Projet collaboratif – GMSI A 2020/2022

Inventer l'école de demain

Groupe 1 composé de :

LEFEUVRE Dylan

PATIN Tom

CHARLES-ROLANDO Thibaud

DOS SANTOS Léo

Table des matières

A. Récapitulatif 3
B. Analyse du besoin client 3
C. Planning de réalisation (Gantt sur MS Project) 4
D. Suivi du projet (Organisation de travail sur Trello) 4
E. Masteriser pour performer (WDS & MDT) 5
I. WDS 6
II. MDT 6
F. Mises à jour (WSUS) 7
G. Sécurisation du parc (PCA/PRA, Firewall, VPN) 8
I. Fournisseurs et équipement 8
II. Le PCA / PRA 10
III. Le Firewall 10
IV. Le VPN 10
H. Scripting du parc (Script d'automatisation avec PowerShell) 11
I. Centraliser le réseau (Solution interne et externe) 12
I. Schéma réseau 12
II. Centre SNTS 13
III. Différents sites (écoles) 14
IV. Services extérieurs 14
J. Devis 15
K. Annexes 16
I. Installation et configuration du WDS & MDT 16
1. Installation et configuration du WDS 16
2. Installation et configuration du MDT 27
II. Installation et configuration du WSUS 50
III. Configuration du Scripting avancé 63

A. Récapitulatif

Lors de notre dernier point en réunion, nos missions étaient de :

- Mise en place et configuration de nouveaux serveurs Windows & Linux
- Création et gestion de comptes
- Automatisation de certaines tâches
- Mise à jour logicielle et matérielle des serveurs
- Solution de gestion à long terme

B. Analyse du besoin client

Constat : A ce jour, les serveurs sont dans les écoles et il y en a actuellement 7. Il est donc nécessaire de proposer une solution propre et efficace sur une longue durée.

Les besoins exprimés par le client sont les suivants :

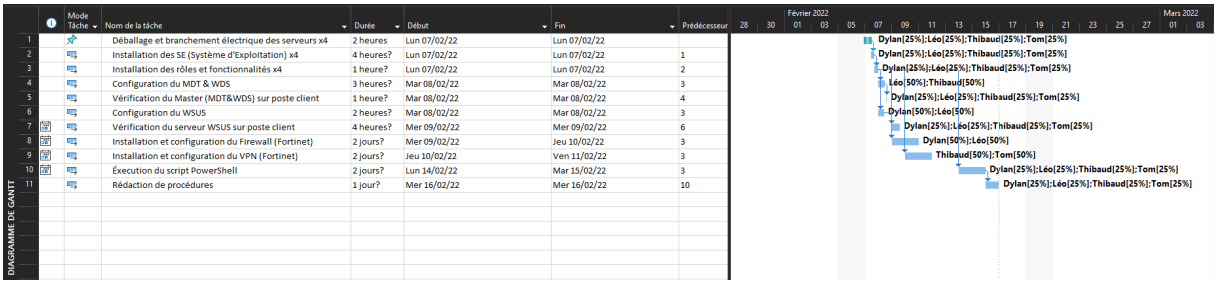
- Obtenir un master fonctionnel pour les ordinateurs
- Maintenir et gérer les mises à jour disponibles
- Sécuriser le parc informatique à l'aide de pare-feu, VPN, PCA/PRA
- Automatiser plusieurs tâches avec PowerShell à savoir la création d'utilisateurs et installation et configuration de DFS/DFSR
- Centraliser le réseau au local du SNTS avec une refonte de l'architecture réseau

Ayant eu un budget n'excédant pas 350 000 €, notre solution a eu un coût d'environ 254 000 € HT.

Il nous reste actuellement environ 96 000 € HT pour le prochain projet au cas où nous aurions besoin d'acheter du matériel supplémentaire.

C. Planning de réalisation (Gantt sur MS Project)

Le Project est disponible dans les éléments joints au rendu du projet collaboratif par le nom : (**Planning de réalisation PC3.mpp**) dans le dossier ***Projet Collaboratif 3 - Liens et documentation*.**



	Mode Tâche	Nom de la tâche	Durée	Début	Fin	Prédécesseur
1		Déballage et branchement électrique des serveurs x4	2 heures	Lun 07/02/22	Lun 07/02/22	
2		Installation des SE (Système d'Exploitation) x4	4 heures?	Lun 07/02/22	Lun 07/02/22	1
3		Installation des rôles et fonctionnalités x4	1 heure?	Lun 07/02/22	Lun 07/02/22	2
4		Configuration du MDT & WDS	3 heures?	Mar 08/02/22	Mar 08/02/22	3
5		Vérification du Master (MDT&WDS) sur poste client	1 heure?	Mar 08/02/22	Mar 08/02/22	4
6		Configuration du WSUS	2 heures?	Mar 08/02/22	Mar 08/02/22	3
7		Vérification du serveur WSUS sur poste client	4 heures?	Mer 09/02/22	Mer 09/02/22	6
8		Installation et configuration du Firewall (Fortinet)	2 jours?	Mer 09/02/22	Jeu 10/02/22	3
9		Installation et configuration du VPN (Fortinet)	2 jours?	Jeu 10/02/22	Ven 11/02/22	3
10		Éxecution du script PowerShell	2 jours?	Lun 14/02/22	Mar 15/02/22	3
11		Rédaction de procédures	1 jour?	Mer 16/02/22	Mer 16/02/22	10

DIAGRAMME DE GANTT

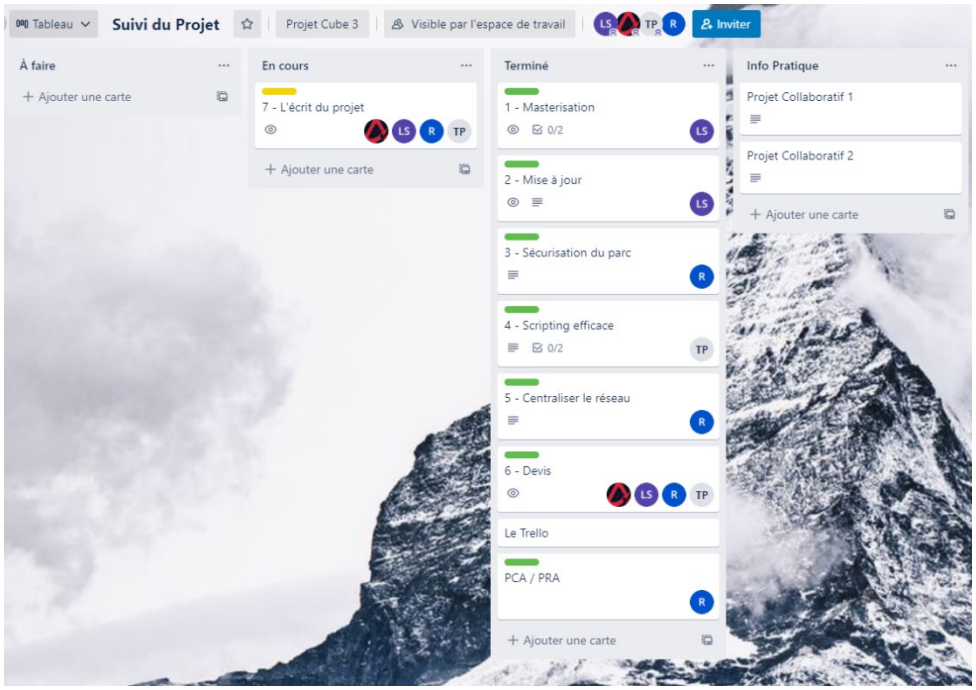
Février 2022 — Mars 2022

Document : Capture d'écran de notre planning de réalisation sur MS Project

D. Suivi du projet (Organisation de travail sur Trello)

Afin d'être organisé dans les meilleures conditions pour ce projet, nous avons décidé d'avoir un tableau collectif où est renseigné l'avancement des différentes tâches de ce projet.

Nous avons jugé utile de vous en faire part afin que vous ayez une idée de notre organisation.



Document : Capture d'écran de notre tableau sur Trello

(Les captures d'écrans de notre Trello sont dans le dossier ***Projet Collaboratif 3 - Liens et documentation*.**)

E. Masteriser pour performer (WDS & MDT)

La masterisation est le déploiement d'un master sur un parc informatique.

Le master permet la personnalisation rapide et optimiser d'un poste en fonction des demandes clientes, nous pouvons par exemple délimiter des accès, ajouter ou supprimer des logiciels ou tout simplement modifier les paramètres de base de Windows.

Un master peut être créer et déployer grâce à différentes plateformes comme :

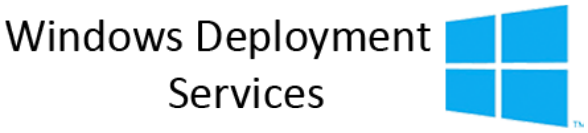
- Windows Deployment Services + Microsoft Deployment Toolkit (WDS + MDT)
- System Center Configuration Manager (SCCM)
- Intune

Dans notre cas nous utilisons Windows Deployment Services et Microsoft Deployment Toolkit.

I. WDS

Windows Deployment Services ou WDS est un rôle sur Windows Server qui permet de déployer un système d'exploitation Windows mais il est désormais possible de déployer une image WIM via le réseau (PXE ou Preboot Execution Environment).

Nous pouvons donc installer notre propre image Windows avec des logiciels préinstallés et des paramétrages préconfigurés grâce à WDS.



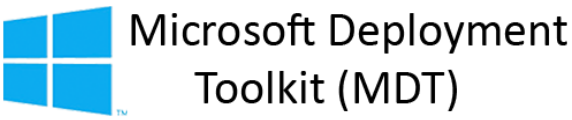
Mais WDS ne suffira pas pour le déploiement de ou des master(s), il va aussi falloir utiliser MDT pour la création des images et ainsi utiliser les 2 services en les faisant communiquer.

II. MDT

Microsoft Deployment Toolkit ou MDT est une solution, un logiciel pour automatiser les créations et déploiements de master.

Il va nous servir à créer les images, c'est grâce à MDT que l'on va pouvoir personnaliser nos masters à l'aide de logiciels ou de services.

MDT a tout de même besoin de 2 prérequis sur le serveur ou il sera installé, il aura besoin de Windows ADK et de PE Windows pour qu'il soit fonctionnel.



Pour ce projet MDT va nous être utile pour faire un master qui nous permettra de configurer tous les postes fixes des salles informatiques ainsi que les postes portables des enseignants et de la direction.

F. Mises à jour (WSUS)

Le service WSUS, autrement appelé Windows Server Updates Services permet de distribuer les nouvelles mises à jour des produits Microsoft.

Celui-ci sert à être exécuté sur les différents ordinateurs possédant un système d'exploitation tel que Windows tout en étant compris au sein d'un parc informatique.

Lorsque ce service est installé sur un Windows Server, il peut devenir un serveur de mises à jour local ou bien encore un proxy de mises à jour.

Il peut également récupérer les mises à jour anciennes comme récentes en les téléchargeant auprès de Windows Update, les stocker et ainsi de les distribuer.

Pour notre part, ce service va pouvoir mettre à jour les logiciels Microsoft, le système d'exploitation Windows et ainsi celles concernant la sécurité de poste informatique.

G. Sécurisation du parc (PCA/PRA, Firewall, VPN)

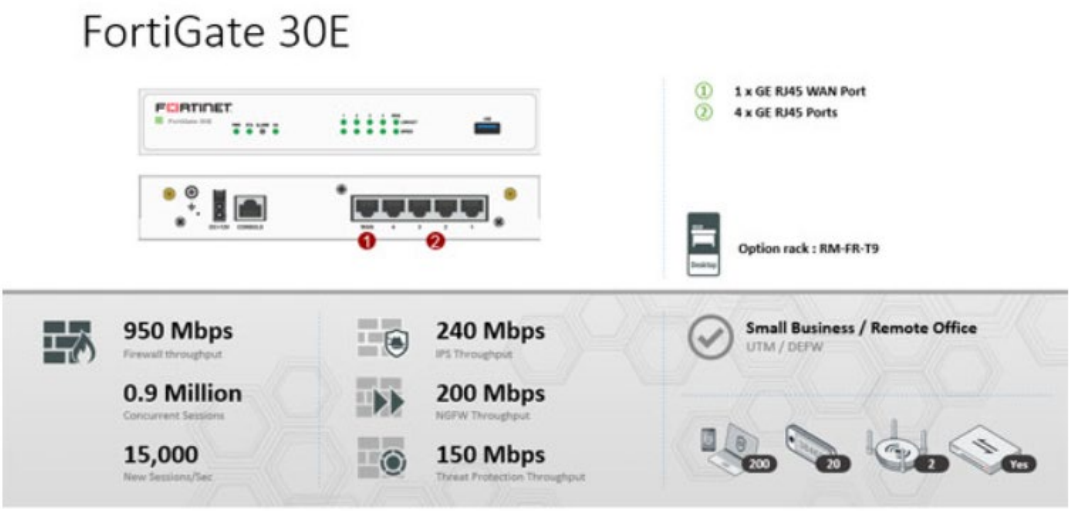
I. Fournisseurs et équipement

Nous avons décidé de choisir Fortinet comme solution Firewall et VPN.

Pour nos besoins nous partons sur 2 équipements par site afin d'avoir une redondance en permanence.

Notre choix s'est porté sur l'équipement FortiGate 30E.

Cet équipement est idéal pour nos architectures de petites/moyennes tailles.



Document : Caractéristique de l'équipement FortiGate 30E

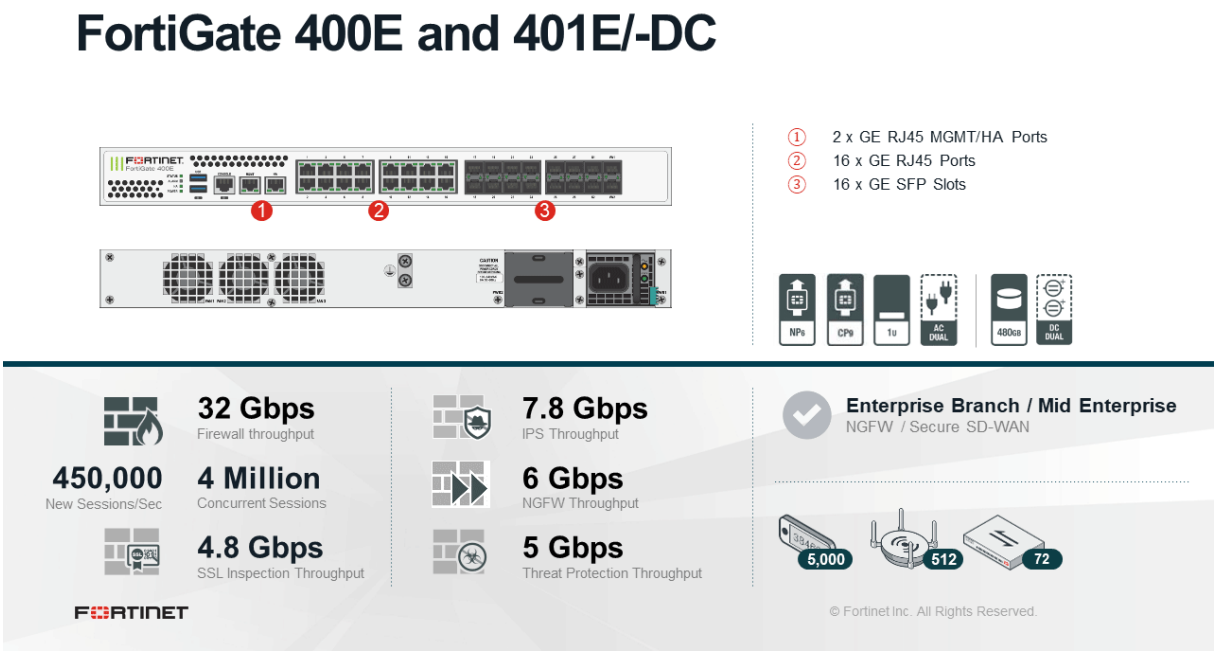
Il permet un maximum de 900 000 connexions maximum au Firewall et 15 000 nouvelles connexions par secondes.

Il nous permet également de créer des connexions IPSEC entre différents équipements Fortinet jusqu'à 80 tunnels IPSEC maximum.

Le choix de Fortinet nous permet également d'avoir notre Firewall et notre VPN sur le même équipement, ainsi ils seront configurables sur la même interface, nous faisant gagner un temps considérable et permettant une utilisation plus facile.

Pour plus d'information sur le produit je vous invite à vous rendre vers :
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_30E.pdf

Pour **le SNTS** notre choix s'est porté sur un FortiGate **400E**.



Document : Caractéristiques de l'équipement FortiGate 400E

Il permet 4 millions de connexions maximum au Firewall et 450 000 nouvelles connexions par secondes.

Il nous permet également de créer des connexions IPSEC entre différents équipements Fortinet jusqu'à 2000 tunnels IPSEC maximum.

Il autorise 5000 SSL.

Pour plus d'informations sur le produit je vous invite à vous rendre vers : https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf

II. Le PCA / PRA

Nous avons à la mairie de Castillon un emplacement de 12U qui nous est réservé.

Nous avons décidé d'utiliser 2 de ces unités afin de créer un cluster de deux nœuds identiques à celui que nous avons au SNTS et qui sera relié également chez OVH afin de pouvoir faire du fail over si notre SNTS devait ne plus fonctionner brutalement.

Il sera, si nous avons la possibilité, branché électriquement sur un onduleur.

III. Le Firewall

Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Nous devons créer différentes zones selon l'utilisation de nos équipements (ordinateurs fixe, imprimantes, ordinateur portable, serveurs, etc…) afin de créer différentes règles et autorisations réseau / ports.

IV. Le VPN

Il existe deux types de connexions VPN :

De site à site, la connexion IPSEC, établi entre deux points donnés une connexion cryptée.

Le but étant d'établir une connexion avec une clé crypté que seuls les deux points connaissent, ainsi n'importe quelle donnée envoyée est crypté avec une clé spécifique et décryptée avec cette même clé lors de l'arrivé à l'autre point.

Le VPN SSL, il permet de simuler une connexion à un réseau de tel façon à ce que le réseau pense que l'équipement se situe en son sein.

Il permet aux utilisateurs d'établir une connexion sécurisée au réseau intranet depuis n'importe quel ordinateur possédant un navigateur web ou le client adéquat.

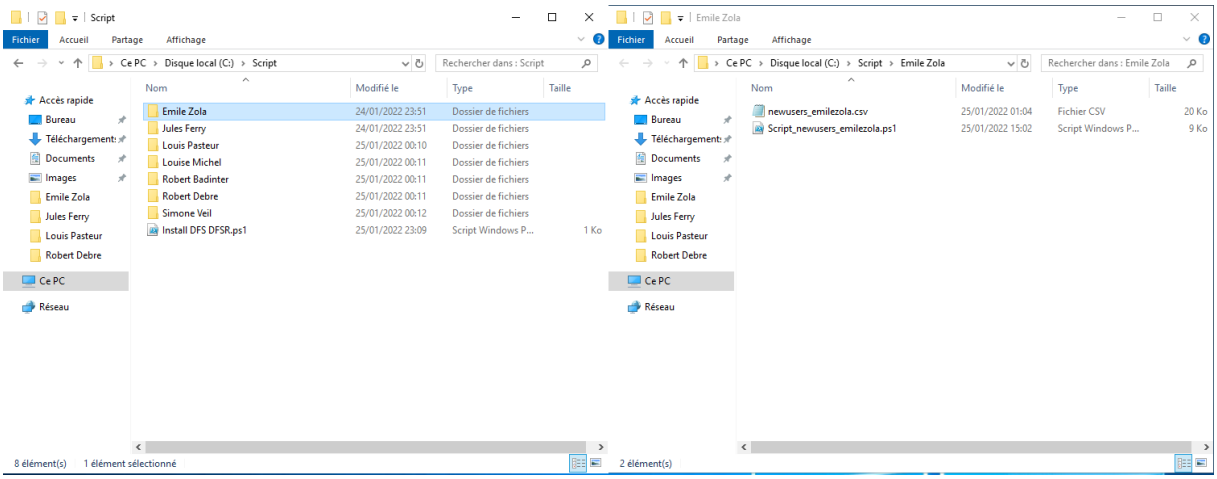
Dans notre cas il sera utilisé pour les professeurs afin d'utiliser les ressources interne tel que leurs espaces de stockage interne.

H. Scripting du parc (Script d'automatisation avec PowerShell)

Un premier script avait été créé pour automatiser la création d'utilisateurs mais celui-ci ne faisait que les créer et les déplaçait dans les unités d'organisations et groupes de sécurités correspondant.

Ce script a été repris et amélioré, la création d'utilisateurs et de dossiers personnels ont été gardé mais pour les unités d'organisations et les groupes de sécurités, ils sont directement créés à partir du fichier CSV.
Le script va d'abord vérifier si les UO ou groupes existent puis va décider de les créer. Une fois ce processus fait, il va déplacer les utilisateurs dans les bonnes UO et bons groupes.

Une fonction a également été rajoutée, celle-ci consiste à remplacer les différents accents dans les prénoms ou nom par la lettre sans accent afin d'éviter tout problèmes de caractères.



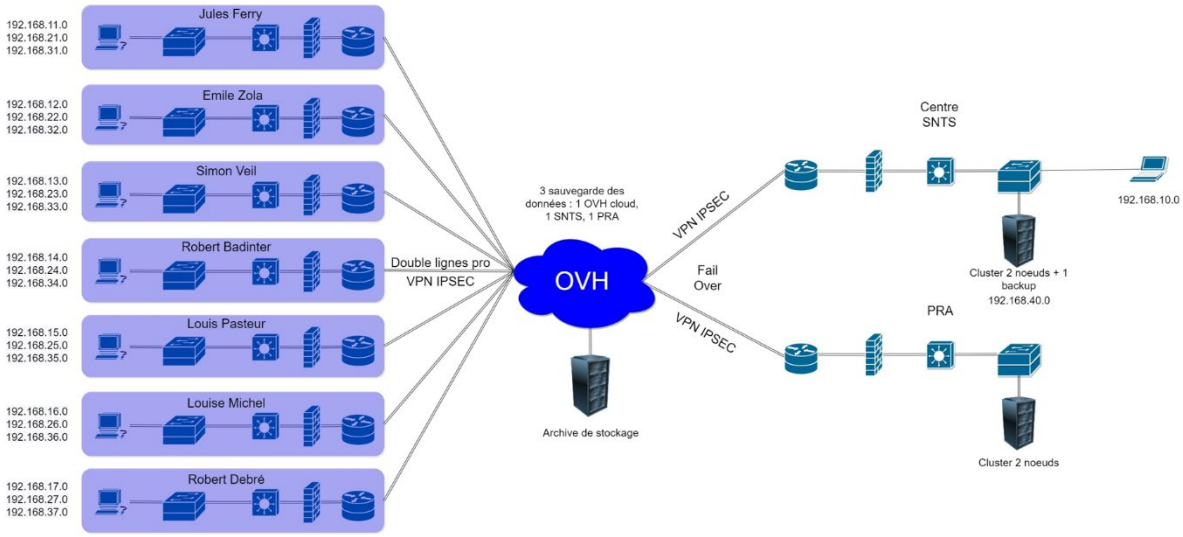
Document : Capture d'écran des différents scripts par école

Comme pour la première version du script, il est divisé en différentes parties.

- La première concerne l'importation du fichier CSV contenant les informations des utilisateurs, les différentes variables faites avec le fichier CSV et la fonction pour les accents sur les prénoms.
- La deuxième est la création des utilisateurs s'ils n'existent pas.
- La troisième est la création des unités d'organisation des écoles si elles n'existent pas et le déplacement des utilisateurs dans ces UO.
- La quatrième est la création des unités d'organisation des classes si elles n'existent pas et le déplacement des utilisateurs dans ces UO.
- La cinquième est la création des groupes de sécurité s'ils n'existent pas et l'ajout de utilisateurs dans ces groupes.
- La dernière partie est la création des répertoires personnels monté sur leur session sous la lettre « P: ».

I. Centraliser le réseau (Solution interne et externe)

I. Schéma réseau



Document : Schéma réseau de notre nouvelle infrastructure

II. Centre SNTS

Nous avons décidé de centraliser les serveurs au centre SNTS en formant un cluster de deux nœuds sur avec nos serveurs tout en laissant un dernier en backup si l'un de nos nœuds se retrouve hors service.

Nous avons choisi pour prendre deux abonnements professionnels chez deux fournisseurs différents afin de palier à une défaillance d'une des deux lignes.

Nous avons choisi un Firewall « Fortinet » que nous placerons au centre SNTS afin de superviser les accès et ports disponible pour notre réseau.

Nous avons également choisi un VPN « Fortinet » qui nous relieras en IPSEC directement chez OVH qui fera ensuite le lien vers nos différents sites

Nous utiliserons aussi leurs VPN SSL afin de permettre aux professeurs, entre autres, de se connecter au réseau de leurs écoles et ainsi avoir accès aux ressources du réseau.

Concernant le PCA nous avons redondés les switches, le firewall et les routeurs afin de palier à une défaillance qui immobiliserais notre réseau.

Chaque serveur sera en production dans une salle différente et ces serveurs seront branché sur des onduleurs.

Nous avons décidé d'isoler notre réseau de serveurs que nous avons placé en 192.168.40.0, s'il devait être décidé par la suite de rajouter des serveurs sur d'autres sites nous utiliserions ce même VLAN en 192.168.4x.0, le X étant le numéro dédié à l'école.

Cette solution n'est certes pas infinie car nous pouvons utiliser ce type d'adressage pour seulement 10 sites, ce qui nous offre tout de même la possibilité d'inclure 2 autres sites dans notre plan d'adressage.

III. Différents sites (écoles)

Comme annoncé plus haut ces sites seront également redondés avec deux abonnements professionnels de deux fournisseurs différents pour, encore une fois, palier à la défaillance d'une des deux liaisons.

Il y aura également un Firewall, et un VPN IPSEC relié à OVH afin de faire la commutation avec notre centre SNTS et notre PRA si besoin.

Nous avons également redondé les équipements réseaux allant de la couche 1 à la couche 3 du modèle OSI (Physique, Liaison de données, Réseau).

Concernant l'adressage réseau il se constitue de la sorte :

- Un VLAN pour les élèves (192.168.1x.0/24)

- Un VLAN pour les professeurs (192.168.2x.0/24)

- Un VLAN pour l'Administration/Direction (192.168.3x.0/24)

- Un VLAN pour l'Administration Réseau du matériel SNTS Local (192.168.40.1/24)

IV. Services extérieurs

Nous avons choisi la société OVH pour ces différents services :

-**Private network** (Cf. https://www.ovhcloud.com/fr/public-cloud/private-network/)

Il va nous permettre de relier nos différents réseaux et de les manager au mieux depuis le client OVH afin de profiter de toutes les autres fonctionnalités.

-**Sauvegarde de données dans le Cloud** (Cf. https://www.ovh.com/fr/storage-solutions/)

En plus de nous transférer les données transmises par les écoles, ils nous garderont une copie stockée sur leurs serveurs et accessible en cloud.

-**Load balancing** (Cf. https://www.ovhcloud.com/fr/public-cloud/load-balancer/)

OVH nous enverra le flux reçu par les écoles vers le SNTS et une copie DATA vers le PRA afin de garder l'aspect PRA.

-**Fail over (Cf. https://www.papercut.com/support/resources/manuals/ng-mf/common/topics/cluster-server-2012-2016.html#Create)**

En cas de perte total de notre centre SNTS il nous suffira de remonter l'incident à OVH pour qu'il transfert le flux principal vers le PRA

Leurs services proposants des choix complets et répondants à nos besoins, nous avons choisis OVH comme ressource tierce qui fera donc le lien entre nos différents sites et nous permettra aussi d'effectuer les sauvegardes de donnés dans la norme dite du 3,2,1.

J. Devis

SNTS
93 Boulevard de la Seine
Nanterre
92050
0155178000
dylan.lefeuvre@viacesi.fr

DEVIS
DEV0002

DATE
25 janv. 2022

SOLDE DÛ
EUR 304 820,46 €

ADRESSE DE FACTURATION

Projet CUBES3
93 Boulevard de la Seine
Nanterre
92050
jberton@viacesi.fr

ARTICLE	PRIX	QTTÉ	MONTANT
HP ProBook 450 G7	429,99 €	111	47 728,89 €
HP 260 G4 Desktop Mini	329,99 €	224	73 917,76 €
RAM G.Skill 8GO (2 x 4 GO) 1600MHZ CL11	38,99 €	82	3 197,18 €
Claviers & Souris filaires HP Pavillon 400	24,99 €	306	7 646,94 €
Écrans HP 22" - Full HD - IPS	89,99 €	306	27 536,94 €
Windows Server 2019 Datacenter	2 999,99 €	4	11 999,96 €
Windows 10 Professionnel	49,99 €	111	5 548,89 €
FortiGate 400E	5 049,00 €	2	10 098,00 €
FortiGate 30E	399,99 €	14	5 599,86 €
Abonnement Pro Orange Fibre	49,99 €	9	449,91 €
Abonnement Pro Bouygues Fibre	59,99 €	9	539,91 €
Switch L2	649,94 €	20	12 998,80 €
Switch L3	916,94 €	20	18 338,80 €
Lenovo ThinkSystem SR630	2 117,33 €	5	10 586,65 €
Prestation OVH	10 000,00 €	1	10 000,00 €
V7 Onduleur 1500VA à montage sur rack 2U	499,99 €	4	1 999,96 €
Western Digital 6 TB Ultrastar DC HC310 3.5" SAS	177,49 €	20	3 549,80 €
Eaton Ellipse ECO 650 USB	94,95 €	24	2 278,80 €

SOUS-TOTAL	254 017,05 €
TAXES (20%)	50 803,41 €
TOTAL	304 820,46 €
SOLDE DÛ	**EUR 304 820,46 €**

1/1

Document : Capture d'écran de notre devis matériel

K. Annexes

I. Installation et configuration du WDS & MDT

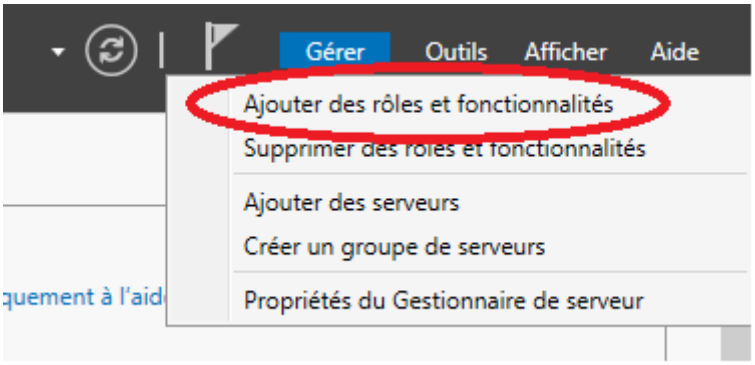
Pour la création du master il faut des prérequis sur le serveur à savoir :

- Un AD DS
- Un DHCP
- UN DNS
- Un iso Windows
- Un lecteur disque E : sur le serveur

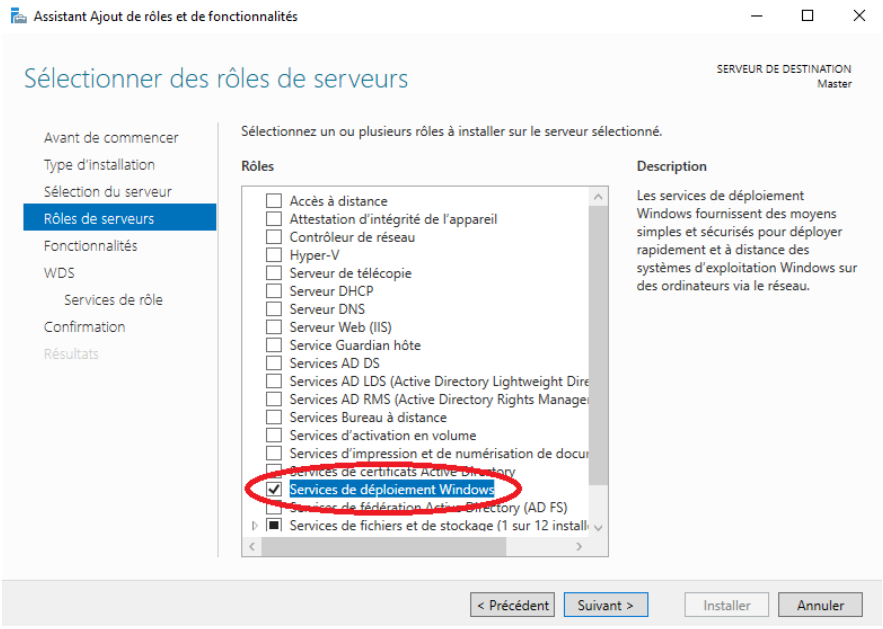
Il va falloir aussi installer le rôle WDS et MDT ainsi que les configurer.

1. Installation et configuration du WDS

➔ Allez sur le gestionnaire de serveur dans la catégorie « **Gérer** » en haut à droite, puis dans « **Ajouter des rôles et fonctionnalités** »

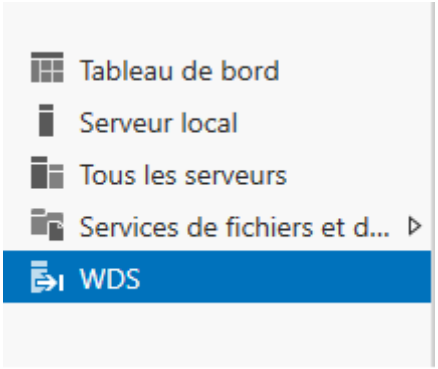


➔ Sélectionnez « **Services de déploiement Windows** »



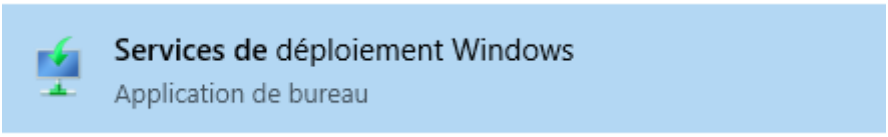
➔ Passez ensuite les étapes jusqu'à l'installation

➔ Le rôle est installé sur le serveur

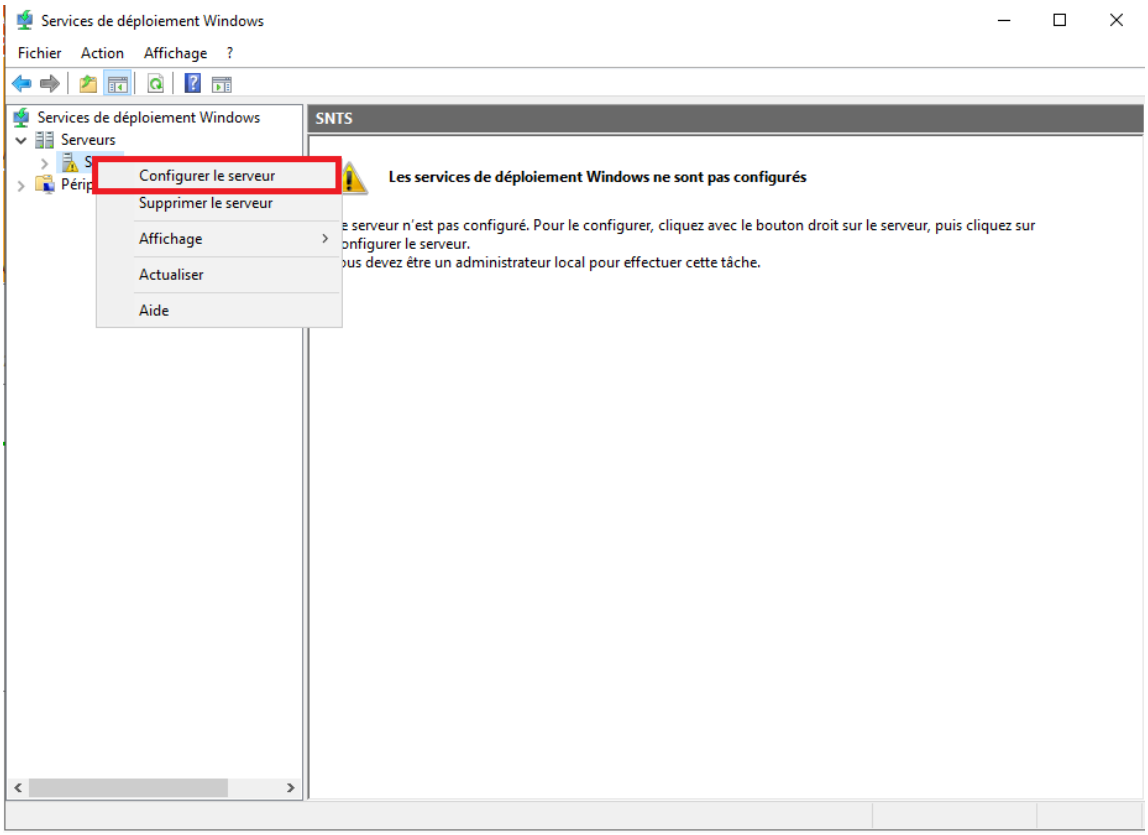


Nous allons ensuite passer à l'installation de WDS :

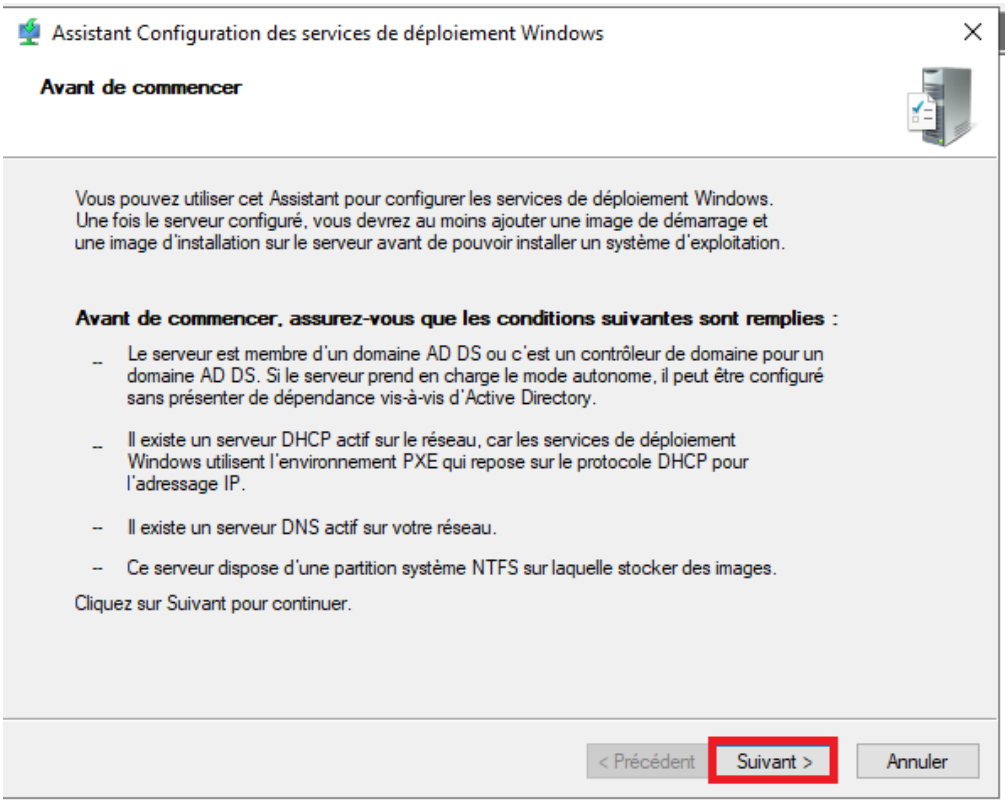
Rendez-vous sur l'application « **Services de déploiement Windows** »



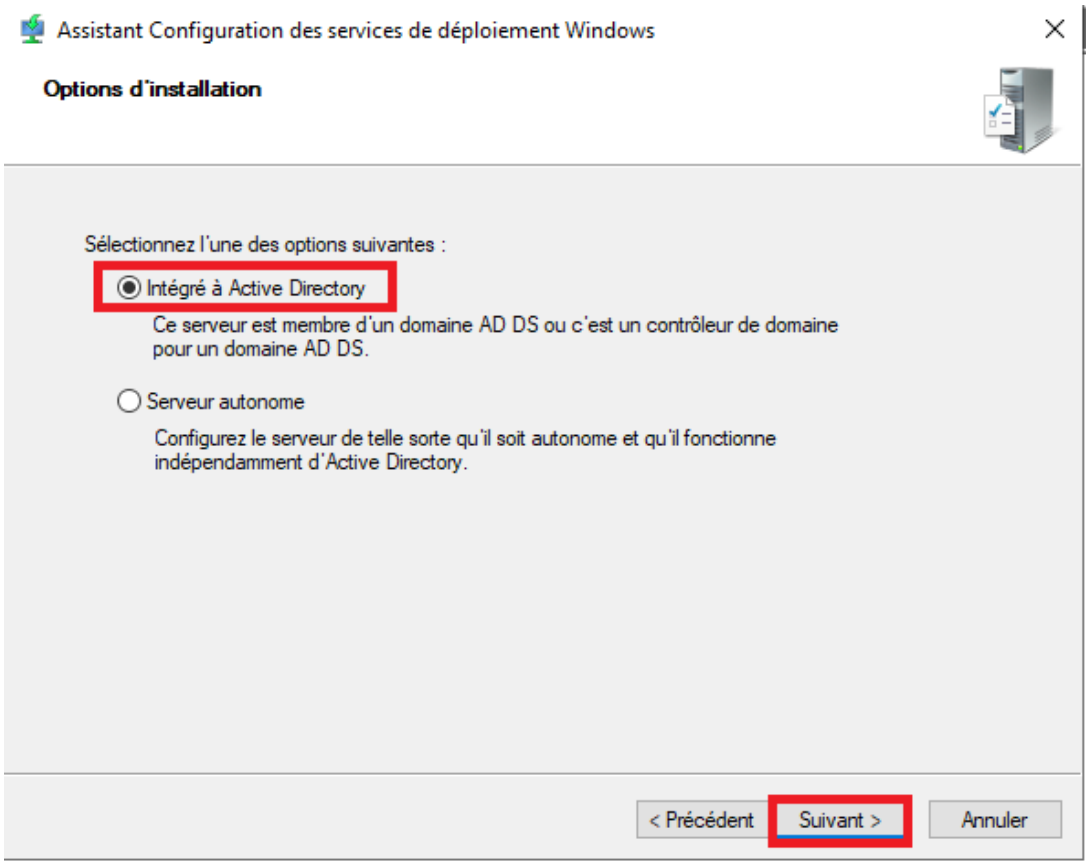
➔ Rendez-vous dans l'onglet « **Serveurs** » et faire un clic droit sur notre serveur pour faire « **Configurer le serveur** »



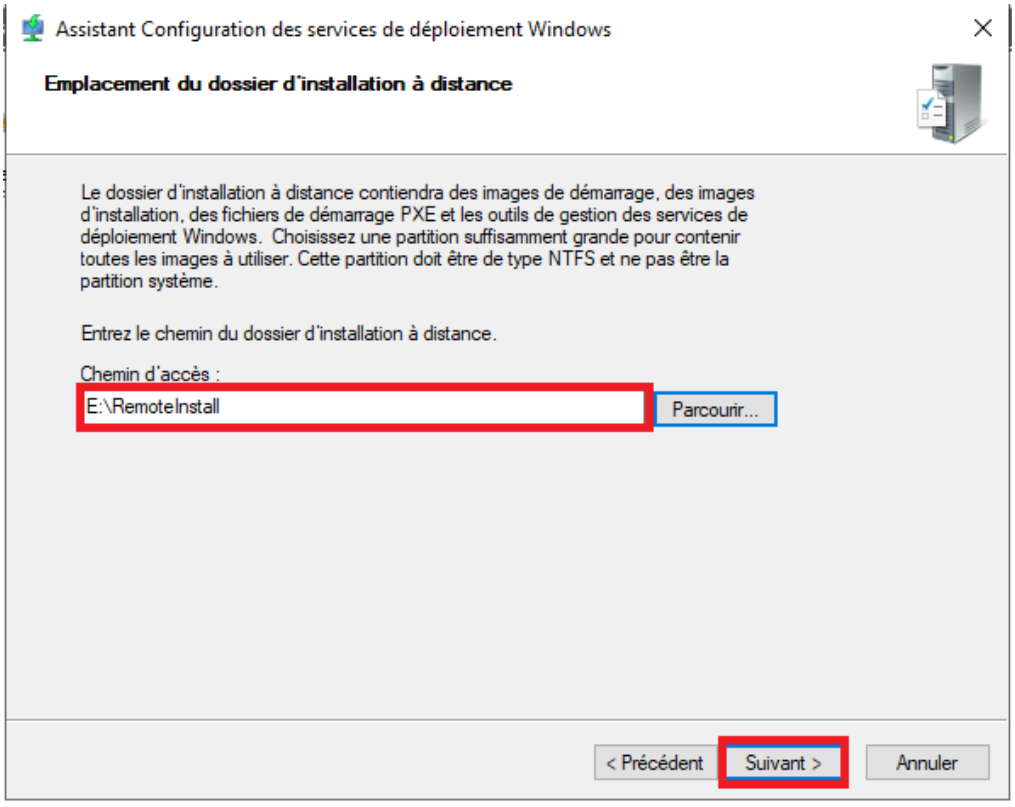
➔ Faites « **Suivant** »



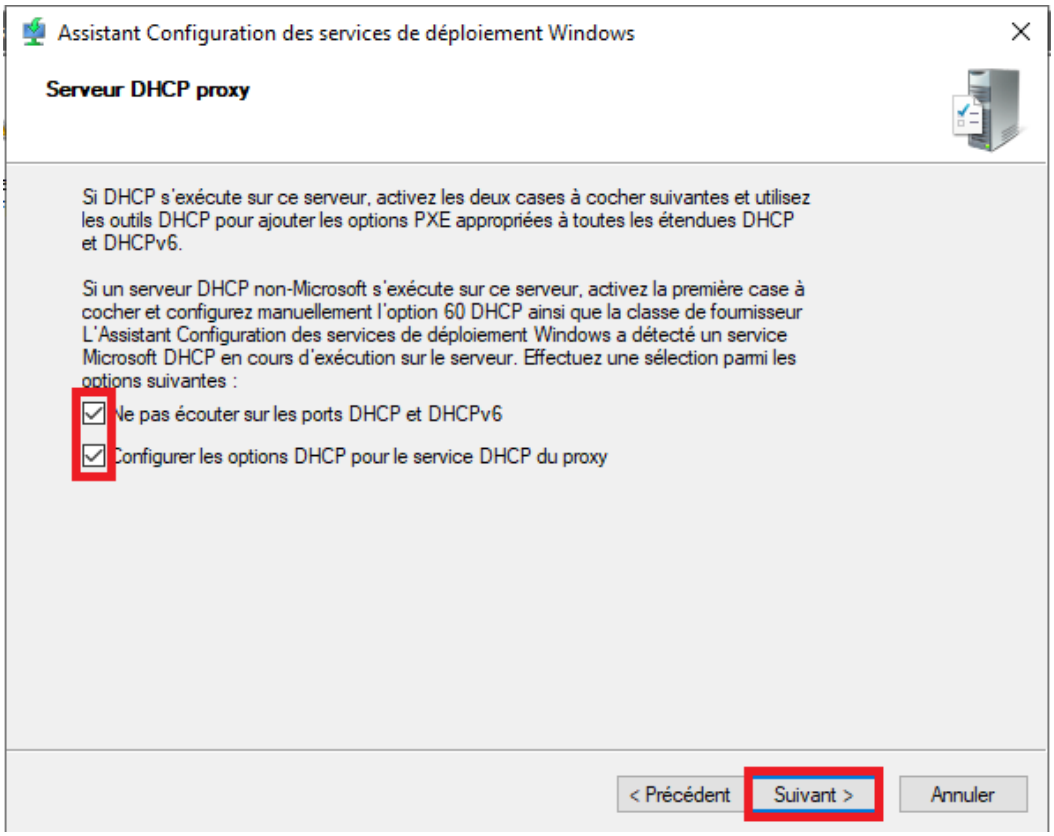
➔ Cochez la case « **Intégré à Active Directory** » puis faites « **Suivant** »



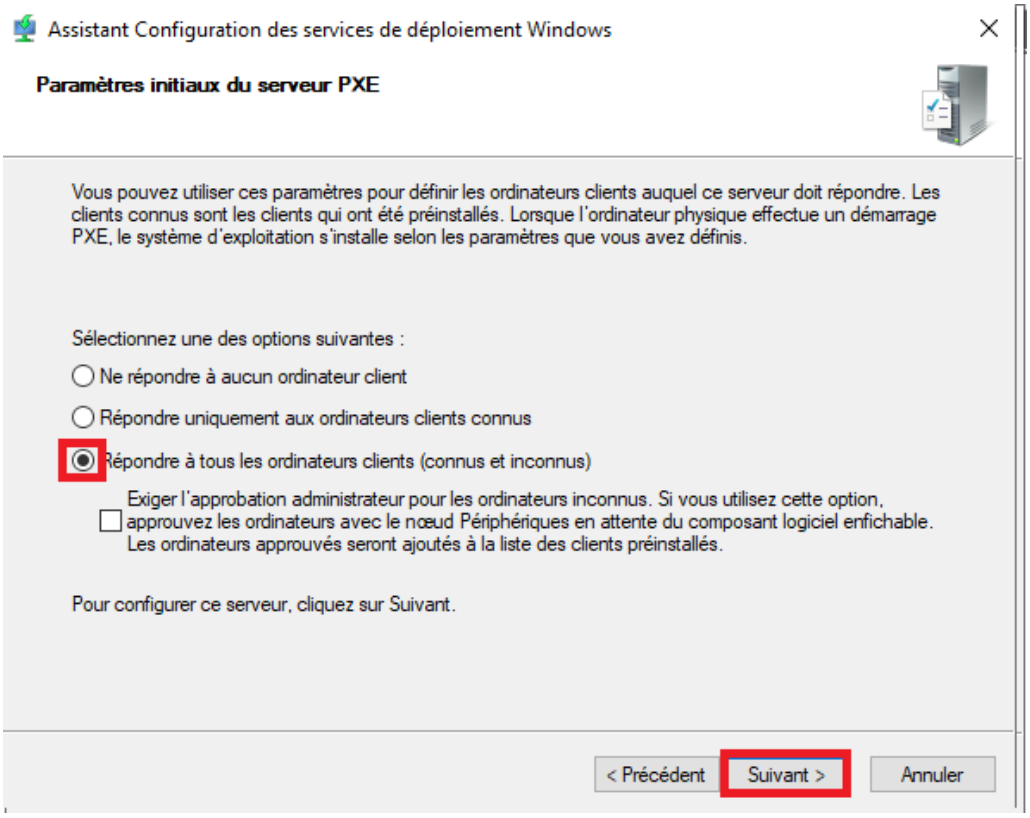
➔ Choisissez comme chemin d'accès le disque « **E :** » créé au préalable sur le serveur et dans le dossier « **RemoteInstall** » et faites « **Suivant** »



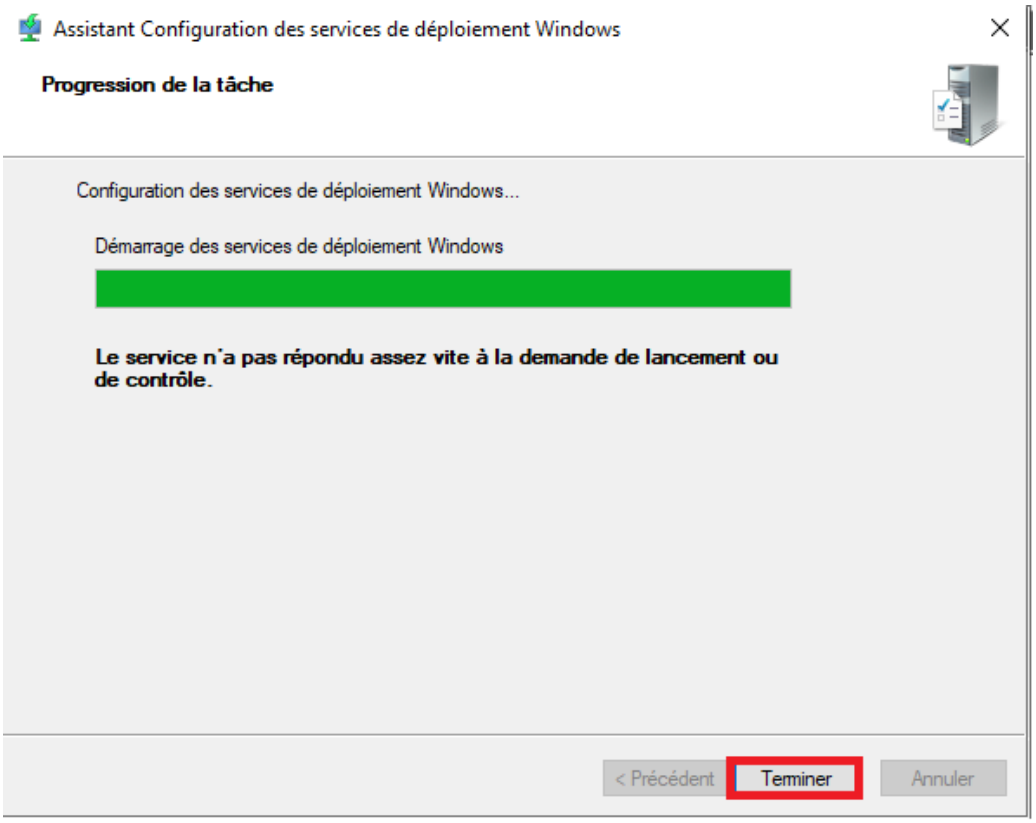
➔ Cochez les 2 cases proposées et faites « **Suivant** »



➔ Cochez la case « **Répondre à tous les ordinateurs clients** » et faites « **Suivant** »



➔ Ensuite faites « **Terminer** »



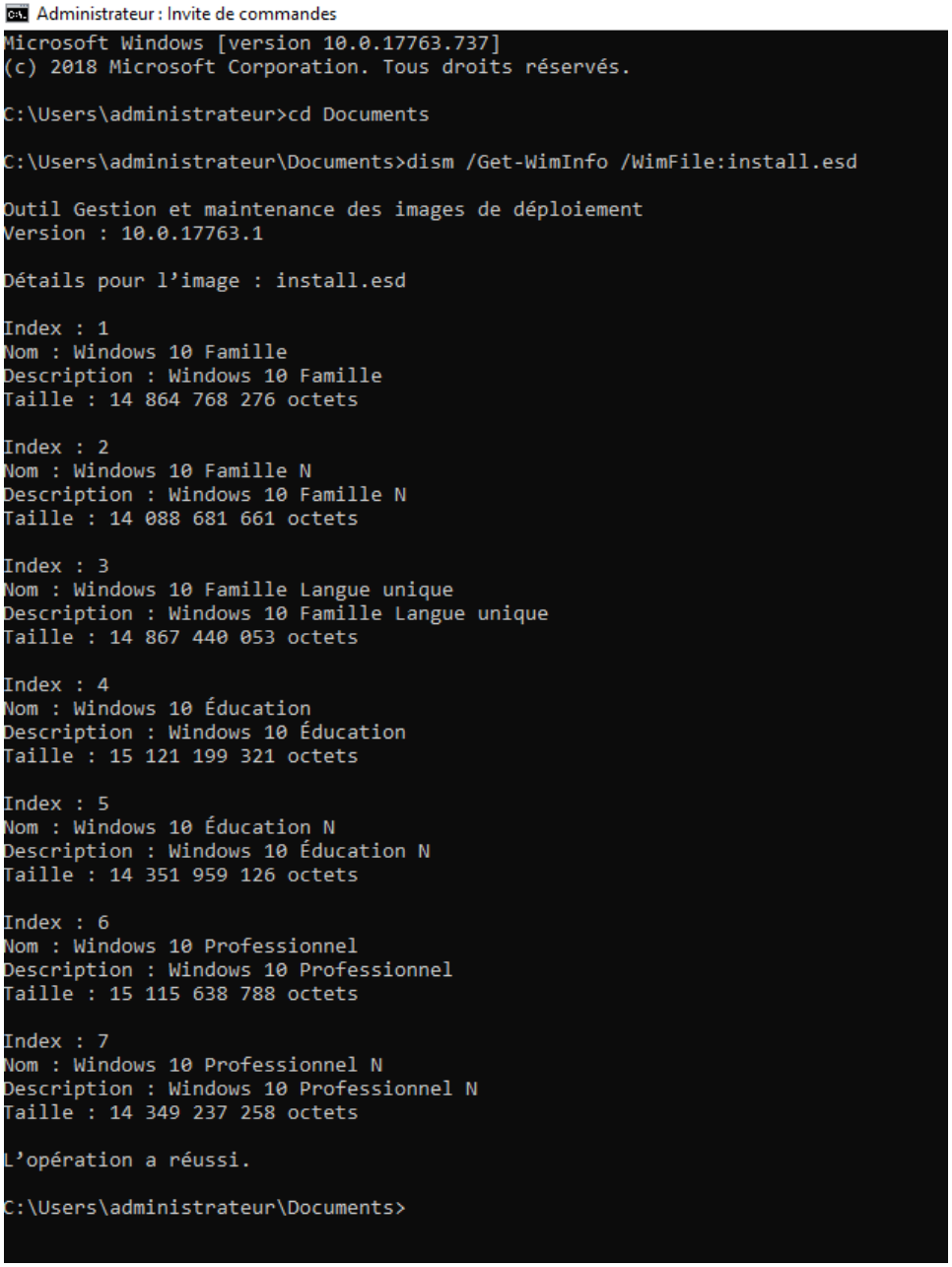
Maintenant que WDS est configuré ; nous allons ajouter une image Windows sur le service WDS. Pour ce faire, il va falloir utiliser le fichier en « **.ESD** » présent dans l'iso Windows qui doit être utilisé pour récupérer une version de Windows en « **.WIM** » :

Pour cet exemple, l'Install.esd a été déplacé dans « **Documents** », voici comment le récupérer :

Ouvrez un CMD et tapez cette commande :

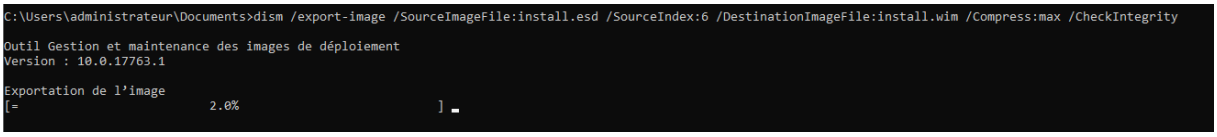
dism /Get-WimInfo /WimFile:install.esd

Cette commande permet d'avoir un détail de l'image « **install.esd** »



Ensuite il faut utiliser cette commande :
dism /export-image /SourceImageFile:install.esd /SourceIndex:6 /DestinationImageFile:install.wim /Compress:max /CheckIntegrity

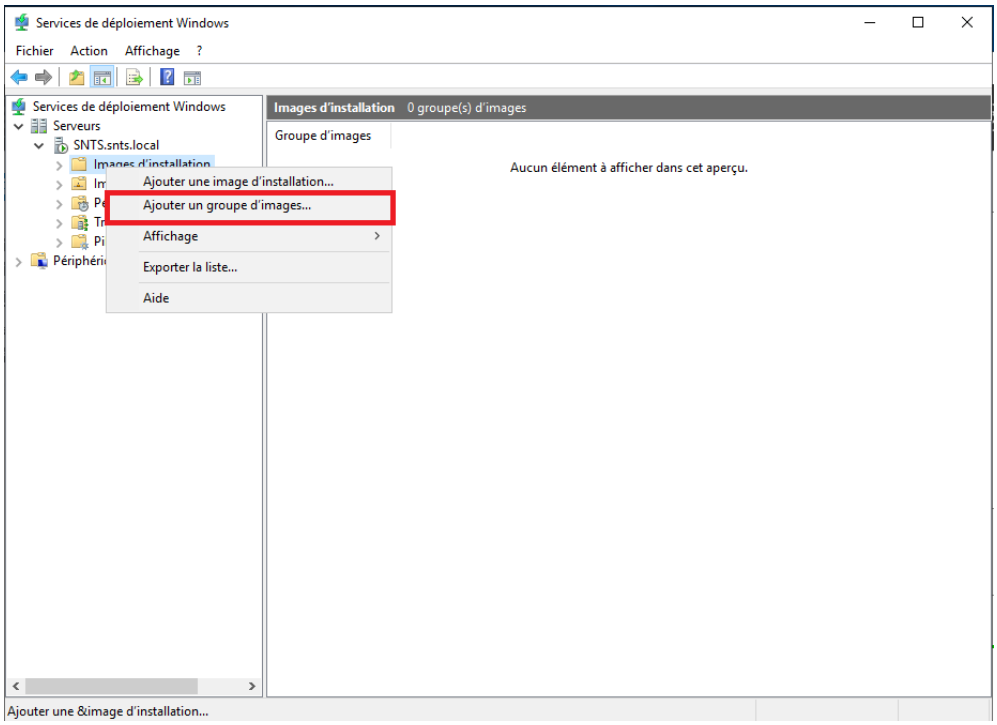
Cette commande permet de convertir un index présent dans le fichier en « **.esd** » en un fichier « **.wim** »



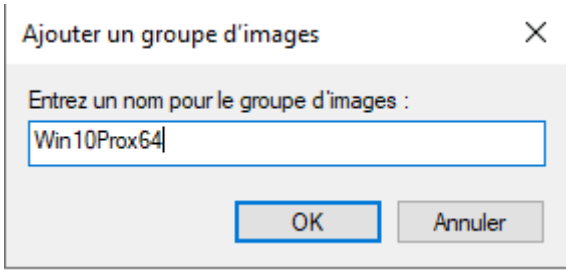
Après quelques temps le fichier « **install.wim** » est présent dans « **Documents** ».

Maintenant que le fichier « **install.wim** » a été créé ;

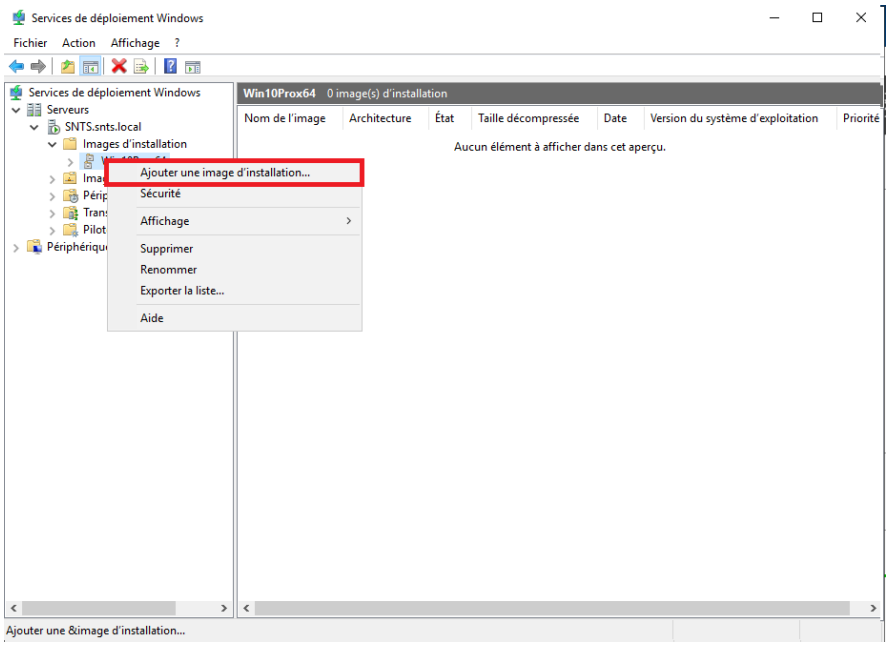
- ➔ Retournez sur le service de déploiement de Windows
- ➔ Allez sur le serveur et dans l'onglet « **Image d'installation** », faites un clic droit « **Ajouter un groupe d'images** »



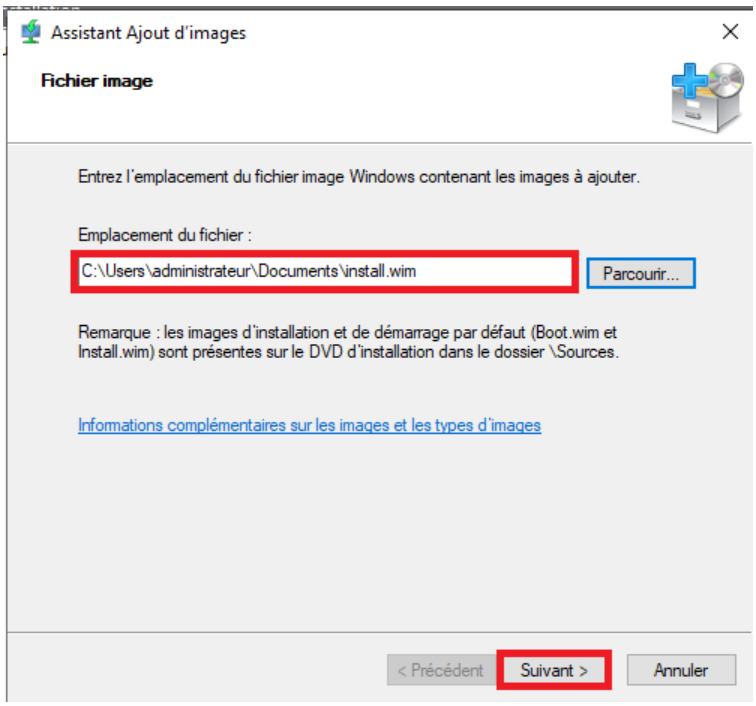
- ➔ Nommez le groupe d'images, ici nous allons l'appeler « **Win10Prox64** ».



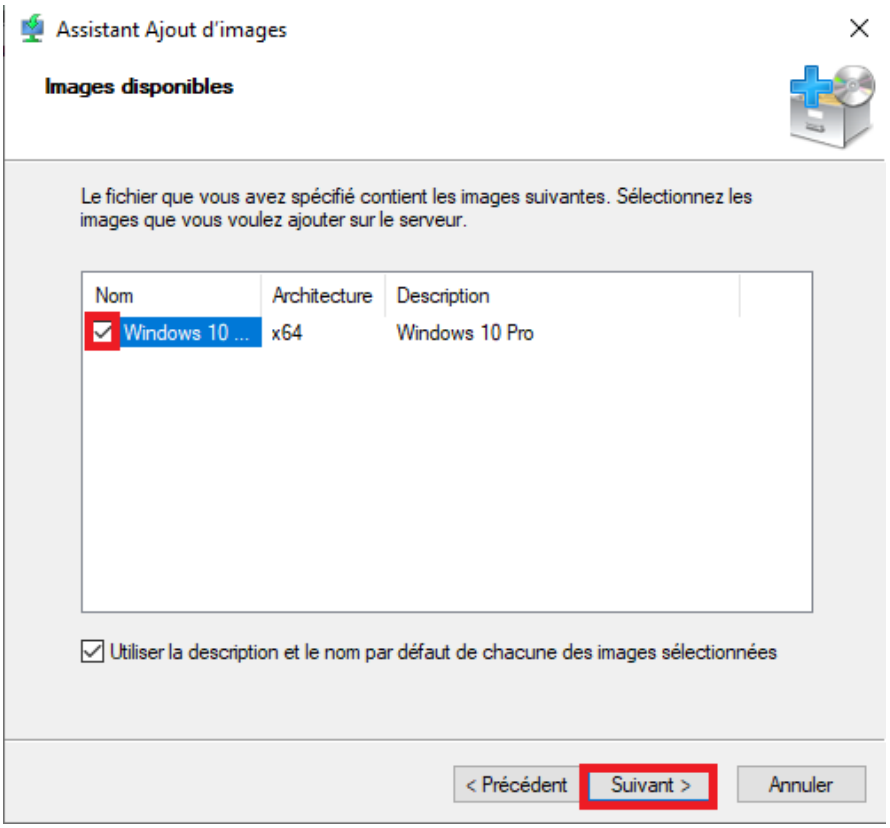
Une fois que le groupe d'image est installé, allez dans le dossier et faites « **Ajouter une image d'installation** ».



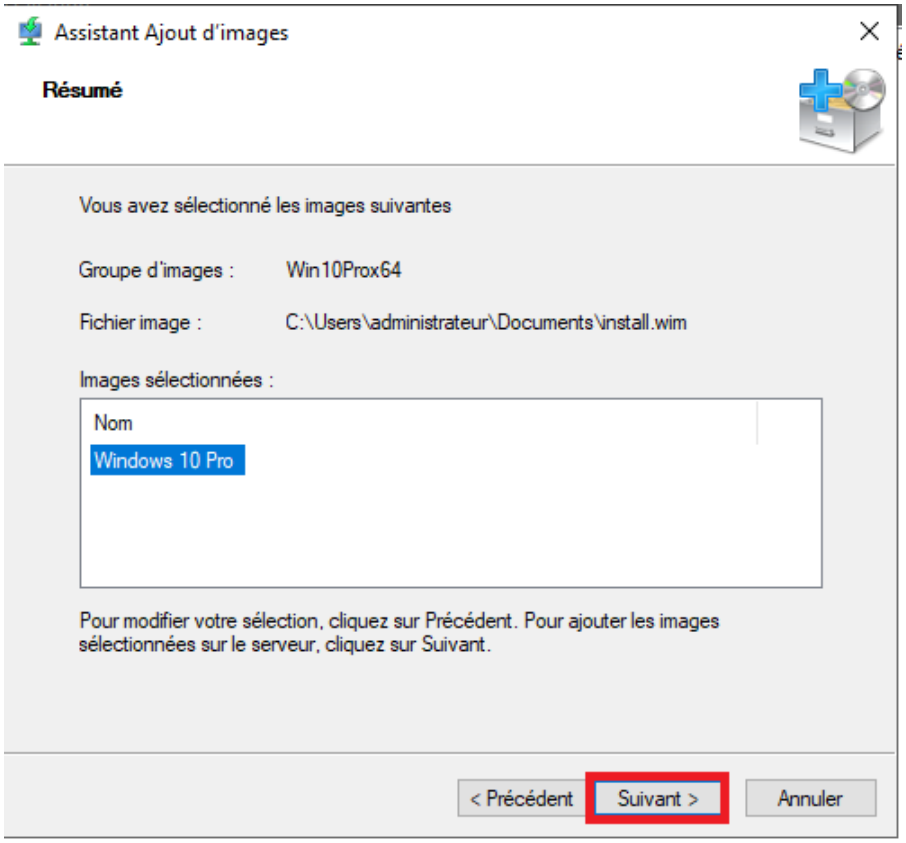
Maintenant il faut allez chercher dans les documents le fichier « **install.wim** » extrait précédemment puis faites « **Suivant** »



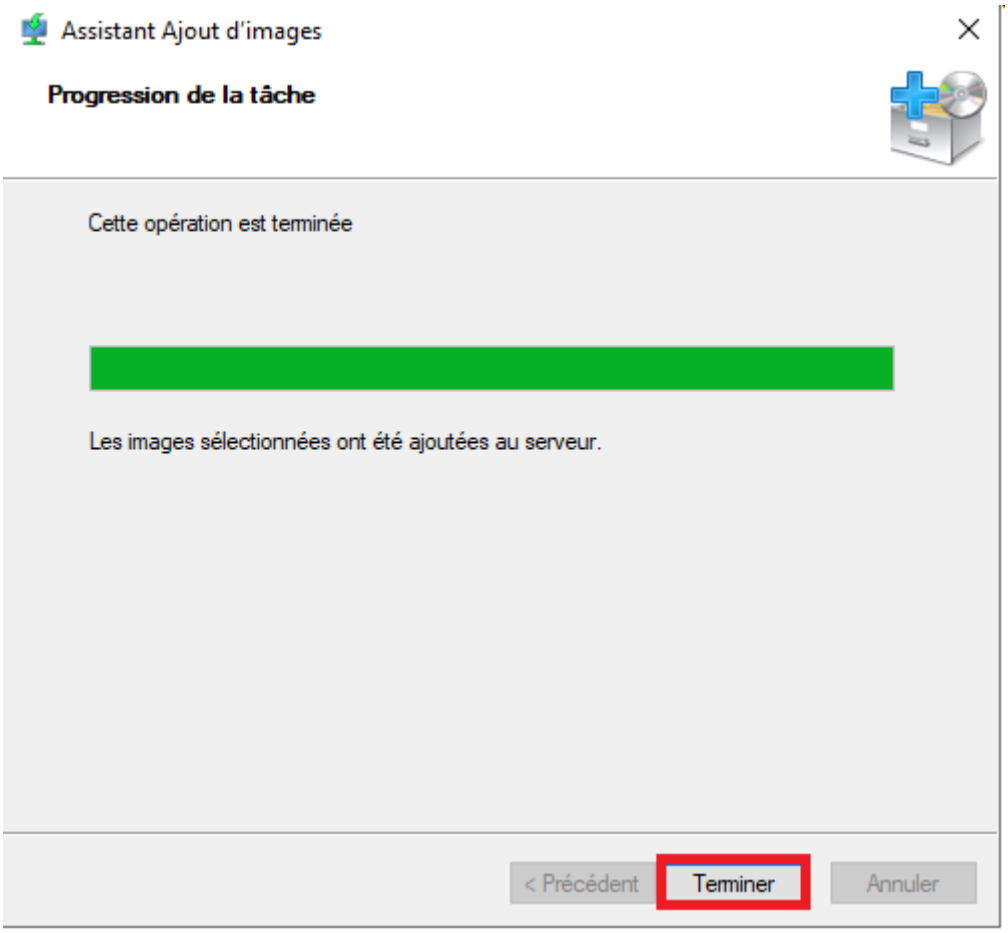
➔ Choisir la version de Windows 10 Pro puis faites « **Suivant** »



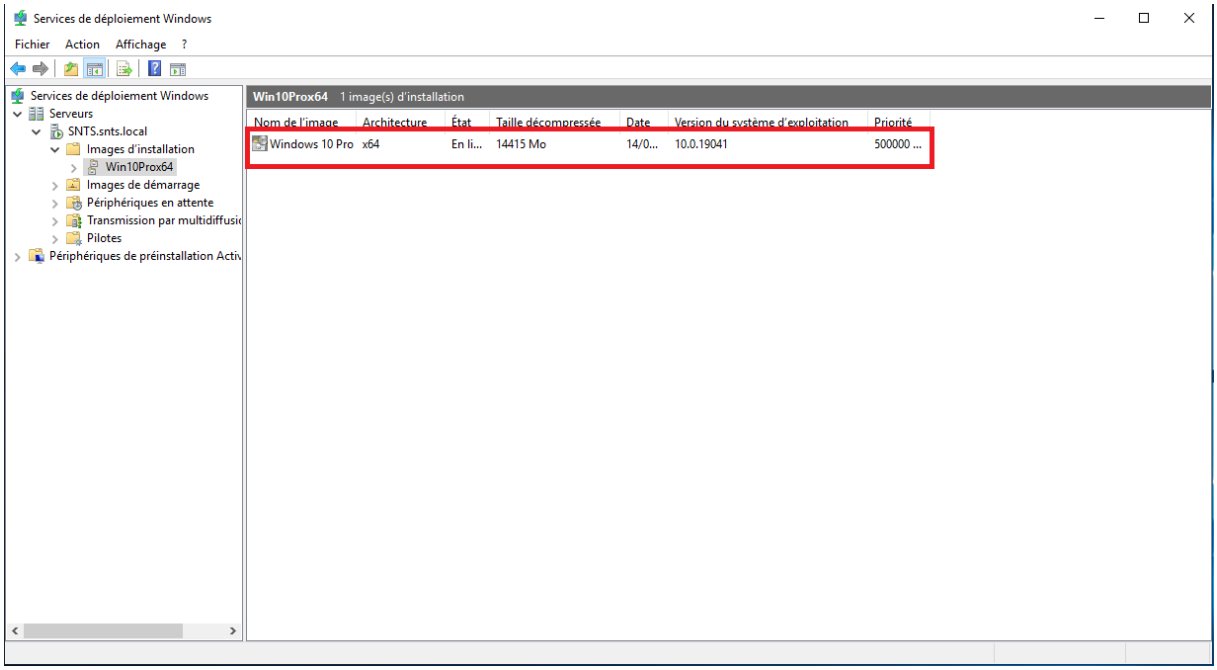
➔ Faites « **Suivant** »



➔ Quand le téléchargement est terminé faites « **Terminer** »



Maintenant l'image de Windows 10 est installé sur WDS.

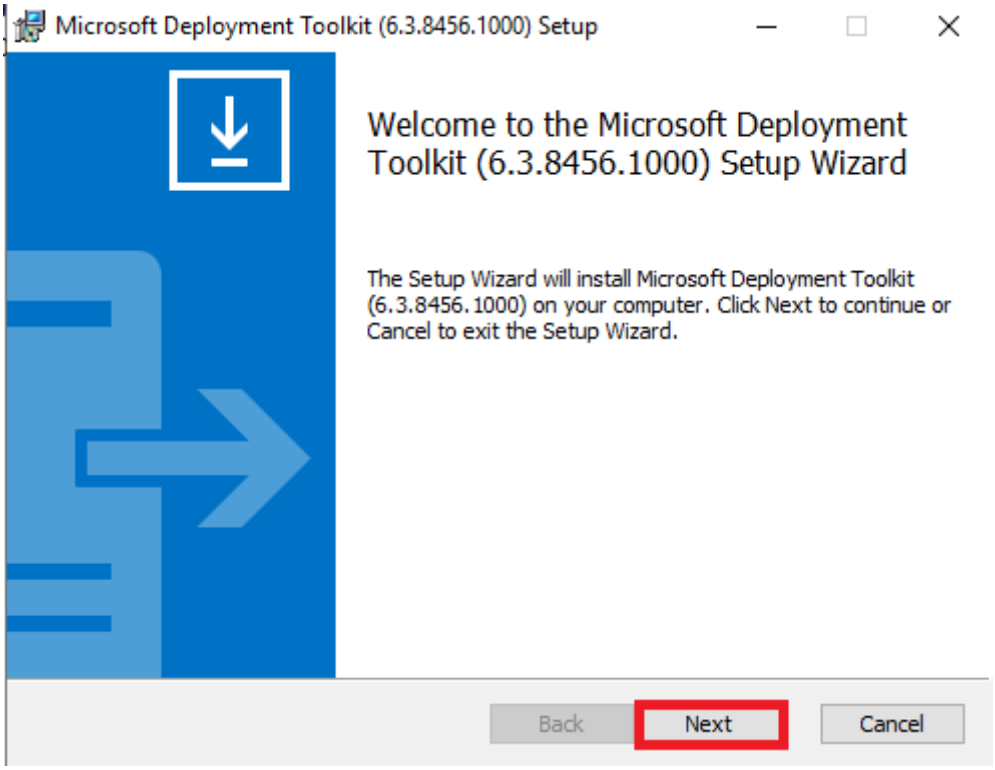


2. Installation et configuration du MDT

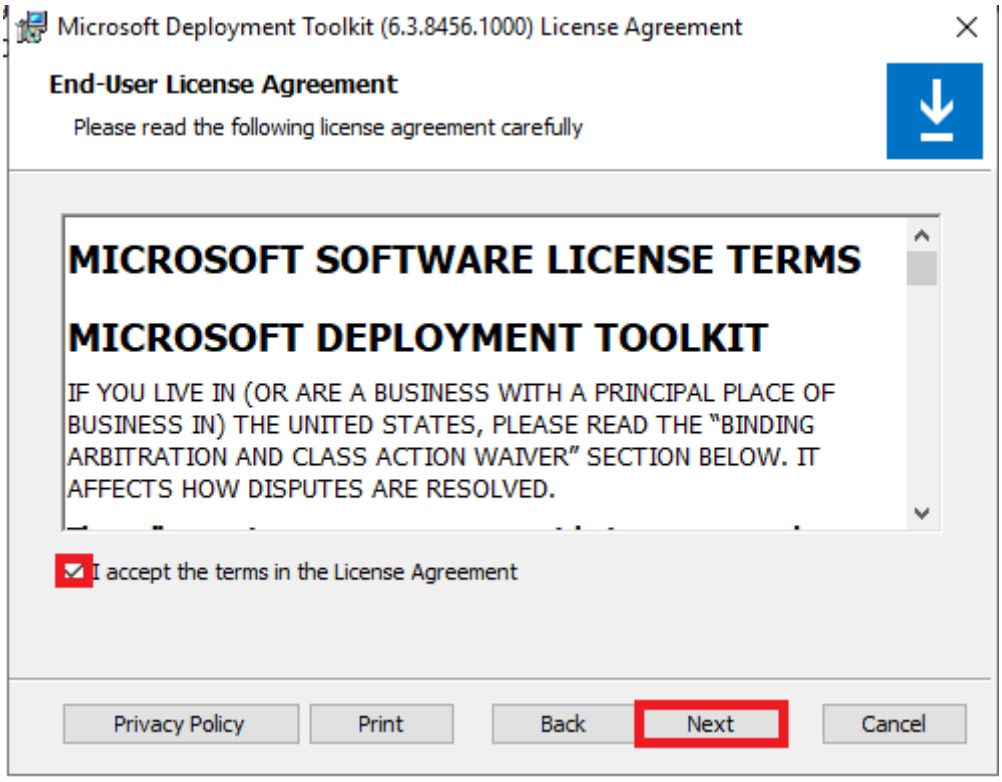
Maintenant que les prérequis sont installés, nous allons passer à l'installation de MDT :

(Lien de téléchargement : [Download Microsoft Deployment Toolkit (MDT) from Official Microsoft Download Center])

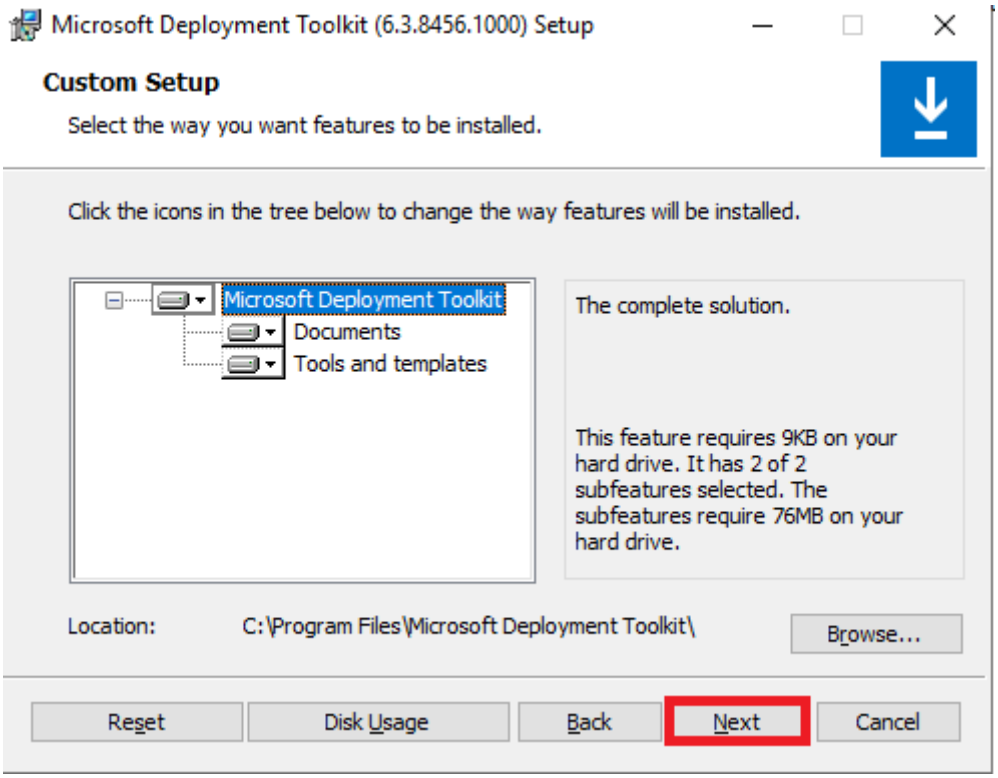
➔ Une fois le setup lancé, il faut faire « **Suivant** »



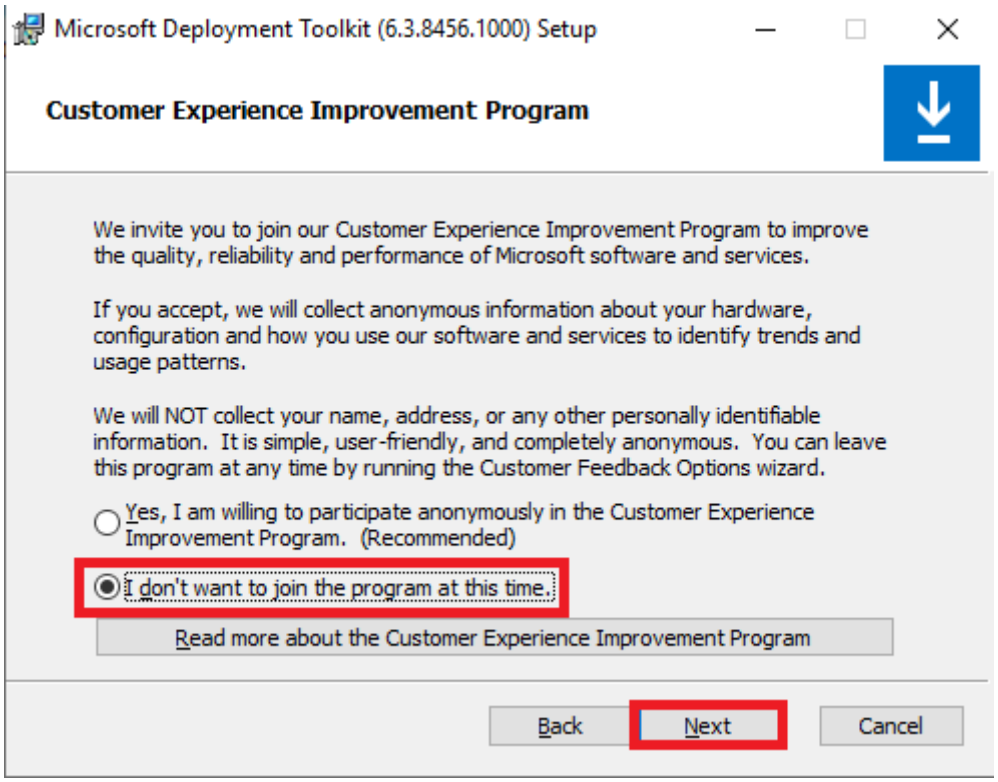
➔ Acceptez les termes de la License puis faire « **Suivant** »



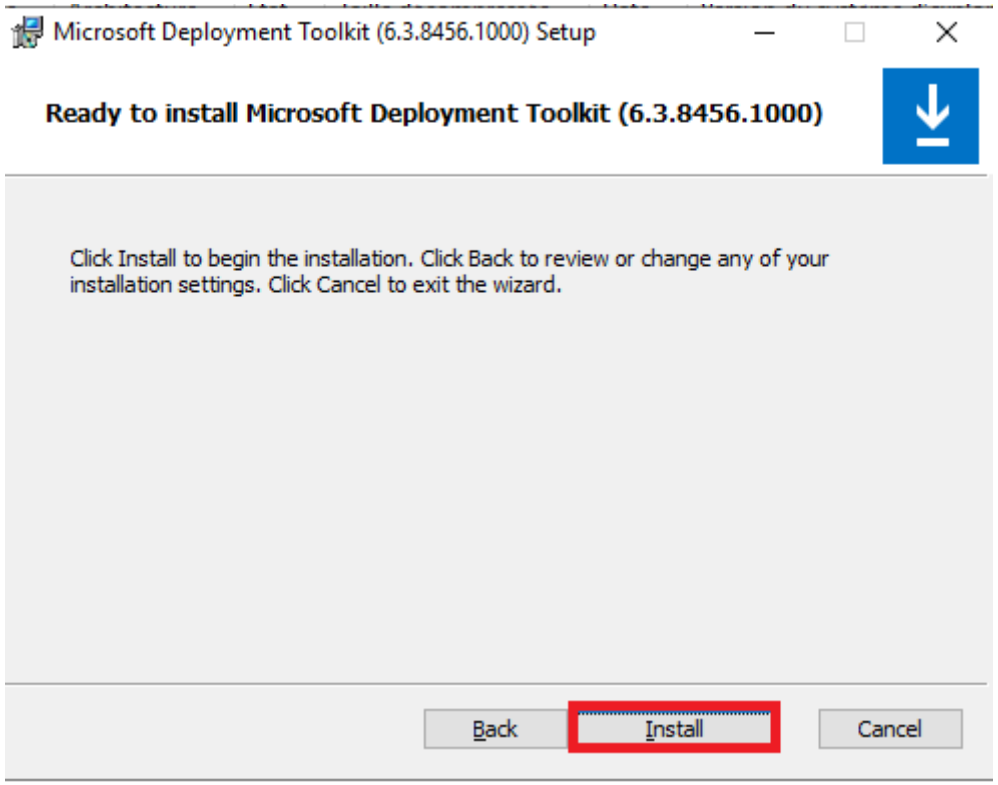
➔ Faites « **Suivant** »



➔ Cochez la dernière case puis faites « **Suivant** »

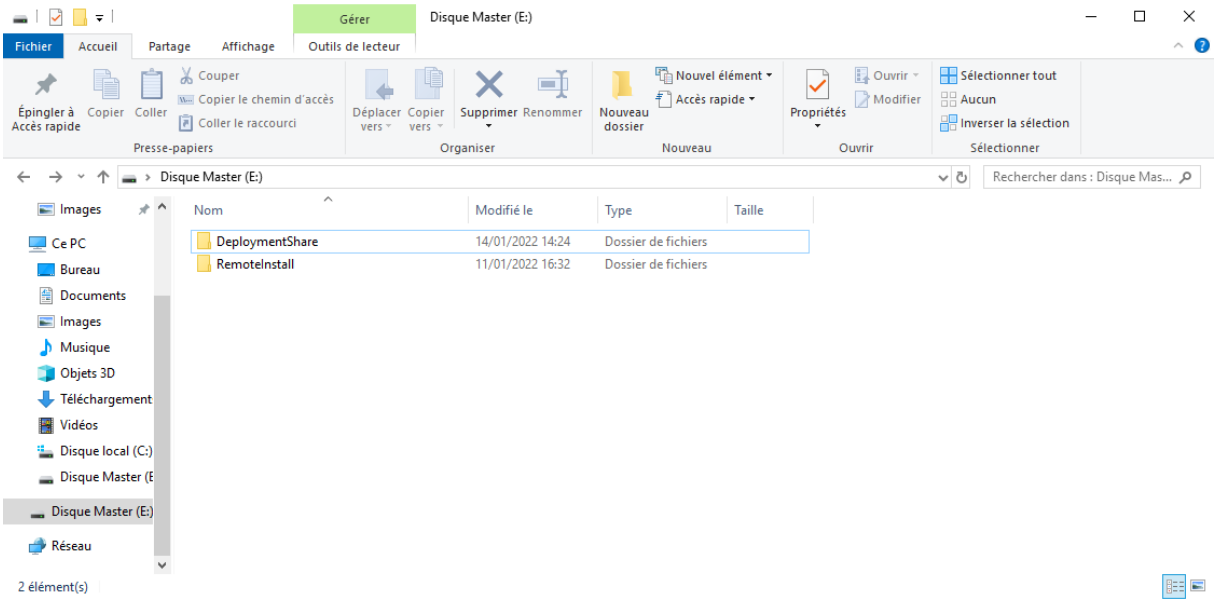


➔ Puis faites « **Installer** »



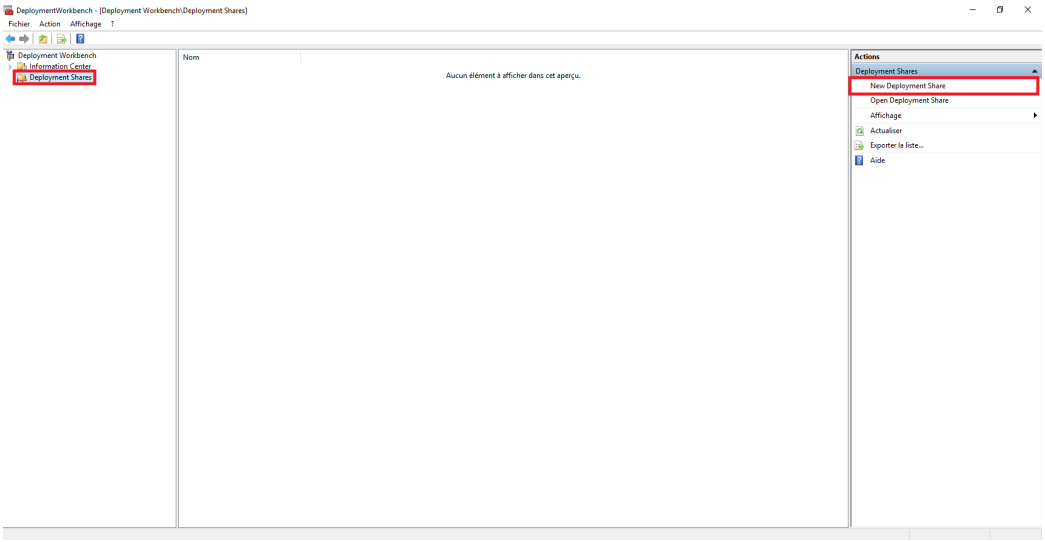
Maintenant nous allons passer à la Configuration de MDT :

Tout d'abord il faut créer un dossier « **DeploymentShare** » qui va recevoir des fichiers nécessaires pour un bon fonctionnement :

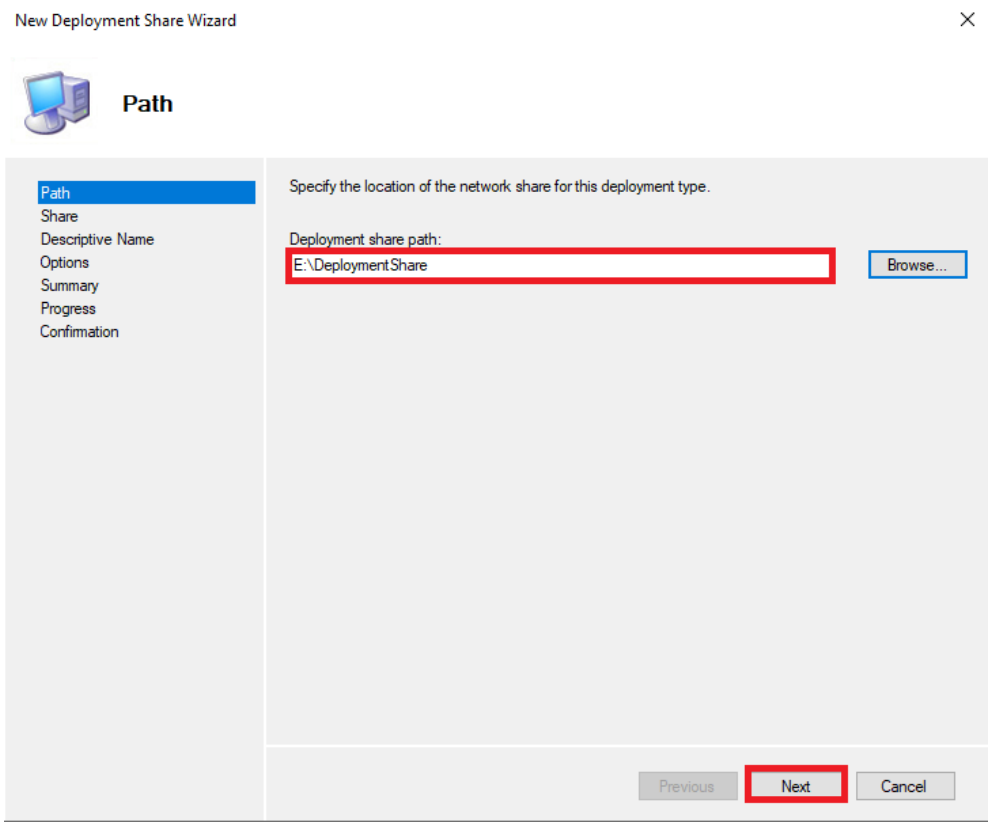


Maintenant il faut ouvrir Deployment Workbench

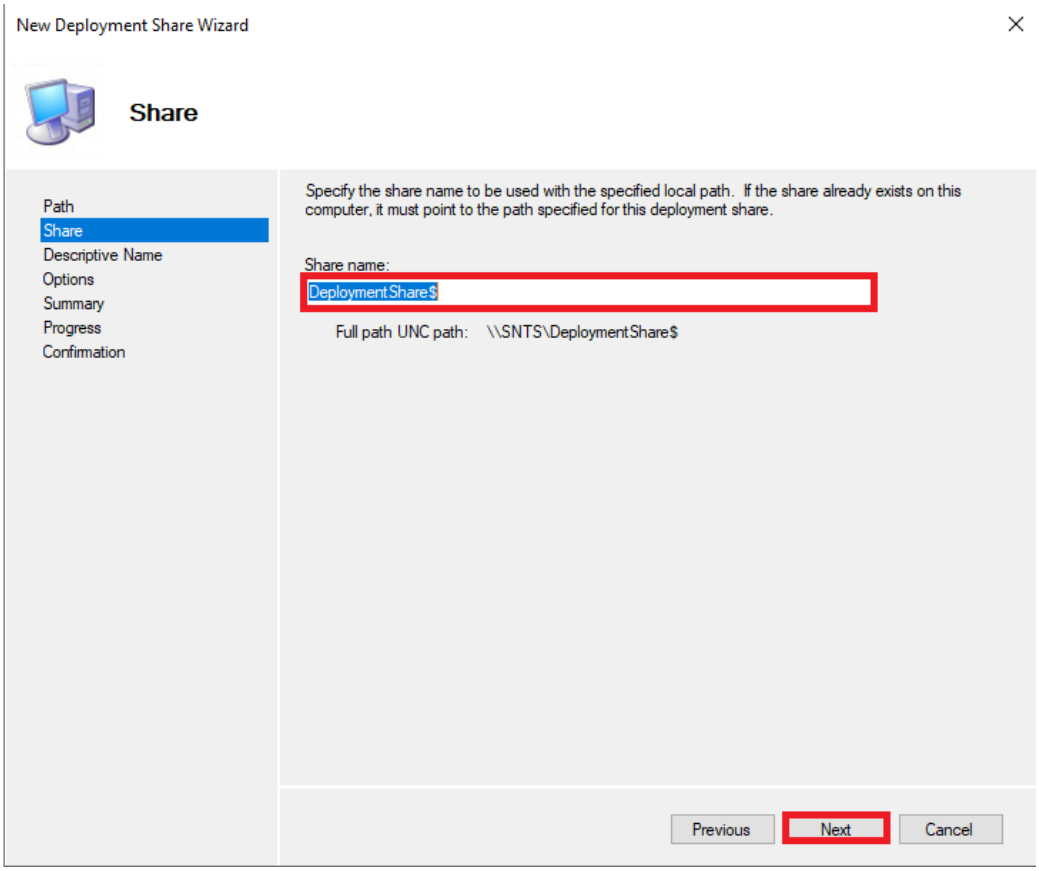
Sur le Deployment Workbench, sélectionnez Deployment Share et faire « **New Deployment Share** »



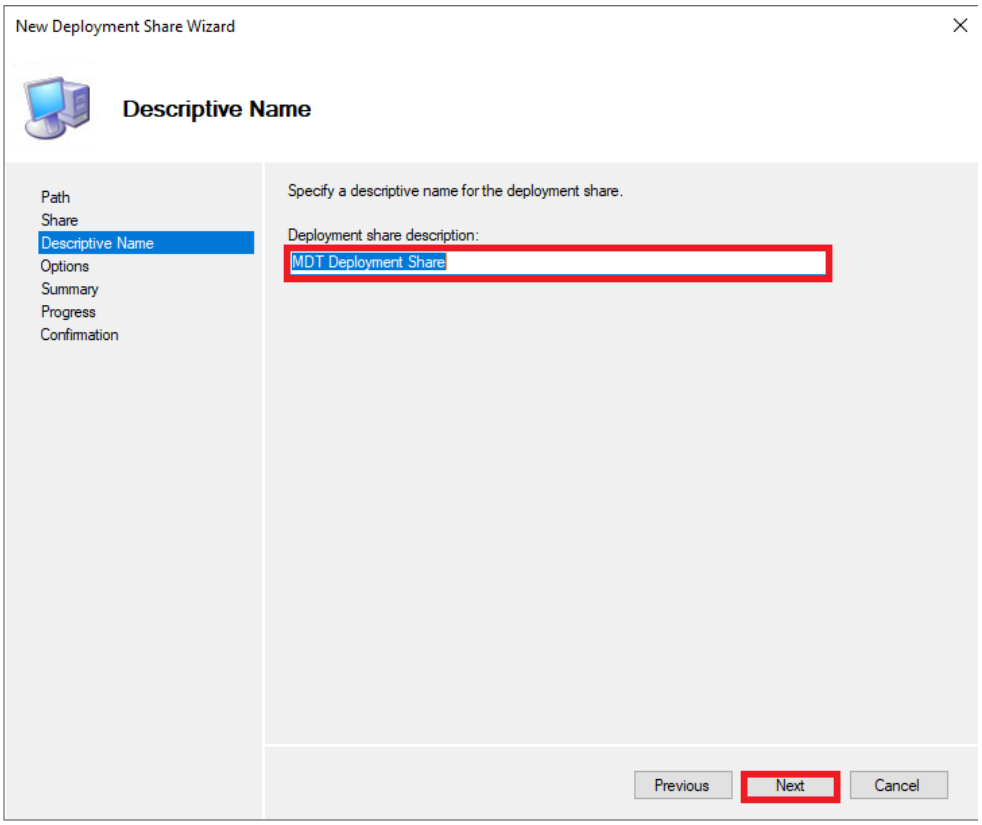
➔ Renseignez le chemin d'accès du fichier créer juste avant qui est « **DeploymentShare** » puis faites « **Suivant** »



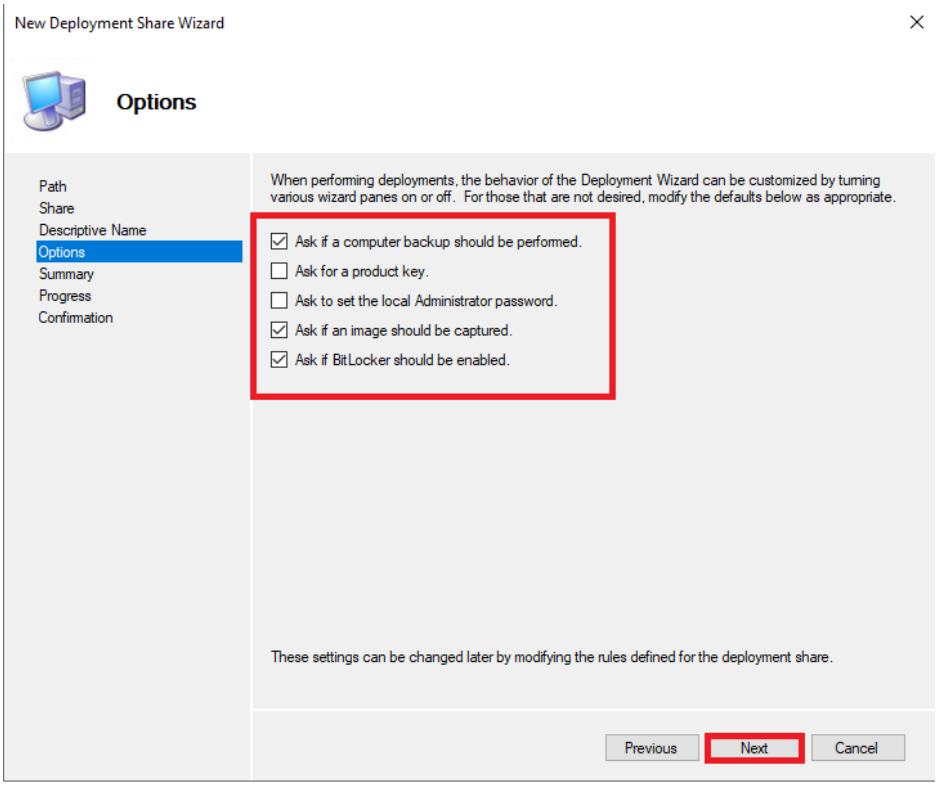
➔ Vérifiez le nom du dossier partagé puis faites « **Suivant** »



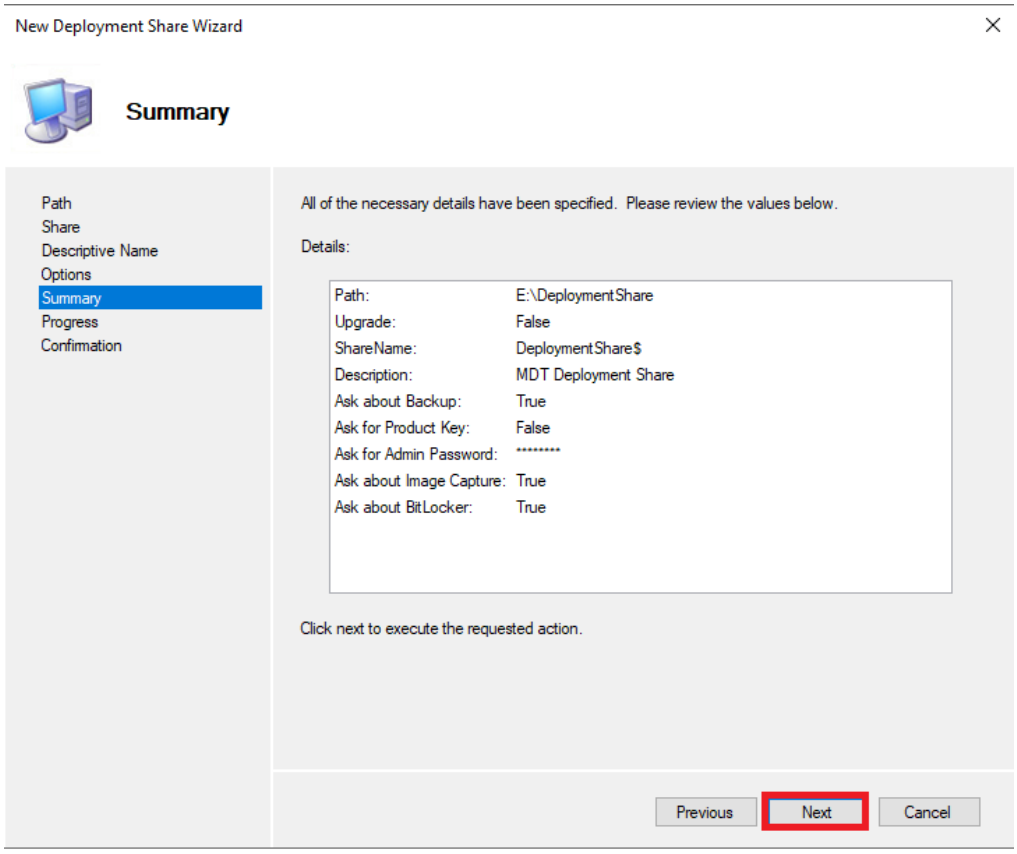
➔ Choisissez une description puis faites « **Suivant** »



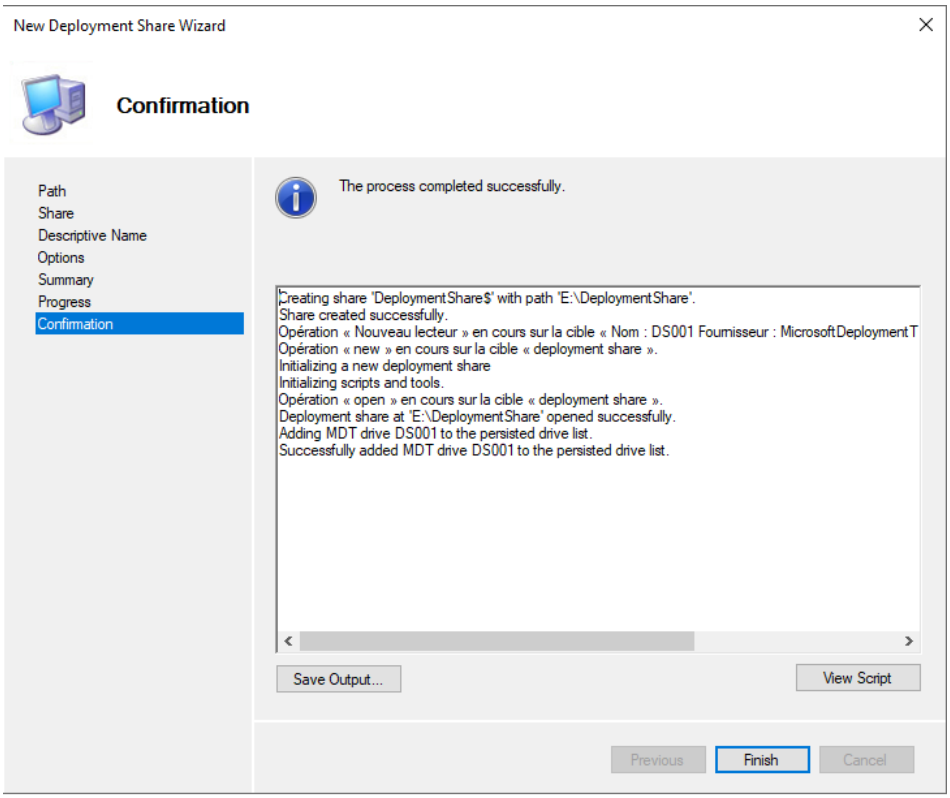
➔ Cochez les différentes cases puis faites « **Suivant** »



➔ Faites « **Suivant** »

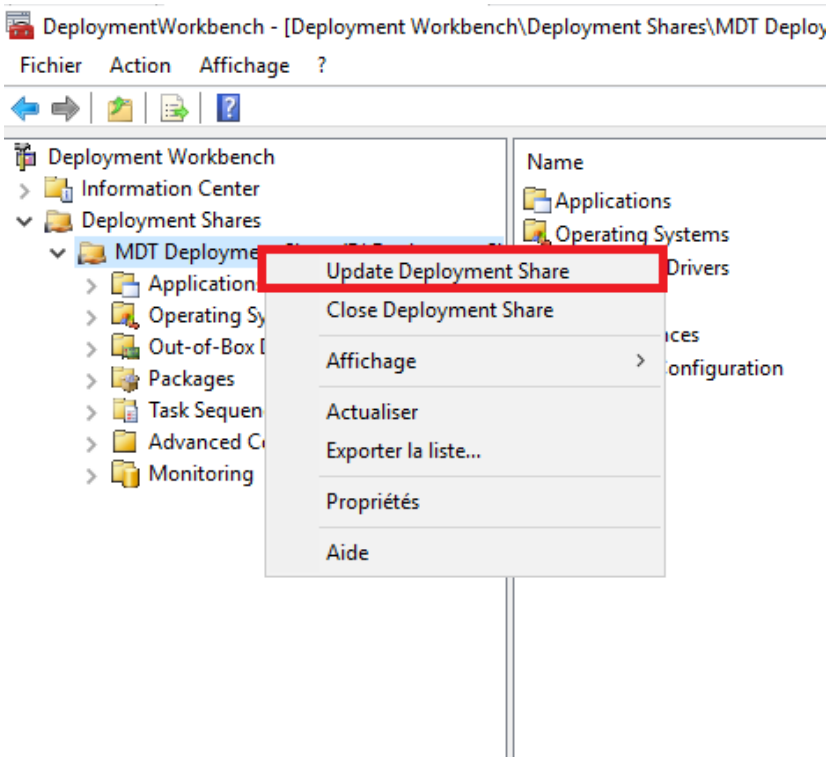


➔ Une fois que le processus est terminé faites « **Terminer** »

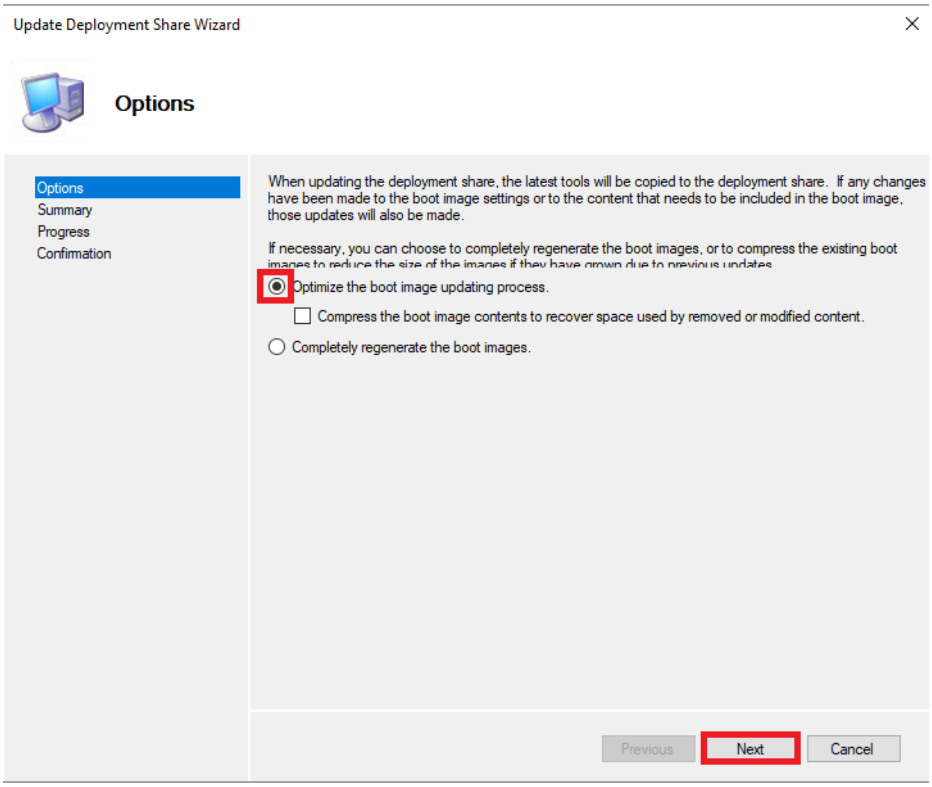


MDT est maintenant configuré, il faut ensuite sur MDT générer une image de boot, pour ce faire il faut :

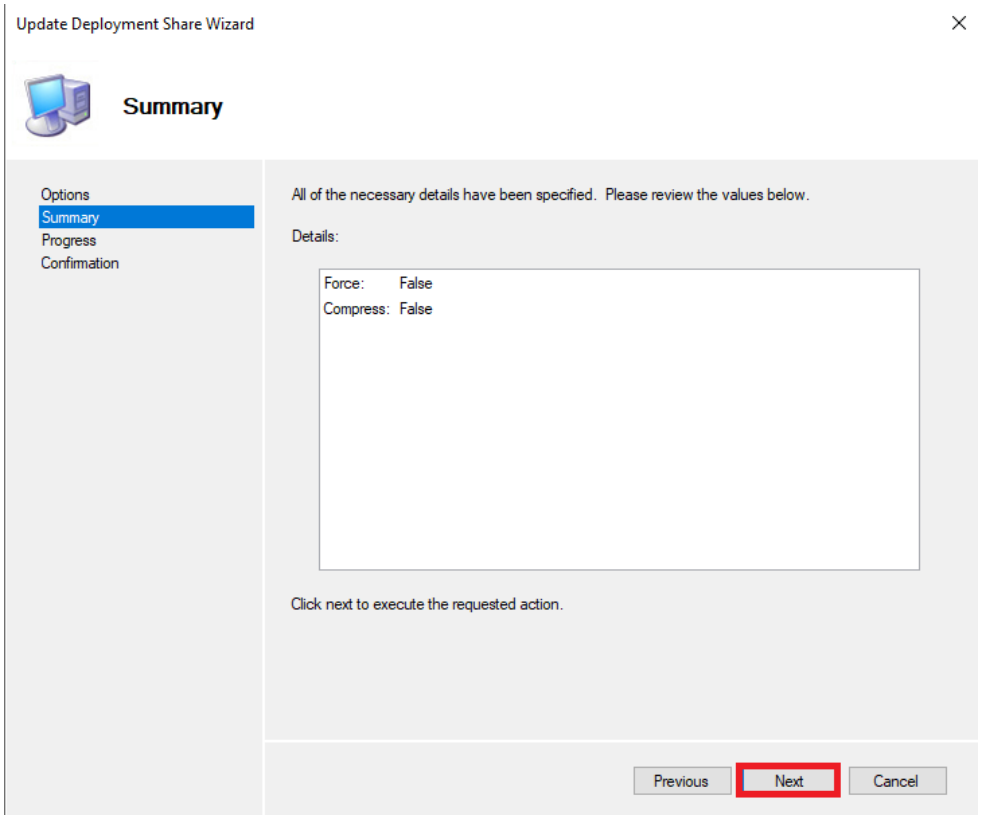
➔ Faites un clic droit sur l'onglet « **MDT Deployment Share** » puis faites « **Update Deployment Share** ».



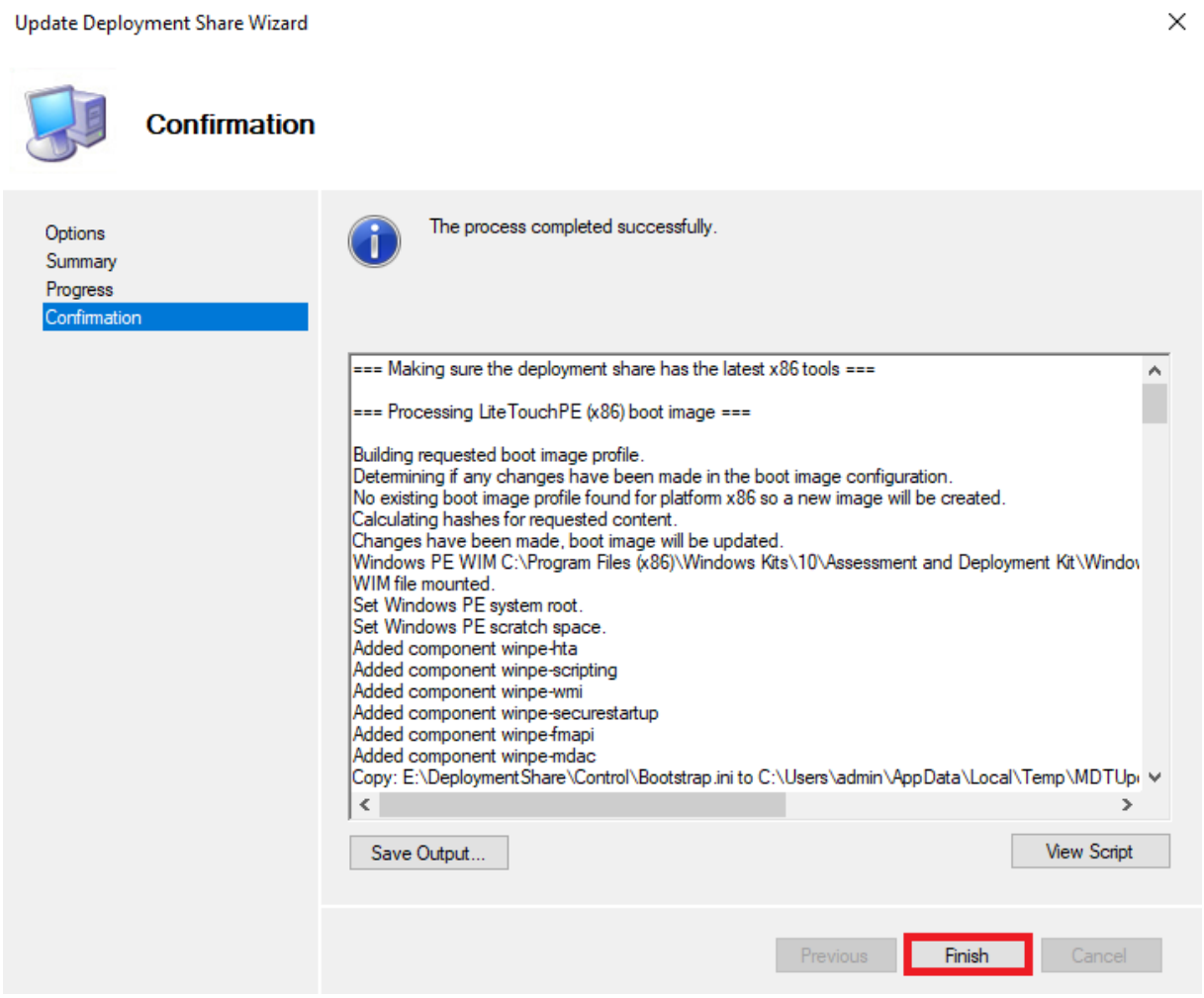
➔ Cochez la case « **Optimize the boot image updating process** » puis faites « **Next** »



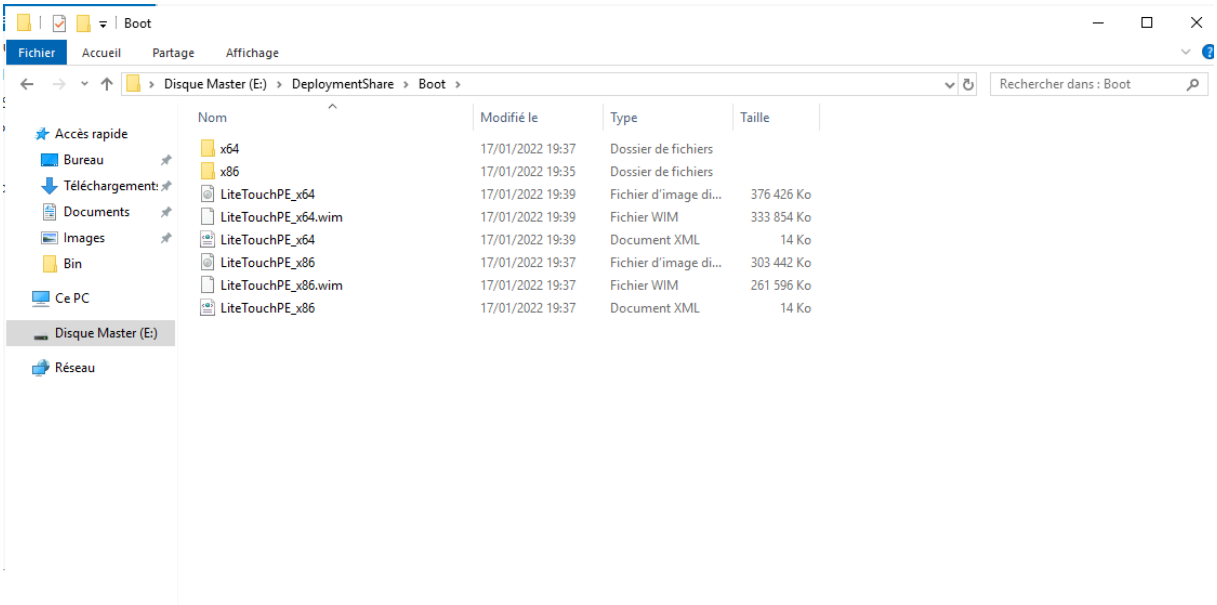
➔ Faites « **Suivant** »



➔ Attendre puis faites « **Terminer** »

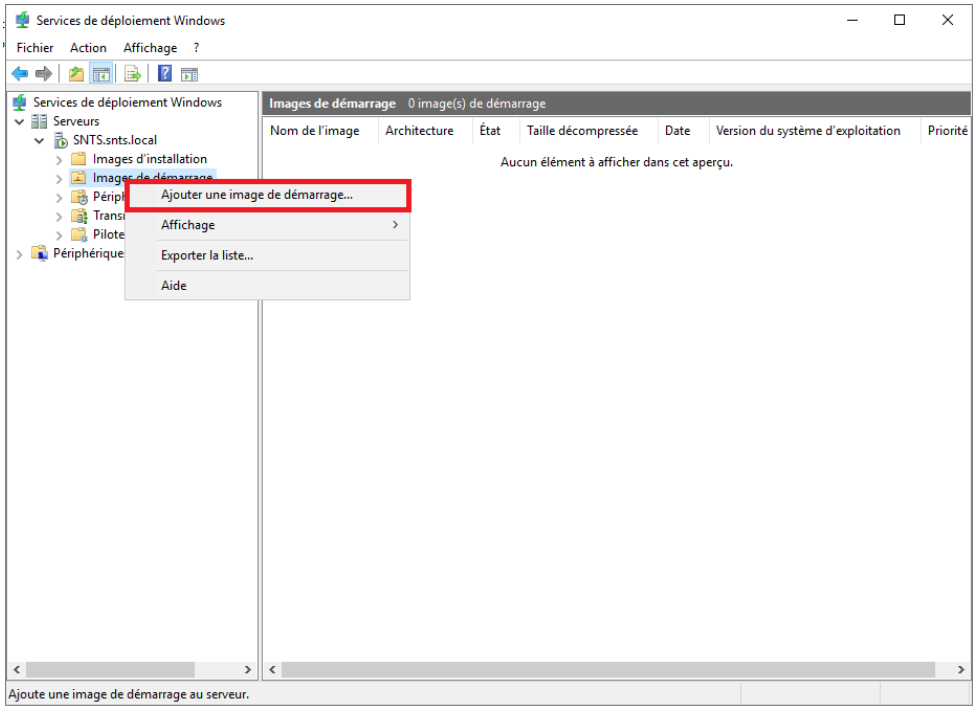


Dans DeploymentShare de MDT, les fichiers d'images ont été créés.



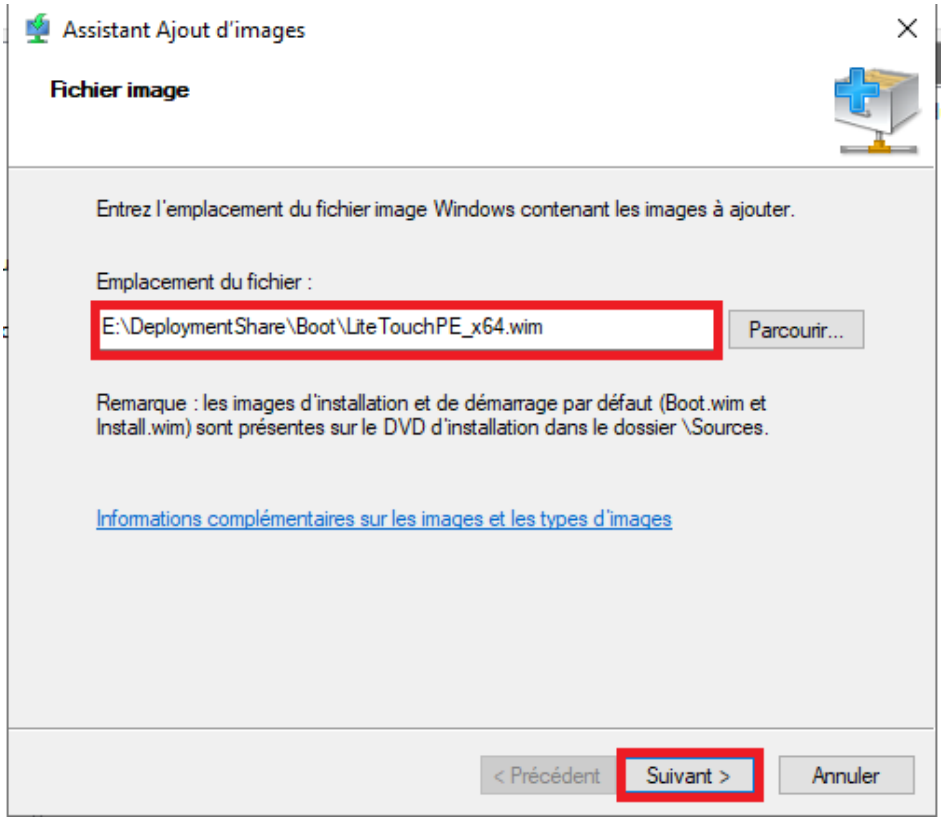
➔ Maintenant il faut ajouter l'image « **LiteTouchPE** » créé juste avant sur WDS.

Pour ce faire il faut se rendre sur le « **Service de déploiement Windows** » dans l'onglet « **Images de démarrage** » et faire un clic droit « **Ajouter une image de démarrage** »

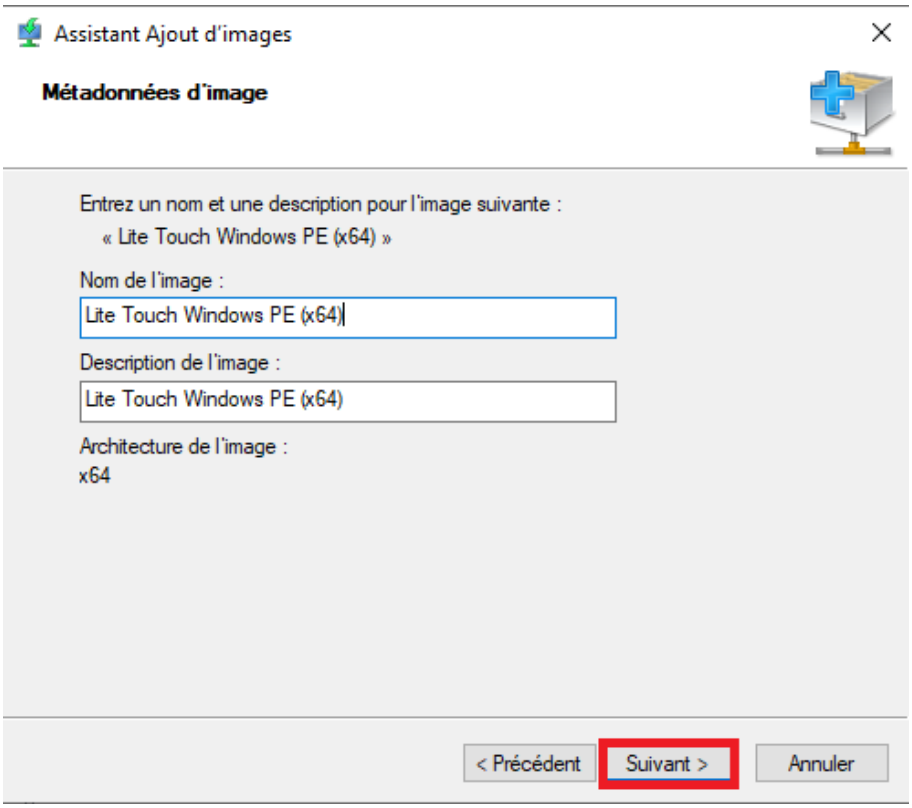


➔ Il va falloir aller chercher le « **LiteTouchPE** » créé avant avec MDT en suivant le chemin sur la capture

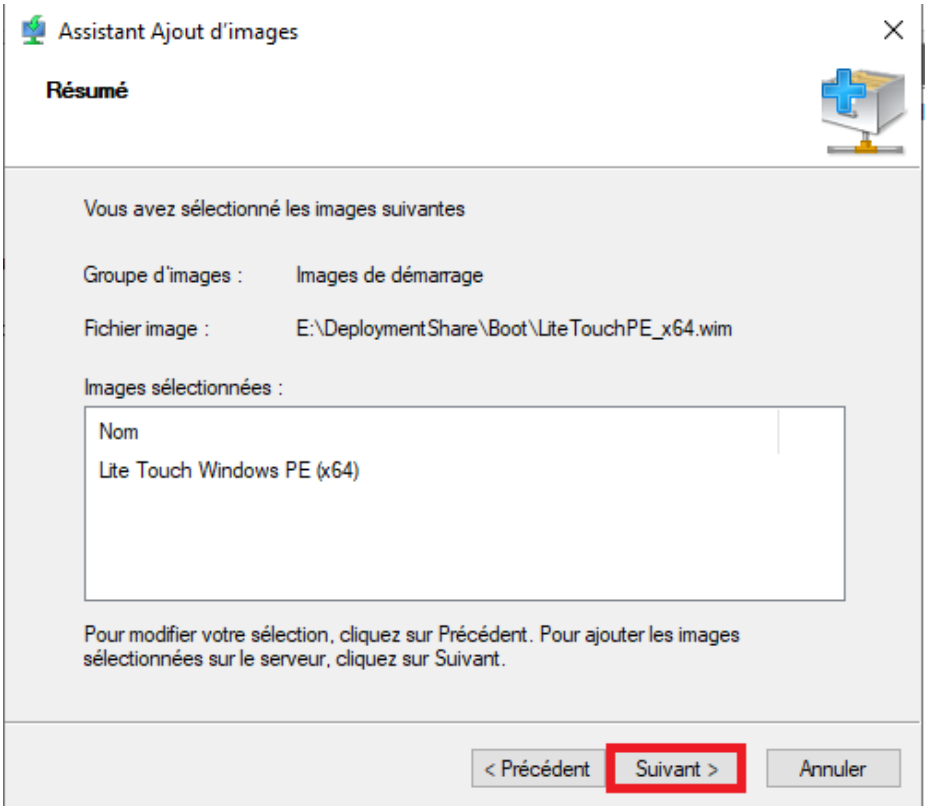
➔ Une fois le « **.wim** » ajouté, faites « **Suivant** ».



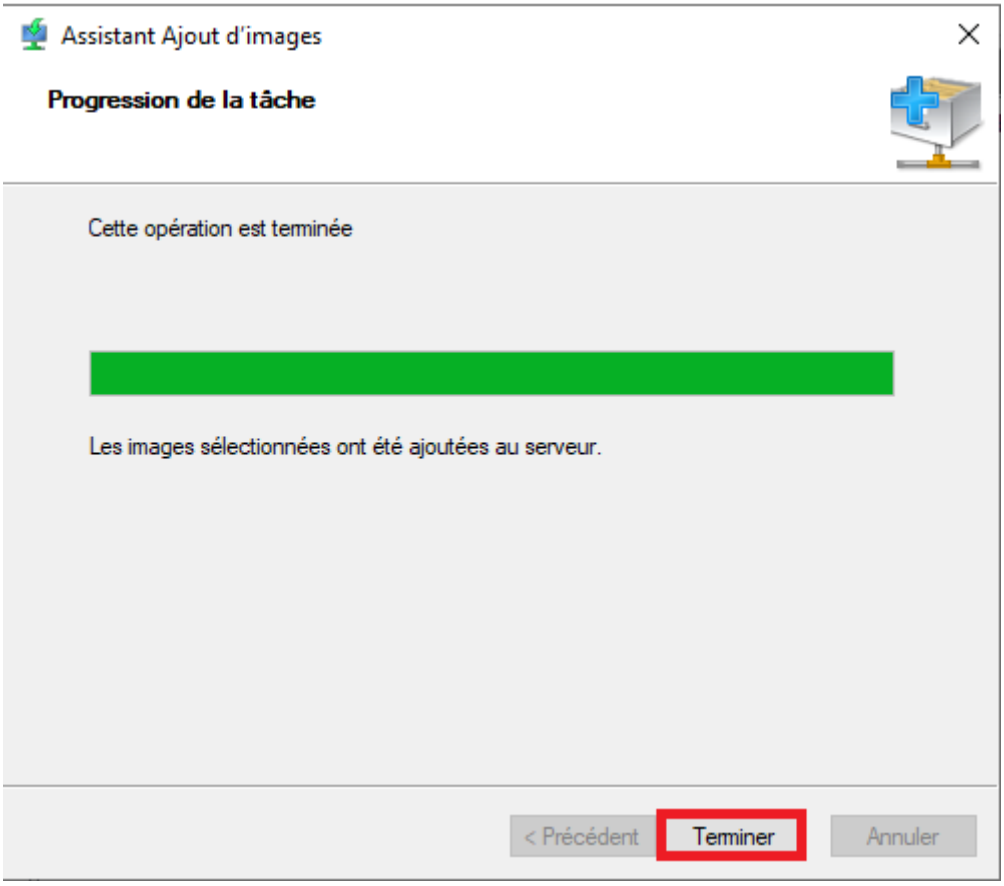
➔ Faites « **Suivant** »



➔ « **Suivant** » encore une fois



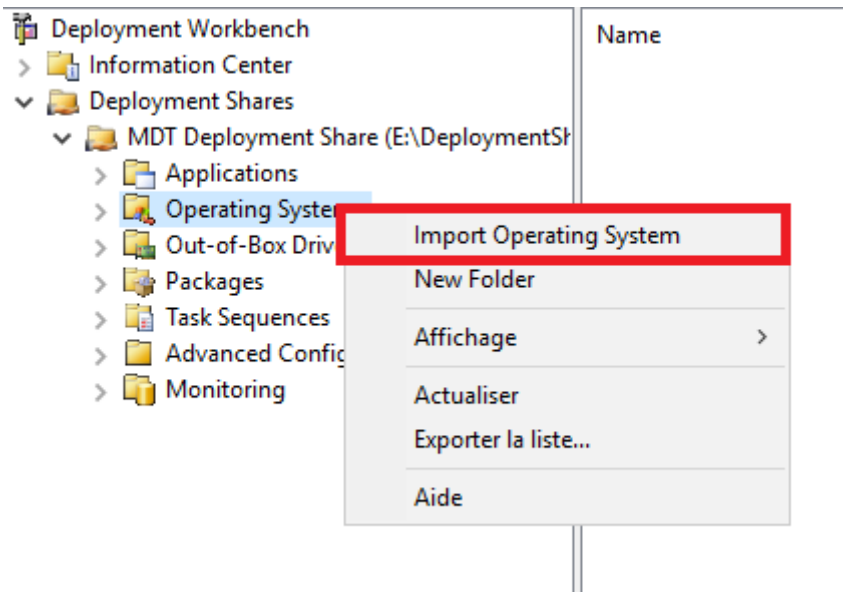
➔ Enfin « **Terminer** »



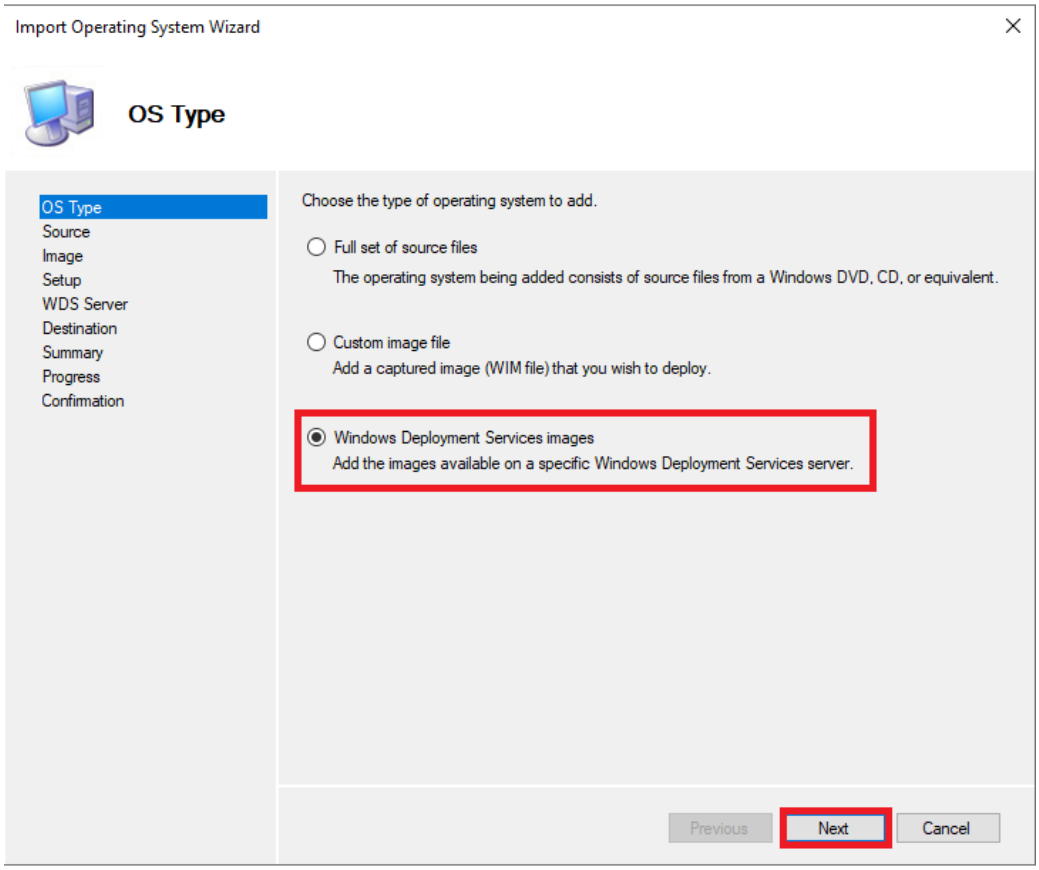
Maintenant, vous avez une image de démarrage dans WDS.

La prochaine étape pour la réalisation du master est d'ajouter une image Windows dans MDT :

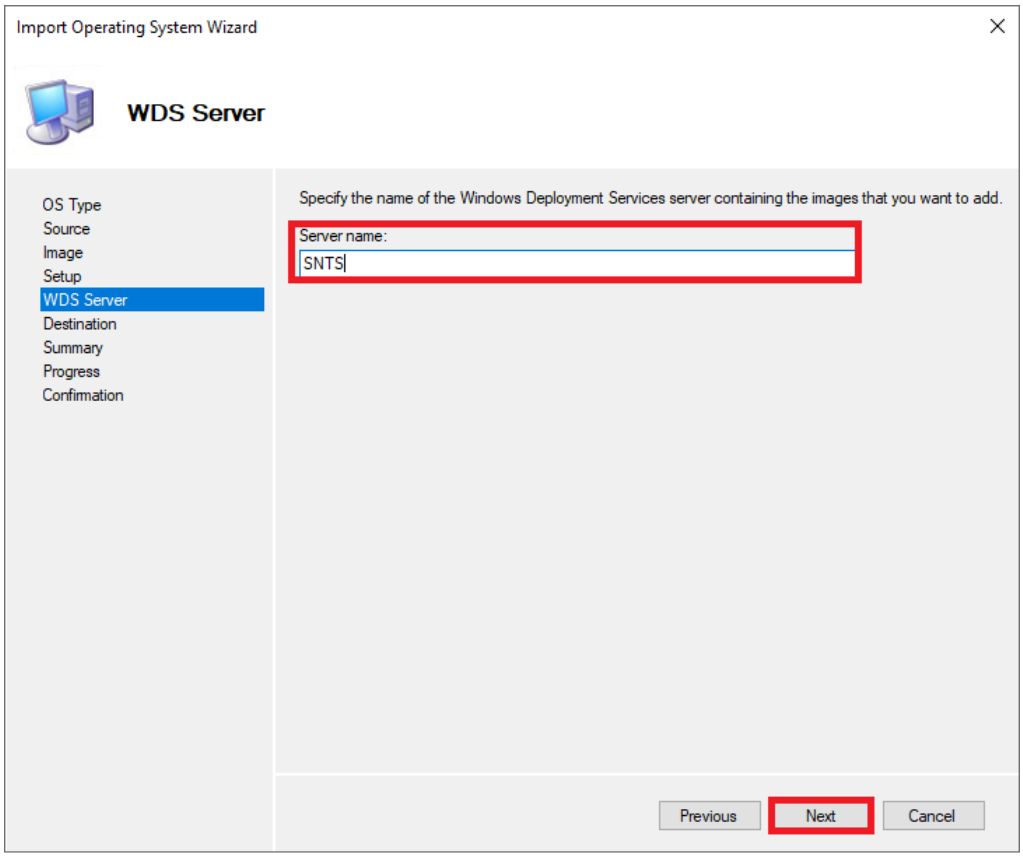
Pour ce faire nous allez retourner sur MDT allez dans l'onglet « **Opertating System** » et faire un clic droit « **Import Operating System** »



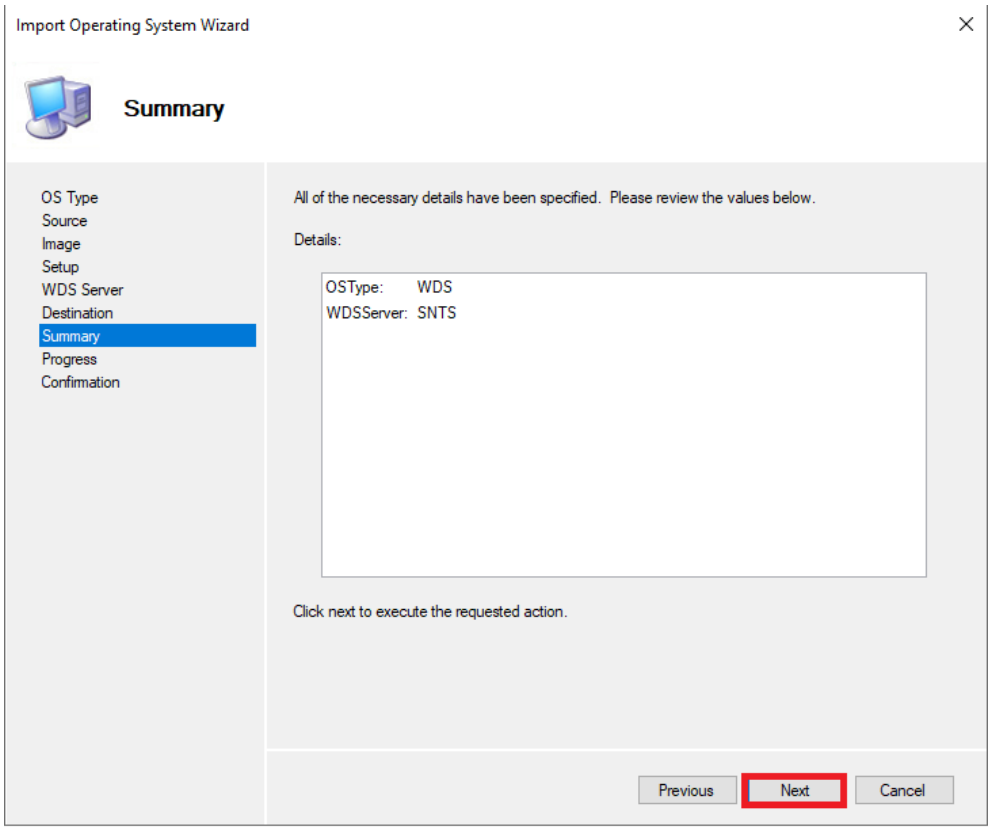
➔ Choisissez la case « **Windows Deployment Services images** » puis faites « **Suivant** »

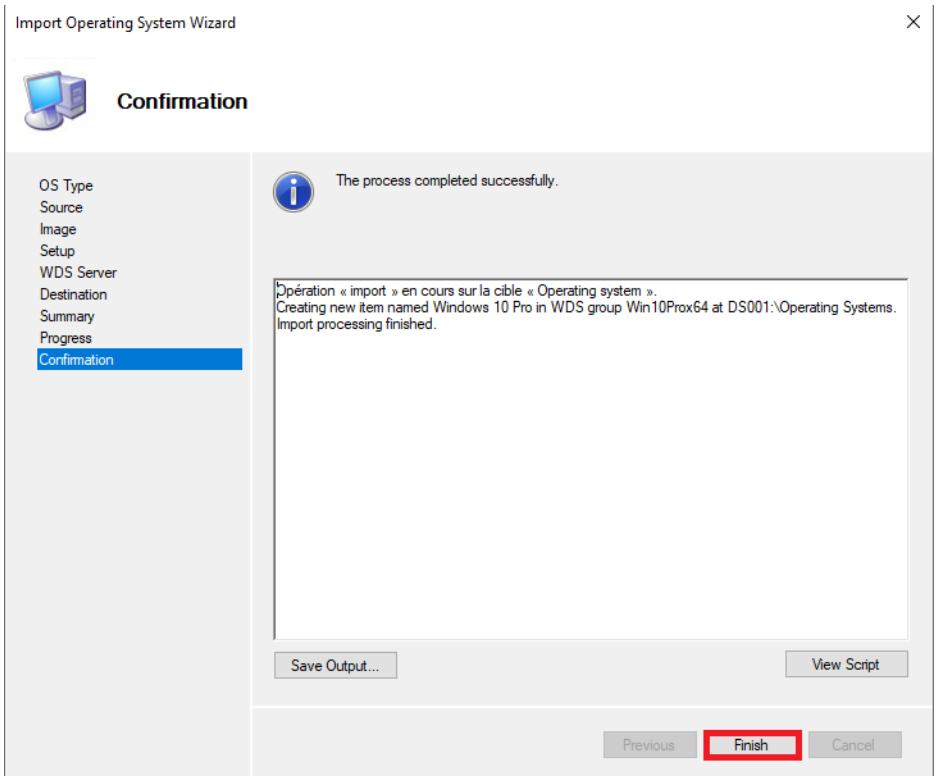


➔ Rentrez le nom du serveur puis faites « **Suivant** »



➔ Faites « **Suivant** »



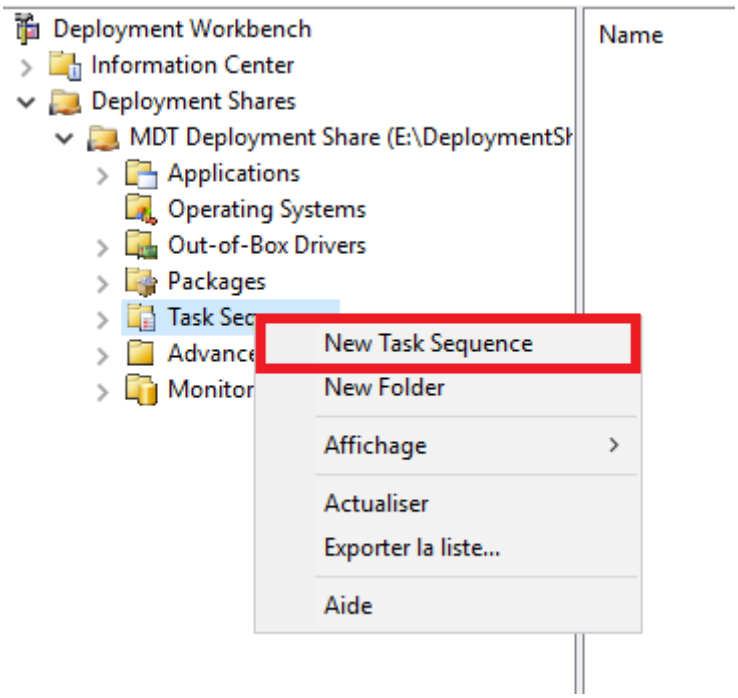


➔ Attendez la fin du chargement puis faites « Terminer »

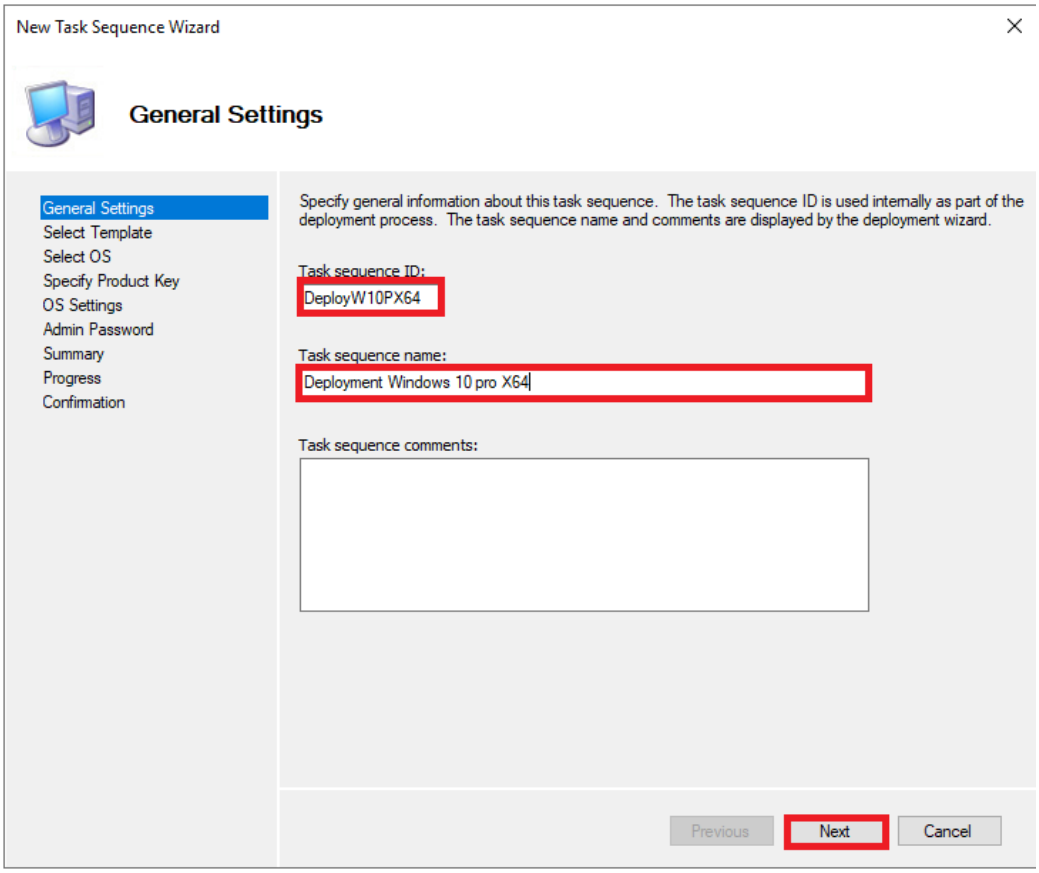
Vous avez maintenant ajouté une image Windows sur MDT.

L'étape suivante est d'ajouter une séquence de tâche sur MDT ; pour ce faire :

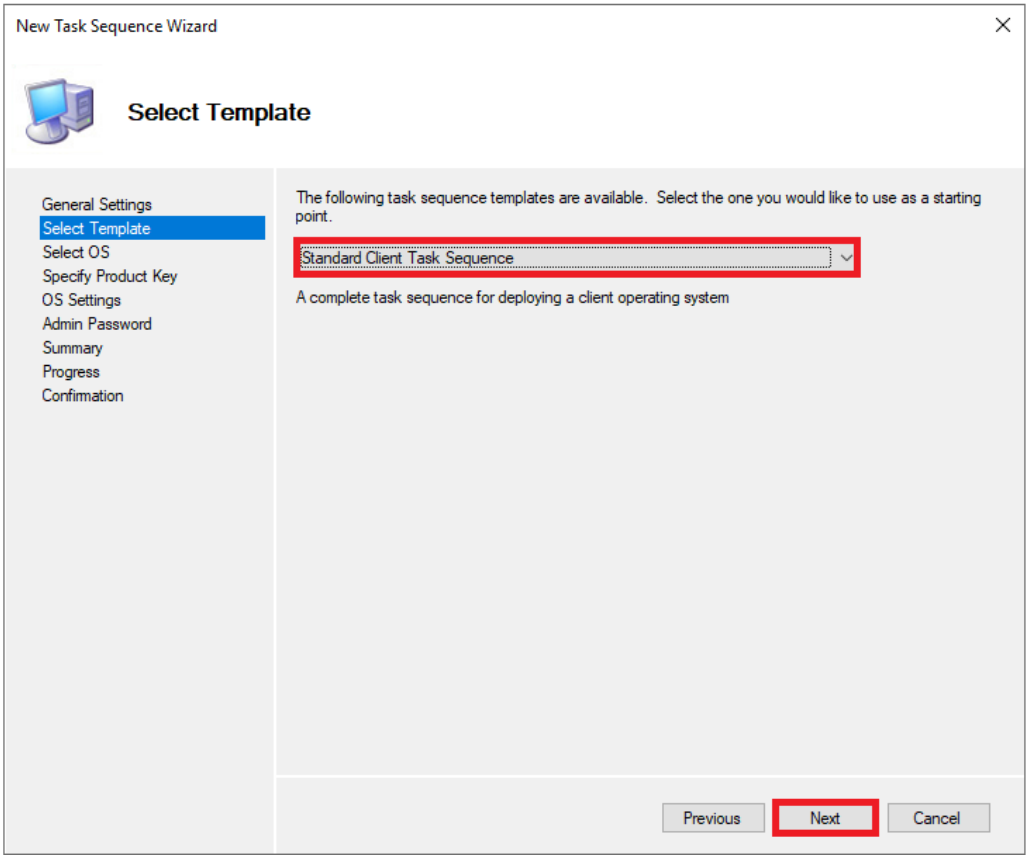
➔ Allez sur MDT dans l'onglet « **Task Sequence** »



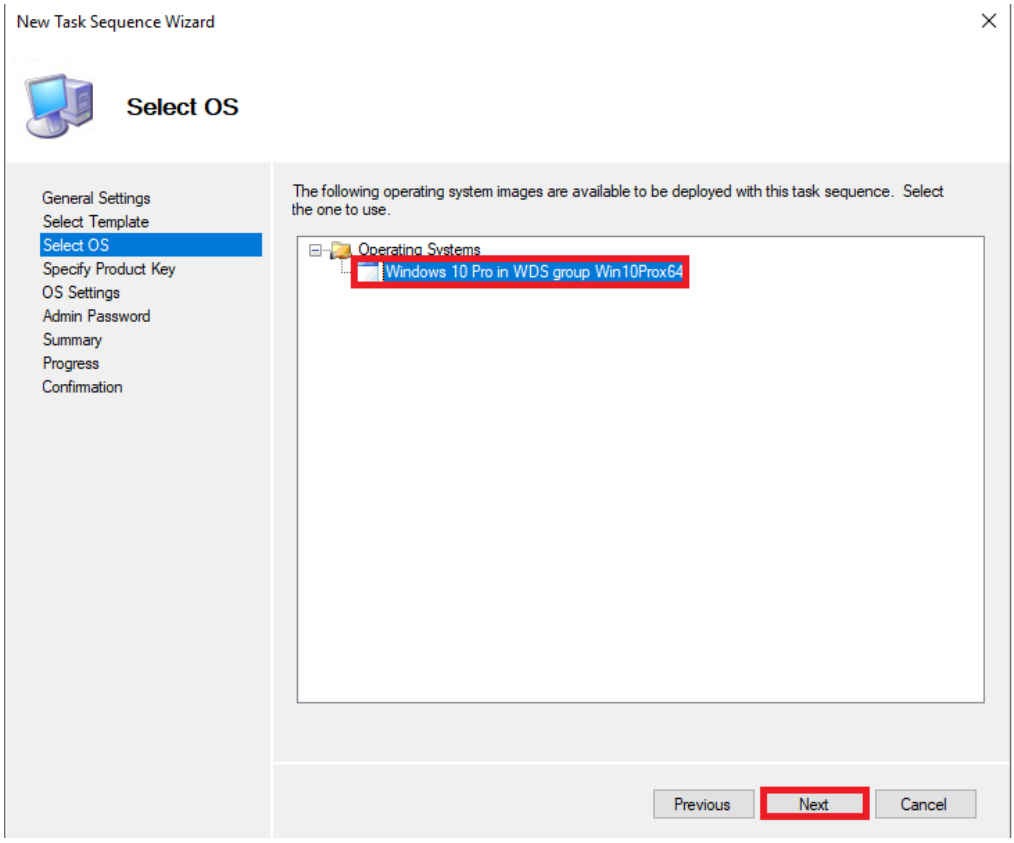
➔ Renseignez une « **Séquence de tâche** » et un « **Nom de séquence** » puis faites « **Suivant** »



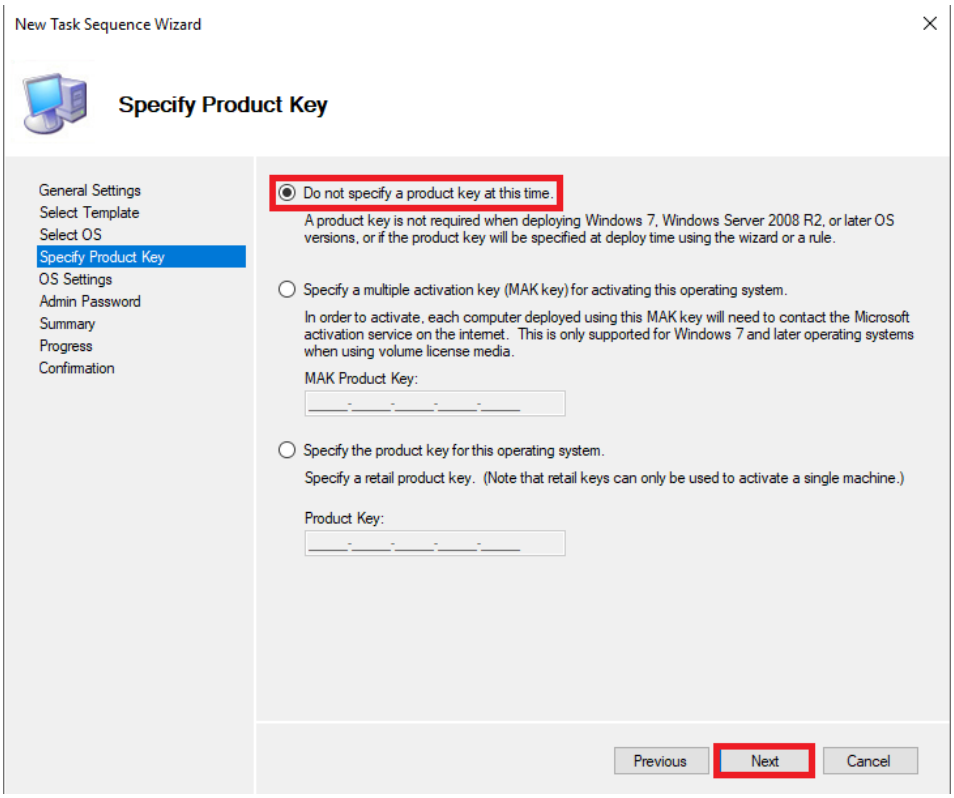
➔ Sélectionnez « **Standard Client Task Sequence** » puis faites « **Suivant** »



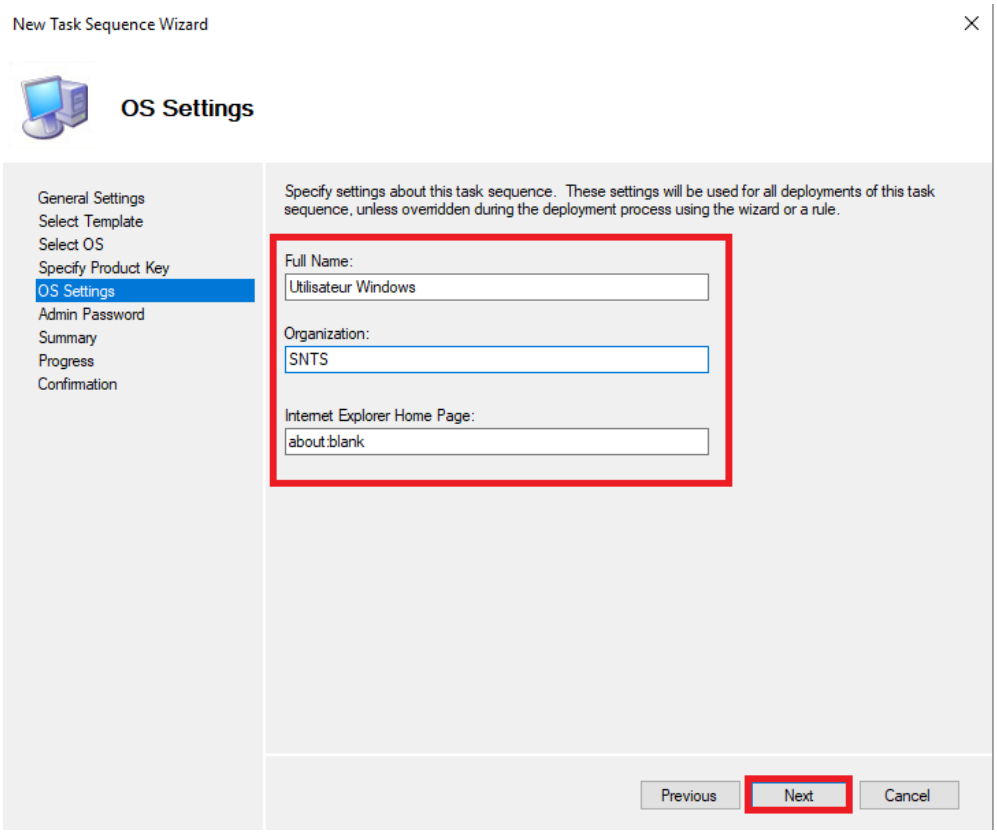
➔ Sélectionnez l'image Windows 10 et faites « **Suivant** »



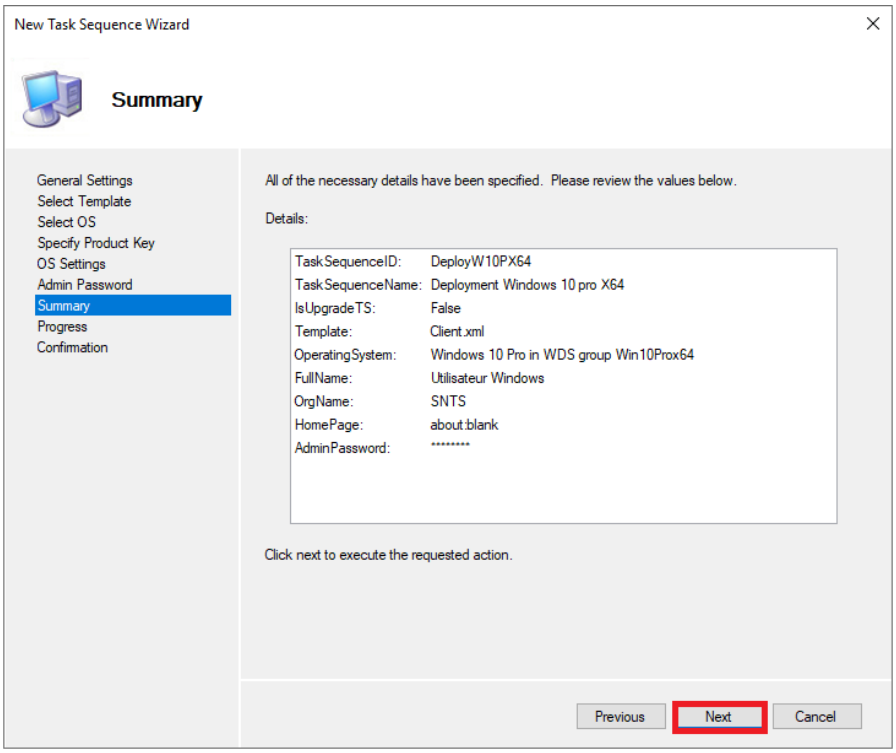
➔ Cochez la première case puis faites « **Suivant** »



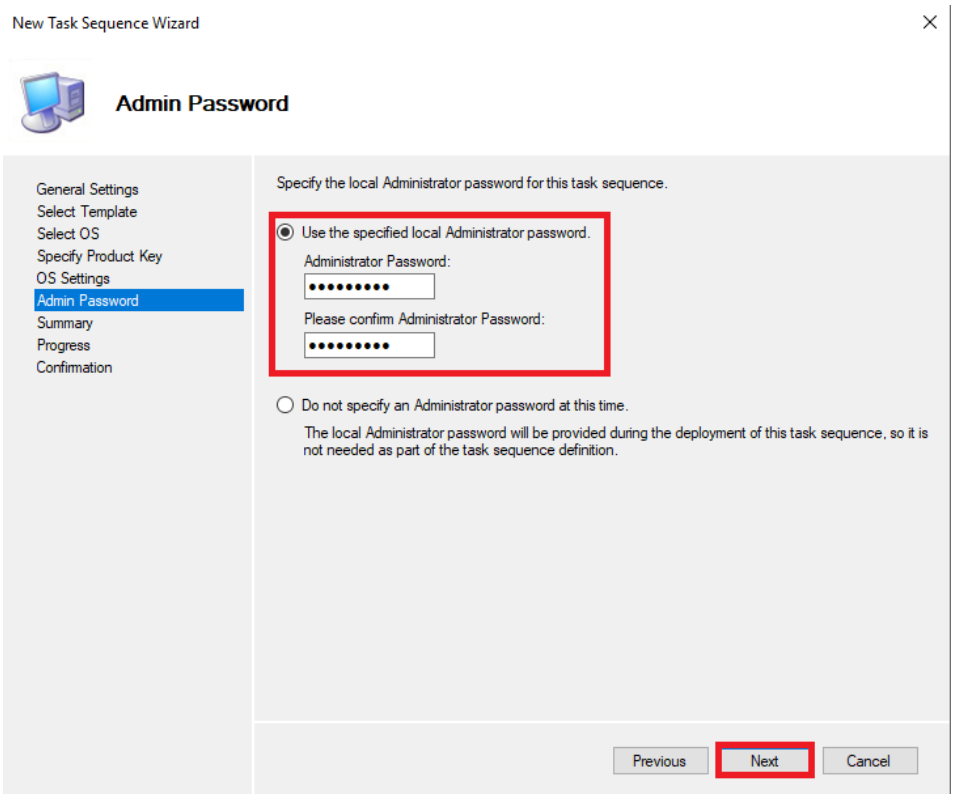
➔ Remplissez les différentes cases comme ci-dessous puis faites « **Suivant** »



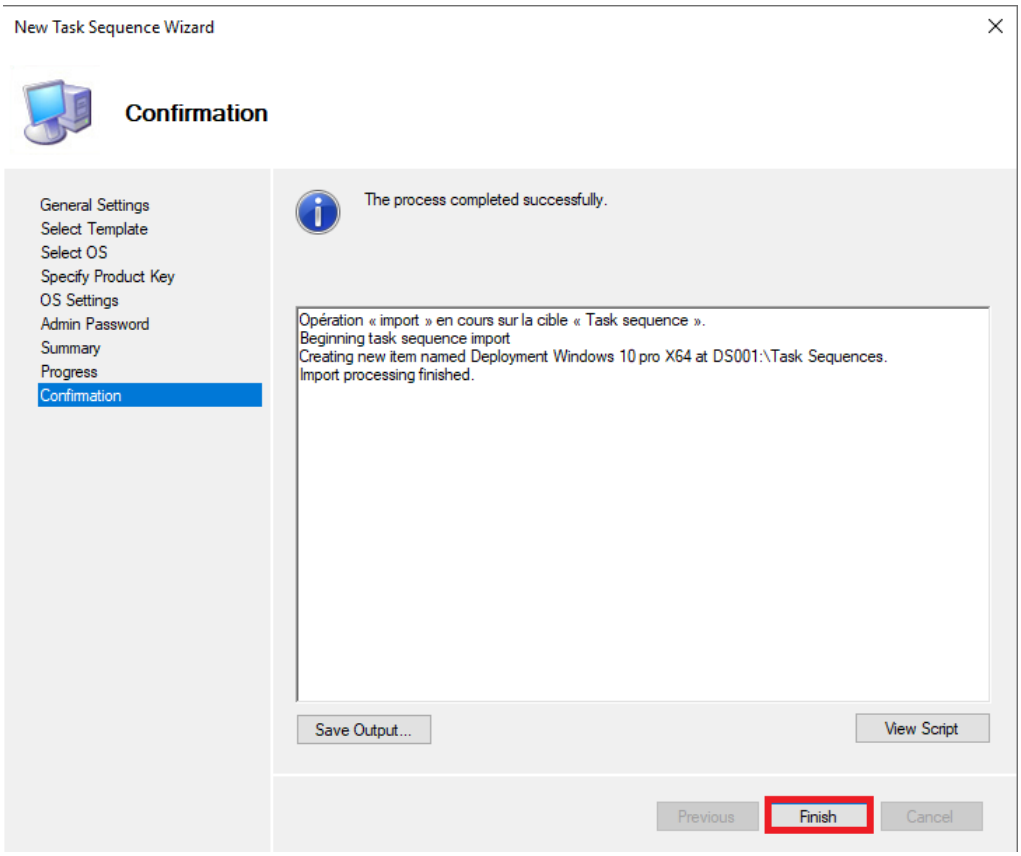
➔ Faites « **Suivant** »



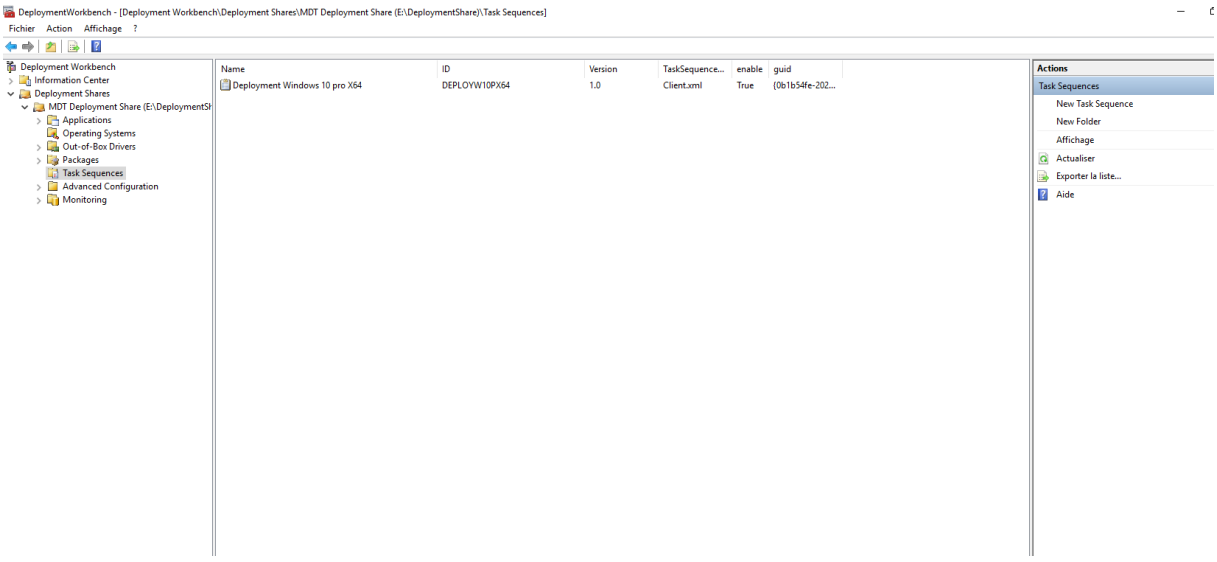
➔ Renseignez un mot de passe admin puis faites « **Suivant** »



➔ Attendez la fin du process puis faites « **Terminer** »



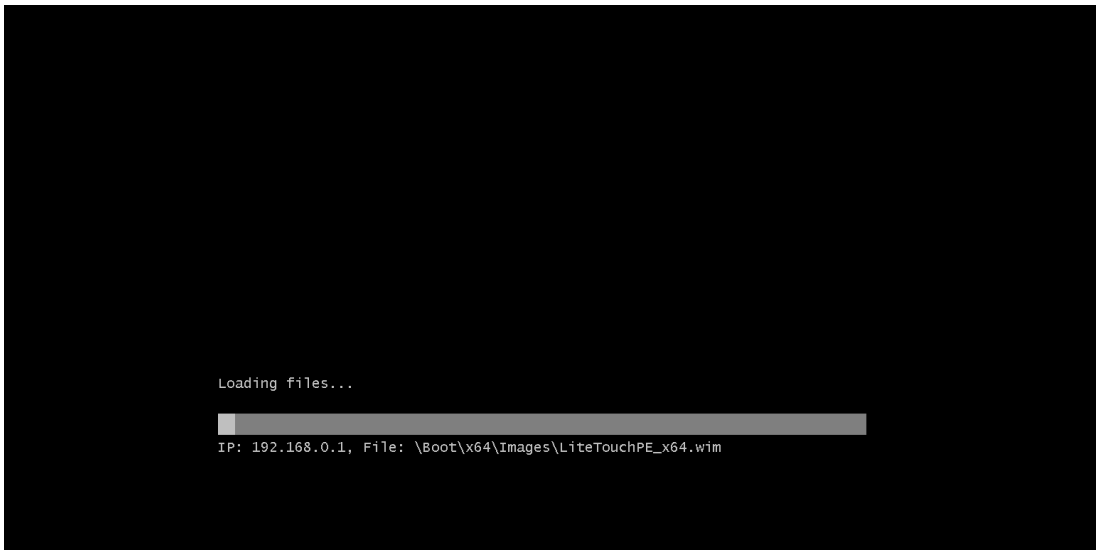
➔ Maintenant votre séquence a été ajoutée.



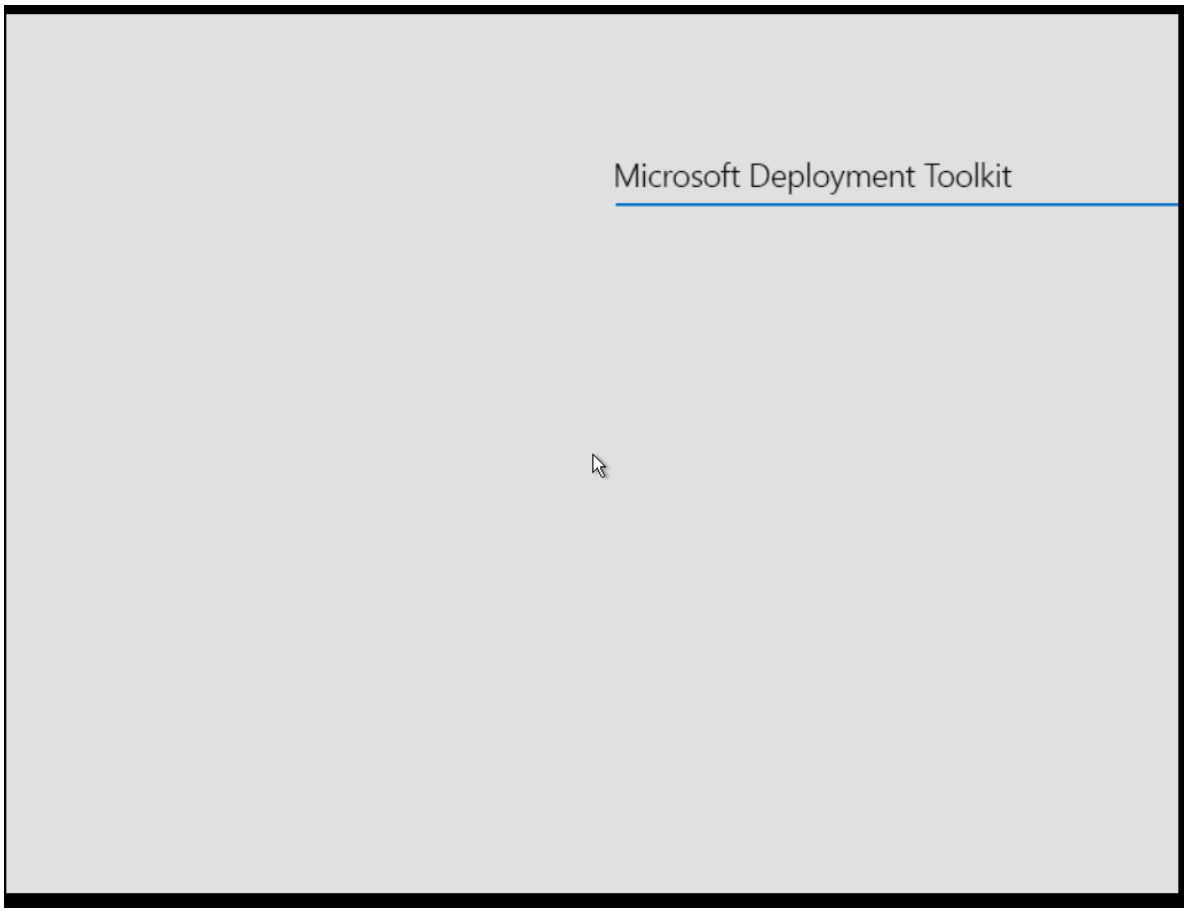
Le master est maintenant opérationnel, nous allons le tester en démarrant une machine sur le réseau.

➔ Une fois que la machine à trouver le DHCP et la Gateway du serveur il faudra appuyer sur F12.

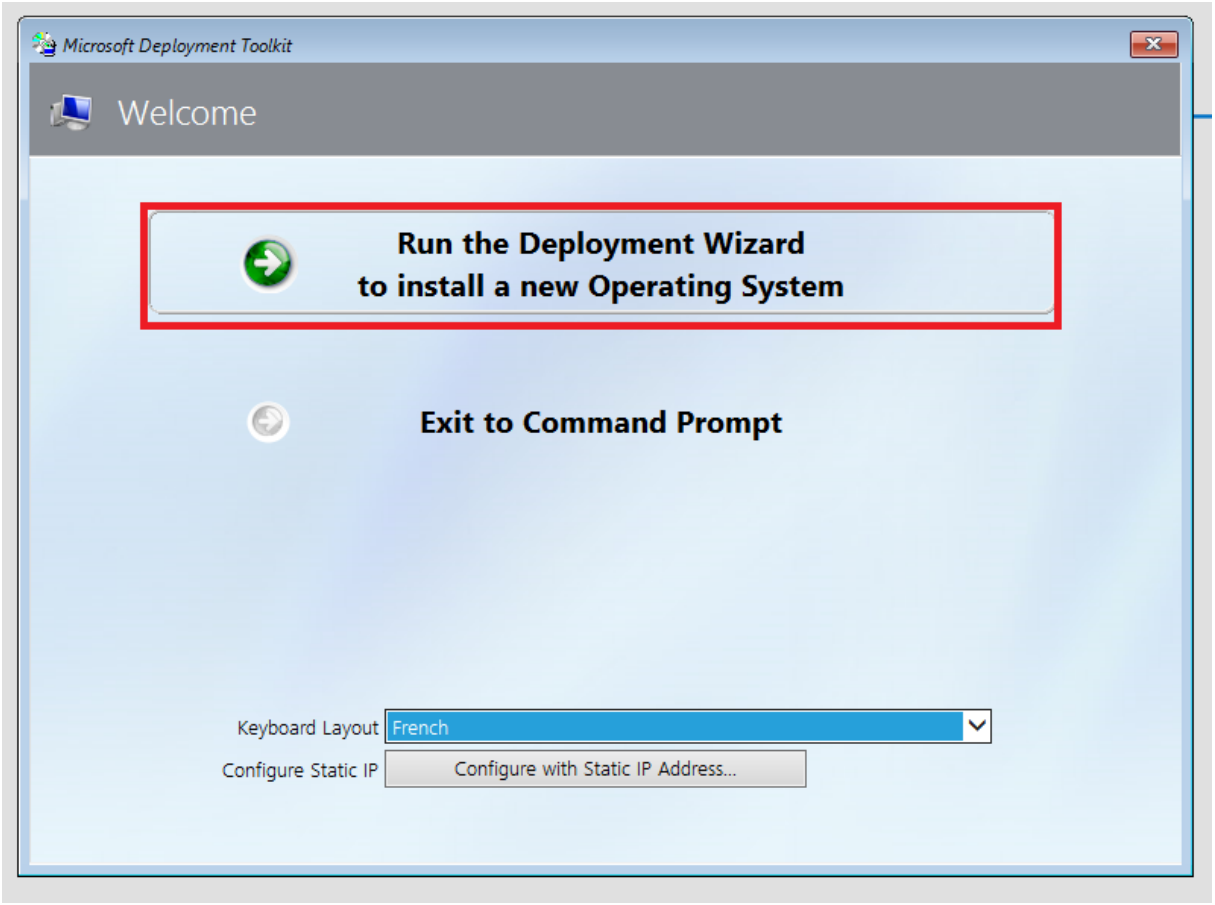
➔ Une fois réalisé vous allez attendre la fin du chargement :



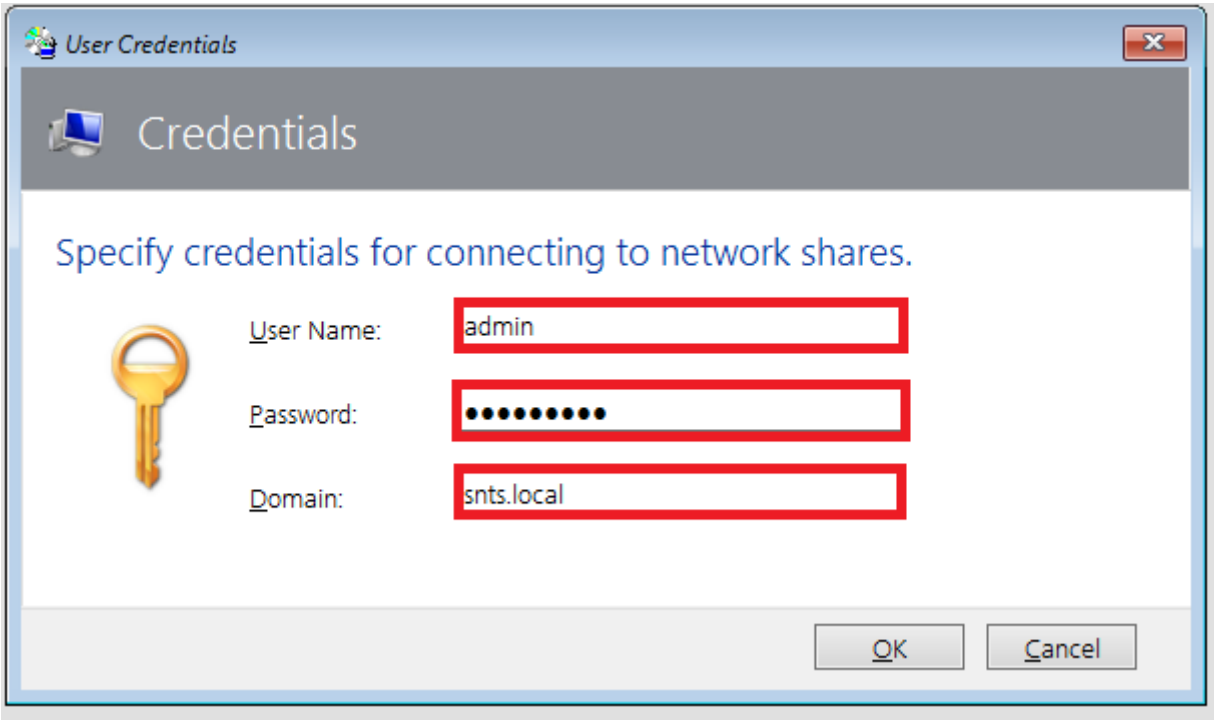
➔ Une fois le téléchargement terminé, vous serez emmené sur la page Microsoft Deployment Toolkit.



➔ Un pop-up apparaitra, cliquez sur la flèche verte.



➔ Rentrez des credentials possédant des droits admins, puis faites « **OK** ».



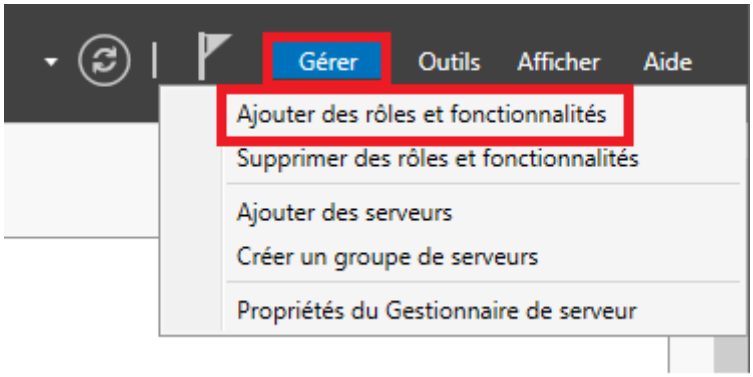
➔ Passez les étapes suivantes pour arriver sur une machine Windows masterisée et opérationnelle.

II. Installation et configuration du WSUS

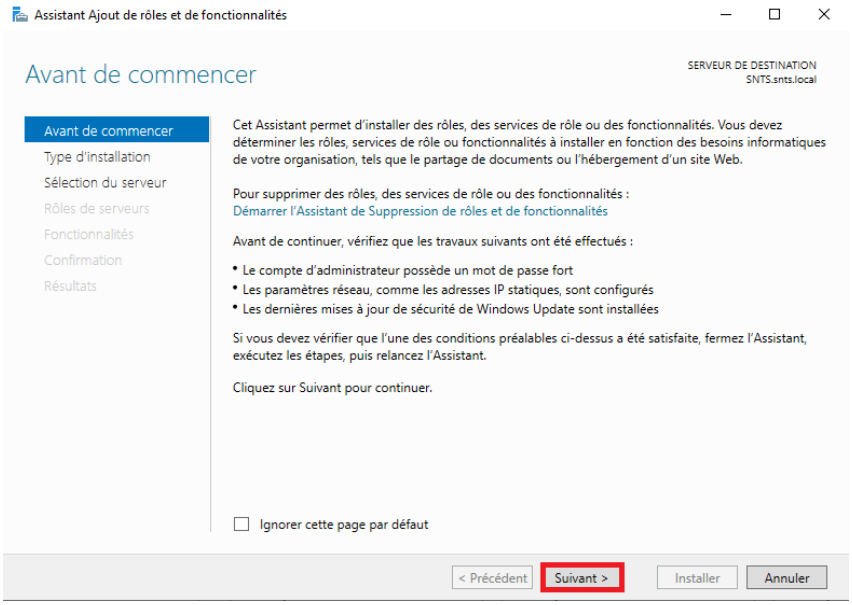
Pour l'installation de WSUS nous allons voir dans un premier temps, comment installer le rôle via le gestionnaire de serveur :

Pour ce faire, il faut :

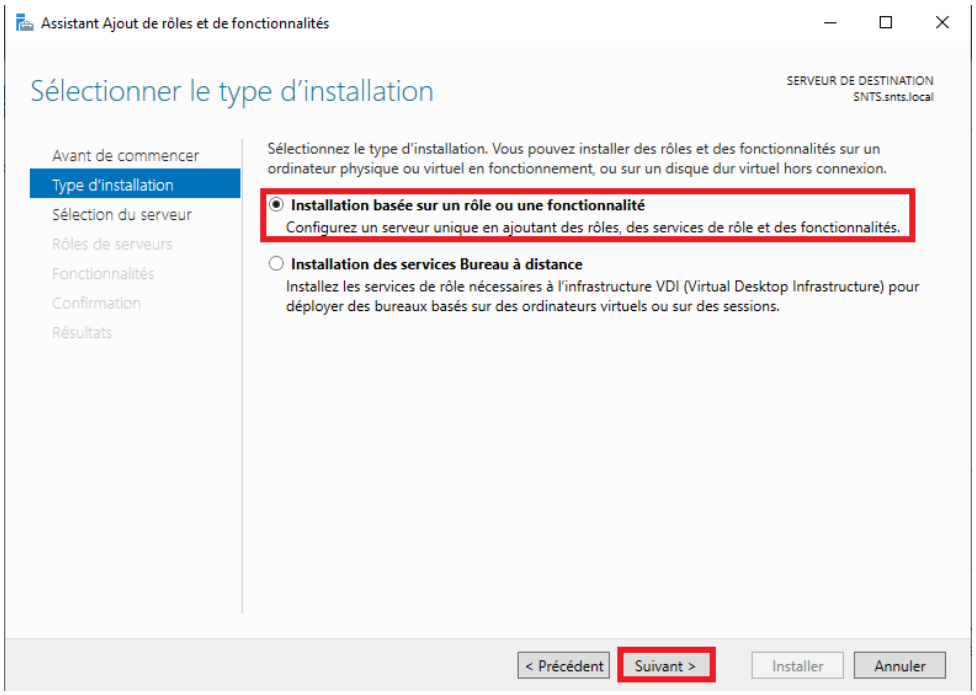
➔ Allez dans « **Gérer** » en haut à droite du gestionnaire et faire « **Ajouter des rôles et fonctionnalités** ».



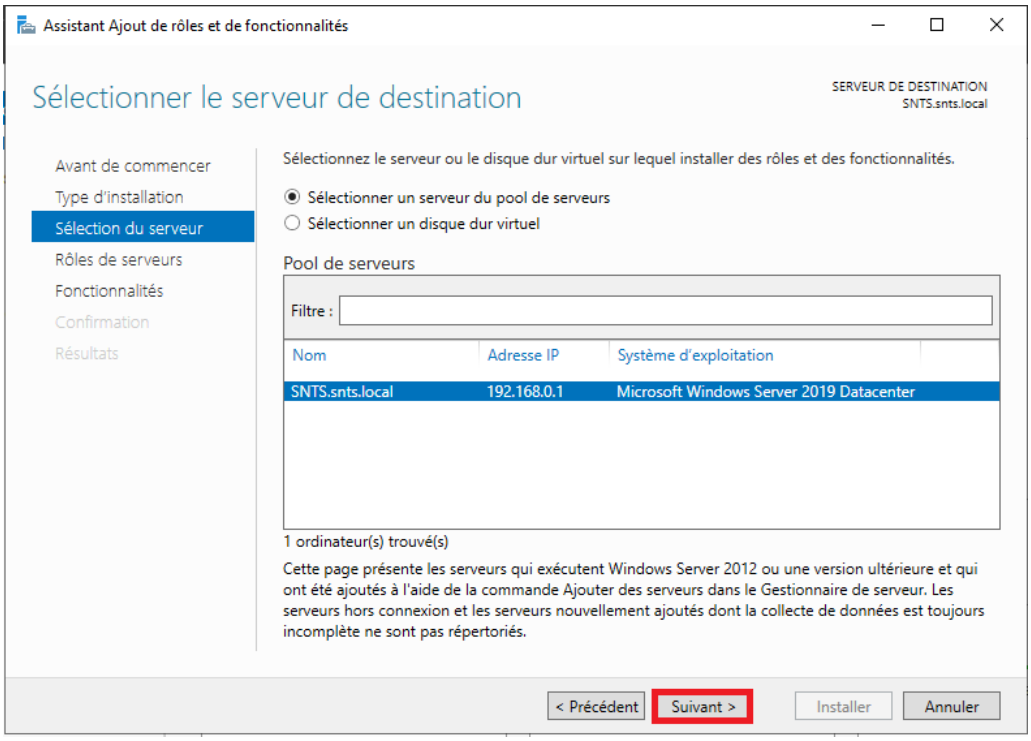
➔ Ensuite faites « **Suivant** ».



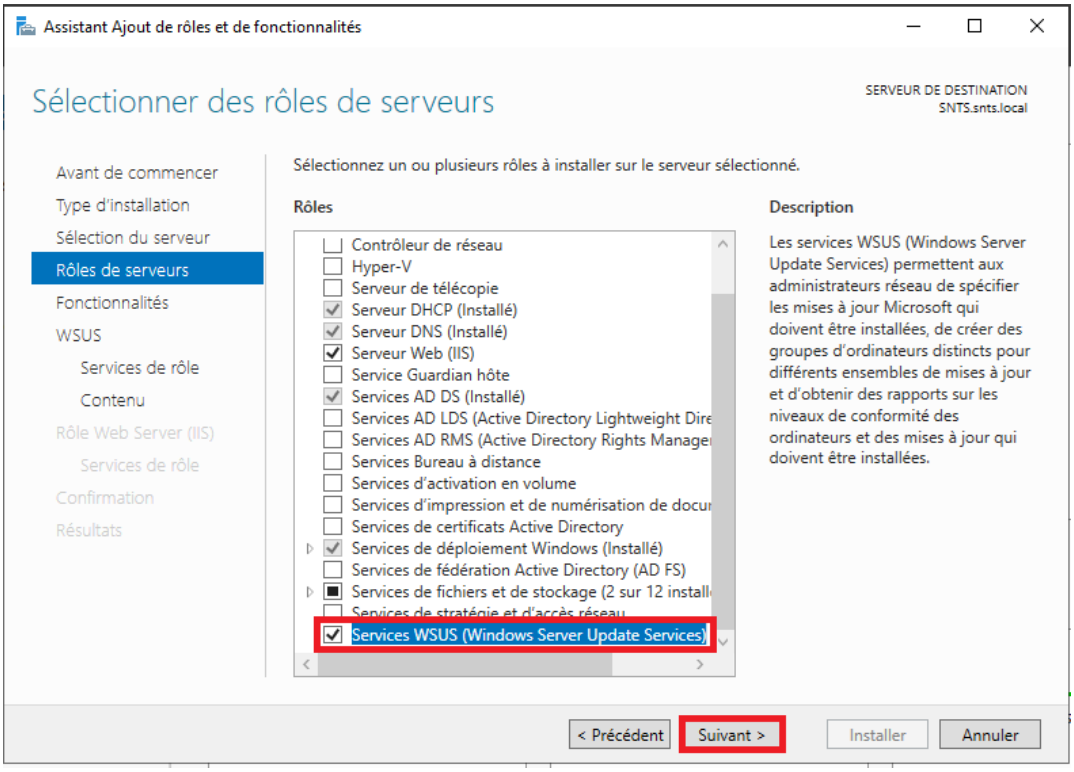
➔ Cochez la première case puis faites « **Suivant** ».



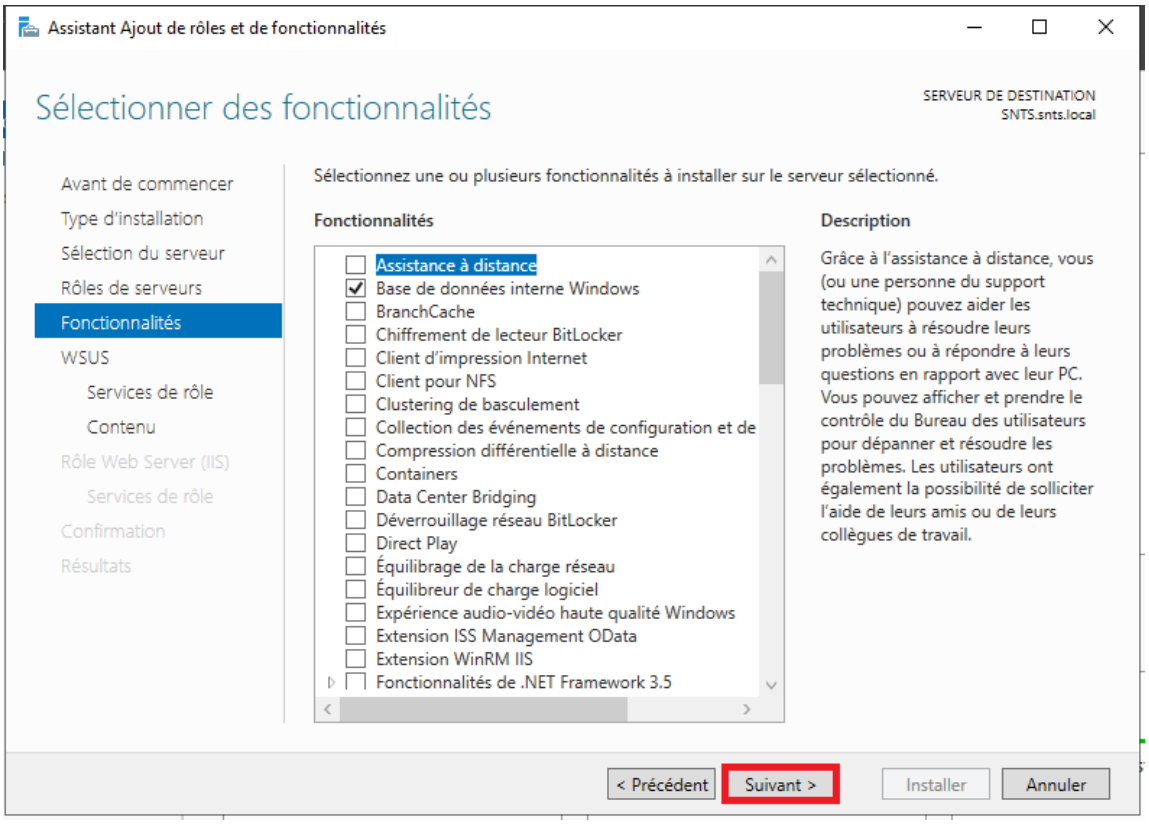
➔ Faites « **Suivant** ».



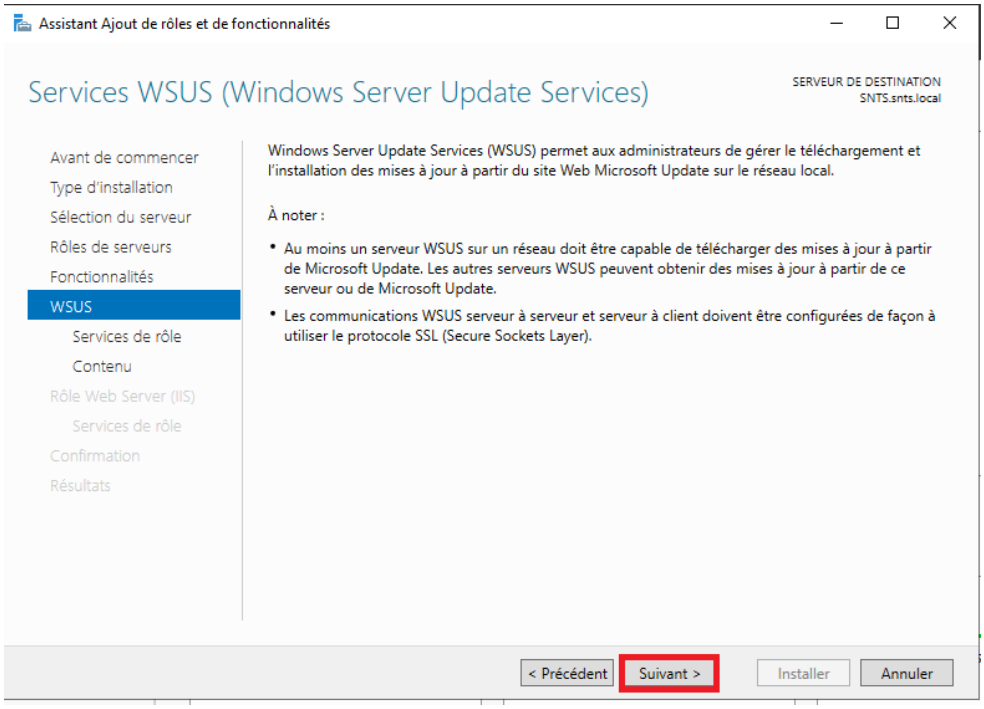
➔ Sélectionnez le service WSUS puis faites « **Suivant** ».



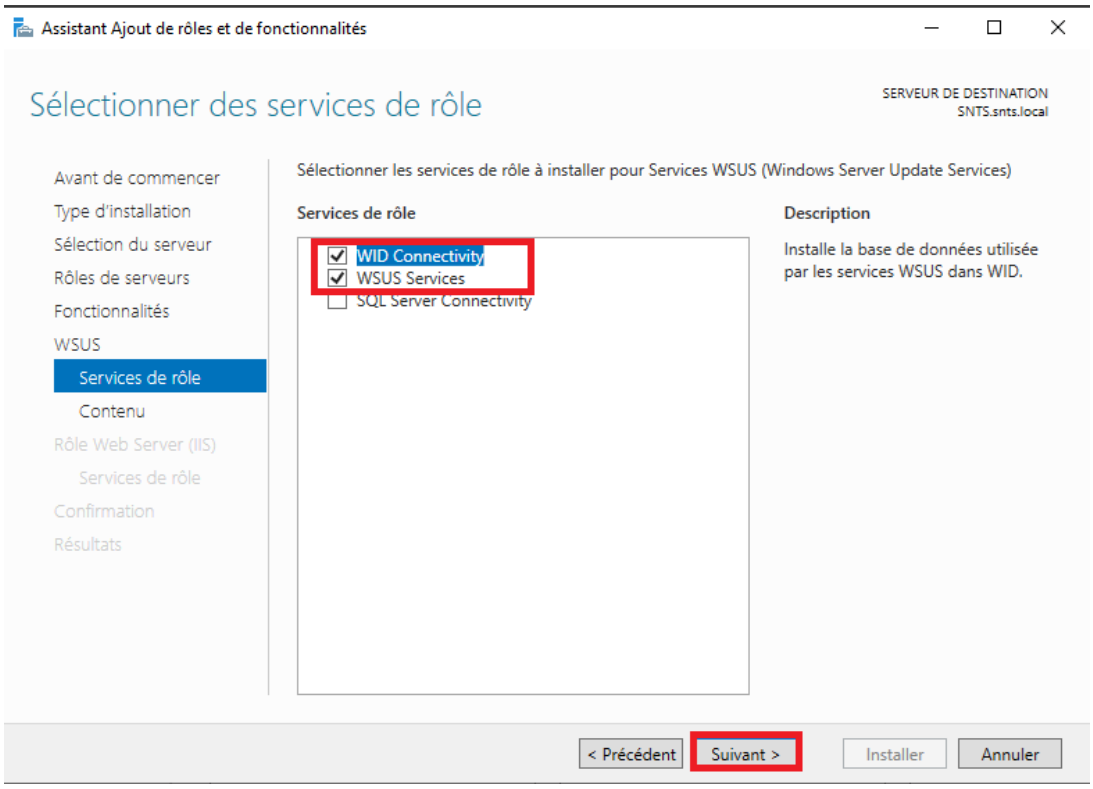
➔ Faites « **Suivant** ».



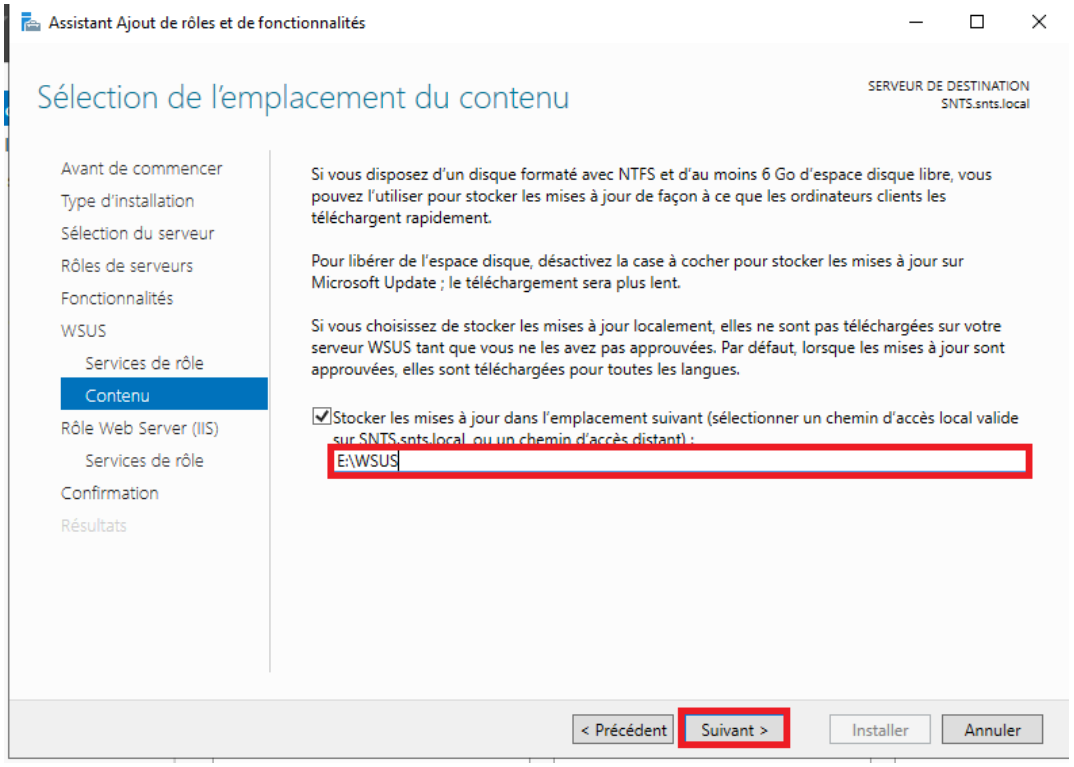
➔ Faites « **Suivant** ».



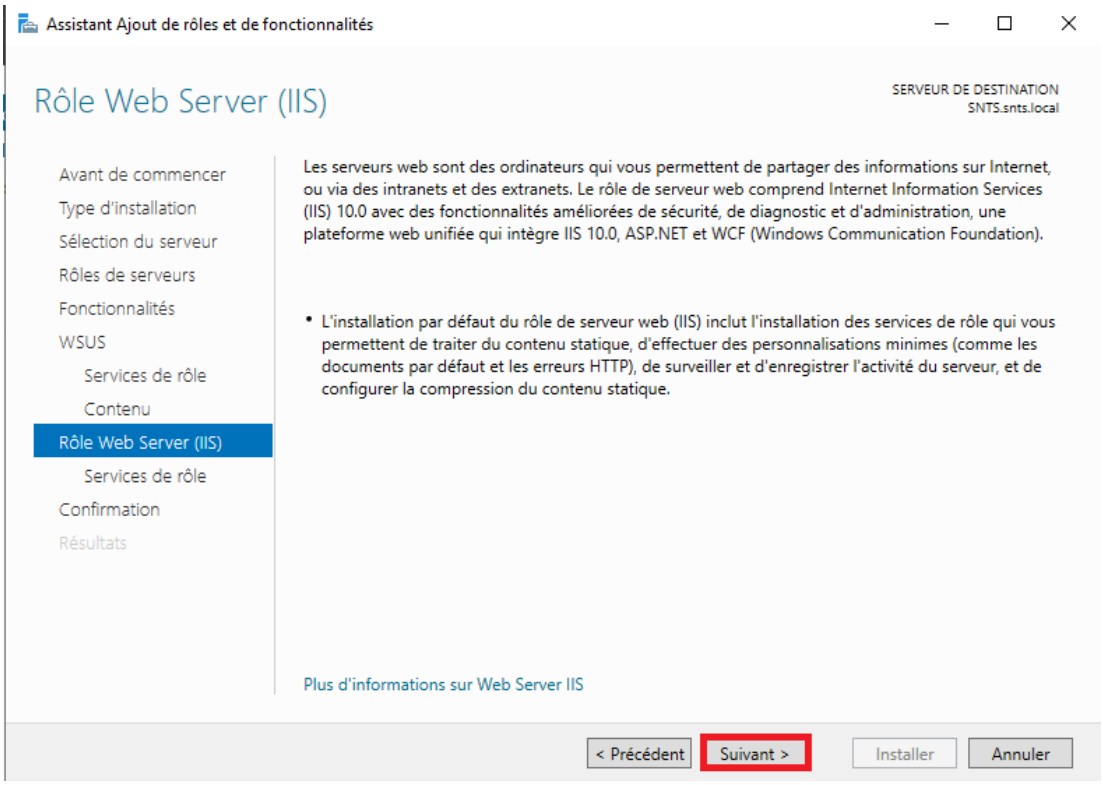
➔ Cochez les 2 premières cases puis faites « **Suivant** ».



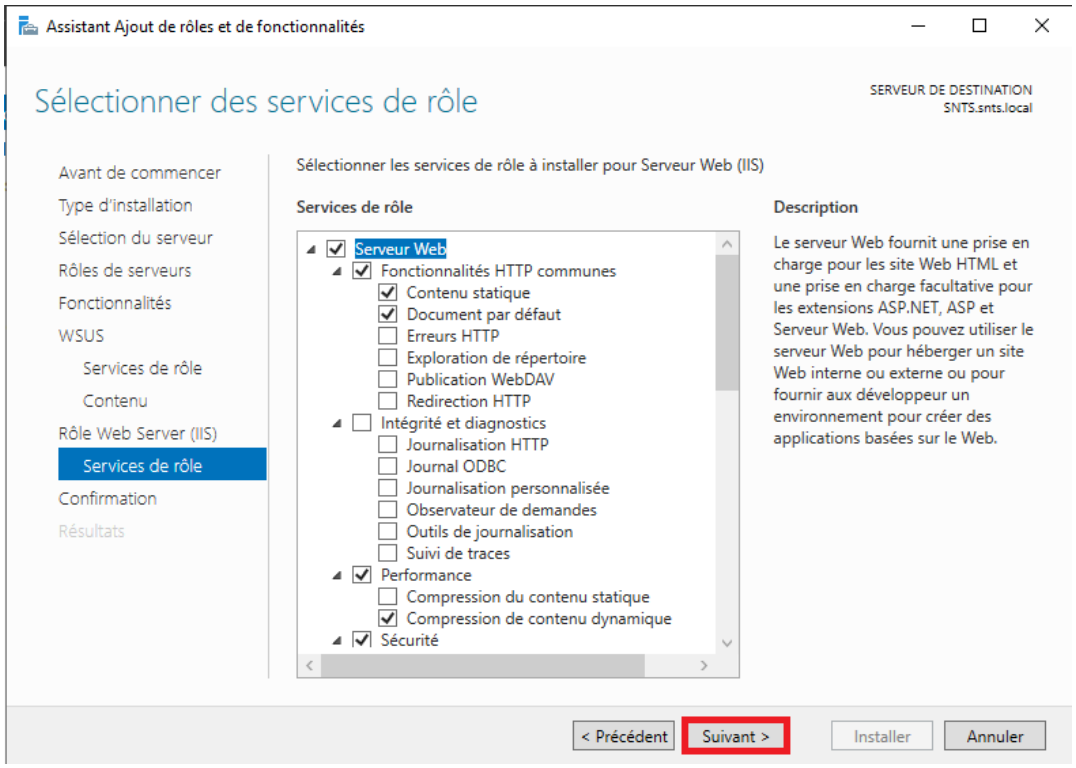
➔ Choisissez un chemin d'accès sur le serveur, dans notre exemple nous allons le placer sur un disque E : installé au préalable puis faites « **Suivant** ».



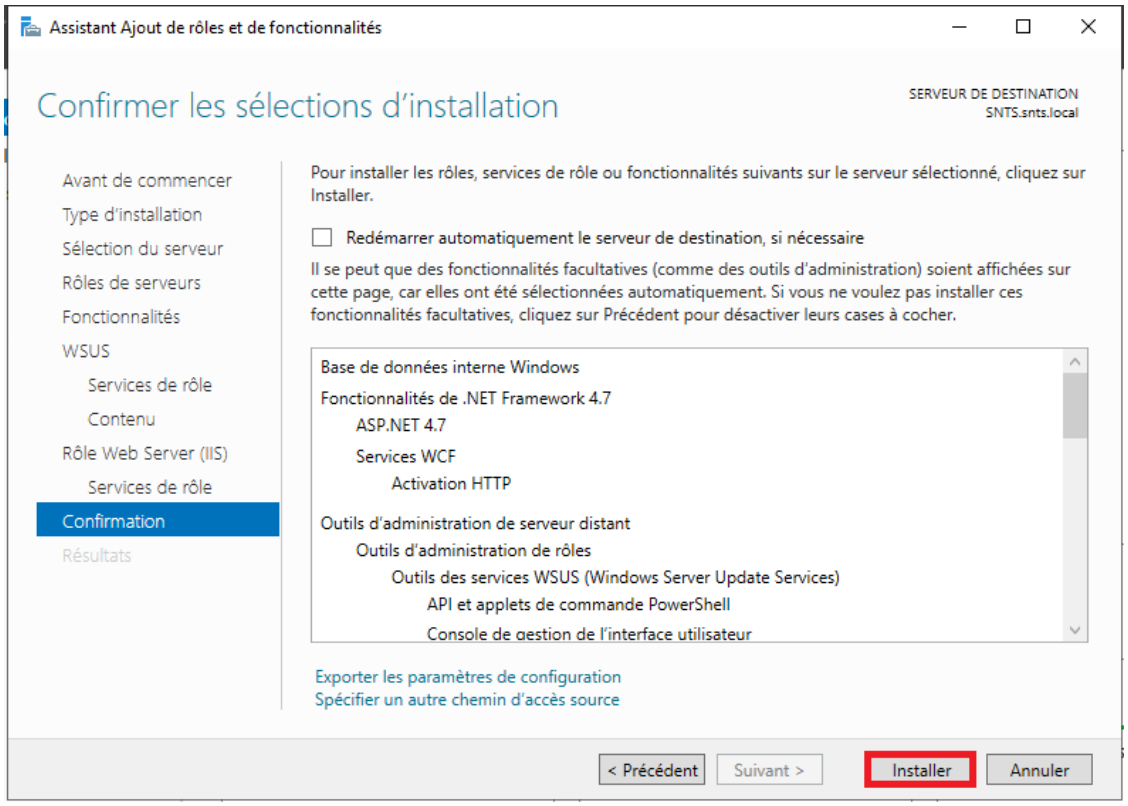
➔ Faites « **Suivant** ».



➔ Faites « **Suivant** ».

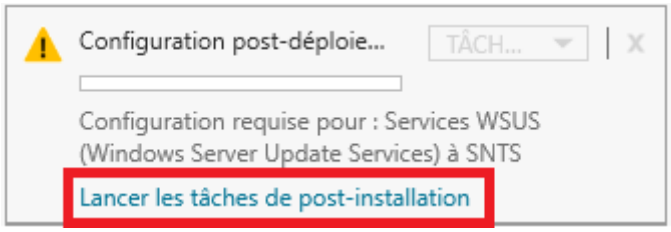


➔ Faites « **Installer** ».

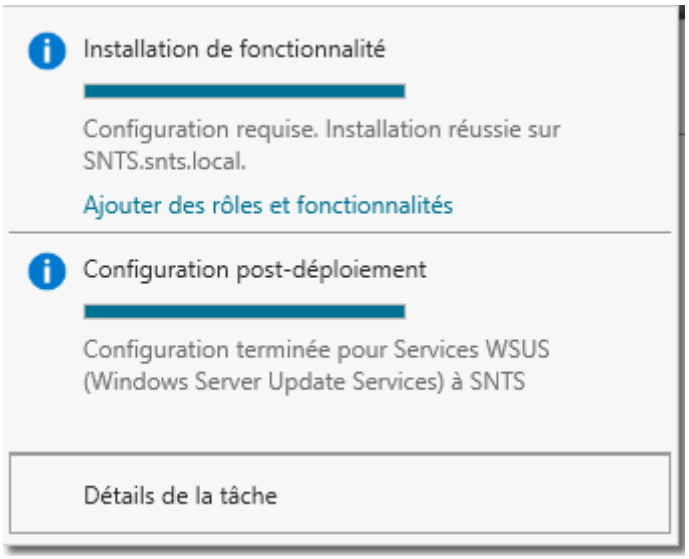


Pour finir l'installation du rôle WSUS ;

➔ Retournez sur le gestionnaire de serveur
➔ Cliquez sur le drapeau en haut à droite
➔ Faites « **Lancer les tâches de post-installation** ».



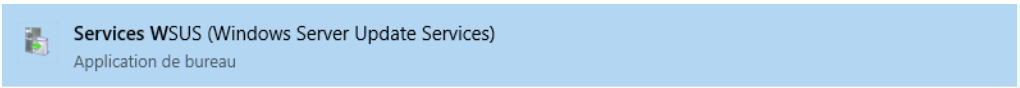
WSUS est installé sur le serveur.



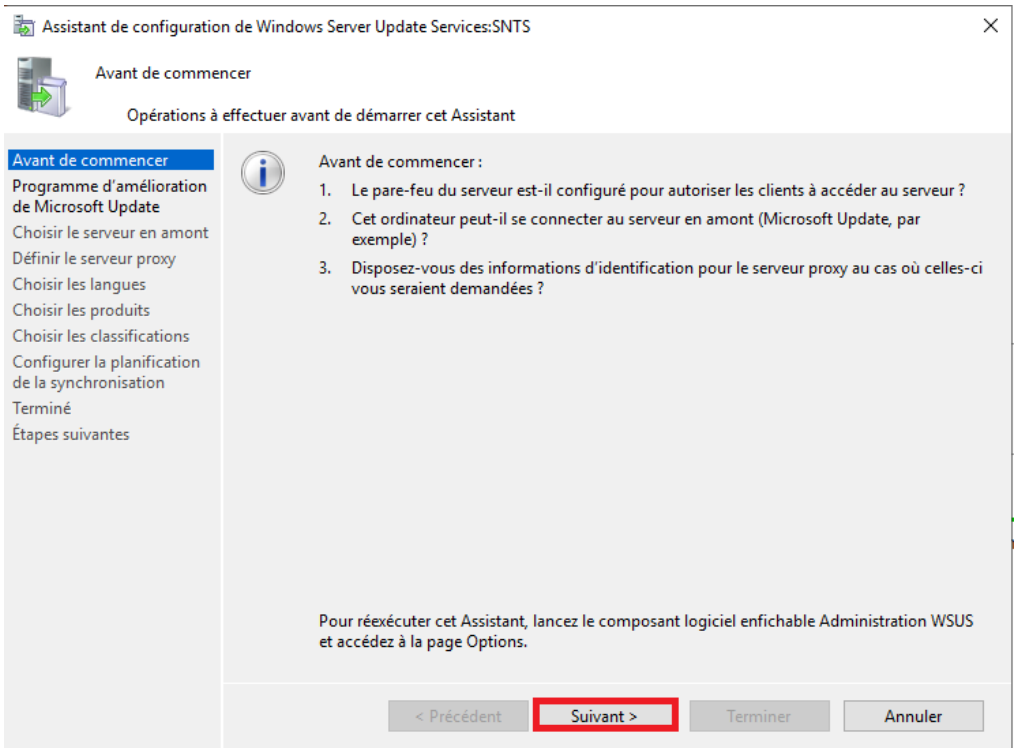
Maintenant nous allons passer à la configuration de WSUS pour notre serveur.

Pour cela il faut :

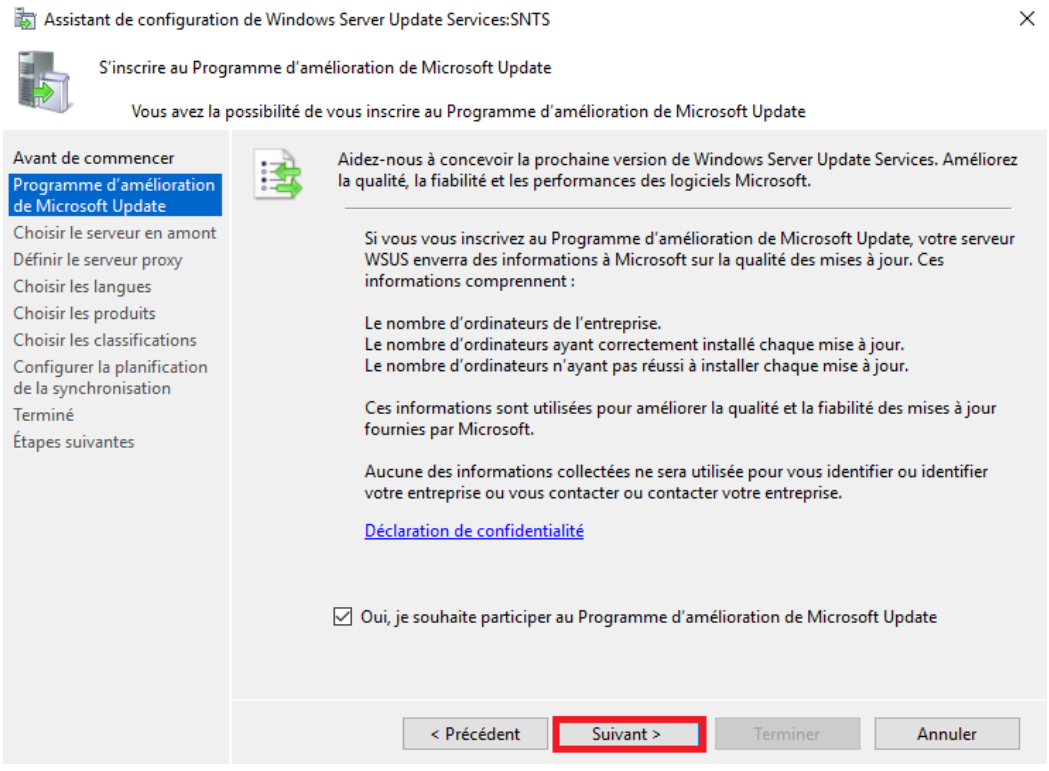
➔ Lancez la console « **Services WSUS** » :



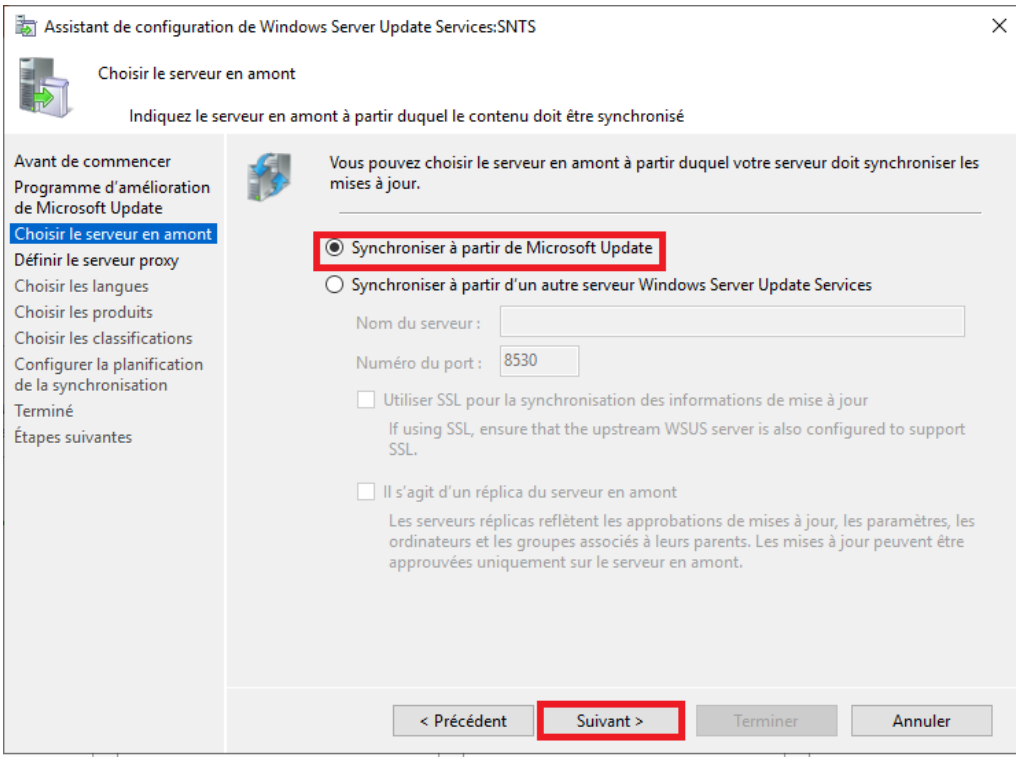
➔ Une fois lancé, une page d'assistance s'ouvrira, faites « Suivant ».



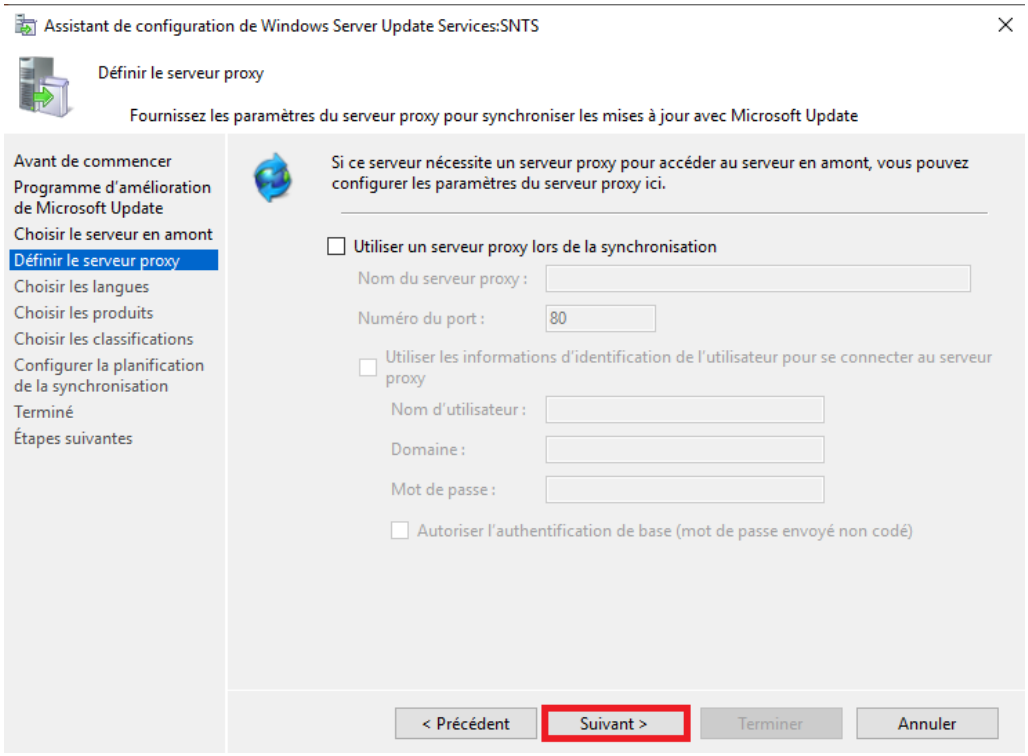
➔ Faites « Suivant ».



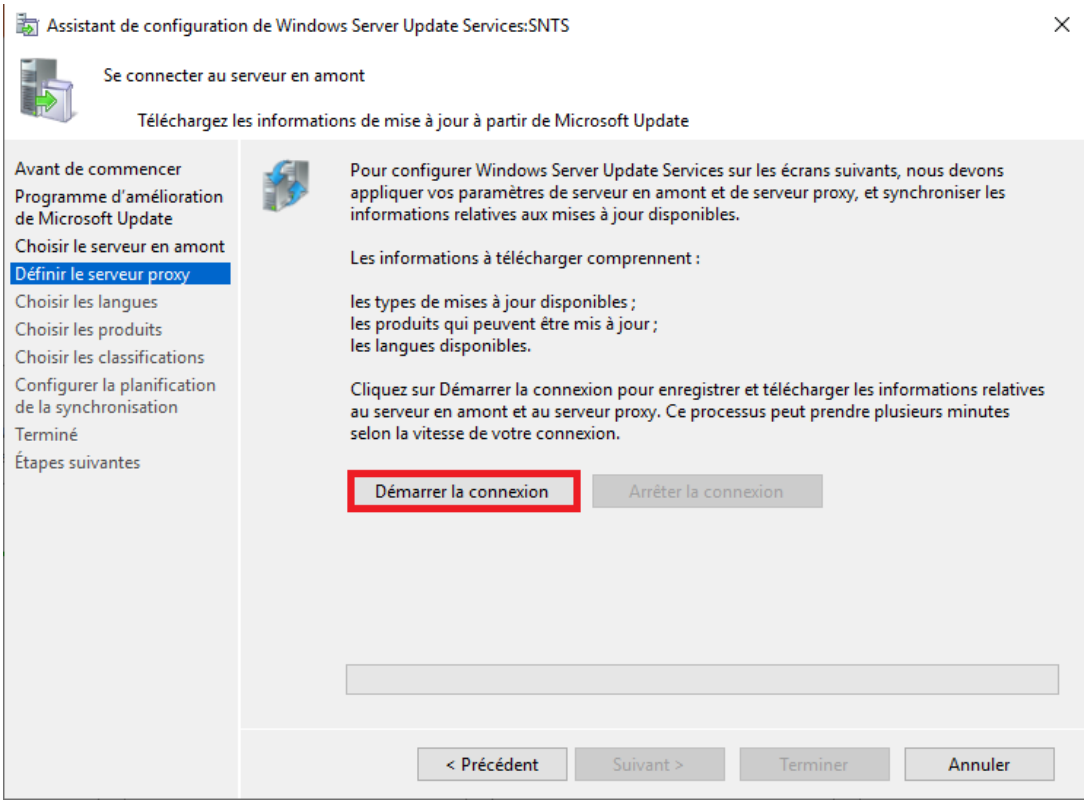
➔ Cochez la première case puis faites « Suivant ».



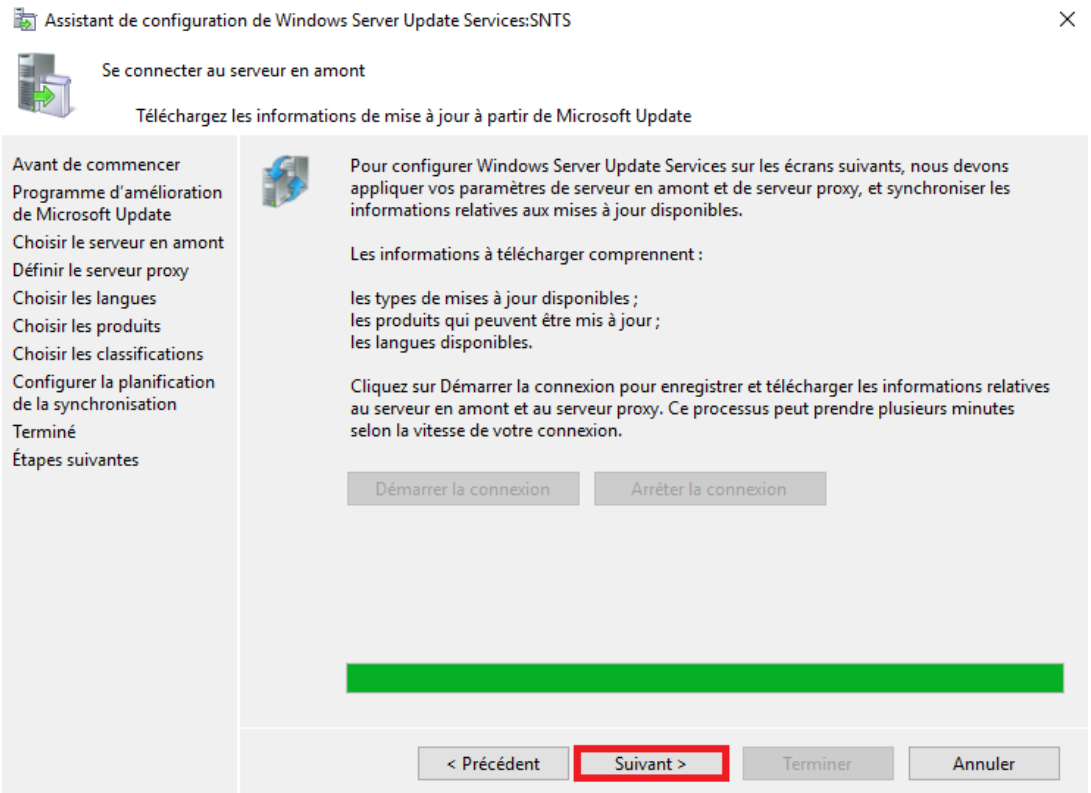
➔ Faites « Suivant ».



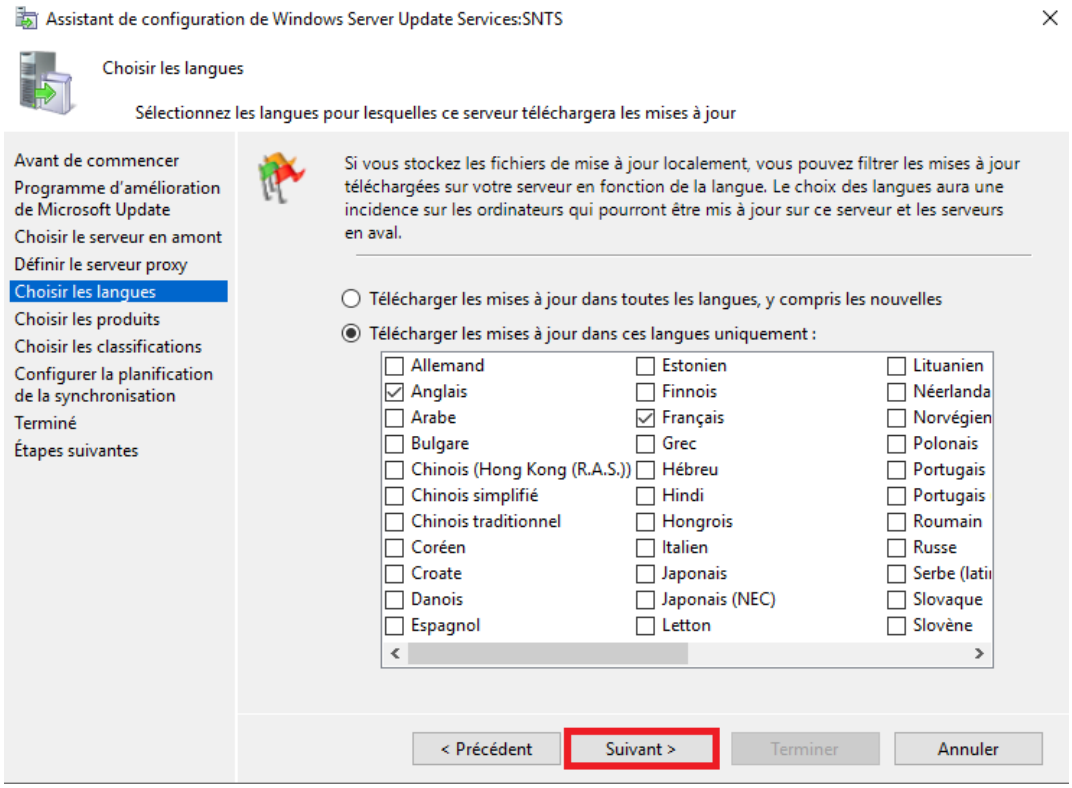
➔ Cliquez sur « **Démarrer la connexion** » puis patientez.



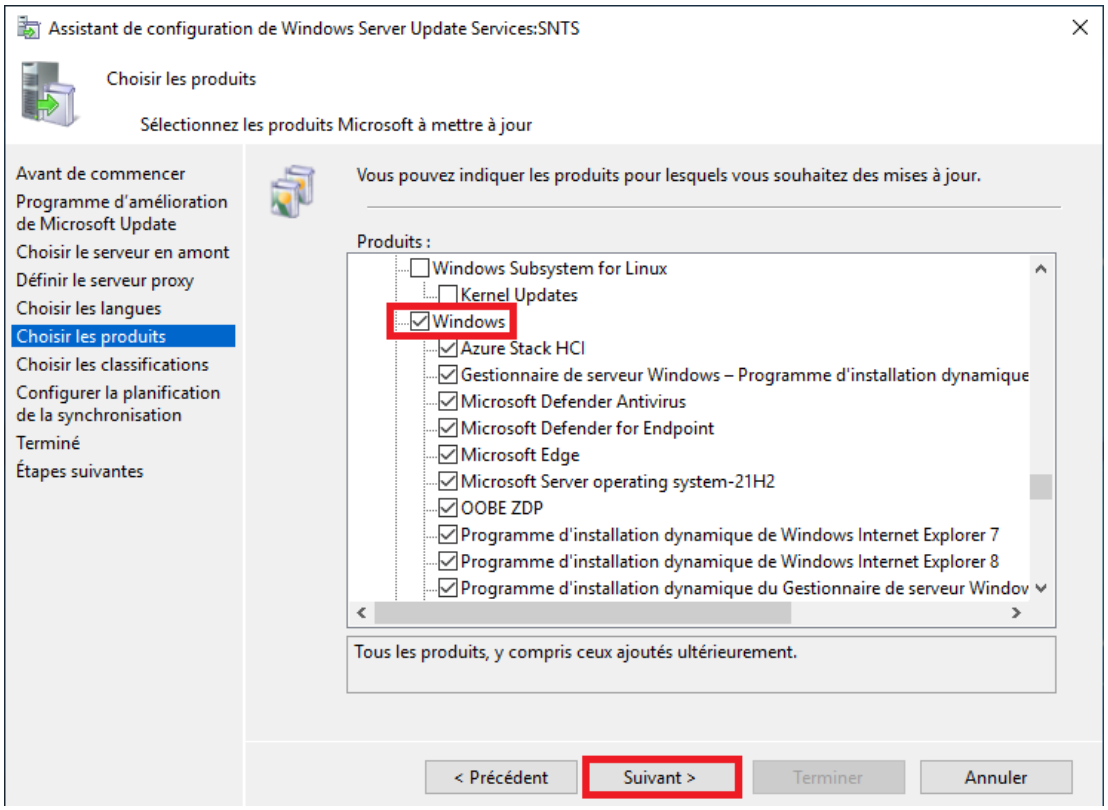
➔ A la fin du téléchargement faites « **Suivant** ».



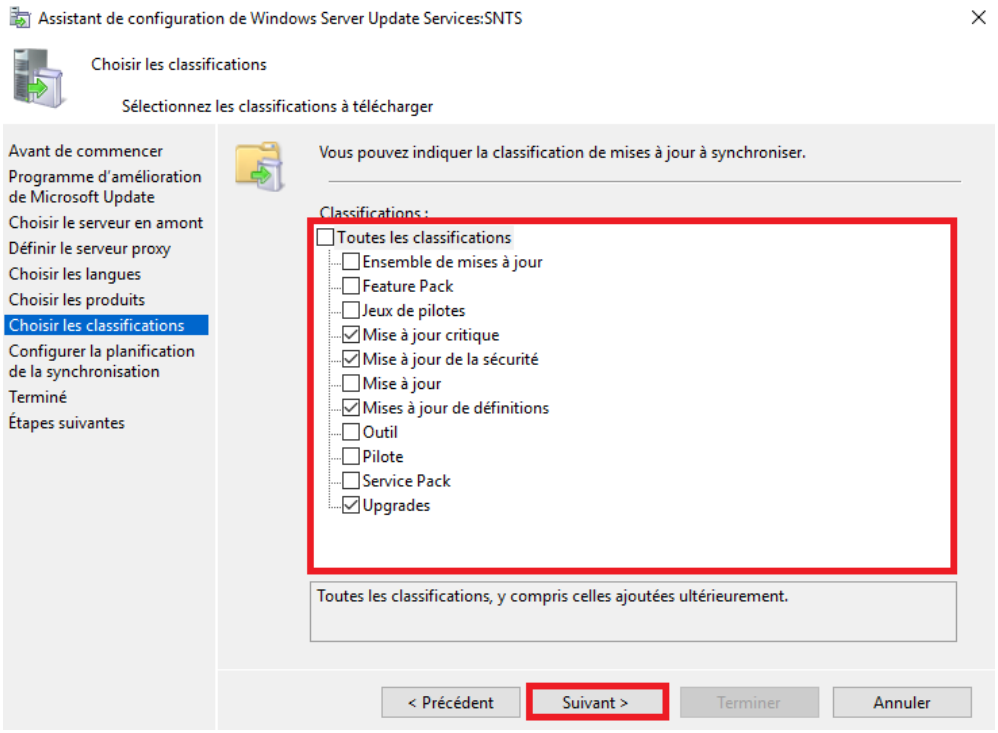
➔ Faites « **Suivant** ».



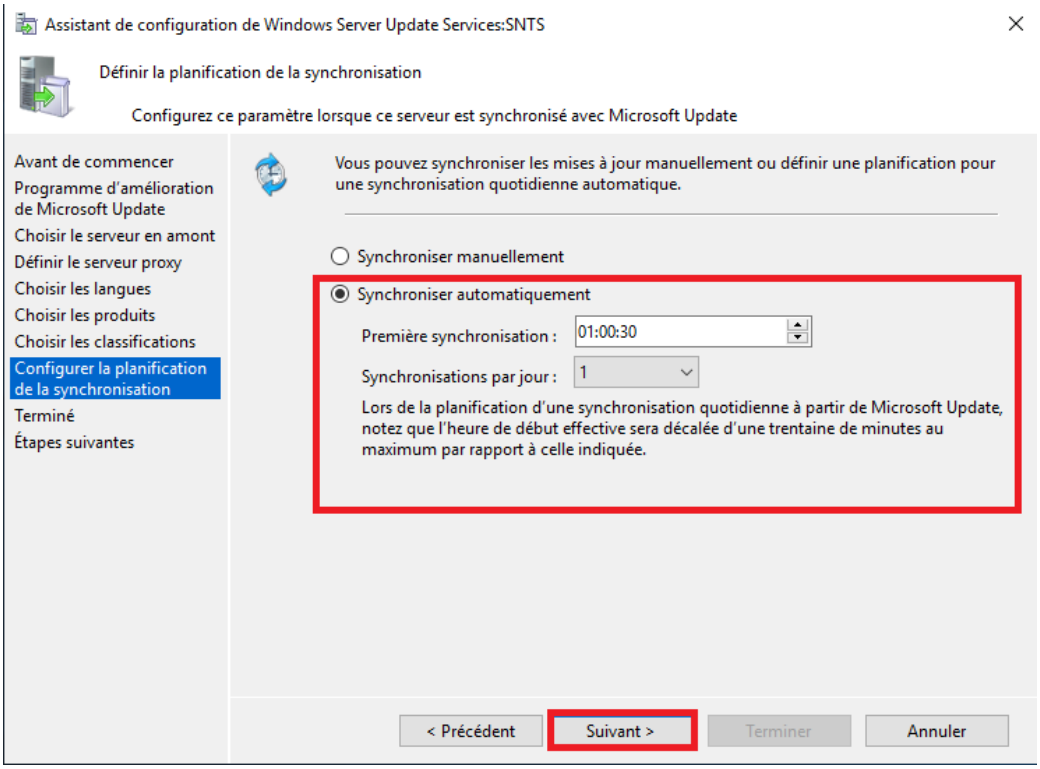
➔ Vérifiez que la case Windows est bien cochée dans la liste des produits puis faites « **Suivant** ».



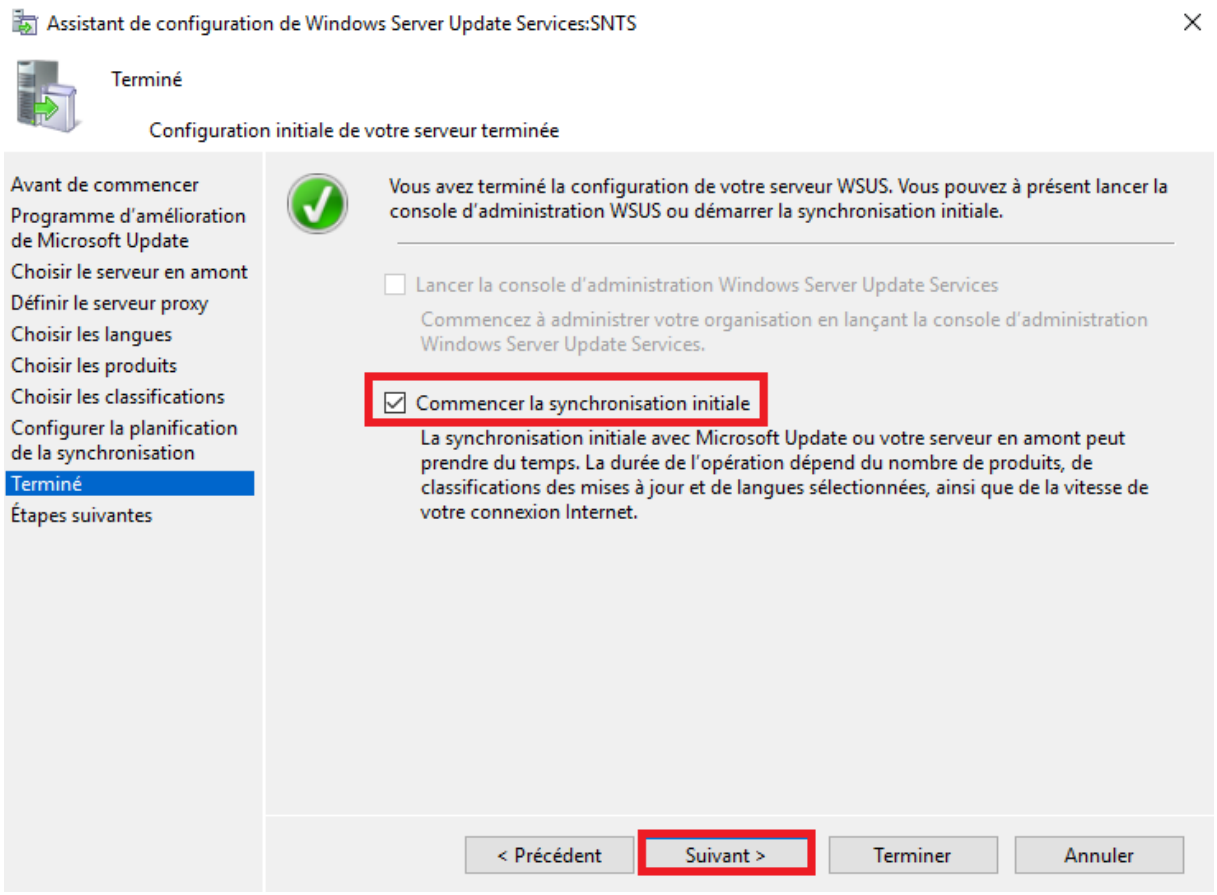
➔ Sélectionnez différentes classifications puis faites « **Suivant** ».



➔ Sélectionnez « **Synchroniser automatiquement** » tous les jours à 1h du matin puis faites suivant



➔ Cochez la 2ème case puis faites « **Suivant** ».



➔ Ensuite faites « **Terminer** ».

Le service de mise à jour WSUS est maintenant installé et configuré sur votre serveur.

III. Configuration du Scripting avancé

Contrairement à l'ancien script, nul besoin de créer au préalable les différentes Unités d'Organisation et les différents groupes, le script va s'en charger.

Pour commencer il faut modifier le fichier CSV à votre convenance en veillant à respecter la casse, pour ceci vous pouvez vous referrez au différents NOM/Prénom/UO/groupes déjà remplies.

Le fichier CSV doit respecter la casse ci-dessous :

NOM Prénom École(UO) Classe/Enseignants(UO) École(Groupe) Classe/Enseignants(Groupe)

Ce fichier sera la liste à laquelle le script va se referrer pour créer les utilisateurs.

Ensuite, une fois le CSV dûment remplie, il suffit de lancer le script en faisant un clic droit dessus puis exécuter avec PowerShell. Voici maintenant comment le script va procéder :

D'abord il va aller chercher les informations contenues sur le CSV et définir les variables à l'aide de celui-ci.

```
#########################
# Import du fichier CSV #
#########################

$CSVFile = "C:\Script\Emile Zola\newusers_emilezola.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8

# Définition des variables en fonction du fichier CSV
    $UtilisateurPrenom = $Utilisateur.Prenom
    $UtilisateurNom = $Utilisateur.Nom
    $UtilisateurLogin = ($UtilisateurPrenom).Substring(0,3).ToLower() + "." + $UtilisateurNom.ToLower()
    $UtilisateurMotDePasse = "[redacted]"
    $UtilisateurGroupe = $Utilisateur.Groupe
    $UtilisateurGroupe2 = $Utilisateur.Groupe2
    $UtilisateurOU = $Utilisateur.OU
    $UtilisateurOU2 = $Utilisateur.OU2
```

Une fonction a été rajouté permettant de supprimer tout caractères accentués qui ne passerait pas une fois sur l'AD.

```
    ######################################################
    # Fonction de suppression des caractères accentuées #
    ######################################################

    function Remove-StringLatinCharacters
    {
        PARAM ([string]$String)
        [Text.Encoding]::ASCII.GetString([Text.Encoding]::GetEncoding("Cyrillic").GetBytes($String))
    }
```

Ensuite le script commence et lance la création des utilisateurs.

```
#####################################
# Création des utilisateurs dans l'AD #
#####################################

Foreach($Utilisateur in $CSVData){

    # Vérification de la présence de l'utilisateur dans l'AD
    if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin})
    {
        Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
    }

    # Création des utilisateurs
    else
    {
        New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
                   -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
                   -GivenName $UtilisateurPrenom `
                   -Surname $UtilisateurNom `
                   -SamAccountName $UtilisateurLogin `
                   -UserPrincipalName "$UtilisateurLogin@snts.local" `
                   -Path "OU=Utilisateurs,DC=snts,DC=local" `
                   -AccountPassword(ConvertTo-SecureString $UtilisateurMotDePasse -AsPlainText -Force) `
                   -ChangePasswordAtLogon $true `
                   -Enabled $true

        Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
    }
}

Write-Host "Création des utilisateurs dans l'AD terminée" -ForegroundColor Green

Start-Sleep -Seconds 5
```

Puis il va créer les Unités d'Organisation et ajouter les utilisateurs dans les bonnes UO.

D'abord les écoles :

```
#############################################################################
# Création des OU école puis déplacement des utilisateurs dans les OU école #
#############################################################################

Foreach($Utilisateur in $CSVData){

    # Création de l'OU si elle n'existe pas
    $ou=Get-ADOrganizationalUnit -Filter {samaccountname -eq $UtilisateurOU}
    if($ou){echo "OU $UtilisateurOU trouvée"}
    else{$ou=New-ADOrganizationalUnit -Name $UtilisateurOU -Path "DC=snts,DC=local" -ProtectedFromAccidentalDeletion $false
    echo "OU $UtilisateurOU créée"}

    # Déplacement des utilisateurs dans les OU parents
    if(@(Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin}).Count -gt 0)
        {
            Move-ADObject -Identity "CN=$UtilisateurNom $UtilisateurPrenom,OU=Utilisateurs,DC=snts,DC=local" -TargetPath "OU=$UtilisateurOU,DC=snts,DC=local"

            Write-Output "Déplacement de l'utilisateur $UtilisateurLogin dans l'OU $UtilisateurOU"
        }
    else
        {
            Write-Warning "L'identifiant $UtilisateurLogin est déjà dans l'OU parents '$UtilisateurOU'"
        }
    }

Write-Host "Déplacement des utilisateurs dans les OU parents terminée" -ForegroundColor Green

Start-Sleep -Seconds 5
```

Puis les classes :

```
#############################################################################
# Création des OU classes puis déplacement des élèves dans les OU classes #
#############################################################################

Foreach($Utilisateur in $CSVData){

    # Création de l'OU si elle n'existe pas
    $ou2=Get-ADOrganizationalUnit -Filter {samaccountname -eq $UtilisateurOU2}
    if($ou2){echo "OU $UtilisateurOU2 trouvée"}
    else{$ou2=New-ADOrganizationalUnit -Name $UtilisateurOU2 -Path "OU=$UtilisateurOU,DC=snts,DC=local" -ProtectedFromAccidentalDeletion $false
    echo "OU $UtilisateurOU2 créée"}

    # Vérification de la présence de l'utilisateur dans l'OU
    if ($UtilisateurOU2 -contains $UtilisateurLogin)
    {
        Write-Warning "L'identifiant $UtilisateurLogin est déjà dans l'OU '$UtilisateurOU2'"
    }

    # Déplacement des élèves dans les OU des classes
    else{
        if (@(Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin} -SearchBase "OU=$UtilisateurOU,DC=snts,DC=local").Count -gt 0)
            {
                Move-ADObject -Identity "CN=$UtilisateurNom $UtilisateurPrenom,OU=$UtilisateurOU,DC=snts,DC=local" -TargetPath "OU=$UtilisateurOU2,OU=$UtilisateurOU,DC=snts,DC=local"

                Write-Output "Déplacement de l'élève $UtilisateurLogin dans l'OU $UtilisateurOU2"
            }
        }
}

Write-Host "Déplacement des élèves dans les OU des classes terminée" -ForegroundColor Green

Start-Sleep -Seconds 5
```

Après les UO, les groupes de sécurités sont créés.

Comme pour les UO, d'abord ceux des écoles, puis ceux des classes :

```
#####################################################################
# Création des groupes puis ajout des utilisateurs dans les groupes #
#####################################################################

Foreach($Utilisateur in $CSVData){

    # Création du groupe "Ecole" si il n'existe pas
    $group=Get-ADGroup -Filter {samaccountname -eq $UtilisateurGroupe}
    if($group){echo "Groupe $UtilisateurGroupe trouvé"}
    else{$group=New-ADGroup -Name $UtilisateurGroupe -SamAccountName $UtilisateurGroupe -GroupCategory Security -GroupScope Global -Path "OU=$UtilisateurOU,DC=snts,DC=local"
    echo "Groupe $UtilisateurGroupe créé"}

    # Création du groupe "Classe" si il n'existe pas
    $group2=Get-ADGroup -Filter {samaccountname -eq $UtilisateurGroupe2}
    if($group2){echo "Groupe $UtilisateurGroupe2 trouvé"}
    else{$group2=New-ADGroup -Name $UtilisateurGroupe2 -SamAccountName $UtilisateurGroupe2 -GroupCategory Security -GroupScope Global -Path "OU=$UtilisateurOU2,OU=$UtilisateurOU,DC=snts,DC=local"
    echo "Groupe $UtilisateurGroupe2 créé"}

    # Ajout des utilisateur au groupe "Ecole"
    Add-ADGroupMember -Identity $UtilisateurGroupe -Members $UtilisateurLogin

    Write-Output "Ajout de l'utilisateur $UtilisateurLogin au groupe $UtilisateurGroupe"

    # Ajout des utilisateur au groupe "Classe"
    Add-ADGroupMember -Identity $UtilisateurGroupe2 -Members $UtilisateurLogin

    Write-Output "Ajout de l'utilisateur $UtilisateurLogin au groupe $UtilisateurGroupe2"

}

Write-Host "Ajout des utilisateurs aux groupes terminée" -ForegroundColor Green

Start-Sleep -Seconds 5
```

Enfin, la dernière étape est la création de répertoires personnels pour chaque utilisateur qui sera monté sur sa session sous la lettre P :

```
#####################################
# Création des répertoires personnels #
#####################################

Foreach($Utilisateur in $CSVData){

    # Définition des variables de l'emplacement des répertoires personnels
    $HomedirsPath = "\\WS19\Homedirs\Emile Zola\"
    $Homedirs = $HomedirsPath + $UtilisateurLogin

    if (!(Test-Path $Homedirs)) {
        New-Item -path $Homedirs -ItemType Directory -Force -ErrorAction Stop

        # Ajout des droits pour l'utilisateur
        $acl = Get-Acl $Homedirs

        $FileSystemRights = [System.Security.AccessControl.FileSystemRights]"FullControl"
        $AccessControlType = [System.Security.AccessControl.AccessControlType]::Allow
        $InheritanceFlags = [System.Security.AccessControl.InheritanceFlags]"ContainerInherit, ObjectInherit"
        $PropagationFlags = [System.Security.AccessControl.PropagationFlags]"None"

        $AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule ((Get-ADUser -Identity $UtilisateurLogin).SID, $FileSystemRights, $InheritanceFlags, $PropagationFlags, $AccessControlType)
        $acl.AddAccessRule($AccessRule)

        Set-Acl -Path $Homedirs -AclObject $acl -ea Stop

        # Suppression des droits pour les utilisateurs
        Remove-NTFSAccess -Path "C:\Homedirs\Emile Zola" -Account "Utilisateurs" -AccessRights FullControl

        Set-ADUser (Get-ADUser -Identity $UtilisateurLogin) -HomeDrive "P:" -HomeDirectory $Homedirs -ea Stop

        Write-Output "Création du répertoire personnel de l'utilisateur $UtilisateurLogin"
    }

    else {
            Write-Warning "Le dossier '$Homedirs' existe déjà"
        }
}

Write-Host "Création des répertoires personnels terminée" -ForegroundColor Green

Start-Sleep -Seconds 5
```