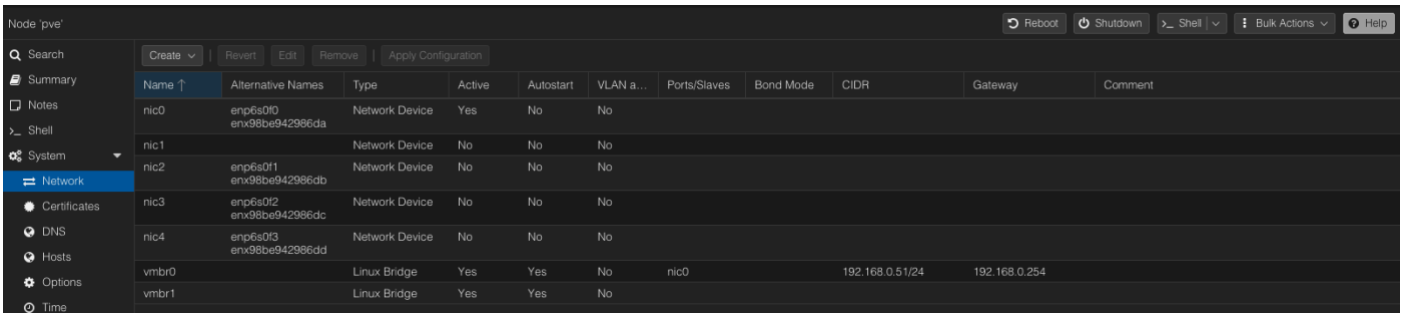
TP
WSUS

Sommaire

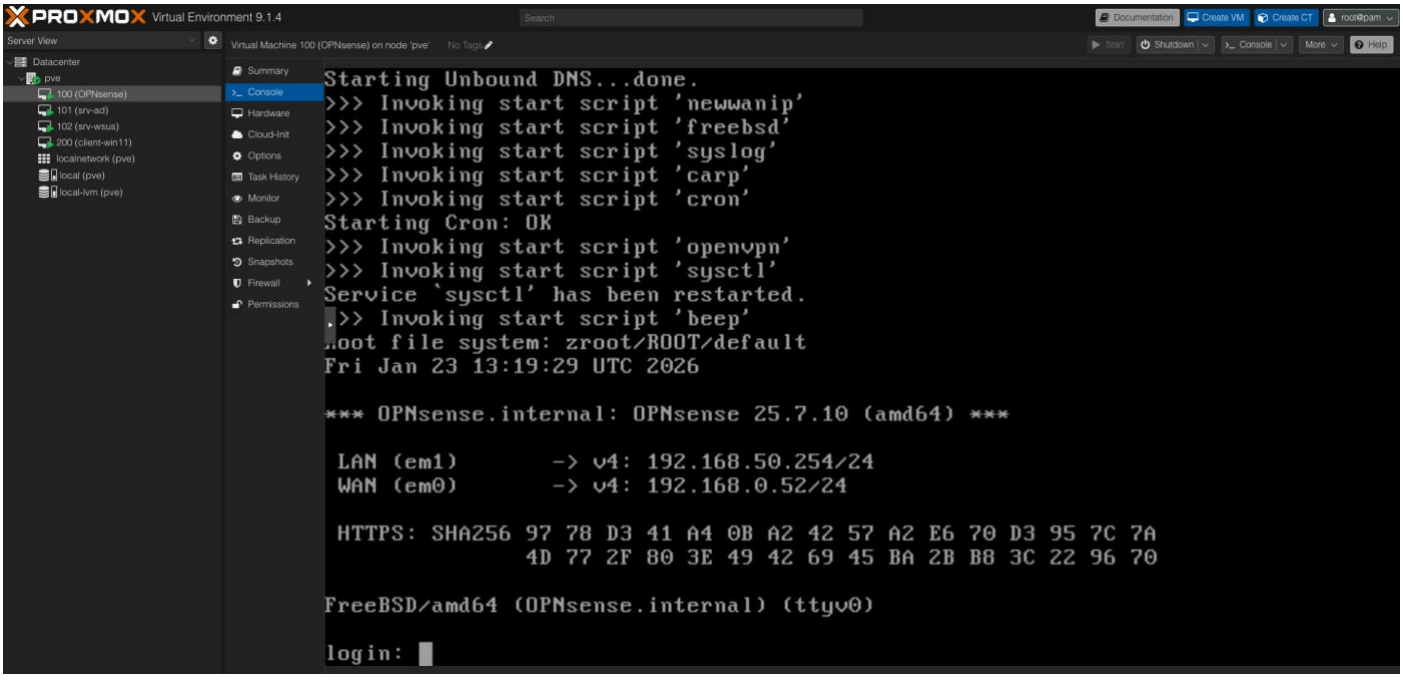
1. Rappel de l'infrastructure réseau 2
2. Installation de WSUS sur le serveur 3
3. Mise en place des GPO sur les postes clients 15

1. Rappel de l'infrastructure réseau

Actuellement, notre Proxmox possède un réseau dans le sous réseau 192.168.50.0/24, qui est présent sur l'interface vmbr1 (l'interface vmbr0 étant sur le réseau de la salle 407) :



Sur ce réseau vmbr1, est présent un OPNsense (192.168.50.254) servant de routeur (NAT) entre le réseau de la 407 et le réseau local. Ainsi, les machines peuvent avoir un accès Internet depuis le LAN. Un serveur DHCP est aussi présent sur l'OPNsense pour les machines clients :

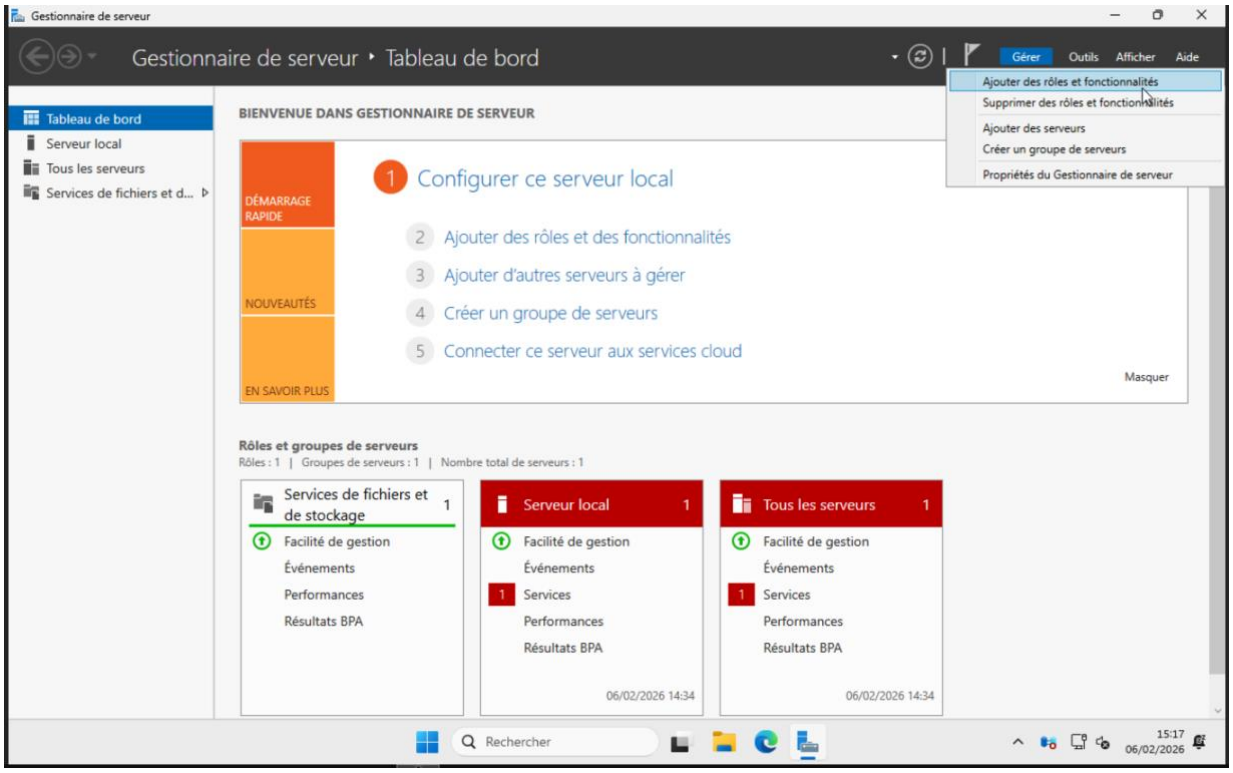


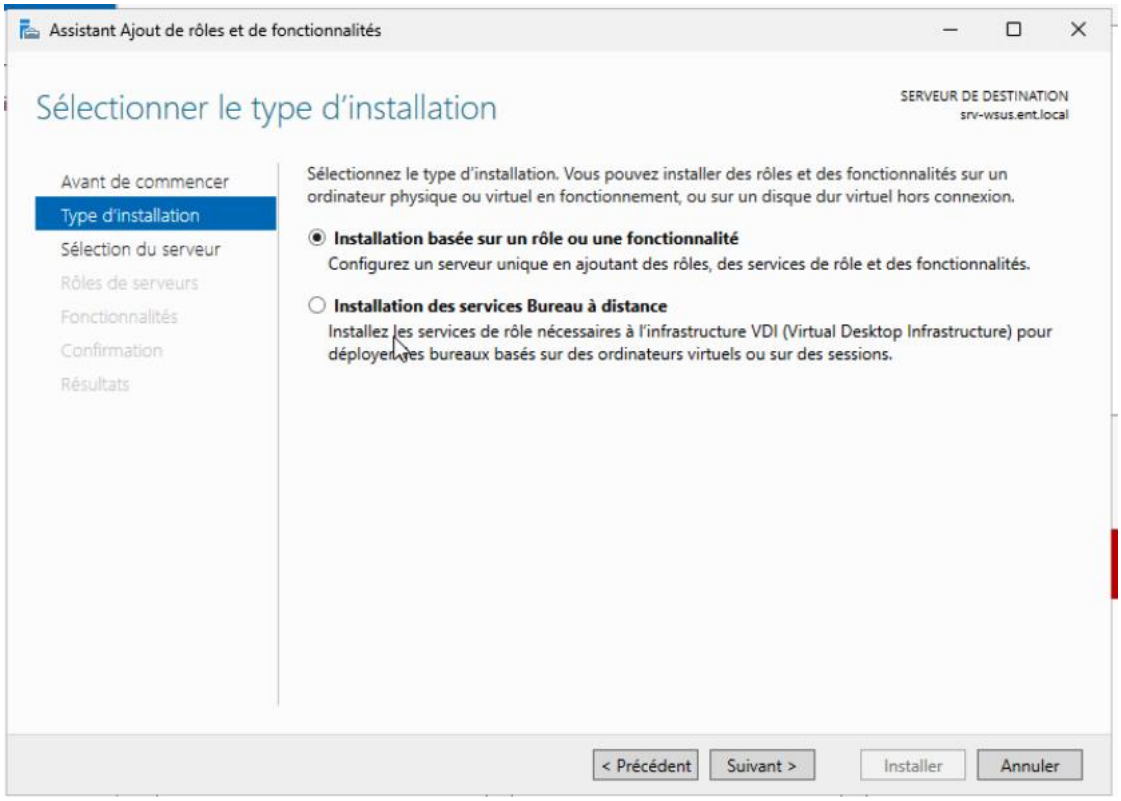
Une fois ceci en place, nous allons mettre en place le plan d'adressage et de nommage pour les serveurs et clients :

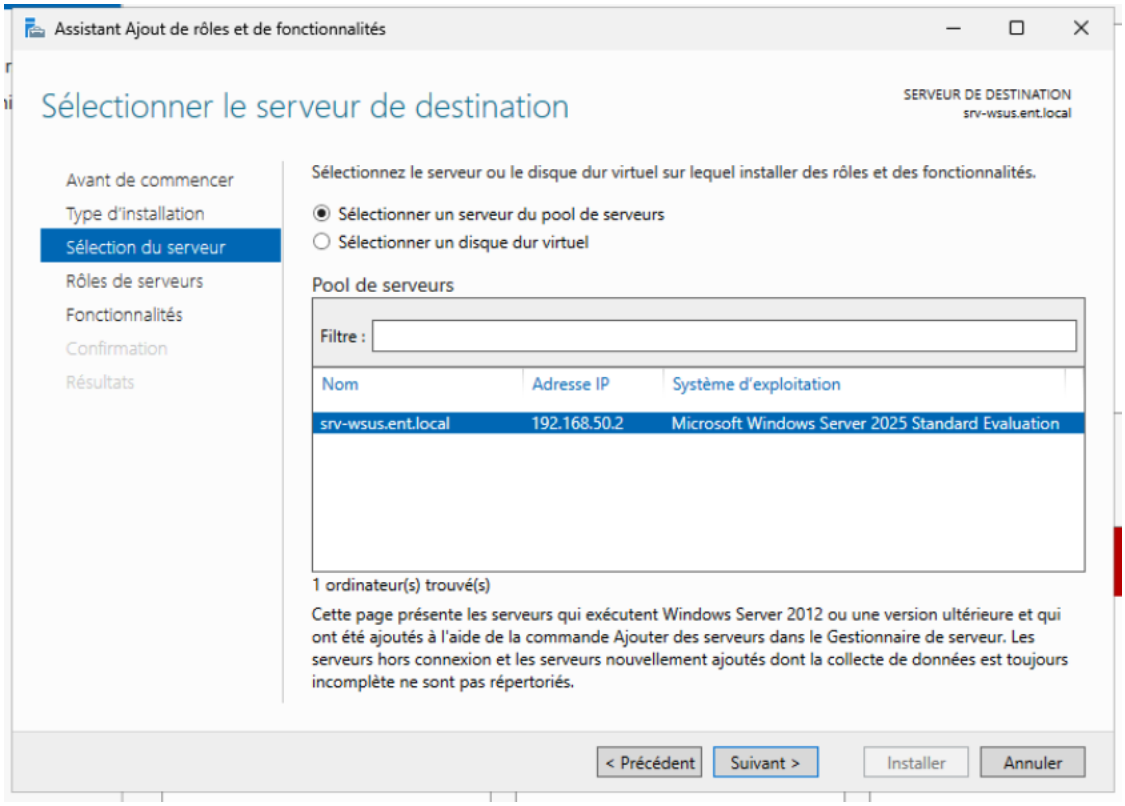
Nom	Type	IP/Masque
OPNsense	Pare-feu, routeur et DHCP	192.168.50.254/24
srv-ad	Windows Server 2025 en tant que contrôleur de domaine	192.168.50.1/24
srv-wsus	Windows Server 2025 en tant que serveur de mise à jour	192.168.50.2/24
client-win11	Client Windows 11 sur le domaine	DHCP

2. Installation de WSUS sur le serveur

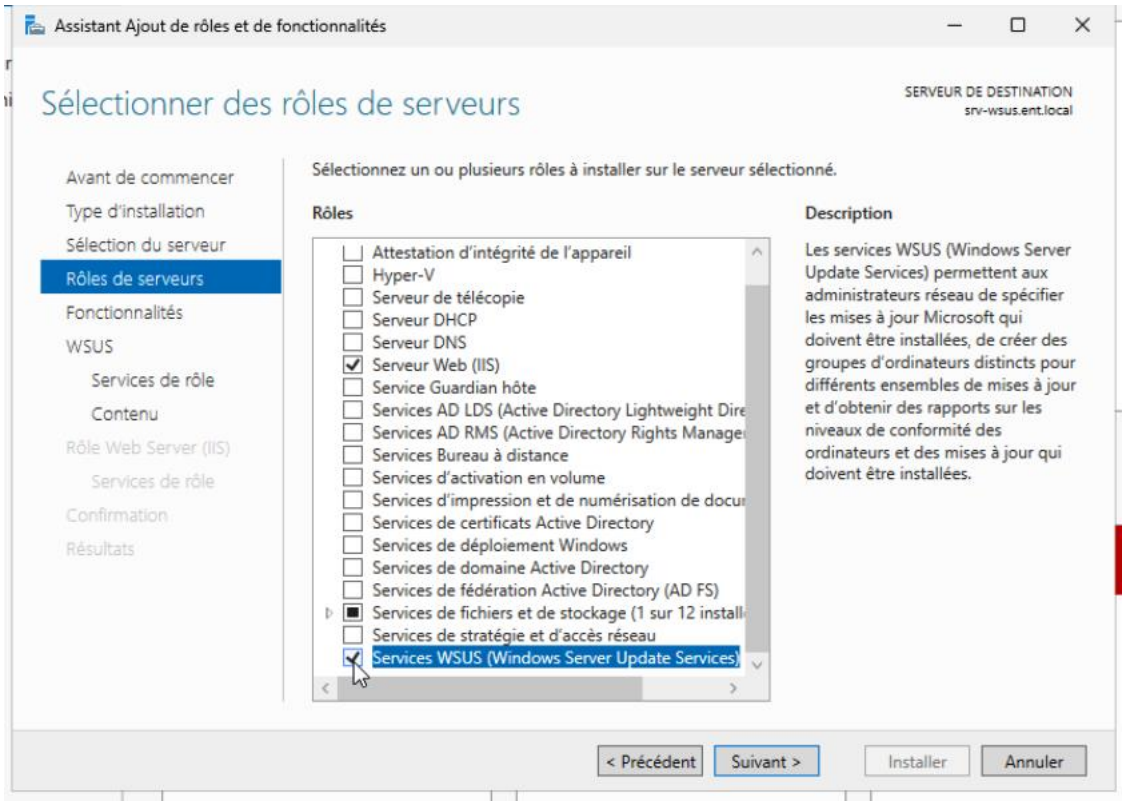
Nous allons maintenant installer le rôle WSUS sur notre serveur srv-wsus. Pour cela, nous allons nous rendre dans le gestionnaire de serveur, dans « Gérer » puis dans « Ajouter des rôles et fonctionnalités » :



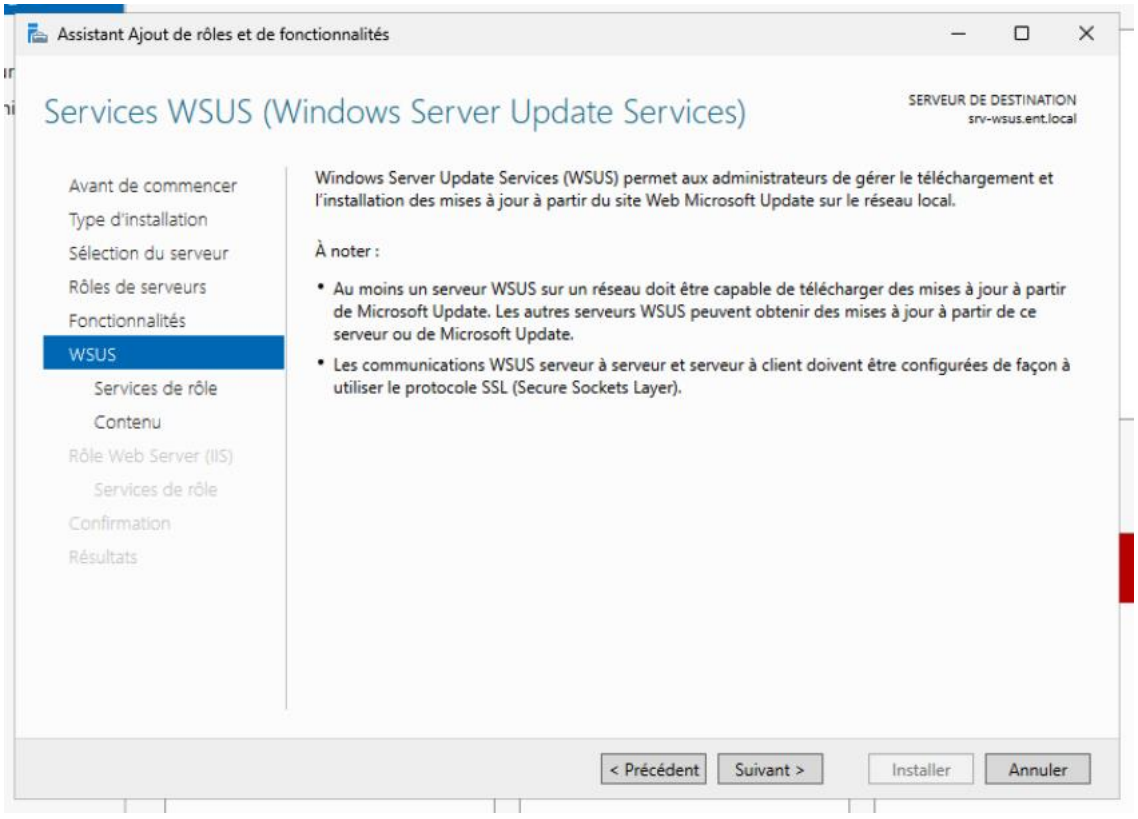




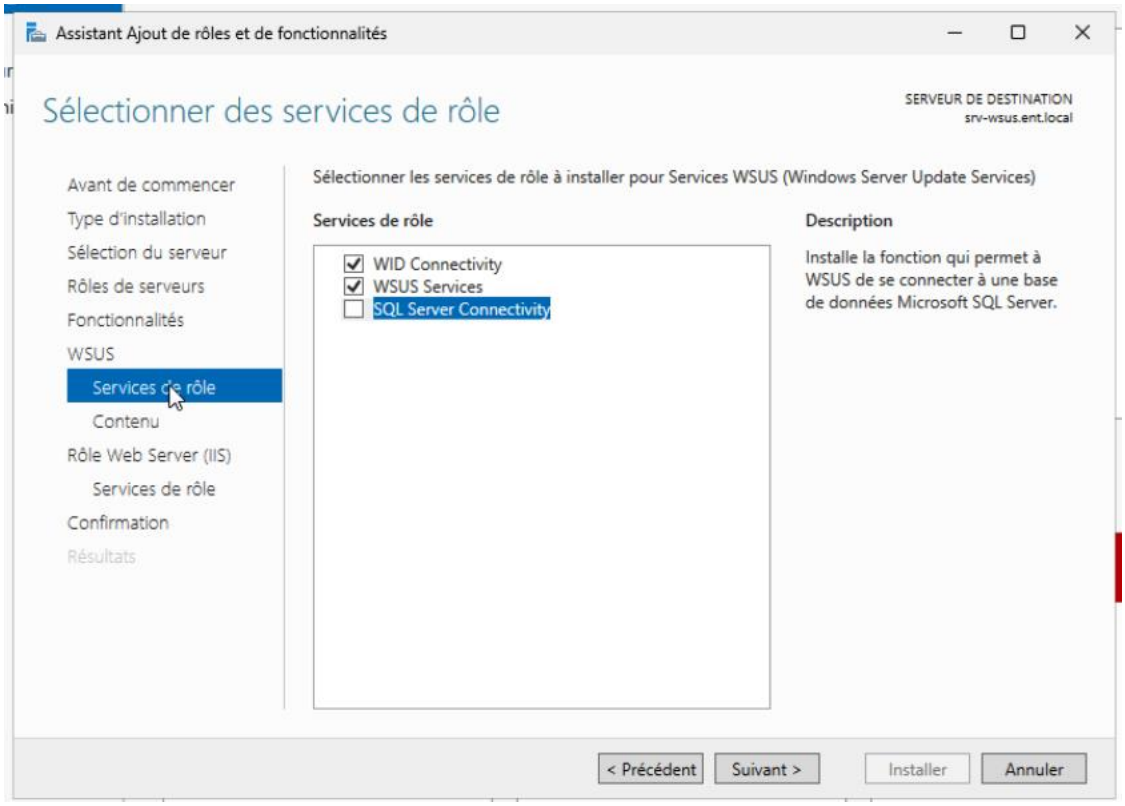
Dans la liste des rôles, nous allons descendre jusqu'à trouver « Service WSUS » et puis nous allons le cocher :

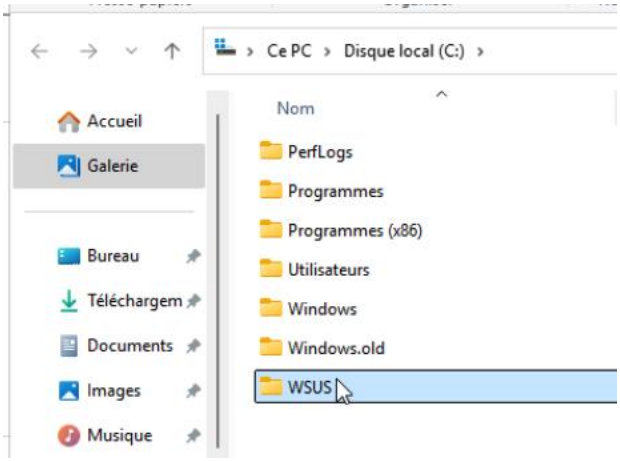


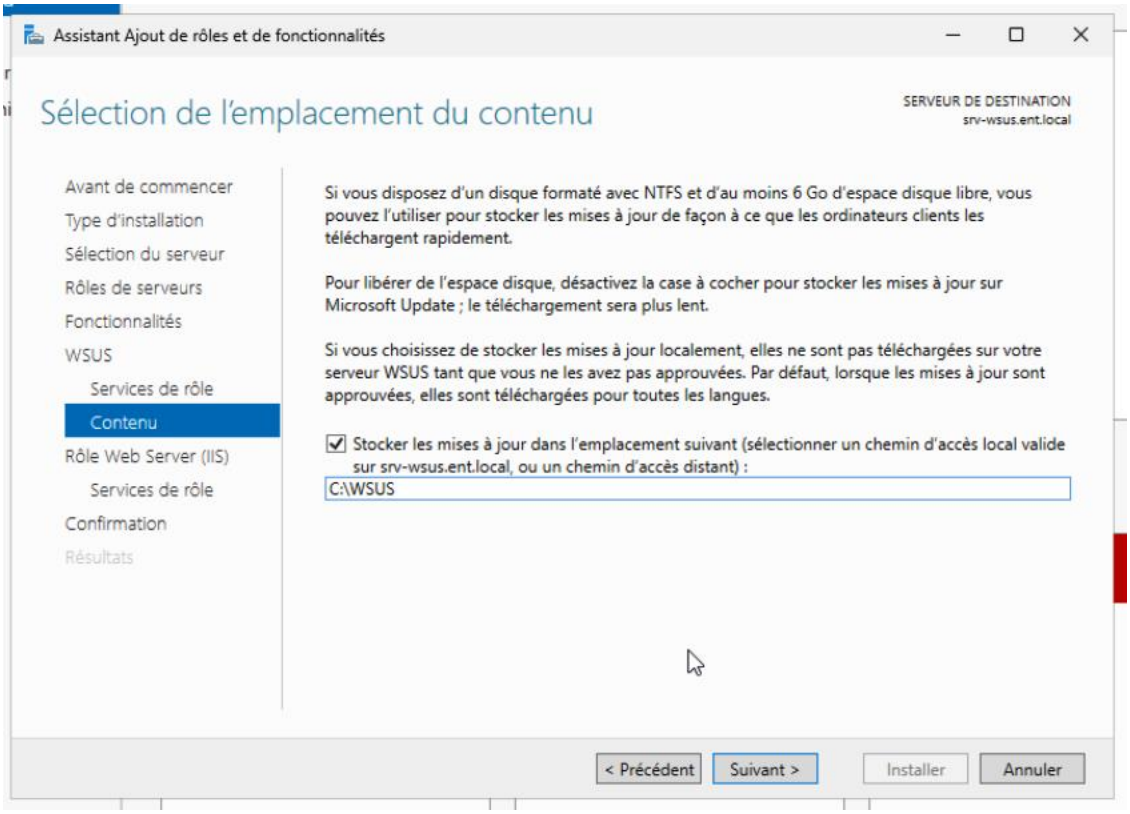
Une fois ceci fait, nous pouvons cliquer sur « Suivant » pour continuer :



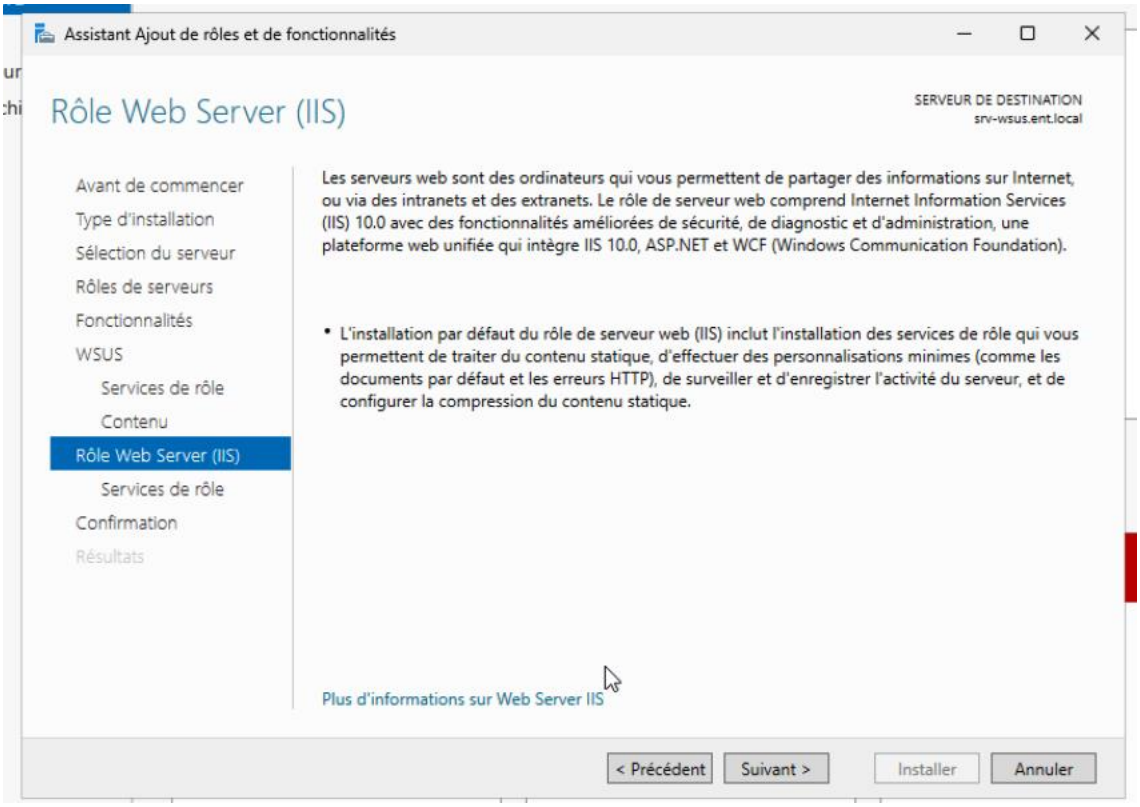
Maintenant, nous allons laisser les services de rôle coché par défaut, puis nous allons créer un dossier WSUS à la racine du disque, pour pouvoir y indiquer l'emplacement ou les mises à jour sont téléchargées :

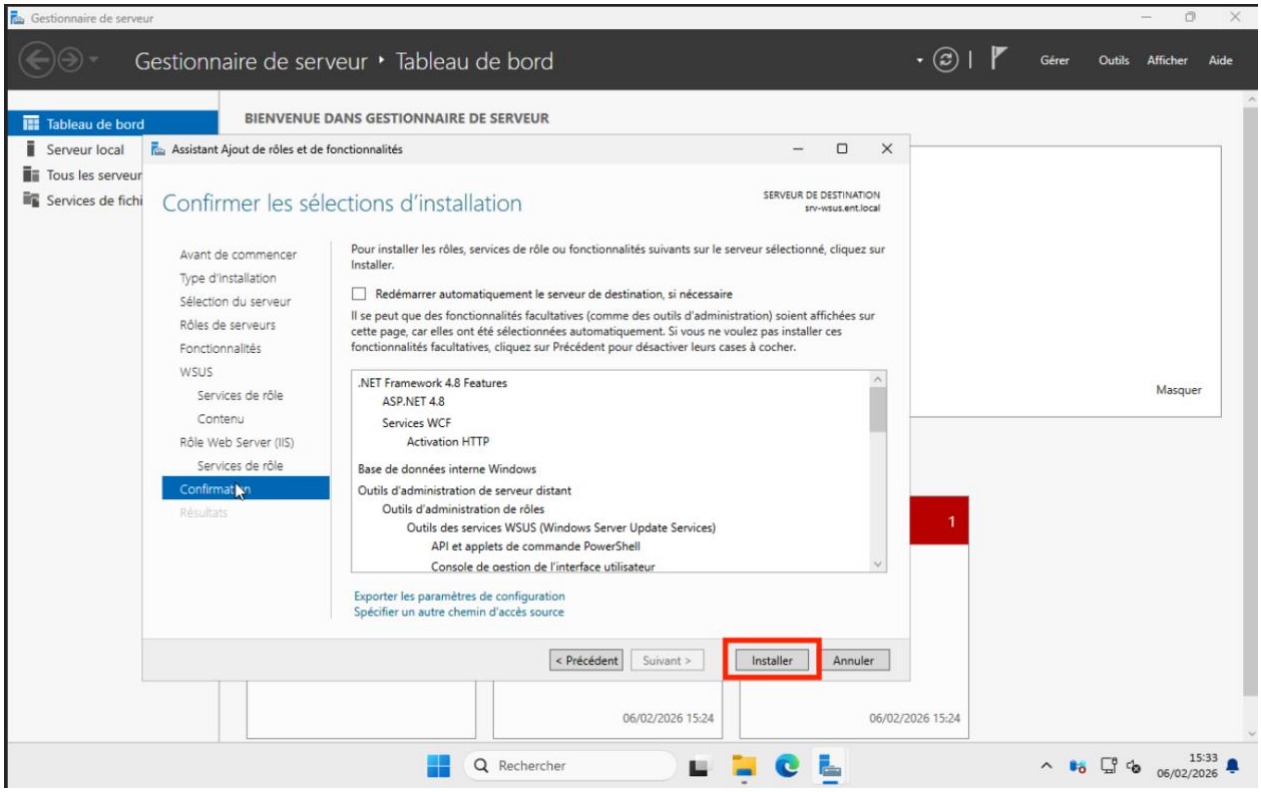




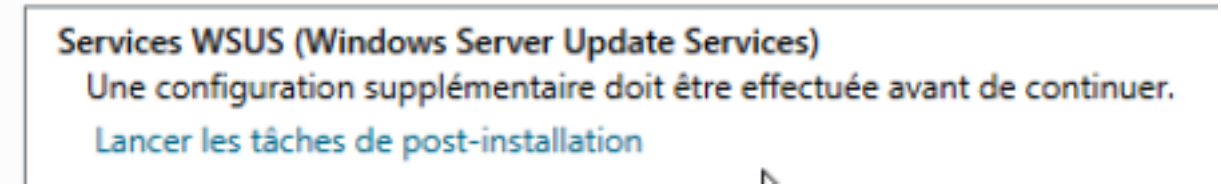


L'installation du service WSUS va aussi installer un serveur web IIS, il suffit de cliquer sur « Suivant » jusqu'à arriver à la confirmation pour installer le service WSUS :

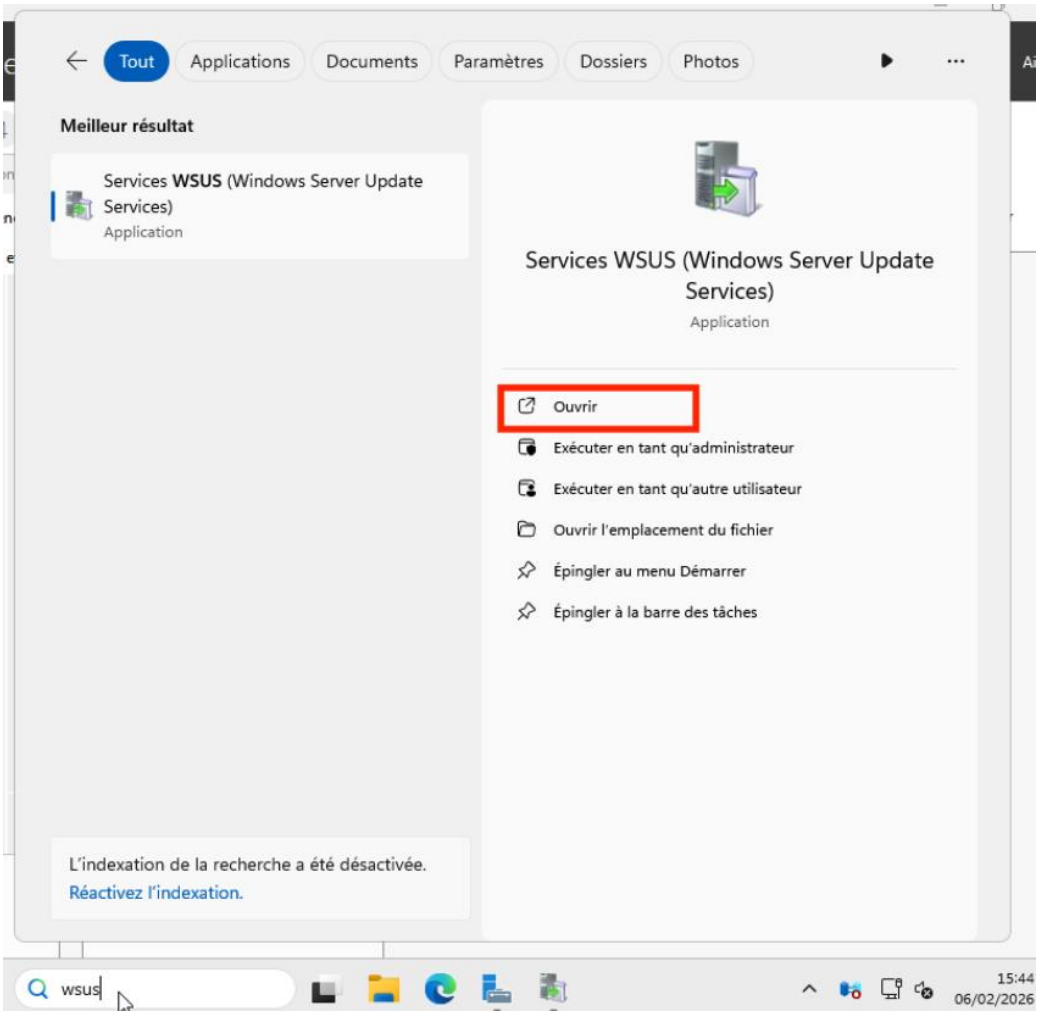




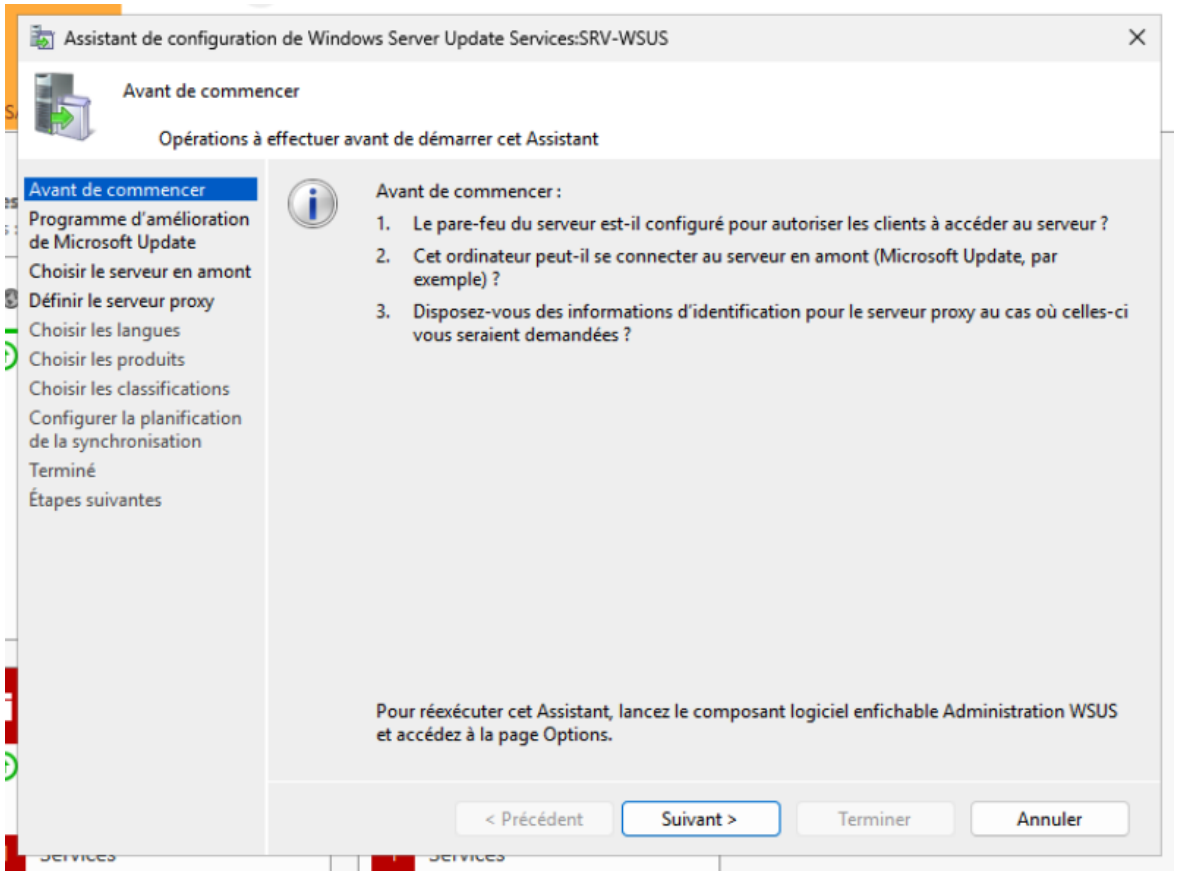
Après l'installation, une étape de post-installation est nécessaire, il suffit de cliquer sur « Lancer les tâches de post-installation » pour continuer :



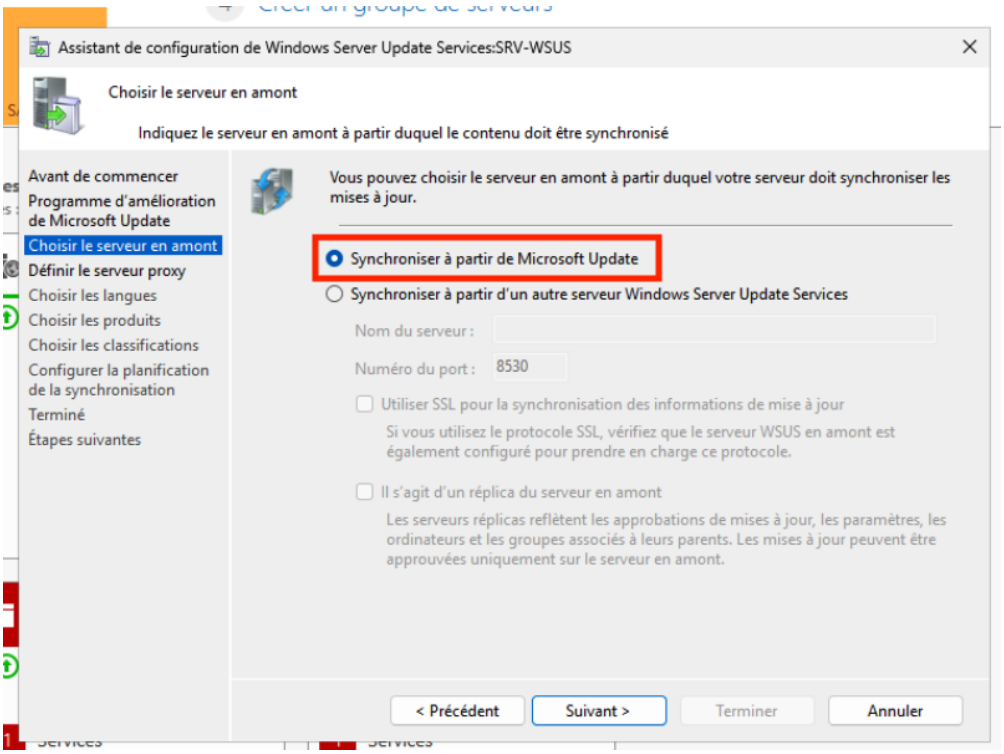
Une fois que l'installation est terminée, nous allons lancer l'assistant de WSUS, pour cela, nous allons chercher dans la barre Windows « WSUS » jusqu'à trouver ce dernier :



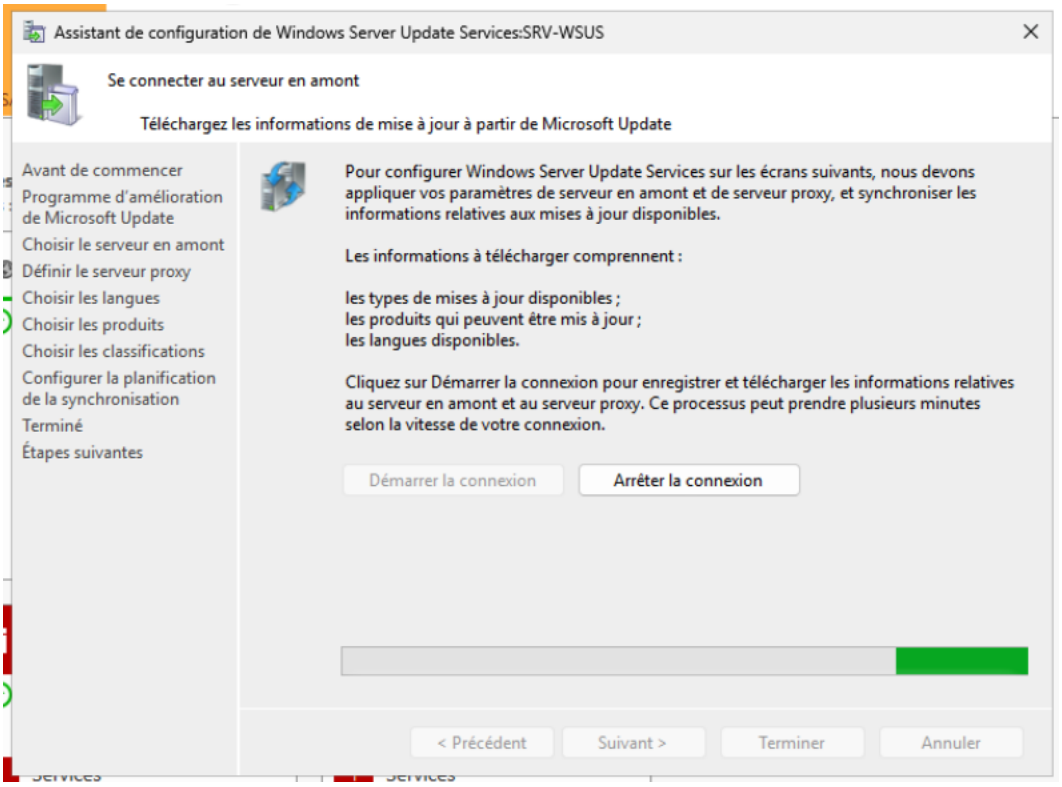
Une fois dans l'assistant, ce dernier va nous poser certaines questions pour savoir si on peut se connecter sur les serveurs de Windows Update (présence d'un pare feu, connexion Internet, proxy…) :



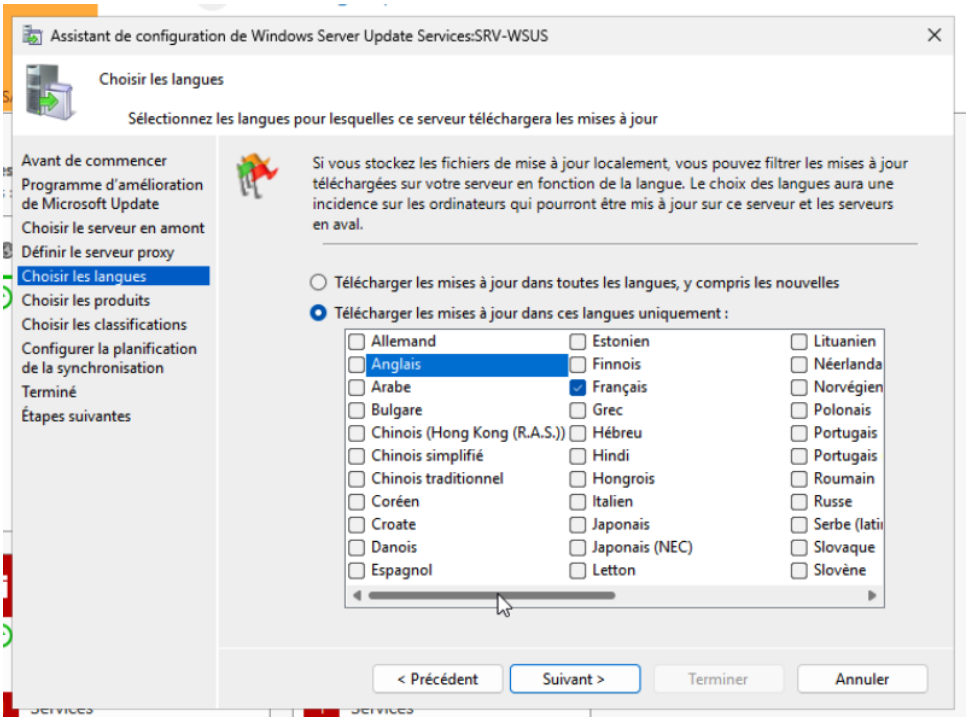
Il est aussi important de sélectionner « Synchroniser à partir de Microsoft Update » car l'on ne possède pas d'autre serveur WSUS sur le réseau :



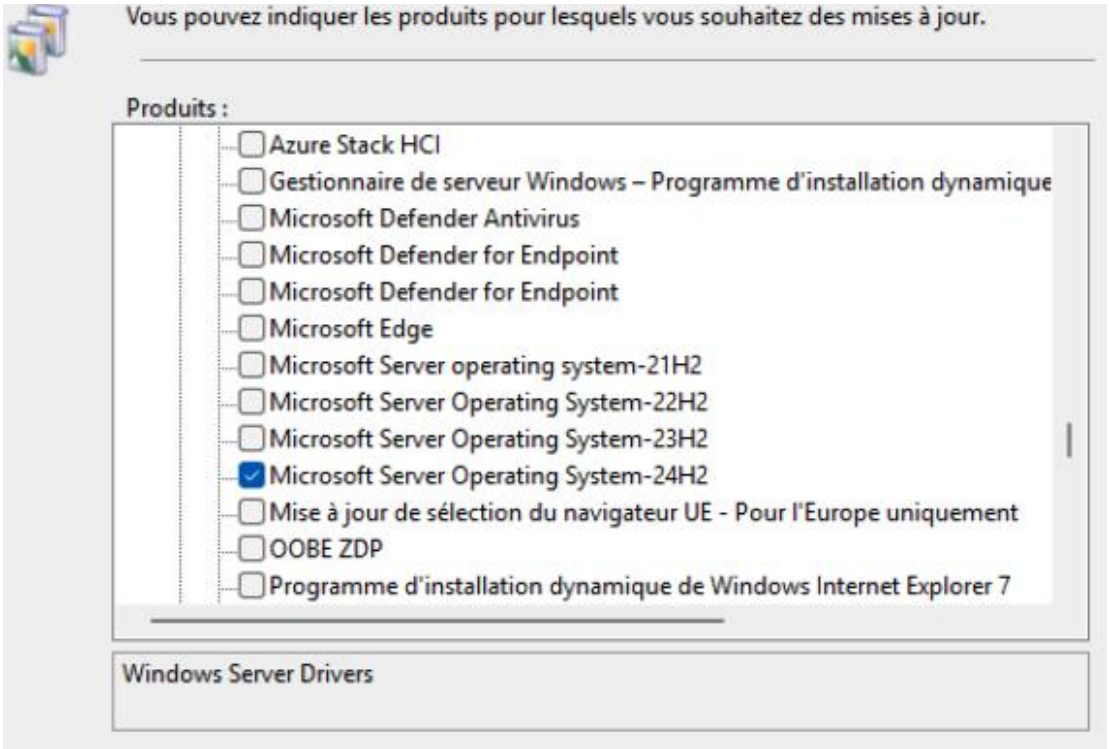
Une fois tout renseigné, l'assistant nous demande de lancer un test de connexion vers les serveurs de Microsoft Update (l'opération peut durer plusieurs minutes voire heures) :

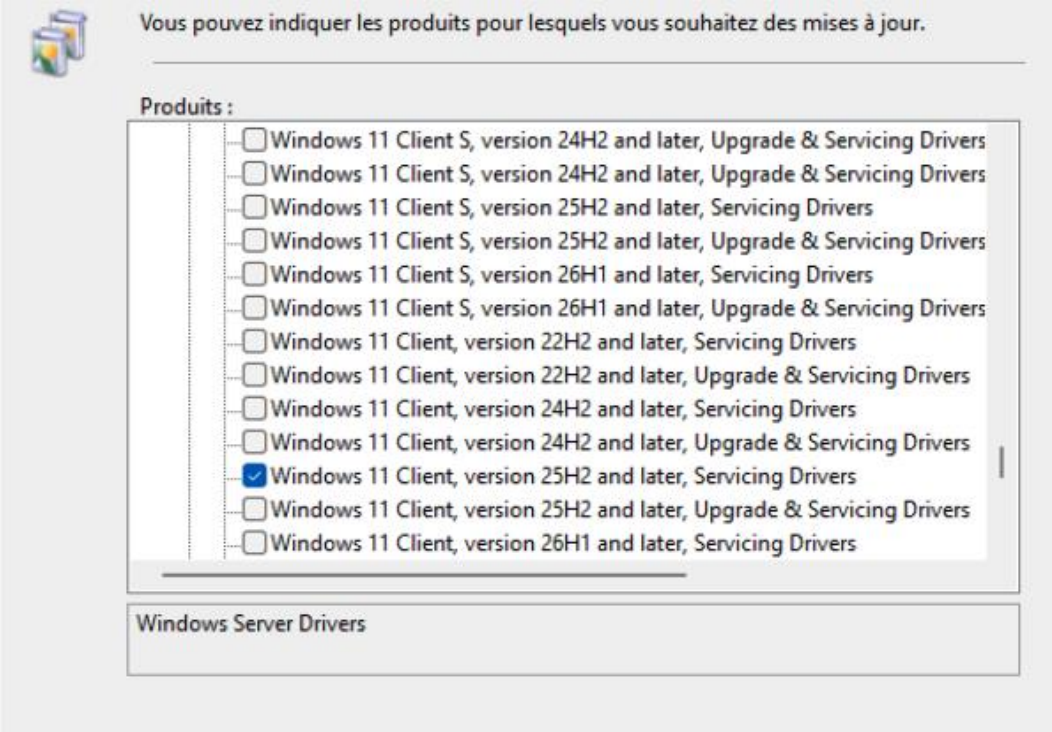


Une fois terminé, nous pouvons sélectionner les langues dans lesquels nous souhaitons avoir les mises à jour (dans notre cas, nous allons désélectionner l'Anglais) :

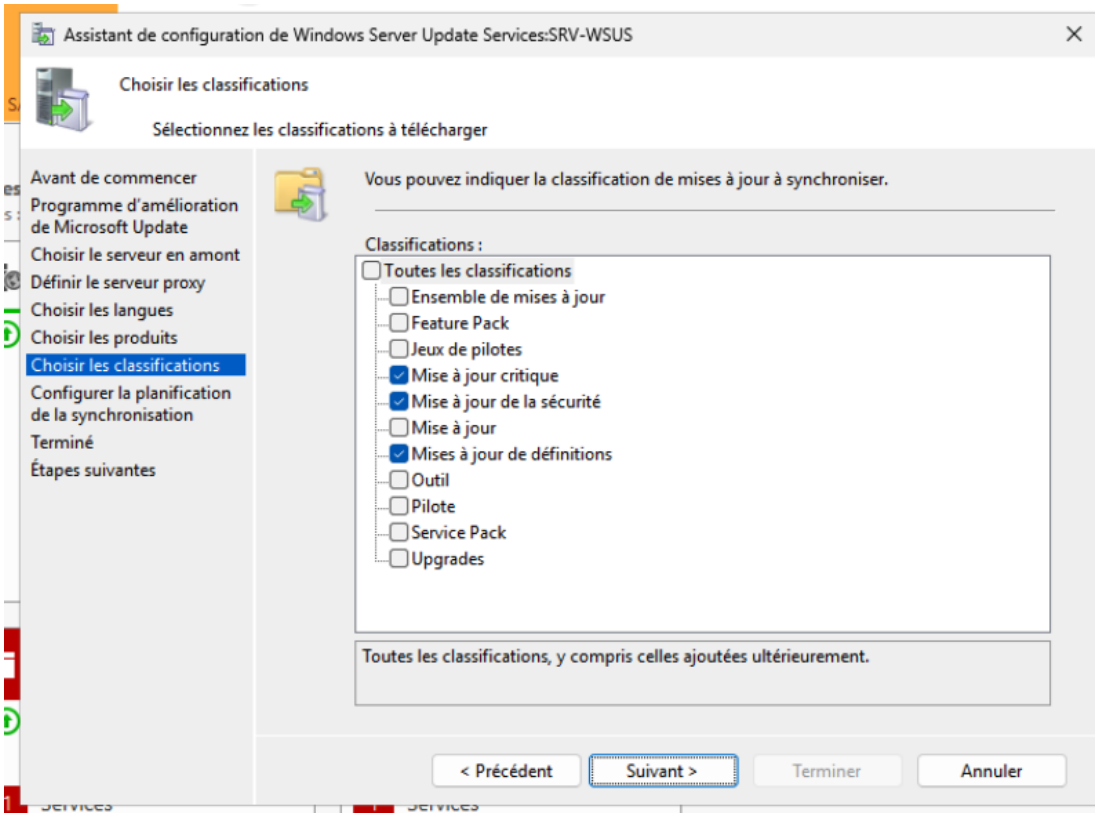


Maintenant, nous allons choisir les produits Microsoft auquel nous souhaitons recevoir des mises à jour, dans notre cas, nous allons sélectionner Windows Server 24h2 et Windows 11 25h2 (Service Drivers) :

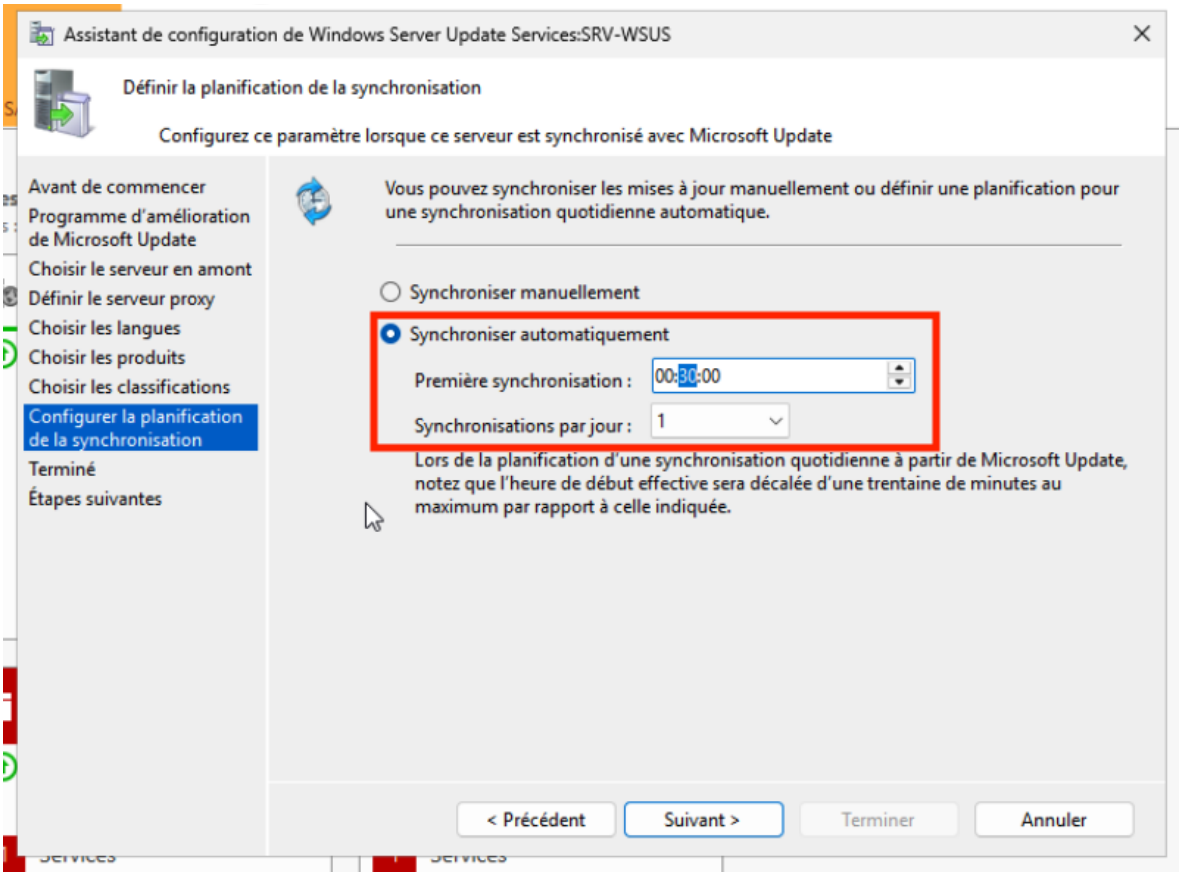




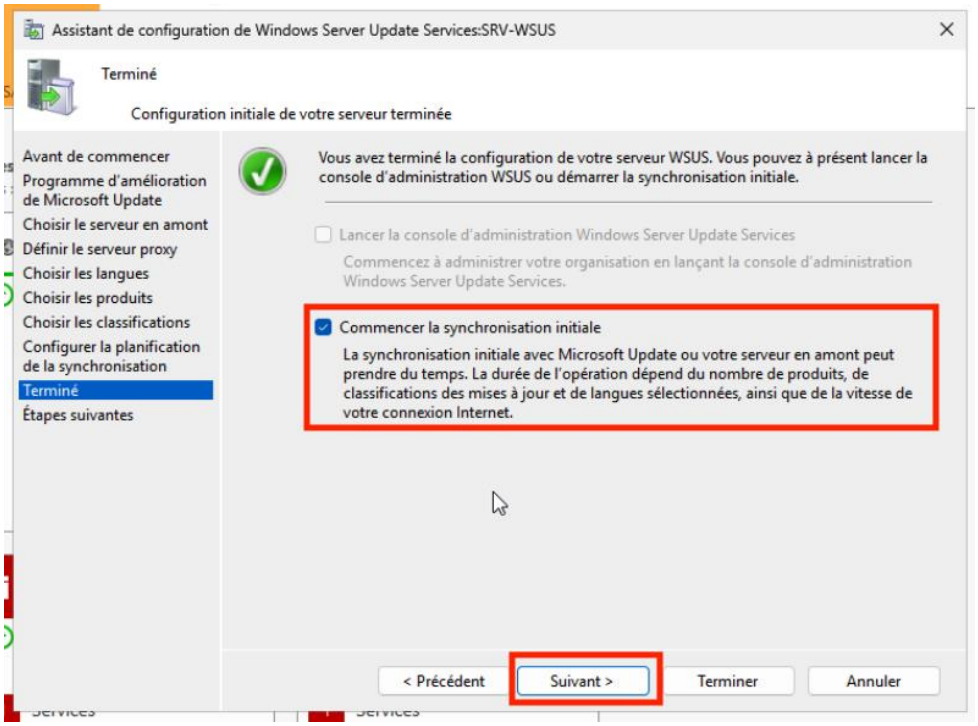
Ensuite, nous allons sélectionner les classifications de mises à jour que l'on souhaite, dans notre cas nous allons laisser celles par défaut :



Maintenant, nous allons définir la synchronisation des mises à jour, nous allons sélectionner la synchronisation automatique et faire en sorte qu'elle s'exécute tous les jours à minuit 30 :

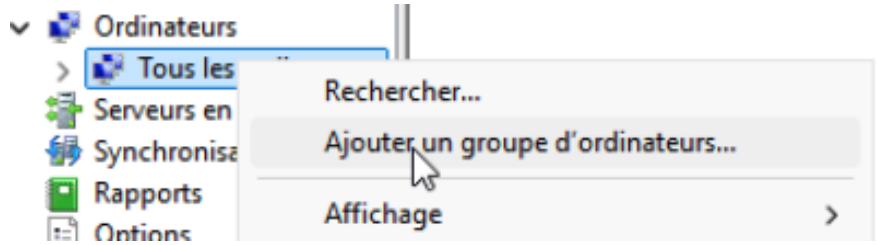


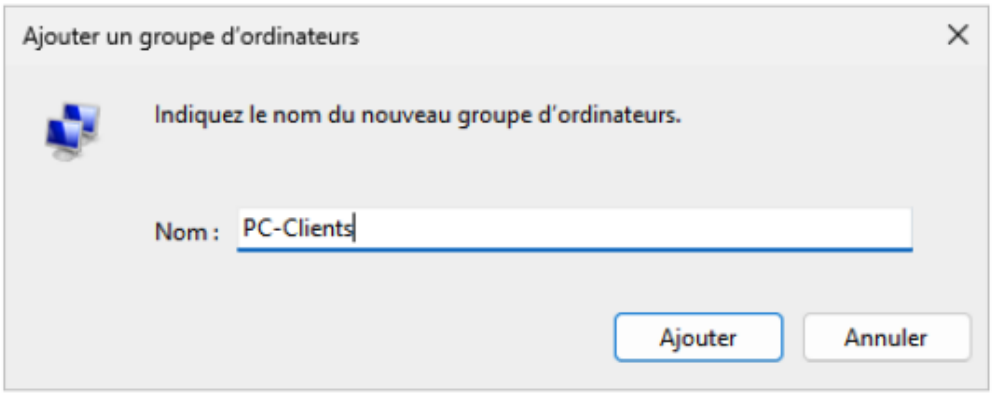
Une fois tout ceci fait, nous allons cocher la case « Commencer la synchronisation initiale » pour que le serveur commence à récupérer les mises à jour :



3. Mise en place des GPO sur les postes clients

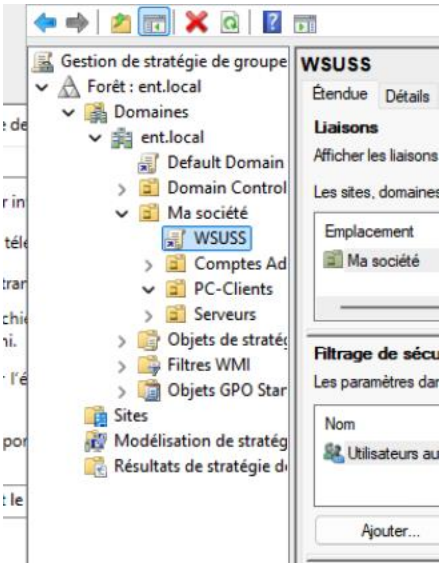
Maintenant que notre serveur WSUS est configuré, nous allons ajouter un groupe d'ordinateur afin que nos ordinateurs puissent rejoindre ce dernier. Pour cela dans WSUS, nous allons nous rendre dans « Ordinateurs », « Tous les ordinateurs » puis nous allons faire clic droit dessus pour créer un nouveau groupe d'ordinateur que nous appellerons « PC-Clients » (Comme dans l'AD) :



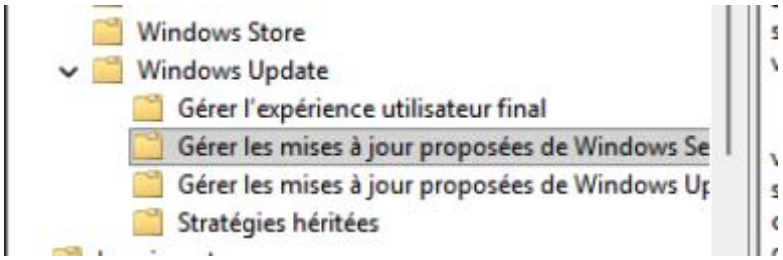


Une fois notre serveur WSUS en place, nous allons pouvoir configurer les GPO pour que nos machines clientes utilisent ce serveur WSUS

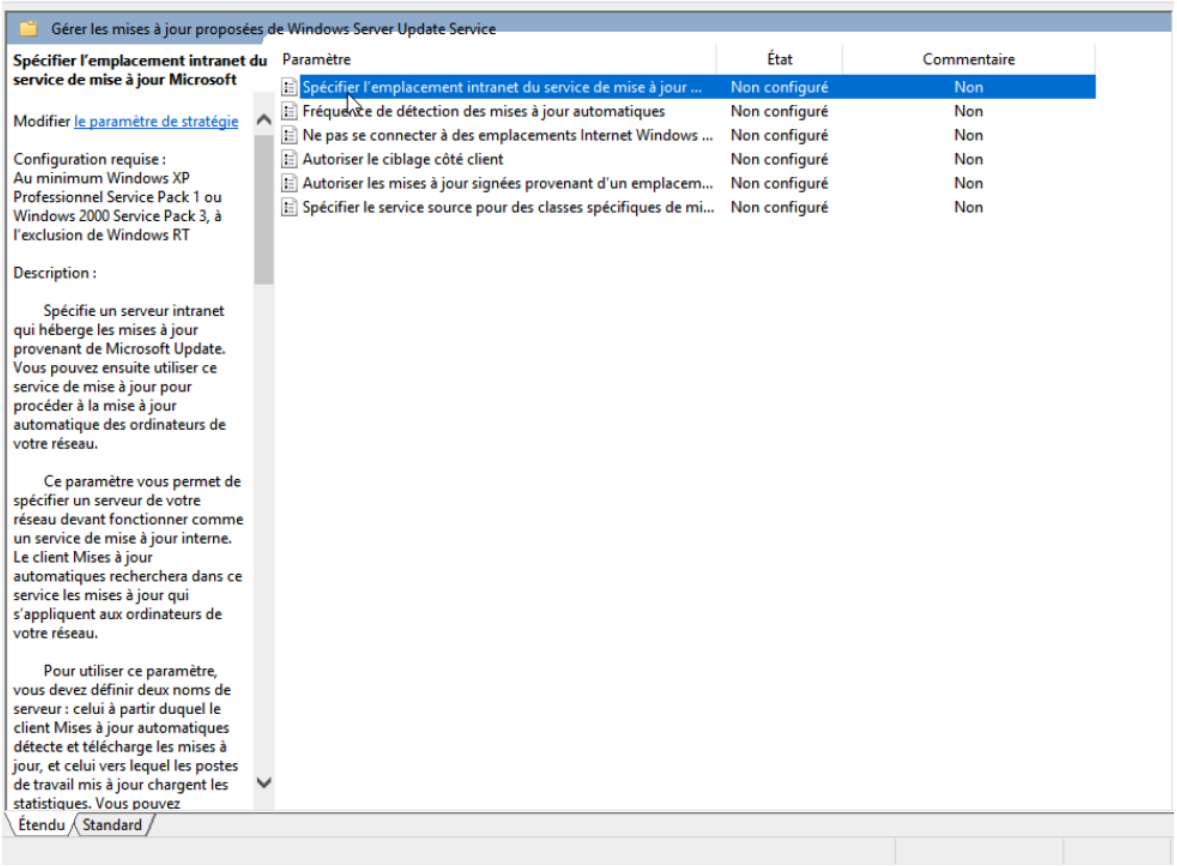
Pour cela, nous allons ouvrir notre serveur AD, puis nous allons créer une nouvelle GPO « WSUS » :



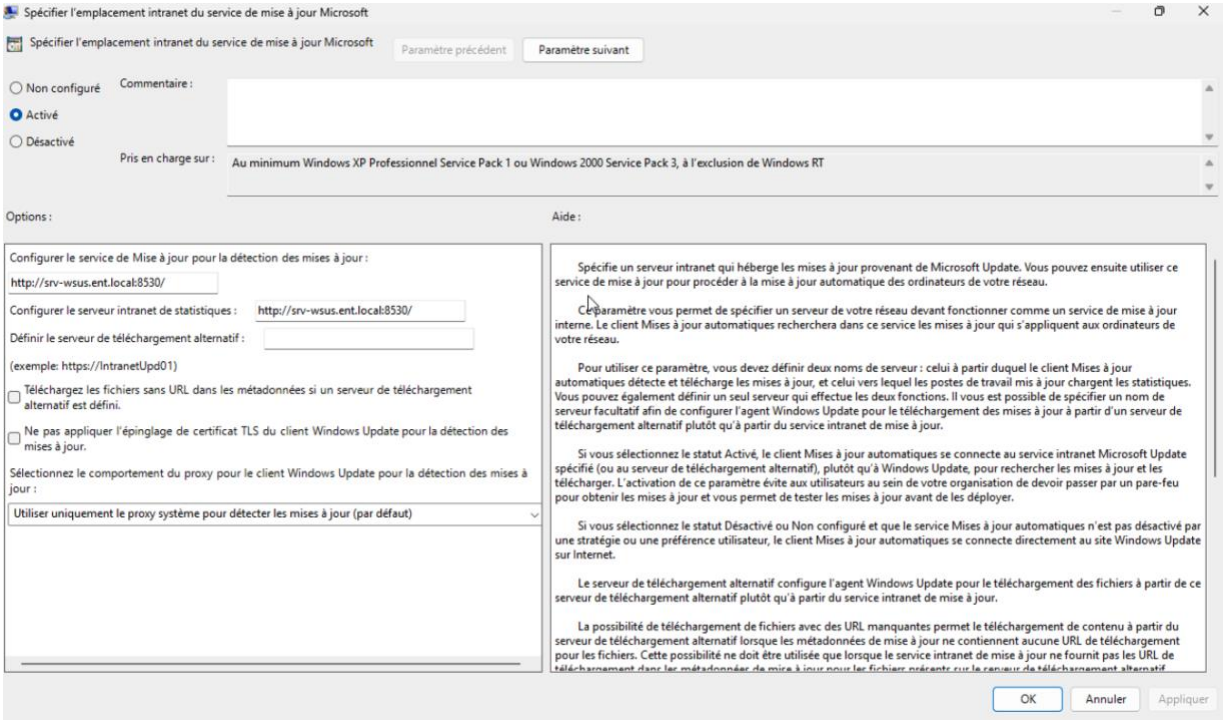
Ensuite, nous allons modifier cette dernière et nous rendre dans l'emplacement suivant : **Configuration Ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update > Gérer les mises à jour proposées de Windows Server Update Service**



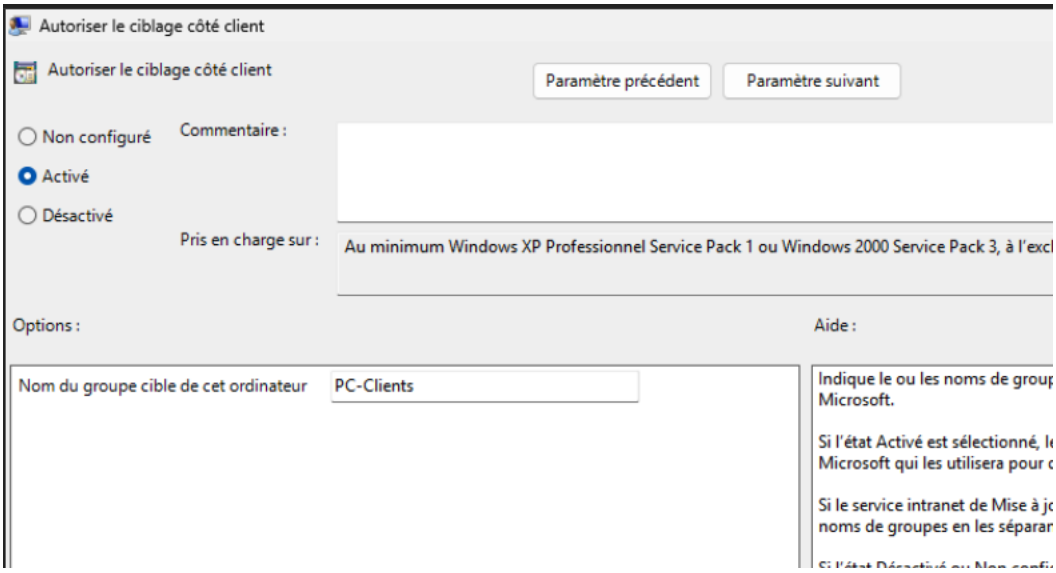
Puis, nous allons modifier la GPO « Spécifier l'emplacement intranet du service de mise à jour Microsoft » :



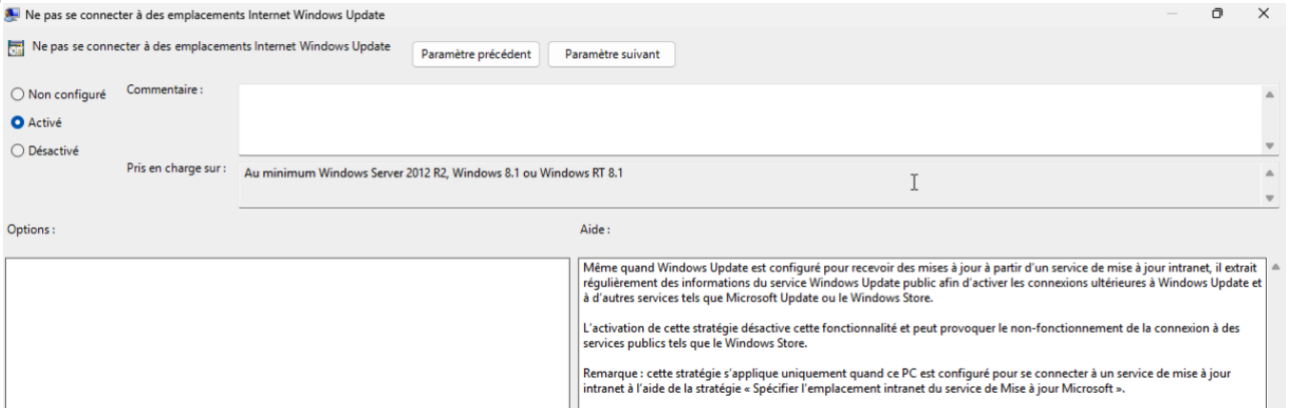
Maintenant, nous allons définir notre serveur WSUS avec le port de ce dernier (par défaut 8530) :



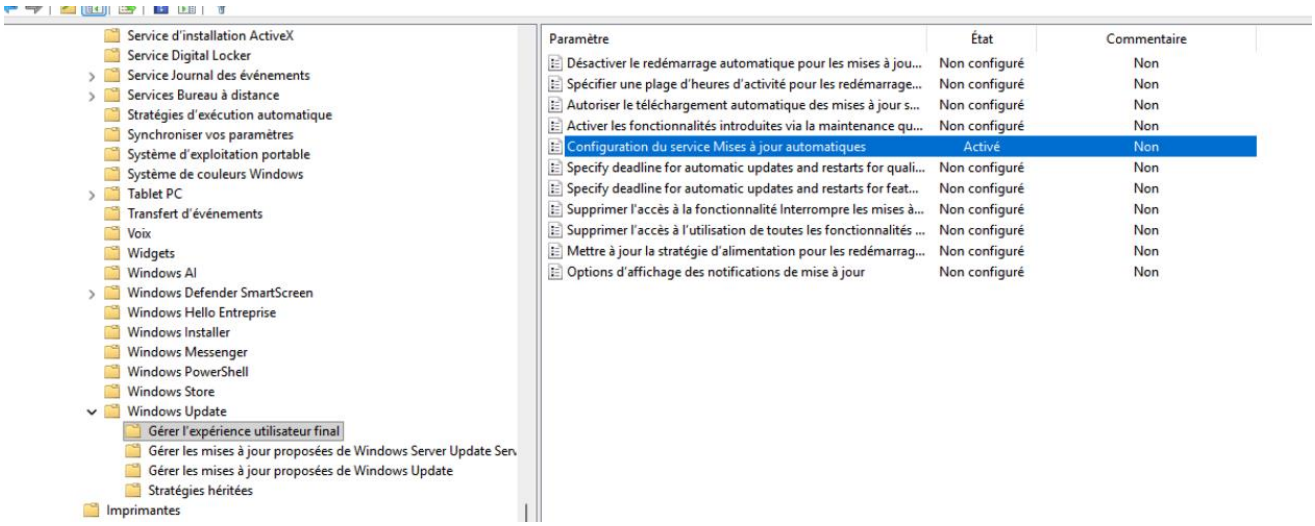
Ensuite, nous allons ouvrir « Autoriser le ciblage côté client » et y écrire « PC-Clients » dans le champ de ce dernier afin que notre serveur WSUS le cible automatiquement dans ce dernier :

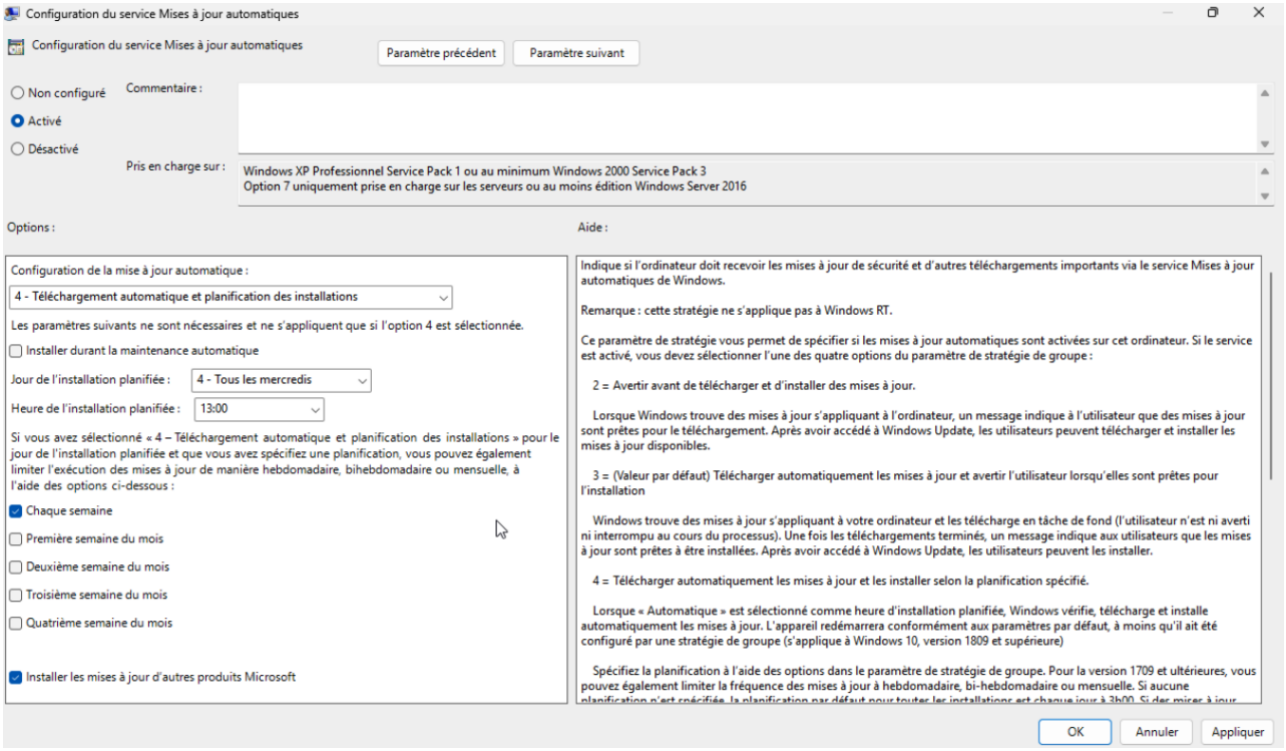


Ensuite, nous allons activer une GPO (Ne pas se connecter à des emplacements Internet Windows Update) pour ne pas récupérer les mises à jour depuis Internet (Windows Update) :

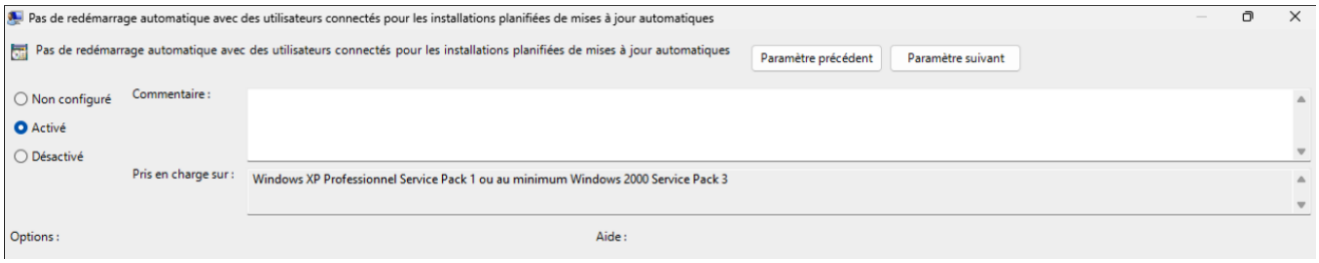


Une fois cela fait, nous allons revenir un peu en arrière dans le répertoire « Gérer l'expérience utilisateur final pour activer la configuration du service Mises à jour automatiques et y définir des paramètres personnalisés sur l'application et le téléchargement des mises à jour (dans notre cas, nous allons faire en sorte que les mises à jour s'installent chaque semaine à 13h) :

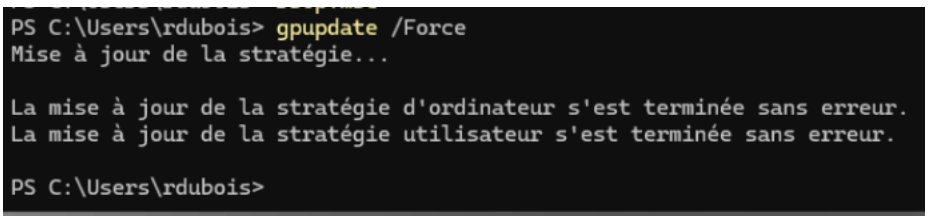




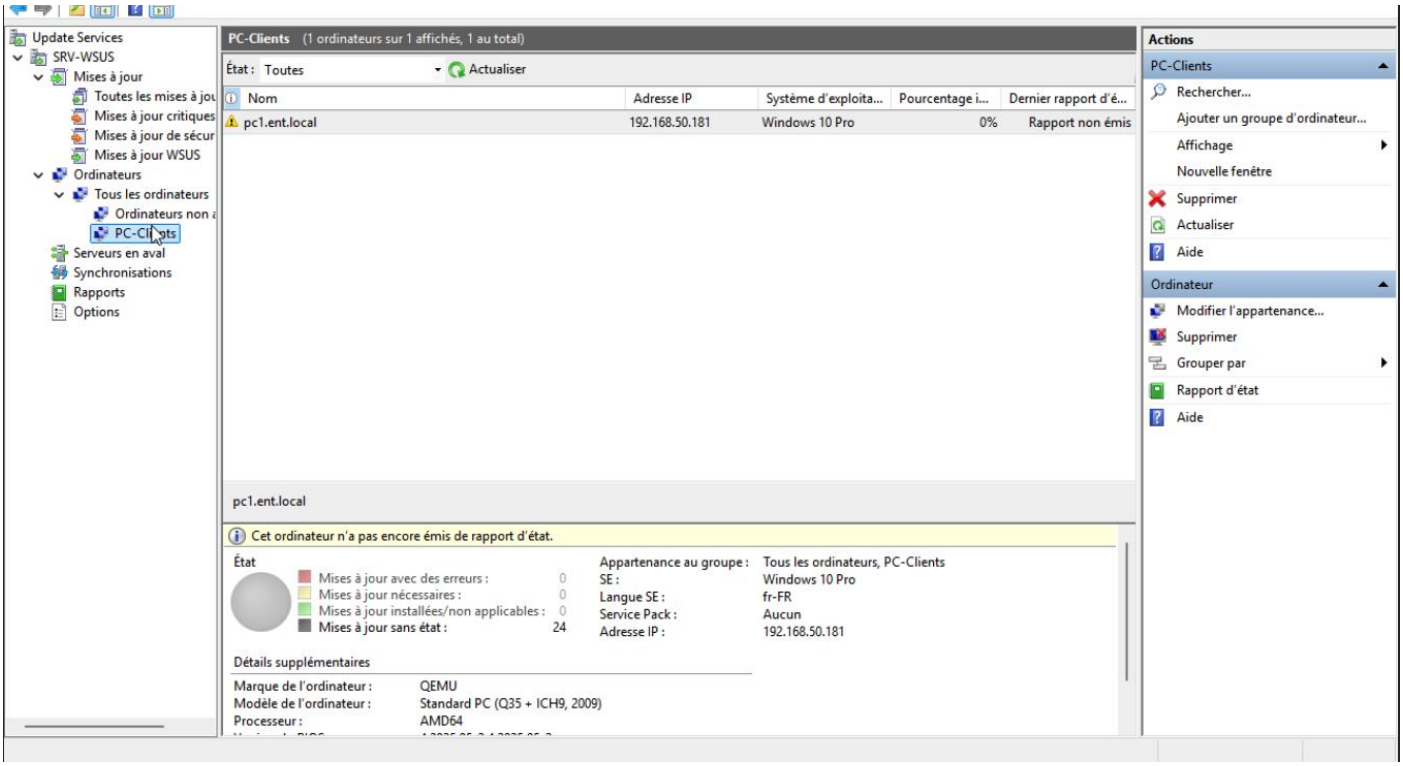
Maintenant, nous allons nous rendre en arrière dans le répertoire « Stratégies héritées » pour activer l'option « Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques » :



Une fois les GPO créer, nous allons les appliquer sur notre machine client grâce à la commande « **gpupdate /Force** » :

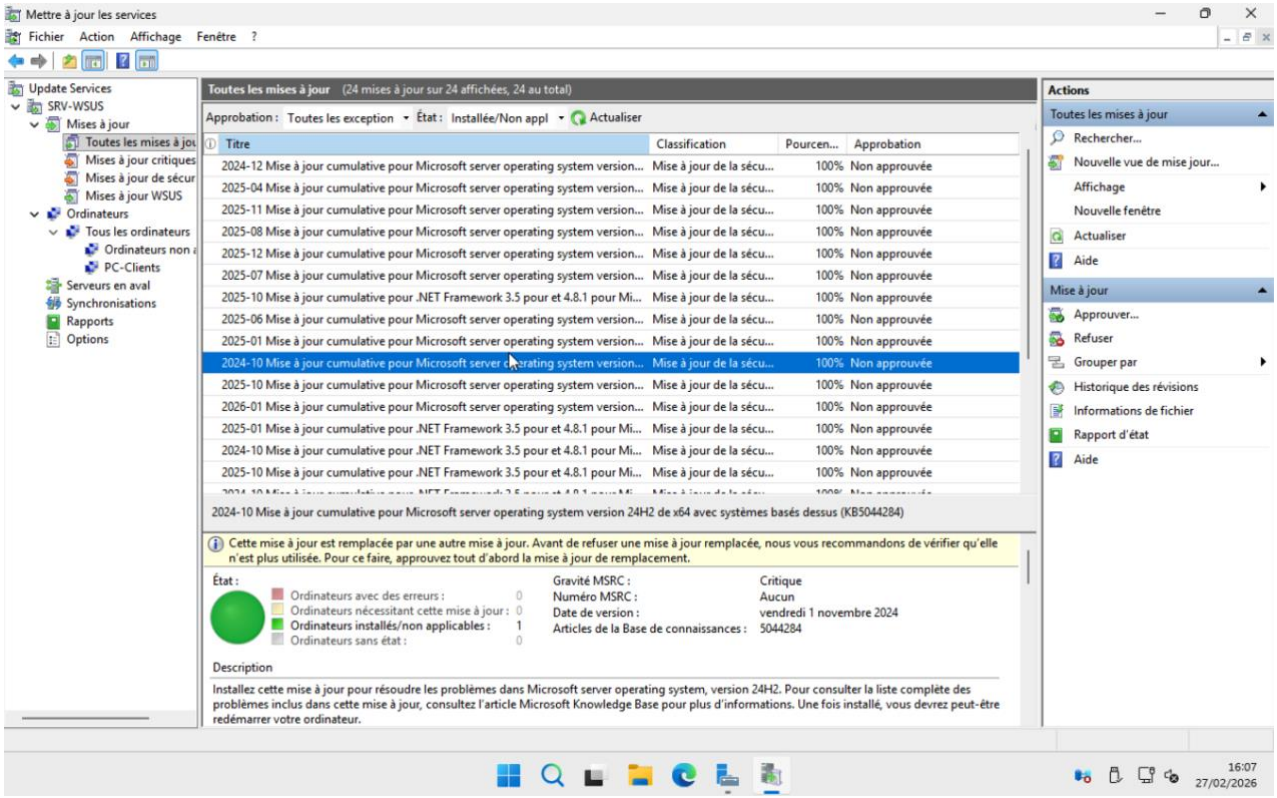


Une fois cela réalisé, la machine client devrait apparaitre sur notre serveur WSUS dans le groupe que nous avons créé :



Sur cet écran, nous pouvons avoir différentes informations sur notre machine tel que son nom, son IP, son OS, et pleins d'autres, on peut aussi voir l'état des différentes mises à jour (erreurs, nécessaires ou installées).

Dans l'onglet « Toutes les mises à jour », on peut observer une liste de mises à jour en attente d'approbation, ces dernières peuvent être approuvées pour par la suite être installées sur nos clients :



Maintenant que nos mises à jour ont été approuvée, nous pouvons vérifier nos clients et tenter de les déployer depuis Windows Update !

