SOMMAIRE

PRESENTATION DES OUTILS

Suite à la réception des ordinateurs, notre prochain objectif sera de déployer le système d'exploitation de notre choix.

Notre premier choix à été le programme ManageEngine OS Deployer.

ManageEngine
OS Deployer

Un programme propriétaire permettant de réaliser la majeure partie de nos objectifs.

Il permet d'avoir une interface graphique agréable et très simple, permettant de faciliter le travail de l'équipe IT.
Seulement deux problèmes majeurs se présentent :
-Le coût : à partir de 650€ par an, là où notre alternative est gratuite. D'autant qu'il fait parti d'une suite d'autre logiciels de gestion de Windows, incitant à dépenser encore pour avoir un écosystème fonctionnel.

-L'incrémentation : s'agissant d'un programme tiers, n'étant pas implémenté de base dans Windows, il est plus sensible aux discordances et plantages, bugs et retard de mise à niveau.

Il aurait pû être une solution stable, viable, payante mais cohérente. Seulement nous allons nous intéresser à une alternative bien plus répandue, car gratuite et implémenté dans l'écosystème Microsoft :

Microsoft Deployment Toolkit (MDT)

MDT (Microsoft Deployment Toolkit)

Créé par Microsoft en 2003, disponible gratuitement et disposant d'une énorme quantité de documentation, vidéos, tutoriels, dans toutes les langues, il s'impose comme un choix logique, malgré une relative complexité et une interface peu agréable, il est notre logiciel de choix.

COMPARATIF

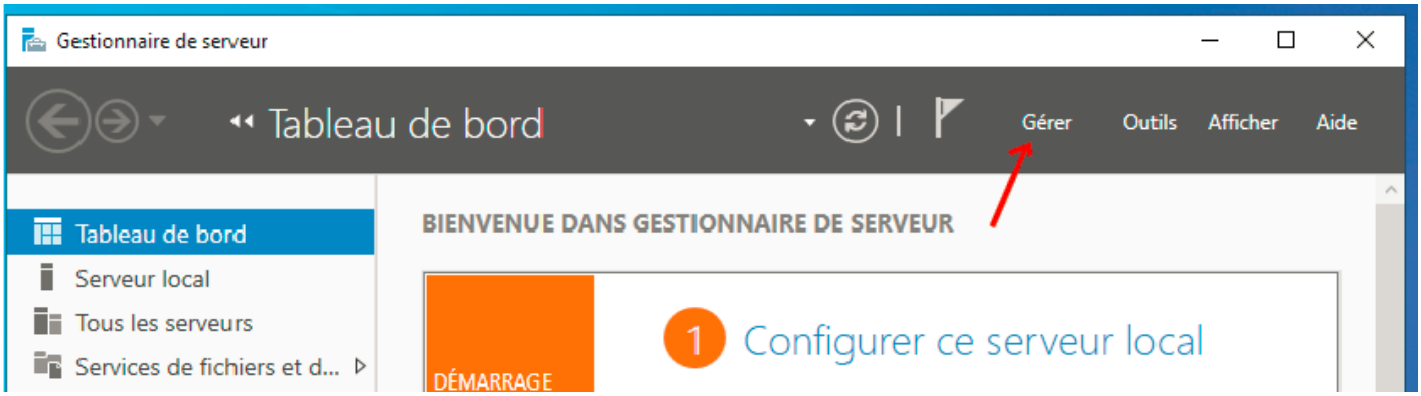
Manage Engine OS Deployer	Microsoft Deployment Toolkit
Interface graphique simple et facile d'accès.	GUI très fonctionnelle
Large prise en charge de matériel	Possibilité de personnaliser des images ISO
Assistance et support pour la résolution de problèmes	Système d'automatisation poussé
Mise en place de service/ AD intégré	Gratuit
	Intégration de plusieurs outils Microsoft (WDS)
Prise en charge matériel moins étendue que WDS	Configuration manuelle un peu ardue pour les novices
Gestion de l'AD unique pour le logiciel, donc conflits potentiels	Pas de support technique dédié
Moins de documentations	
Payant	

METHODE DE DEPLOIEMENT

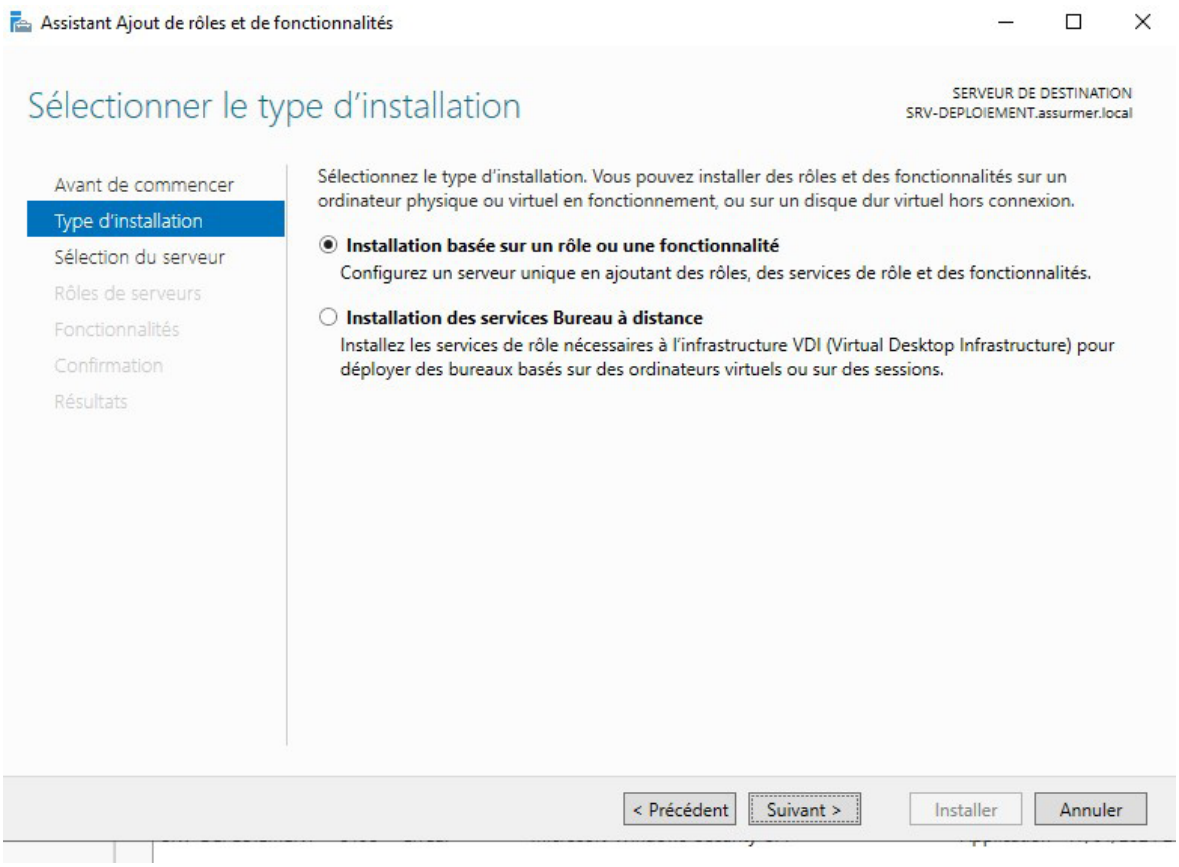
Tout d'abord, s'assurer d'avoir un Active Directory fonctionnel, dans le cas d'Assurmer, ce dernier existe déjà sous le nom de domaine "assurmer.local".
Si jamais il n'est pas déjà en place, pour ajouter ce rôle sur le serveur "SVR-ADWS", suivre la meme méthode que pour le serveur DHCP.

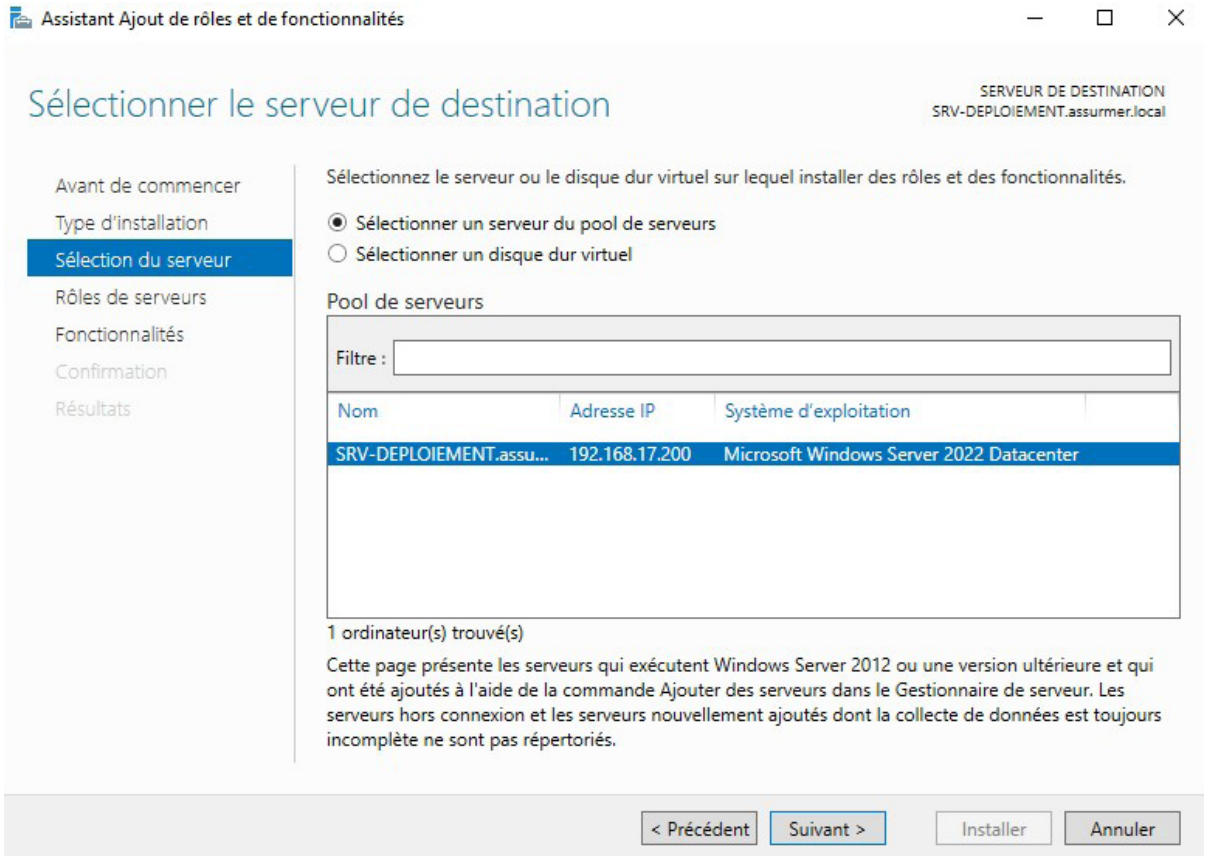
Concernant le DHCP, voici comment procéder:

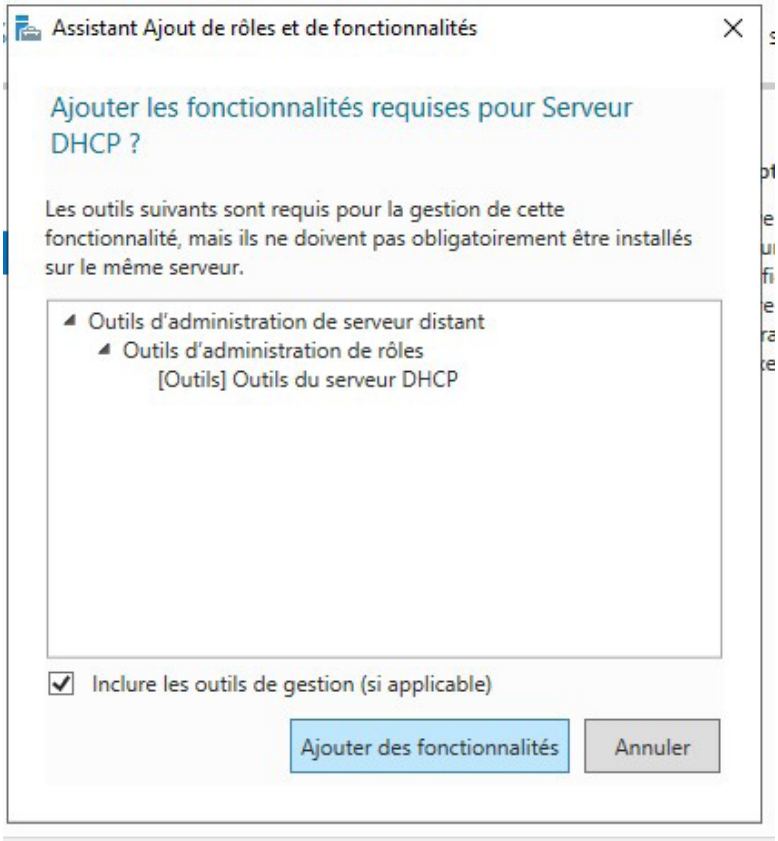
Cliquer sur "Gérer en haut à droite puis sur "ajout de rôles et fonctionnalités"

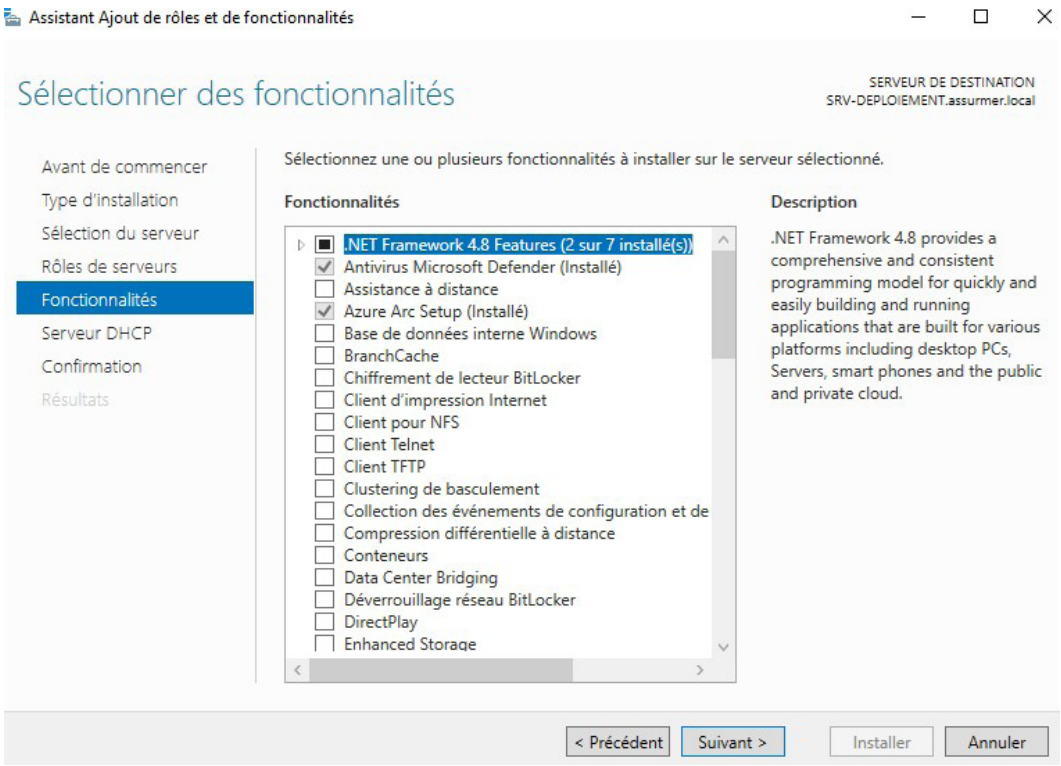


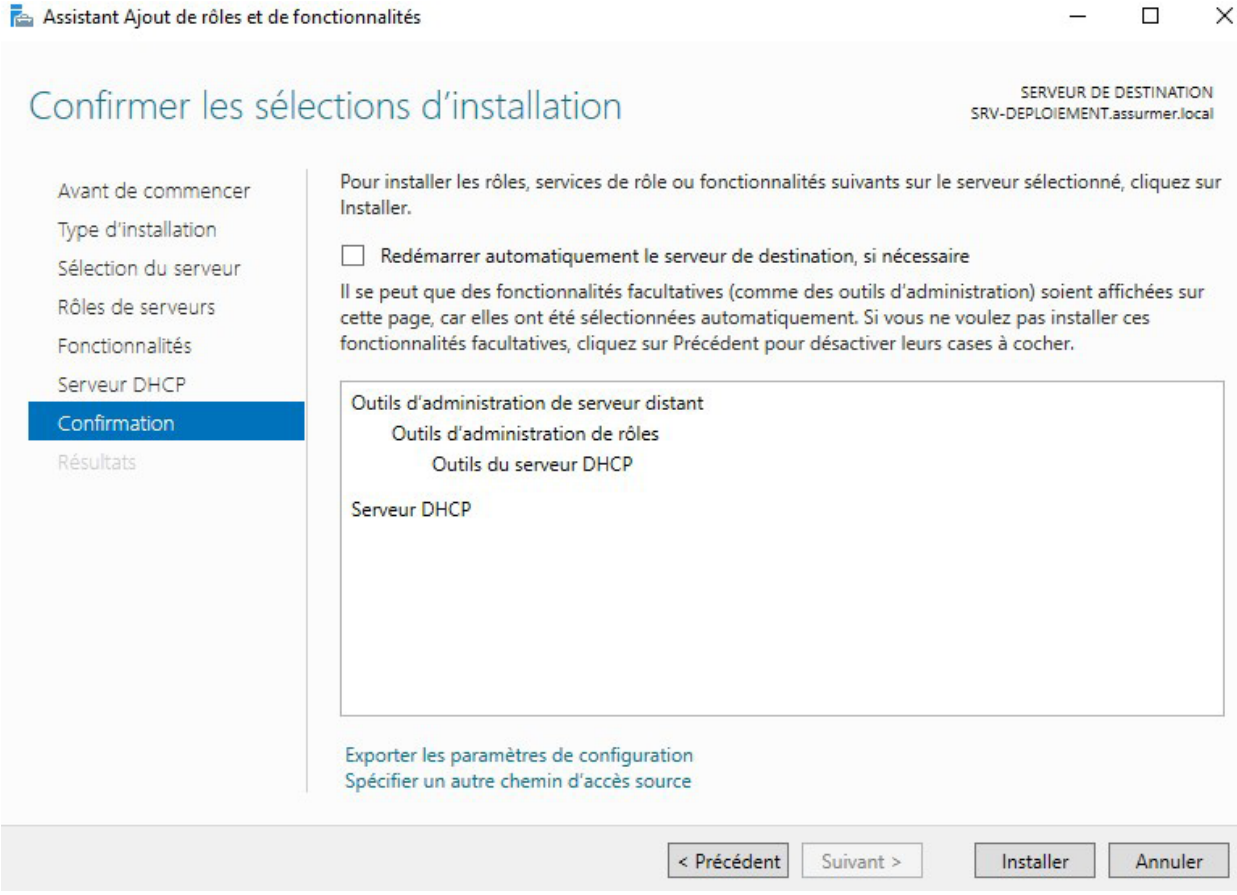
Ensuite, lancer l'installation du rôle de cette manière :



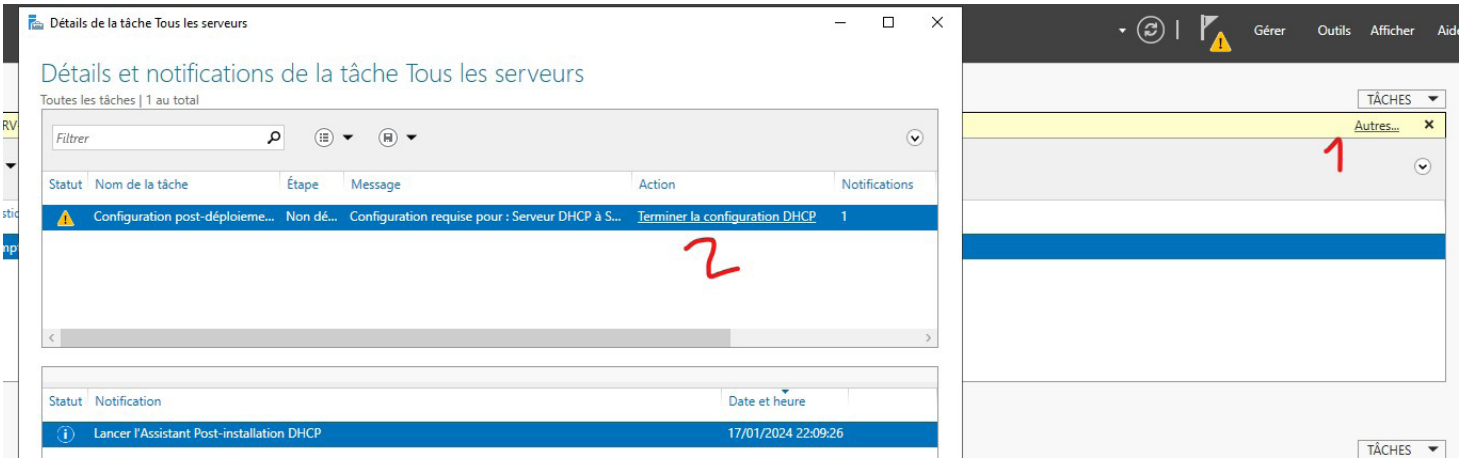

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
SRV-DEPLOIEMENT.assurmer.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
SRV-DEPLOIEMENT.assu...
192.168.17.200
Microsoft Windows Server 2022 Datacenter
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

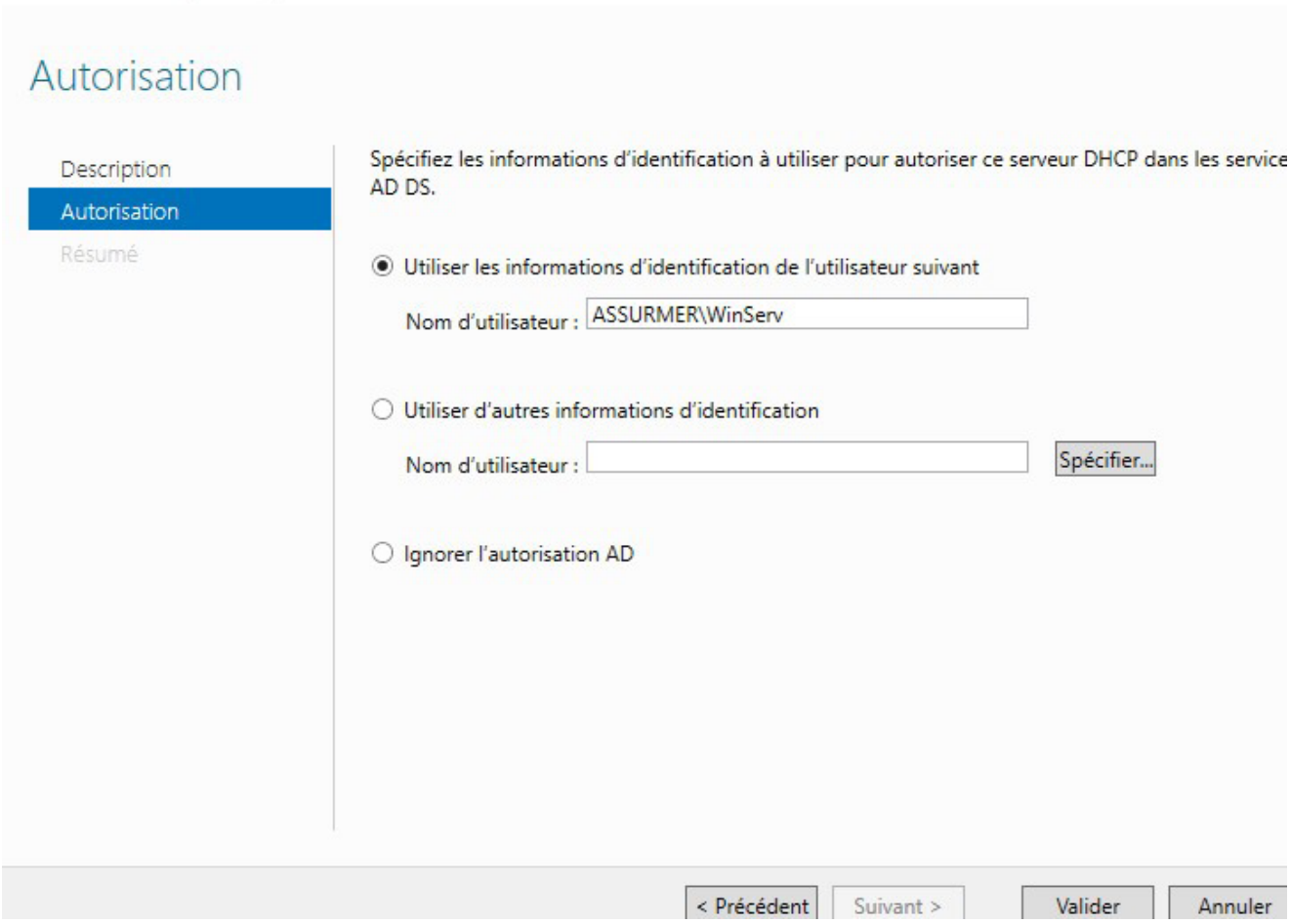

Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Serveur DHCP ?
Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.
Outils d'administration de serveur distant
Outils d'administration de rôles
[Outils] Outils du serveur DHCP
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des fonctionnalités
SERVEUR DE DESTINATION
SRV-DEPLOIEMENT.assurmer.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.
Fonctionnalités
.NET Framework 4.8 Features (2 sur 7 installé(s))
Antivirus Microsoft Defender (Installé)
Assistance à distance
Azure Arc Setup (Installé)
Base de données interne Windows
BranchCache
Chiffrement de lecteur BitLocker
Client d'impression Internet
Client pour NFS
Client Telnet
Client TFTP
Clustering de basculement
Collection des événements de configuration et de
Compression différentielle à distance
Conteneurs
Data Center Bridging
Déverrouillage réseau BitLocker
DirectPlay
Enhanced Storage
Description
.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
SRV-DEPLOIEMENT.assurmer.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP
Serveur DHCP
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

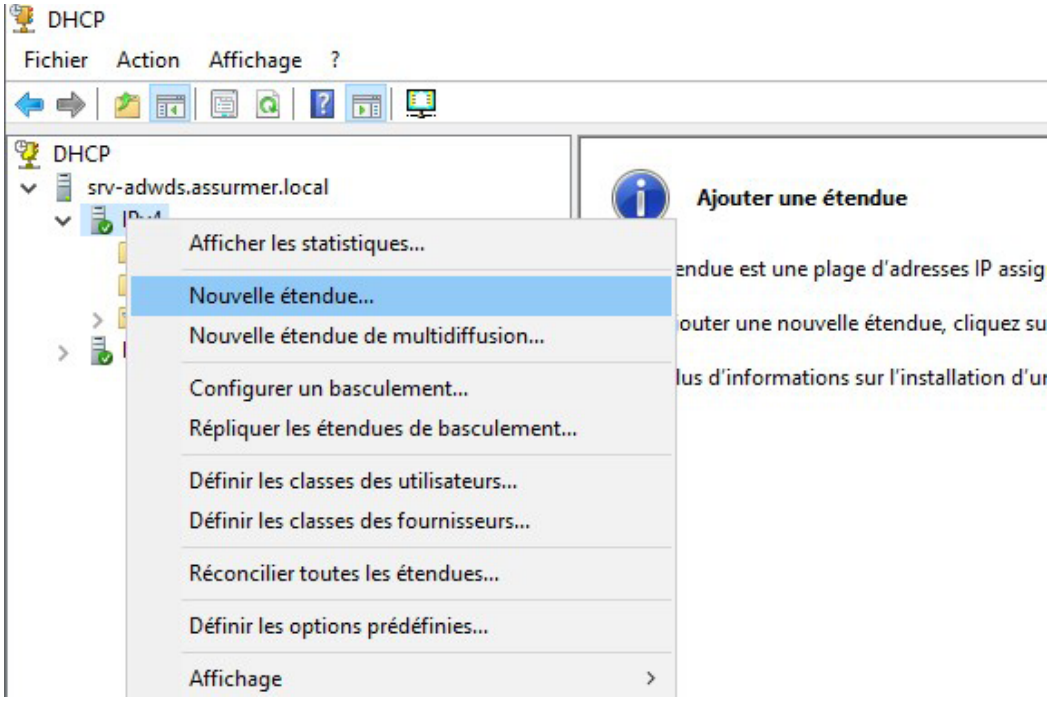
Il faut maintenant configurer le serveur DHCP, se rendre dans Autres (1) puis cliquer sur "Configuration post déploiement".

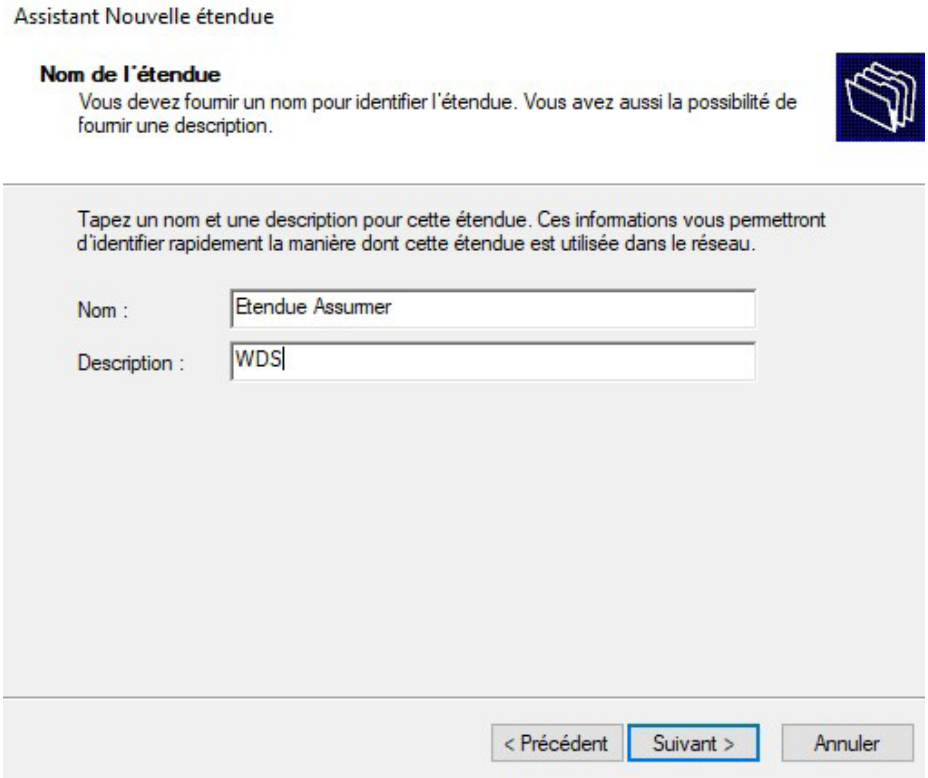


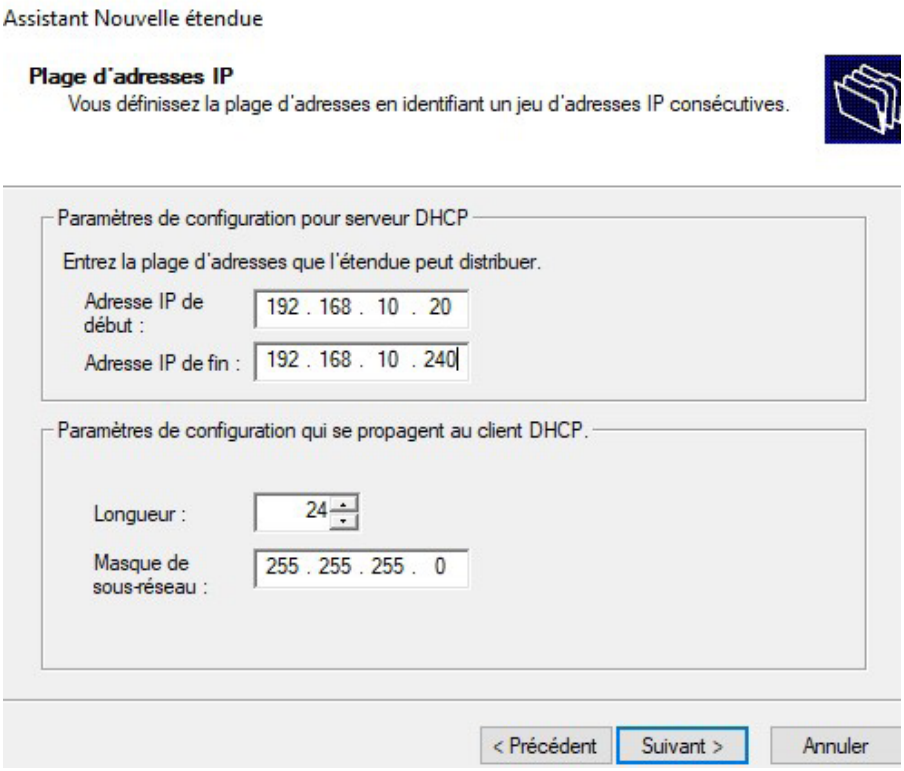


Une fois promu et paramétré selon nos besoins, regler la plage d'adressage IP (suffisante pour le nombre de poste à installer), pour cela il faut créer une nouvelle étendue.

Taper DHCP dans la recherche Windows et cliquer pour accéder à la fenêtre. Suivre les étapes çi dessous pour créer l'étendue.



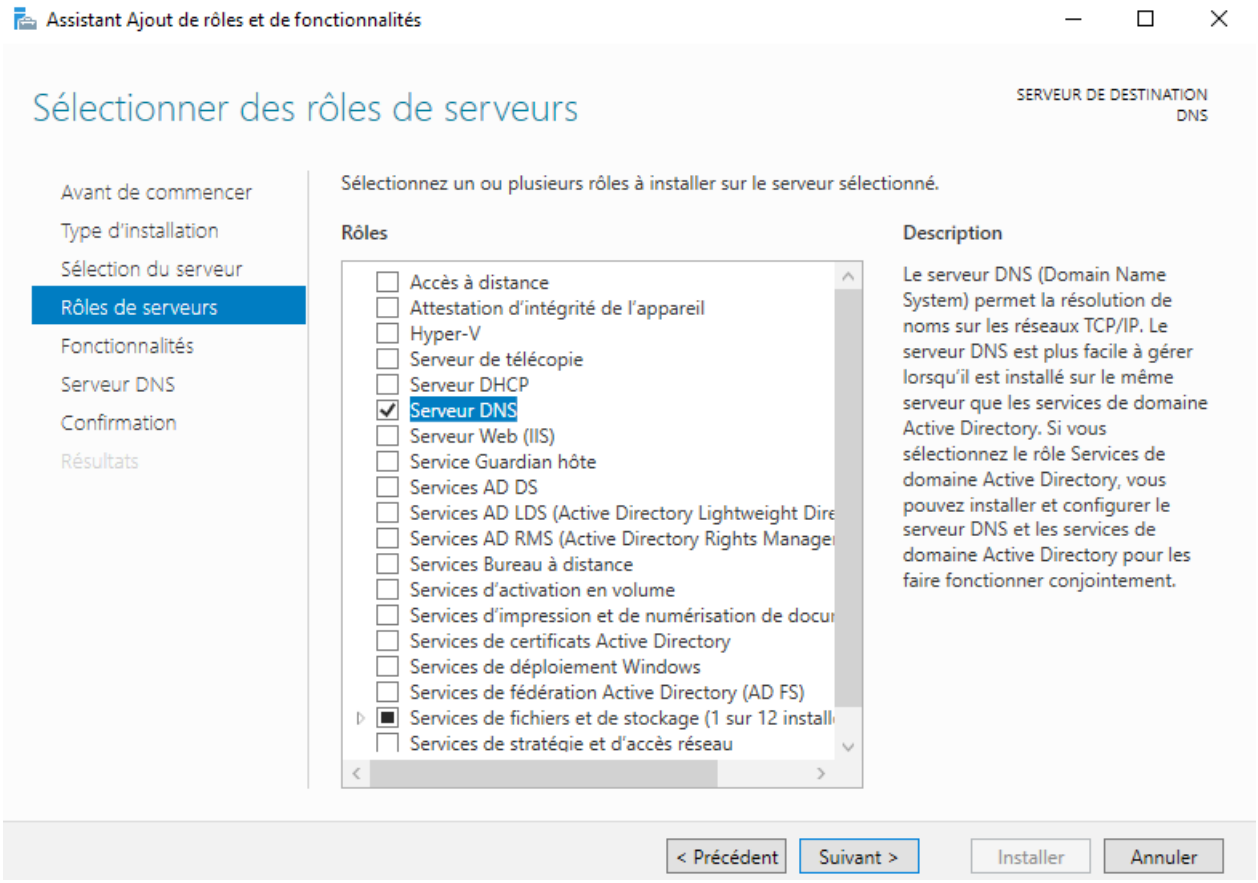


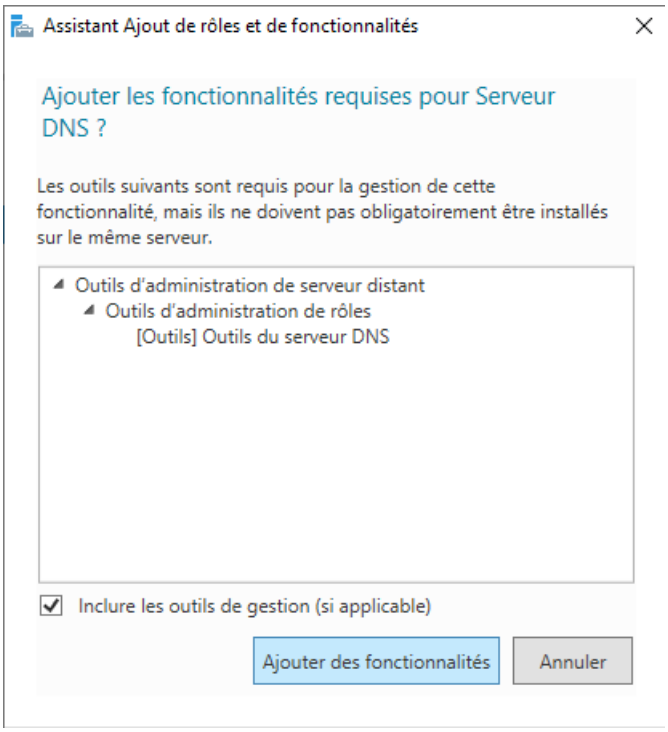


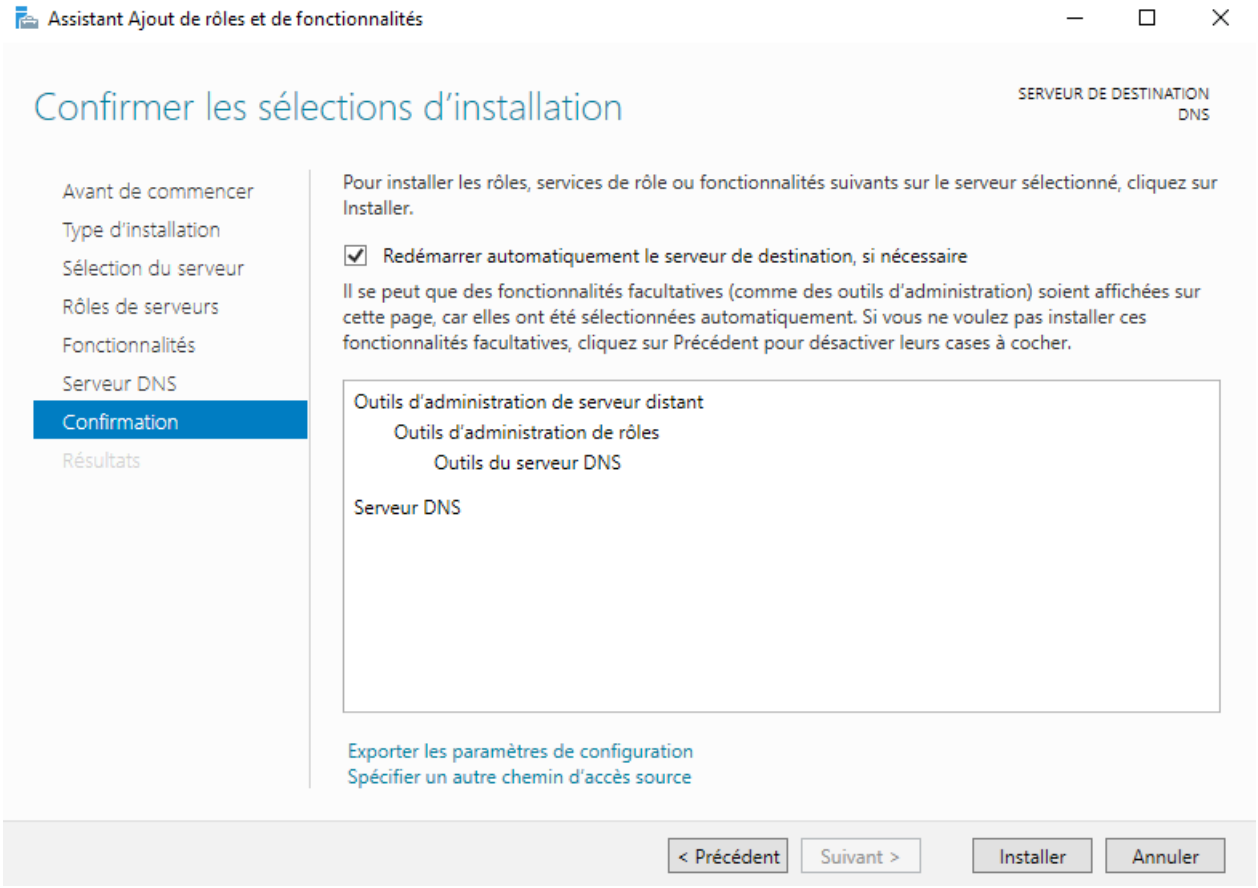
Nous laisserons l'ajout d'exclusion vierge et la durée du bail par défaut, indiquer l'IP du serveur pour la passerelle et le nom de demaine sera "assurmer. local". pas de serveur WINS et on termine par activer l'étendue.

L'étendue étant activée, il faut activer le rôle DNS et DHCP, voici comment procéder.

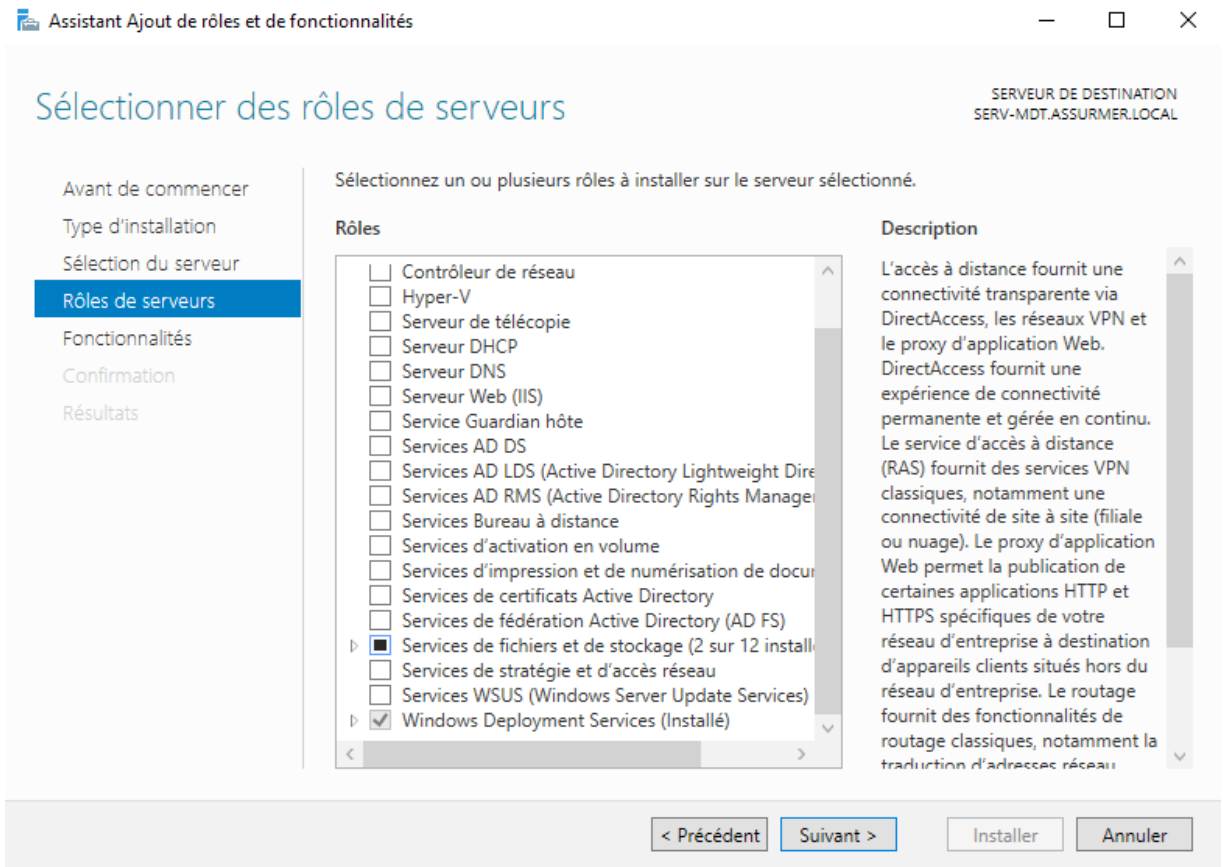
Pour le DNS :



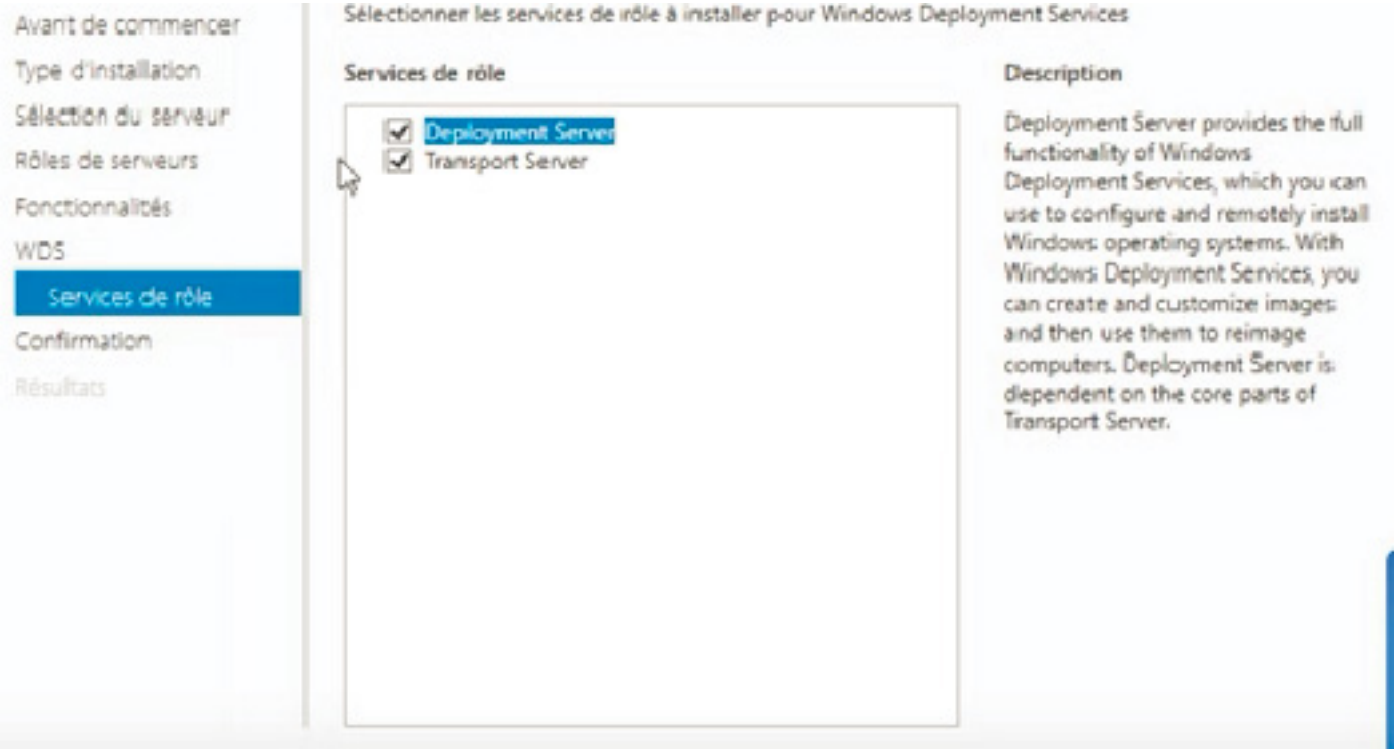



Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
DNS
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DNS
Serveur DNS
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

Pour le DWS :

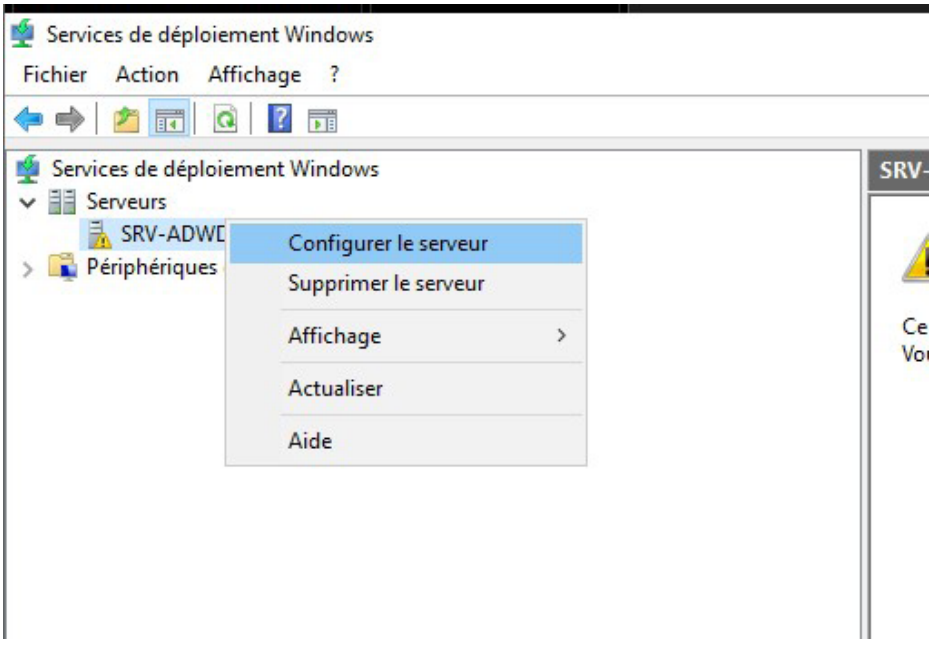

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
SERV-MDT.ASSURMER.LOCAL
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (2 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Windows Deployment Services (Installé)
Description
L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la
< Précédent
Suivant >
Installer
Annuler

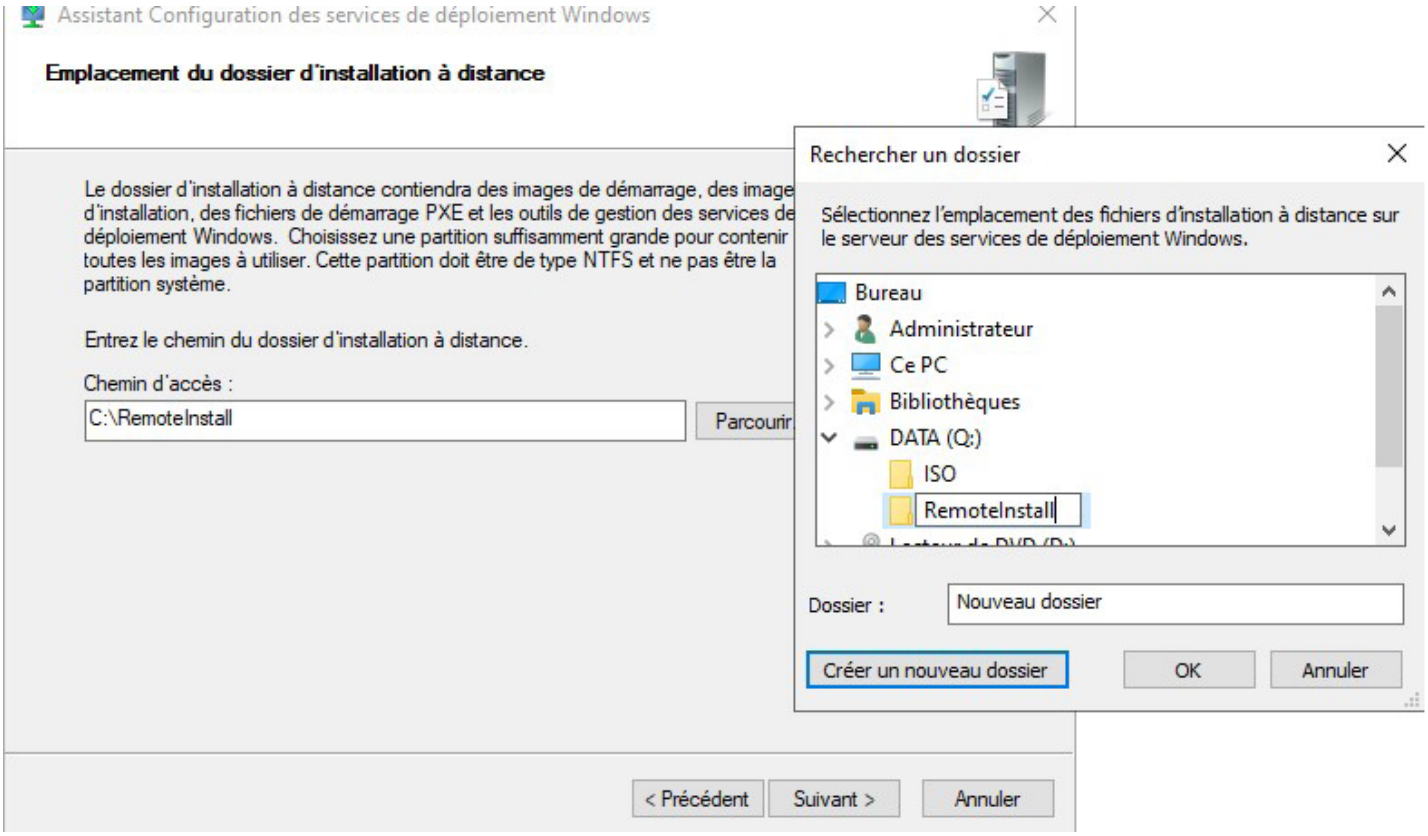
Laisser cochés les deux services de rôles et continuer jusqu'a pouvoir lancer l'installation.

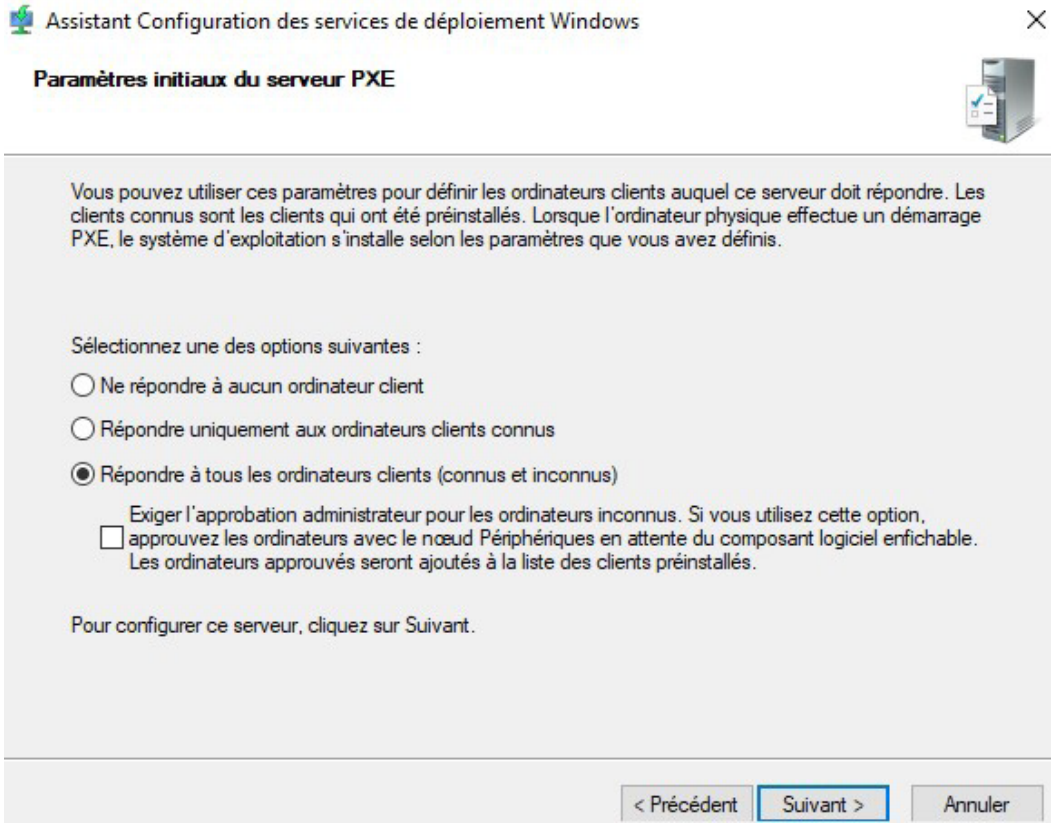


Taper "wds" dans la barre de recherche Windows et ouvrir Services de deploiement Windows que nous avons préalablement installé.

Ensuite, faire un clic droit sur le serveur et cliquer sur "configurer le serveur"

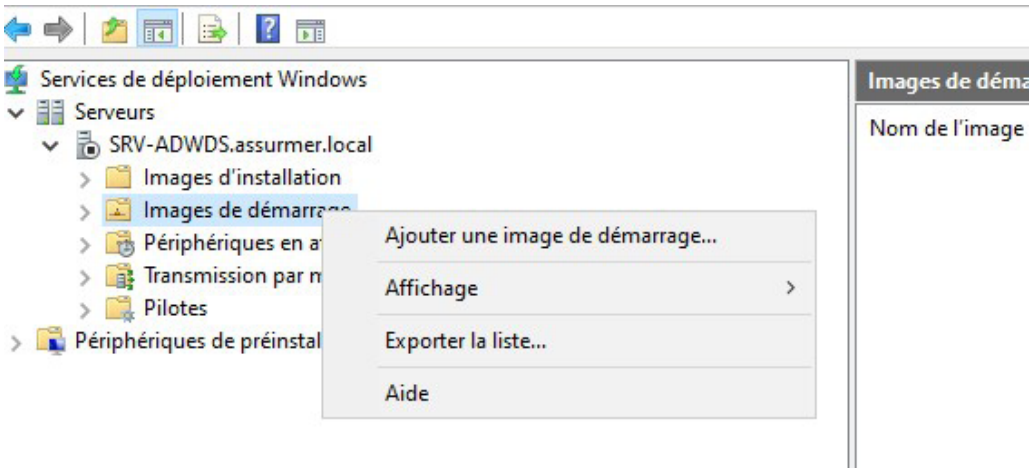


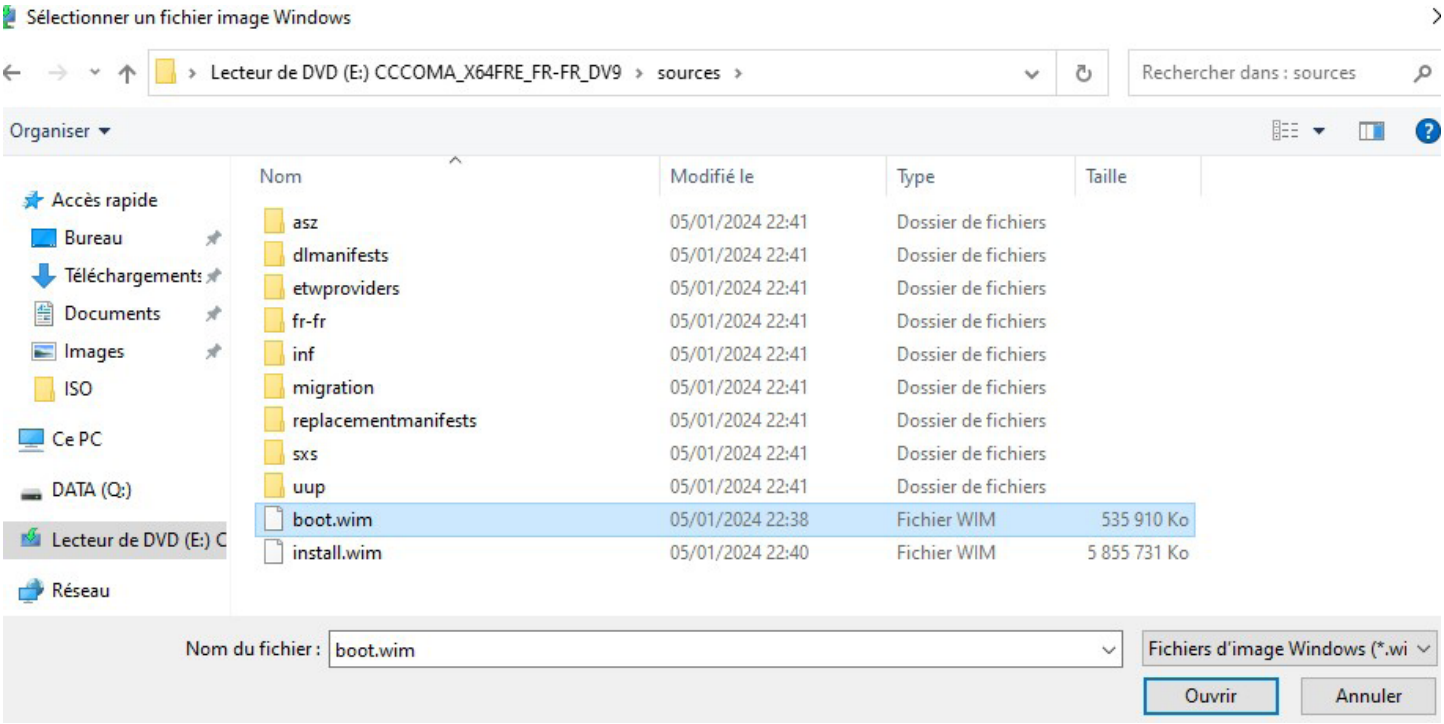

Assistant Configuration des services de déploiement Windows
Emplacement du dossier d'installation à distance
Le dossier d'installation à distance contiendra des images de démarrage, des image
d'installation, des fichiers de démarrage PXE et les outils de gestion des services de
déploiement Windows. Choisissez 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 :
C:\RemoteInstall
Parcourir
Rechercher un dossier
Sélectionnez l'emplacement des fichiers d'installation à distance sur
le serveur des services de déploiement Windows.
Bureau
Administrateur
Ce PC
Bibliothèques
DATA (Q:)
ISO
RemoteInstall
Dossier :
Nouveau dossier
Créer un nouveau dossier
OK
Annuler
< Précédent
Suivant >
Annuler

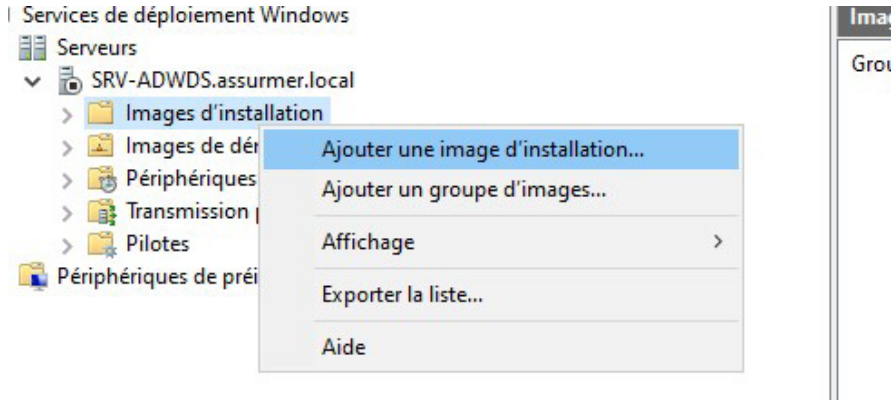

Assistant Configuration des services de déploiement Windows
Paramètres initiaux du serveur PXE
Vous pouvez utiliser ces paramètres pour définir les ordinateurs clients auquel ce serveur doit répondre. Les
clients connus sont les clients qui ont été préinstallés. Lorsque l'ordinateur physique effectue un démarrage
PXE, le système d'exploitation s'installe selon les paramètres que vous avez définis.
Sélectionnez une des options suivantes :
Ne répondre à aucun ordinateur client
Répondre uniquement aux ordinateurs clients connus
Répondre à tous les ordinateurs clients (connus et inconnus)
Exiger l'approbation administrateur pour les ordinateurs inconnus. Si vous utilisez cette option,
approuvez les ordinateurs avec le nœud Périphériques en attente du composant logiciel enfichable.
Les ordinateurs approuvés seront ajoutés à la liste des clients préinstallés.
Pour configurer ce serveur, cliquez sur Suivant.
< Précédent
Suivant >
Annuler

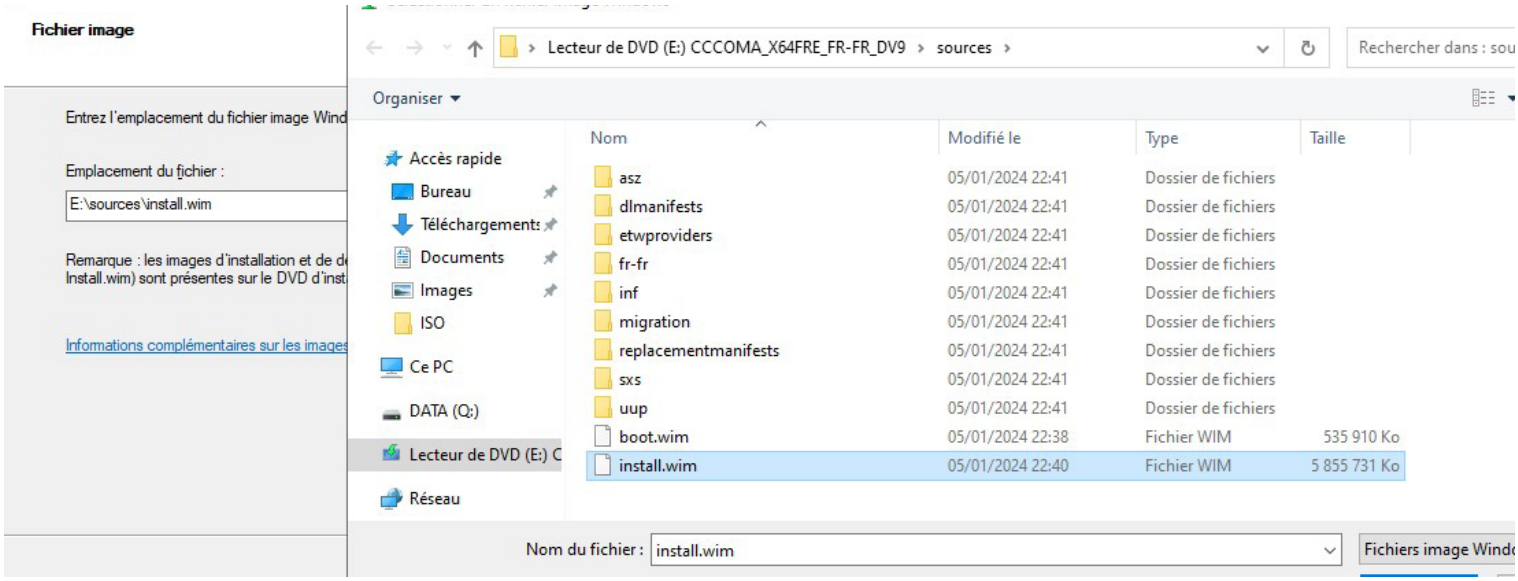
Au préalable, monter l'ISO dans un lecteur de disque virtuel (E:) dans lequel on trouvera le dossier "sources" puis boot.wim

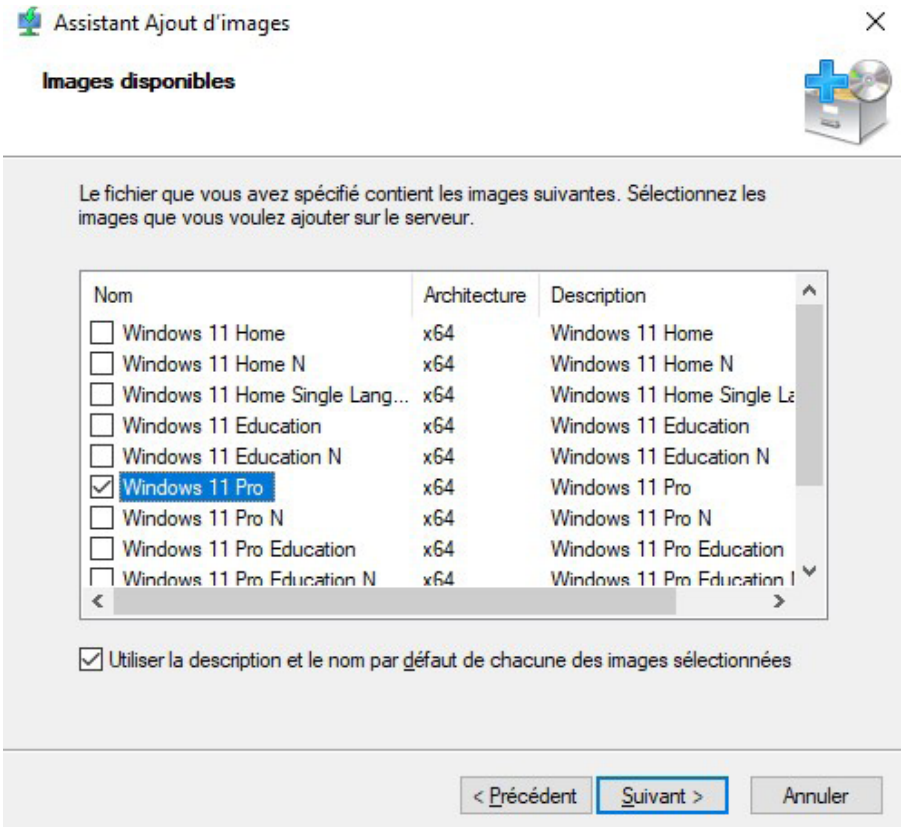
Maintenant, nous allons ajouter notre image de démarrage ainsi que notre image d'installation.











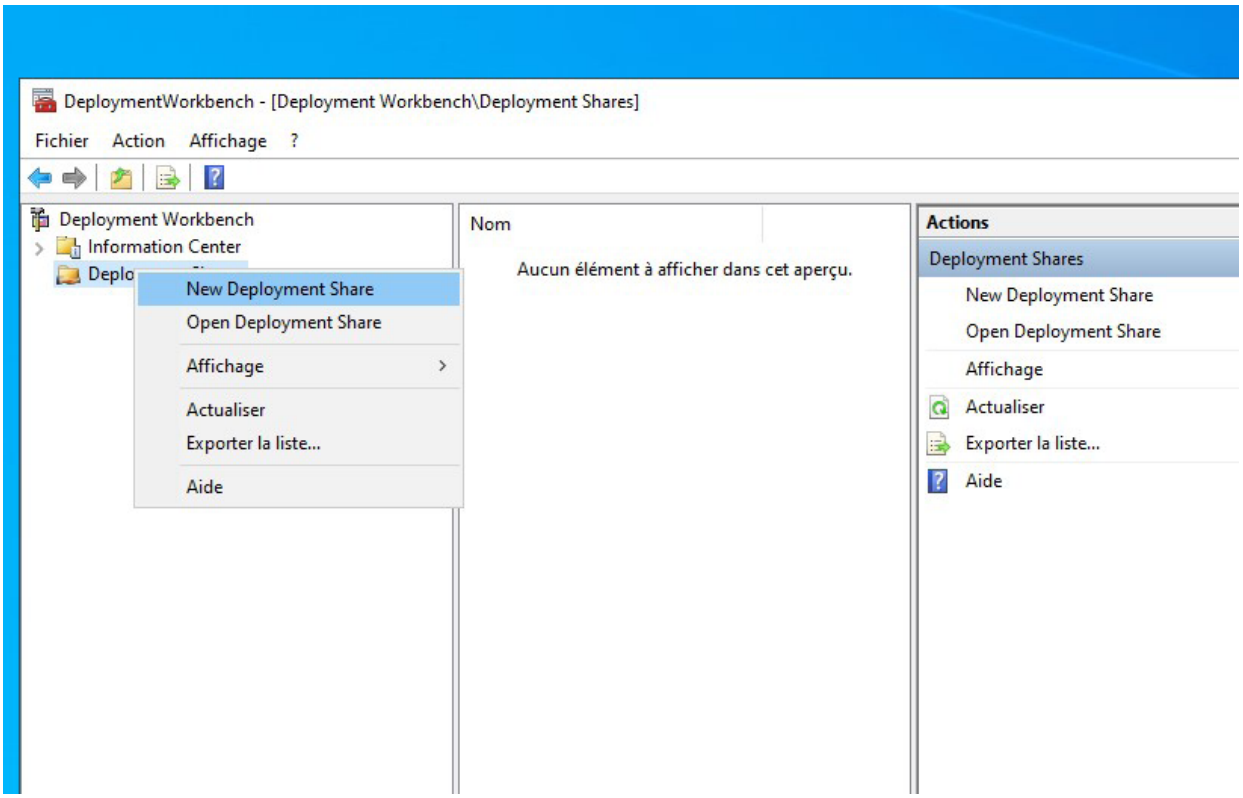
Enfin, faire un clic droit sur le serveur et le démarrer.

Pour Assurmer, nous avons opté pour l'utilisation de W11 (pro) afin de s'assurer d'avoir un OS à jour, compatible avec des outils récents et qui aura un support sur le long terme.

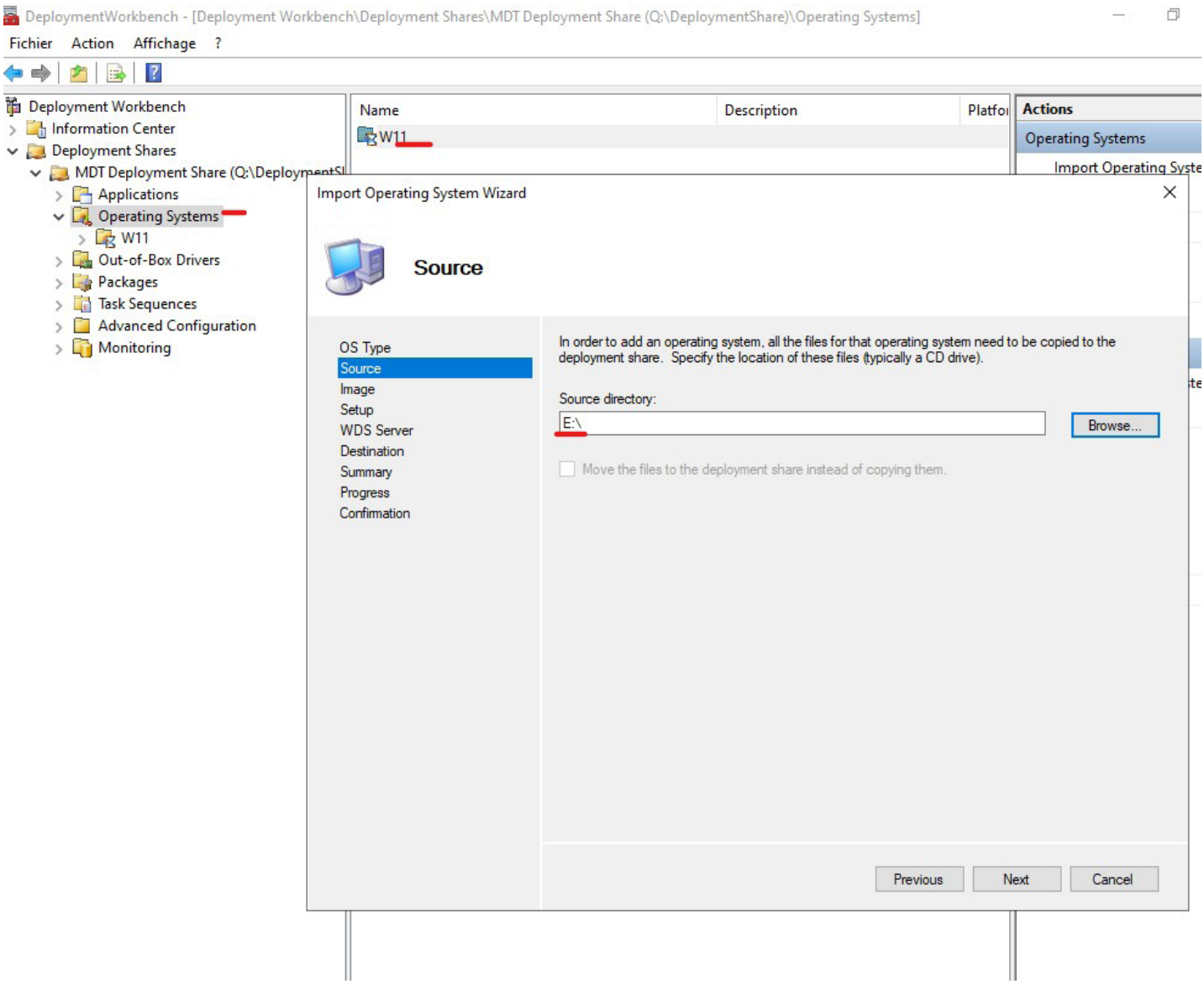
Précedemment, W10 jusqu'a la version 21h1, ne demandait que WDS pour déployer l'OS dans un environnement PxE. Désormais, depuis les versions plus récentes et celle qui nous intéresse, donc W11 23h2, il nous faut l'outil "MDT".

Ce dernier permet de deployer W11 en tenant compte des sécurités, telles que le TPM 2.0, obligatoire pour notre OS.

Télécharger MDT, Windows ADK et Winpe, puis les installer.
Ensuite ouvrir Deployment Workbench qui s'est installé et faire un clic droit sur DeploymentShare, puis cliquer sur New Deployment Share.



Pour le chemin du Deployment Share, ce dernier doit aller sur notre second support de stockage.

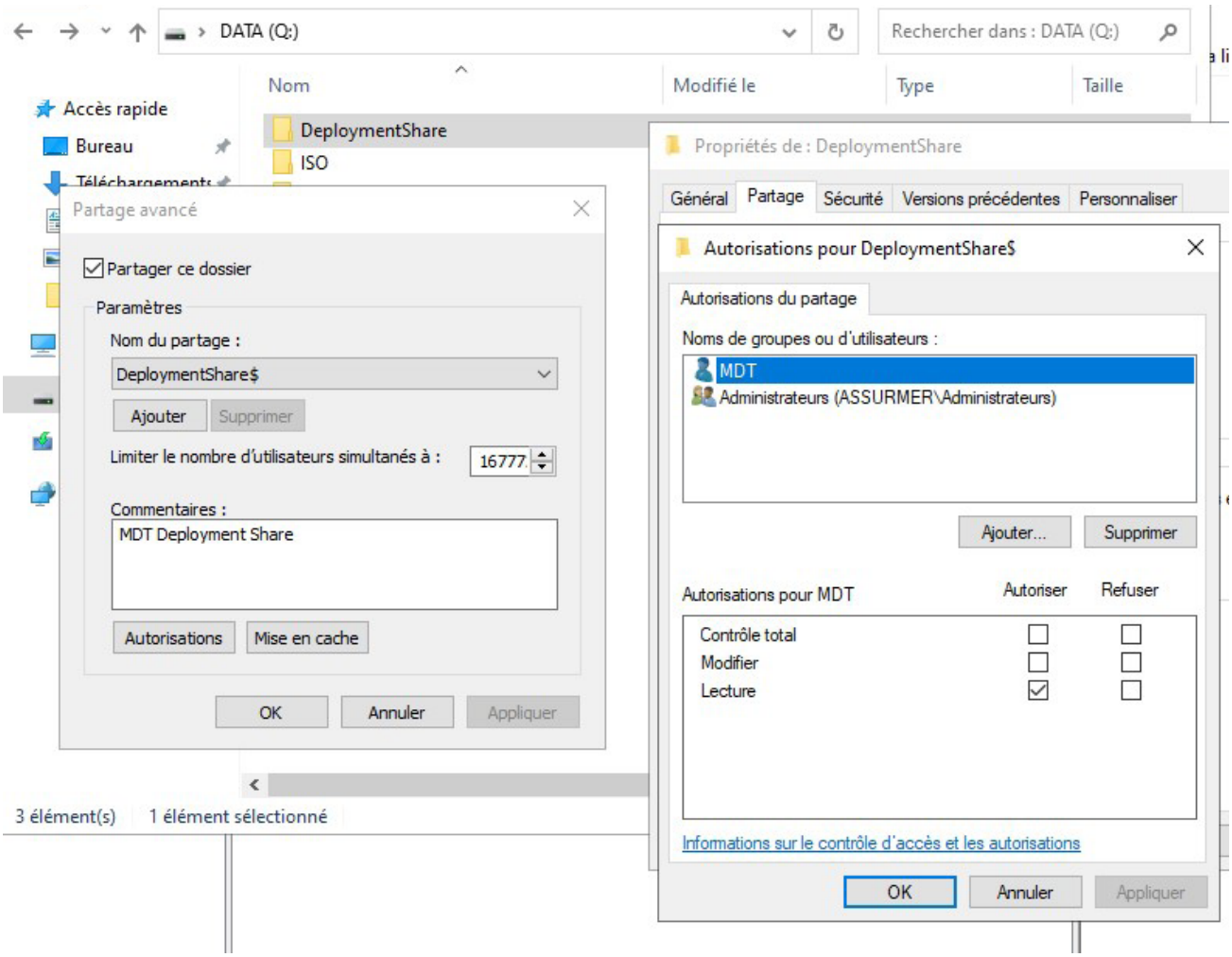


Laisser les options par défaut et poursuivre jusqu'à la fin de l'installation.

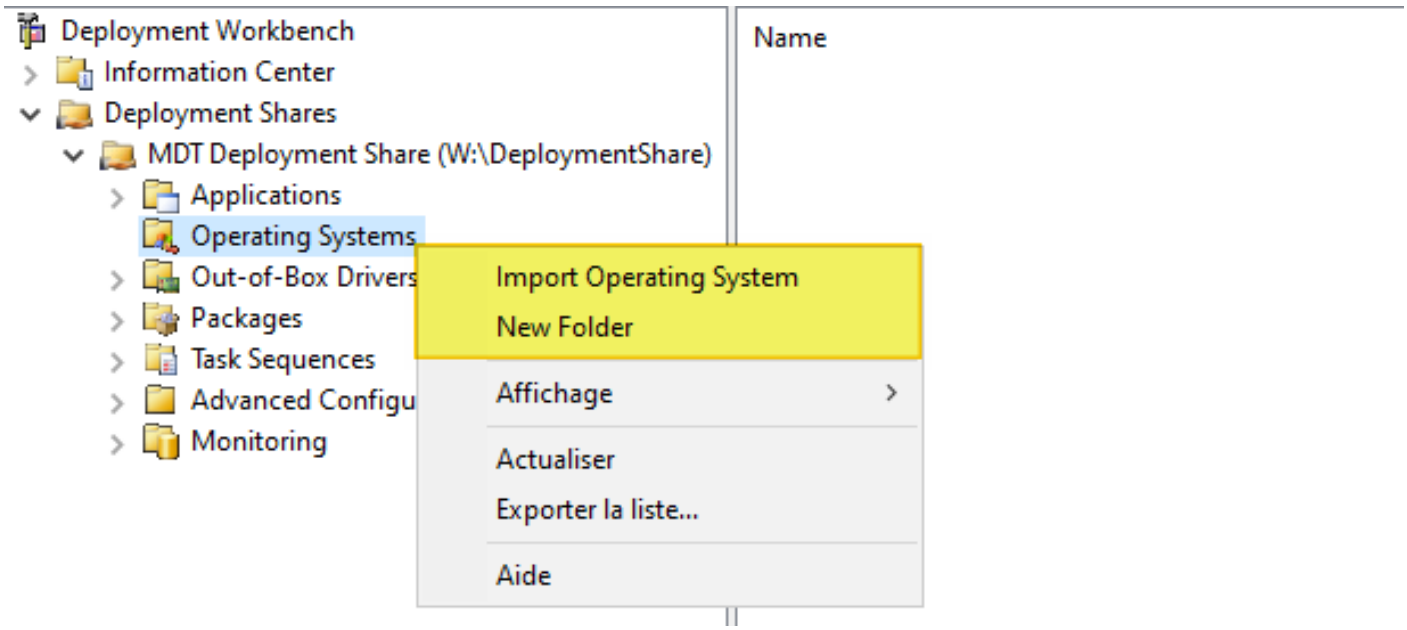
Il faut ensuite procéder à la création de l'utilisateur MDT, à l'aide de ce scrypt powershell, ajuster si besoin le nom du service et le mot de passe.

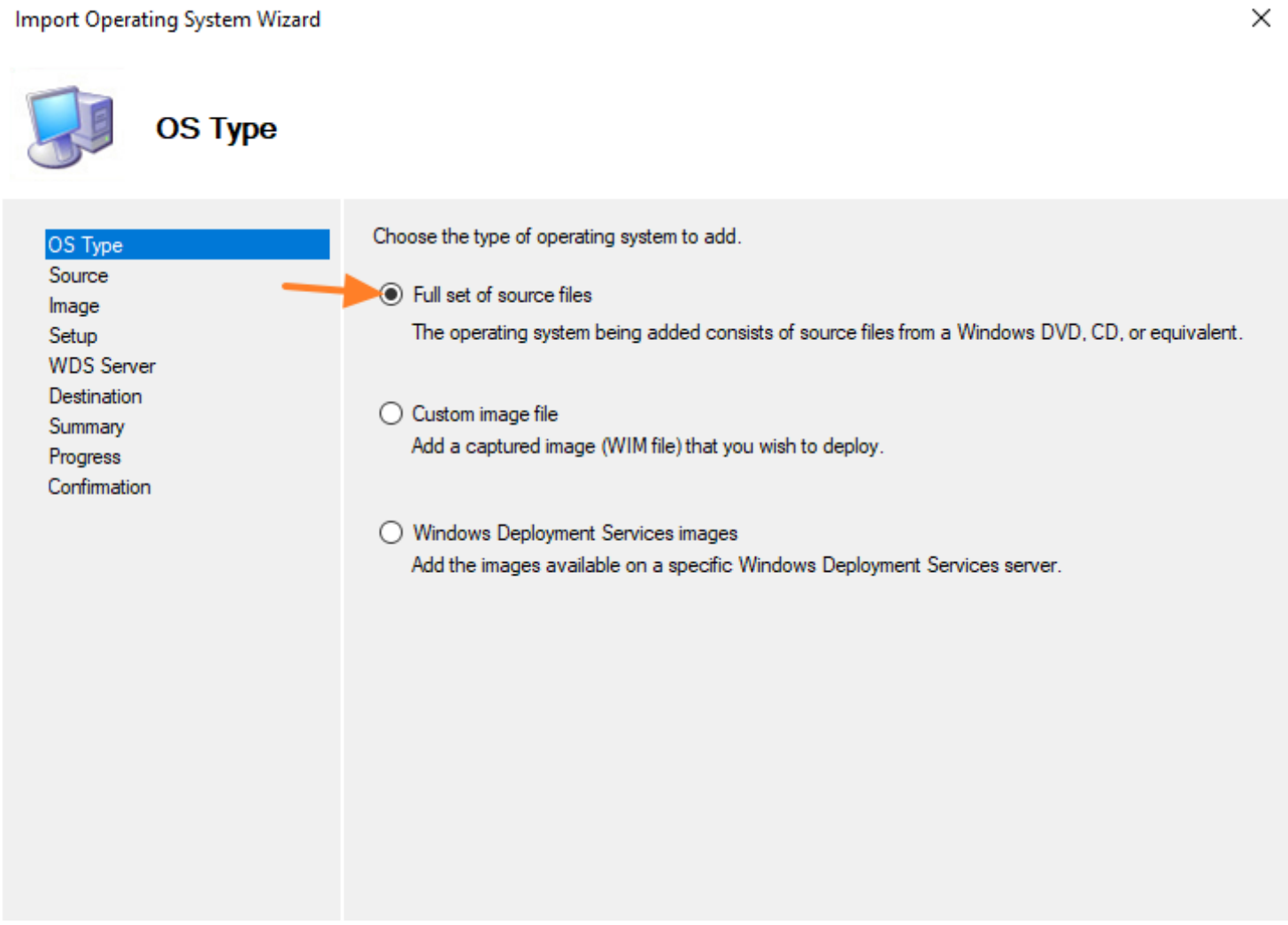
```
# Spécifier le nom et le mot de passe du compte de service
$ServiceAccountName = "Service_MDT"
$ServiceAccountPassword = ConvertTo-SecureString "P@ssword123!" -AsPlainText -Force

# 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
$MDTSharePath = "\\$env:COMPUTERNAME\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
```

Verifier si l'utilisateur a bien été créé.

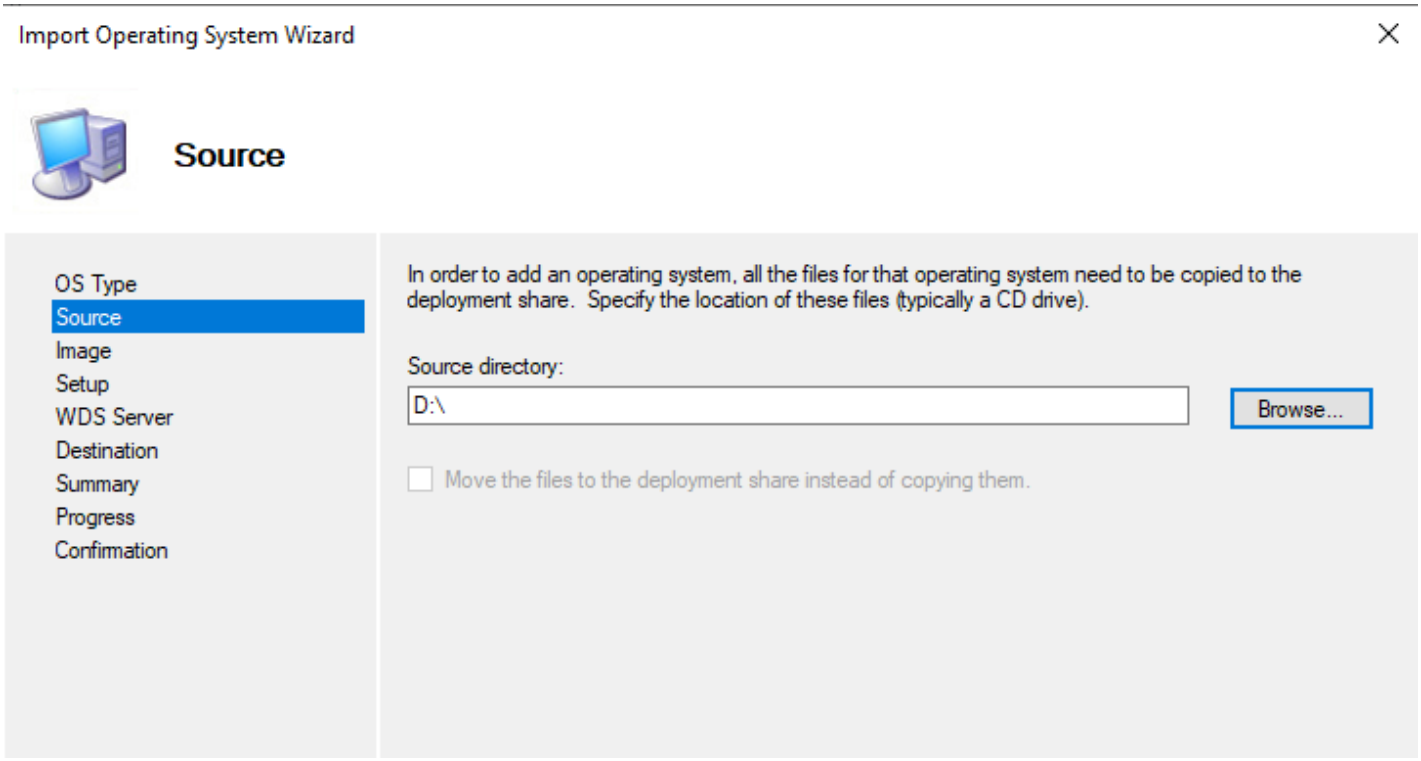


Pour importer l'image de Winwods 11 dans MDT, voici comment procéder :

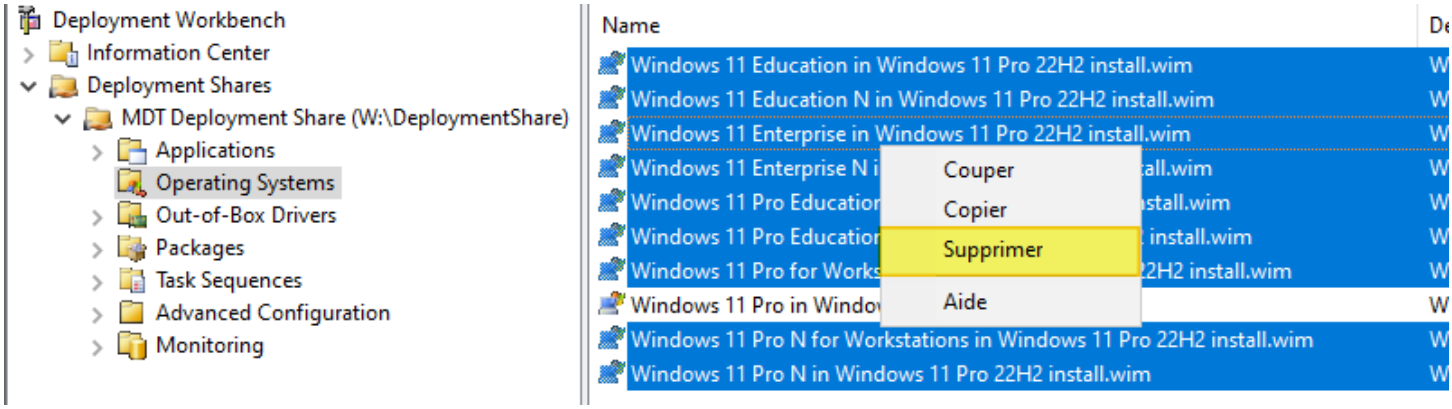




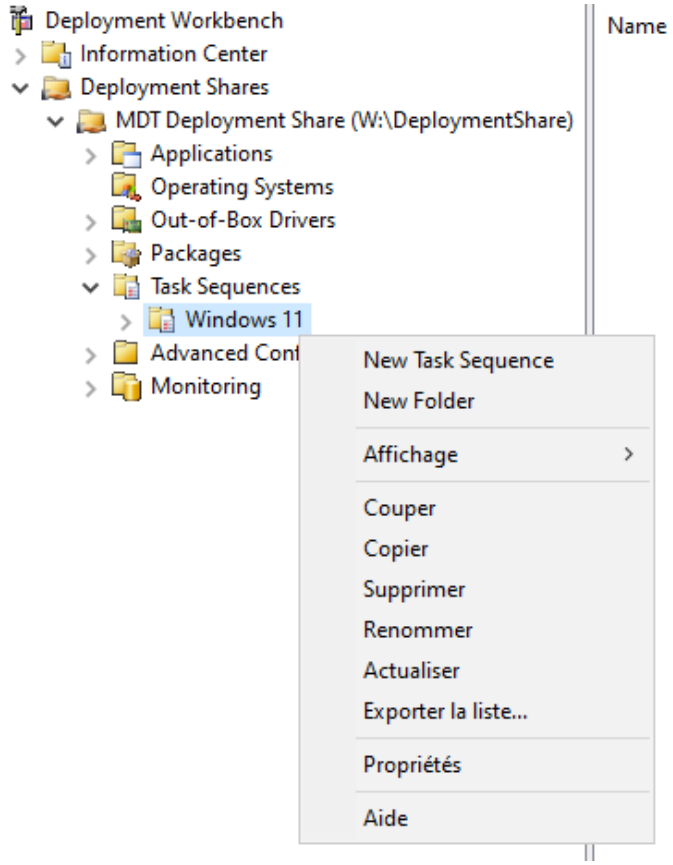
Selectionner le lecteur E, où il y a le fichier d'installation de Windows 11, et nommer simplement "Windows 11 23H2".



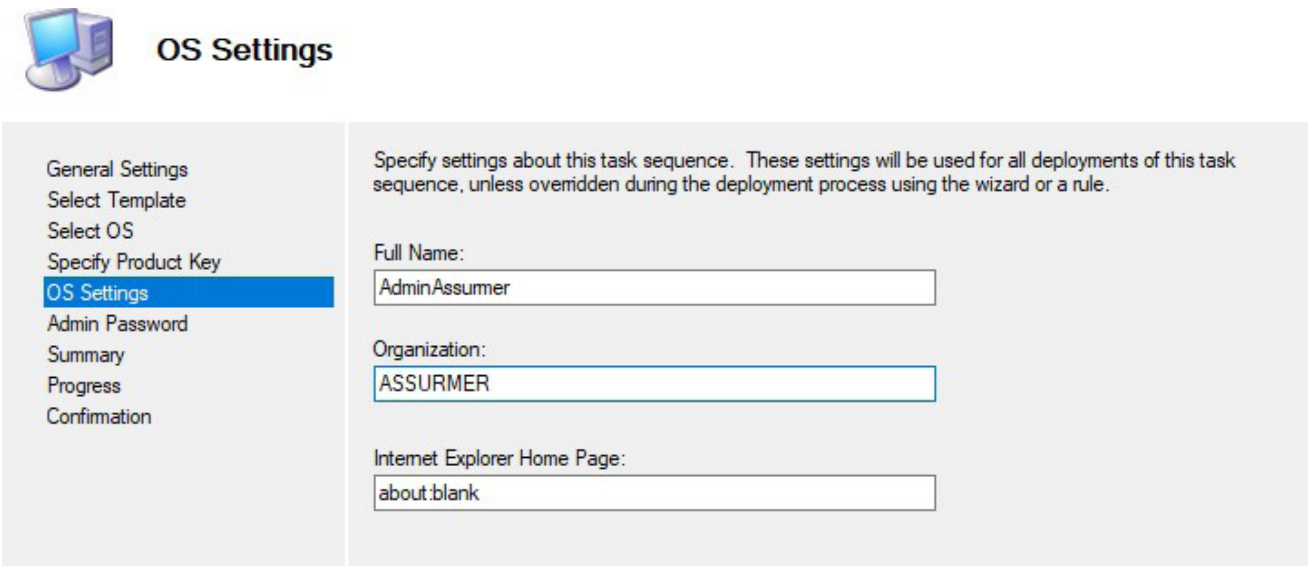
Après l'installation, aller dans Operating system et ne garder que Windows 11 Pro, supprimer le reste.



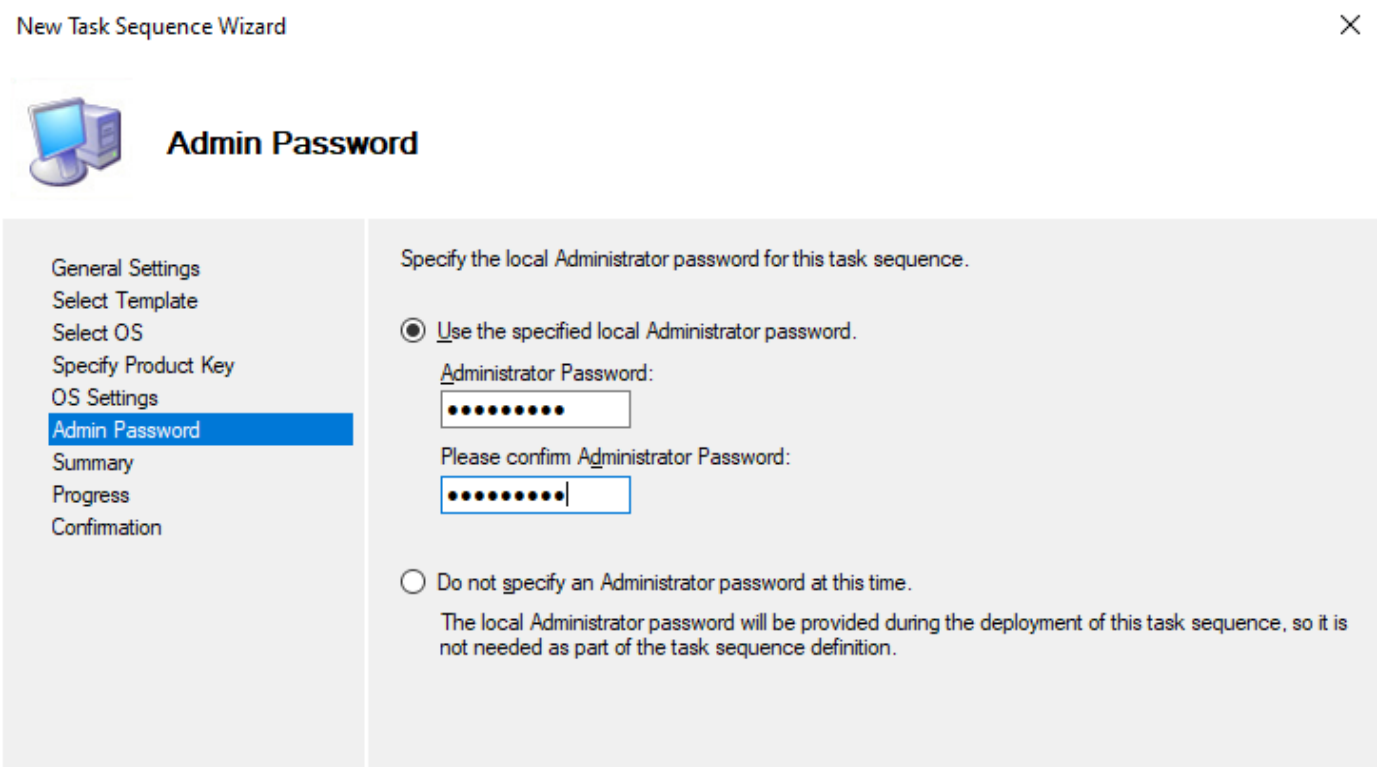
Faire une nouvelle sequence de tâche, aller dans task sequences et faire un clic droit "New Task sequence"



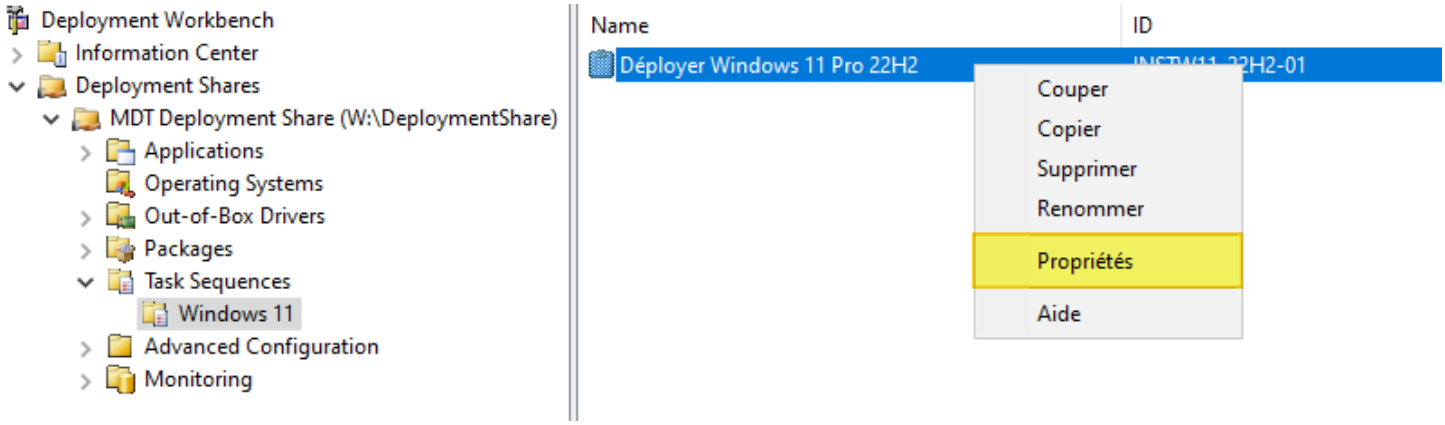
Renseigner par la suite un ID "INST-W1123H2" et le nommer "Deploiement Windows 11 23H2", au choix suivant séléctionner standard Client task sequence, et dans select OS, choisir tout simplement l'image importée de Windows 11.
Par la suite ne pas renseigner de clé de produit, et remplir OS Settings de la manière suivante:



Choisir un mot de passe robuste.



L'installation terminée, il faut éditer la tâche, aller sur Windows 11 et clic droit Propriétés.



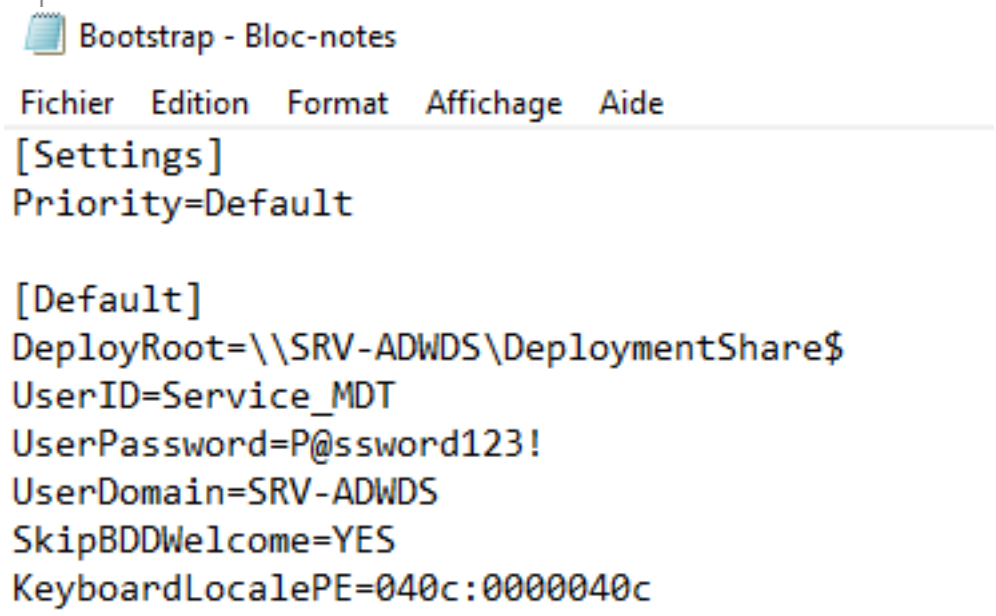
Cliquer sur State Restore et sur Windows Update, l'activer.

Actuellement, MDT rencontre plusieurs problématique, il est primordial de se renseigner sur les solutions disponibles afin de résoudre les eventuels bugs. La meilleure source d'information reste internet, au travers d'autres tutoriels de dépannage ou bien la documentation Microsoft. Pensez à tenir les logiciels à jour pour ne pas rater de correctifs.

Configurer les deux fichier bootstrap.ini et le CustomSettings.ini.
Pour cela, faire un clic droit sur le Deployment Share, propriétés puis cliquer sur l'onglet "Rules", et modifier "CustomSettings.ini" comme ceci :

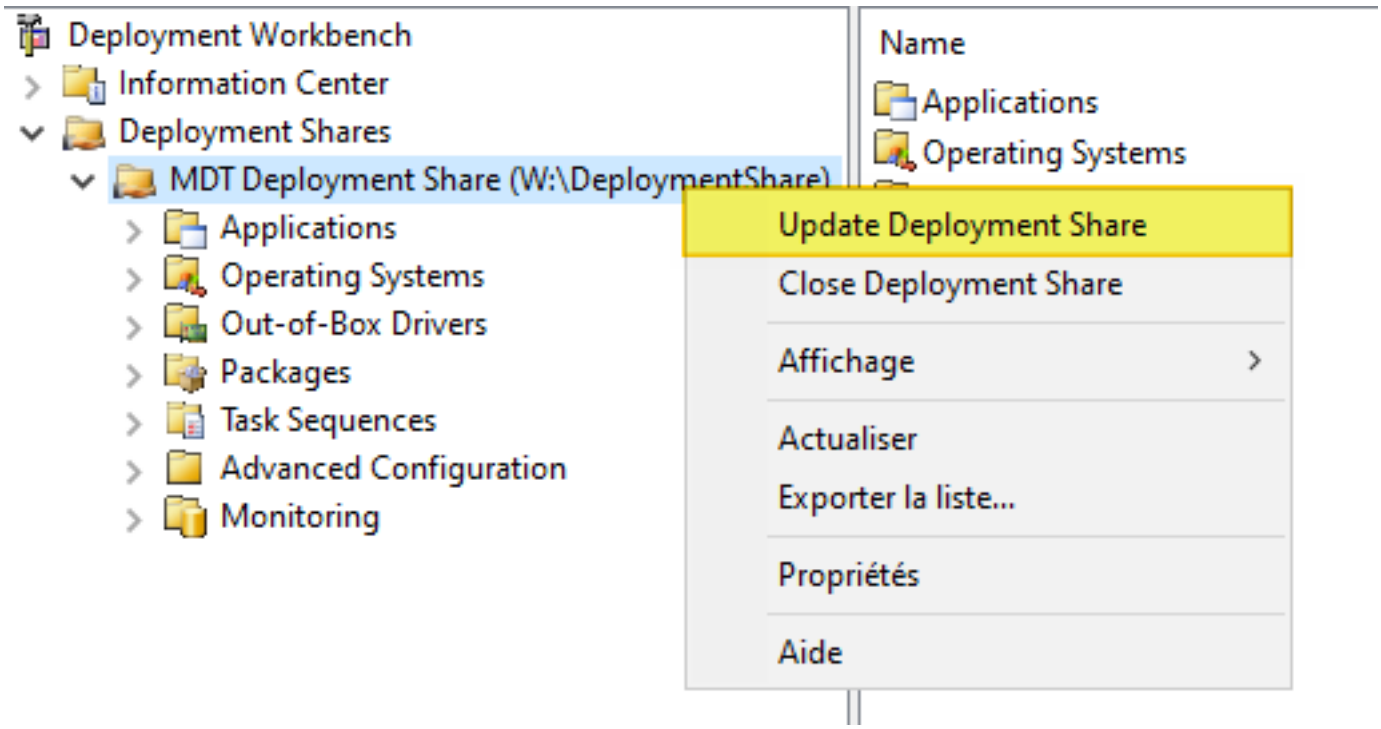
```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
OSInstall=Y
SkipCapture=NO
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=NO
SkipBitLocker=NO

_SMSTSORGNAME=Assurmer

TimeZone=105
TimeZoneName=Romance Standard Time
```

Cliquer sur le bouton "Edit Bootstrap.ini" pour editer Bootstrap :

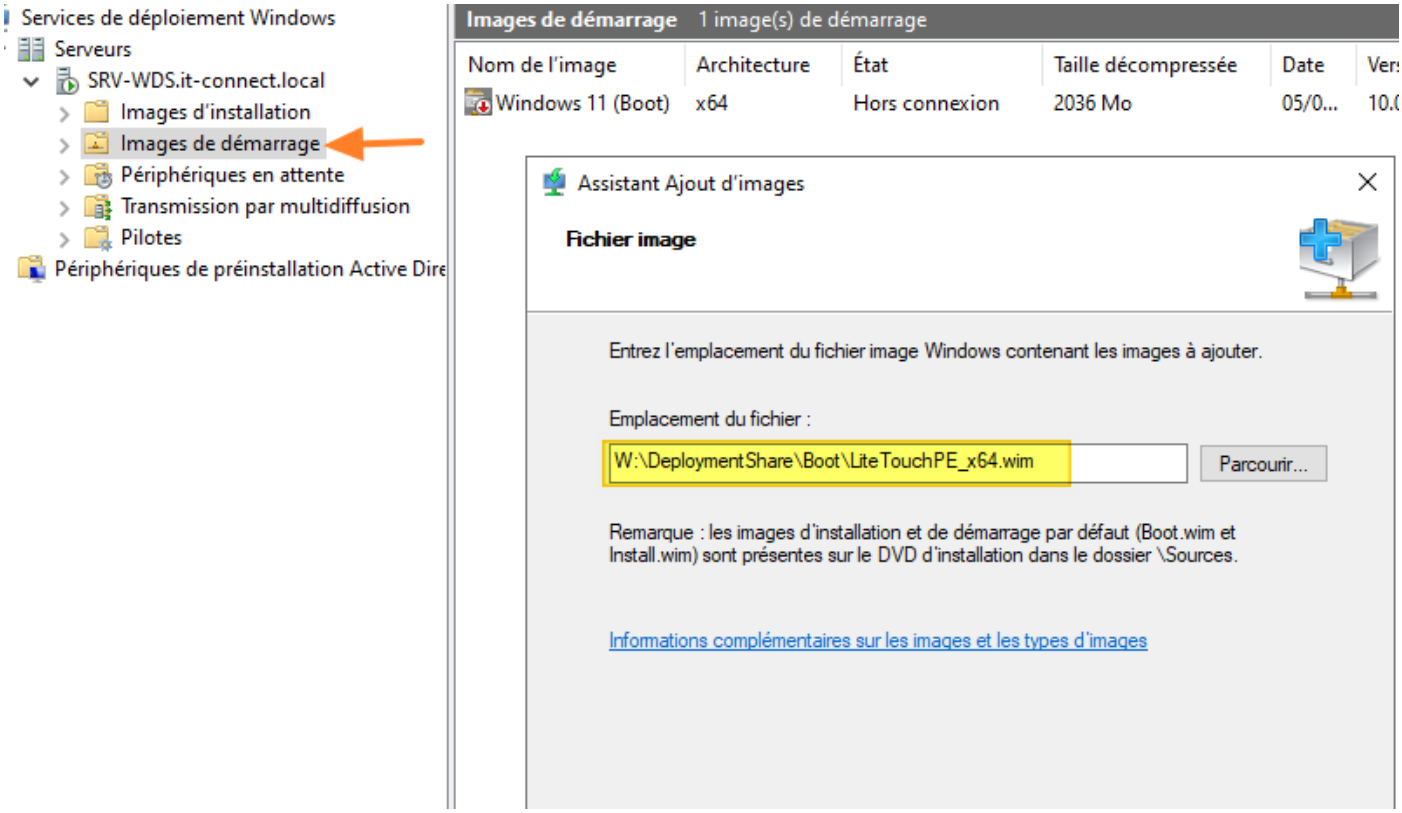


Dans l'onglet "Général" nous allons décocher l'option "Platform Supported" > x86, nous ne voulons que l'option x64 pour des raisons de compatibilité.

Enfin, nous allons devoir générer l'image Lite Touch et l'importer dans WDS.



Conserver les choix par défauts et poursuivre jusqu'à la fin de l'installation.
Taper "wds" dans la recherche Windows, puis accéder à la console et charger Lite TouchPE en nouvelle image de démarrage.



BONNES PRATIQUES & INSTRUCTIONS AUX UTILISATEURS

Communication avec les utilisateurs

Une fois les machines prêtes, nous enverrons ce mail aux utilisateurs :

Mail
Objet : a l'attention des collaborateurs Assurmer

>
Dans le cadre de nos projets concernant les JO 2024, vous êtes de ceux qui recevront un matériel adapté à vos déplacements.Vous serez invités à venir les chercher dans les locaux en date du xx/xx/xx.
Vous seront communiqué très bientôt, le mot de passe de vos sessions respectives, par sms, à la réception de votre matériel. Vous serez invités à venir les chercher dans les locaux en date du xx/xx/xx.

Ce mot de passe robuste respecte les recommandations de la CNIL et assure la sécurité des informations contenues dans votre ordinateur. Les événements à venir et la recrudescence des attaques informatique nécessite de renforcer les accès, via l'utilisation de mots de passe forts et d'une authentification à deux facteurs.
D'autre part, vous pourrez choisir, si vous le désirez, de modifier ce mot de passe. Nous vous communiqueront le lien de la CNIL à ce sujet, afin que vous puissiez trouver un mot de passe à la fois conforme et adapté à vous même.
Nous vous mettrons à disposition un outil de double authentification obligatoire pour valider la connexion à vos comptes
Vous aurez également un VPN, avec vos propres identifiants, afin de vous permettre de sécuriser vos connexions et d’accéder aux serveurs d’Assurmer.
Un Gestionnaire de mot de passe sera mis à disposition, afin de vous aider à exploiter votre ordinateurs et les différents identifiants.

D'autre part, nous vous demanderons de nous répondre afin de savoir si vous désirez avoir une souris dédié (et un pavé numérique).

Notre équipe se tient, bien évidemment, à votre disposition pour répondre à toutes vos questions.