasswordNeverExpires= $true
}
New-ADUser @userParams

# Autoriser à joindre des machines (10 max)
Set-ADObject -Identity "CN=Computers,DC=pxe,DC=local" -Add @{
    "ms-DS-MachineAccountQuota" = "10" }
```

b. Créer la GPO

1. Ouvrir Gestion des stratégies de groupe (gpmc.msc)

2. Créer une GPO :

Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups

- Ajouter Domain Admins au groupe Administrators local

3. Script de démarrage :

Computer Configuration > Policies > Windows Settings > Scripts (Startup)

- Ajouter Join-Domain.ps1

3. Script PowerShell d'intégration (Join-Domain.ps1)

```
powershell

# Sauvegarder dans \\SRV-DEPLOY\Deploy$\Scripts\
$domain = "pxe.local"
$ou = "OU=Workstations,DC=pxe,DC=local"
$credential = New-Object
System.Management.Automation.PSCredential("pxe\SVC_JoinDomain",
(ConvertTo-SecureString "P@ssw0rdComplex!" -AsPlainText -Force))

try {
    Add-Computer -DomainName $domain -Credential $credential -OUPath $ou -Force
-ErrorAction Stop
    Write-Output "[SUCCESS] Machine jointe au domaine $domain"
} catch {
    Write-Output "[ERROR] Échec de jonction : $_"
    exit 1
}
```

4. Fichier de partitionnement (partition.txt)

```
diskpart

# Sauvegarder dans \\SRV-DEPLOY\Deploy$\Scripts\

select disk 0

clean

convert gpt

create partition efi size=500

format quick fs=fat32 label="System"

assign letter="S"

create partition msr size=128

create partition primary

format quick fs=ntfs label="Windows"

assign letter="D"

exit
```

5. Script principal de déploiement (deploy.ps1)

```
powershell

# Variables

$imagePath = "\SRV-DEPLOY\Deploy$\Images\Win10_22H2.wim"

$scriptsPath = "\SRV-DEPLOY\Deploy$\Scripts"

# 1. Partitionnement

Start-Process -FilePath "diskpart" -ArgumentList "/s
$scriptsPath\partition.txt" -Wait -NoNewWindow

# 2. Application de l'image

dism /apply-image /imagefile:$imagePath /index:1 /applydir:D:\

# 3. Configuration du boot

bcdboot D:\Windows /s S: /f UEFI

# 4. Post-installation

Copy-Item "$scriptsPath\Join-Domain.ps1" -Destination
"D:\Windows\Setup\Scripts\"

# 5. Redémarrage

Write-Output "Déploiement terminé. Redémarrage dans 10 secondes..."

Start-Sleep -Seconds 10

Restart-Computer -Force
```

6. Configuration WDS pour l'automatisation

1. Modifier `unattend.xml`:

2. xml

```
<FirstLogonCommands>

    <SynchronousCommand wcm:action="add">

        <CommandLine>powershell.exe -ExecutionPolicy Bypass -File
D:\Windows\Setup\Scripts\Join-Domain.ps1</CommandLine>

        <Order>1</Order>

    </SynchronousCommand>

</FirstLogonCommands>
```

3. Injecter dans l'image :

```
powershell

Mount-WindowsImage -Path "C:\Mount" -ImagePath "Win10_22H2.wim" -Index 1

Copy-Item "unattend.xml" -Destination "C:\Mount\Windows\Panther\"

Dismount-WindowsImage -Path "C:\Mount" -Save
```

7. Déploiement et Validation

1. Démarrer un client PXE :

- Le partitionnement et l'installation se lancent automatiquement
- La machine rejoint le domaine au premier démarrage

2. Vérifier dans AD :

```
powershell

Get-ADComputer -Filter * -SearchBase "OU=Workstations,DC=pxe,DC=local"
```

7/ Sécurisation d'Image et du serveur

Sécuriser WDS :

- **Filtrage MAC : Autoriser uniquement les machines connues.**
- **Chiffrement BitLocker :**

```
powershell
```

```
manage-bde -on E: -usespaceonly
```

Chiffre les données utilisé sur le disque E

- **Pare-feu : Bloquer tout sauf PXE (ports 67, 68, 69, 4011).**

Sécuriser les Images :

- **Signer les images :**

```
powershell
```

```
signtool sign /fd SHA256 /f C:\cert.pfx /p "MotDePasse" C:\Images\Win10.wim
```

- **Permissions NTFS : Restreindre E:\RemoteInstall aux admins.**

Validation et Tests

Tests à Effectuer

1. Test PXE :
 - Démarrer une VM en PXE → Vérifier que le menu WDS s'affiche.
 2. Test DNS :
 - Depuis un client : nslookup srv-pxe.pxe.local doit résoudre l'IP.
 3. Test Déploiement :
 - Lancer WinPE → Vérifier que le script PowerShell s'exécute.
-

Difficultés et Solutions

| Problème | Solution |
|------------------------------|---|
| Client ne boot pas en PXE | Vérifier DHCP Option 60 et pare-feu TFTP |
| Image ne s'applique pas | Vérifier les pilotes dans WinPE |
| Erreur d'intégration AD | Vérifier la GPO et les crédentiel PS |

Résumé des Outils Utilisés

- WDS : Serveur PXE/TFTP.
- ADK : Création d'images (imagex.exe, dism).
- PowerShell : Automatisation (déploiement, AD).
- GPO : Politiques pour l'automatisation.

