CLINIQUE
TAMALOU

DIRECTION DES SYSTÈMES D'INFORMATION

Pôle Infrastructures & Sécurité

Création de l'infrastructure LEARN avec le domaine learn.local

Déploiement et Configuration d'une infrastructure Multi-Sites

Objet : Mise en place d'une infrastructure d'entreprise, réseaux, AD DS multi-sites, Routage (RRAS), DHCP, serveur WDS et MDT.

Auteur : Damien POLINSKY
Date : 1 janvier 2026

Table des matières

1 PRÉPARATION DE L'ENVIRONNEMENT VIRTUEL ET RÉSEAU

1.1 Création des réseaux virtuels

Préparation du terrain dans VMware en créant 4 réseaux distincts (Hôte uniquement). Il y aura un réseau de production et un réseau d'administration pour chaque site (Paris et Lyon).

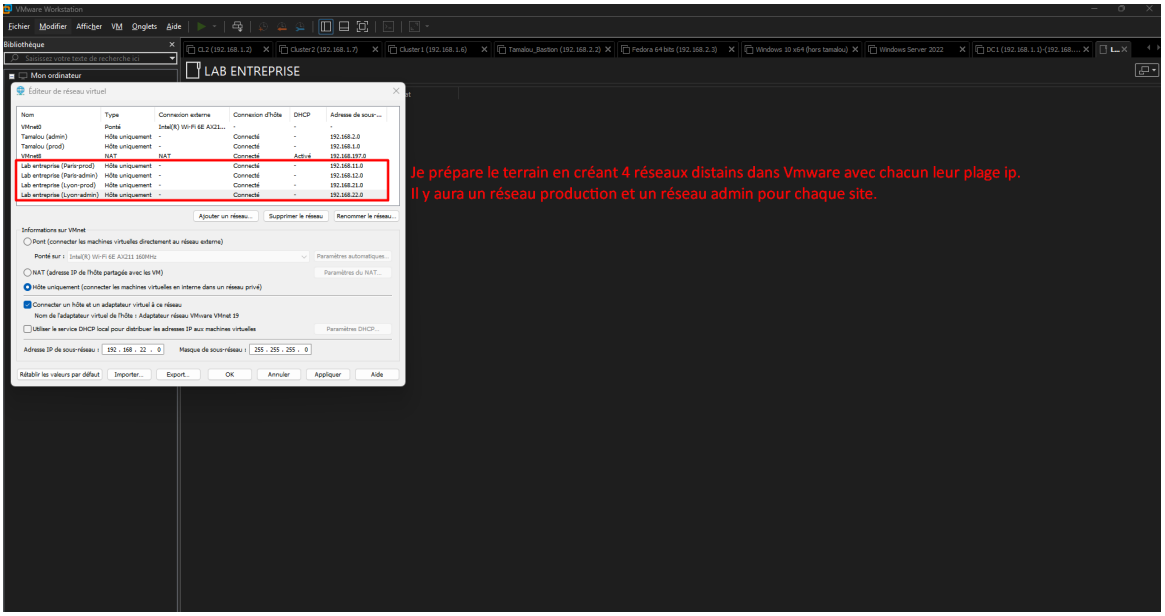

FIGURE 1 – Configuration des 4 réseaux (VMnet) dans l'éditeur VMware

1.2 Création des machines virtuelles

Création de 10 VMs réparties sur les deux sites. Le serveur RRAS fait exception : il doit disposer de 4 cartes réseau virtuelles car il fera office de passerelle pour faire communiquer les réseaux Admin et Prod.

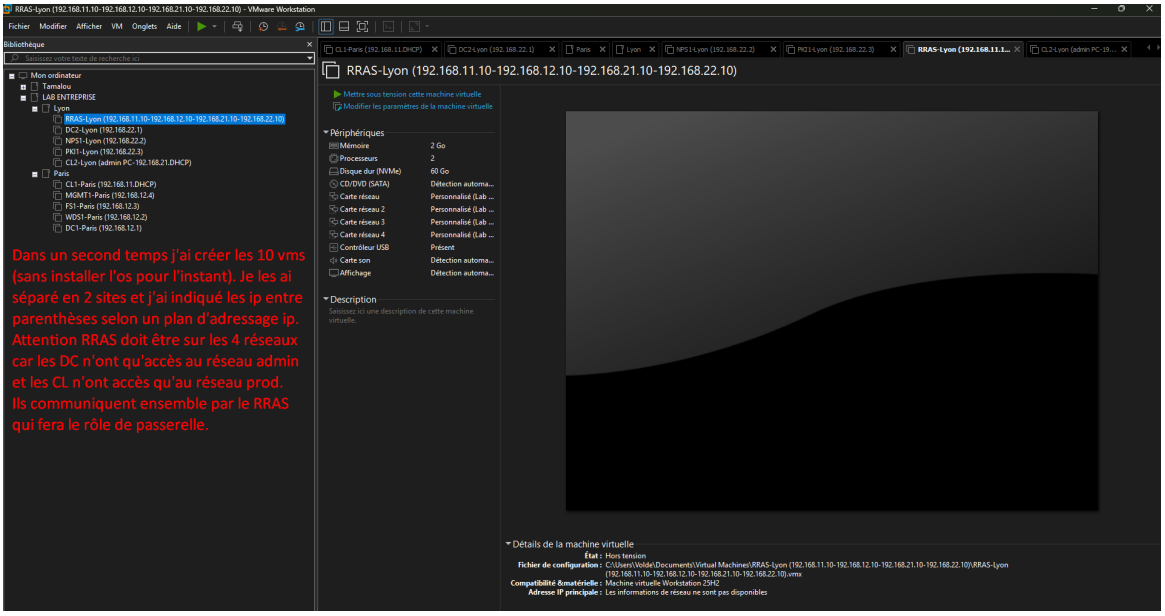

FIGURE 2 – Paramètres matériels du routeur RRAS (4 cartes réseau)

1.3 Installation du système d'exploitation

Installation de Windows Server 2025 sur les 8 serveurs de l'infrastructure (l'OS client Windows 11 sera installé plus tard).

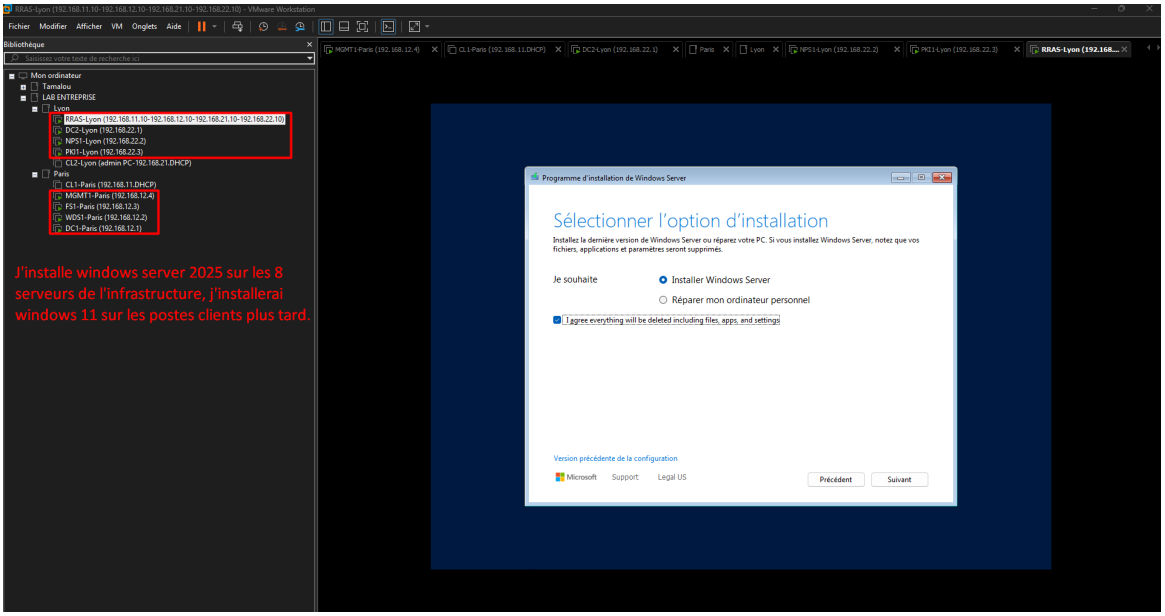

FIGURE 3 – Installation de Windows Server 2025

2 CONFIGURATION DU CONTRÔLEUR DE DOMAINE (DC1)

2.1 Configuration IPv4 de DC1

Attribution de l'adresse statique `192.168.12.1/24` à DC1. La passerelle par défaut pointe vers le futur RRAS (`192.168.12.10`) et le DNS pointe sur localhost (`127.0.0.1`).

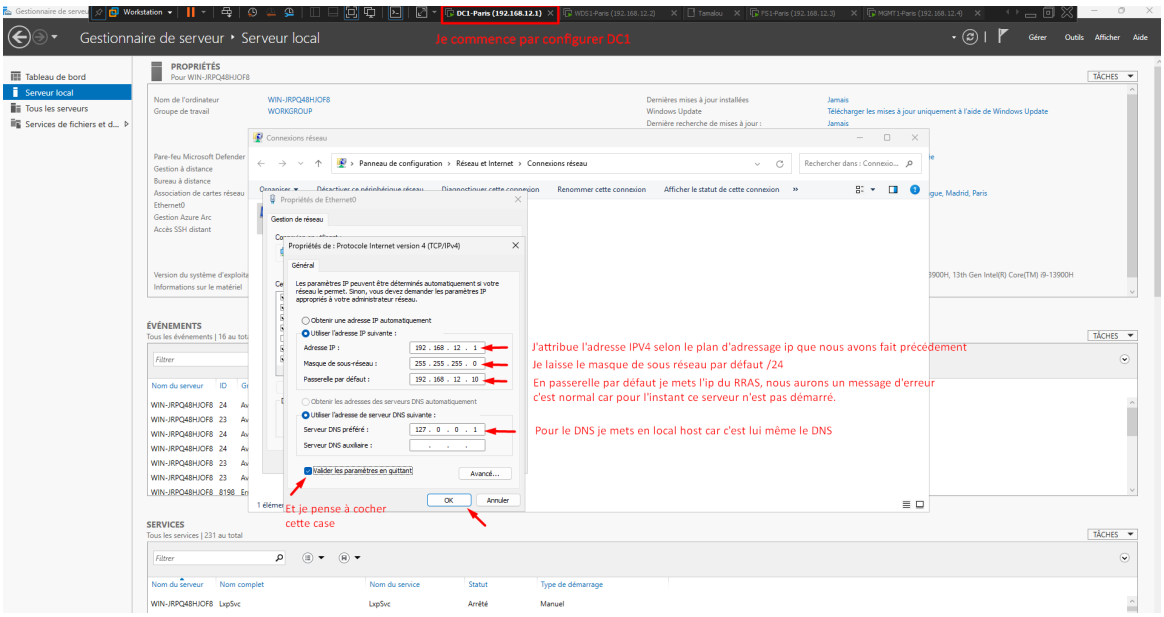

FIGURE 4 – Configuration IP statique du serveur DC1

2.2 Correction du conflit d'IP hôte

Pour éviter un conflit avec l'adresse `192.168.12.1`, l'adresse IP de la carte virtuelle correspondante sur la machine physique hôte est modifiée (ex : en `.253`).

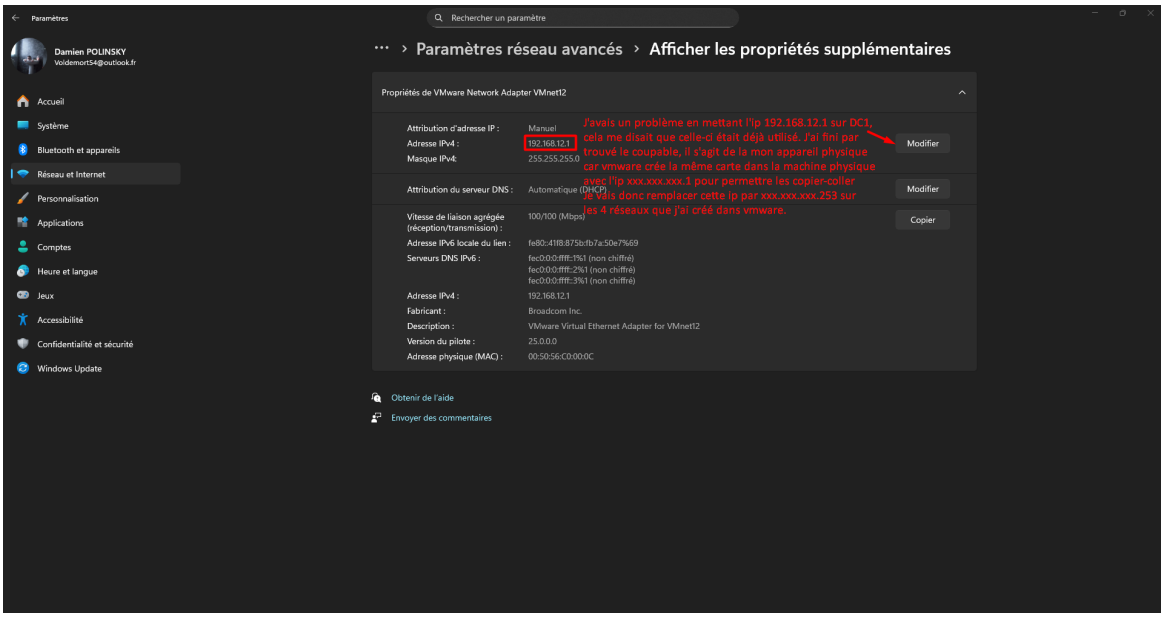

FIGURE 5 – Modification de l'IP de la carte VMnet sur l'hôte physique

2.3 Renommage du serveur

Modification du nom de l'ordinateur en `DC1` via les propriétés système, nécessitant un redémarrage.

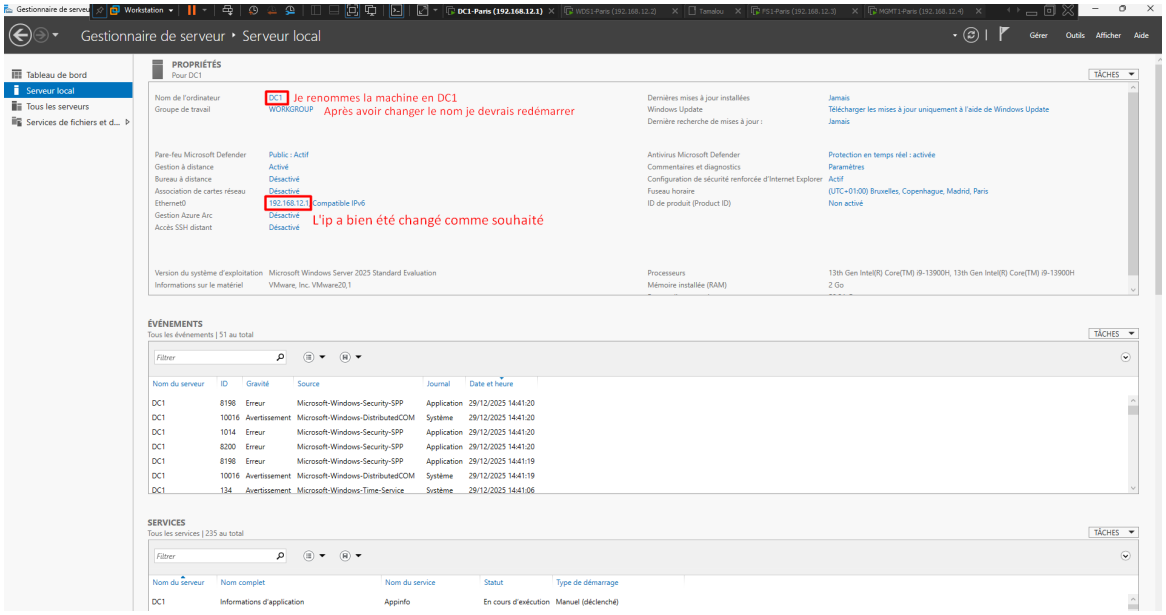

FIGURE 6 – Renommage de la machine en DC1

2.4 Lancement de l'ajout de rôles

Depuis le tableau de bord du Gestionnaire de serveur, lancement de l'assistant pour ajouter le rôle Active Directory.

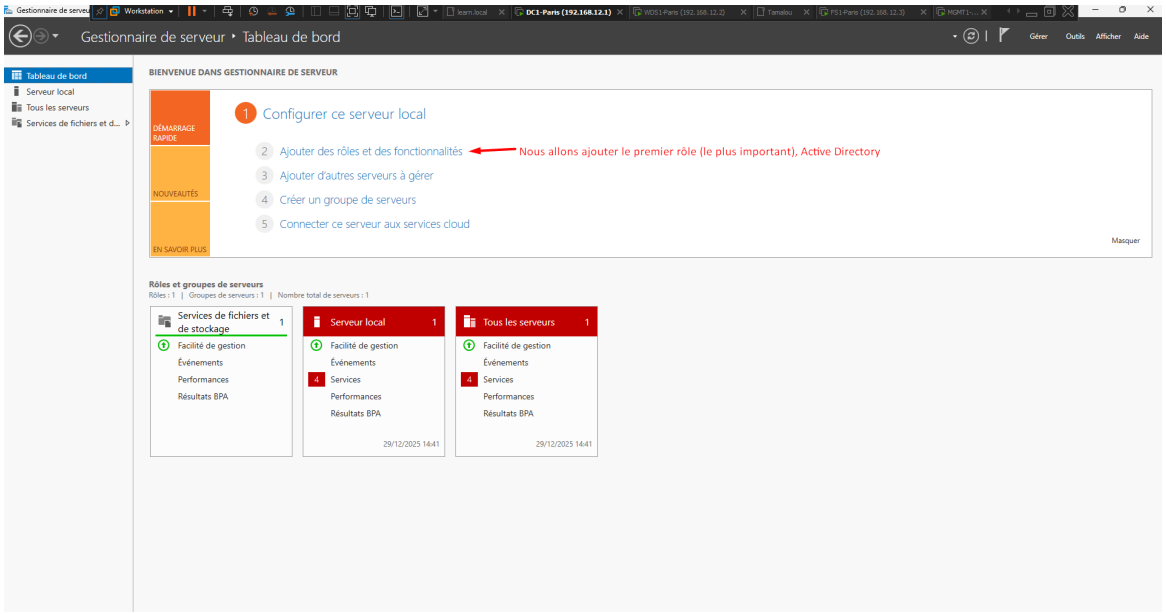

FIGURE 7 – Tableau de bord du Gestionnaire de serveur sur DC1

2.5 Sélection du rôle AD DS

Sélection du rôle "Services de domaine Active Directory" (AD DS) dans l'assistant.

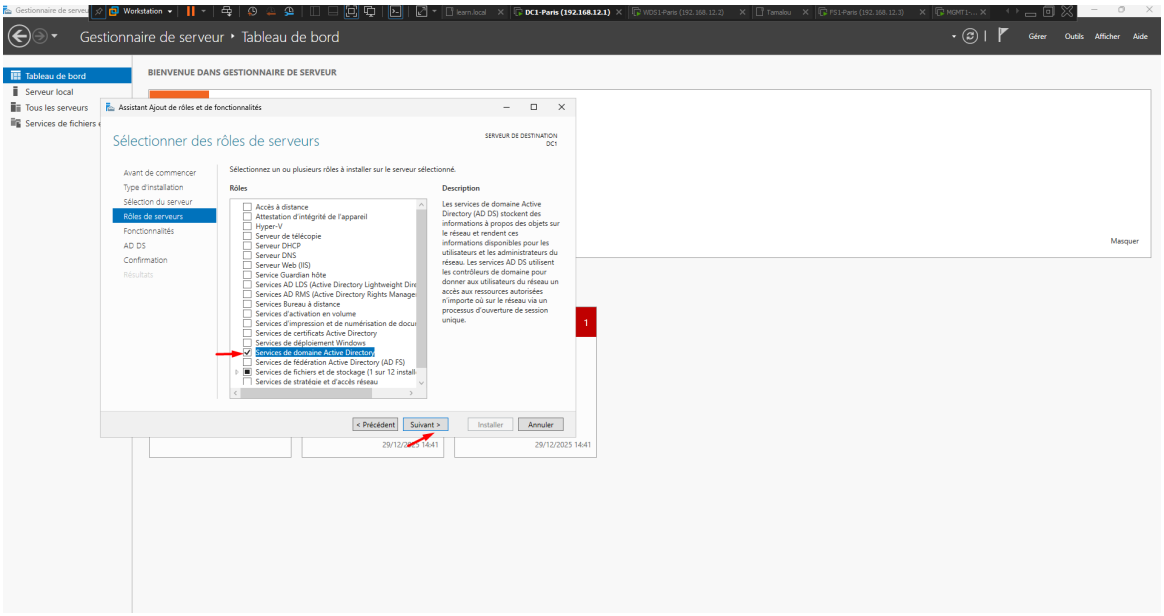

FIGURE 8 – Cochage du rôle AD DS

2.6 Promotion du serveur

Une fois l'installation terminée, un clic sur "Promouvoir ce serveur en contrôleur de domaine" lance la configuration.

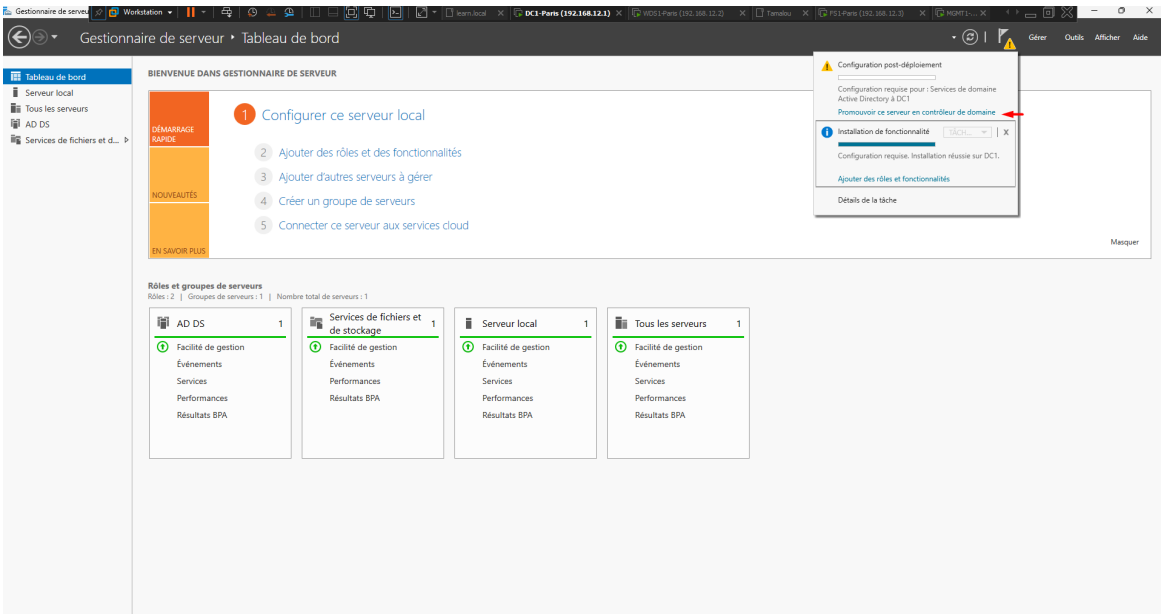

FIGURE 9 – Lien de promotion post-déploiement AD DS

2.7 Création d'une nouvelle forêt

Dans l'assistant, sélection de "Ajouter une nouvelle forêt" et définition du nom de domaine racine : `learn.local`.

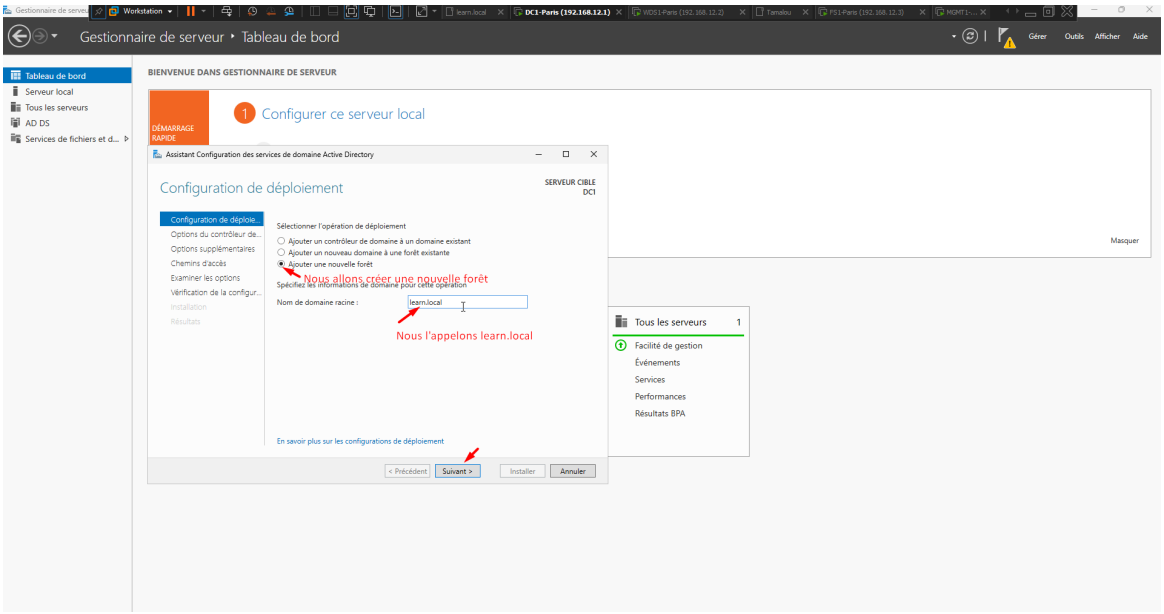

FIGURE 10 – Création de la forêt learn.local

2.8 Options du contrôleur de domaine

Maintien des options par défaut (Serveur DNS et Catalogue global cochés) et saisie d'un mot de passe de restauration (DSRM) robuste.

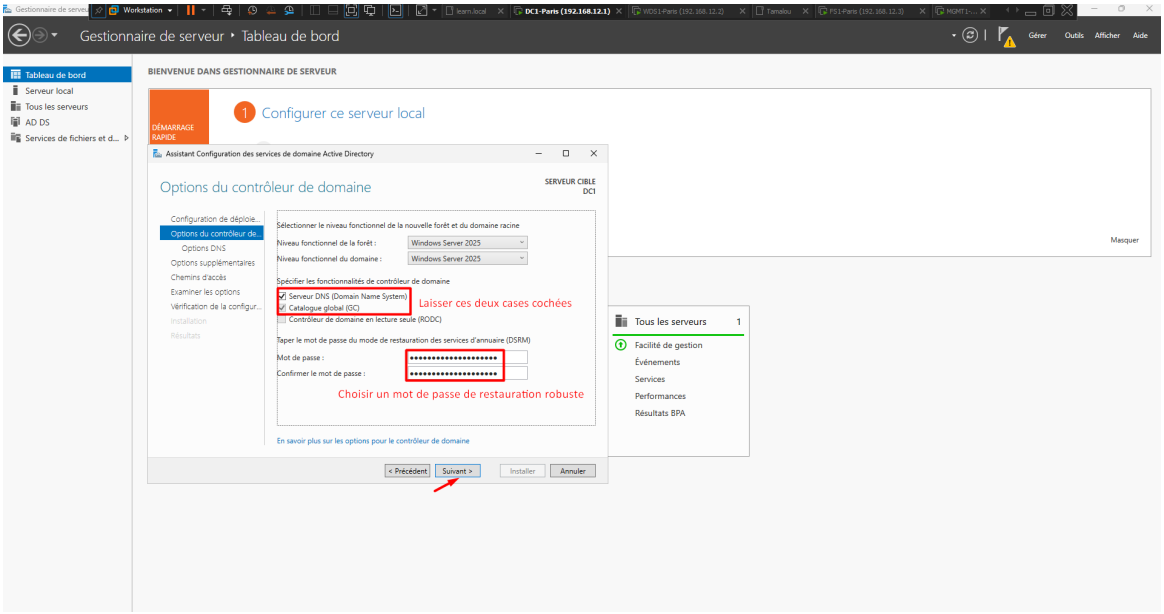

FIGURE 11 – Options du DC et mot de passe de restauration

2.9 Avertissement de délégation DNS

L'avertissement concernant la délégation DNS peut être ignoré dans ce contexte de création de forêt autonome.

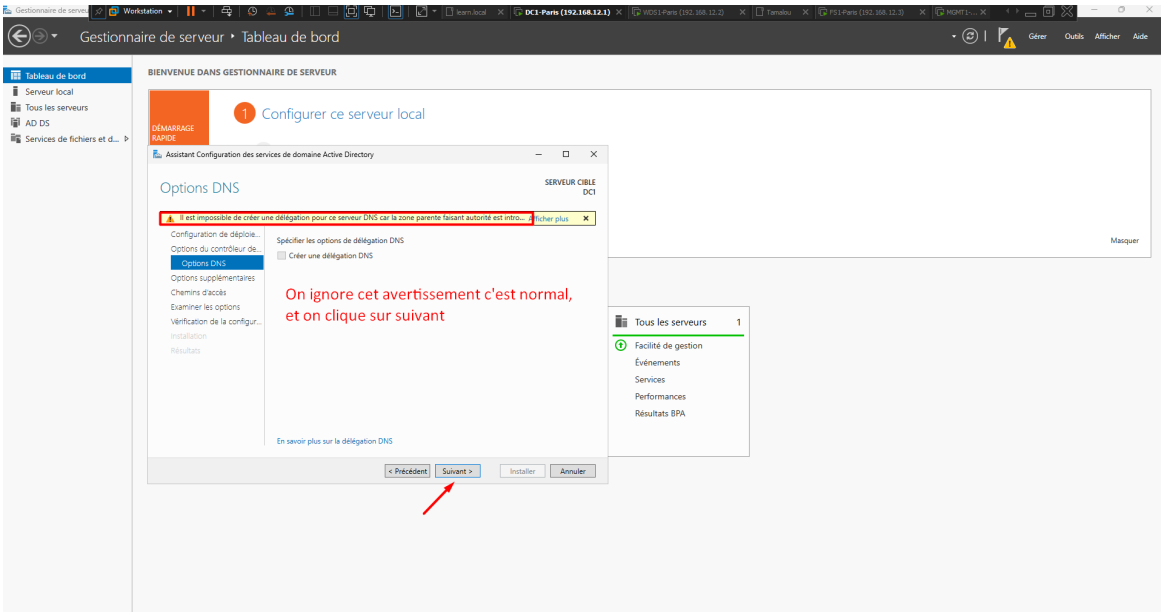

FIGURE 12 – Avertissement sur la délégation DNS

2.10 Nom de domaine NetBIOS

Le nom de domaine NetBIOS généré automatiquement (`LEARN`) est conservé.

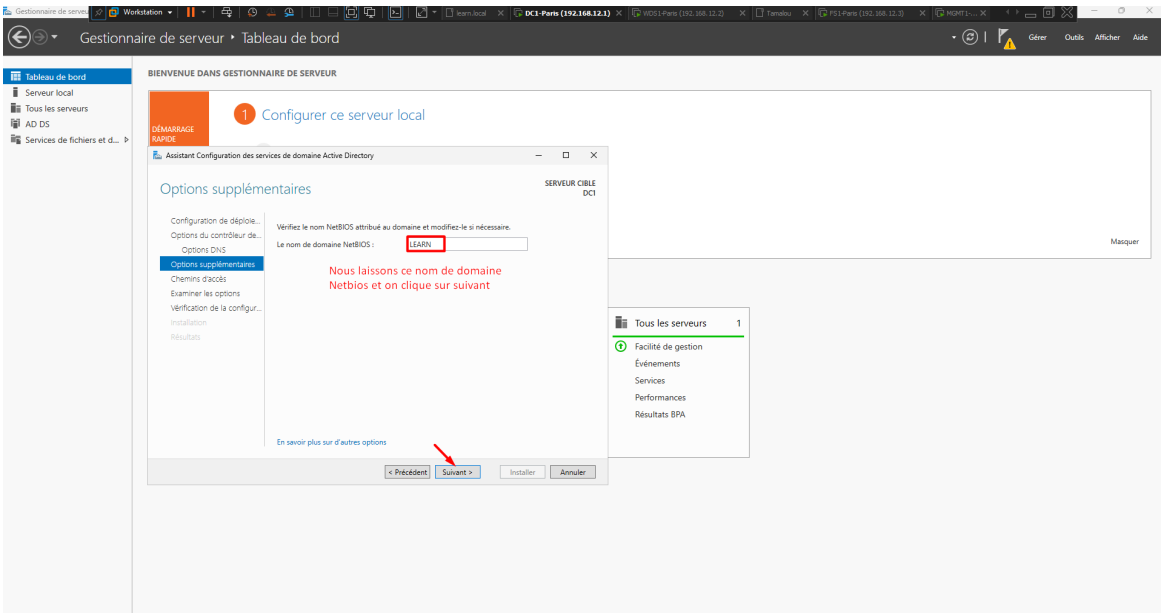

FIGURE 13 – Validation du nom NetBIOS LEARN

2.11 Chemins d'accès AD DS

Les chemins d'accès par défaut pour la base de données, les fichiers journaux et le dossier SYSVOL sont laissés tels quels.

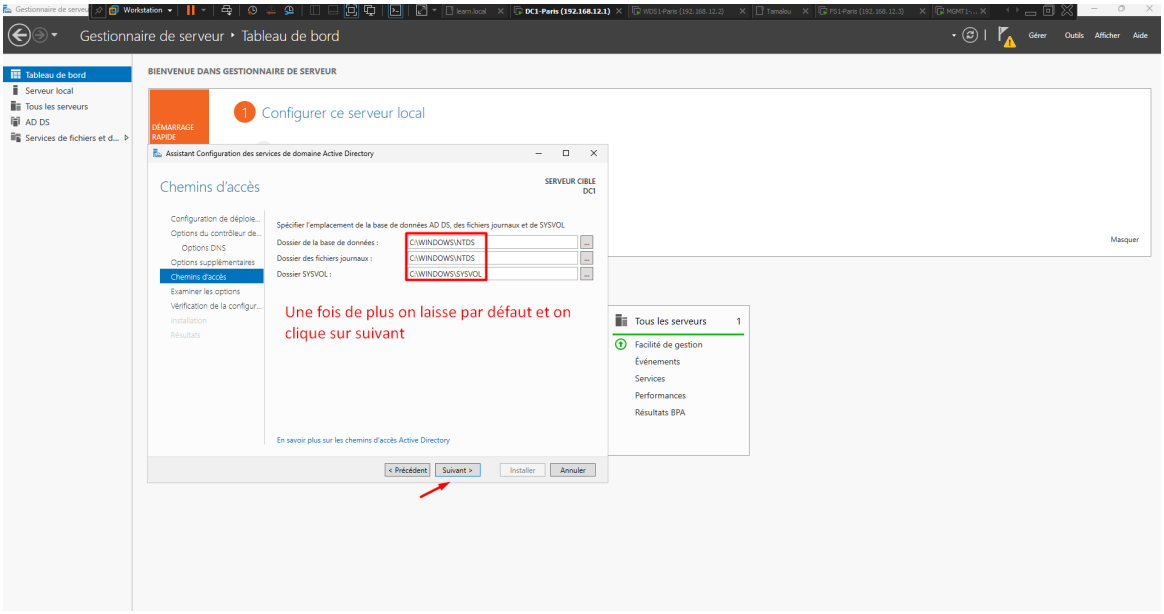

FIGURE 14 – Chemins d'accès aux fichiers de la base de données

2.12 Validation et installation

Toutes les vérifications de la configuration requise ayant donné satisfaction, l'installation est lancée. Le serveur redémarrera automatiquement.

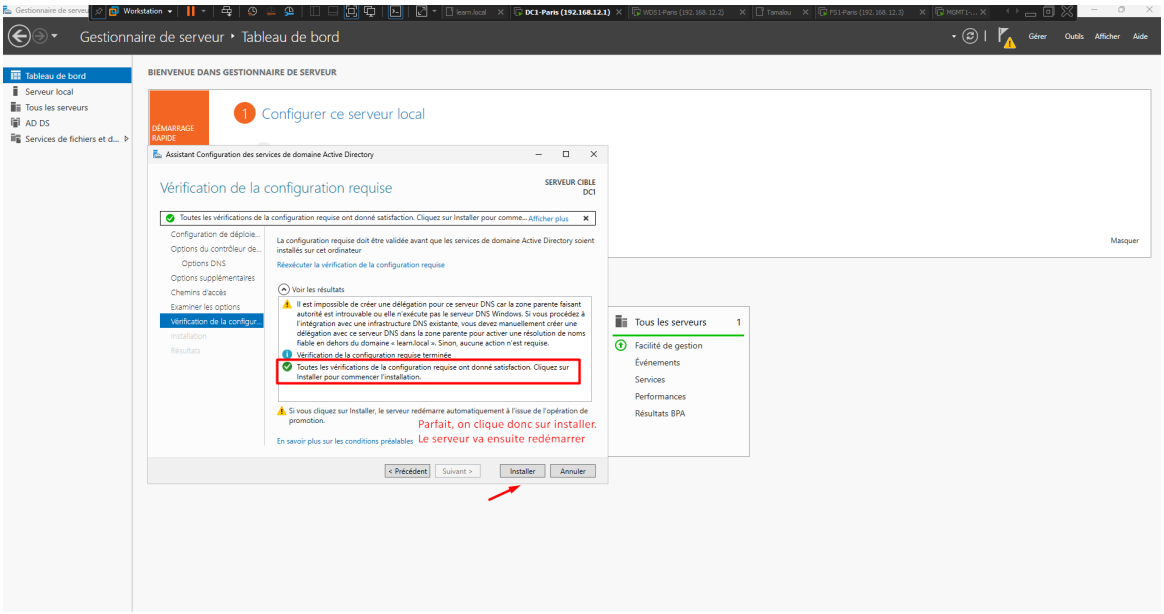

FIGURE 15 – Succès de la vérification de la configuration requise

3 CONFIGURATION DU SERVEUR DE ROUTAGE (RRAS)

3.1 Configuration IP du routeur RRAS

La machine est renommée `RRAS`. Ses 4 cartes réseau sont renommées (Lyon-admin, Lyon-prod, Paris-admin, Paris-prod) et configurées avec leurs adresses IP respectives se terminant par `.10`.

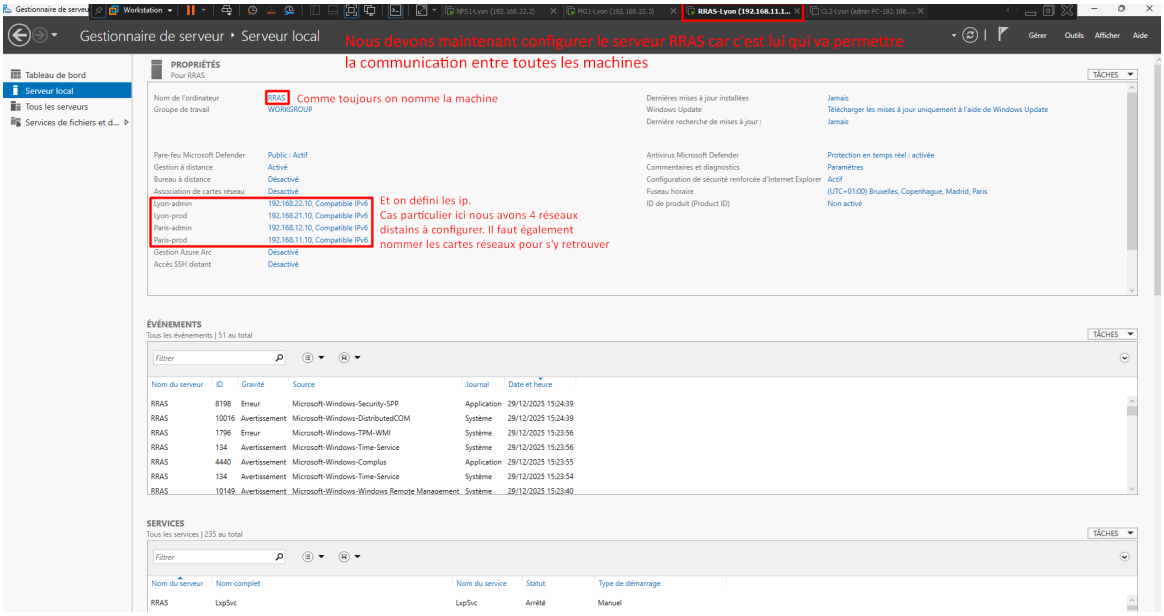

FIGURE 16 – Configuration du nom et des 4 cartes réseau du RRAS

3.2 Ajout du rôle d'accès distant

Dans le Gestionnaire de serveur, lancement de l'assistant d'ajout de rôles et sélection du rôle "Accès à distance".

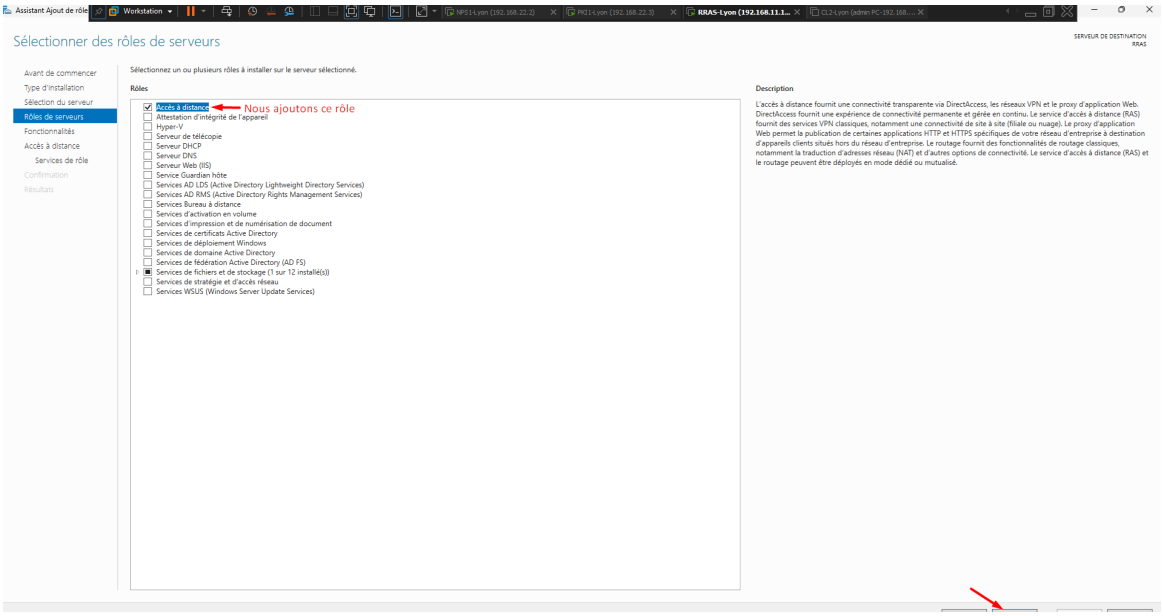

FIGURE 17 – Sélection du rôle Accès à distance

3.3 Services de rôle (Routage)

Il est indispensable de cocher la case "Routage" (qui coche automatiquement DirectAccess et VPN) pour permettre la communication inter-réseaux.

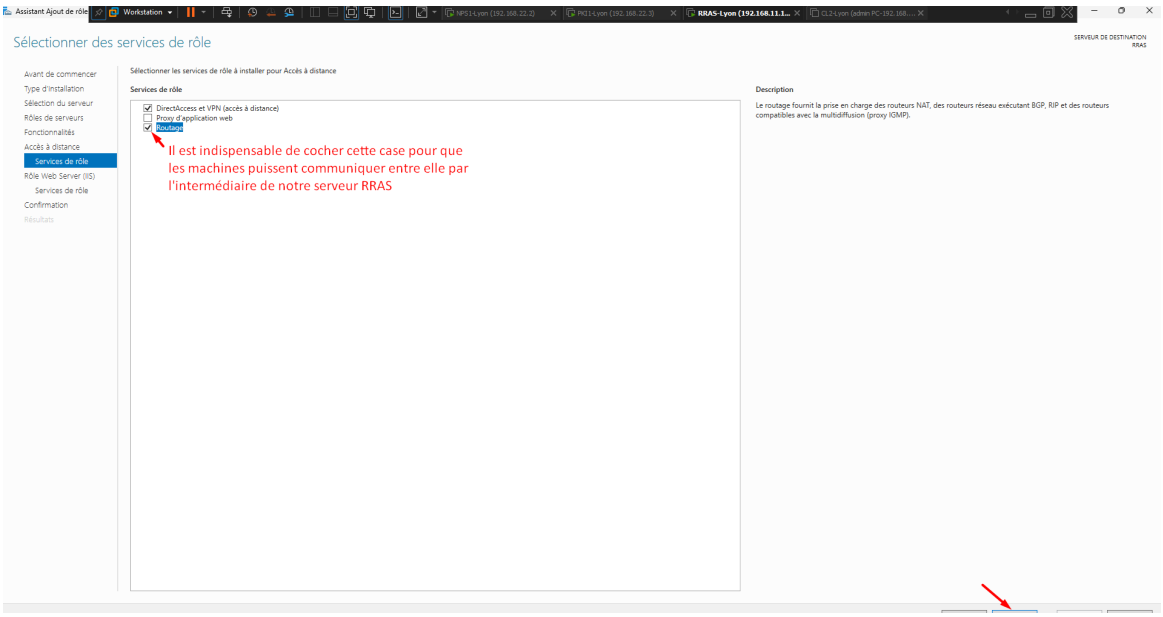

FIGURE 18 – Sélection du service de rôle Routage

3.4 Confirmation d'installation (RRAS)

L'assistant affiche le résumé des fonctionnalités à installer (Routage, Serveur Web IIS, etc.).

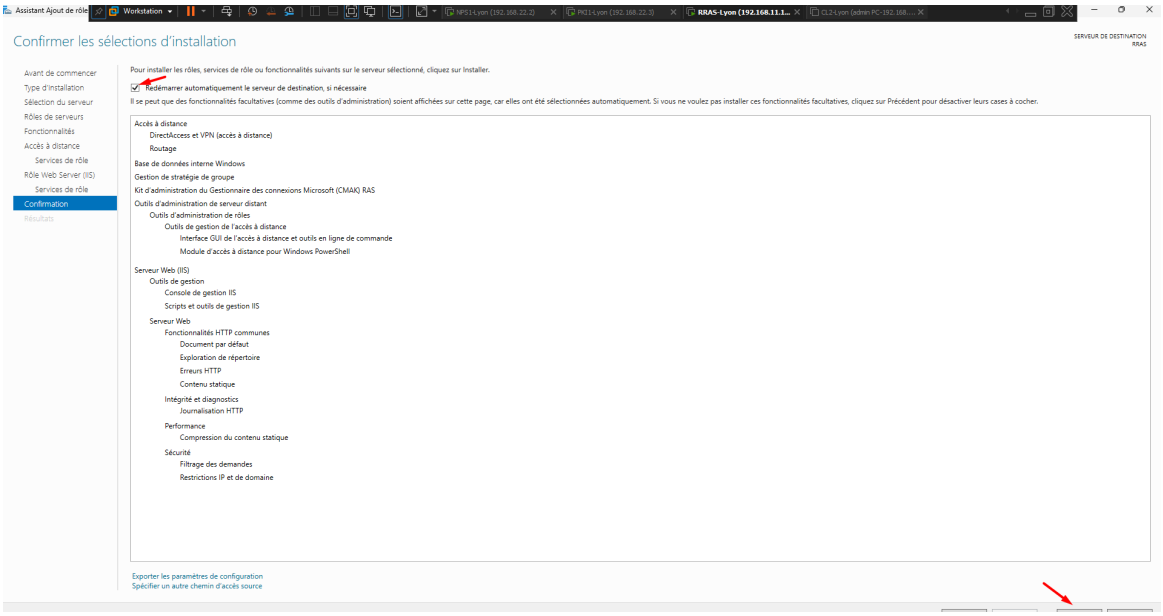

FIGURE 19 – Confirmation avant installation du rôle sur RRAS

3.5 Tableau de bord après installation

De retour sur le Gestionnaire de serveur de RRAS, on constate que le rôle "Accès à distance" (ainsi que IIS, installé comme dépendance) est désormais présent dans le tableau de bord.

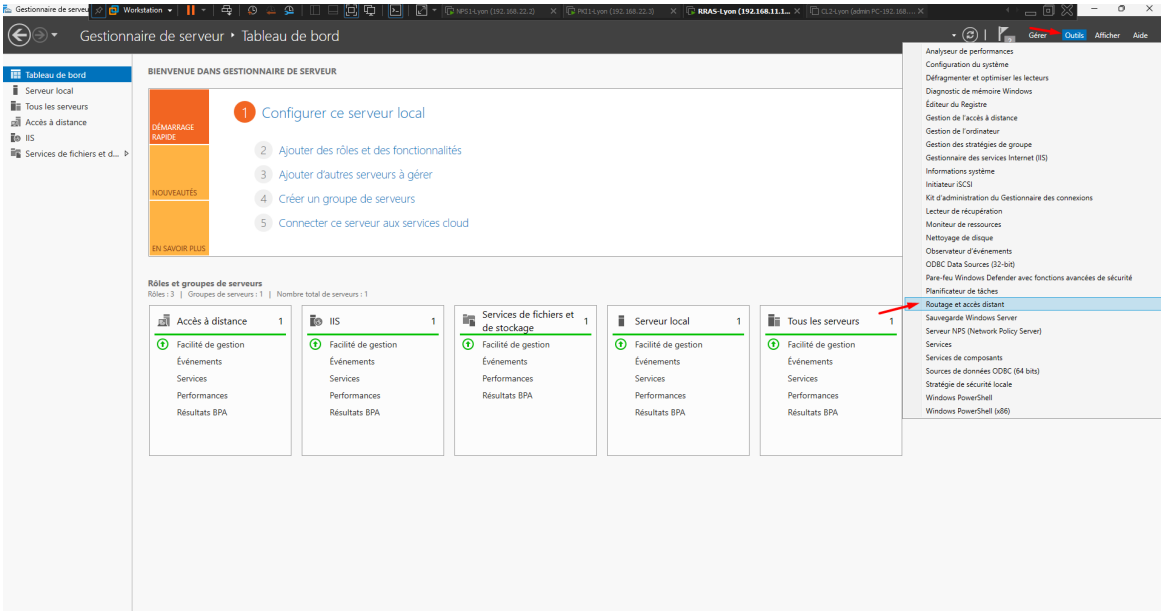

FIGURE 20 – Le rôle Accès à distance est installé sur le serveur RRAS

3.6 Configuration du routage

On ouvre la console "Routage et accès distant". On effectue un clic-droit sur le serveur local (RRAS) et on sélectionne "Configurer et activer le routage et l'accès à distance".

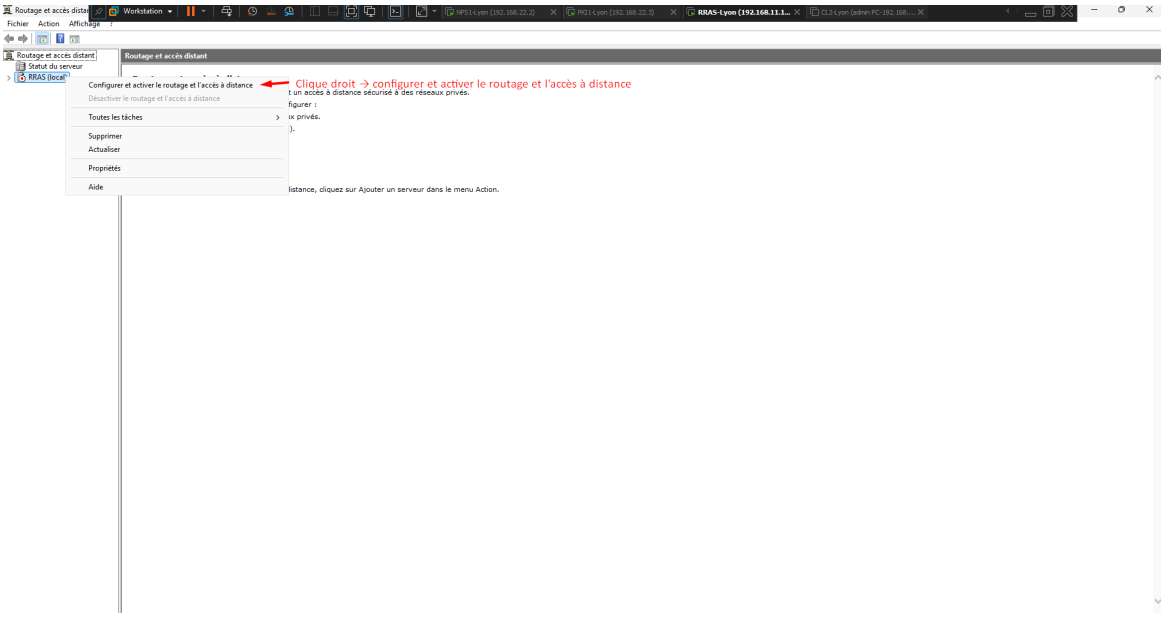

FIGURE 21 – Lancement de l'assistant de configuration RRAS

3.7 Configuration personnalisée

Dans l'assistant d'installation, nous choisissons l'option "Configuration personnalisée" afin de sélectionner manuellement les services dont nous avons besoin.

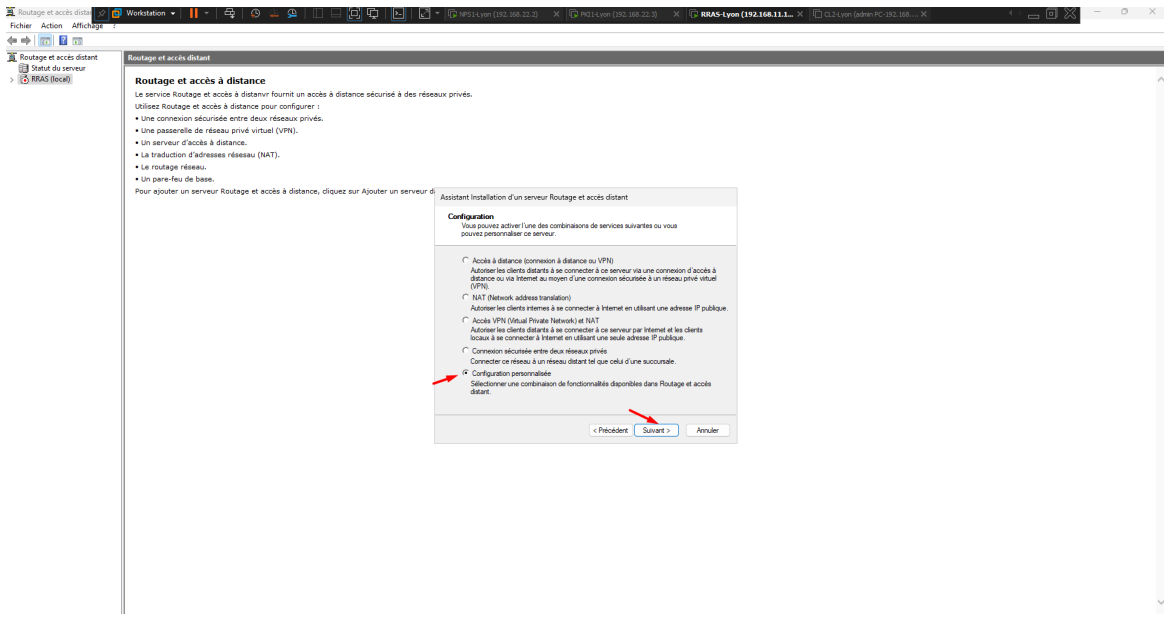

FIGURE 22 – Sélection de la configuration personnalisée

3.8 Sélection des services de routage

Nous cochons "Routage réseau" en priorité pour que tout le monde puisse communiquer ensemble. Nous activons également "Accès VPN" (que nous configurerons plus tard).

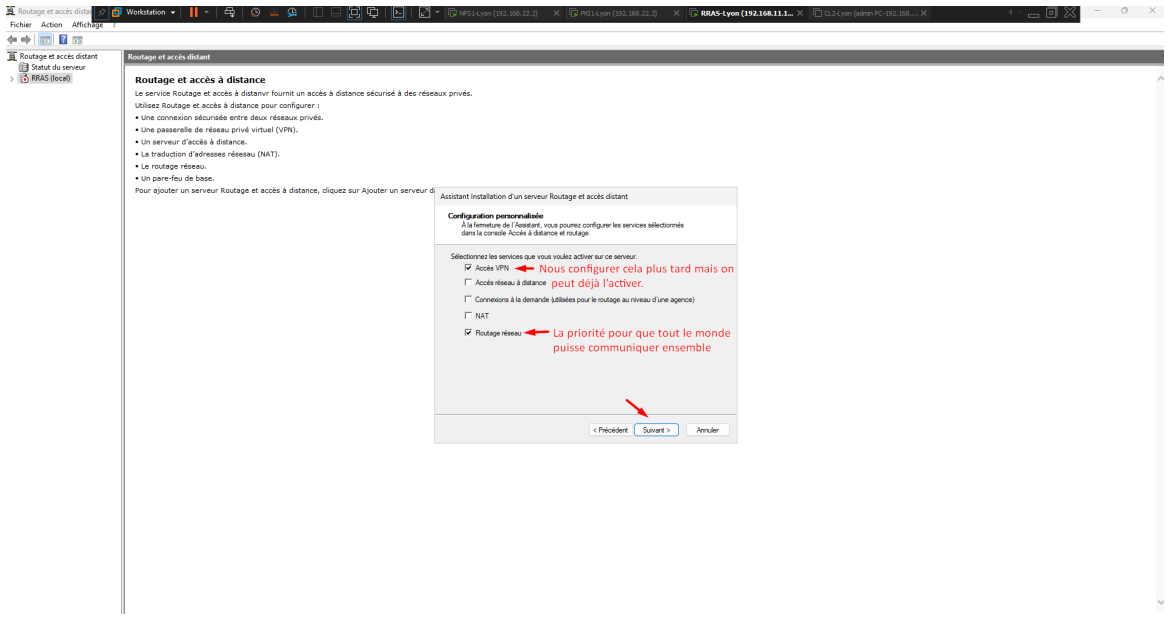

FIGURE 23 – Sélection des services VPN et Routage

3.9 Démarrage du service

L'assistant termine la configuration. Le service de routage est bien démarré, comme l'indique la flèche verte sur l'icône du serveur dans la console.

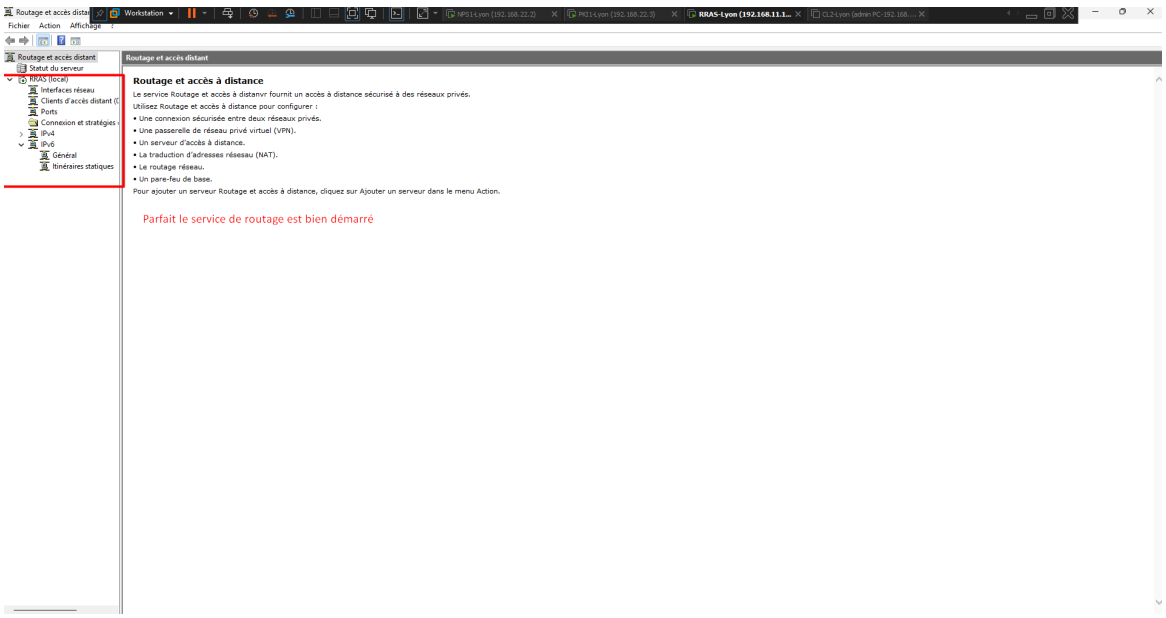

FIGURE 24 – Le service de routage est actif et opérationnel

3.10 Test de routage (Ping)

Depuis DC1, après avoir autorisé les requêtes ICMP dans le pare-feu du RRAS, nous effectuons des tests de ping. Le ping vers l'interface `192.168.12.10` (même plage) et vers `192.168.22.10` (plage Lyon-admin) fonctionne. Cela signifie que le routage fonctionne correctement.

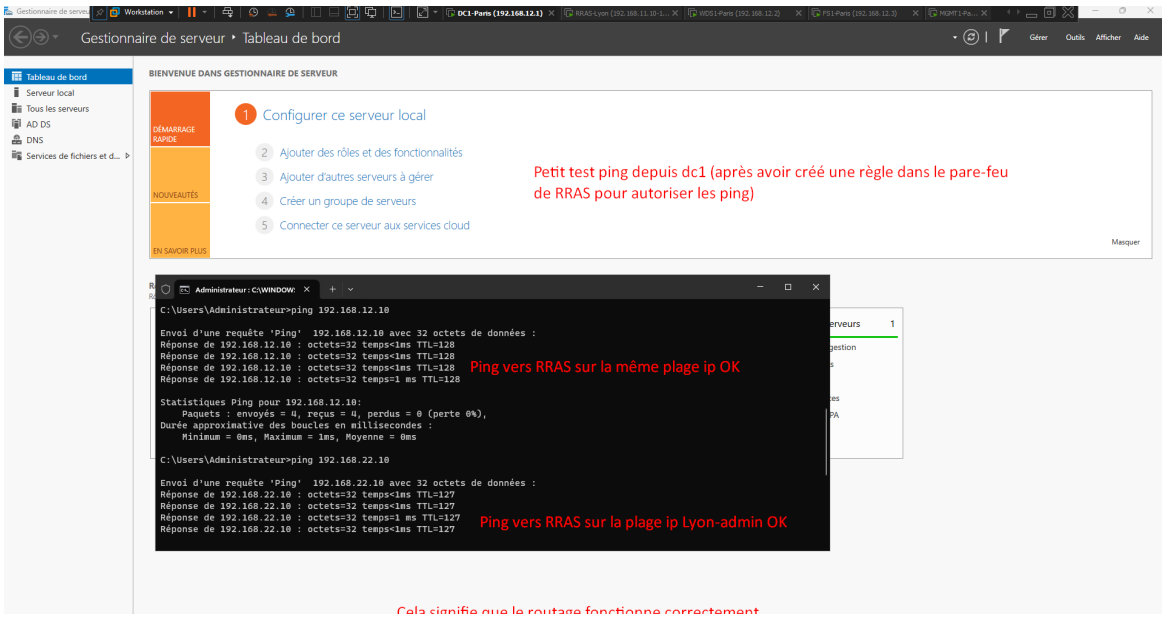

FIGURE 25 – Tests de connectivité inter-réseaux réussis depuis DC1

3.11 Configuration DNS sur RRAS

Maintenant que la communication est établie, nous allons pouvoir joindre RRAS au domaine `learn.local`. Mais avant, il est important de définir DC1 (`192.168.12.1`) comme serveur DNS principal sur la carte réseau "Paris-admin".

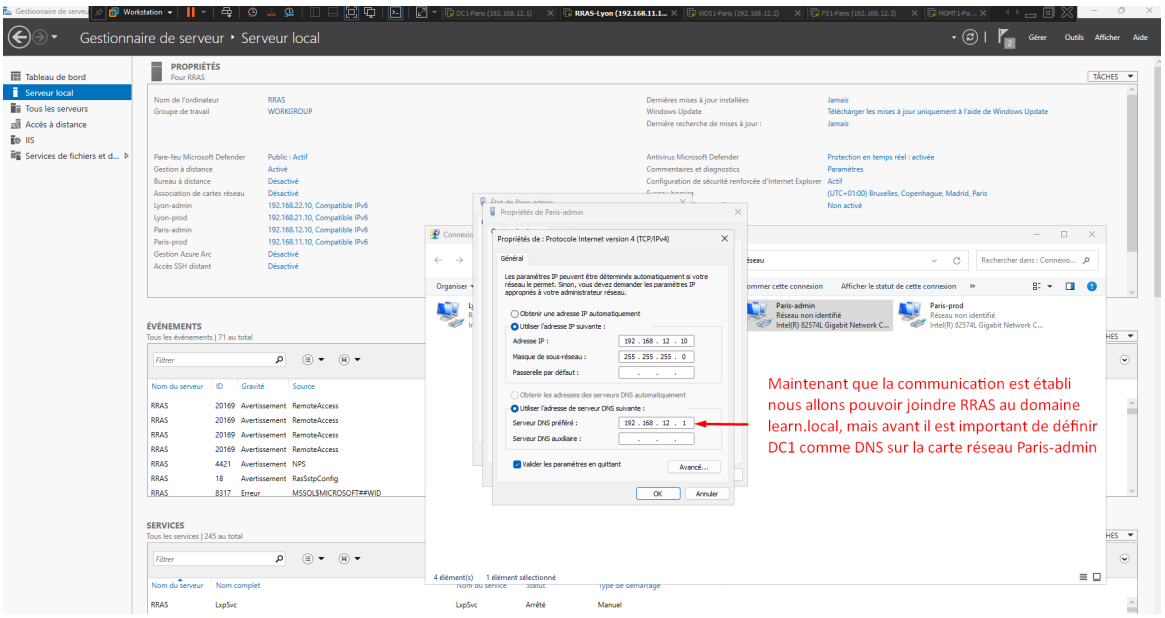

FIGURE 26 – Définition de DC1 comme serveur DNS sur le routeur

3.12 Jonction au domaine

Dans les propriétés système du serveur RRAS, on clique sur Modifier pour changer le nom de domaine. On indique le domaine à rejoindre, ici `learn.local`, puis on valide avec les identifiants administrateur.

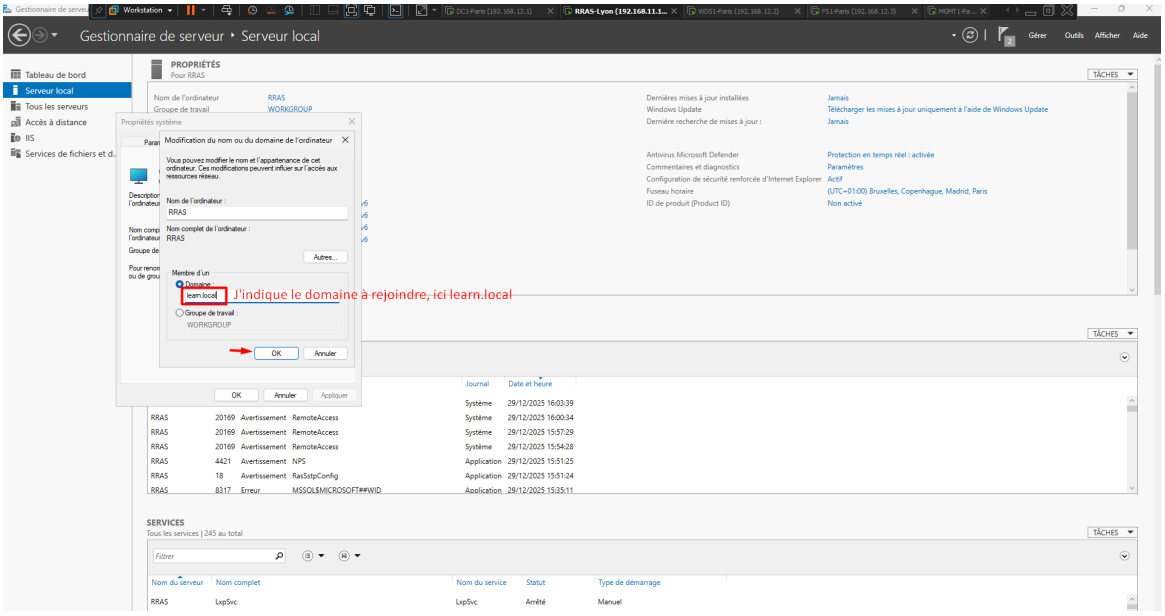

FIGURE 27 – Intégration du serveur RRAS au domaine

4 TOPOLOGIE ACTIVE DIRECTORY (SITES ET SERVICES)

4.1 Lancement de l'outil Sites et services

Sur DC1, nous allons maintenant configurer le multi-site pour Paris et Lyon. Depuis le menu Outils du Gestionnaire de serveur, on ouvre la console "Sites et services Active Directory".

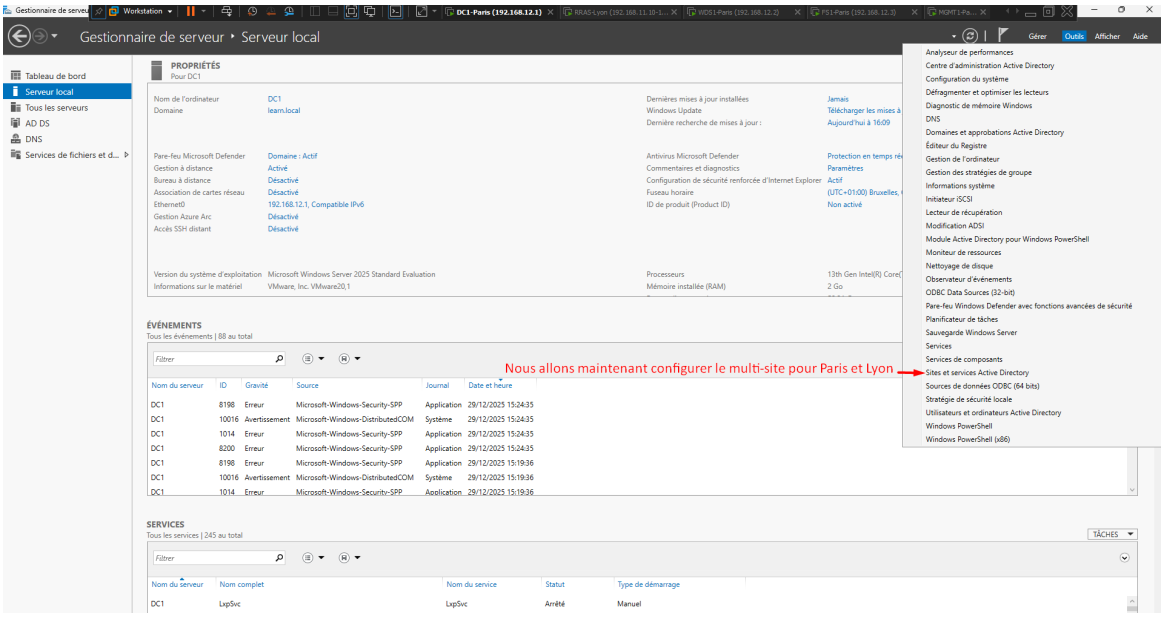

FIGURE 28 – Accès à la console Sites et services Active Directory

4.2 Renommage du site par défaut

Par défaut, le premier site se nomme "Default-First-Site-Name". On effectue un clic-droit sur cet objet, on sélectionne "Renommer" et nous l'appelons "Paris".

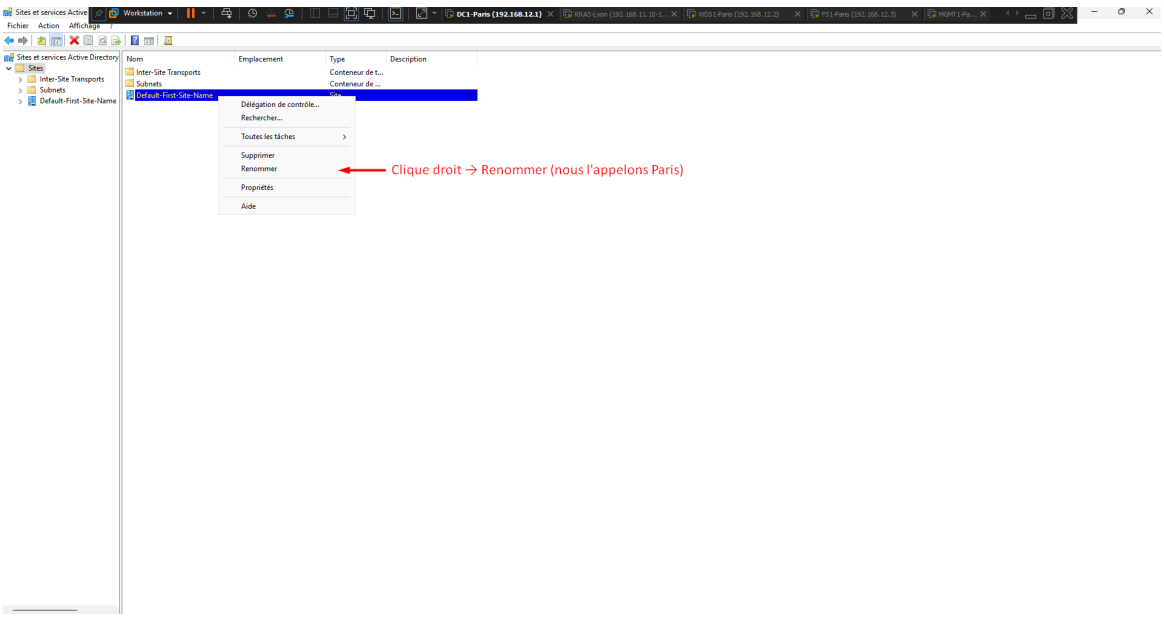

FIGURE 29 – Le site principal est renommé en Paris

4.3 Création du site de Lyon

On effectue un clic-droit sur le dossier "Sites" puis on sélectionne "Nouveau site..." pour créer le site distant de Lyon.

FIGURE 30 – Création du nouveau site logique pour Lyon

4.4 Création des sous-réseaux

Nous allons maintenant créer les 4 sous-réseaux et les lier aux sites correspondants. On effectue un clic-droit sur le dossier "Subnets" et on choisit "Nouveau sous-réseau...".

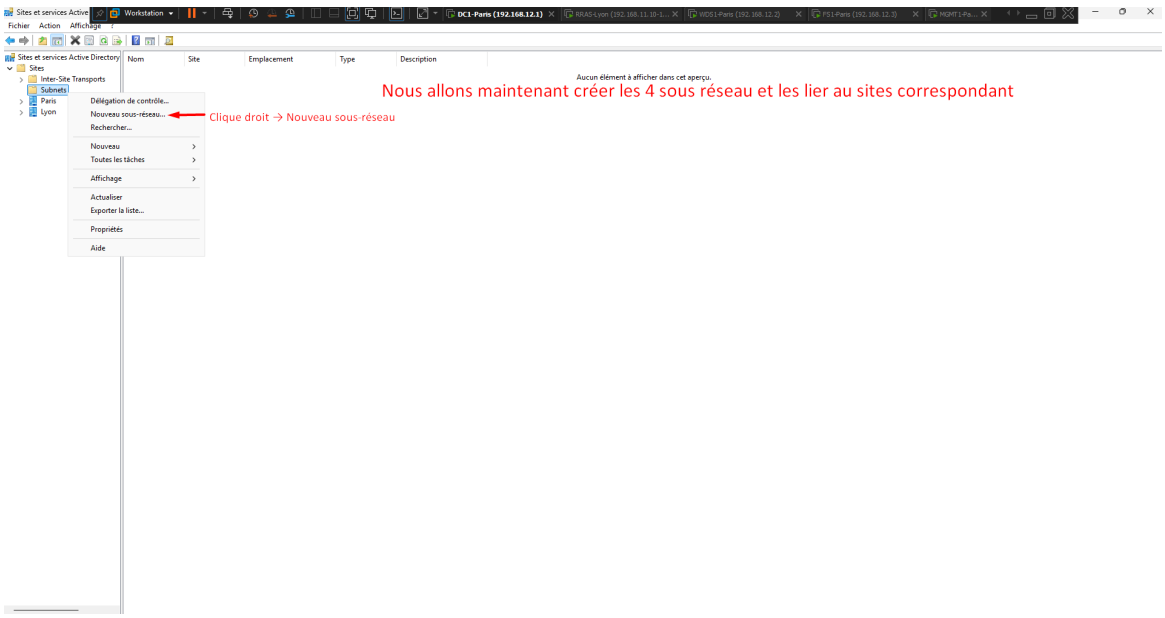

FIGURE 31 – Lancement de la création d'un nouveau sous-réseau

4.5 Association d'une plage IP à un site

On indique le préfixe réseau, par exemple la plage `192.168.11.0/24` (Paris-prod), puis nous sélectionnons le site correspondant dans la liste en dessous.

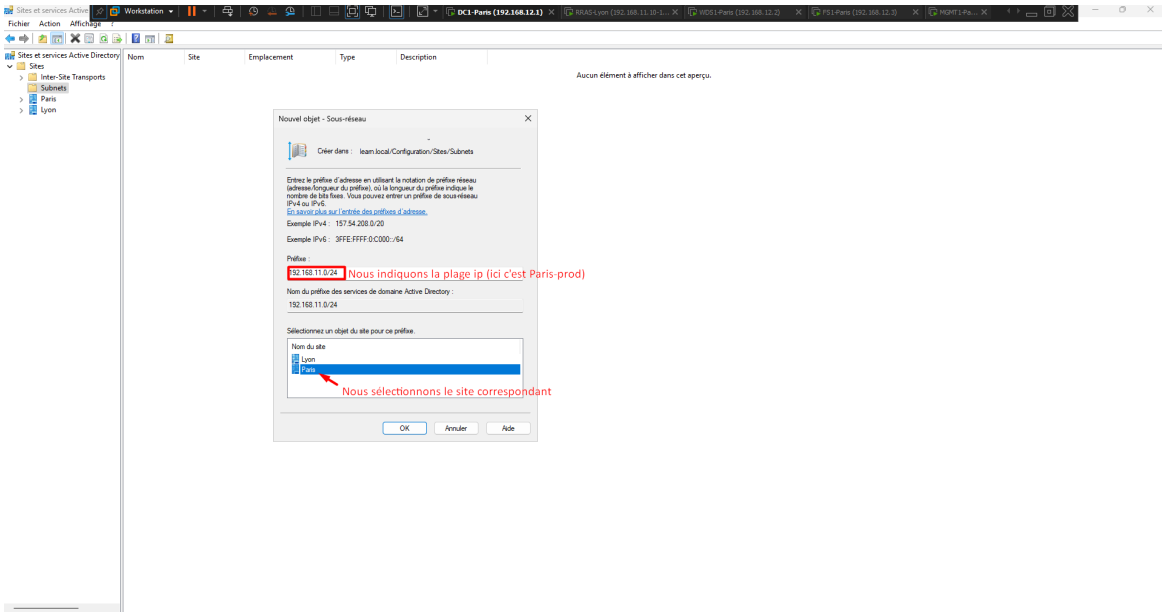

FIGURE 32 – Liaison du sous-réseau 192.168.11.0/24 à son site

4.6 Vérification de la topologie

Nous avons créé nos 4 sous-réseaux (`192.168.11.0/24`, `192.168.12.0/24`, `192.168.21.0/24`, `192.168.22.0/24`) et nous les avons tous liés au bon site (Paris ou Lyon).

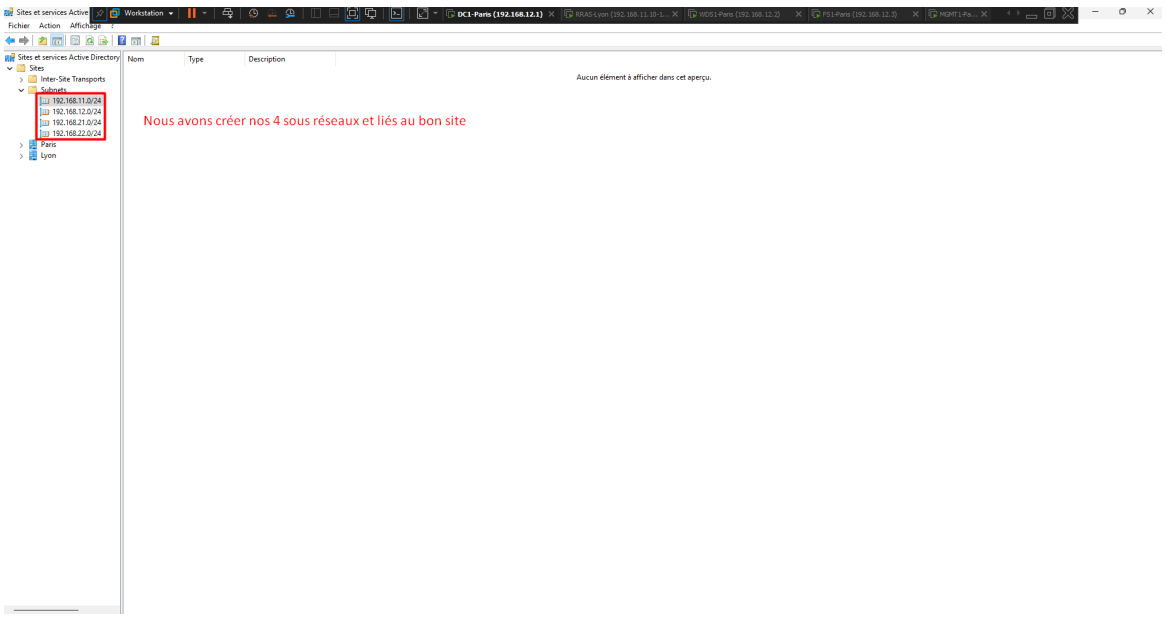

FIGURE 33 – Vue globale des sous-réseaux associés à l'Active Directory

5 DÉPLOIEMENT DU CONTRÔLEUR DE DOMAINE DE LYON (DC2)

5.1 Configuration IP de DC2

Nous allons maintenant configurer DC2 (site de Lyon) pour qu'il puisse rejoindre le domaine `learn.local`. On commence par la configuration IP statique : Adresse IP (`192.168.22.1`), masque par défaut, et la passerelle du RRAS (`192.168.22.10`). En serveur DNS, nous devons mettre DC1 (`192.168.12.1`) en principal et l'adresse de boucle locale en secondaire.

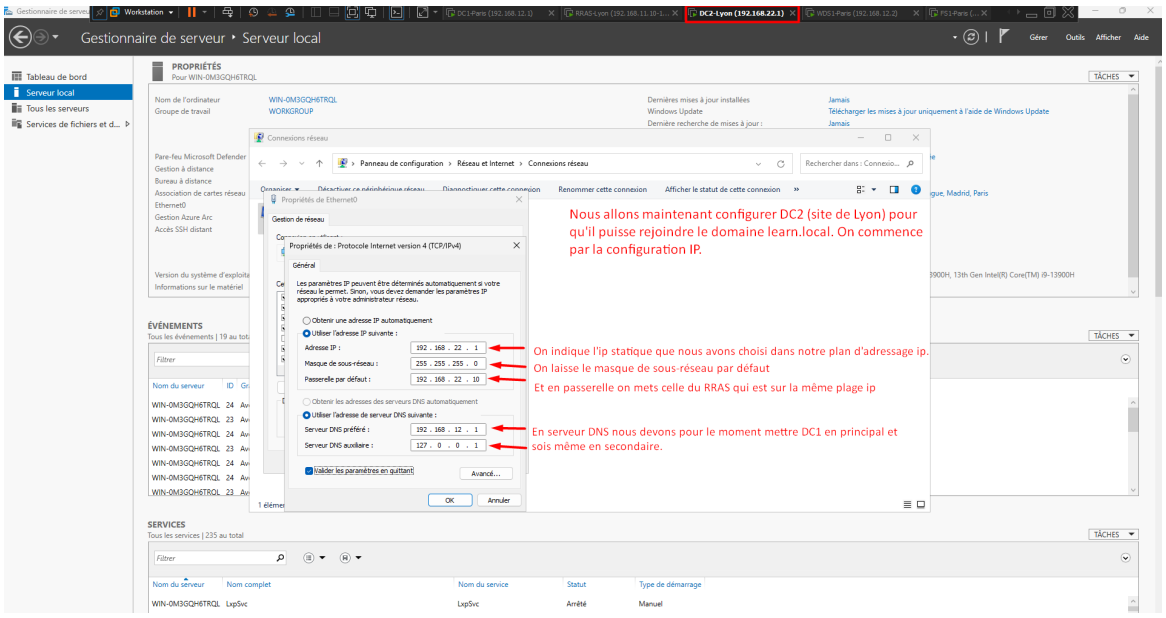

FIGURE 34 – Configuration IPv4 du serveur DC2 avec DC1 en DNS primaire

5.2 Promotion de DC2

Sur DC2, après avoir également installé le rôle AD, nous lançons l'assistant de configuration. Nous sélectionnons "Ajouter un contrôleur de domaine à un domaine existant" et spécifions le domaine `learn.local`.

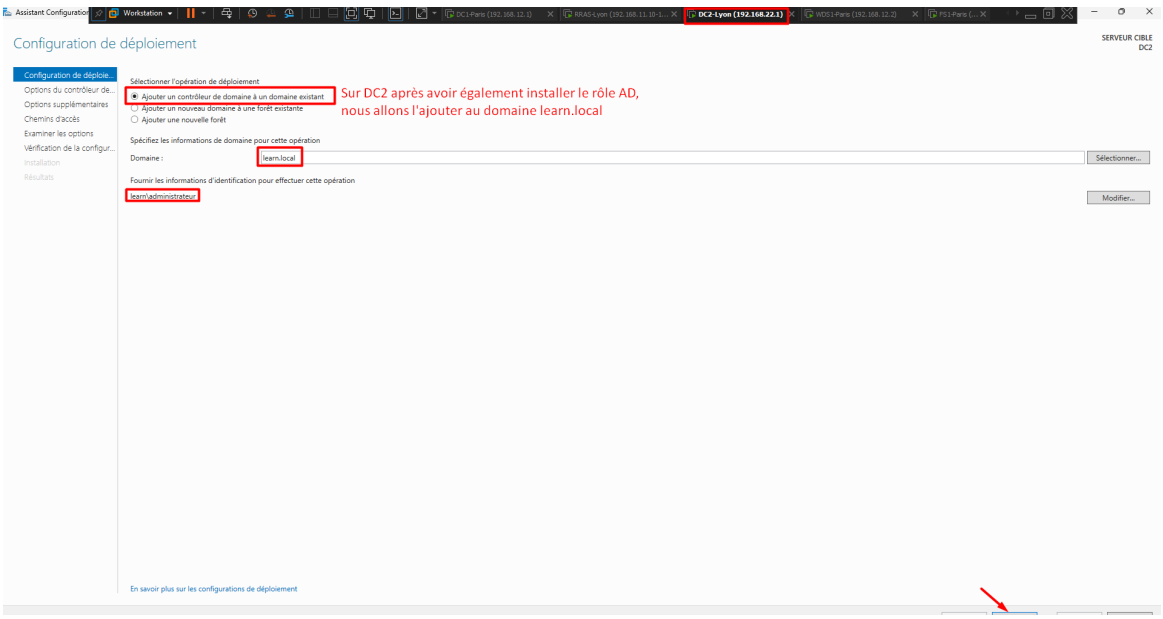

FIGURE 35 – Sélection de l'ajout d'un DC à un domaine existant

5.3 Sélection automatique du site

L'assistant détecte l'emplacement et doit automatiquement mettre le bon site (Lyon) à partir de notre IP, grâce aux sites que nous avons configurés juste avant. Nous choisissons également un mot de passe robuste pour la restauration (DSRM).

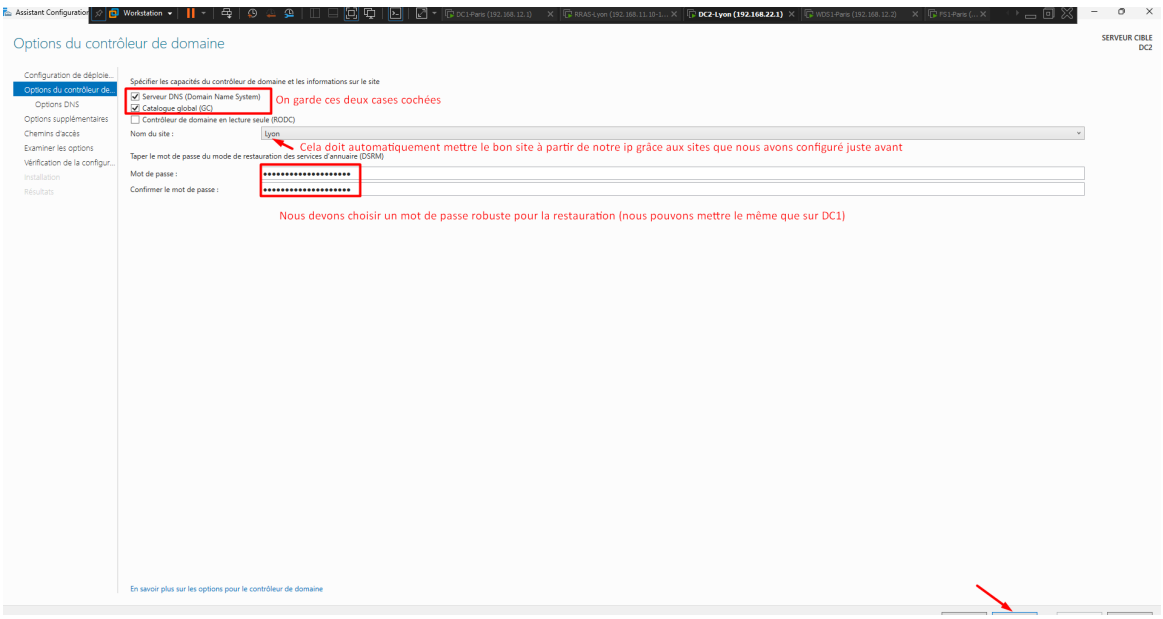

FIGURE 36 – Options du contrôleur de domaine avec le site Lyon pré-sélectionné

5.4 Options de réplication

Dans les options supplémentaires, nous définissons que les données de l'annuaire se répliqueront depuis `DC1.learn.local`.

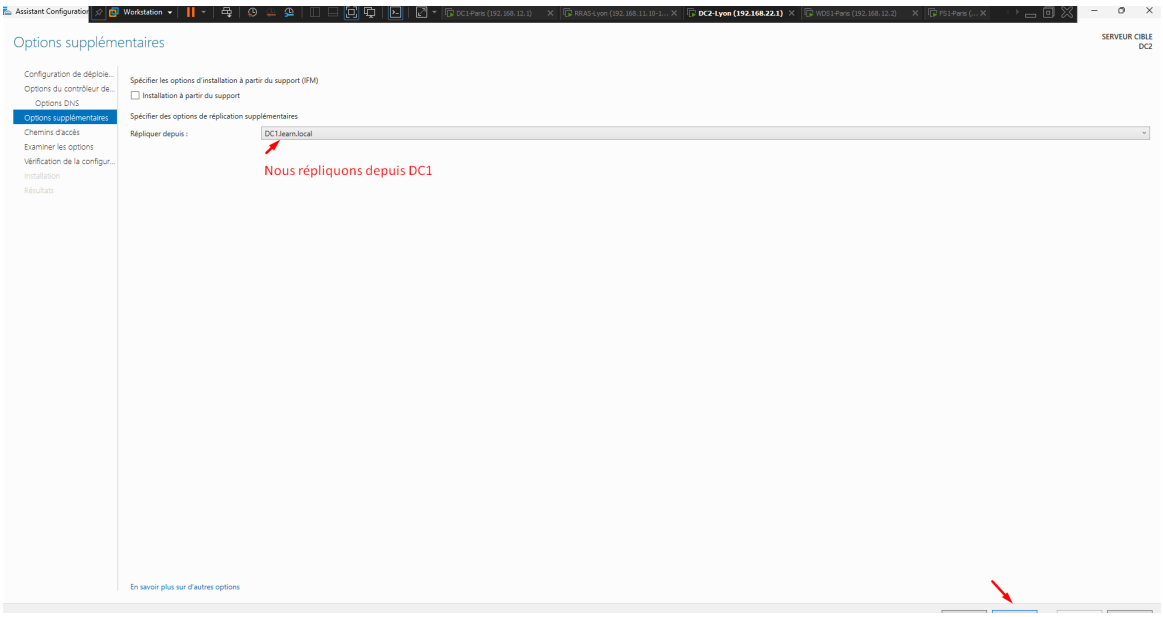

FIGURE 37 – Spécification du serveur partenaire de réplication

5.5 Lancement de l'installation

Toutes les vérifications de la configuration requise ont donné satisfaction. Tout le reste de l'assistant est identique à l'installation faite sur DC1. On clique sur Installer.

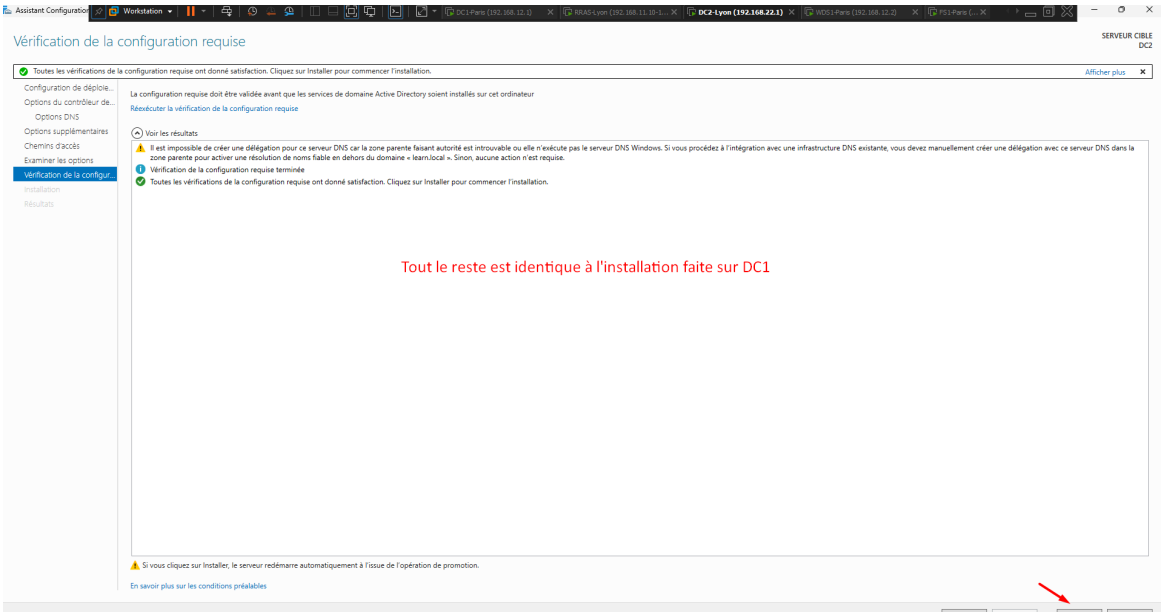

FIGURE 38 – Validation des prérequis et lancement de la promotion de DC2

6 CONFIGURATION DU SERVICE DHCP

6.1 Installation du rôle Serveur DHCP

Nous allons maintenant installer à l'identique le rôle "Serveur DHCP" sur DC1 et DC2 via l'assistant d'ajout de rôles et de fonctionnalités.

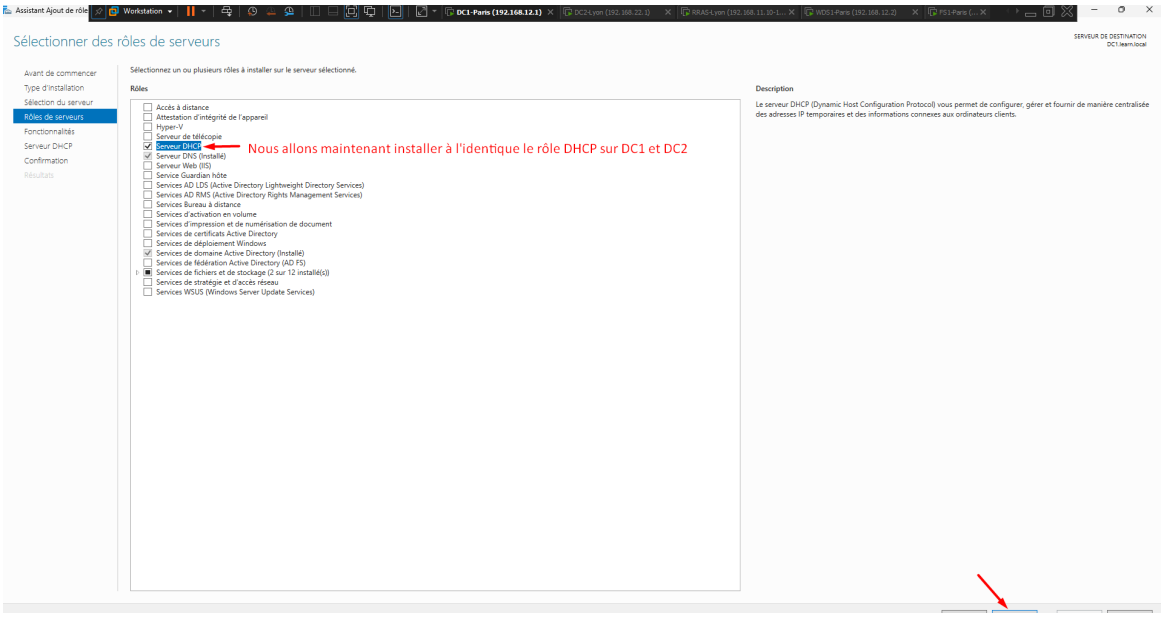

FIGURE 39 – Sélection du rôle Serveur DHCP sur DC1

6.2 Post-déploiement DHCP

Une fois les binaires du rôle installés sur DC1, une notification apparaît dans le tableau de bord du Gestionnaire de serveur. Nous cliquons sur "Terminer la configuration DHCP".

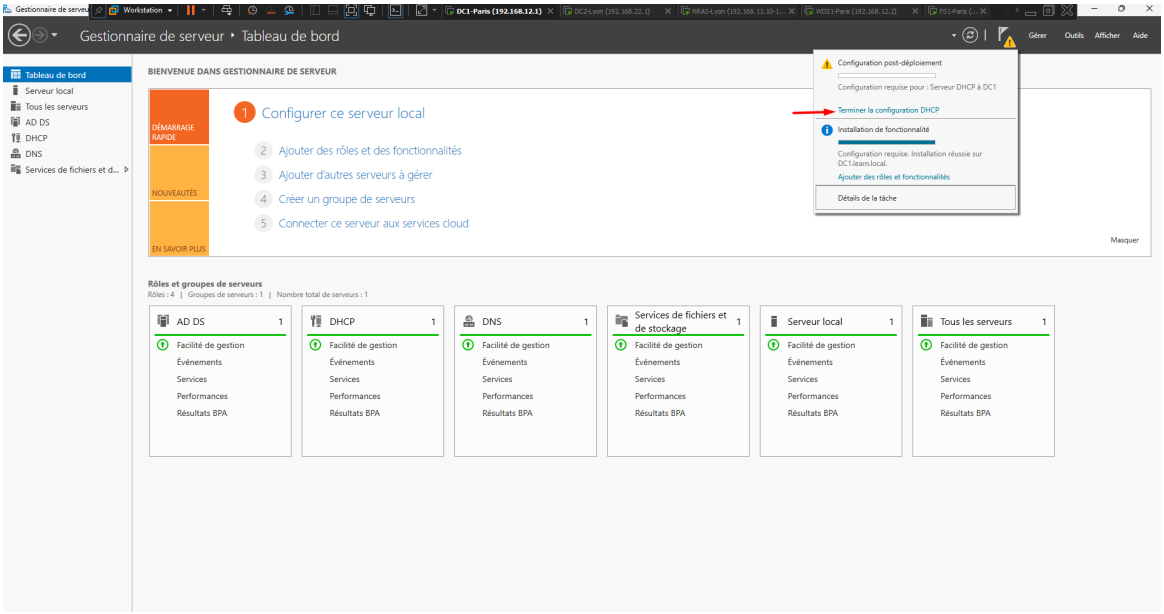

FIGURE 40 – Notification pour terminer la configuration du serveur DHCP

6.3 Autorisation du serveur DHCP dans l'AD

Pour que le serveur DHCP soit autorisé à distribuer des adresses IP dans notre domaine Active Directory, nous validons l'étape d'autorisation en utilisant les informations d'identification `LEARN\Administrateur`.

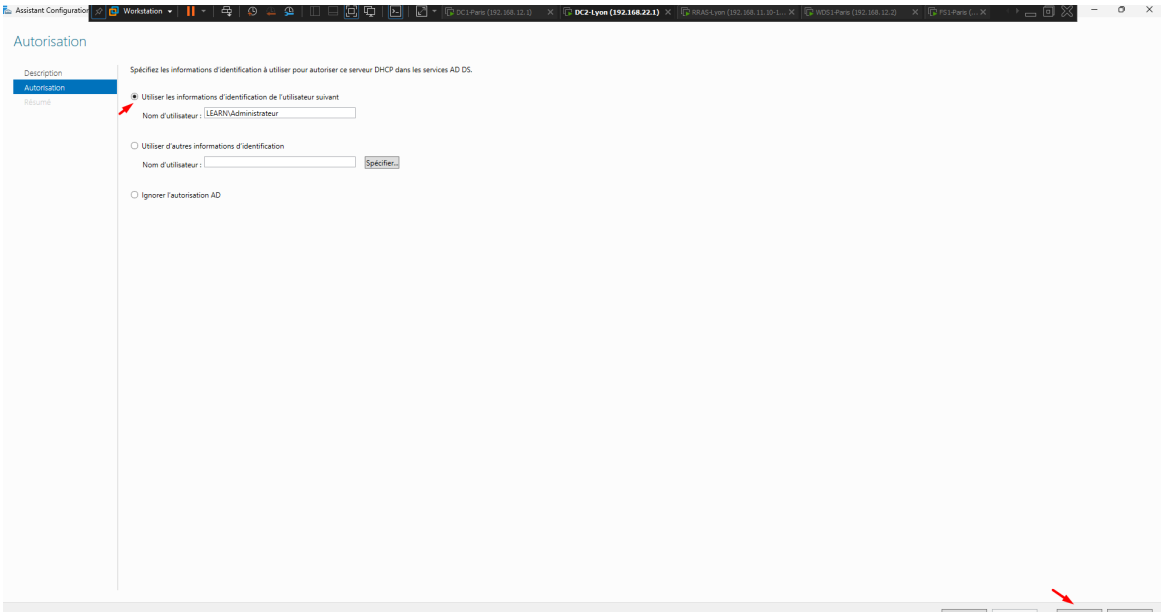

FIGURE 41 – Autorisation du DHCP dans les services AD DS

6.4 Création d'une nouvelle étendue

Nous ouvrons la console DHCP. Un clic-droit sur le nœud "IPv4" nous permet de sélectionner "Nouvelle étendue..." pour configurer notre première plage d'adresses.

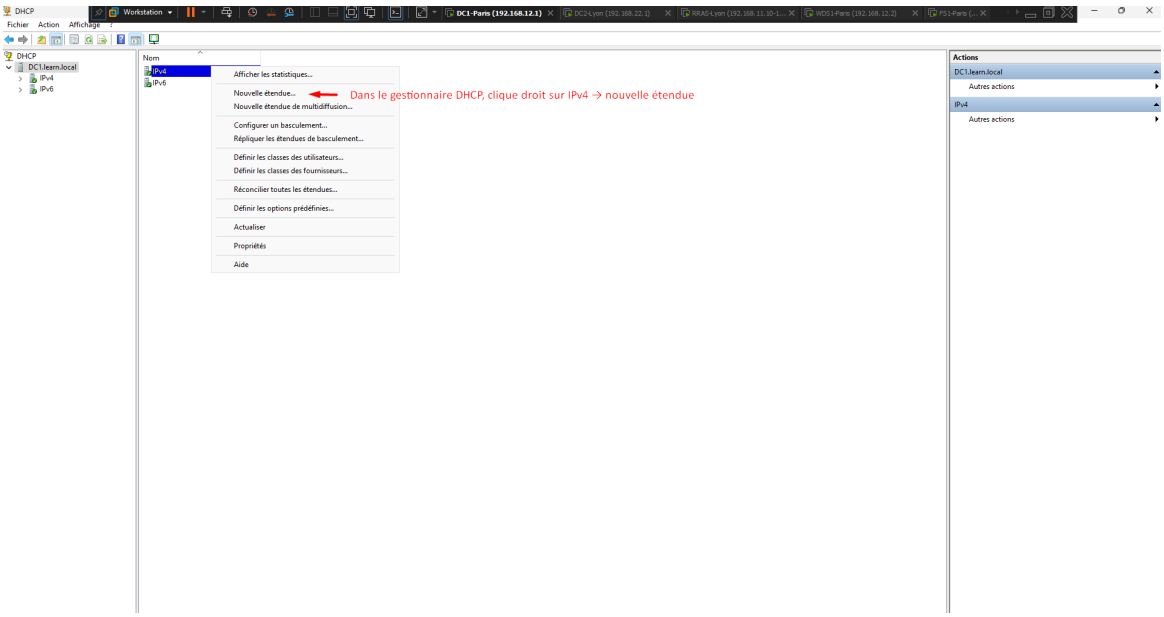

FIGURE 42 – Création d'une nouvelle étendue IPv4 dans la console DHCP

6.5 Définition de la plage d'adresses IP

Nous définissons la plage de l'étendue de Paris-prod : de `192.168.11.21` à `192.168.11.250` avec un masque `/24`. Nous choisissons volontairement d'exclure les 20 premières adresses IP pour pouvoir les attribuer de manière statique plus tard si nécessaire.

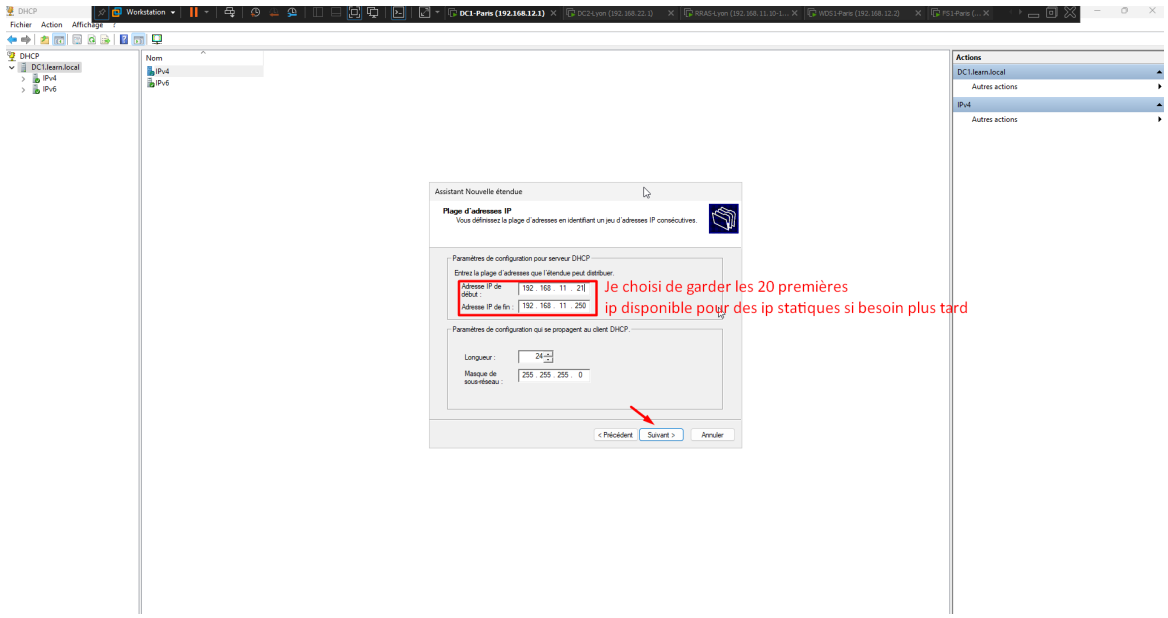

FIGURE 43 – Configuration de la plage d'adresses de l'étendue

6.6 Passerelle par défaut (Routeur)

Dans les options de l'étendue, nous spécifions l'adresse IP du routeur (passerelle par défaut) qui sera distribuée aux clients. Nous ajoutons l'adresse du serveur RRAS côté Paris-prod : `192.168.11.10`.

FIGURE 44 – Ajout de l'adresse du RRAS en tant que passerelle

6.7 Serveurs DNS

Nous définissons le domaine parent (`learn.local`) et ajoutons les adresses de nos deux contrôleurs de domaine, DC1 (`192.168.12.1`) et DC2 (`192.168.22.1`), comme serveurs DNS pour les clients.

FIGURE 45 – Ajout des serveurs DNS DC1 et DC2 dans les options DHCP

6.8 Configuration du basculement (Failover)

Pour assurer la haute disponibilité de notre service DHCP (tolérance de panne), nous faisons un clic-droit sur le nœud IPv4 et sélectionnons "Configurer un basculement...".

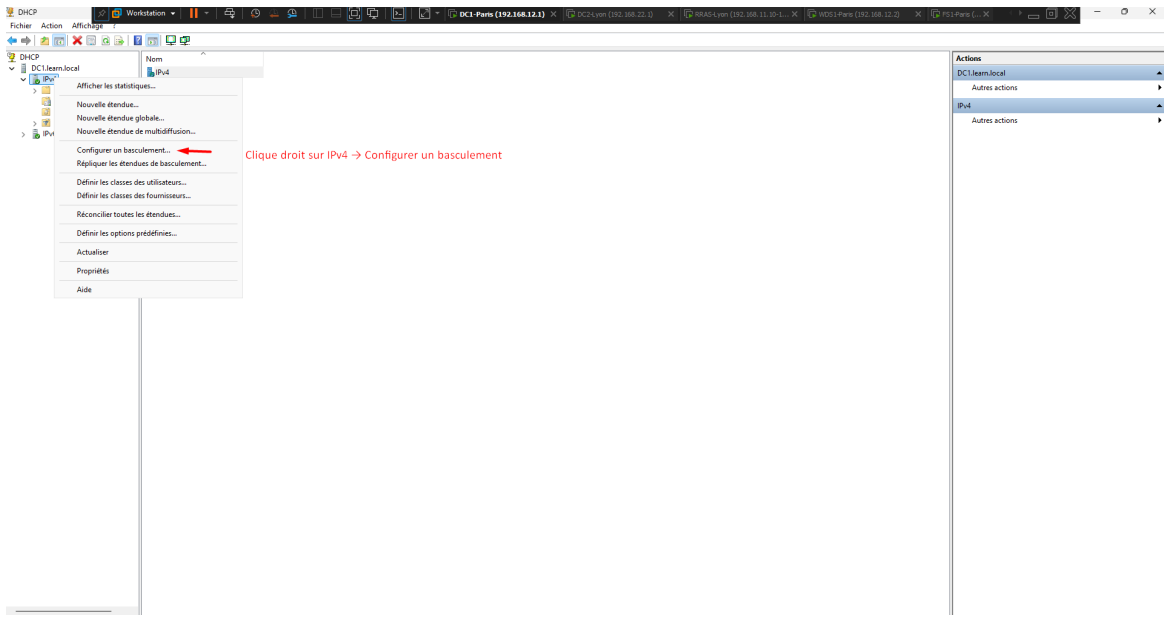

FIGURE 46 – Lancement de la configuration du basculement DHCP

6.9 Sélection de l'étendue pour le basculement

L'assistant nous demande de sélectionner l'étendue concernée. Nous cochons notre étendue `192.168.11.0` qui vient d'être créée.

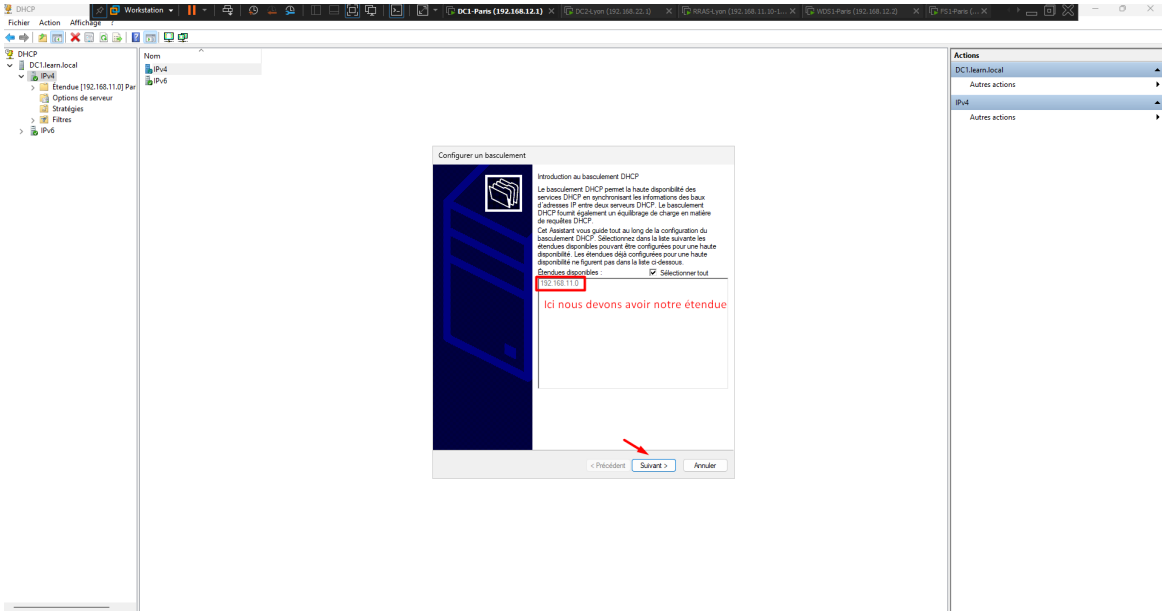

FIGURE 47 – Sélection de l'étendue à hautement rentabiliser

6.10 Spécification du serveur partenaire

Il faut maintenant indiquer le serveur DHCP partenaire avec lequel notre DC1 va se synchroniser.

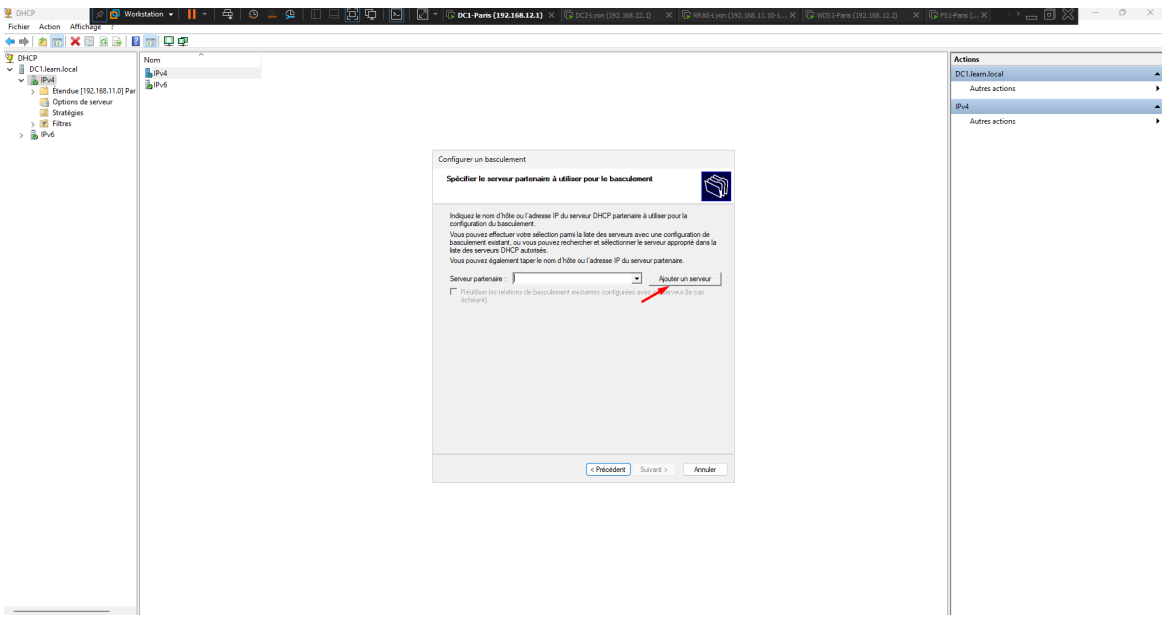

FIGURE 48 – Écran de sélection du serveur partenaire pour le basculement

6.11 Ajout du partenaire DC2

Nous sélectionnons le serveur autorisé `DC2.learn.local` (`192.168.22.1`) dans la liste pour établir la relation.

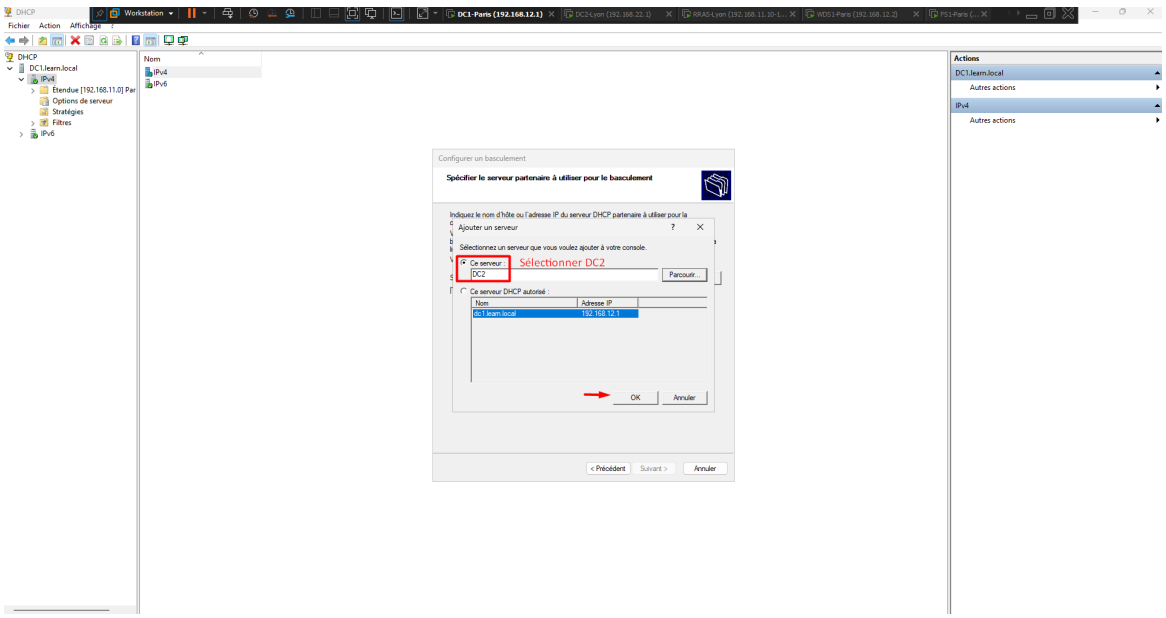

FIGURE 49 – Sélection de DC2 comme serveur de basculement

6.12 Création de la relation (Serveur de secours)

Nous nommons la relation "Paris-vers-Lyon". Comme nos serveurs sont sur deux sites distants, nous choisissons le mode "Serveur de secours" (Hot Standby) avec le rôle "Veille" pour le partenaire. Nous définissons également un mot de passe (secret partagé).

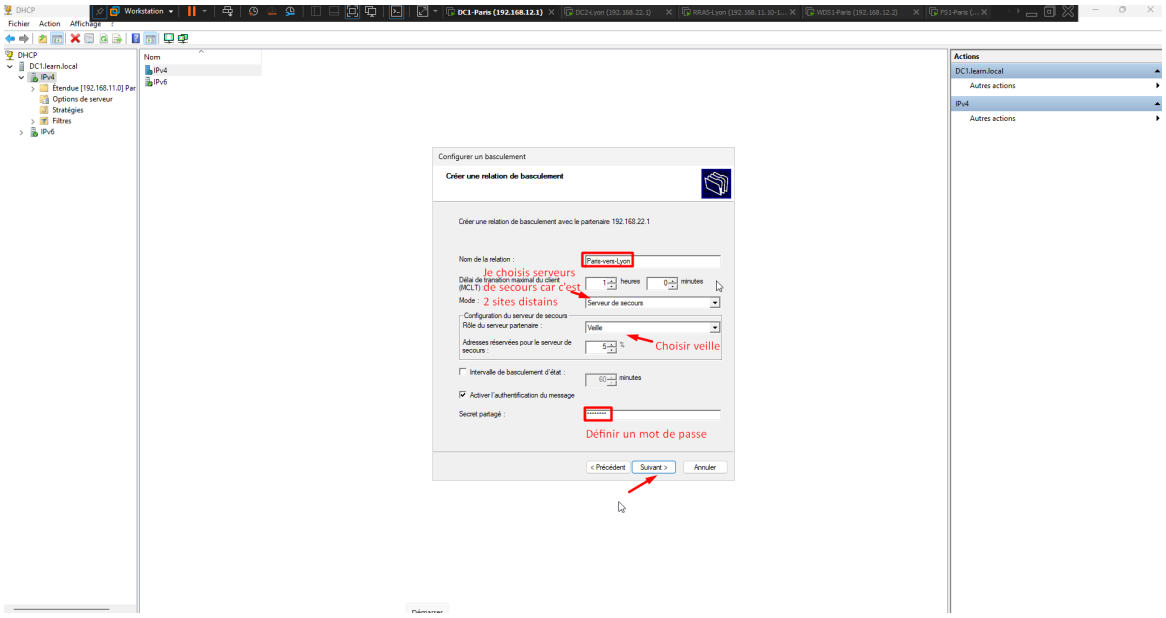

FIGURE 50 – Paramètres de la relation de basculement DHCP

6.13 Ajout de l'Agent de relais DHCP (RRAS)

Les clients (sur les réseaux de production) et les serveurs DHCP (sur les réseaux d'administration) étant sur des sous-réseaux différents pour des raisons de sécurité, les requêtes DHCP seront bloquées. Nous devons ajouter un agent de relais sur le routeur RRAS pour contourner ce problème.

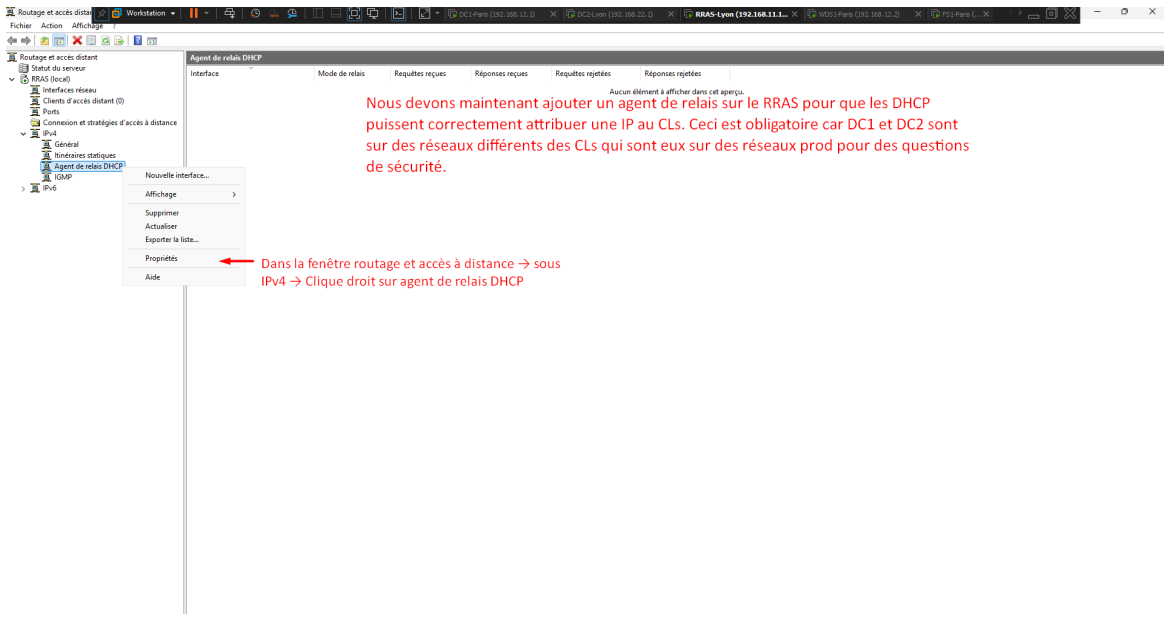

FIGURE 51 – Accès à la rubrique Agent de relais DHCP dans la console RRAS

6.14 Définition des serveurs cibles pour le relais

Dans les propriétés de l'Agent de relais DHCP, nous ajoutons les adresses IP de nos deux serveurs DHCP (`192.168.12.1` et `192.168.22.1`) à qui les demandes des clients doivent être transmises.

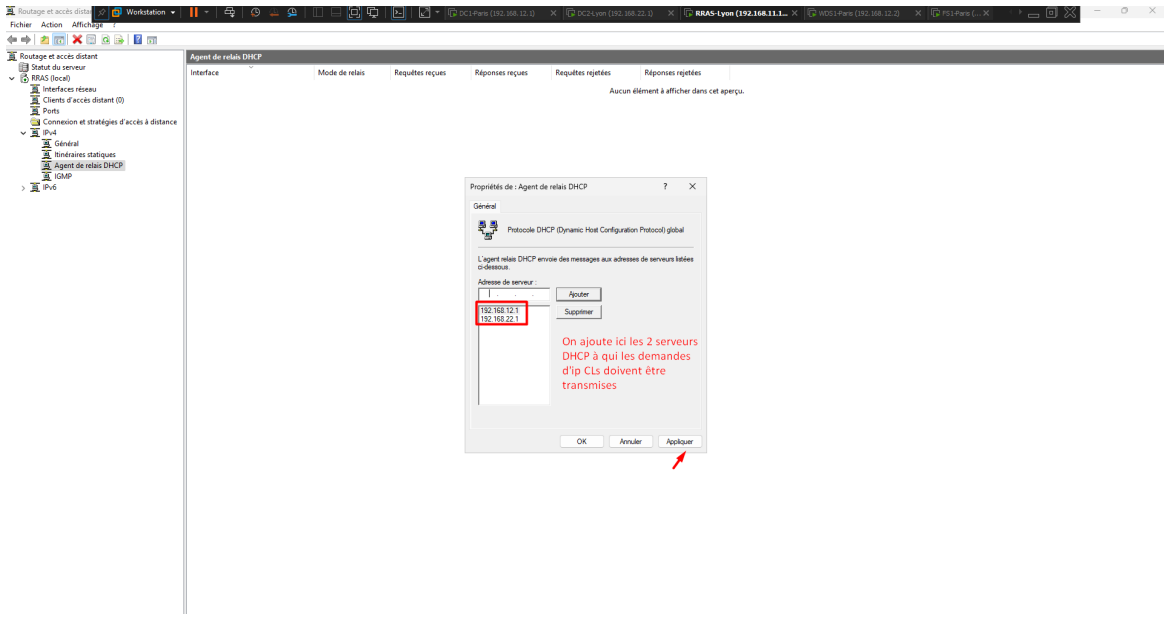

FIGURE 52 – Ajout des serveurs DHCP dans la configuration du relais

6.15 Déclaration des interfaces d'écoute

Il faut indiquer au relais sur quelles cartes réseau il doit écouter. On effectue un clic-droit sur l'Agent de relais DHCP et on choisit "Nouvelle interface...". Nous y ajouterons les réseaux de production.

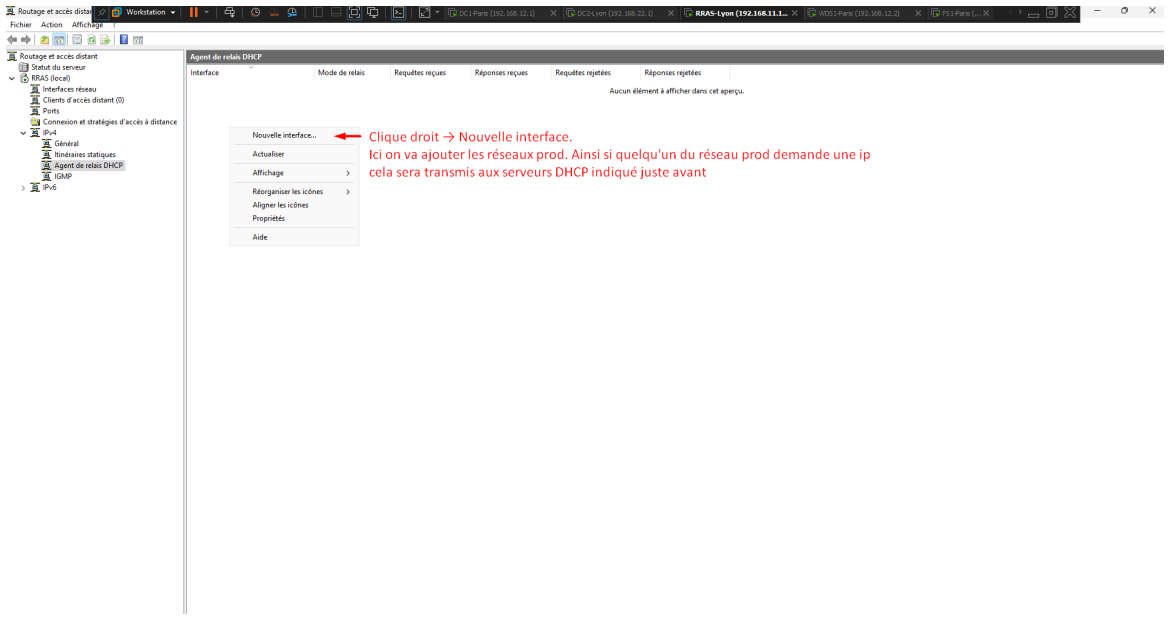

FIGURE 53 – Ajout d'une nouvelle interface au relais DHCP

6.16 Validation des interfaces de relais

Les interfaces "Lyon-prod" et "Paris-prod" sont désormais ajoutées avec le mode de relais "Activé". Le RRAS va maintenant transférer les requêtes.

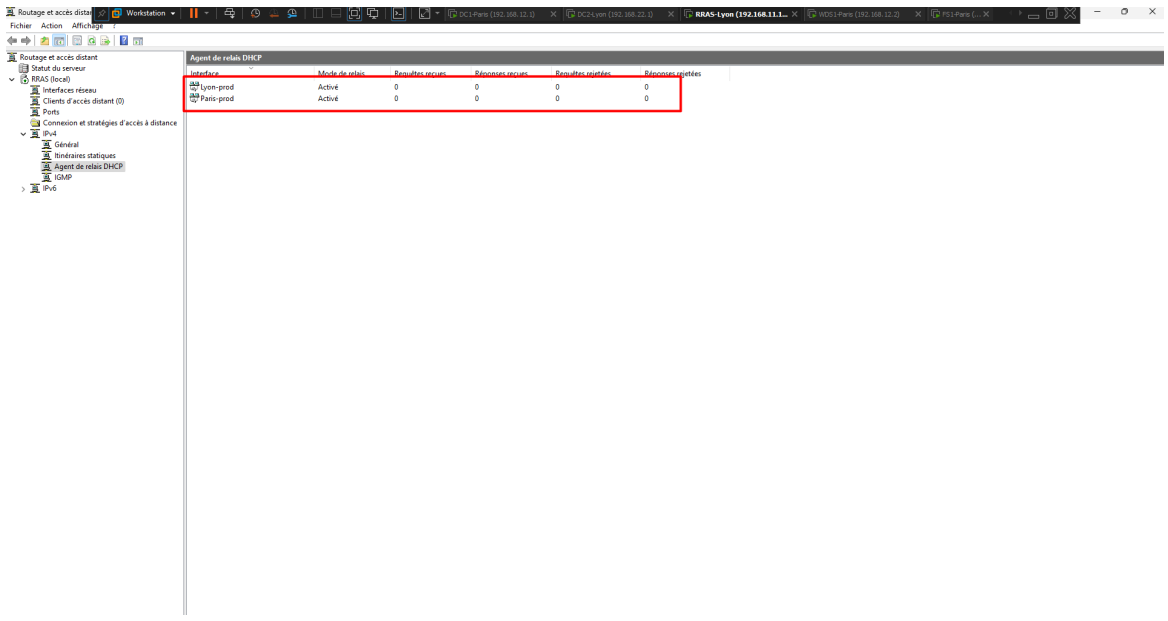

FIGURE 54 – Les interfaces réseau sont actives pour le relais DHCP

6.17 Test d'attribution DHCP sur le client

Depuis la machine virtuelle cliente `CL1-Paris`, nous utilisons la commande `ipconfig /all`. Le test est un succès : le poste a reçu l'adresse IP `192.168.11.21` attribuée par `192.168.12.1` (DC1). Le RRAS est bien la passerelle, et les deux serveurs DNS sont renseignés. Le poste est prêt à joindre le domaine.

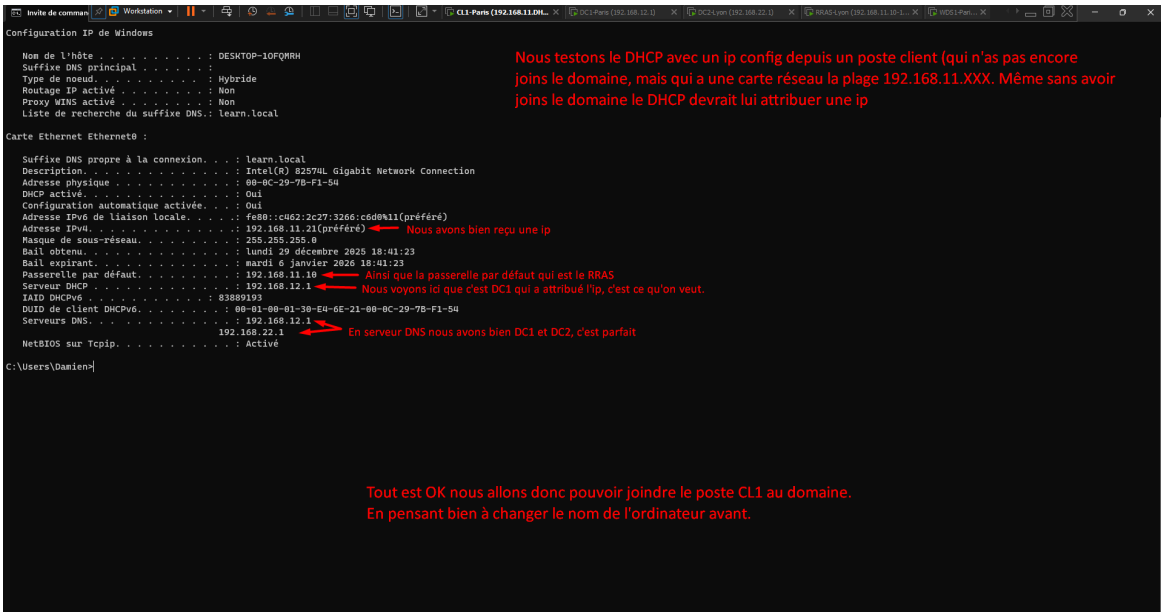

FIGURE 55 – Vérification de la configuration IP sur le poste CL1

7 ORGANISATION ACTIVE DIRECTORY

7.1 Création des Unités d'Organisation (OU)

L'infrastructure de base (DNS, DHCP, Routage) étant fonctionnelle, nous organisons notre annuaire. Nous créons une OU racine "LEARN", contenant deux sous-OU "Paris" et "Lyon". Chacune d'elles contient des OU dédiées : Utilisateurs, Ordinateurs, Serveurs et Groupes.

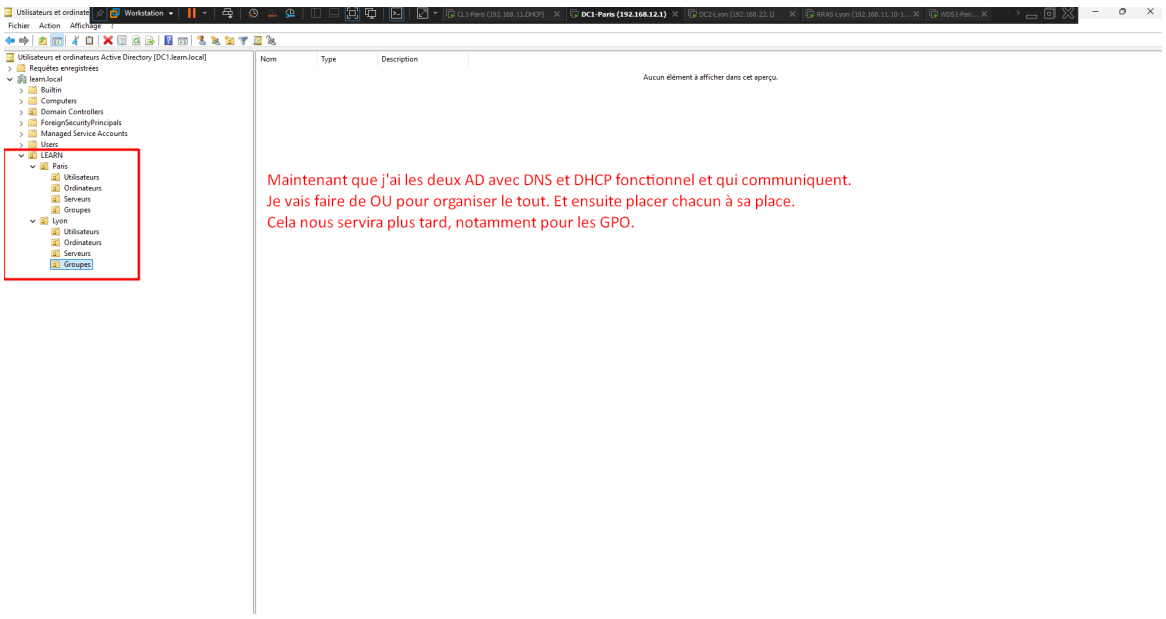

FIGURE 56 – Arborescence des Unités d'Organisation dans l'AD

8 PRÉPARATION DU SERVEUR DE DÉPLOIEMENT (WDS)

8.1 Configuration initiale du serveur WDS1

Nous passons à la configuration du serveur qui permettra d'installer Windows 11 sur les postes clients automatiquement. La machine est renommée `WDS1` et l'adresse IP statique `192.168.12.2` lui est attribuée.

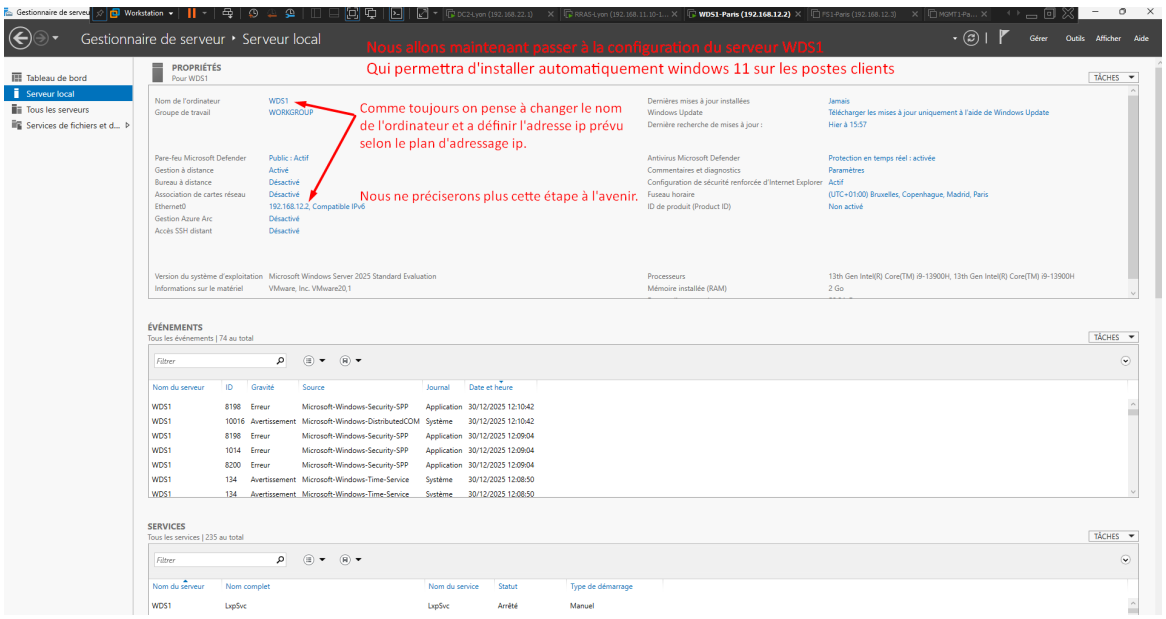

FIGURE 57 – Propriétés du serveur WDS1 dans le Gestionnaire de serveur

8.2 Ajout du rôle WDS

Depuis l'assistant d'ajout de rôles, nous sélectionnons "Services de déploiement Windows" (WDS).

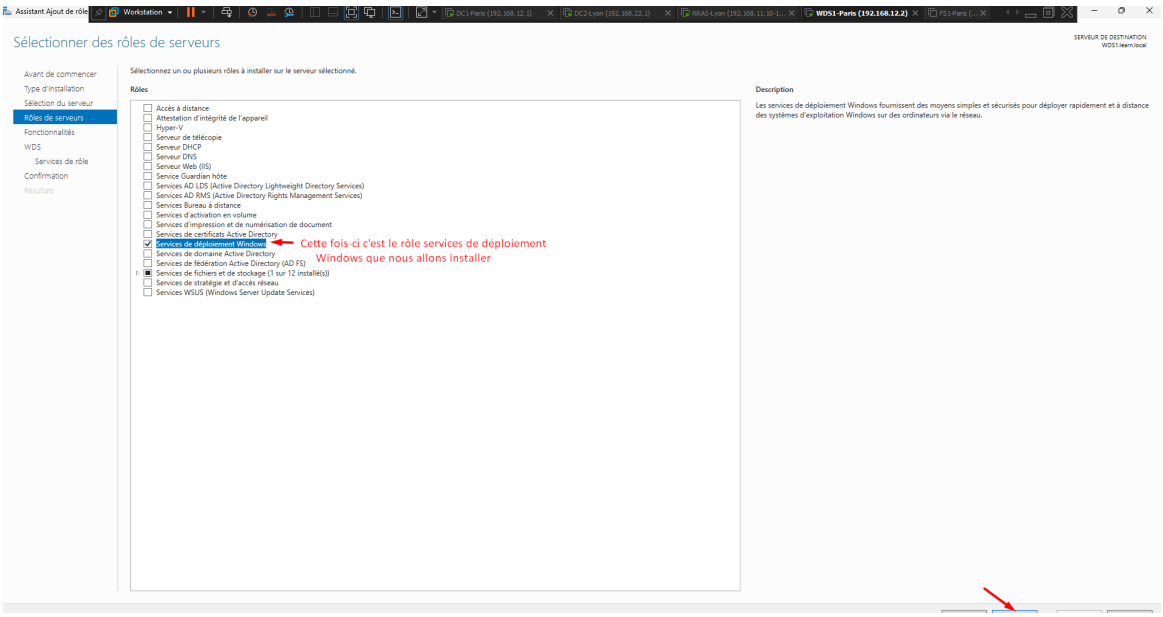

FIGURE 58 – Sélection du rôle Services de déploiement Windows

8.3 Outils de déploiement (ADK et WinPE)

Pour préparer nos images personnalisées, nous avons besoin de l'outil ADK et de son add-on WinPE. Ces exécutables (`adksetup` et `adkwinpesetup`) ont été téléchargés depuis le site de Microsoft. L'installation de l'ADK doit être effectuée en premier.

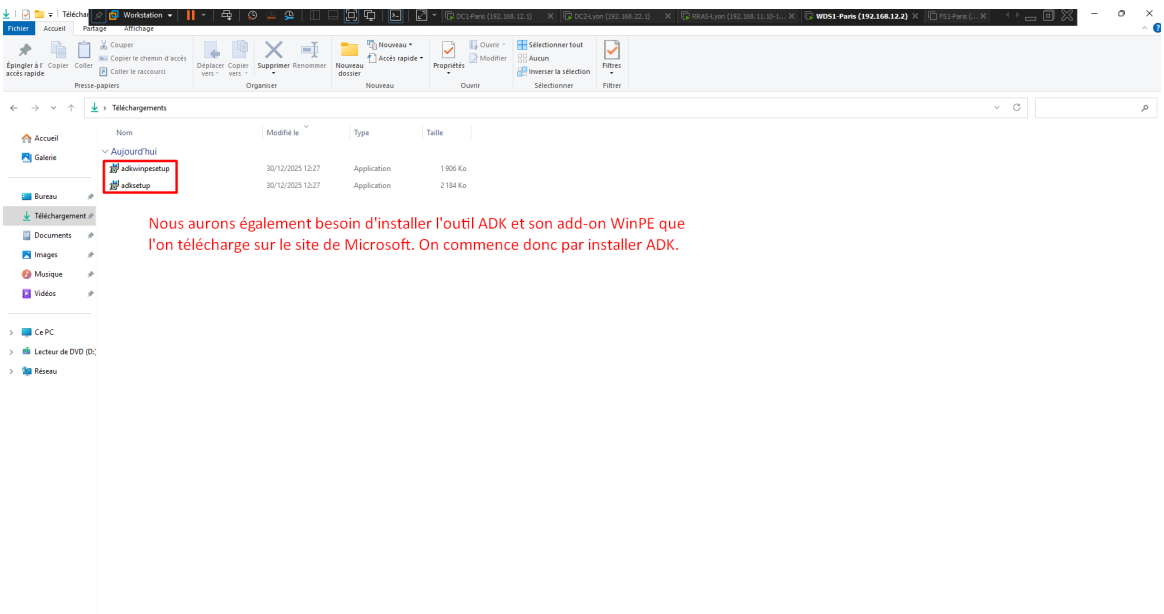

FIGURE 59 – Exécutables d'installation Windows ADK et WinPE

8.4 Lancement de l'installation de l'ADK

Sur le serveur WDS1, nous commençons par exécuter le fichier `adksetup.exe` pour installer le Kit de déploiement et d'évaluation Windows. Nous conservons le chemin d'installation par défaut.

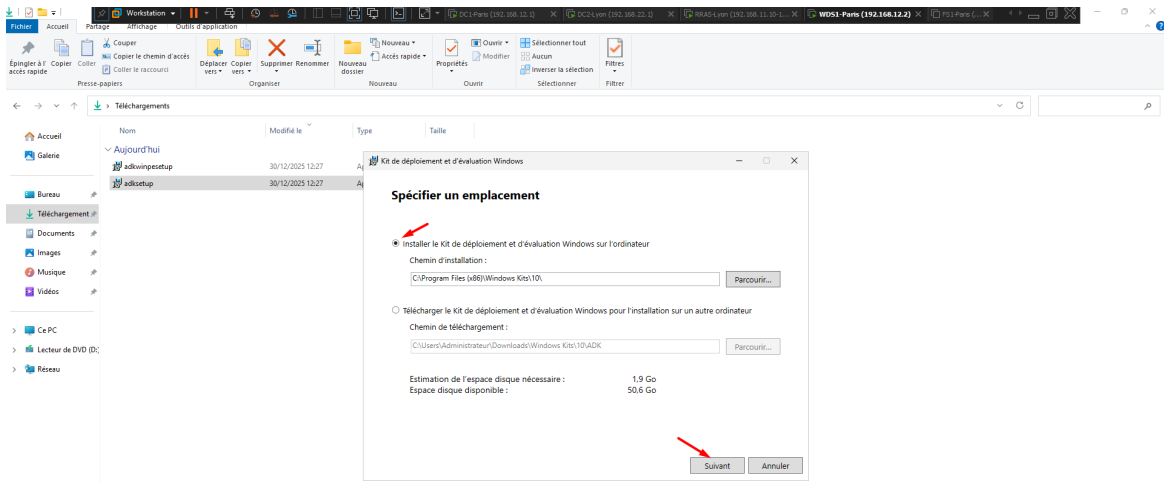

FIGURE 60 – Installation de Windows ADK sur le serveur de déploiement

8.5 Confidentialité des kits Windows

À l'étape concernant la collecte des données de diagnostic, nous choisissons "Non" pour ne pas envoyer d'informations d'utilisation à Microsoft.

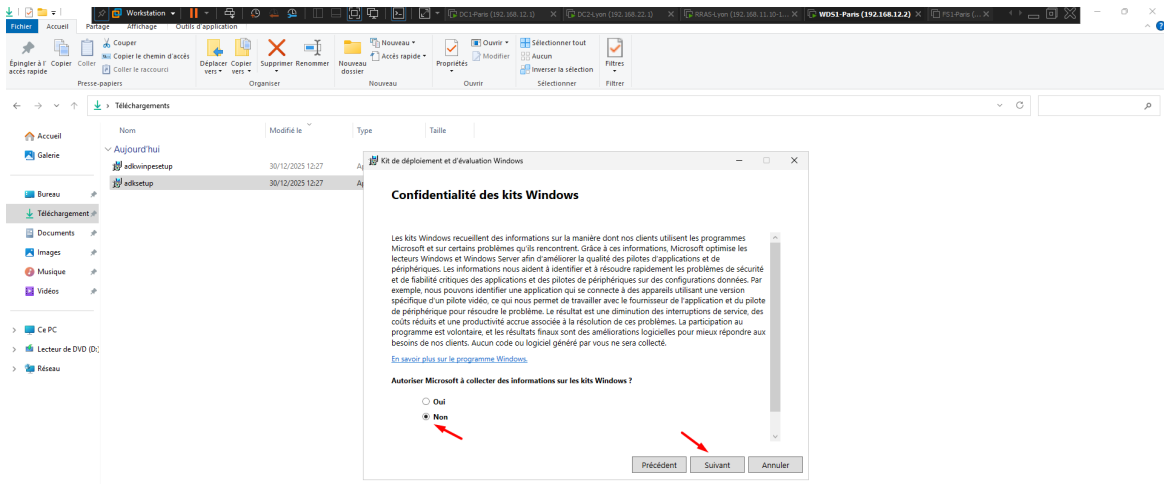

FIGURE 61 – Refus de la collecte de données par Microsoft

8.6 Sélection des fonctionnalités ADK

Dans notre cas, nous nous limitons au strict nécessaire. Nous cochons uniquement les "Outils de déploiement" (ainsi que l'environnement WinPE via son setup dédié) pour ne pas surcharger le serveur avec des outils inutiles.

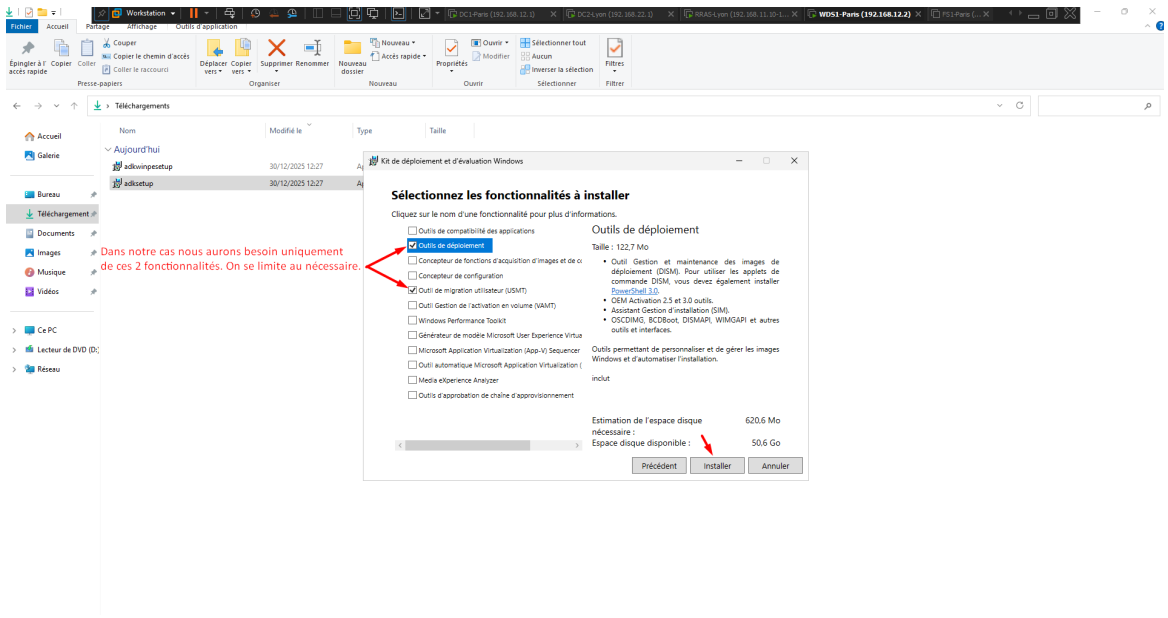

FIGURE 62 – Sélection restreinte des fonctionnalités à installer

8.7 Création du dossier de déploiement (MDT)

Une fois l'ADK et MDT installés, nous ouvrons la console "Deployment Workbench". Nous effectuons un clic-droit sur "Deployment Shares" puis nous sélectionnons "New Deployment Share".

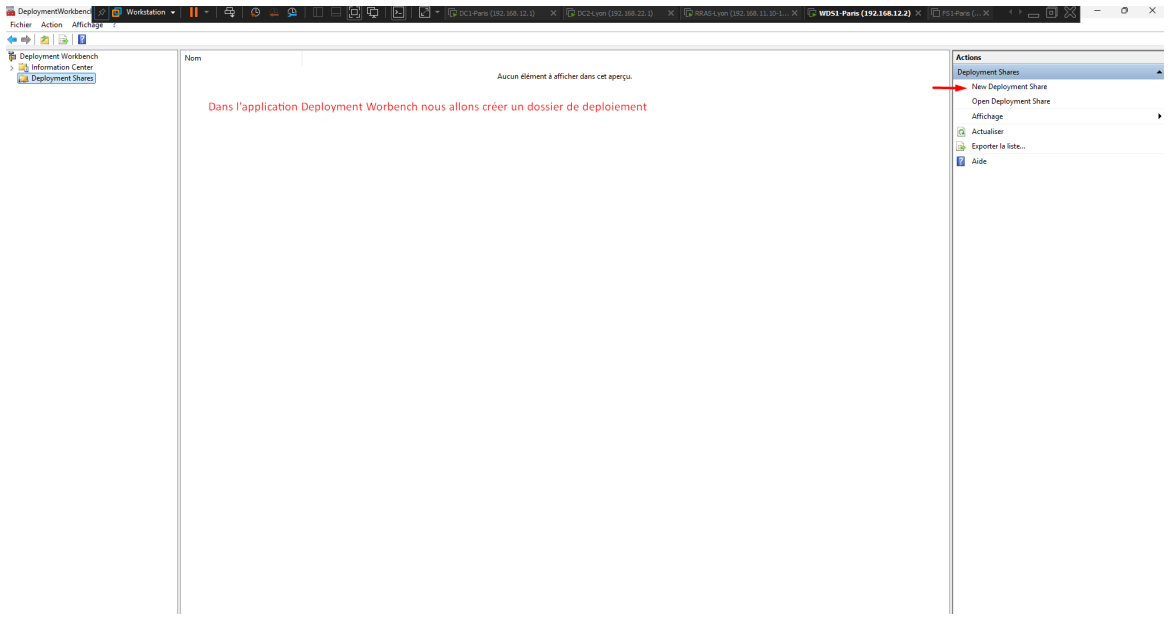

FIGURE 63 – Lancement de la création du Deployment Share dans MDT

8.8 Emplacement du Deployment Share

Nous indiquons l'emplacement où seront stockées les installations. Pour de meilleures performances et séparer les données du système, nous avons ajouté un second disque virtuel. Le chemin sera par exemple `E:\DeploymentShare`.

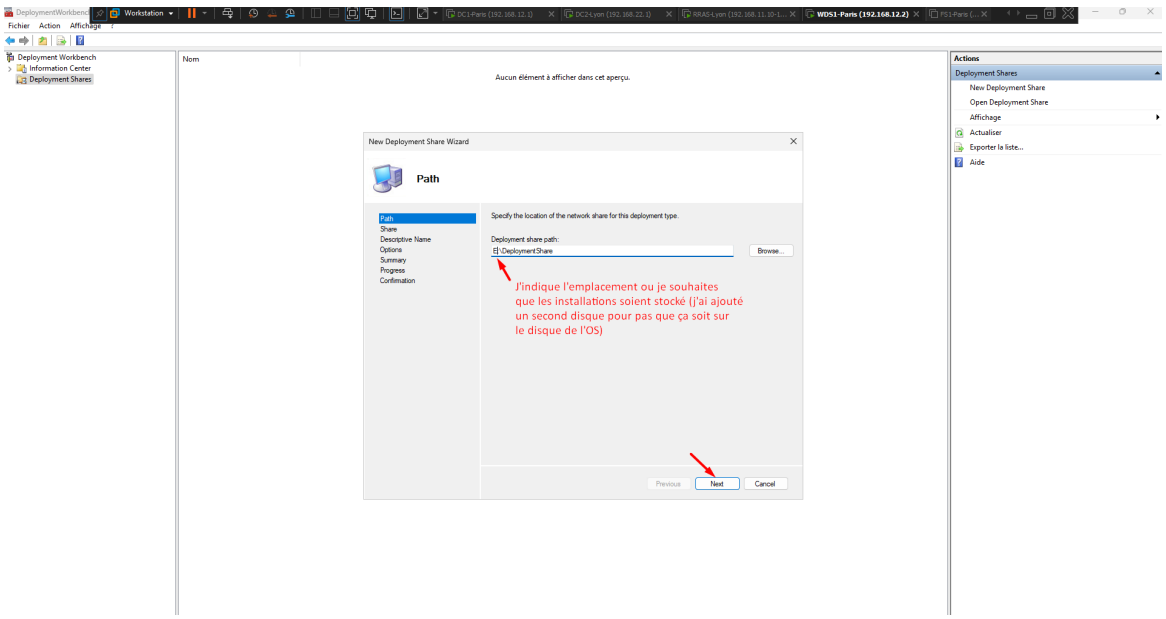

FIGURE 64 – Définition de l'emplacement du partage sur le disque E :

8.9 Options du Deployment Share

Dans les options de l'assistant, nous décochons toutes les cases (BitLocker, Admin password, Product key, etc.). L'objectif est de supprimer toutes les questions inutiles lors de l'installation du client (mode LiteTouch).

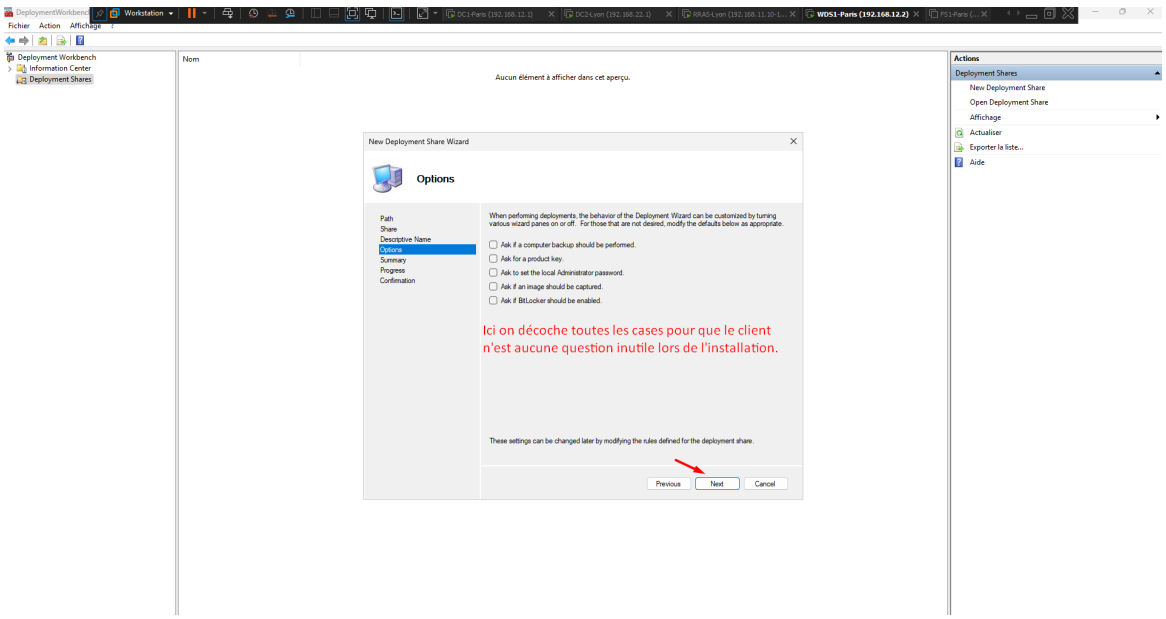

FIGURE 65 – Désactivation des invites utilisateur lors du déploiement

8.10 Importation du système d'exploitation

Toujours dans la console Deployment Workbench, on se rend dans le dossier "Operating Systems". On fait un clic-droit puis on sélectionne "Import Operating System".

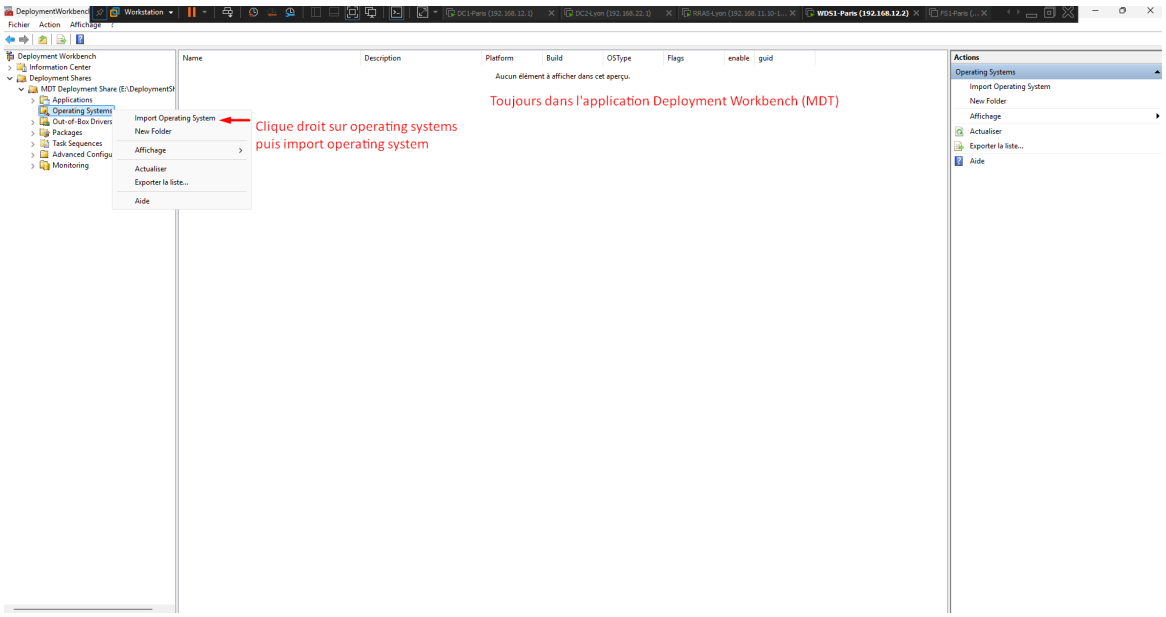

FIGURE 66 – Lancement de l'importation de l'image de l'OS

8.11 Type de système d'exploitation

L'assistant nous demande le type de source. Nous choisissons "Full set of source files" puisque nous allons importer le système complet depuis une image ISO montée.

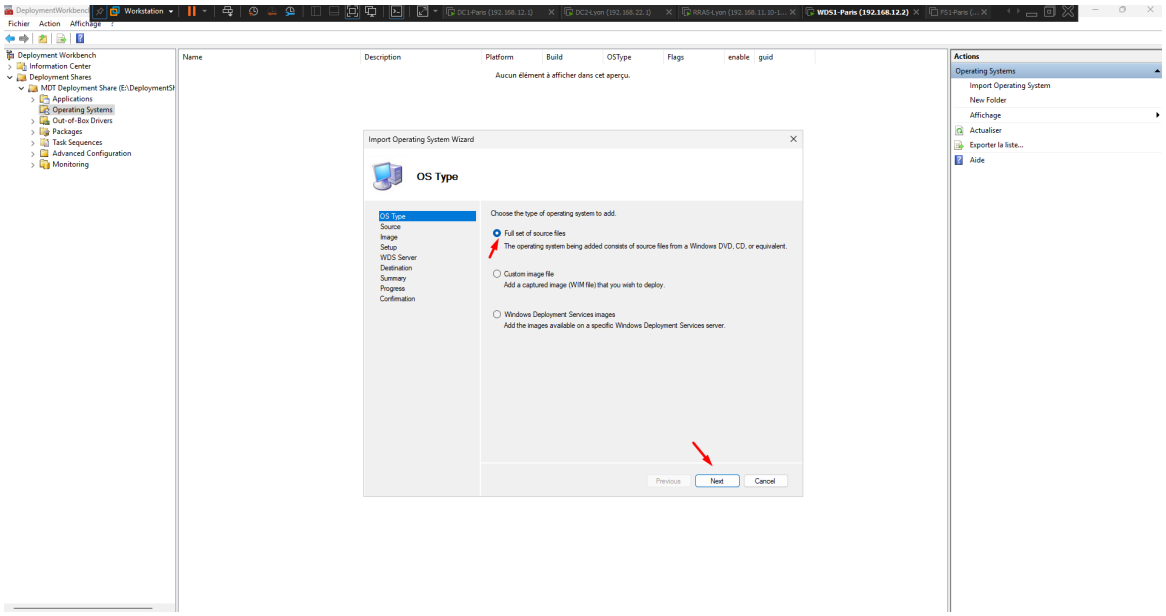

FIGURE 67 – Sélection d'un import à partir des fichiers sources complets

8.12 Sélection du lecteur source

Nous indiquons le lecteur (ici `D:\`) qui contient le DVD d'installation du système que l'on souhaite déployer sur les postes clients. Dans notre cas, il s'agit de Windows 11, dont l'ISO a été préalablement monté sur WDS1.

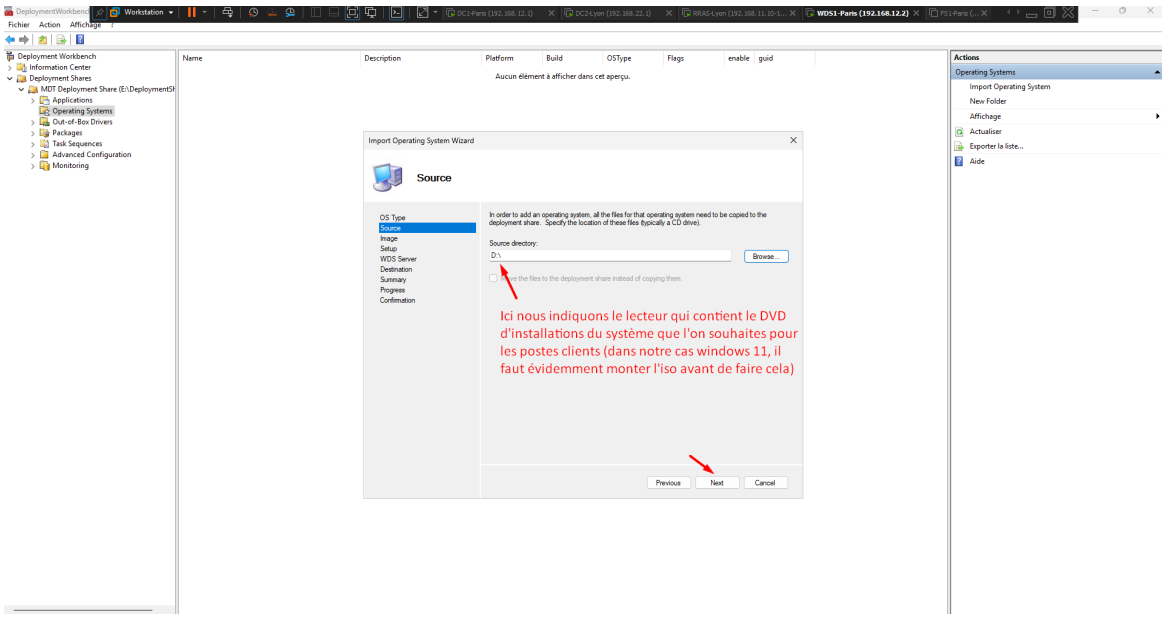

FIGURE 68 – Sélection du lecteur contenant les fichiers sources de Windows 11

8.13 Succès de l'importation

Le processus de copie s'exécute. À la fin, l'assistant affiche que l'opération s'est terminée avec succès et que les différentes éditions de l'image ont été extraites.

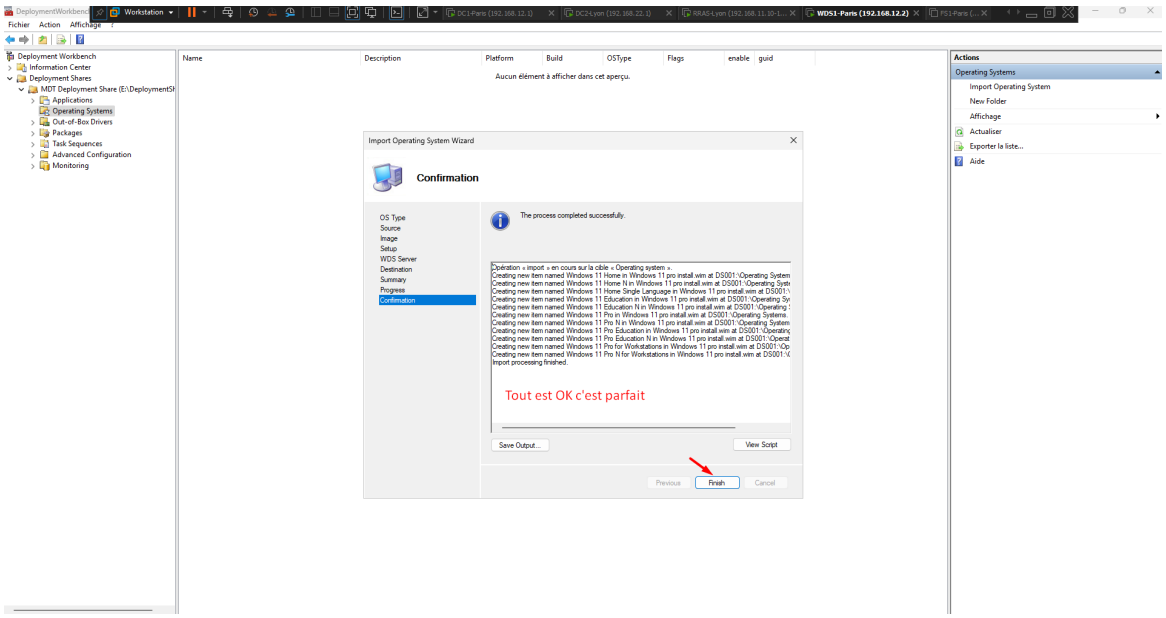

FIGURE 69 – Validation de l'importation réussie du système

8.14 Nettoyage des éditions inutiles

Le DVD de Windows 11 contient plusieurs éditions (Home, Education, etc.). Pour que notre console soit plus propre et éviter toute erreur, nous sélectionnons toutes les éditions inutiles et nous les supprimons. Nous ne conservons que "Windows 11 Pro".

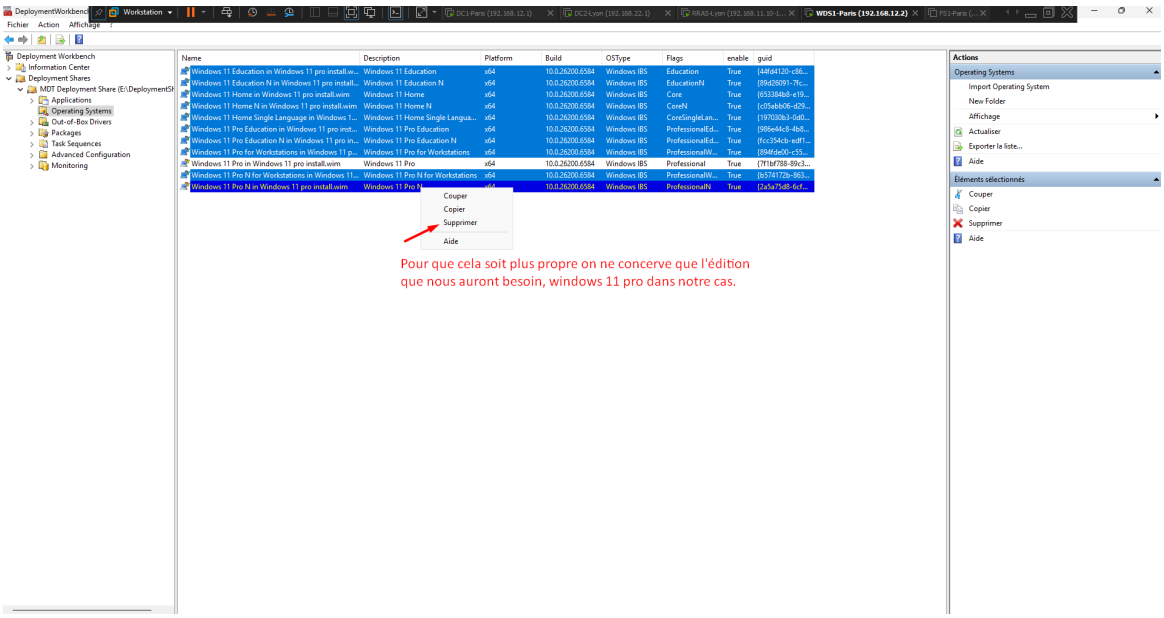

FIGURE 70 – Suppression des versions de Windows 11 non requises

8.15 Création d'une séquence de tâches

Il faut maintenant créer le scénario d'installation. Dans le Deployment Workbench, on fait un clic-droit sur le nœud "Task Sequences" et on sélectionne "New Task Sequence".

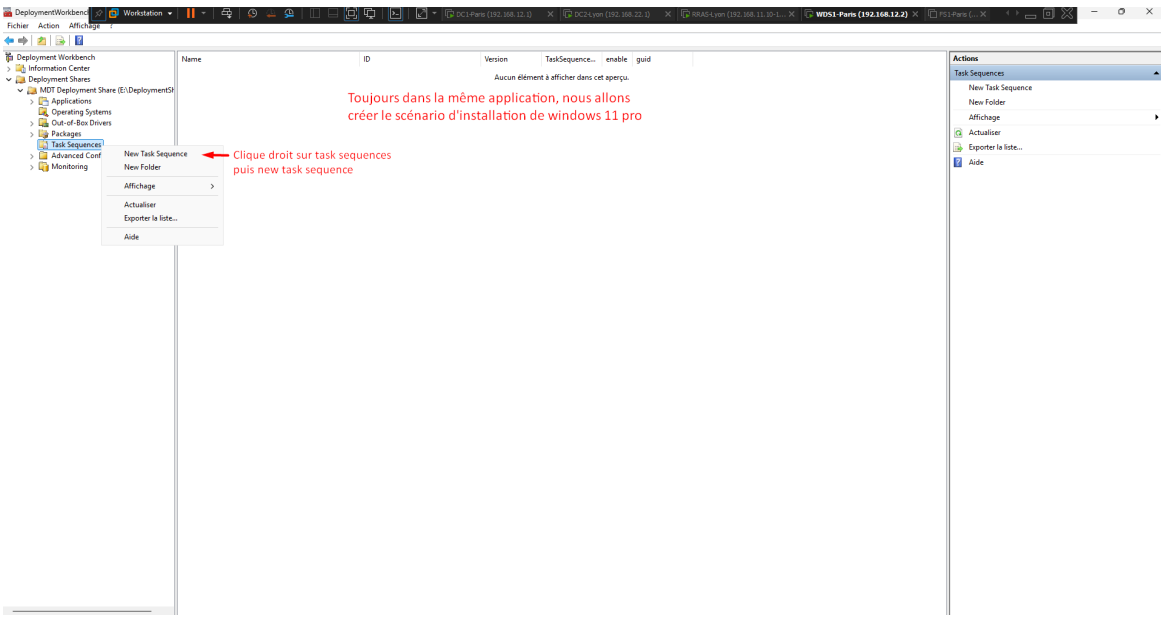

FIGURE 71 – Lancement de l'assistant de nouvelle séquence de tâches

8.16 Identification de la séquence

Nous définissons un identifiant (ID) pour la séquence, par exemple `W11-PRO-01`, ainsi qu'un nom explicite comme "Déploiement Windows 11 Pro". On peut également y ajouter des commentaires si nécessaire.

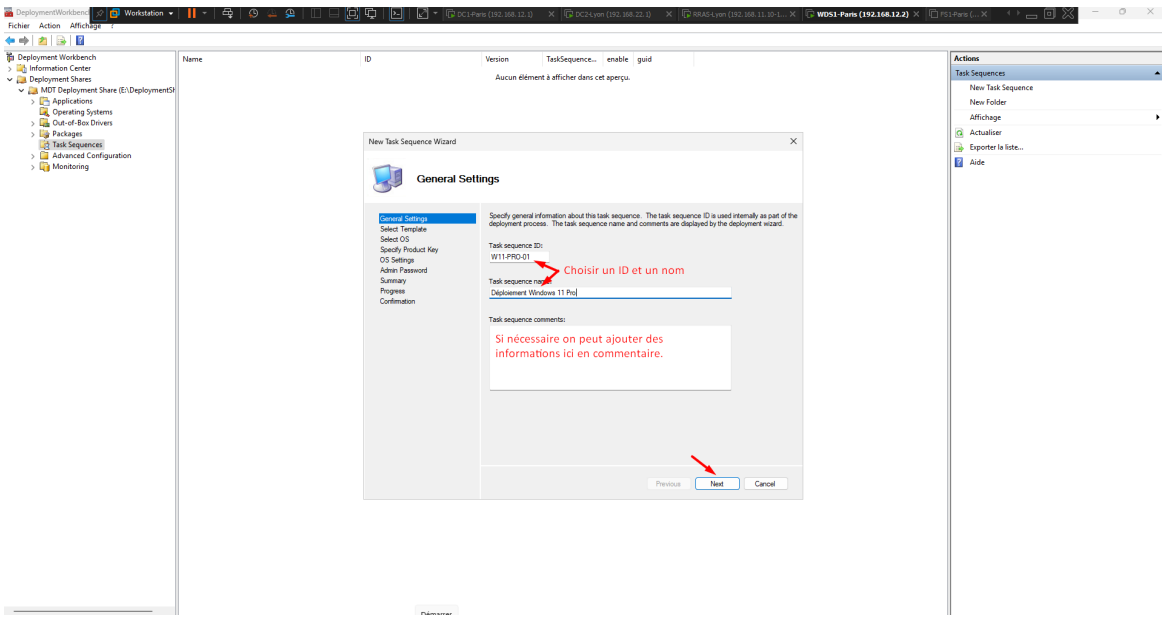

FIGURE 72 – Attribution de l'ID et du nom de la Task Sequence

8.17 Choix du modèle de séquence

Nous sélectionnons le modèle "Standard Client Task Sequence". Ce modèle pré-configuré gérera automatiquement le formatage du disque, l'installation de l'OS et l'injection des drivers.

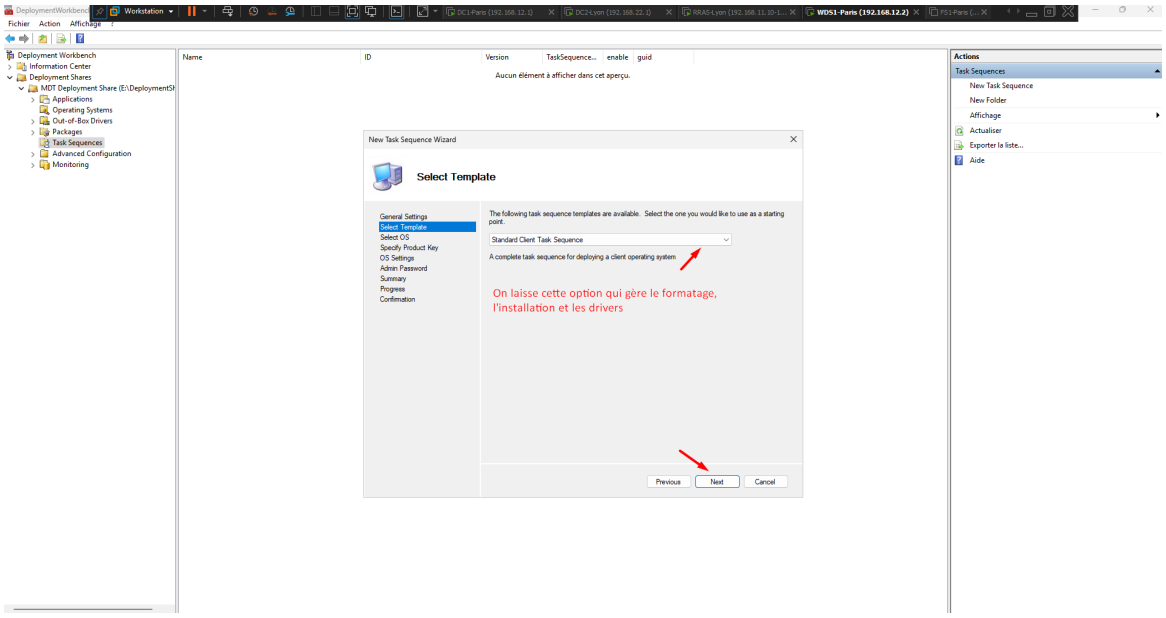

FIGURE 73 – Sélection du modèle Standard Client

8.18 Sélection du système à installer

L'assistant nous demande quel système d'exploitation lier à ce scénario. Nous sélectionnons l'image "Windows 11 Pro" que nous avons importée précédemment.

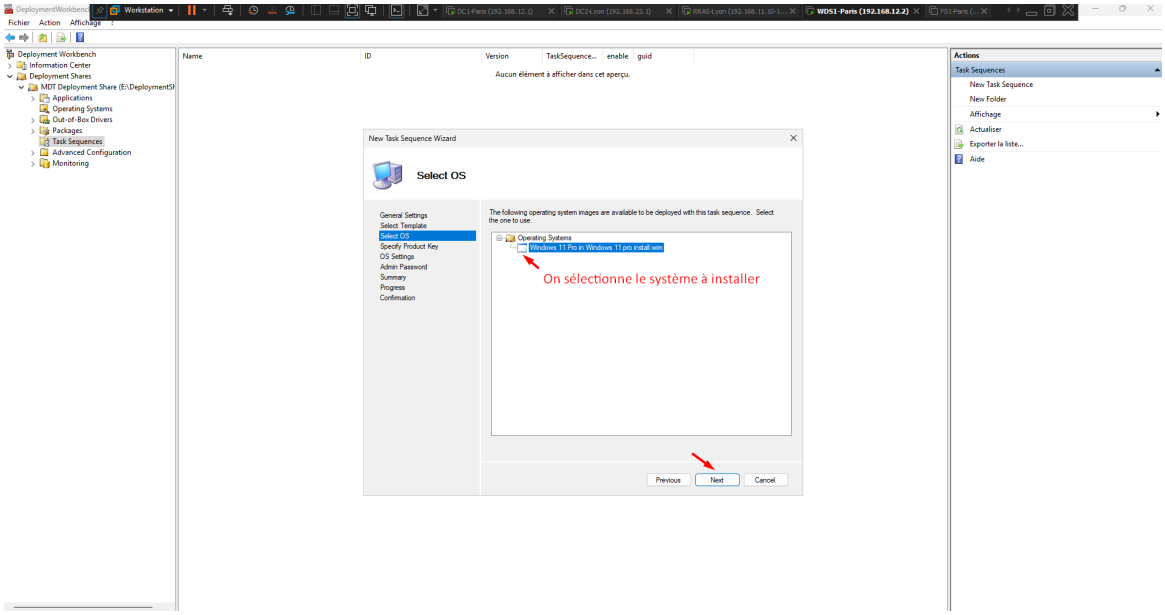

FIGURE 74 – Sélection de Windows 11 Pro pour la séquence

8.19 Spécification de la clé de produit

Pour la gestion des licences, nous choisissons "Do not specify a product key at this time". La licence pourra être gérée plus tard via un serveur KMS (VAMT) ou des règles spécifiques.

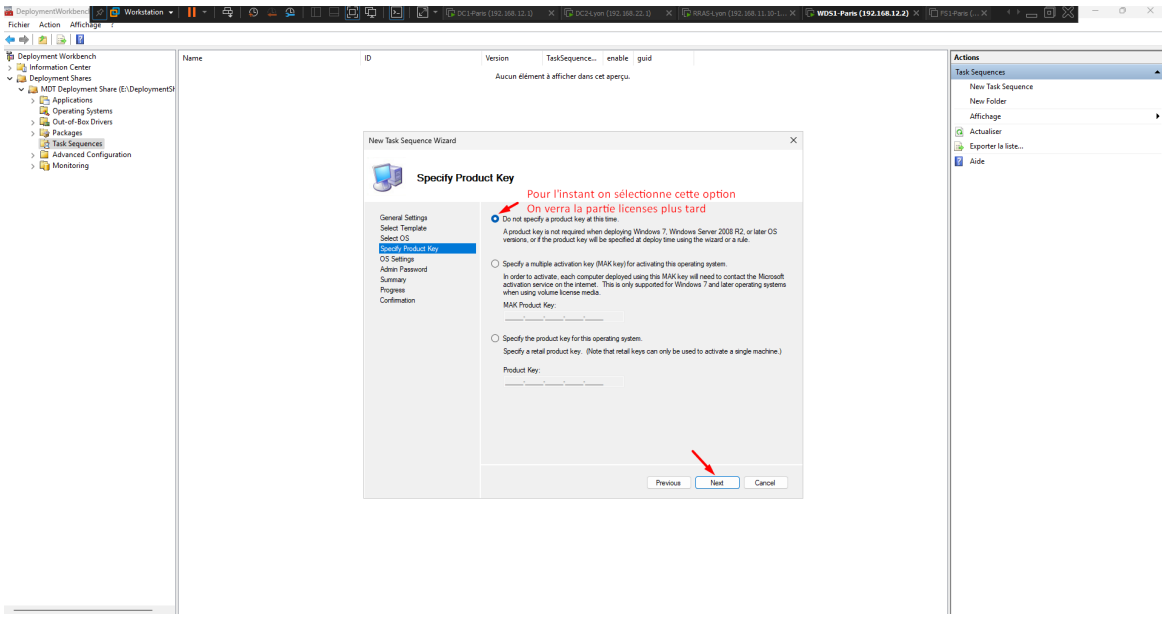

FIGURE 75 – Configuration pour ne pas saisir de clé de produit

8.20 Paramètres de l'OS (Nom et Organisation)

On indique un nom d'utilisateur (temporaire, ex : Administrateur) et le nom de notre organisation (`LEARN`). Il est aussi possible de forcer une page d'accueil d'entreprise pour le navigateur web à cette étape.

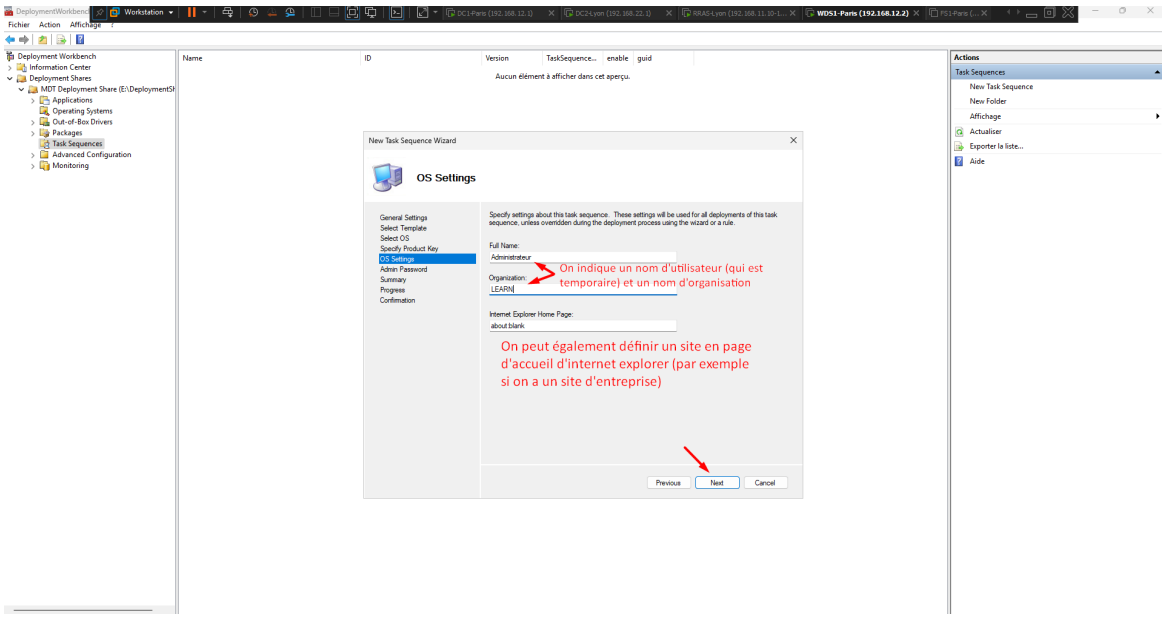

FIGURE 76 – Saisie des métadonnées de l'organisation

8.21 Mot de passe Administrateur local

Nous choisissons "Do not specify an Administrator password at this time". Aucun mot de passe local statique n'est défini ici ; les techniciens s'authentifieront avec leurs identifiants Active Directory une fois la machine jointe au domaine.

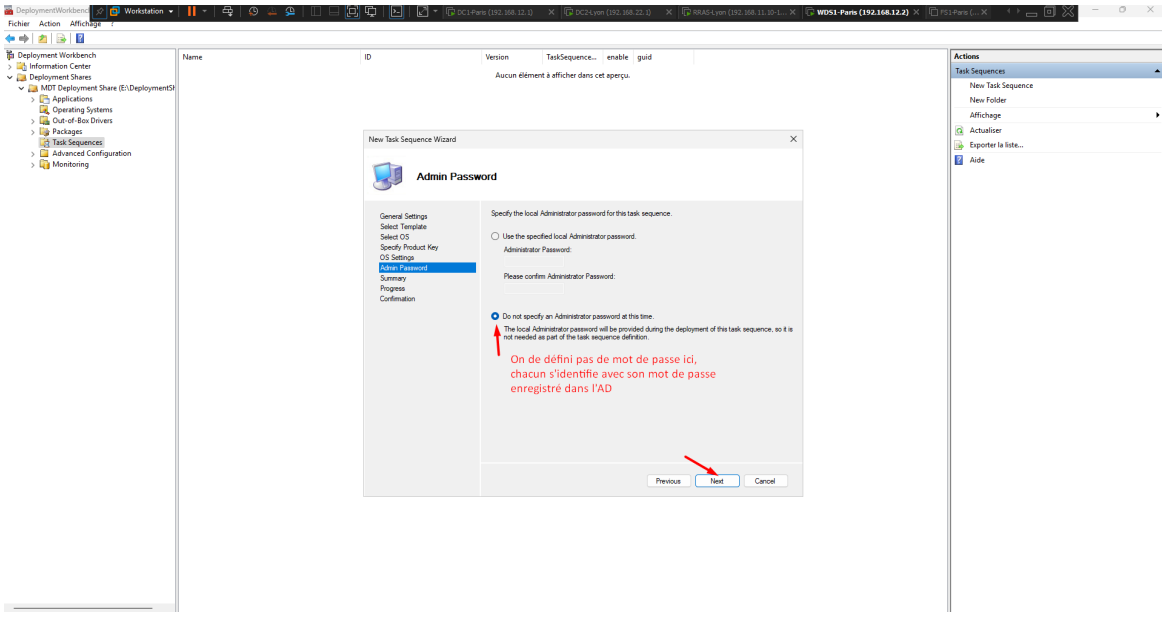

FIGURE 77 – Désactivation de la définition du mot de passe admin local

8.22 Fin de l'assistant de Task Sequence

La création du scénario d'installation est un succès. On ferme l'assistant.

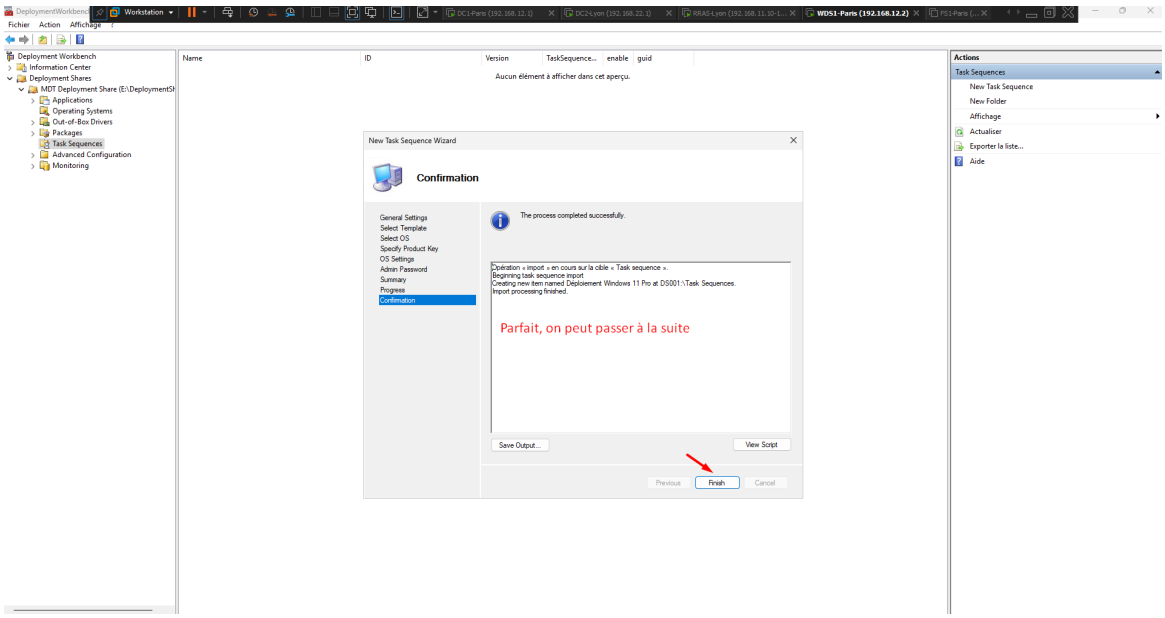

FIGURE 78 – Confirmation de la création de la séquence de tâches

8.23 Accès aux propriétés du Deployment Share

Pour finaliser l'automatisation de l'installation et éviter que Windows ne pose des questions sur le fuseau horaire ou la langue du clavier, nous faisons un clic-droit sur notre "MDT Deployment Share" et ouvrons les propriétés pour modifier les règles de déploiement (`Rules`).

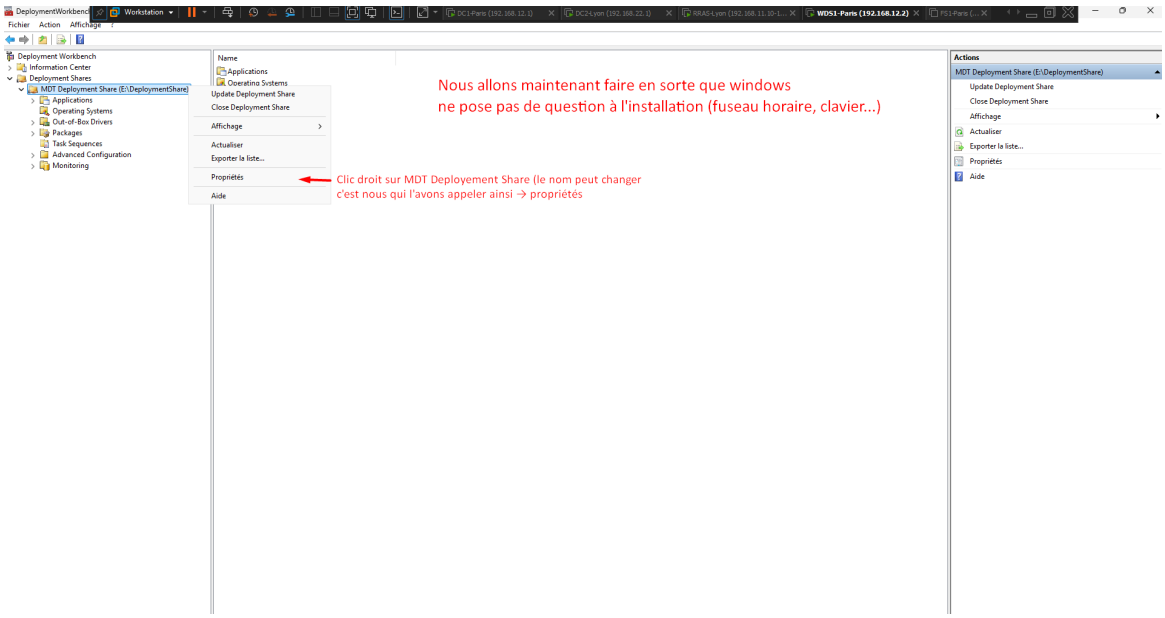

FIGURE 79 – Ouverture des propriétés du Deployment Share

8.24 Configuration des règles (Rules) du Deployment Share

Dans les propriétés du Deployment Share, nous allons dans l'onglet "Rules". Nous y collons un ensemble de paramètres (ex : `SkipTimeZone=YES`, `SkipLocaleSelection=YES`) afin d'automatiser l'installation et éviter que Windows ne pose des questions inutiles à l'utilisateur lors du déploiement.

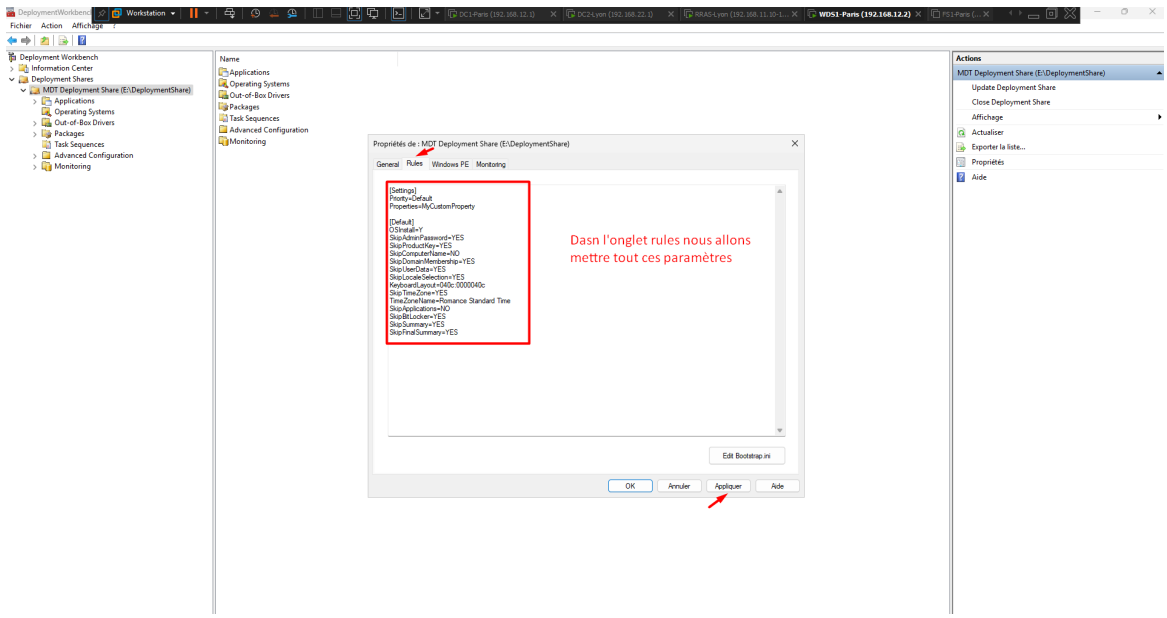

FIGURE 80 – Paramétrage des règles d'automatisation dans l'onglet Rules

8.25 Correction du bug x86 et Mise à jour du Deployment Share

Le déploiement x86 n'étant plus géré correctement avec Windows 11 et Server 2025, cela fait planter l'installation. Nous éditons d'abord le fichier `Settings.xml` dans le dossier `Control` pour remplacer la balise `<SupportX86>True</SupportX86>` par `False`. Ensuite, nous faisons un clic-droit sur le Deployment Share pour faire un "Update deployment share" en choisissant "completely regenerate the boot images".

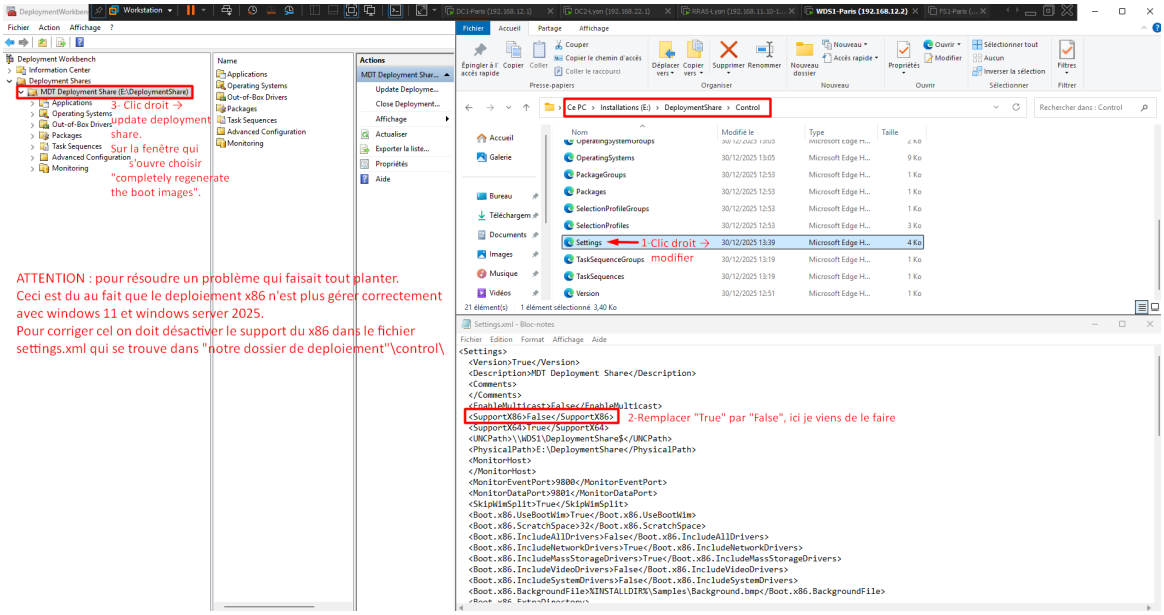

FIGURE 81 – Désactivation du support x86 et régénération des images de boot

8.26 Correction du chemin WinPE_OCs

Un second bug persiste : WinPE cherche le dossier `WinPE_OCs` au mauvais endroit. Nous devons nous rendre dans les dossiers d'installation du Windows ADK (`Windows Preinstallation Environment\amd64`), et copier ce dossier vers un nouveau répertoire `x86` que nous créons au même niveau.

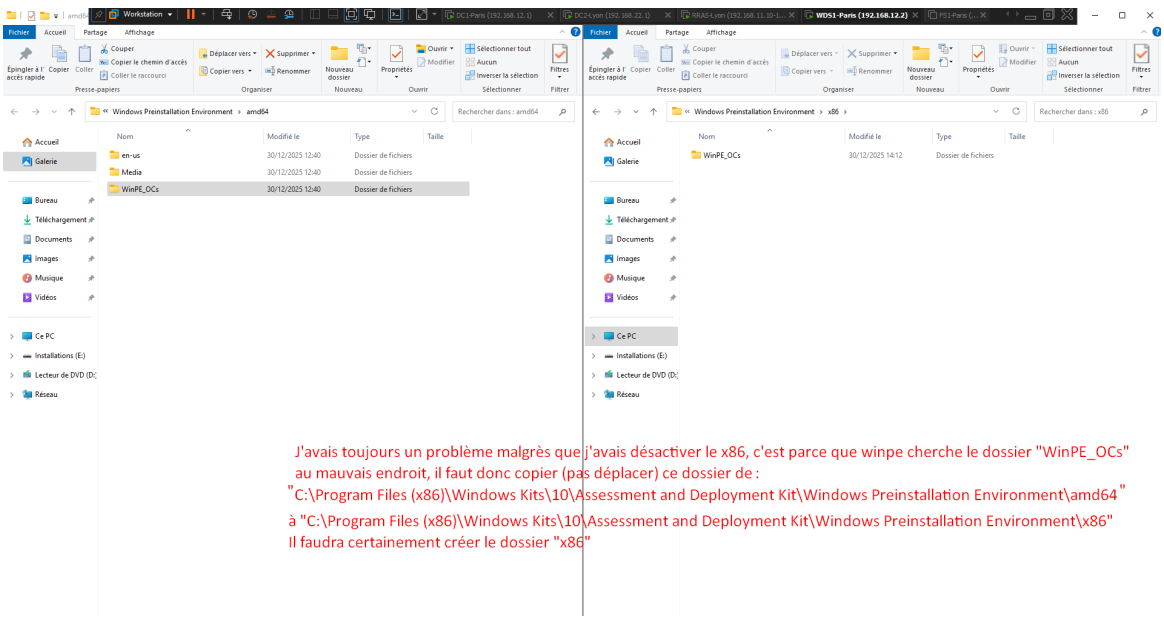

FIGURE 82 – Copie du dossier WinPE_OCs vers le répertoire x86

8.27 Configuration du Scratch Space (Windows PE)

De retour dans les propriétés du Deployment Share, dans l'onglet "Windows PE" (plateforme x64), nous augmentons la taille de la mémoire temporaire ("Scratch space size") à 128 Mo pour garantir une installation plus fluide.

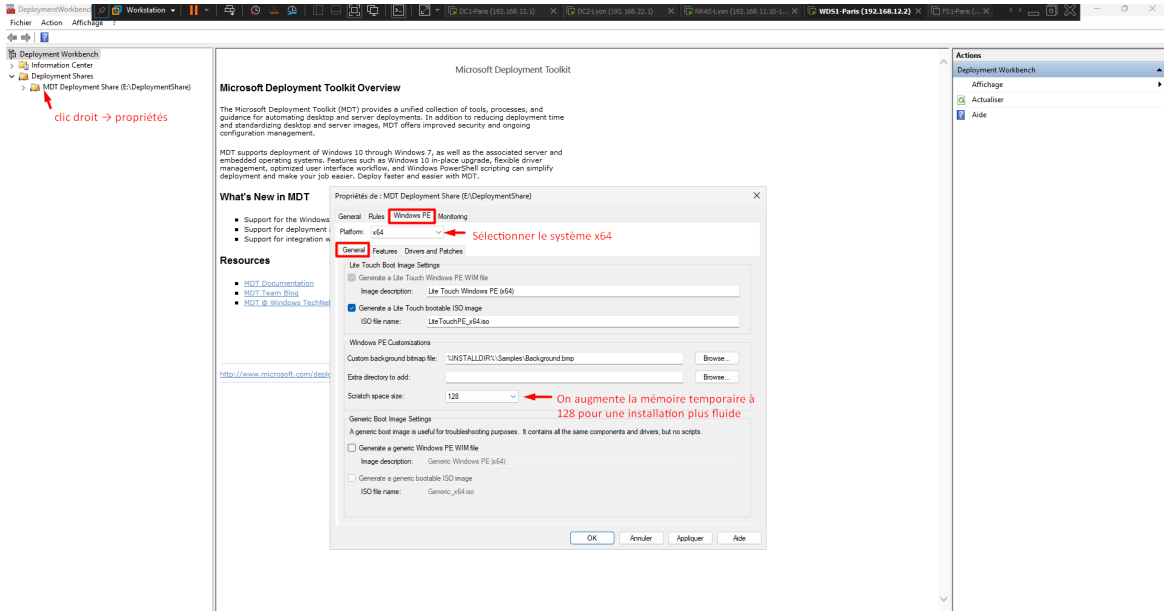

FIGURE 83 – Augmentation du Scratch space à 128 Mo

8.28 Activation des fonctionnalités WinPE

Toujours dans l'onglet "Windows PE", sous la section "Features", il est impératif de cocher trois éléments : `DISM Cmdlets`, `Windows PowerShell`, et `Storage Management Cmdlets`. On valide ensuite par OK.

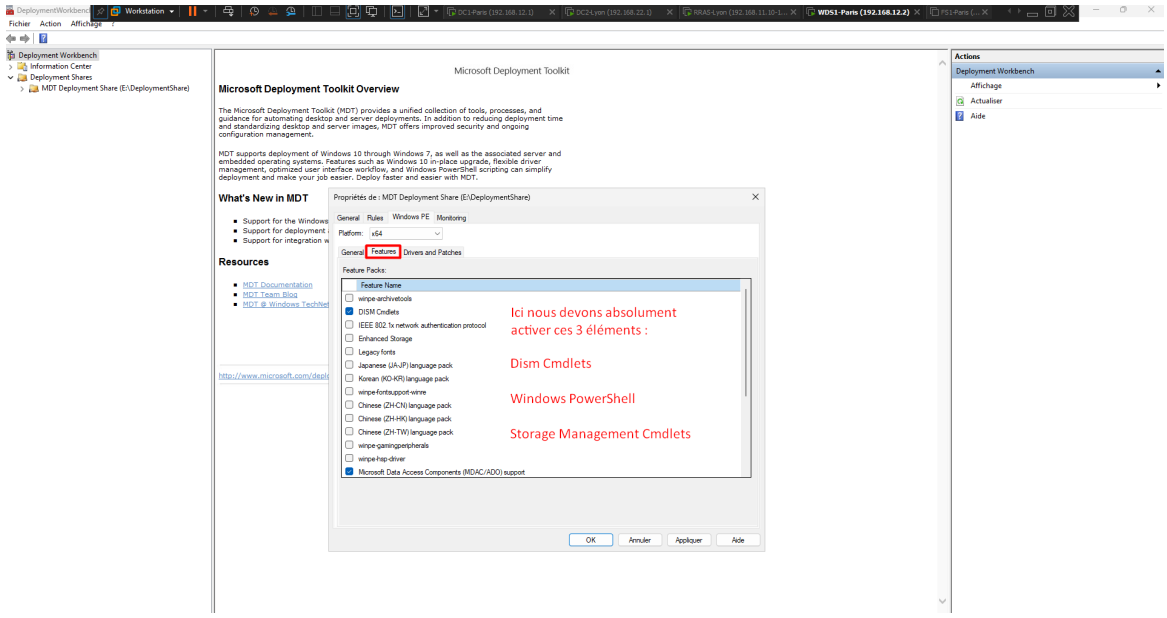

FIGURE 84 – Sélection des Feature Packs nécessaires pour WinPE

8.29 Lancement des Services de déploiement

Maintenant que notre image MDT est prête et corrigée, nous passons au déploiement sur le réseau. Depuis le menu Outils du Gestionnaire de serveur sur WDS1, nous lançons la console "Services de déploiement Windows".

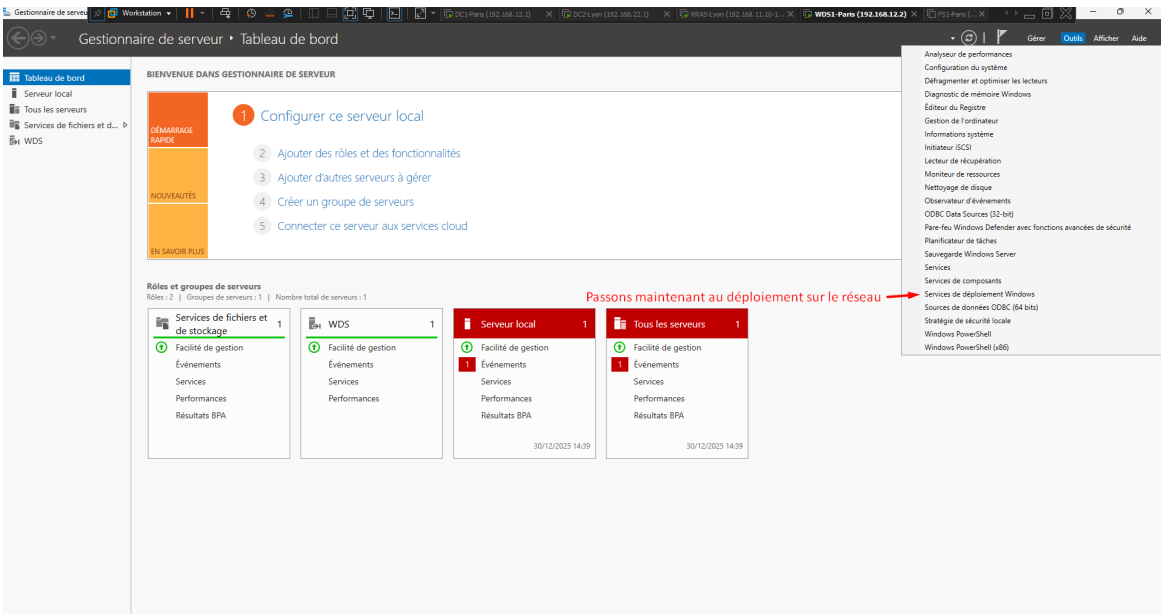

FIGURE 85 – Ouverture de la console WDS depuis le Gestionnaire de serveur

8.30 Configuration initiale du serveur WDS

Dans la console WDS, on fait un clic-droit sur notre serveur `WDS1.learn.local` et on sélectionne "Configurer le serveur".

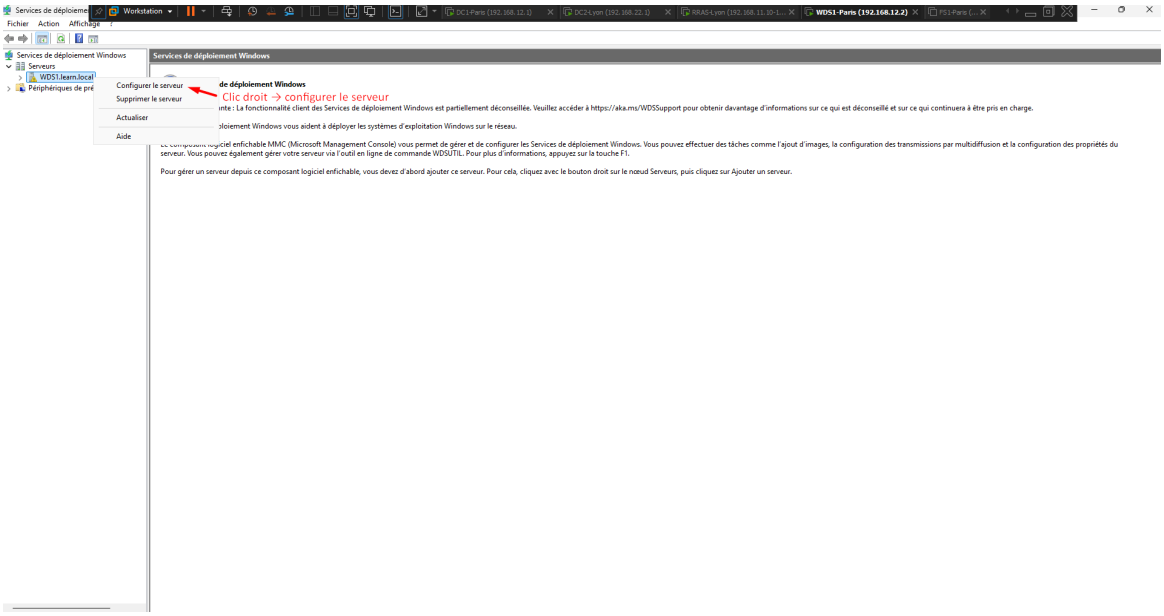

FIGURE 86 – Lancement de la configuration du serveur WDS

8.31 Option d'intégration Active Directory

Dans l'assistant d'installation, nous choisissons l'option "Intégré à Active Directory" puisque notre serveur WDS1 est membre du domaine `learn.local`.

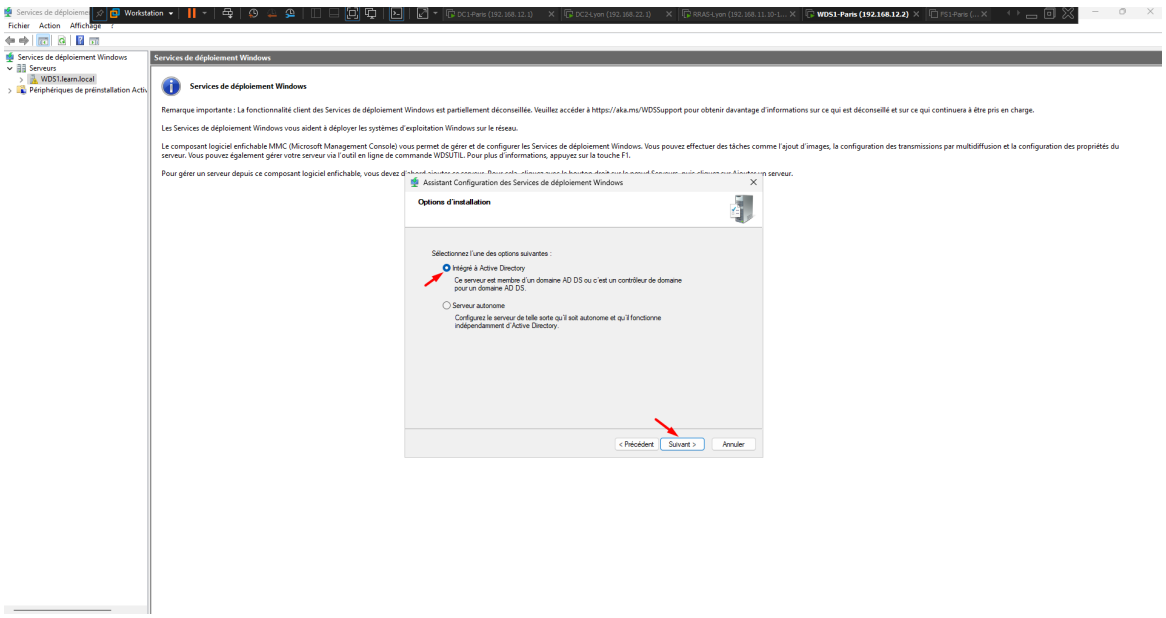

FIGURE 87 – Choix de l'intégration AD DS pour WDS

8.32 Emplacement du dossier d'installation

Nous indiquons un nouveau dossier pour stocker les fichiers d'installation à distance, `E:\RemoteInstall`, qui se situe sur notre disque dédié aux installations réseau.

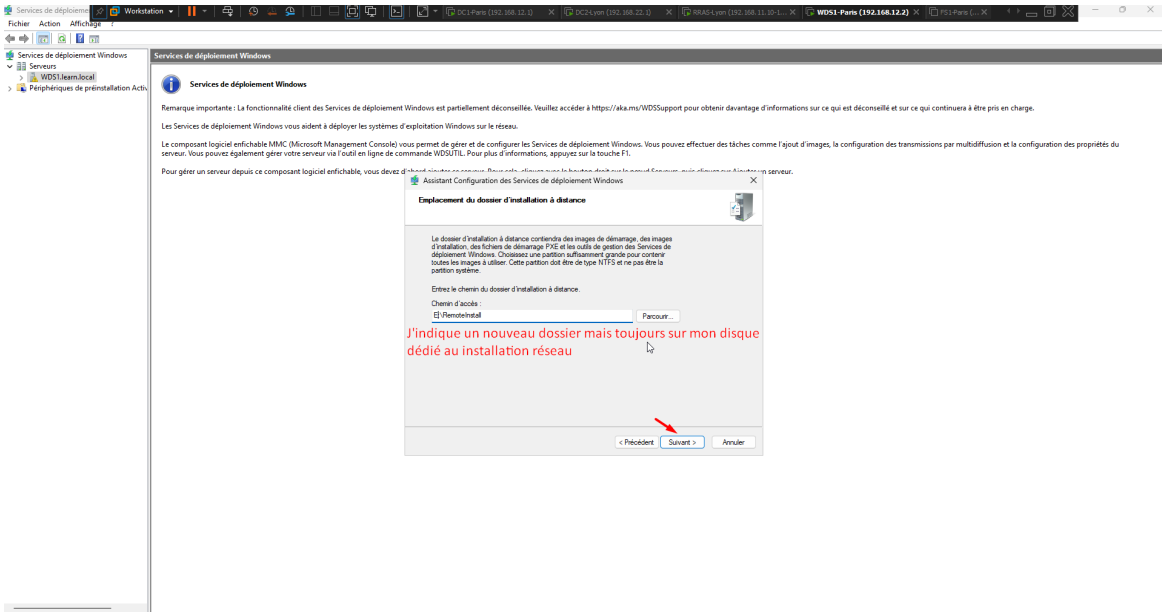

FIGURE 88 – Spécification du répertoire RemoteInstall

8.33 Paramètres de réponse PXE

Pour permettre à n'importe quel nouveau poste de s'installer, nous sélectionnons l'option "Répondre à tous les ordinateurs clients (connus et inconnus)".

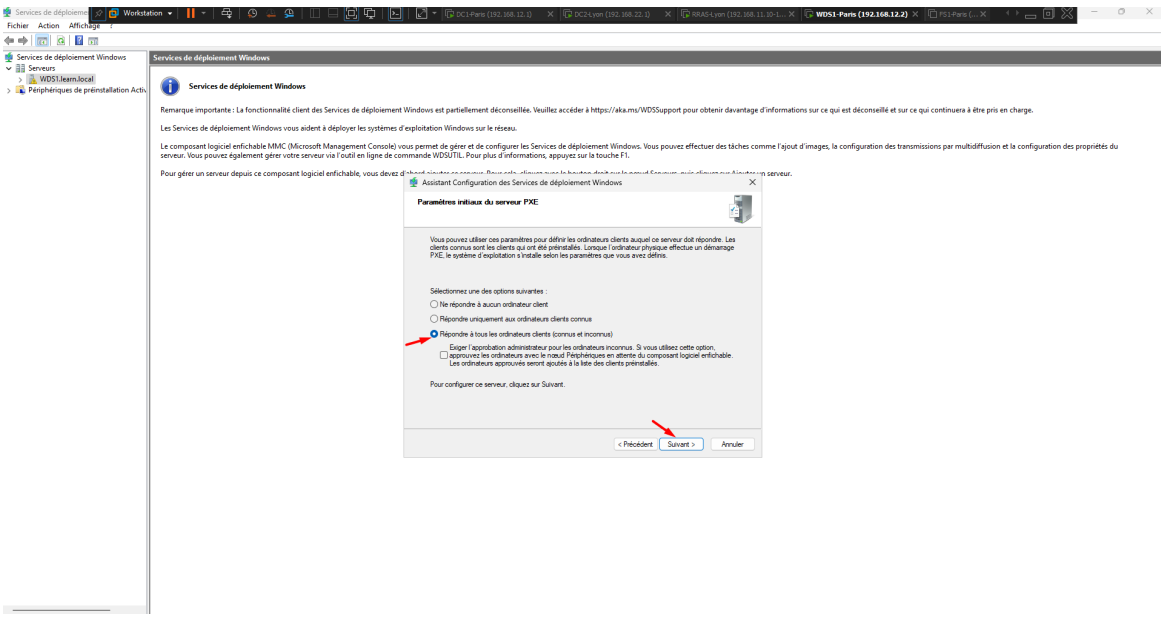

FIGURE 89 – Configuration du serveur PXE pour répondre à tous les clients

8.34 Fin de la configuration WDS

L'assistant est terminé. Il est très important de décocher la case "Ajouter les images au serveur maintenant" car nous allons ajouter manuellement l'image générée par le MDT.

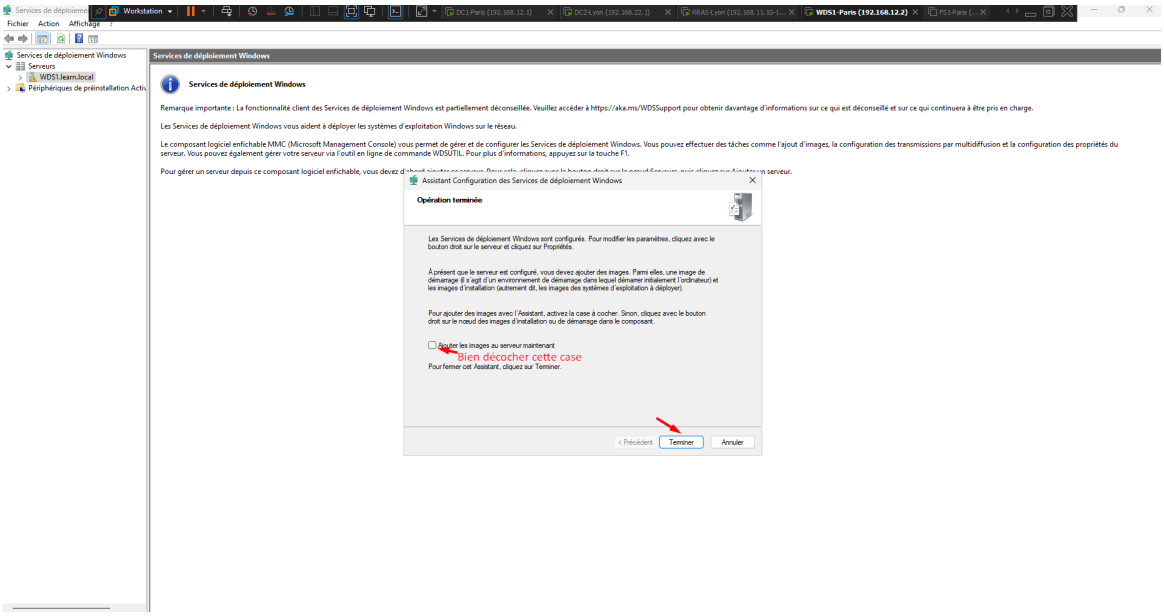

FIGURE 90 – Clôture de l'assistant sans ajout d'image automatique

8.35 Ajout de l'image de démarrage

Dans l'arborescence du serveur WDS1, on fait un clic-droit sur le dossier "Images de démarrage" puis on sélectionne "Ajouter une image de démarrage...".

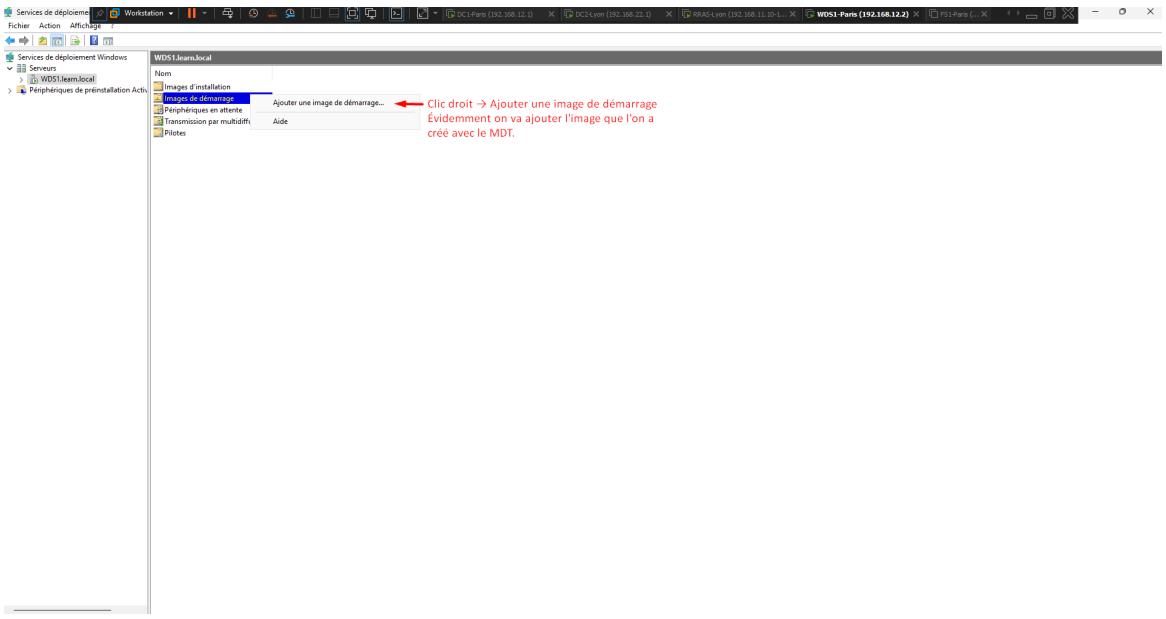

FIGURE 91 – Assistant d'ajout d'une image de démarrage dans WDS

8.36 Sélection du fichier LiteTouch WIM

Nous parcourons l'arborescence pour sélectionner l'image que nous avons créée avec le MDT : `E:\DeploymentShare\Boot\LiteTouchPE_x64.wim`.

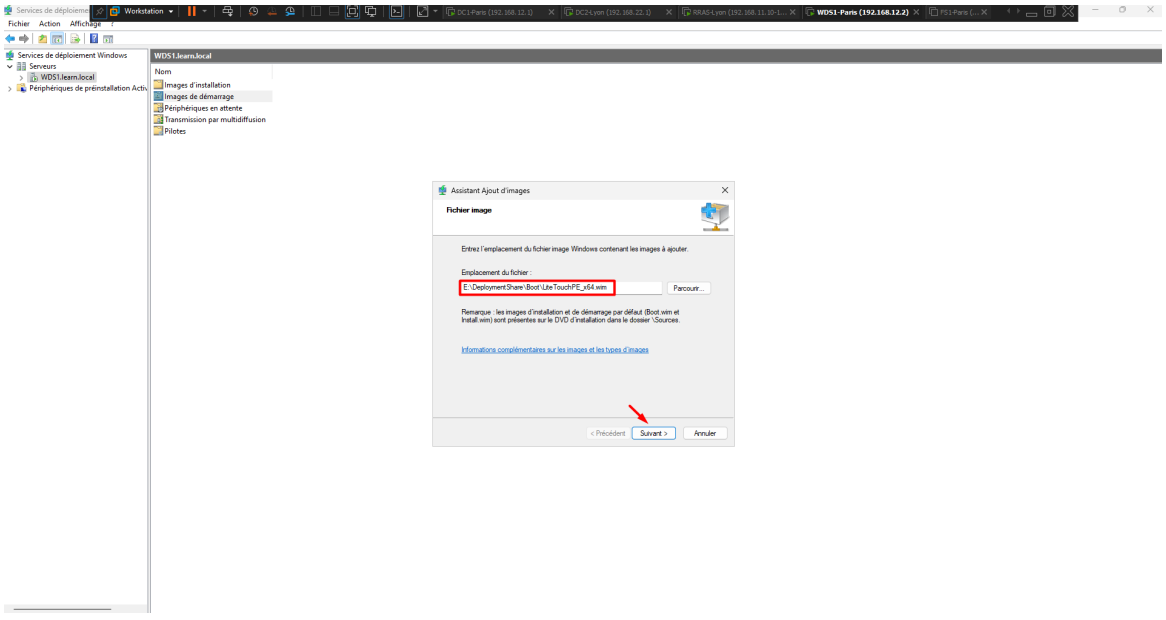

FIGURE 92 – Sélection de l'image de boot personnalisée MDT

8.37 Configuration des options d'étendue DHCP

Étant donné que nos clients et serveurs sont sur des sous-réseaux différents, le broadcast PXE ne passera pas naturellement. Nous devons ajouter des options dans nos étendues DHCP. Sur DC1, on fait un clic-droit sur "Options d'étendue" de l'étendue Paris prod, puis "Configurer les options...".

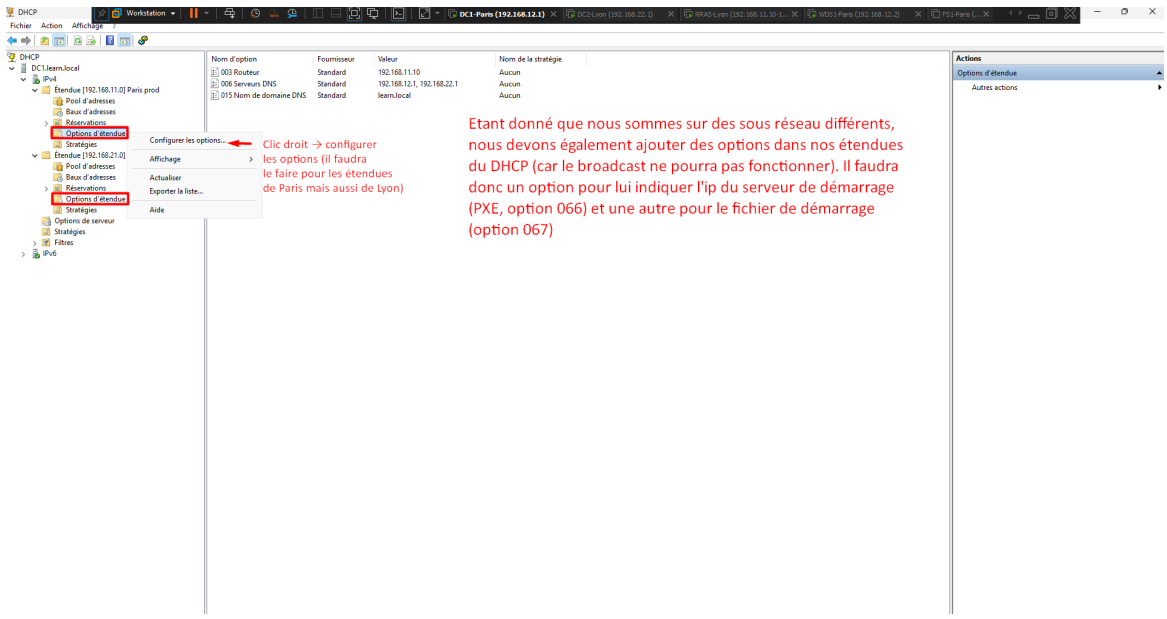

FIGURE 93 – Accès aux options de l'étendue DHCP

8.38 Option 066 (Nom d'hôte du serveur de démarrage)

On active l'option **066**, et en valeur de chaîne, on renseigne l'adresse IP de notre serveur WDS1 : `192.168.12.2`.

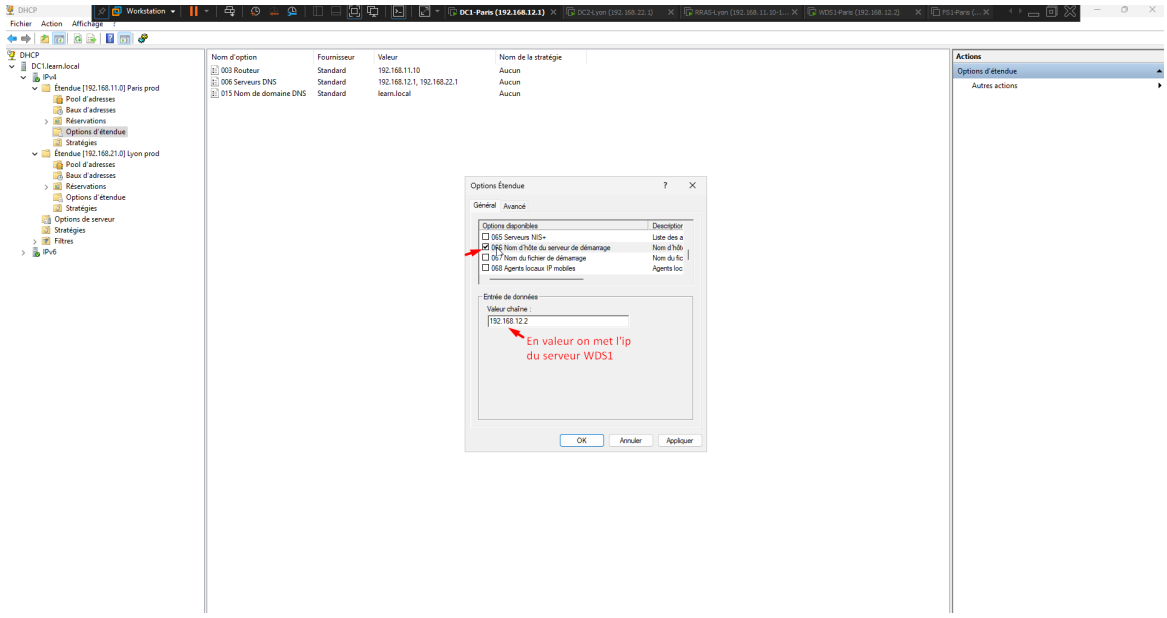

FIGURE 94 – Configuration de l'option 066 avec l'IP du serveur WDS

8.39 Option 067 (Nom du fichier de démarrage)

On active ensuite l'option **067**, et on y inscrit le chemin du bootloader utilisé pour amorcer l'installation : `boot\x64\wdsnbp.com`.

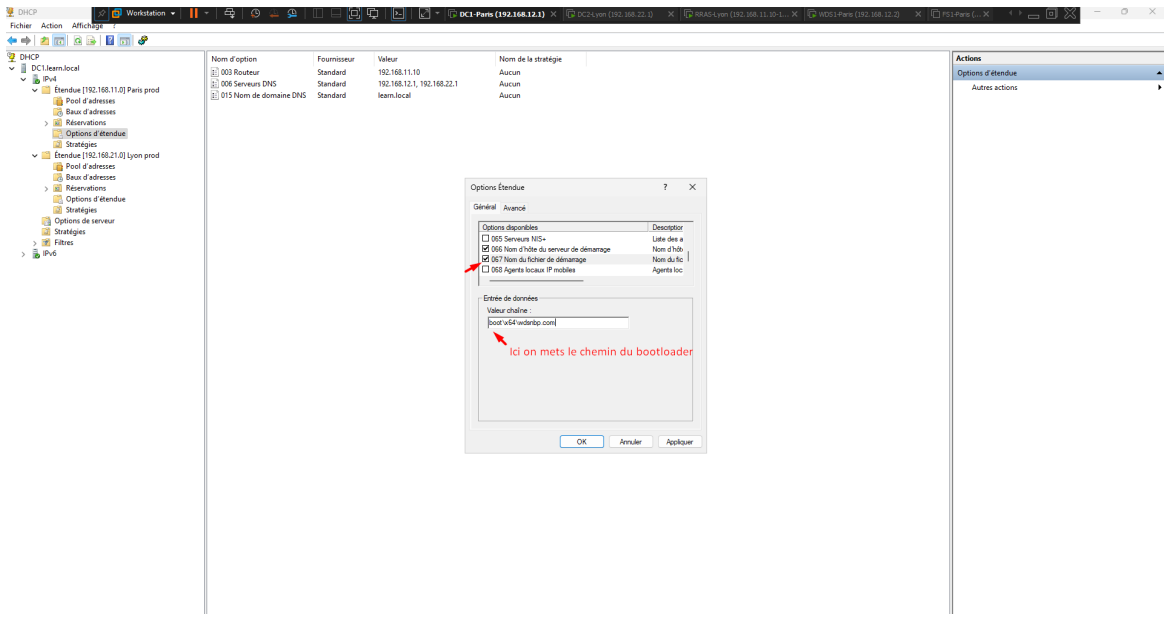

FIGURE 95 – Configuration de l'option 067 avec le chemin du bootloader

8.40 Synchronisation des étendues de basculement

Après avoir configuré nos 2 options (pour Paris et pour Lyon), nous devons synchroniser cela. Grâce au basculement DHCP configuré précédemment, on fait un clic-droit sur le nœud "IPv4" et on sélectionne "Répliquer les étendues de basculement...".

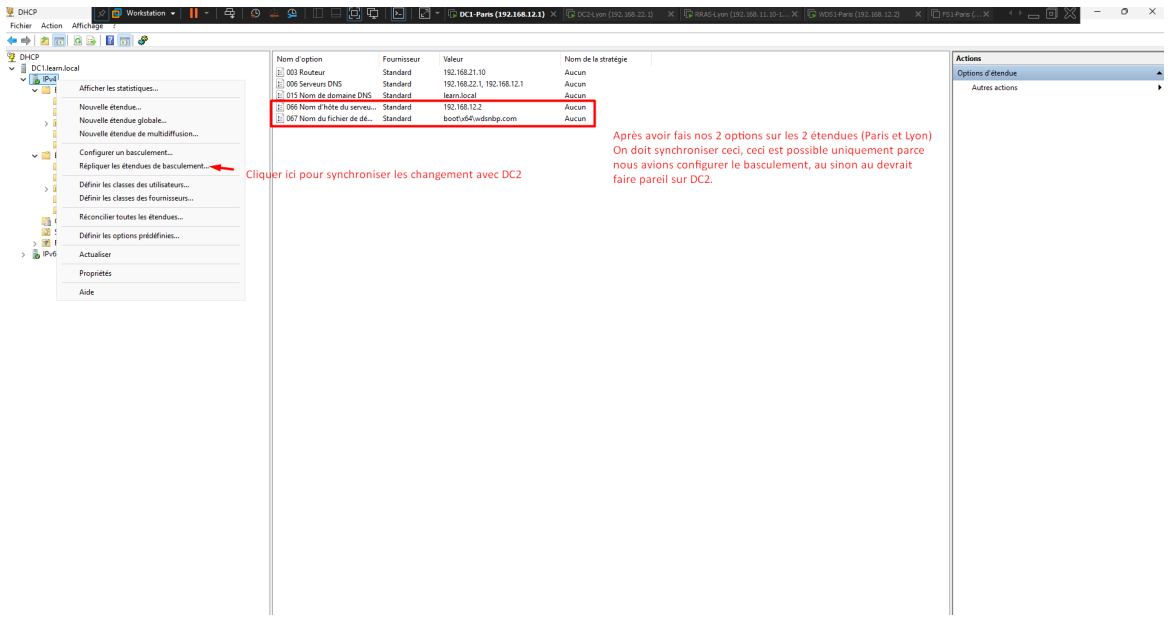

FIGURE 96 – Lancement de la réplication des modifications vers DC2

8.41 Vérification de la synchronisation sur DC2

En nous connectant sur DC2, nous vérifions l'étendue de Lyon prod. Nous constatons avec succès que les options 066 et 067 se sont bien synchronisées sur DC2.

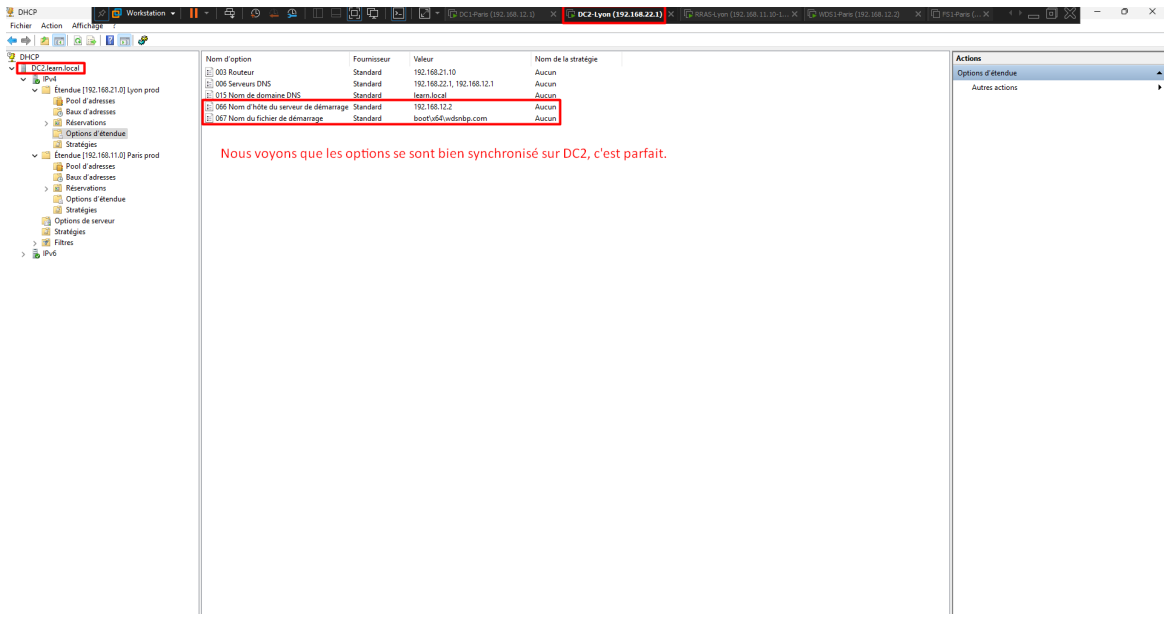

FIGURE 97 – Vérification des options DHCP synchronisées sur DC2

8.42 Ajout de WDS à l'Agent de relais DHCP (RRAS)

Dernière étape indispensable pour que les installations PXE fonctionnent : sur le serveur RRAS, dans la console Routage et accès distant, on ouvre les propriétés de l'Agent de relais DHCP et on ajoute l'adresse IP du serveur WDS1 (`192.168.12.2`) dans la liste des serveurs.

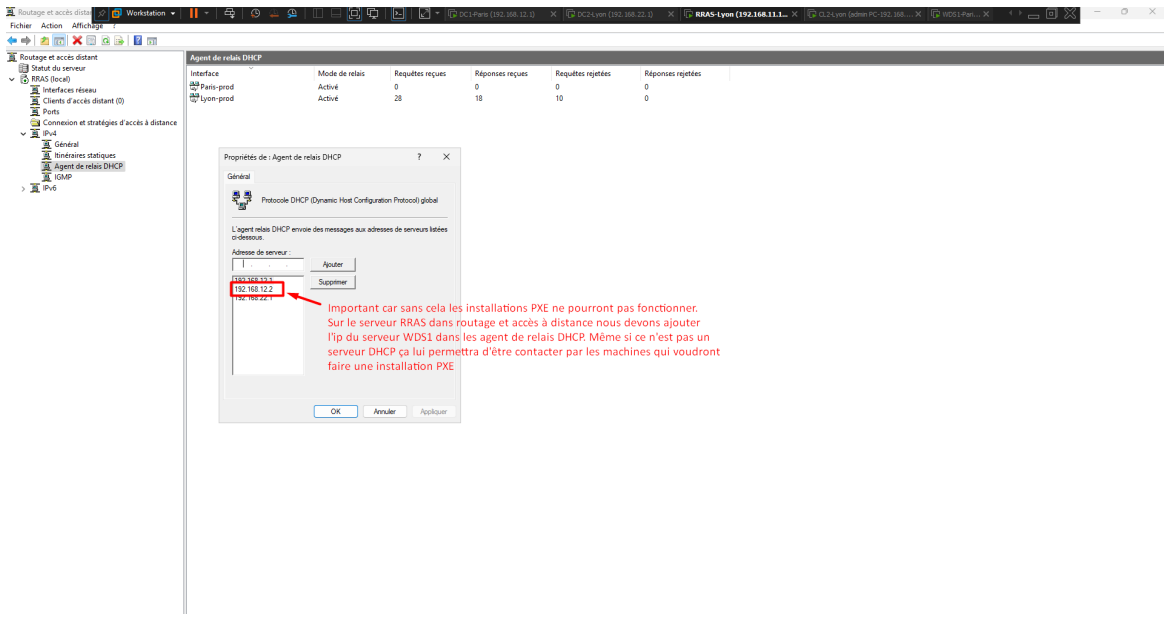

FIGURE 98 – Ajout de l'IP du WDS dans les relais DHCP du routeur

9 TEST ET DÉPLOIEMENT DU POSTE CLIENT (CL2)

9.1 Préparation de la machine virtuelle cliente

Le moment est venu de tester tout ça. Nous allons procéder à l'installation de CL2 (le poste admin à Lyon) en PXE. On s'assure que sa carte réseau est bien sur le bon réseau ("Lab entreprise (Lyon-prod)") dans les paramètres VMware.

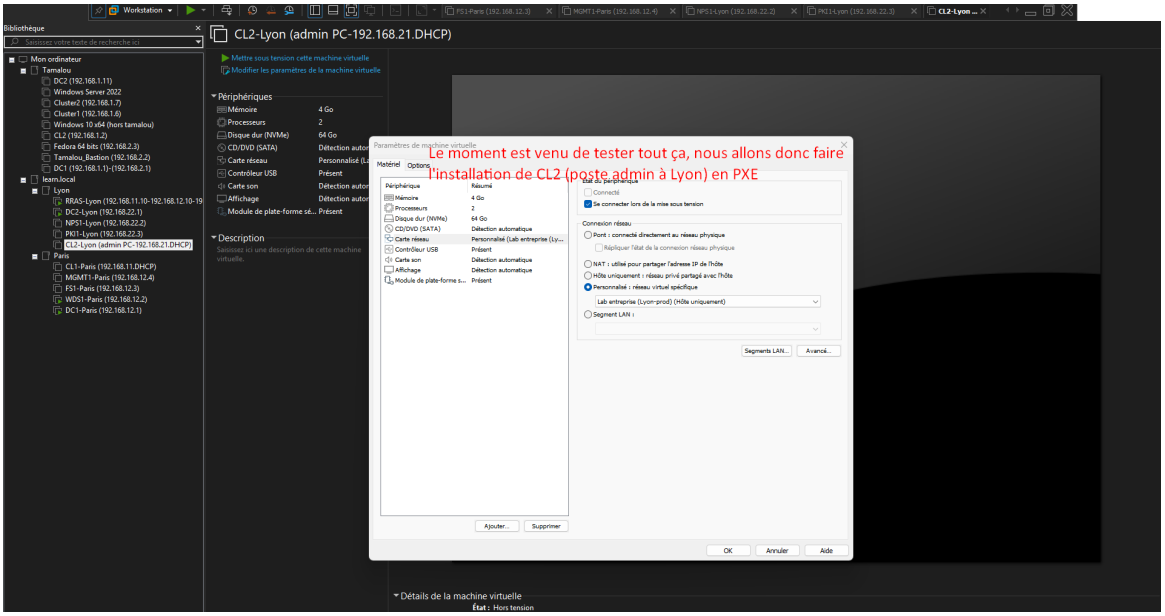

FIGURE 99 – Paramétrage réseau de la VM cliente CL2 avant démarrage

9.2 Chargement de l'environnement WinPE

Le client CL2 démarre sur le réseau et récupère avec succès l'image de boot générée par WDS1 via le réseau. Les fichiers se chargent en mémoire.

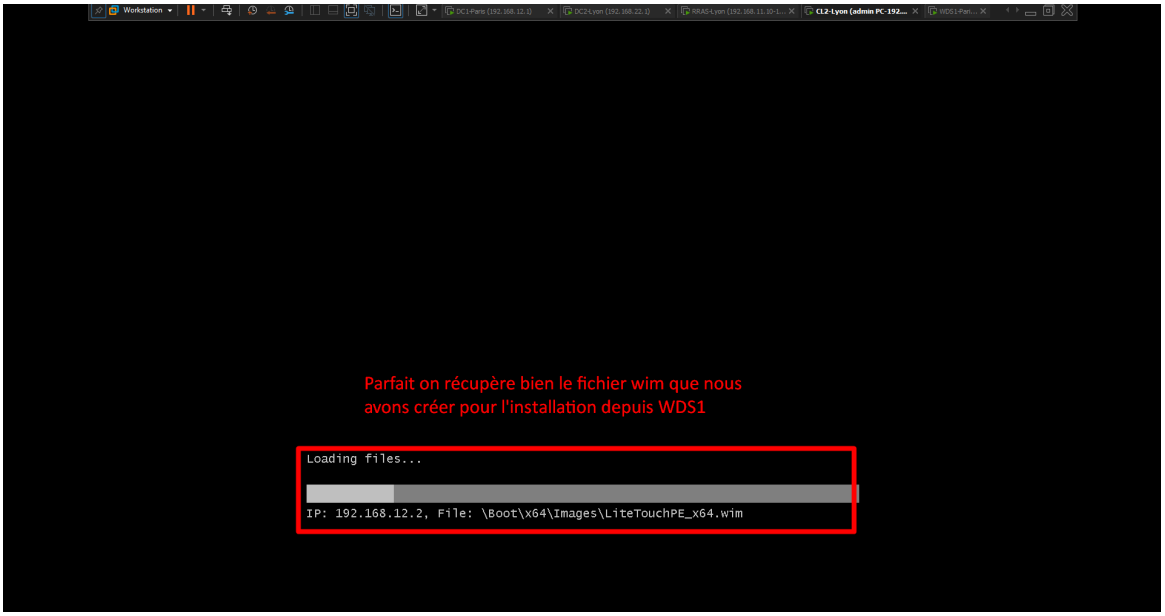

FIGURE 100 – Chargement en mémoire de l'image de démarrage LiteTouch

9.3 Écran de bienvenue MDT

L'interface du Microsoft Deployment Toolkit s'affiche correctement sur la machine cliente. Nous cliquons sur le bouton "Run the Deployment Wizard" pour lancer l'installation.

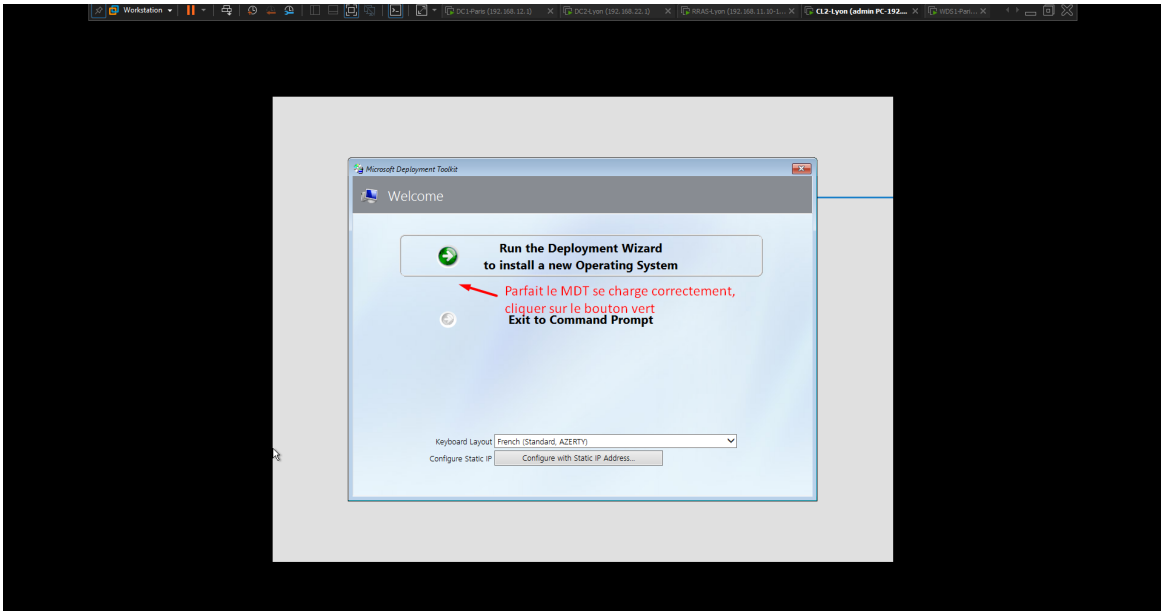

FIGURE 101 – Écran d'accueil de l'assistant LiteTouch MDT

9.4 Erreur de connexion (Absence de pilotes)

Une erreur "Wizard Error" apparaît : "A connection to the deployment share could not be made". Cela est dû au fait que nous sommes sur une machine virtuelle VMware, et que l'environnement WinPE natif ne possède pas les pilotes de la carte réseau virtuelle (`vmxnet3`) pour contacter le partage réseau.

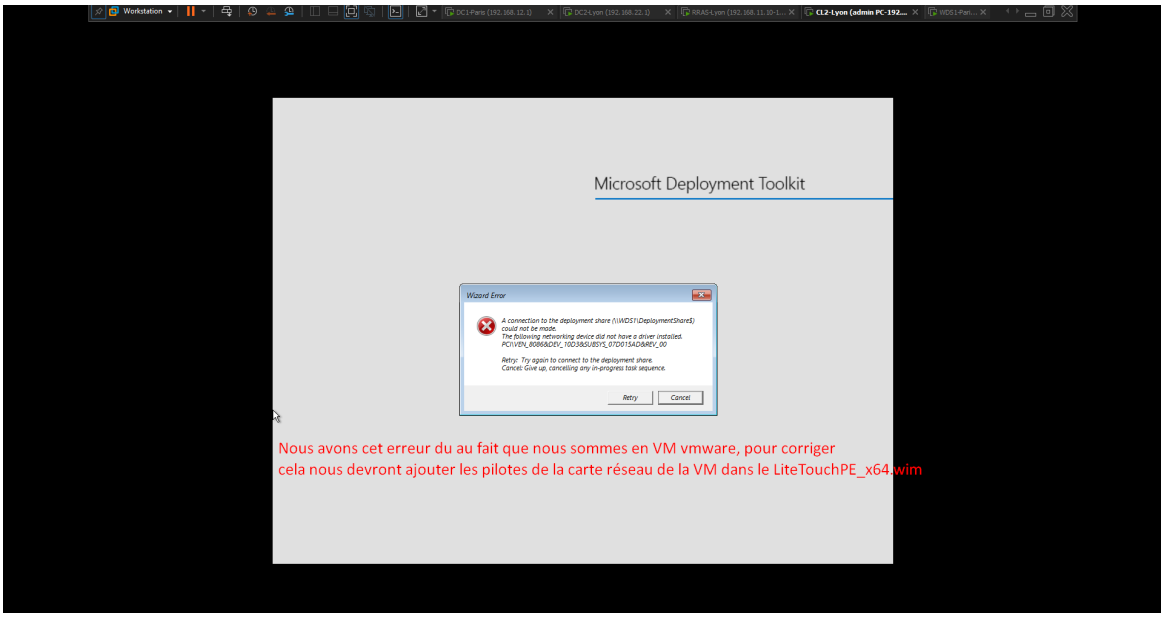

FIGURE 102 – Échec de connexion au Deployment Share dû à un manque de pilotes

9.5 Récupération des pilotes VMware

Pour corriger cela, nous devons injecter les pilotes réseau de VMware dans notre image `.wim`. Nous récupérons les fichiers `vmxnet3.inf` (situés originellement dans `C:\Windows\System32\DriverStore\` et nous les copions dans un dossier de travail local, par exemple `C:\Drivers_VM` sur notre serveur WDS1.

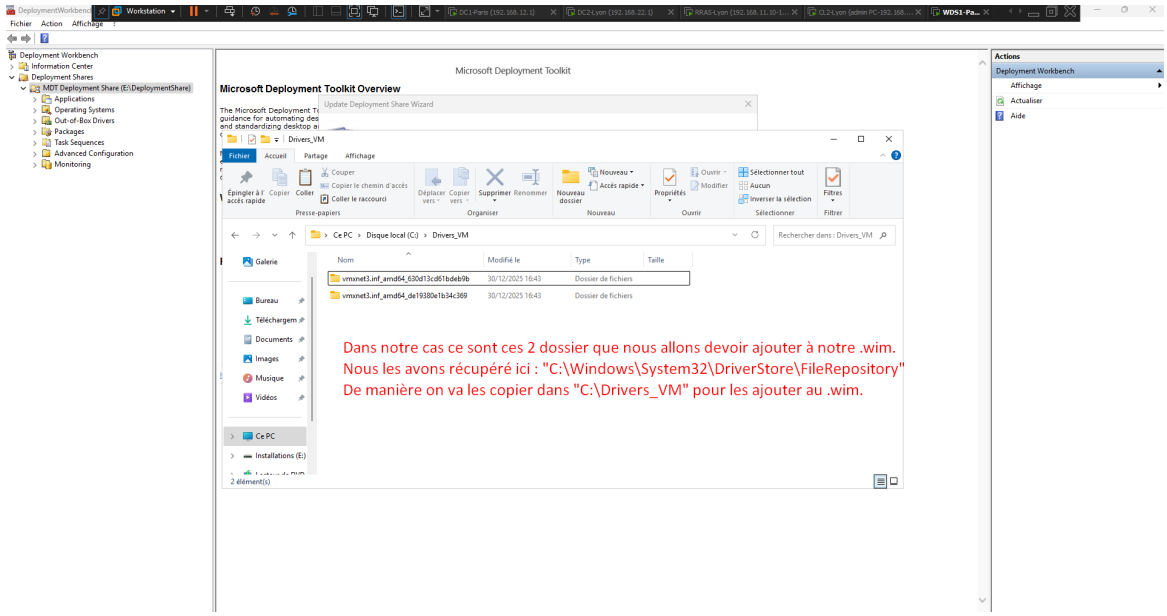

FIGURE 103 – Dossier contenant les pilotes réseau VMware extraits

9.6 Importation des pilotes dans MDT

De retour dans la console Deployment Workbench sur WDS1, nous faisons un clic-droit sur le dossier "Out-of-Box Drivers" et choisissons "Import Drivers".

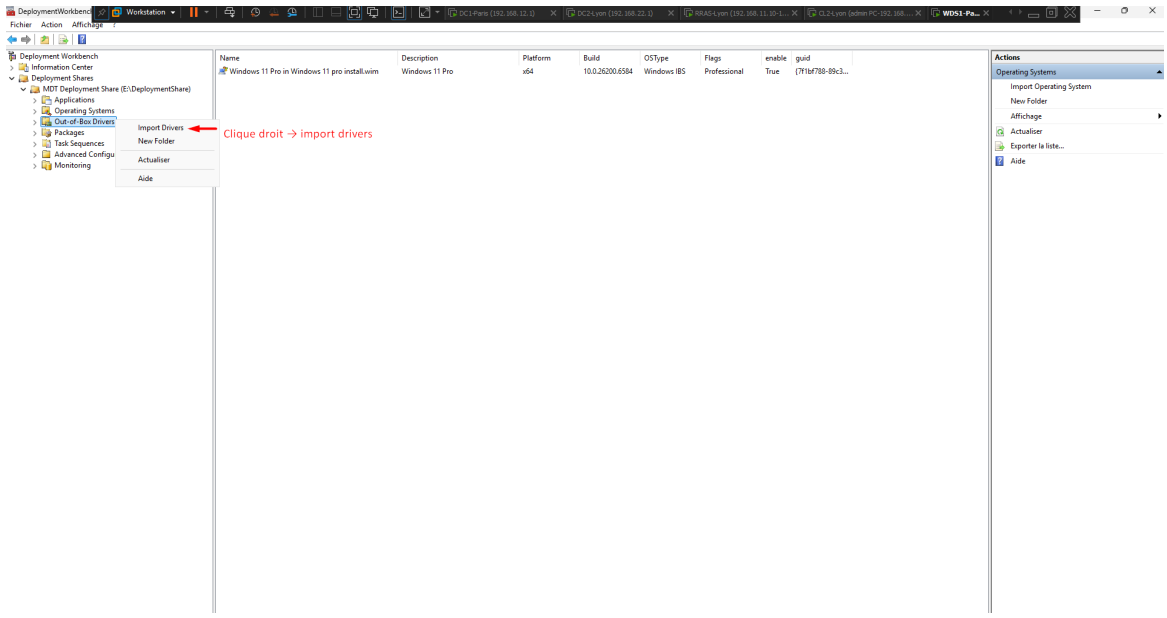

FIGURE 104 – Lancement de l'assistant d'importation de pilotes

9.7 Sélection du répertoire source

Dans l'assistant, nous indiquons le chemin où nous avons stocké les pilotes : `C:\Drivers_VM`. Nous validons les étapes suivantes jusqu'à la fin de l'importation.

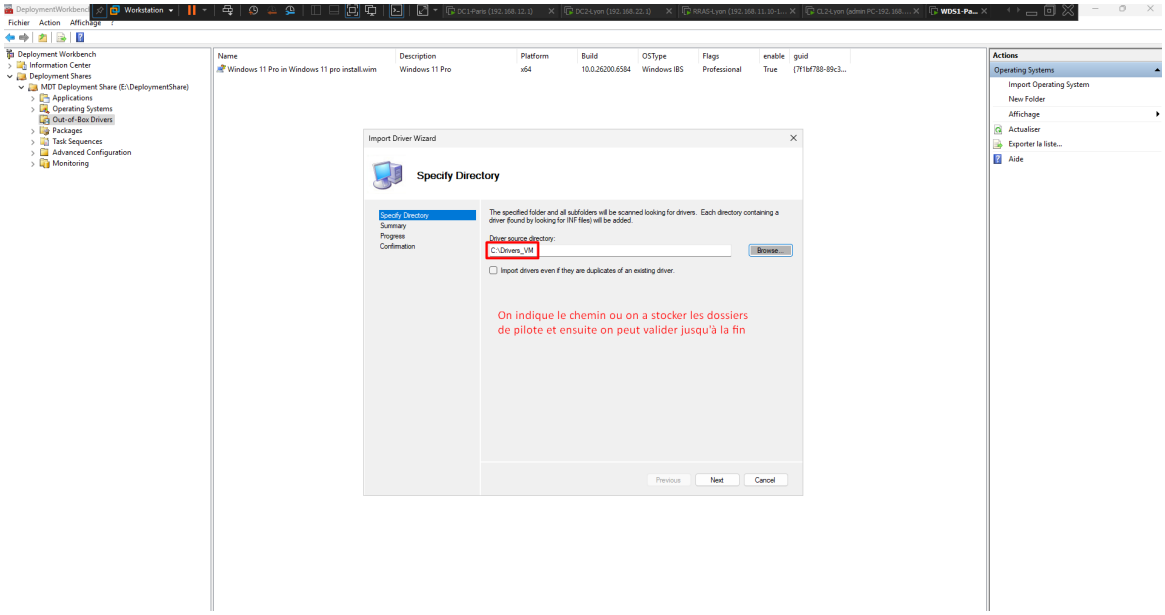

FIGURE 105 – Sélection du répertoire contenant les pilotes à importer

9.8 Mise à jour du Deployment Share

Maintenant que le pilote réseau VMware est importé dans la console, nous devons régénérer l'image. On fait un clic-droit sur le Deployment Share et on sélectionne "Update Deployment Share" pour recréer le fichier `.wim` avec les pilotes intégrés.

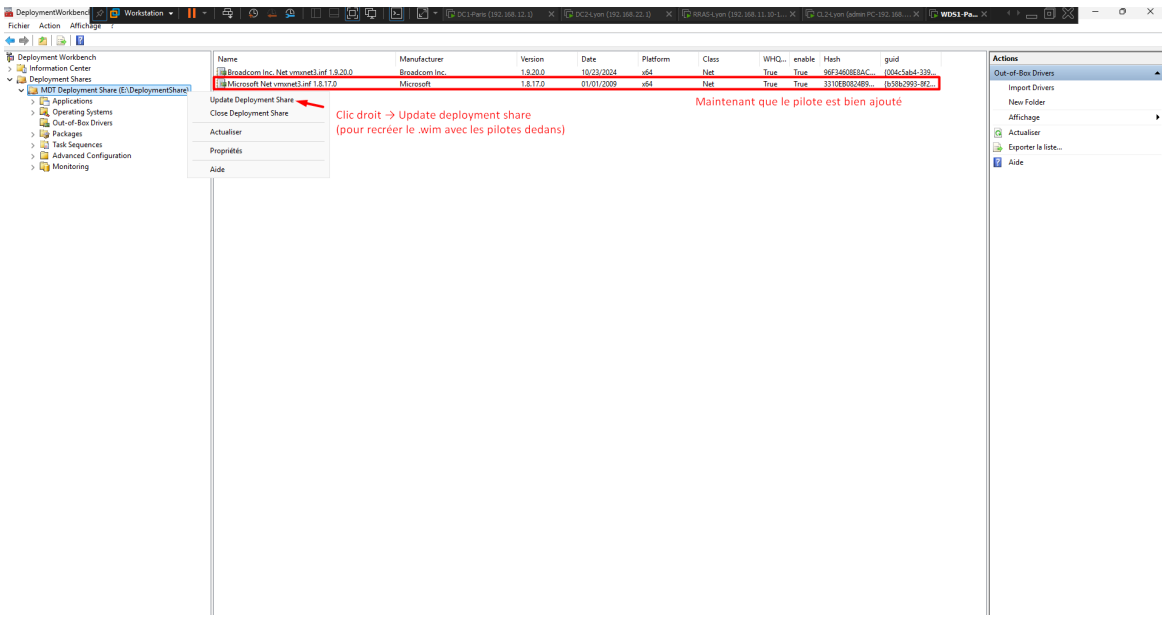

FIGURE 106 – Lancement de la mise à jour pour intégrer les nouveaux pilotes

9.9 Remplacement de l'image de démarrage dans WDS

Il ne faut pas oublier de mettre à jour le serveur WDS. Dans la console Services de déploiement Windows, on fait un clic-droit sur notre ancienne image "Boot W11-Pro" et on sélectionne "Remplacer l'image...".

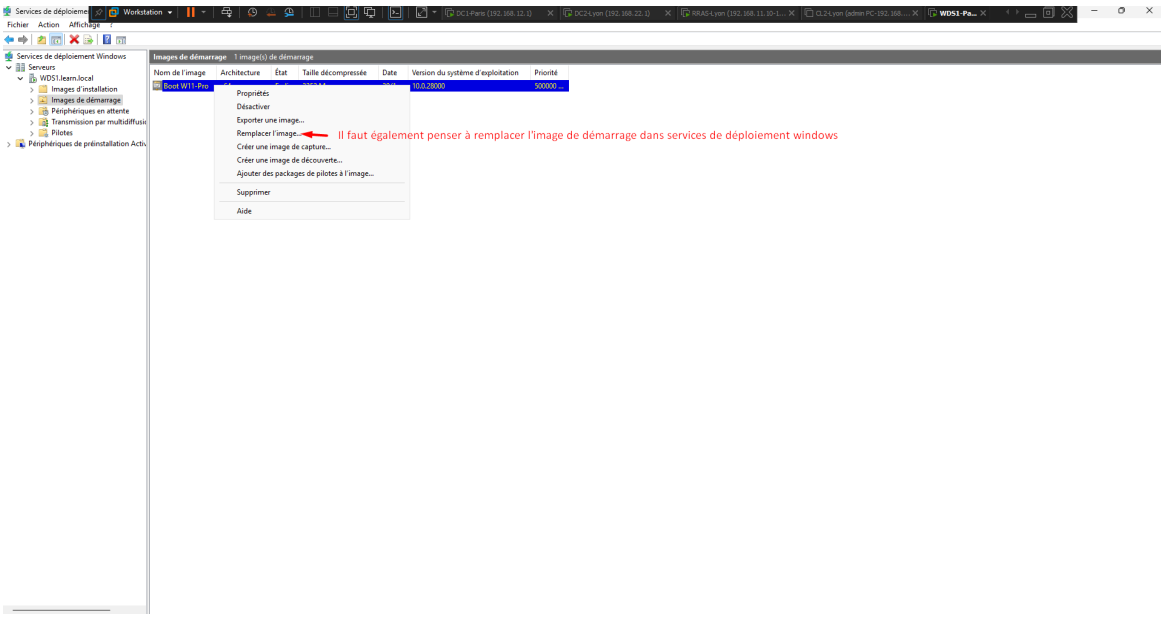

FIGURE 107 – Option de remplacement de l'image dans la console WDS

9.10 Sélection de l'image mise à jour

Dans l'assistant, nous pointons vers le fichier qui vient d'être mis à jour par le MDT : `E:\DeploymentShare\Boot\LiteTouchPE_x64.wim`.

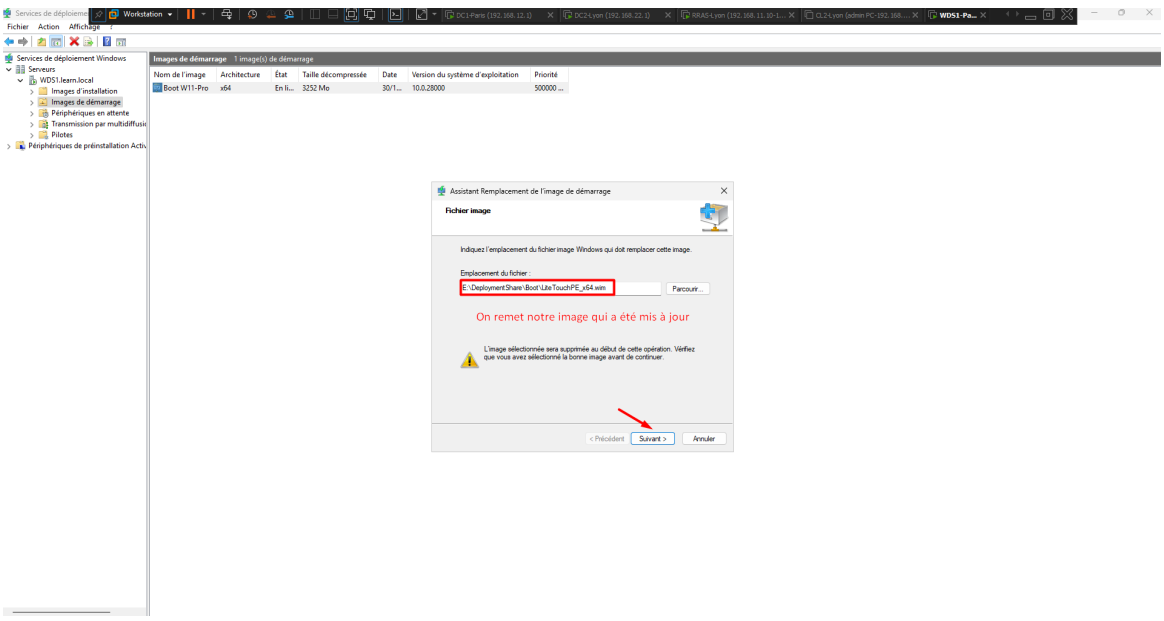

FIGURE 108 – Sélection du fichier WIM régénéré contenant les pilotes

9.11 Authentification MDT (Credentials)

Nous redémarrons la VM cliente CL2. Cette fois, la carte réseau fonctionne. L'assistant MDT demande les informations d'identification pour se connecter au partage réseau. Nous renseignons `Administrateur` et le domaine `LEARN`.

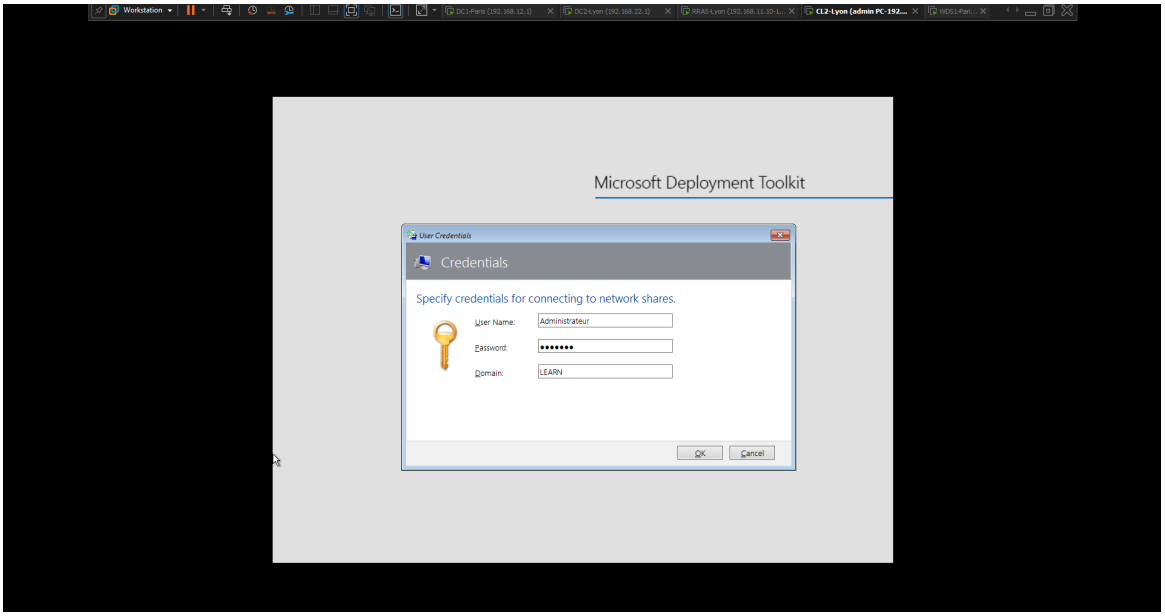

FIGURE 109 – Saisie des identifiants d'accès au Deployment Share

9.12 Sélection de la Task Sequence

Nous sélectionnons la séquence de tâches que nous avons créée précédemment ("Déploiement Windows 11 Pro").

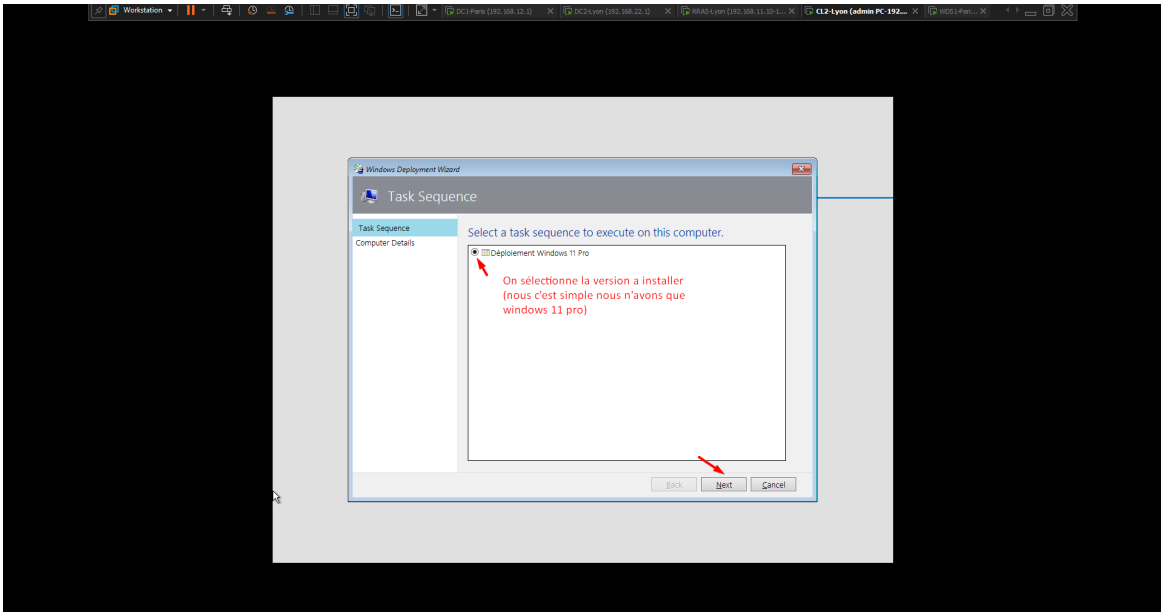

FIGURE 110 – Choix de la séquence de tâches à exécuter

9.13 Nommage de l'ordinateur

L'assistant nous demande de nommer l'ordinateur. Nous saisissons `CL2`. (Il est possible d'automatiser cette étape).

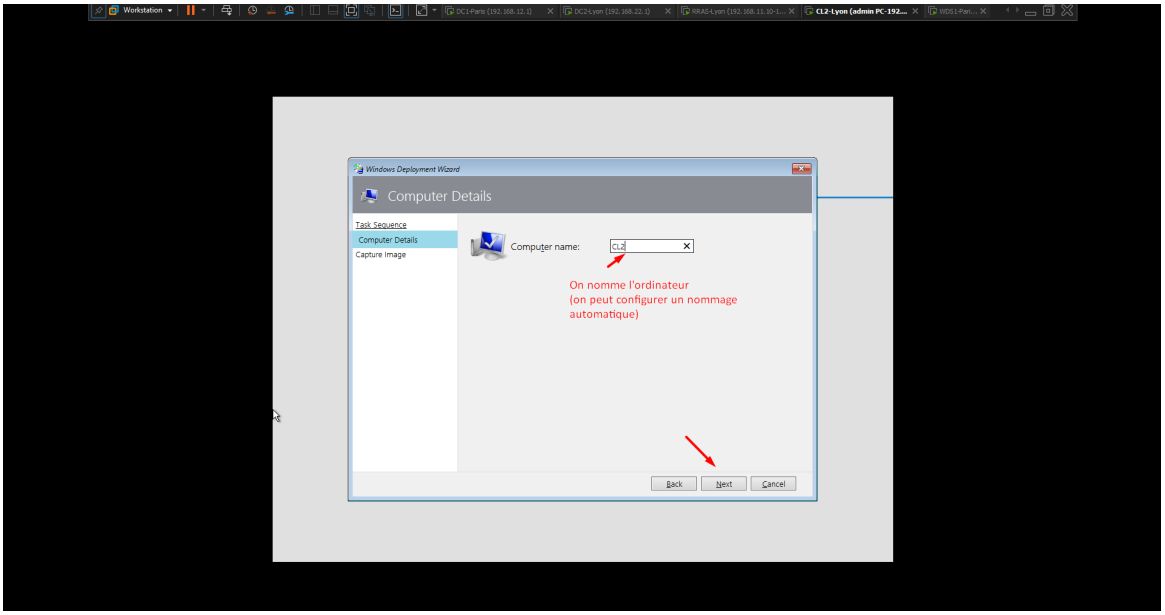

FIGURE 111 – Définition manuelle du nom d'hôte de la machine

9.14 Automatisation via les Rules (Optionnel)

Pour éviter d'avoir à saisir le nom manuellement à l'avenir, nous pouvons retourner dans les propriétés du Deployment Share (onglet Rules) et ajouter les lignes `OSDComputerName=CL%SerialNumber%` et `SkipComputerName=YES`.

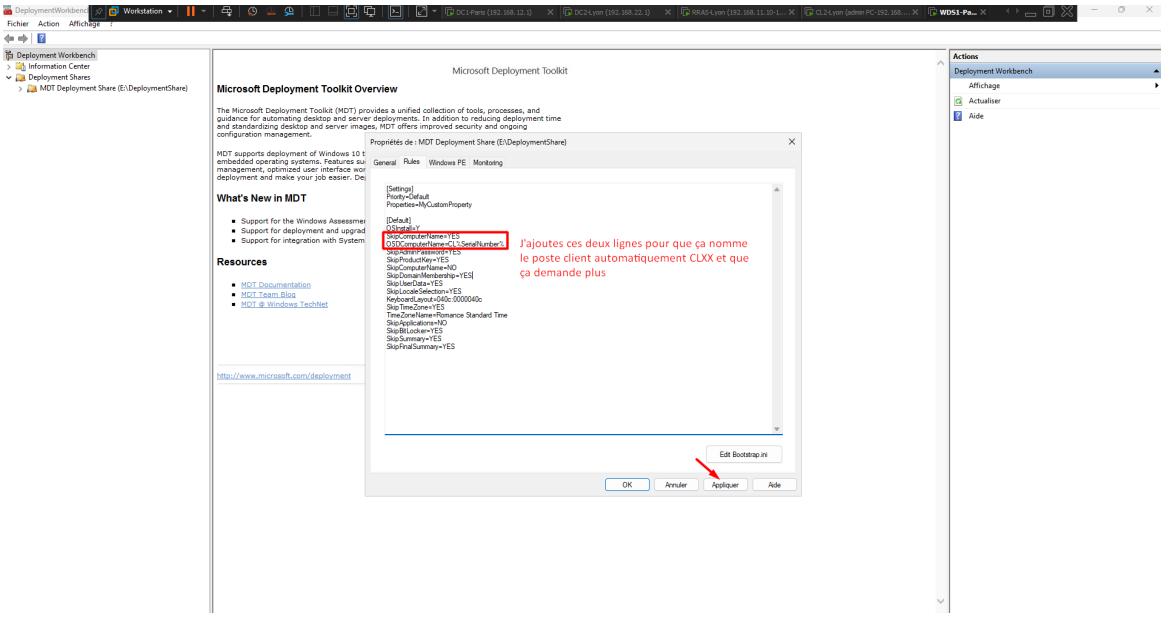

FIGURE 112 – Ajout de règles d'automatisation pour le nommage des postes

9.15 Déploiement en cours

L'installation est lancée avec succès. Le formatage, le partitionnement UEFI et la copie des fichiers s'effectuent via le réseau.

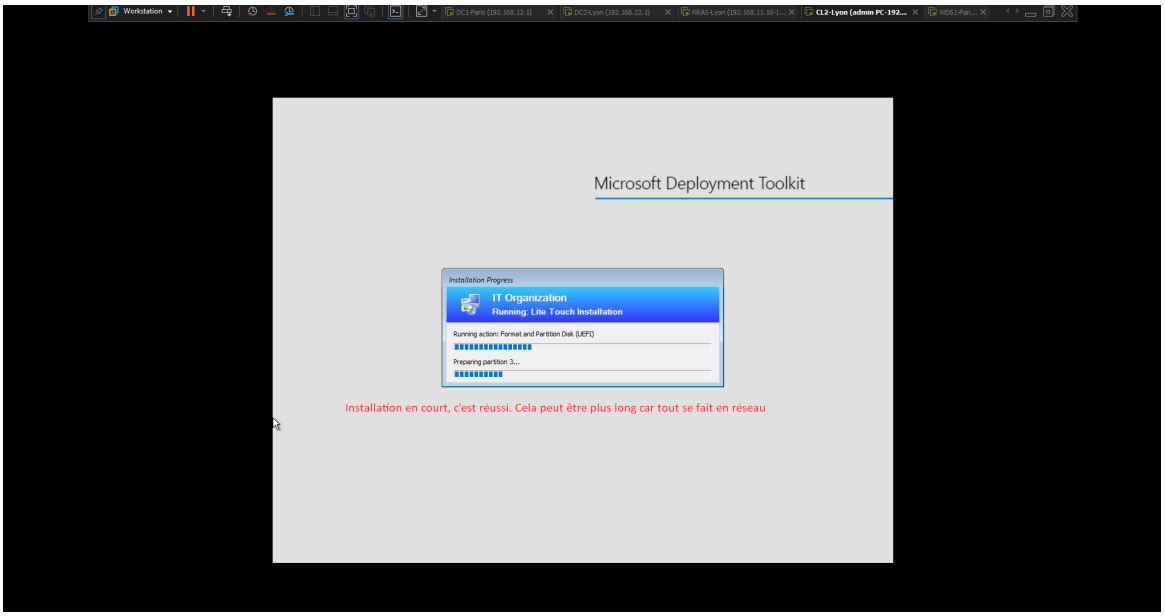

FIGURE 113 – Progression de l'installation automatisée sur le client

10 MISE EN PLACE DU SERVEUR DE MANAGEMENT (MGMT1)

10.1 Présentation et rôle de MGMT1

Nous passons à la configuration du serveur `MGMT1` (192.168.12.4). Son rôle sera de centraliser la distribution des mises à jour (WSUS), la collecte des journaux d'événements (WEF) et la gestion de l'adressage IP (IPAM).

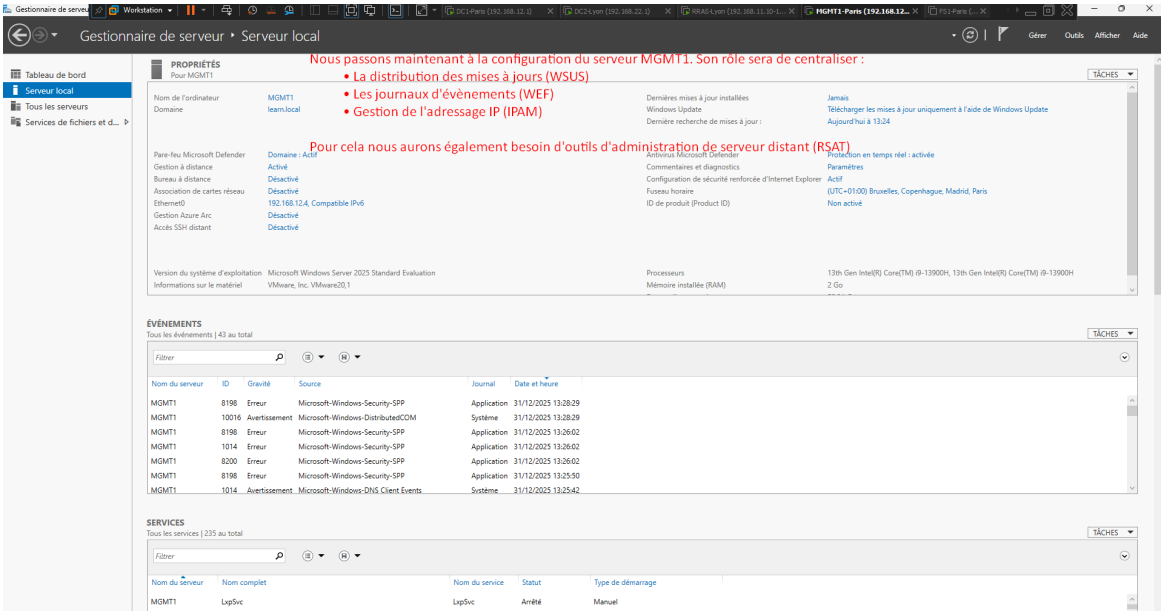

FIGURE 114 – Tableau de bord et propriétés du serveur MGMT1

10.2 Installation des outils RSAT

Pour gérer notre infrastructure à distance depuis ce serveur, nous lançons l'assistant d'ajout de rôles et fonctionnalités. Dans la partie "Fonctionnalités", nous cochons les "Outils d'administration de serveur distant" (RSAT), notamment pour AD DS, DNS et DHCP.

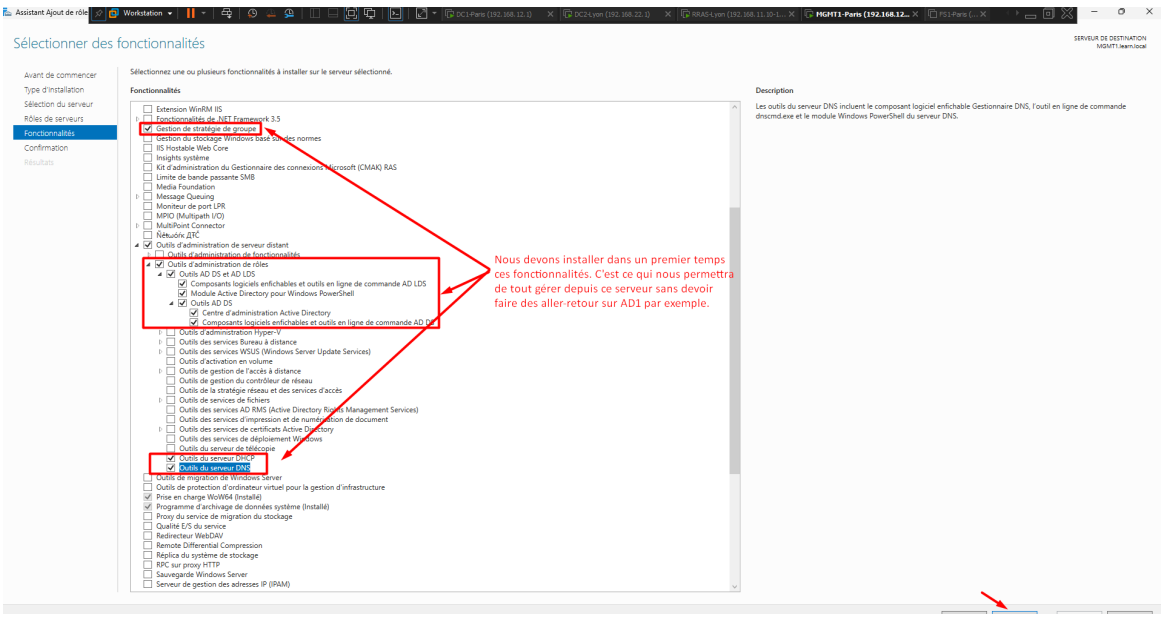

FIGURE 115 – Sélection des outils d'administration distants (RSAT)

10.3 Sélection du rôle WSUS

Toujours dans le même assistant, dans la section "Rôles", nous cochons "Services WSUS (Windows Server Update Services)".

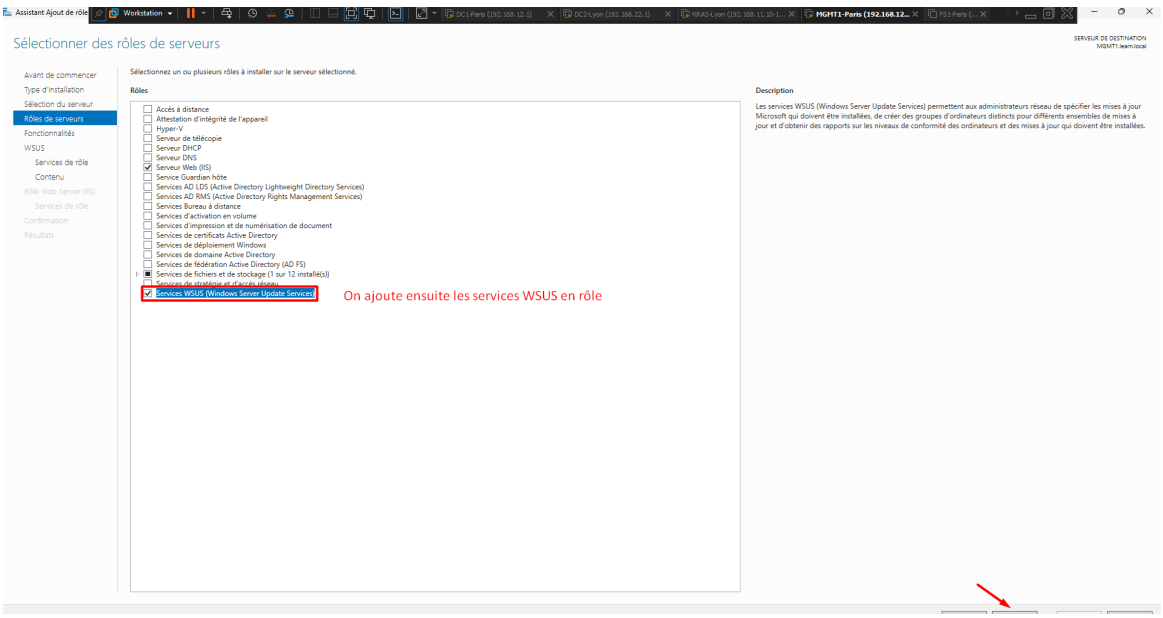

FIGURE 116 – Sélection du rôle de gestion des mises à jour (WSUS)

10.4 Sélection de la fonctionnalité IPAM

De retour dans la section "Fonctionnalités", nous sélectionnons également "Serveur de gestion des adresses IP (IPAM)". Note : Pour le service WEF (Windows Event Forwarding), il n'y a rien à installer, la fonctionnalité est native, il suffira de la configurer plus tard.

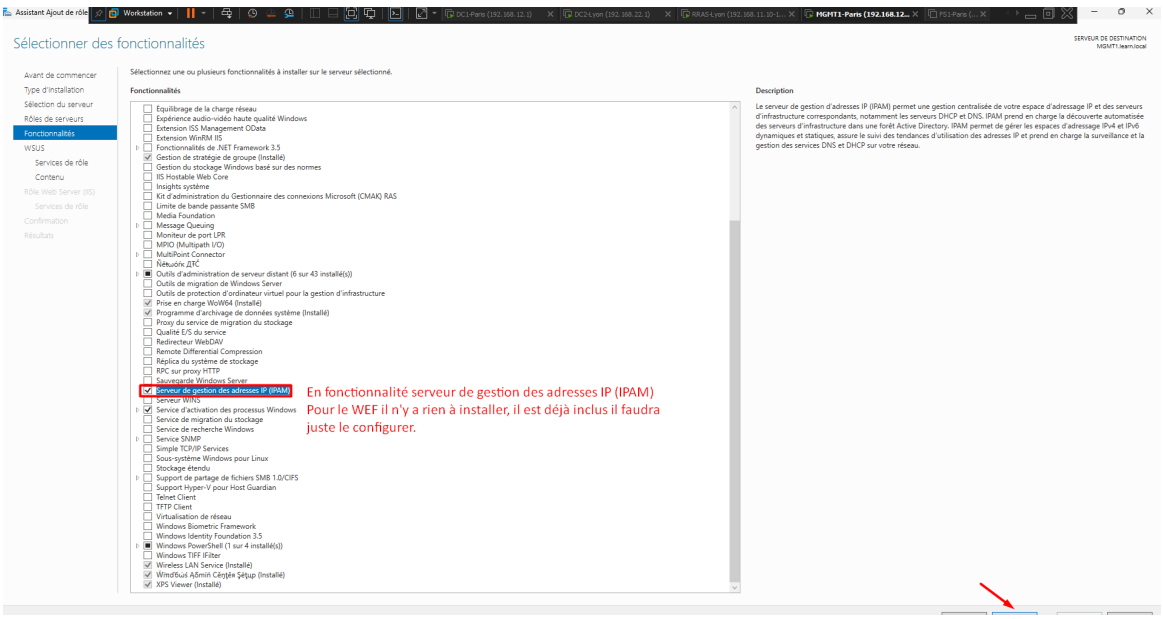

FIGURE 117 – Sélection de la fonctionnalité de gestion IPAM

10.5 Services de rôle WSUS (WID Connectivity)

Lors de la configuration spécifique du rôle WSUS, nous sélectionnons les services "WID Connectivity" et "WSUS Services". Cela installera une base de données interne (Windows Internal Database) dédiée à WSUS.

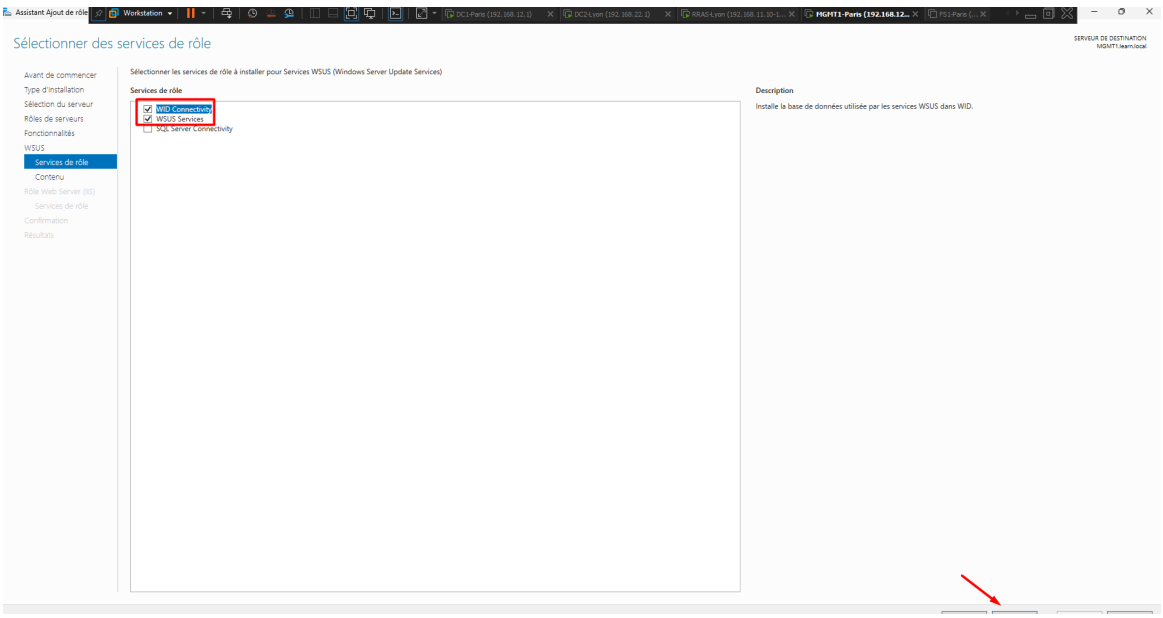

FIGURE 118 – Sélection de la connectivité WID pour WSUS

10.6 Emplacement du contenu WSUS

L'assistant nous demande où stocker physiquement les mises à jour qui seront distribuées au parc informatique. Nous indiquons le chemin local `C:\WSUS` (ce dossier doit être créé en amont et disposer de suffisamment d'espace disque).

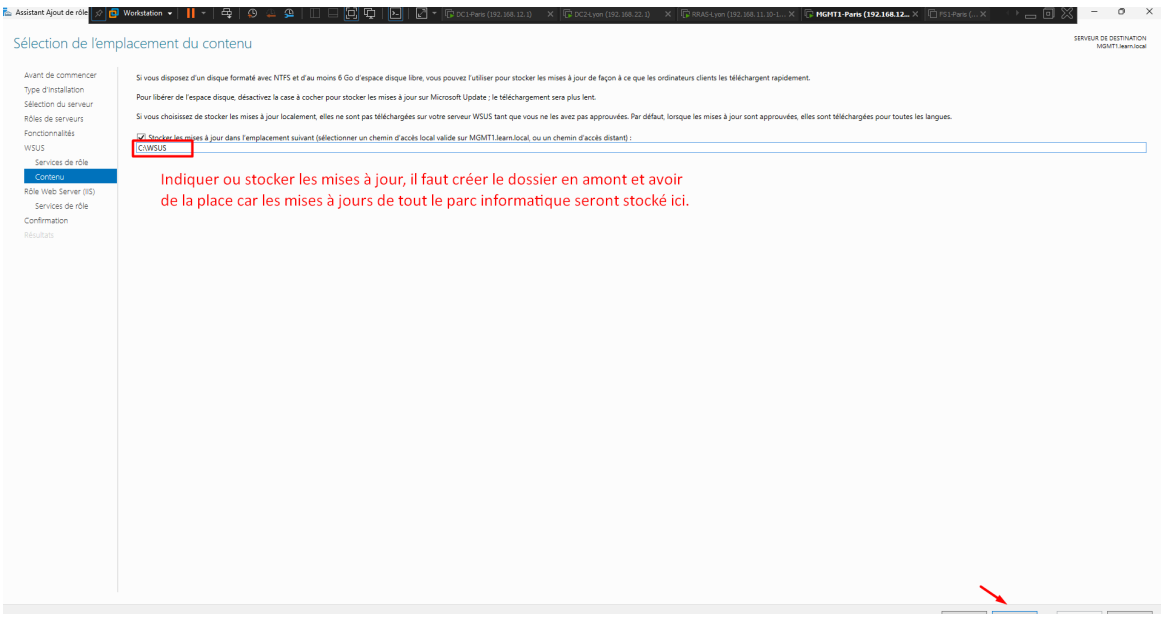

FIGURE 119 – Spécification du répertoire local de stockage des mises à jour

10.7 Tableau de bord après installation

Nous allons maintenant configurer l'IPAM. Sur le tableau de bord de MGMT1, on constate que les rôles IIS, IPAM et WSUS sont bien installés et présents dans le menu.

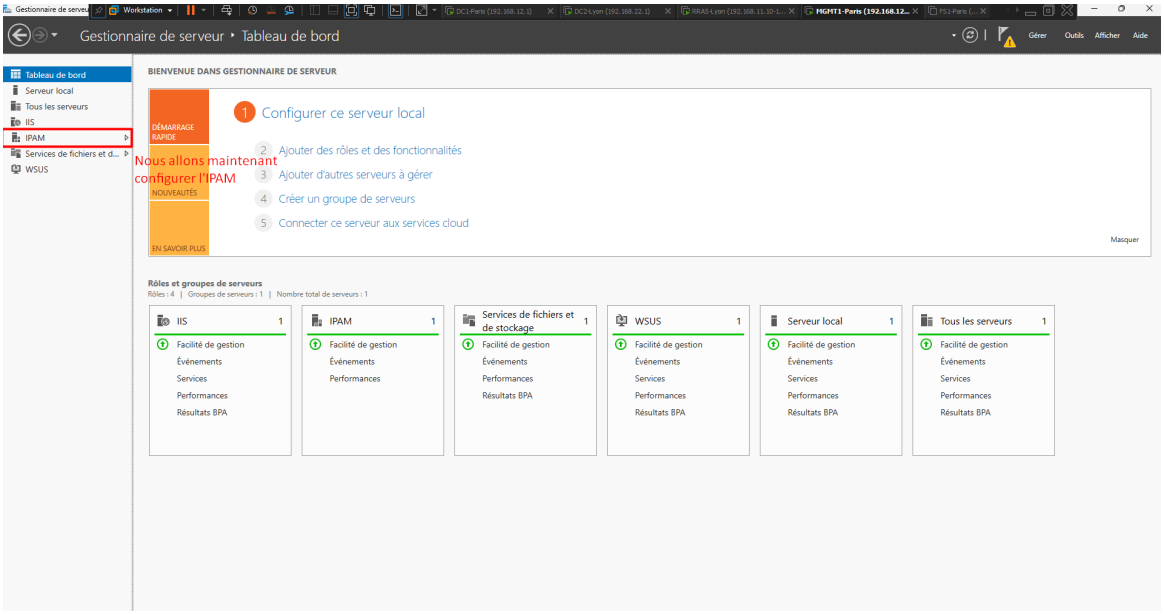

FIGURE 120 – Le tableau de bord de MGMT1 avec les nouveaux rôles

10.8 Vue d'ensemble IPAM

Nous cliquons sur IPAM à gauche. Dans la vue d'ensemble, on observe que l'étape 1 "Se connecter au serveur IPAM" est déjà validée (connecté en tant qu'administrateur LEARN).

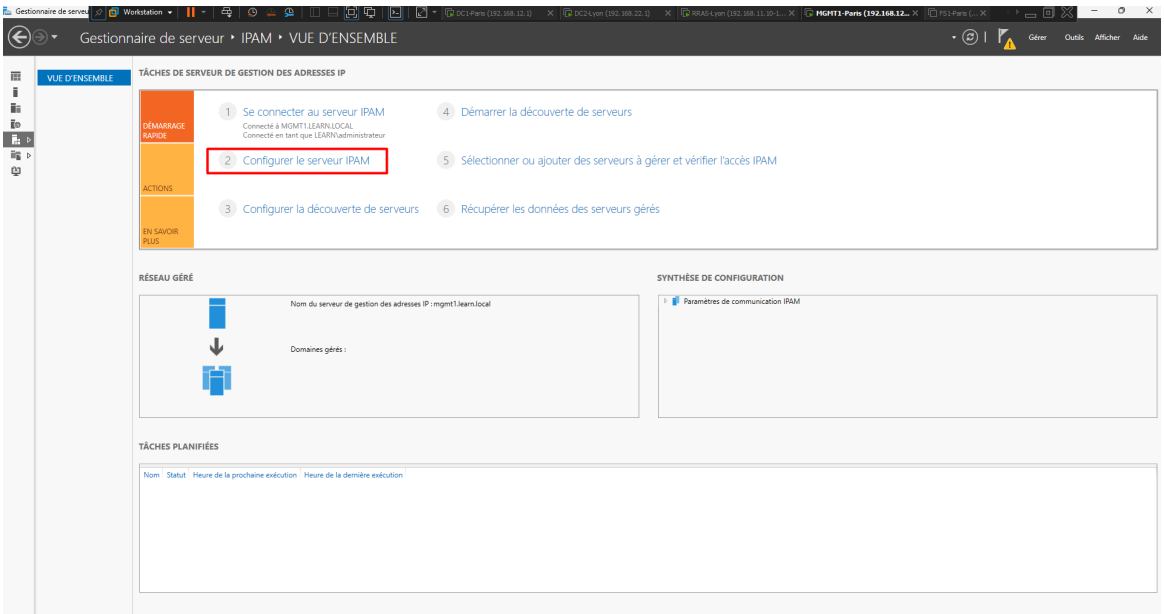

FIGURE 121 – Interface de vue d'ensemble pour la configuration d'IPAM

10.9 Approvisionnement de la base de données

Nous passons à l'étape 2 "Configurer le serveur IPAM". L'assistant nous demande de spécifier le type de base de données. Nous laissons l'option par défaut "Base de données interne Windows (WID)" et son chemin d'installation.

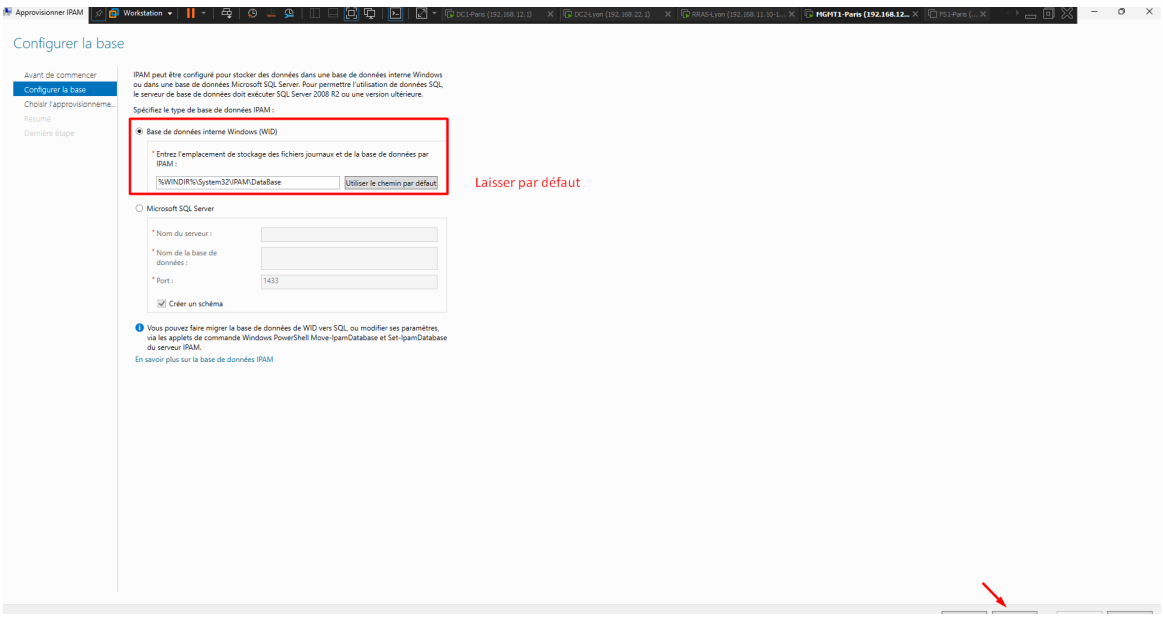

FIGURE 122 – Sélection de la base de données interne WID

10.10 Méthode d'approvisionnement (GPO)

À l'étape "Choisir l'approvisionnement", nous sélectionnons la méthode "Basée sur une stratégie de groupe". Nous allons configurer cela avec une GPO que l'on nomme avec un nom court et identifiable, on saisit donc le préfixe `IPAM`.

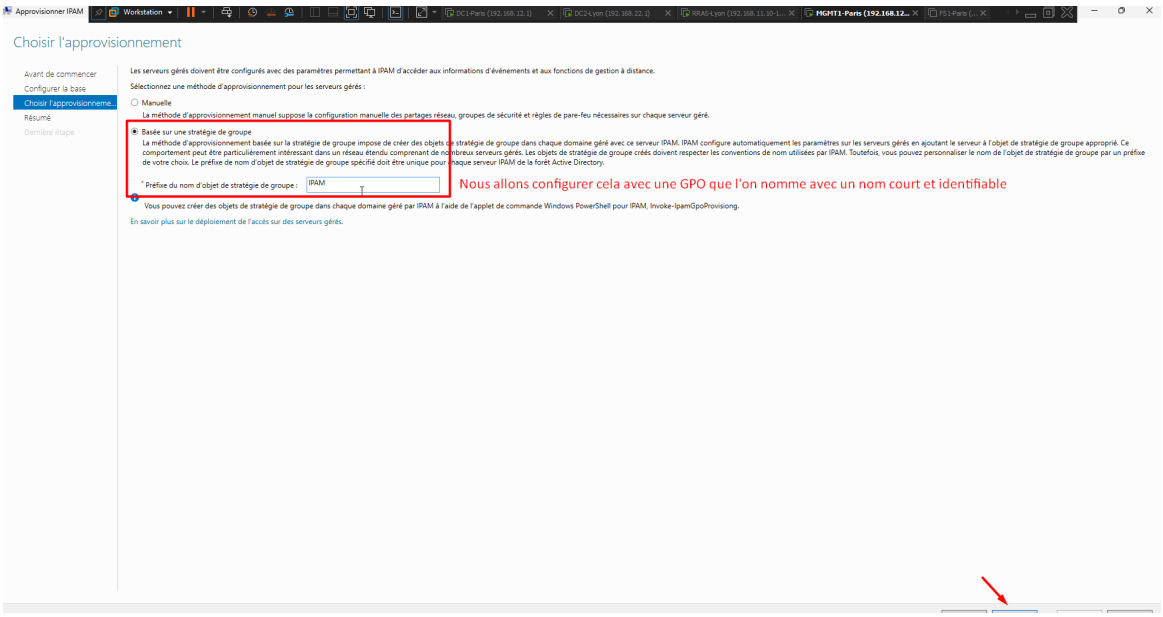

FIGURE 123 – Choix de l'approvisionnement par GPO et définition du préfixe

10.11 Validation de l'approvisionnement IPAM

La dernière étape confirme que les paramètres ont été correctement approvisionnés. C'est presque bon, il faut maintenant lancer une commande PowerShell en administrateur pour créer physiquement ces GPO dans le domaine.

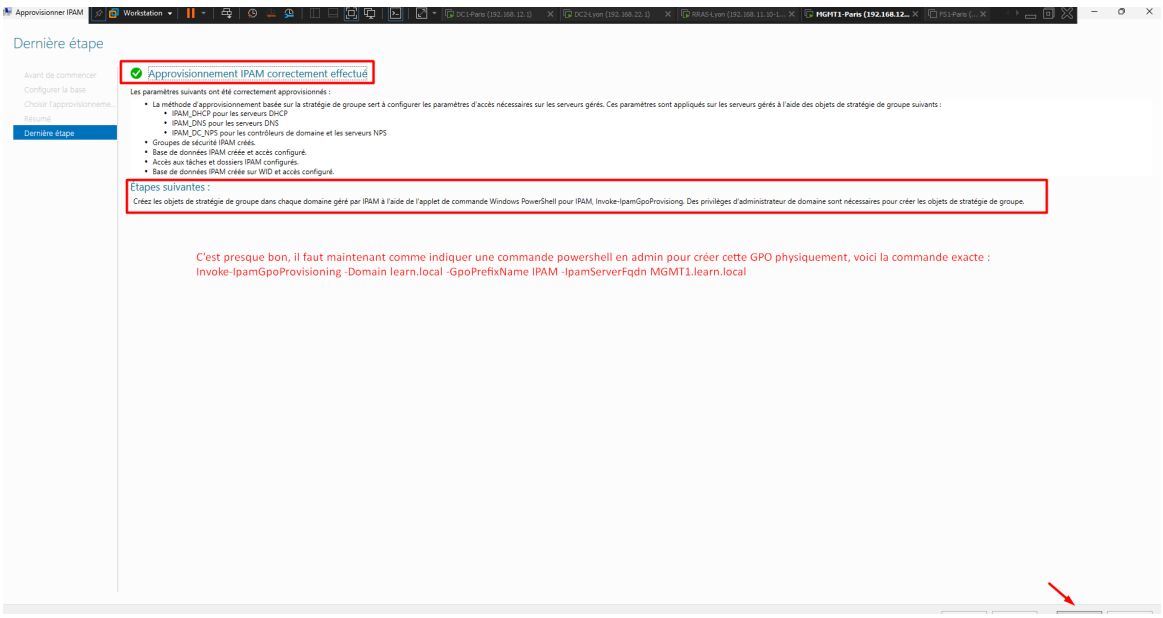

FIGURE 124 – Confirmation de l'approvisionnement et consigne PowerShell

10.12 Exécution du script de provisionnement (PowerShell)

Dans une console PowerShell (en administrateur), nous tapons la commande exacte : `Invoke-IpamGpoProvisioning -Domain learn.local -GpoPrefixName IPAM -IpamServerFqdn MGMT1.learn.local`. Nous validons les messages d'avertissement en tapant "O" (Oui).

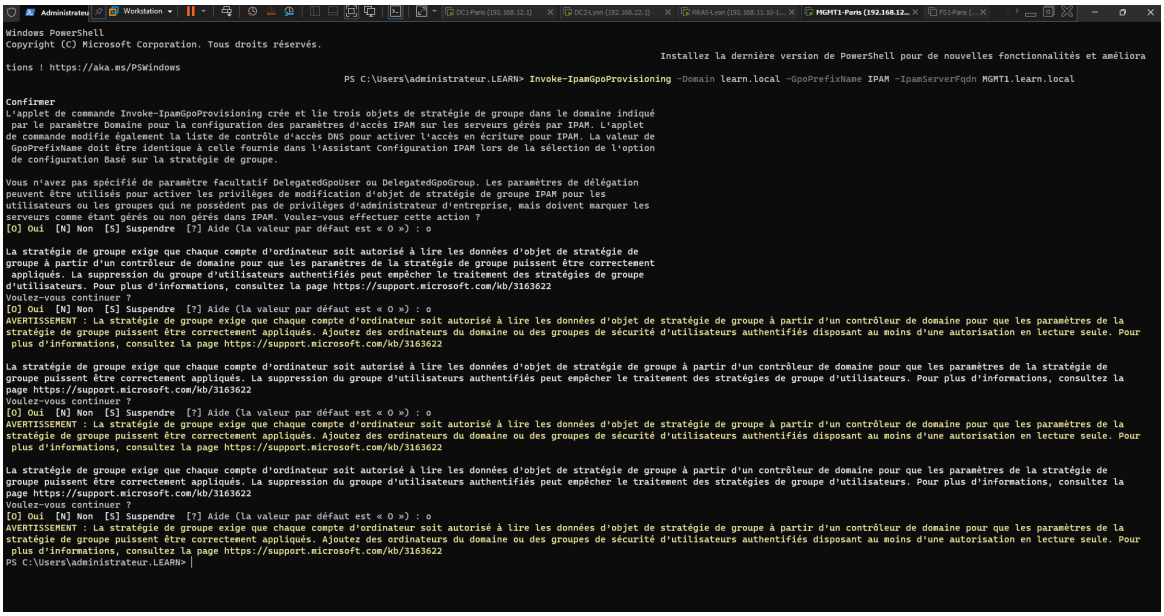

FIGURE 125 – Création des GPO IPAM via l'applet de commande PowerShell

10.13 Configurer la découverte de serveurs

De retour dans la vue d'ensemble d'IPAM, l'étape 2 est maintenant marquée comme terminée. Nous cliquons sur l'étape 3 : "Configurer la découverte de serveurs".

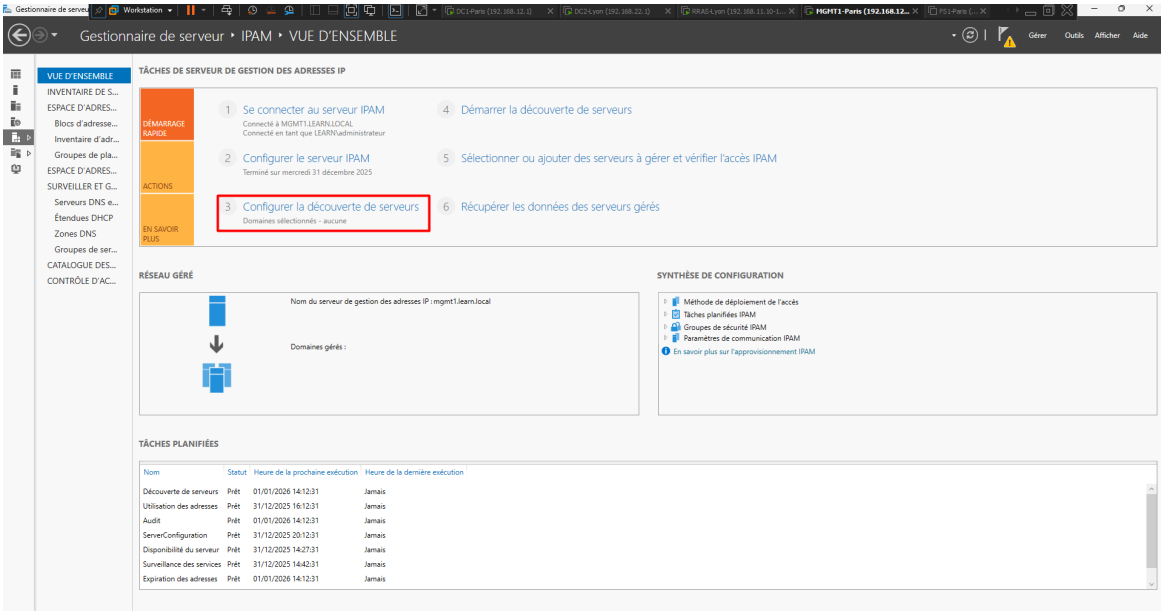

FIGURE 126 – Avancement des tâches de configuration IPAM

10.14 Sélection du domaine à découvrir

Dans la fenêtre, nous sélectionnons la forêt, puis nous cliquons sur "Ajouter" pour inclure notre domaine `learn.local`. Nous laissons cochés les rôles à découvrir (Contrôleur de domaine, Serveur DHCP, Serveur DNS).

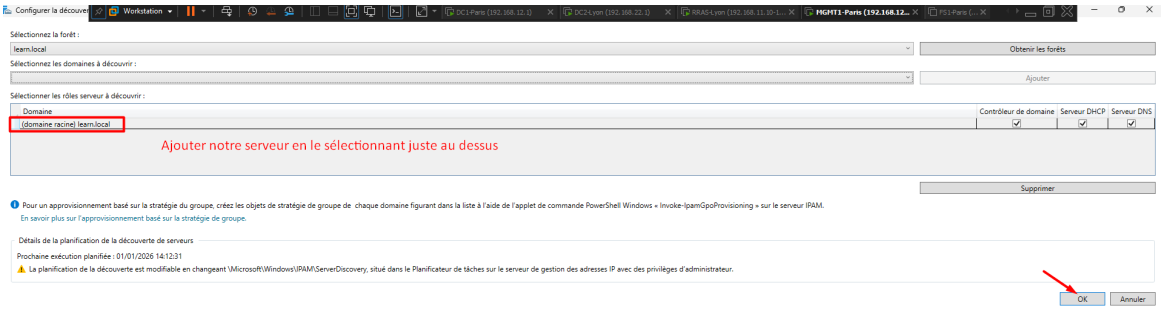

FIGURE 127 – Ajout du domaine learn.local à la liste de découverte

10.15 Lancement de la découverte de serveurs

Nous cliquons ensuite sur l'étape 4 : "Démarrer la découverte de serveurs". Une tâche planifiée se lance en arrière-plan pour scanner le réseau à la recherche de nos serveurs.

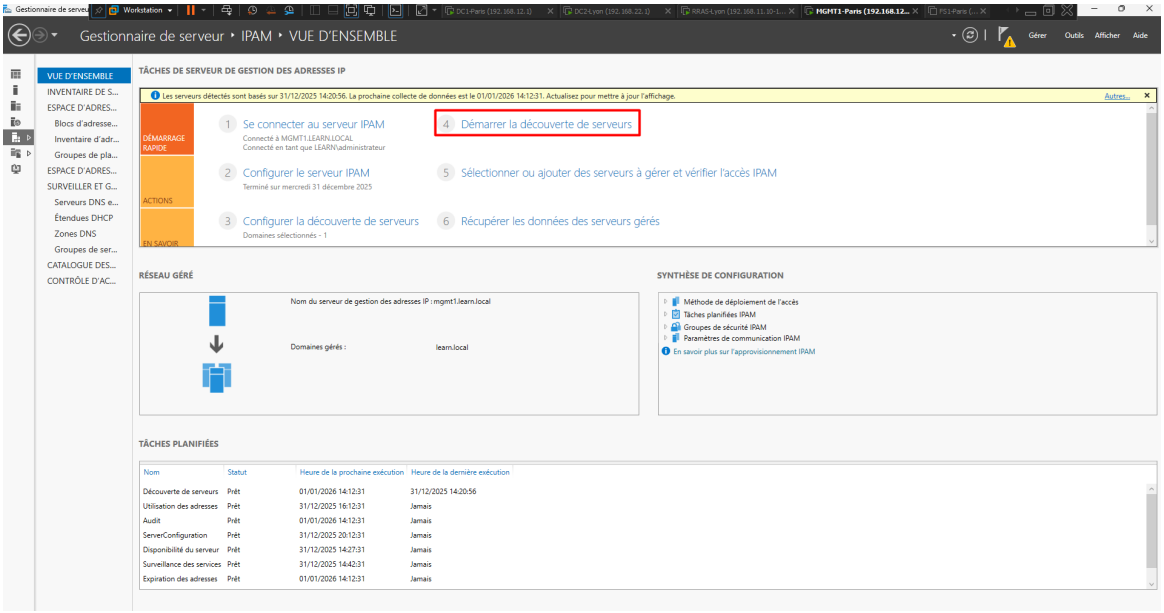

FIGURE 128 – Exécution manuelle de la tâche de découverte

10.16 Inventaire des serveurs (État initial)

Dans le menu "INVENTAIRE DE SERVEUR", nous voyons que DC1 et DC2 ont été détectés. Cependant, l'état de l'accès IPAM est "Bloqué" et l'état de gestion est "Non spécifié".

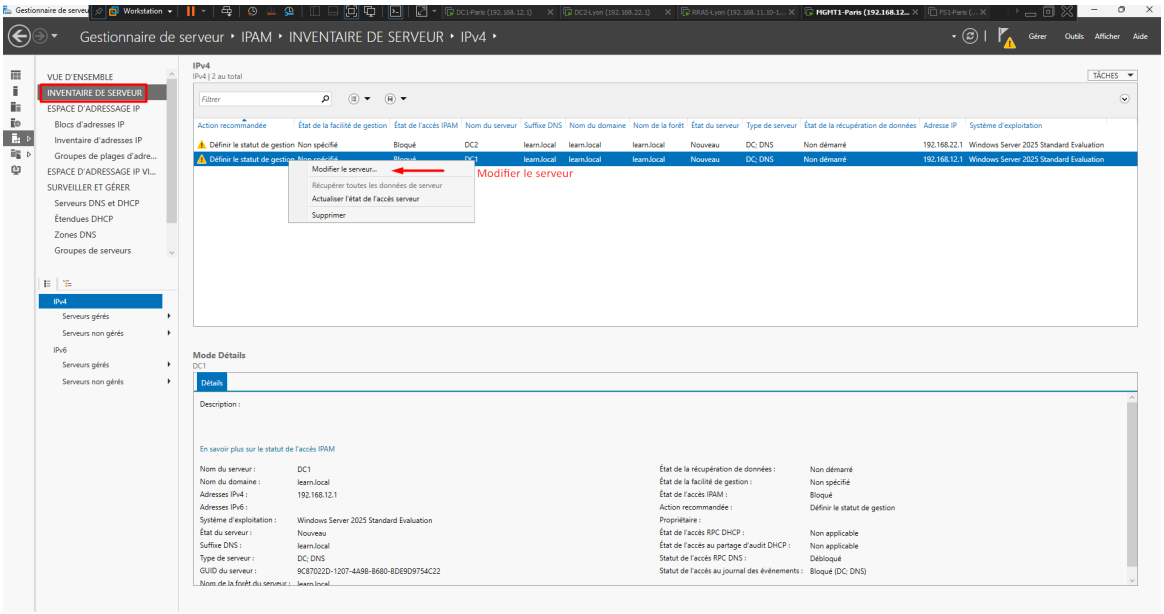

FIGURE 129 – Les serveurs DC1 et DC2 apparaissent dans l'inventaire en statut bloqué

10.17 Définition de l'état de gérabilité

On fait un clic-droit sur le serveur DC1 pour le modifier, et on passe l'État de gérabilité sur "Géré". On répète cette même opération pour DC2.

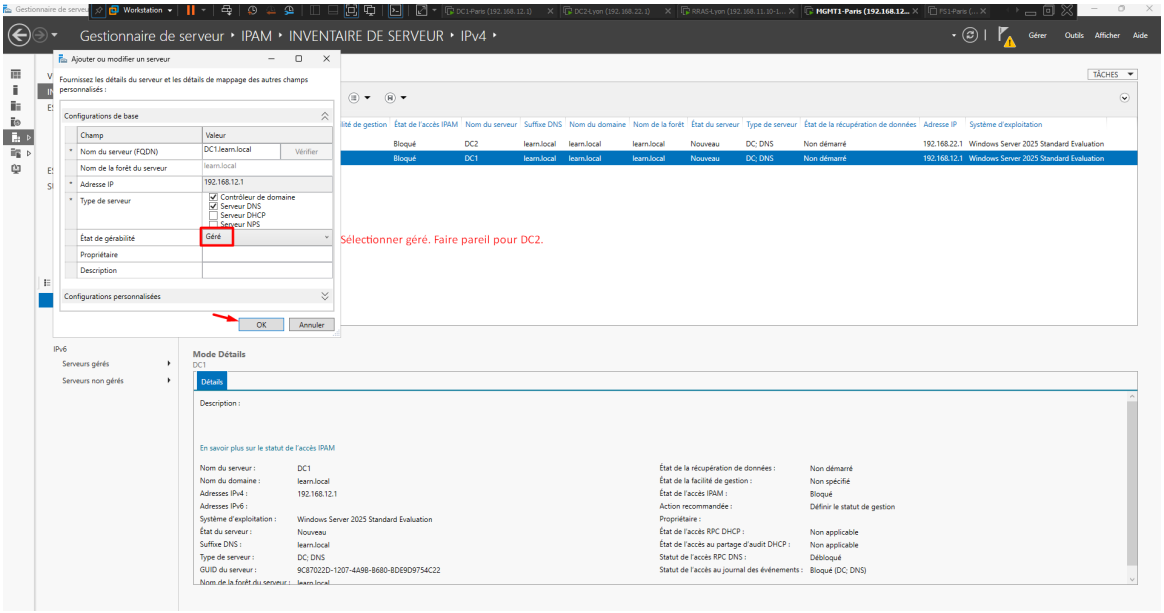

FIGURE 130 – Modification du statut de gestion à "Géré"

10.18 Serveurs DNS et DHCP opérationnels

En allant dans le sous-menu "Serveurs DNS et DHCP", nous pouvons voir que la disponibilité est "En cours d'exécution". Nous pouvons maintenant gérer toute la partie IP depuis l'IPAM (DHCP, DNS...).

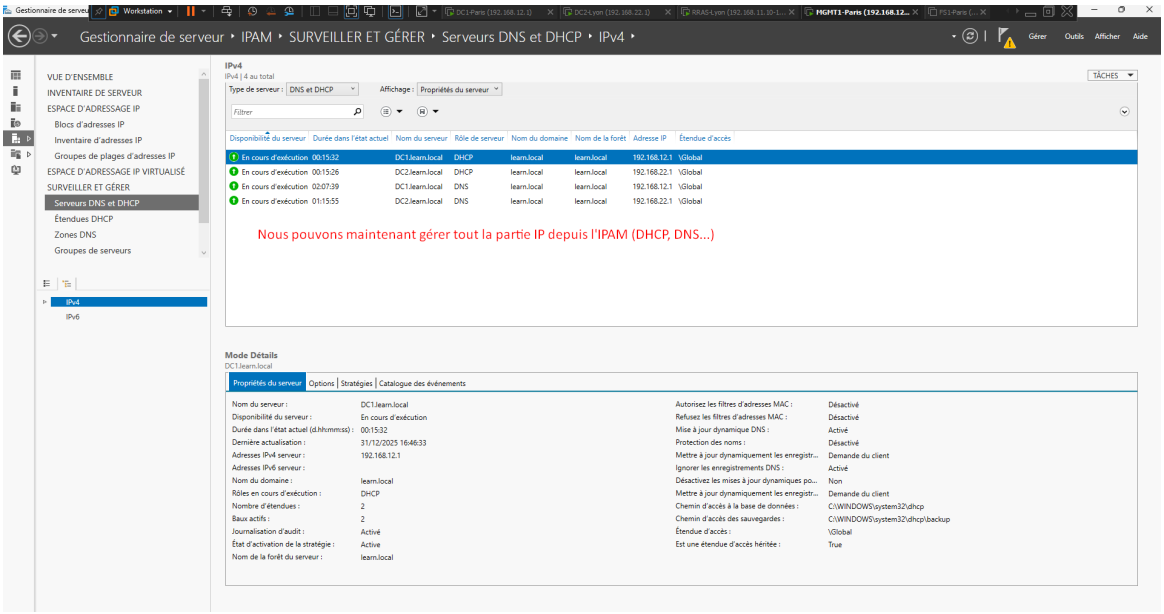

FIGURE 131 – Les services DNS et DHCP remontent correctement dans IPAM

10.19 Analyse de l'anomalie d'accès IPAM

Attention : malgré une remontée fonctionnelle des données DNS et DHCP, la console maintient un état global "Bloqué". Dans le détail, l'erreur est "Statut de l'accès au journal des

événements : Bloqué". Il s'agit d'une problématique liée au durcissement des ACL sur le canal RPC de Windows Server 2025 (détaillée dans les annotations).

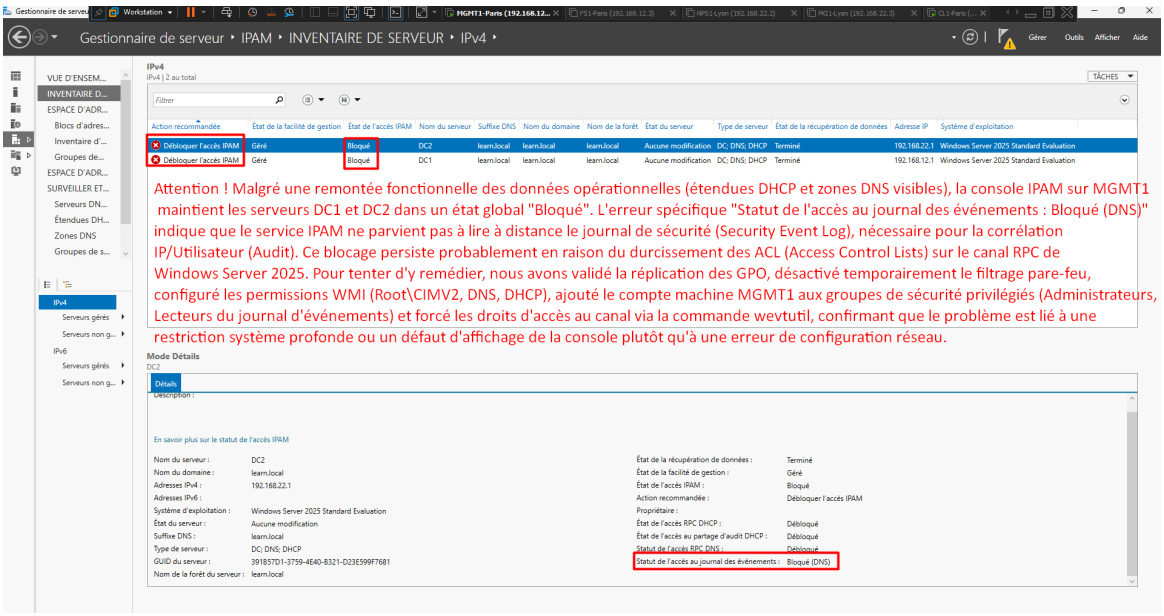

FIGURE 132 – Détail de l'erreur d'accès au journal de sécurité distant

10.20 Lancement des tâches WSUS

Nous passons ensuite à la configuration des mises à jour. Depuis le tableau de bord de MGMT1, nous cliquons sur le drapeau de notification et sélectionnons "Lancer les tâches de post-installation" pour WSUS.

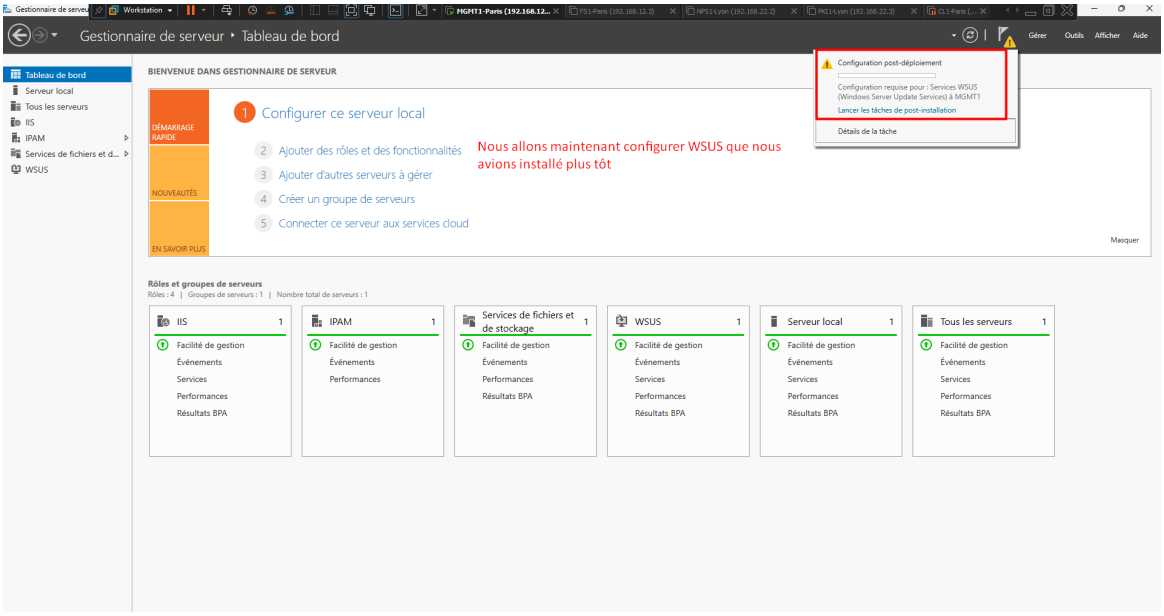

FIGURE 133 – Lancement de la configuration post-déploiement de WSUS

10.21 Ajout d'une carte réseau sur RRAS

Avant de configurer WSUS, nous ajoutons une carte réseau en pont sur la VM du serveur RRAS pour avoir un accès internet (indispensable pour récupérer les mises à jour). On ne met pas cette carte directement sur MGMT1 pour des raisons de sécurité.

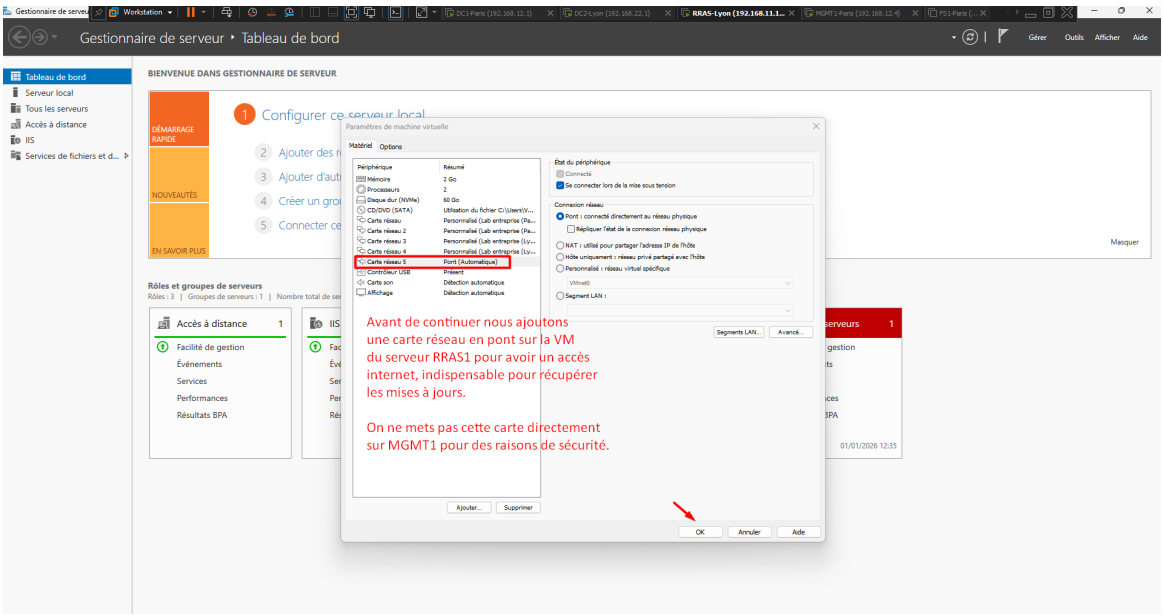

FIGURE 134 – Ajout d'une 5ème carte réseau en mode Pont sur la VM RRAS

10.22 Configuration du protocole NAT

Toujours sur RRAS, dans la console "Routage et accès distant", nous allons ajouter le routage NAT. On fait un clic-droit sur "Général" sous IPv4, puis on sélectionne "Nouveau protocole de routage..." et on choisit NAT.

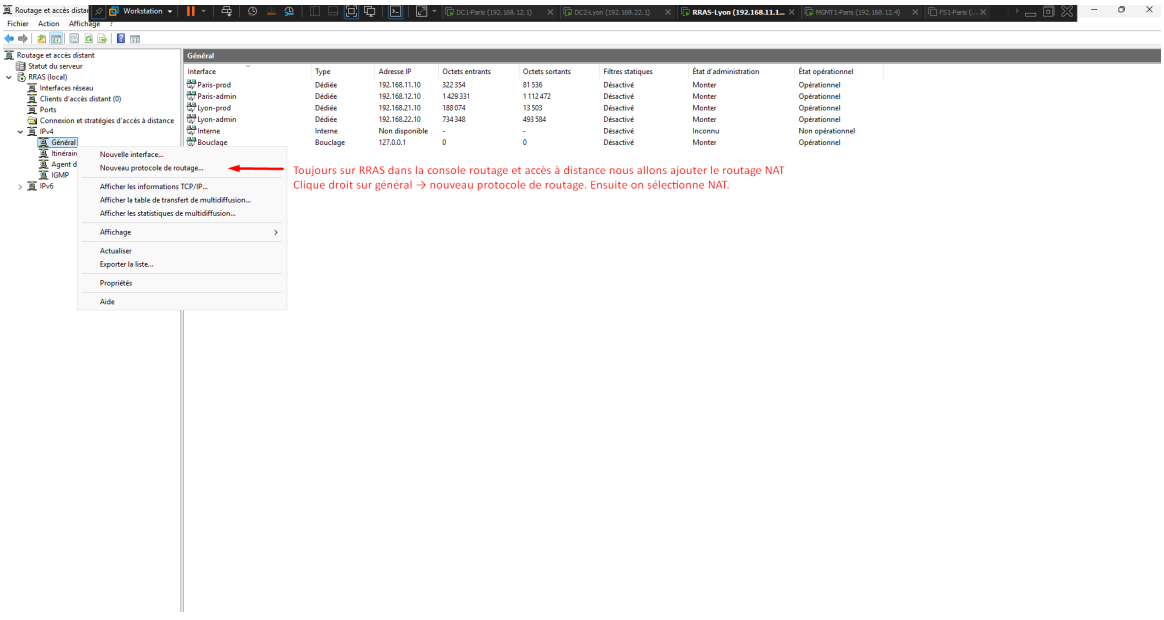

FIGURE 135 – Ajout du protocole de routage NAT sur le RRAS

10.23 Ajout de la carte publique au NAT

Maintenant que le protocole NAT est présent, nous allons lui ajouter la carte réseau dédiée à Internet. Clic-droit sur NAT > Nouvelle interface, on sélectionne notre carte, en cochant bien la case pour activer le NAT et en spécifiant qu'il s'agit de l'interface publique.

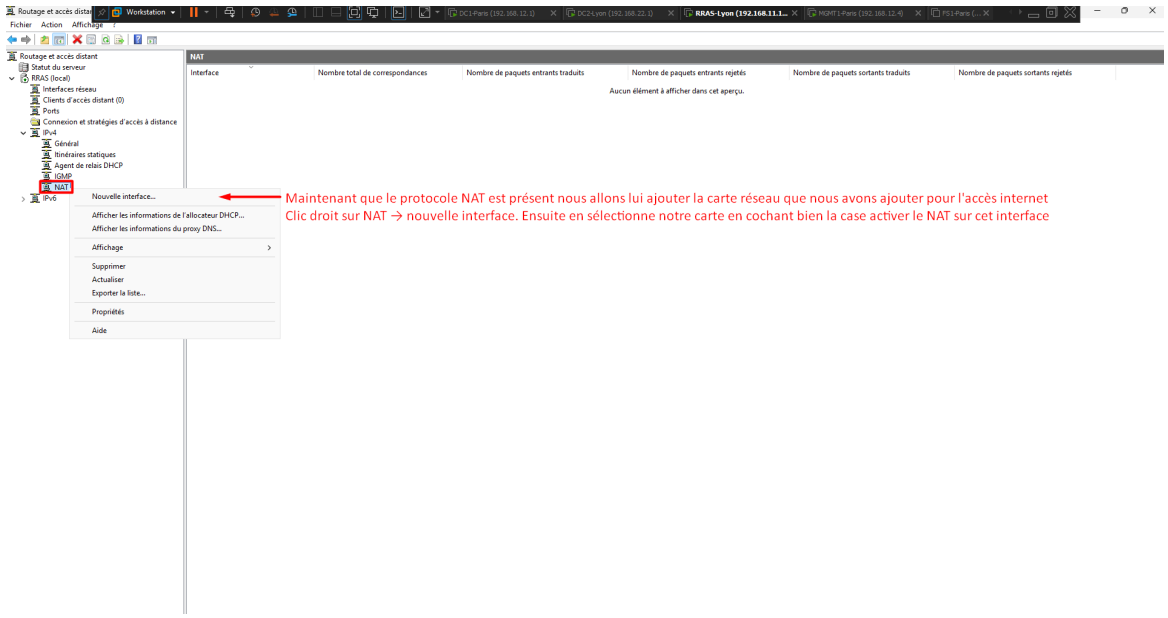

FIGURE 136 – Liaison de l'interface publique au protocole NAT

10.24 Test d'accès Internet depuis MGMT1

MGMT1 a bien accès à Internet maintenant (toutes les autres machines du réseau d'ailleurs, mais en passant par le RRAS d'abord). On le vérifie en faisant un ping vers `8.8.8.8`.

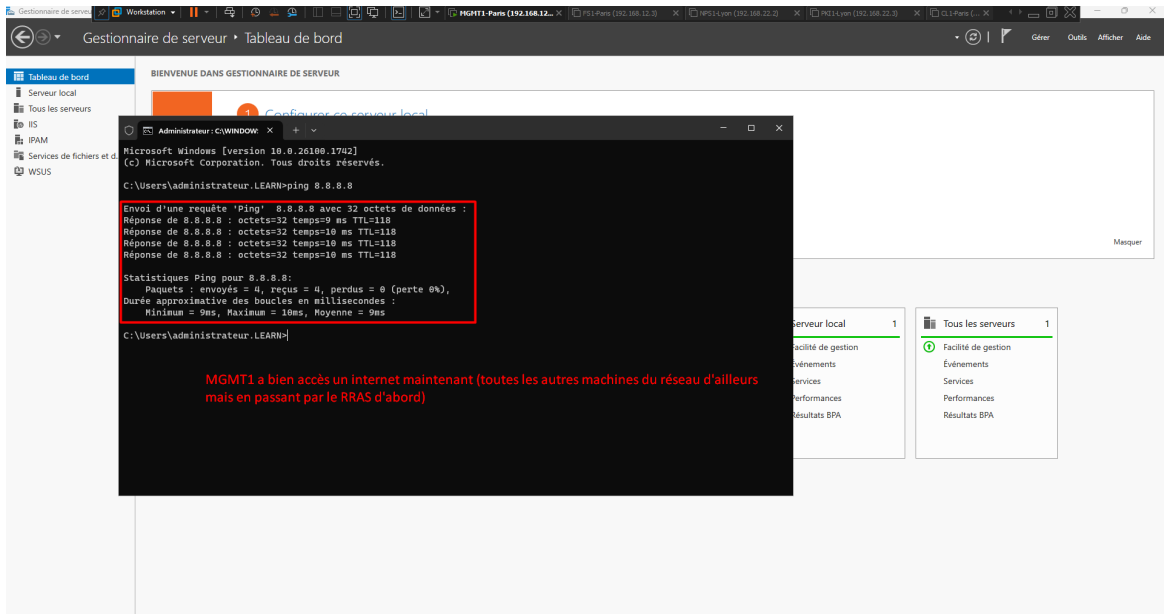

FIGURE 137 – Ping réussi vers Internet depuis le serveur MGMT1

10.25 Serveur en amont (WSUS)

L'assistant de configuration WSUS s'est ouvert. À l'étape "Choisir le serveur en amont", on laisse la sélection par défaut : "Synchroniser à partir de Microsoft Update".

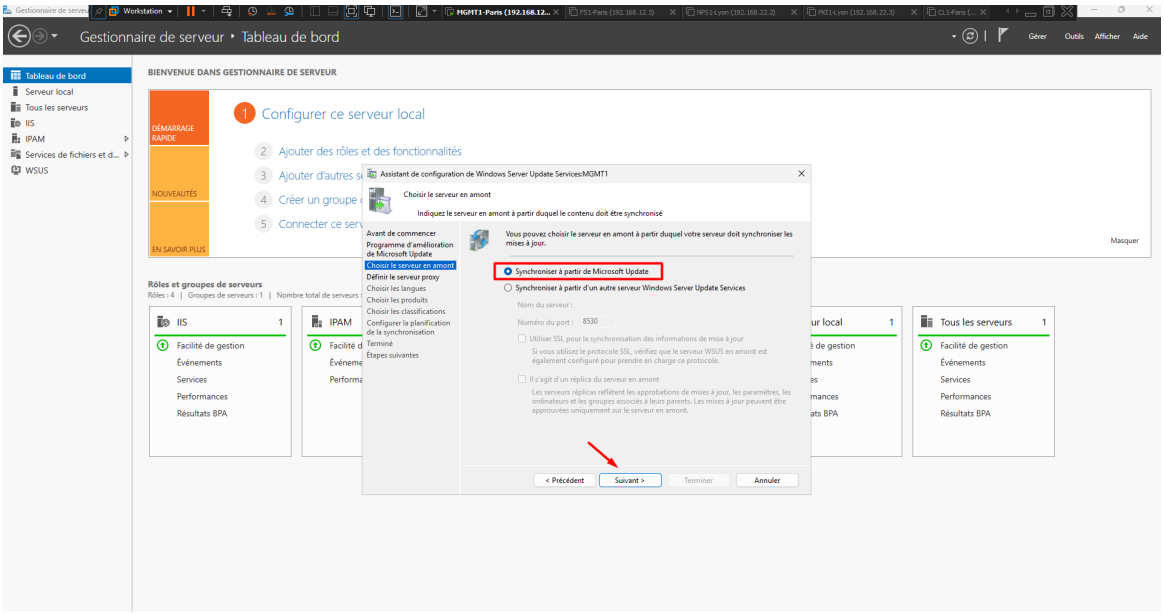

FIGURE 138 – Sélection de la source de synchronisation WSUS

10.26 Lancement de la connexion initiale

On clique sur "Démarrer la connexion". Ça peut prendre plus de 10 minutes car le serveur télécharge toutes les informations sur le catalogue des produits Microsoft.

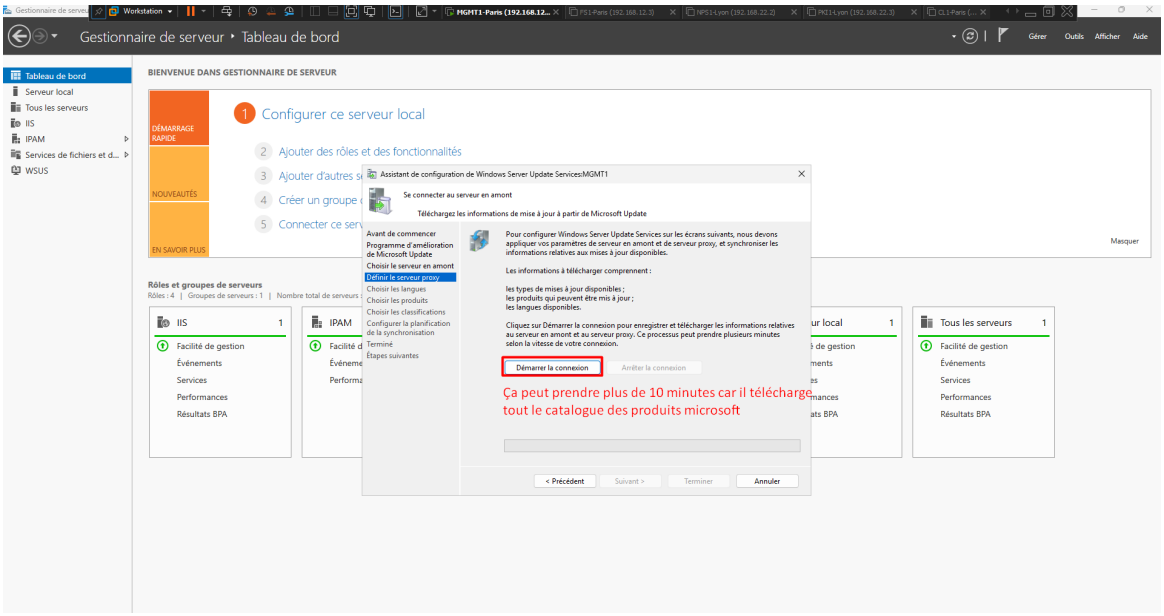

FIGURE 139 – Démarrage de la connexion initiale avec Microsoft Update

10.27 Connexion au serveur en amont (WSUS)

La connexion initiale aux serveurs de Microsoft Update est en cours. Ce processus permet de récupérer la liste des langues et produits disponibles avant de choisir ce que l'on souhaite télécharger.

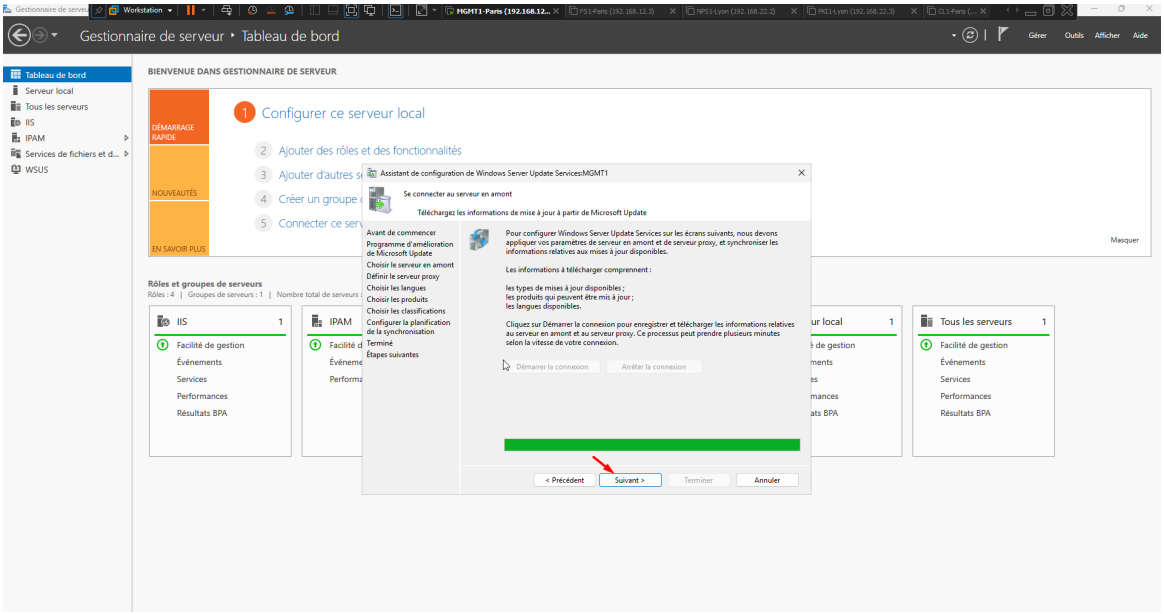

FIGURE 140 – Téléchargement des informations depuis Microsoft Update

10.28 Choix des langues des mises à jour

Une fois la connexion établie, l'assistant nous demande quelles langues télécharger. Pour optimiser l'espace de stockage de notre lab, nous cochons "Télécharger les mises à jour dans ces langues uniquement" et nous sélectionnons uniquement l'Anglais et le Français.

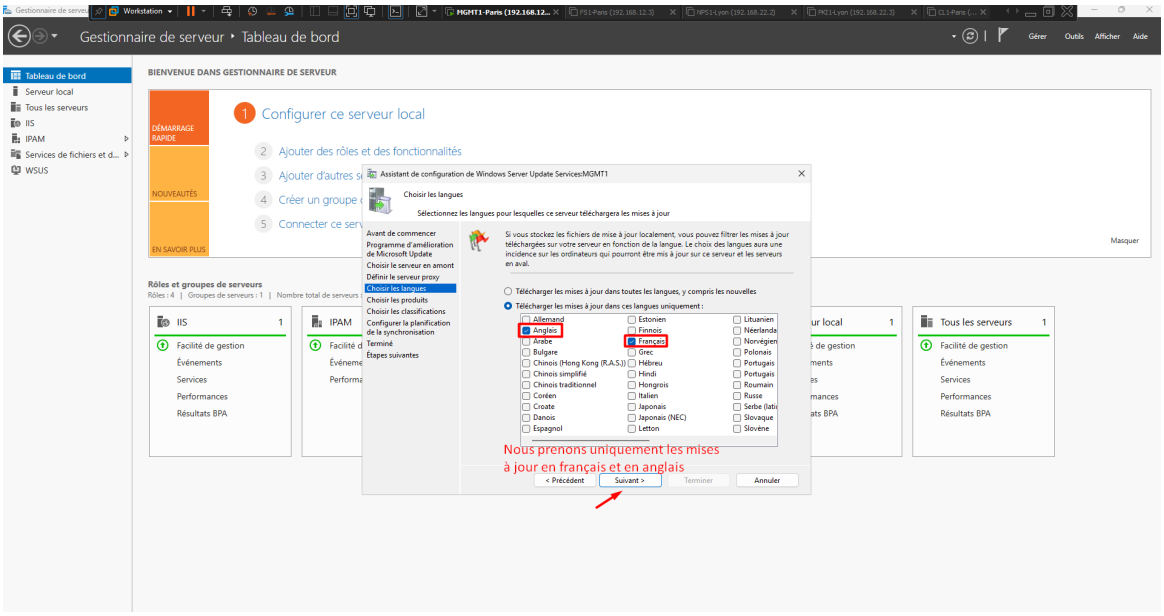

FIGURE 141 – Sélection restreinte aux langues Anglais et Français

10.29 Fin de la configuration et synchronisation WSUS

Nous terminons l'assistant (en sélectionnant les produits Windows 11 / Server 2025 et les classifications de sécurité). La console WSUS s'ouvre sur le serveur MGMT1. Une fois la configuration finie, WSUS va chercher qui a besoin de quelle mise à jour et les télécharger. Il n'y a plus qu'à laisser faire.

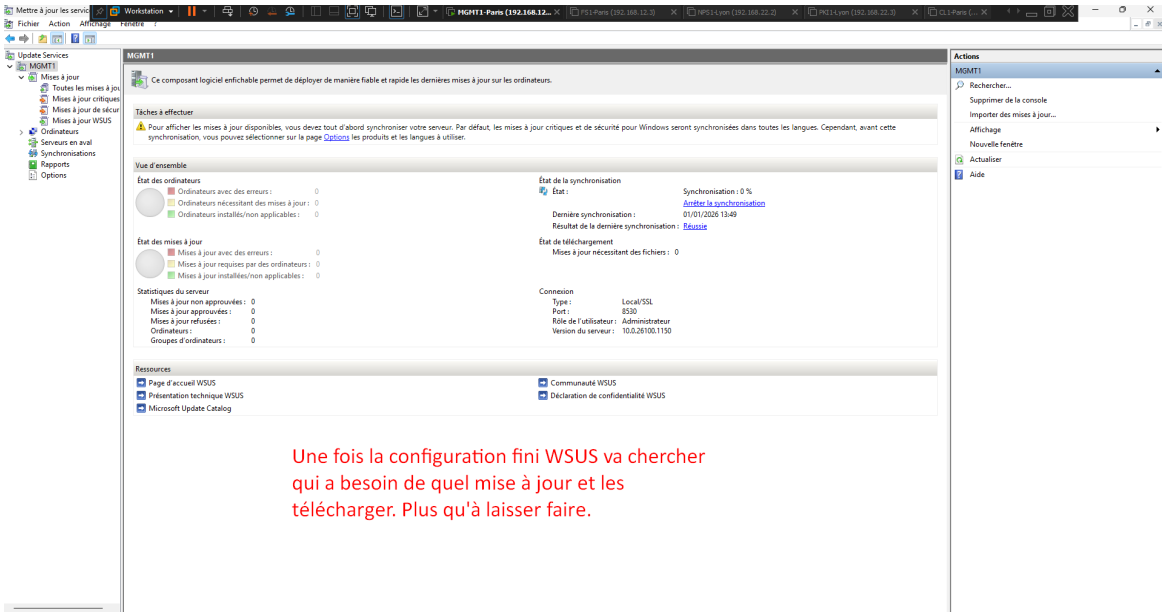

FIGURE 142 – Console d'administration de Windows Server Update Services

11 CENTRALISATION DES JOURNAUX D'ÉVÉNEMENTS (WEF)

11.1 Activation du service WEF sur MGMT1

Nous allons configurer MGMT1 pour qu'il centralise tous les journaux (logs) de l'infrastructure. Dans une invite PowerShell en tant qu'administrateur, nous exécutons la commande `wecutil qc` pour configurer le service de collecte, et nous validons par `O` (Oui).

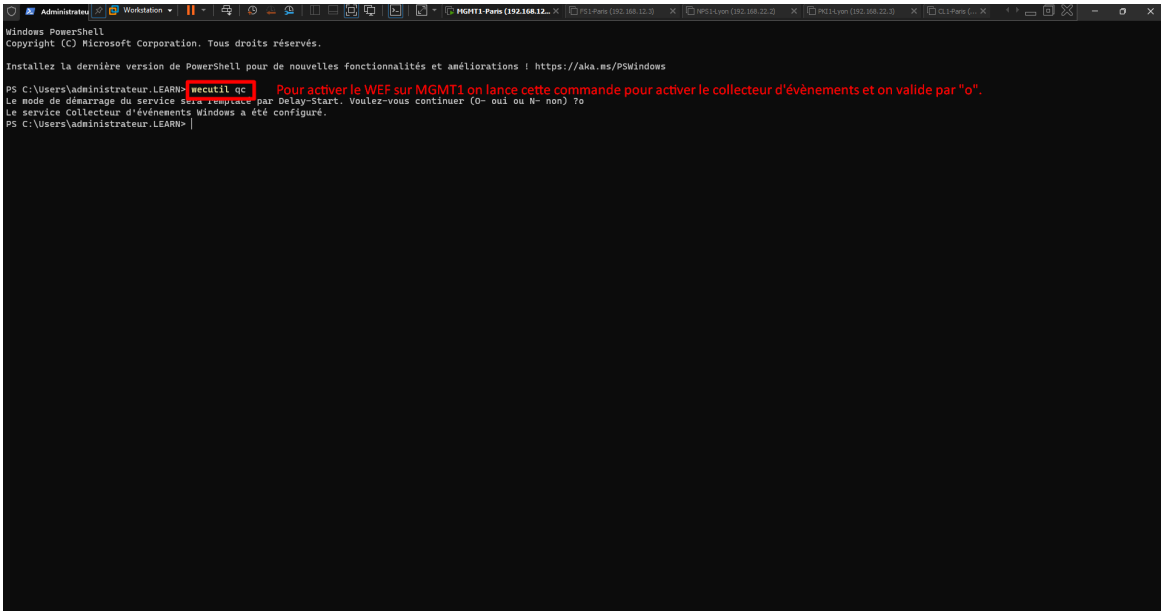

FIGURE 143 – Activation du collecteur d'événements via la commande wecutil qc

11.2 Lancement de la création d'un abonnement

Toujours sur MGMT1, nous ouvrons la console "Observateur d'événements". Nous effectuons un clic-droit sur le dossier "Abonnements" et sélectionnons "Créer un abonnement...".

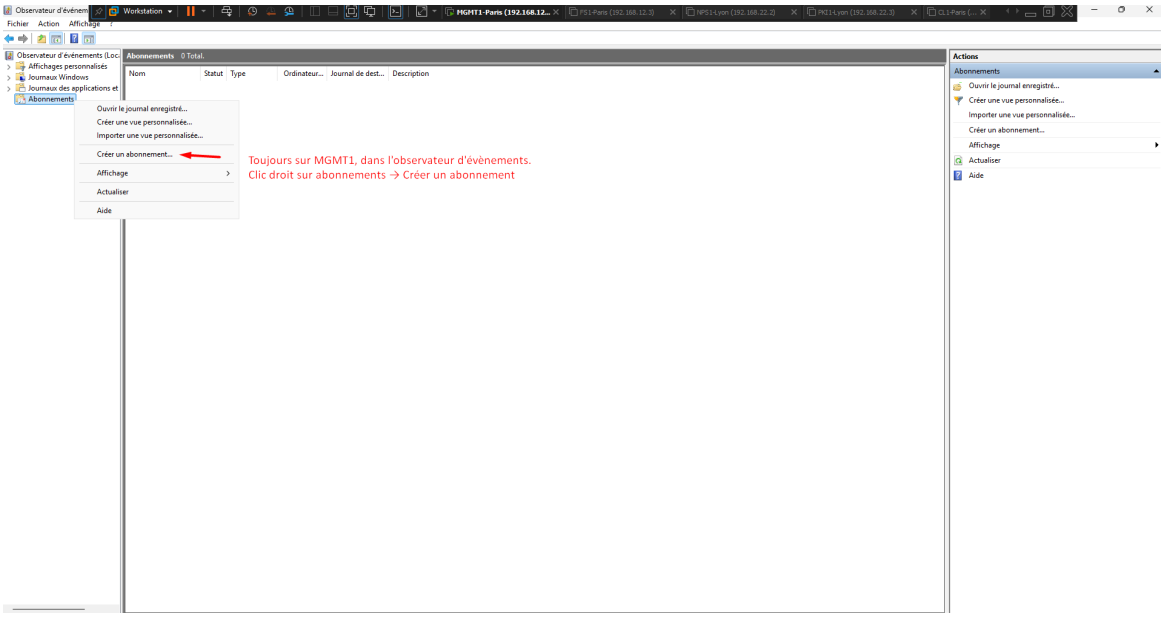

FIGURE 144 – Création d'un nouvel abonnement dans l'Observateur d'événements

11.3 Propriétés de l'abonnement WEF

Nous nommons cet abonnement `WEF-Global` et définissons le journal de destination sur "Événements transférés". Nous choisissons l'option "Initialisation par l'ordinateur source", puis nous cliquons sur "Sélectionner des groupes d'ordinateurs..." pour y ajouter les groupes "Ordinateurs du domaine" et "Contrôleurs de domaine".

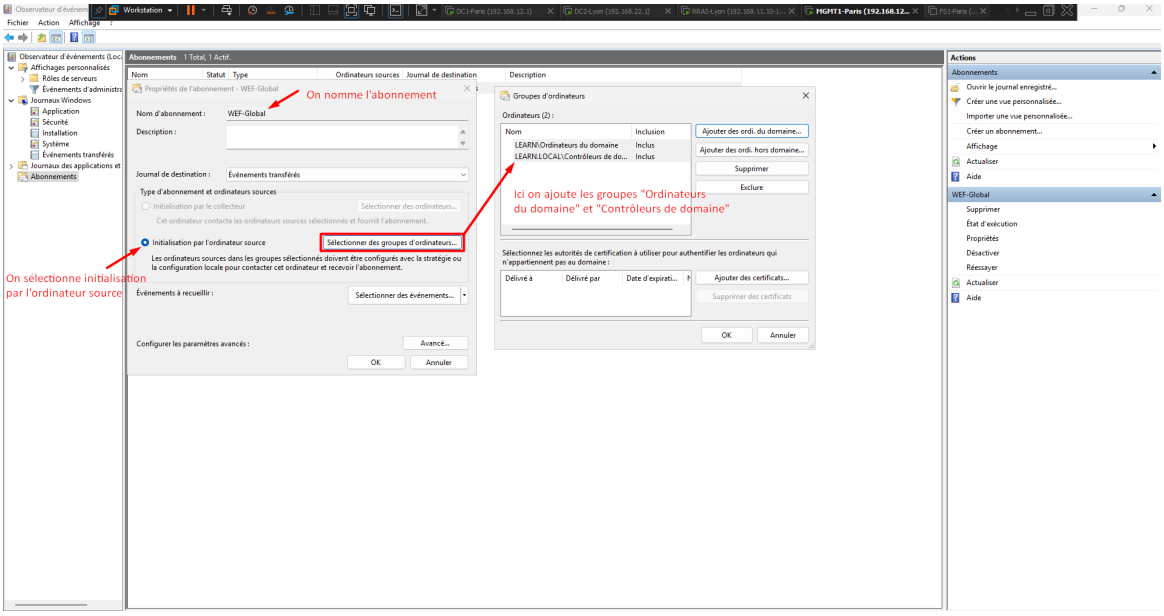

FIGURE 145 – Configuration des ordinateurs sources et du type d'abonnement

11.4 Filtrage des événements à collecter

Dans les propriétés de l'abonnement, nous cliquons sur "Sélectionner des événements...". Nous cochons les niveaux de gravité "Critique", "Avertissement" et "Erreur". Dans la liste déroulante "Journaux d'événements", nous sélectionnons l'ensemble des "Journaux Windows" (Application, Sécurité, Installation, Système).

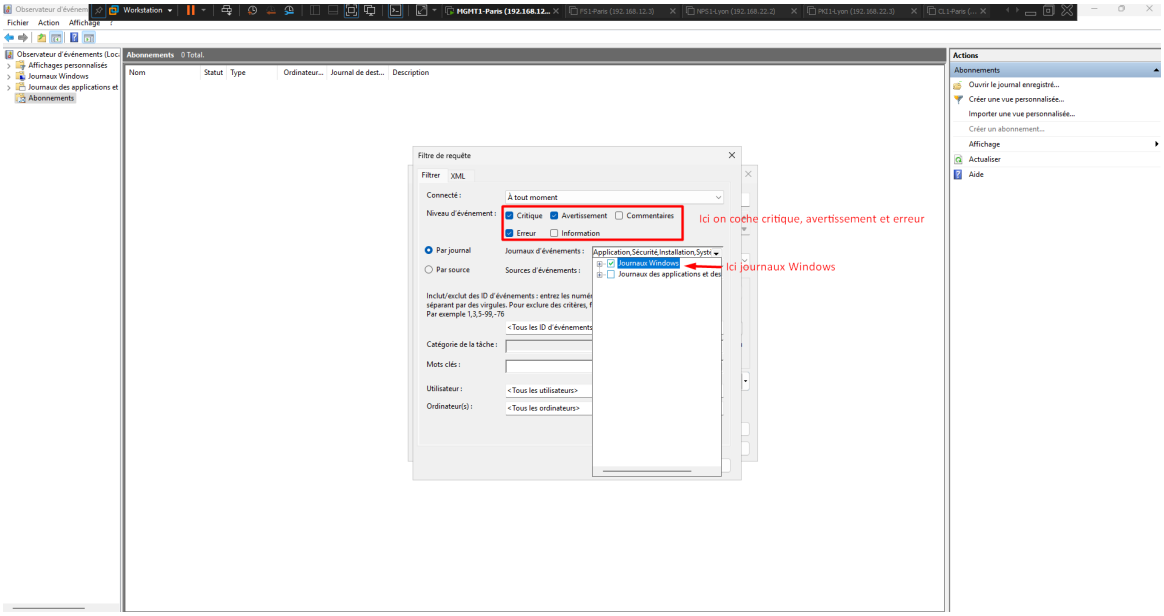

FIGURE 146 – Sélection des niveaux de gravité et des journaux cibles

11.5 Création de la GPO pour le déploiement WEF

Pour forcer tous les postes et serveurs du domaine à envoyer leurs journaux vers MGMT1, nous créons une GPO nommée `WEF_Clients` liée à la racine du domaine. Elle configure le service

WinRM (via le paramètre de transfert d'événements "Configurer le Gestionnaire d'abonnements cible" pointant sur l'URL de MGMT1) et ajoute le groupe "SERVICE RÉSEAU" au groupe local "Lecteurs des journaux d'événements".

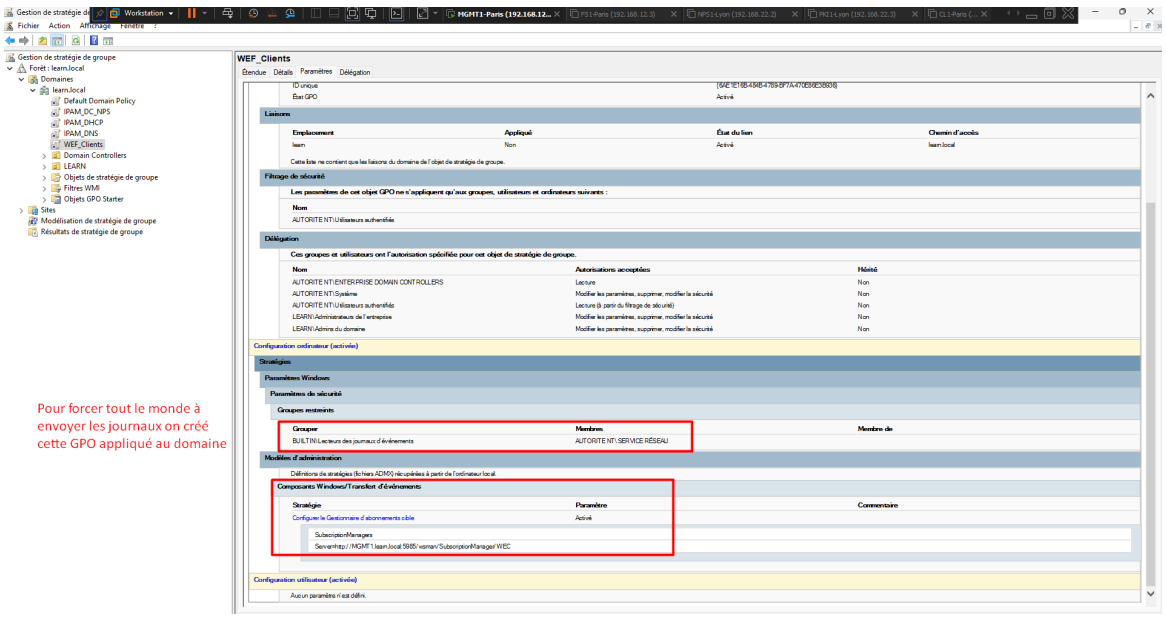

FIGURE 147 – Résumé des paramètres appliqués par la GPO WEF_Clients

11.6 Vérification de la réception des logs

Après l'application de la GPO, nous retournons dans l'Observateur d'événements de MGMT1, dans le dossier "Événements transférés". Le système est fonctionnel : nous voyons désormais remonter les journaux critiques et les erreurs de l'ensemble de l'infrastructure (ex : DC1 et RRAS).

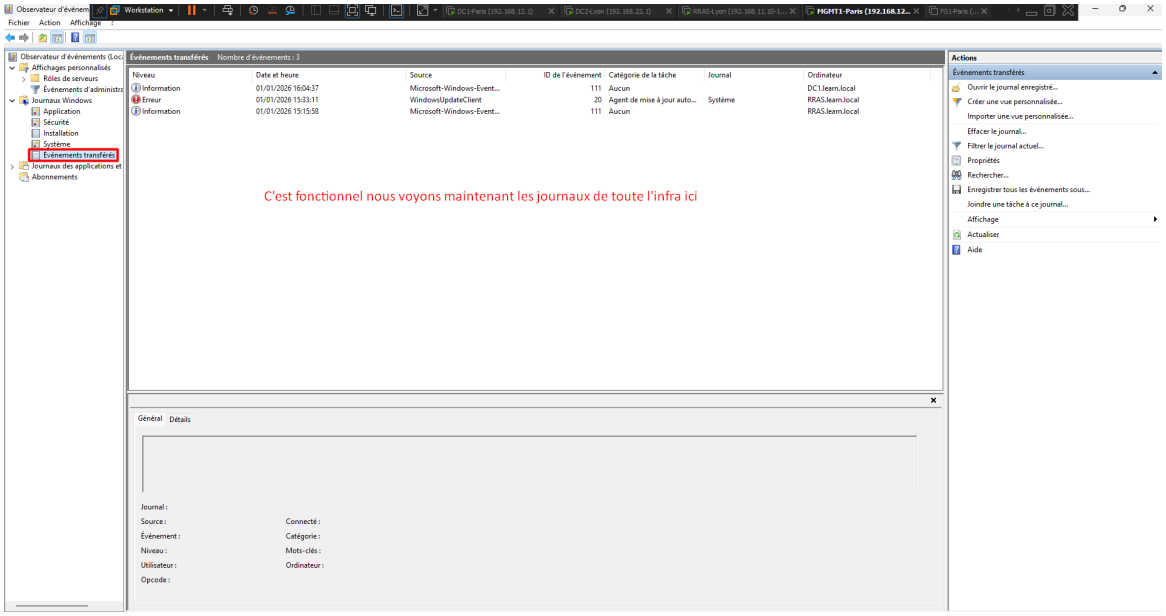

FIGURE 148 – Affichage centralisé des événements de l'infrastructure sur MGMT1

12 SERVEUR DE FICHIERS ET DFS (FS1)

12.1 Installation des rôles DFS sur FS1

Nous passons sur le serveur `FS1`, qui a préalablement été joint au domaine `learn.local`. Depuis l'assistant d'ajout de rôles, nous sélectionnons "Serveur de fichiers", "Espaces de noms DFS" et "Réplication DFS".

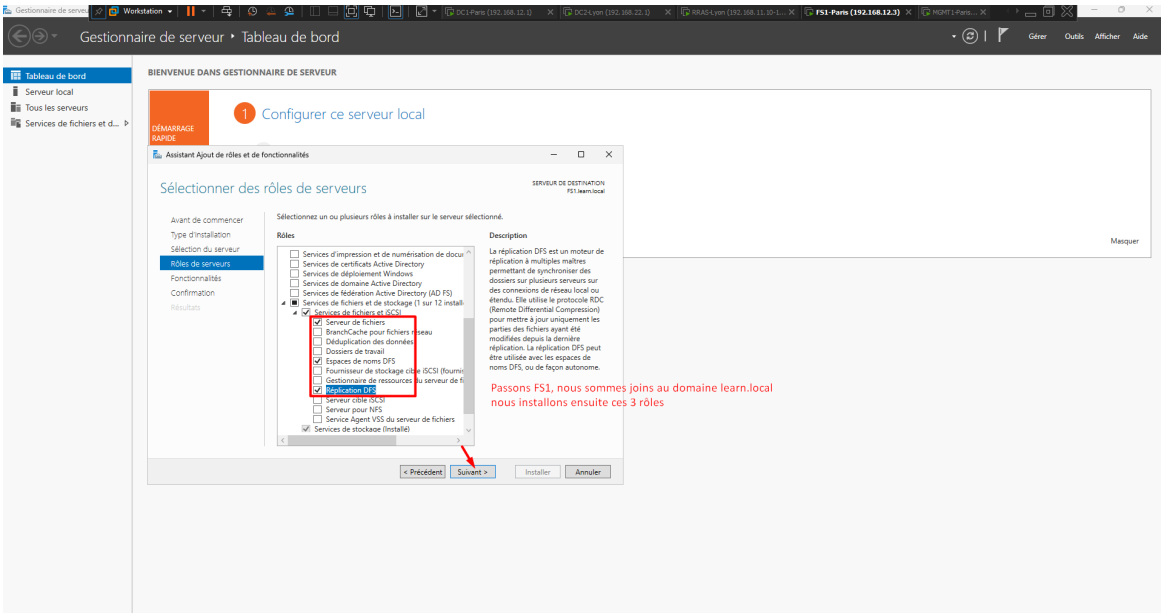

FIGURE 149 – Sélection des rôles liés aux services de fichiers et DFS

12.2 Création de l'Espace de noms

Une fois les rôles installés, nous ouvrons la console "Gestion du système de fichiers distribués" (DFS Management). Nous y créons notre espace de noms de domaine (ex : `\\learn.local\Public`) et nous lui attribuons le dossier "données" qui est stocké sur le disque `E:` que nous avons ajouté spécifiquement pour le stockage.

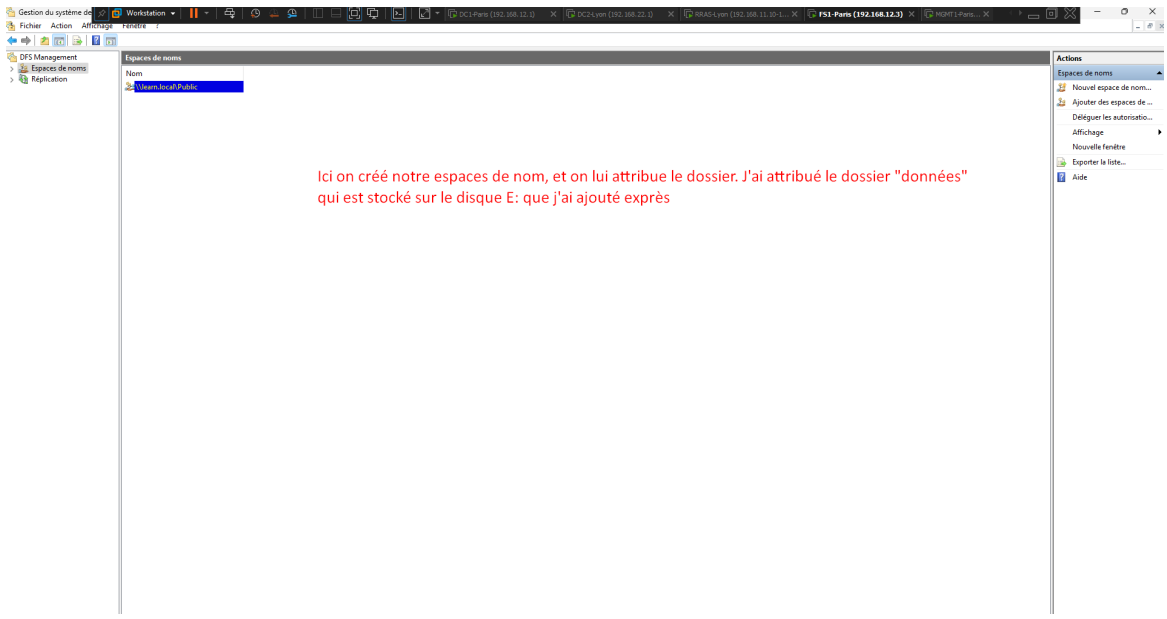

FIGURE 150 – Configuration de l'espace de noms racine DFS

13 SÉCURITÉ DES ACCÈS DISTANTS (NPS ET PKI)

13.1 Installation du rôle NPS

Nous passons maintenant à la configuration du serveur `NPS1.learn.local`. Depuis le Gestionnaire de serveur, nous lançons l'assistant et nous cochons le rôle "Services de stratégie et d'accès réseau" qui nous permettra d'authentifier les requêtes VPN.

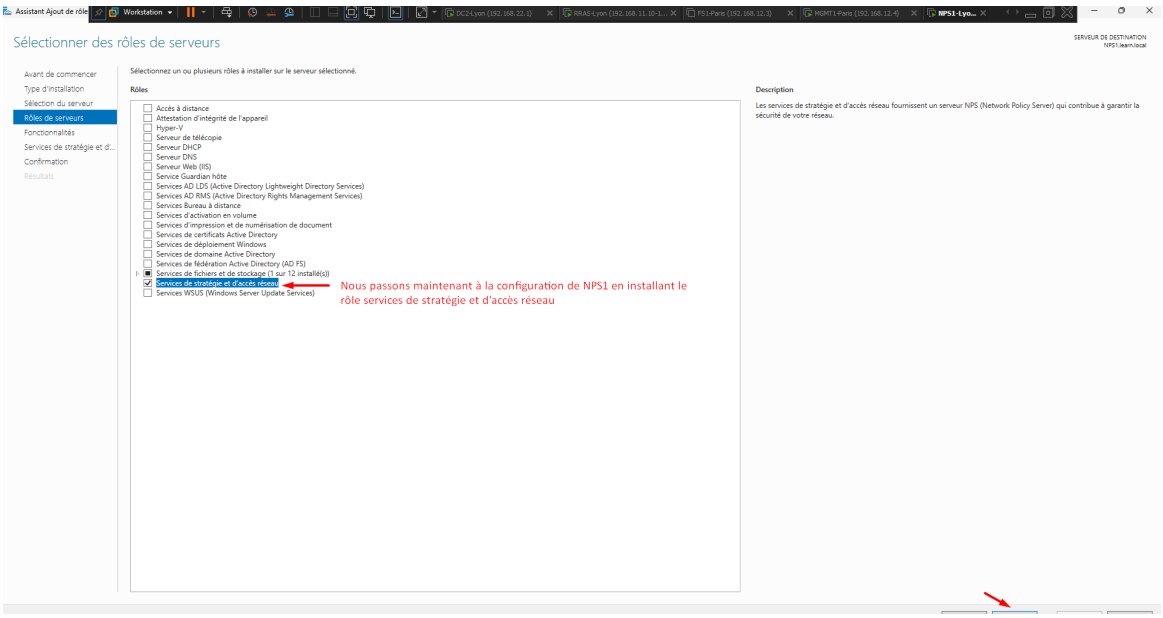

FIGURE 151 – Sélection du rôle Services de stratégie et d'accès réseau

13.2 Tableau de bord NPS1

L'installation est terminée avec succès. Le rôle "Services de stratégie et d'accès réseau" est maintenant visible dans la colonne de gauche du tableau de bord du serveur NPS1.

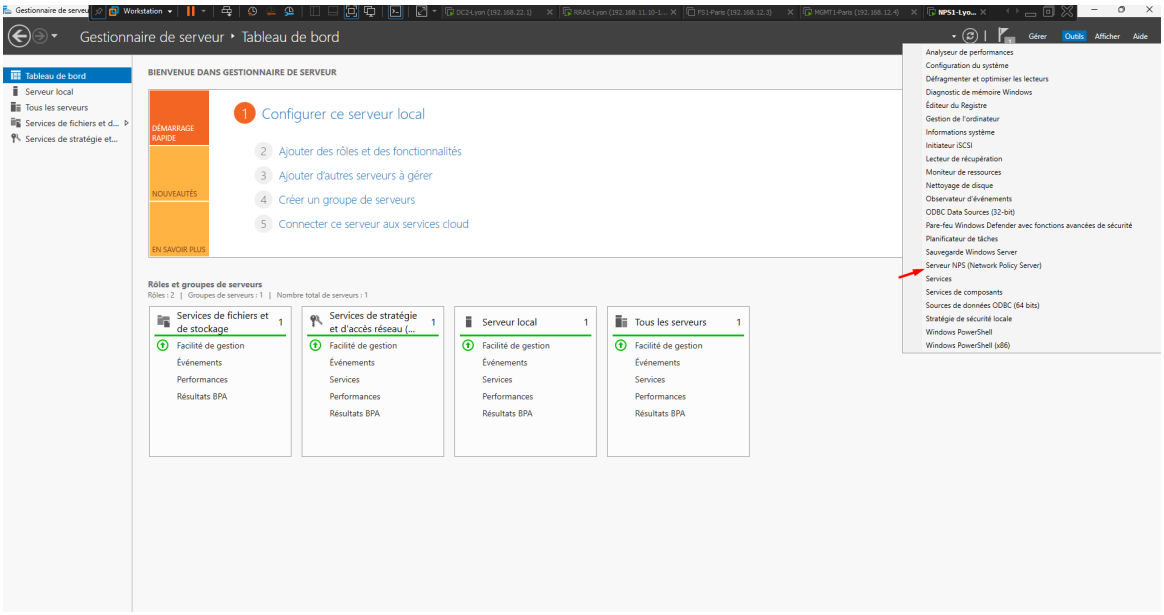

FIGURE 152 – Le rôle NPS est actif sur le tableau de bord

13.3 Ouverture de la console NPS

Nous ouvrons la console "Serveur NPS (Local)". L'interface principale affiche la section "Configuration standard" avec les options par défaut.

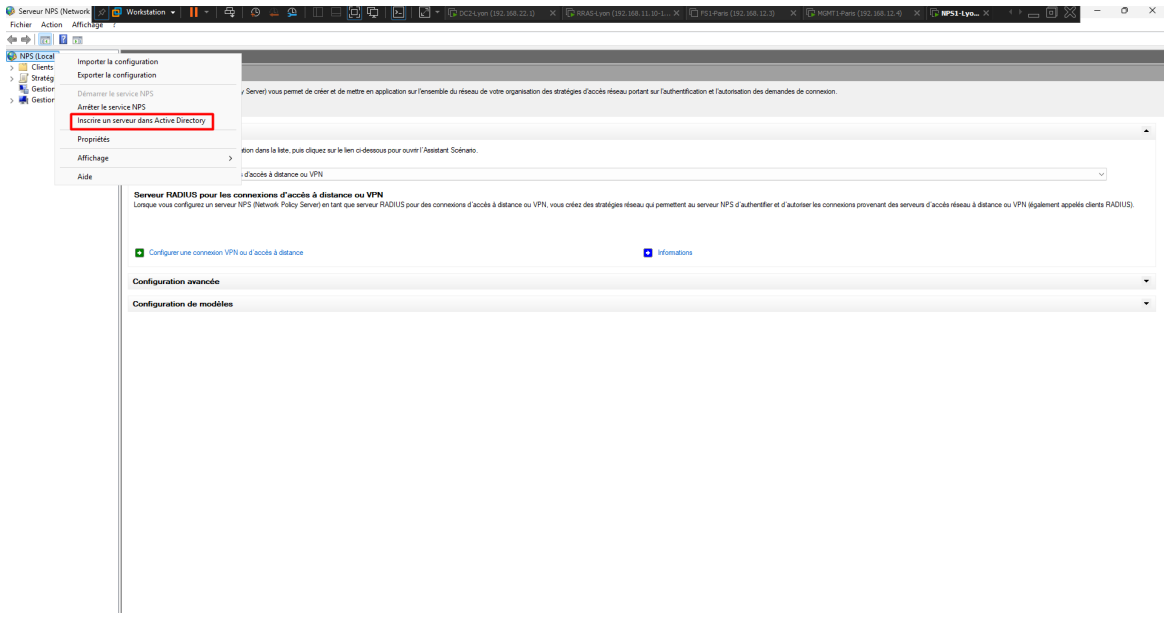

FIGURE 153 – Écran d'accueil de la console Serveur NPS (Local)

13.4 Sélection du scénario RADIUS et pause

Dans la liste déroulante des scénarios, nous sélectionnons "Serveur RADIUS pour les connexions d'accès à distance ou VPN". Avant de cliquer sur "Configurer le VPN...", nous devons faire une pause sur ce serveur : notre serveur NPS aura besoin d'un certificat pour prouver son identité. Nous allons donc d'abord mettre en place notre Autorité de Certification (PKI).

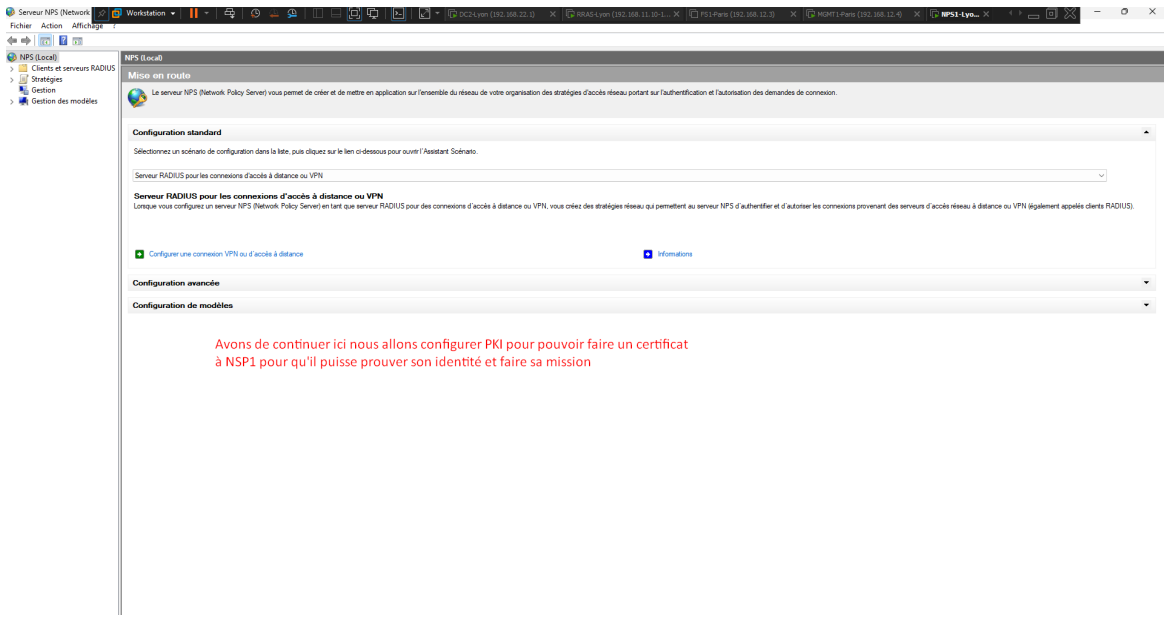

FIGURE 154 – Sélection du scénario RADIUS avant de basculer sur la PKI

13.5 Installation du rôle AD CS sur PKI1

Nous basculons sur le serveur `PKI1.learn.local`. Depuis l'assistant d'ajout de rôles, nous cochons "Services de certificats Active Directory" (AD CS) pour mettre en place notre Autorité de Certification interne.

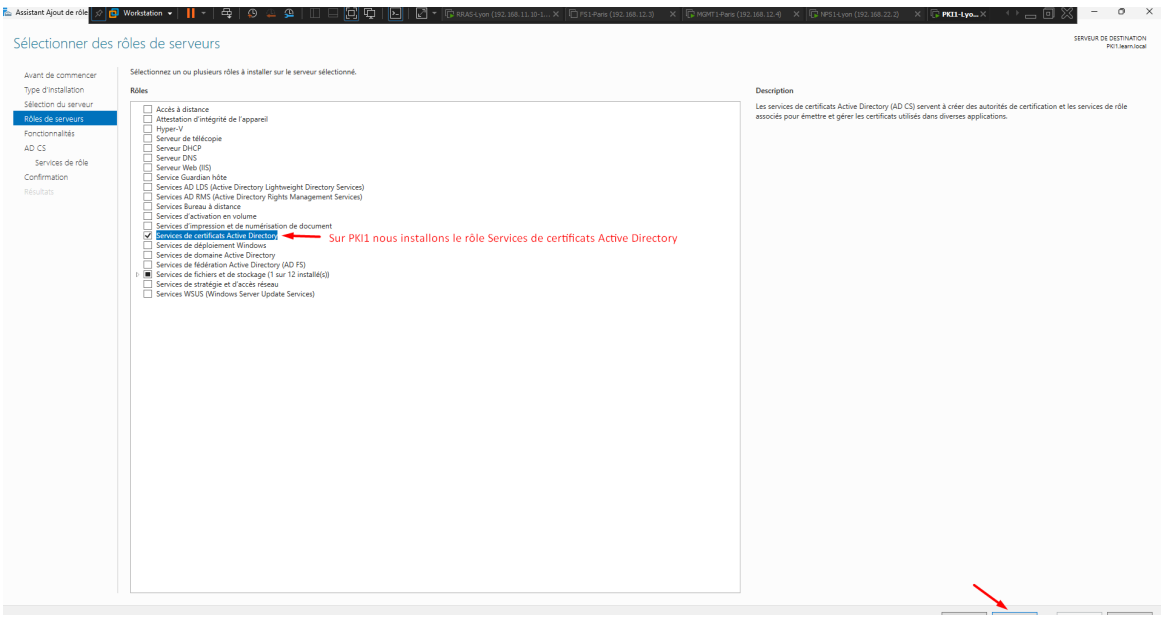

FIGURE 155 – Sélection du rôle Services de certificats Active Directory

13.6 Sélection du service Autorité de certification

Dans l'onglet "Services de rôle" de l'assistant, nous n'aurons besoin de cocher uniquement la case "Autorité de certification" pour notre infrastructure.

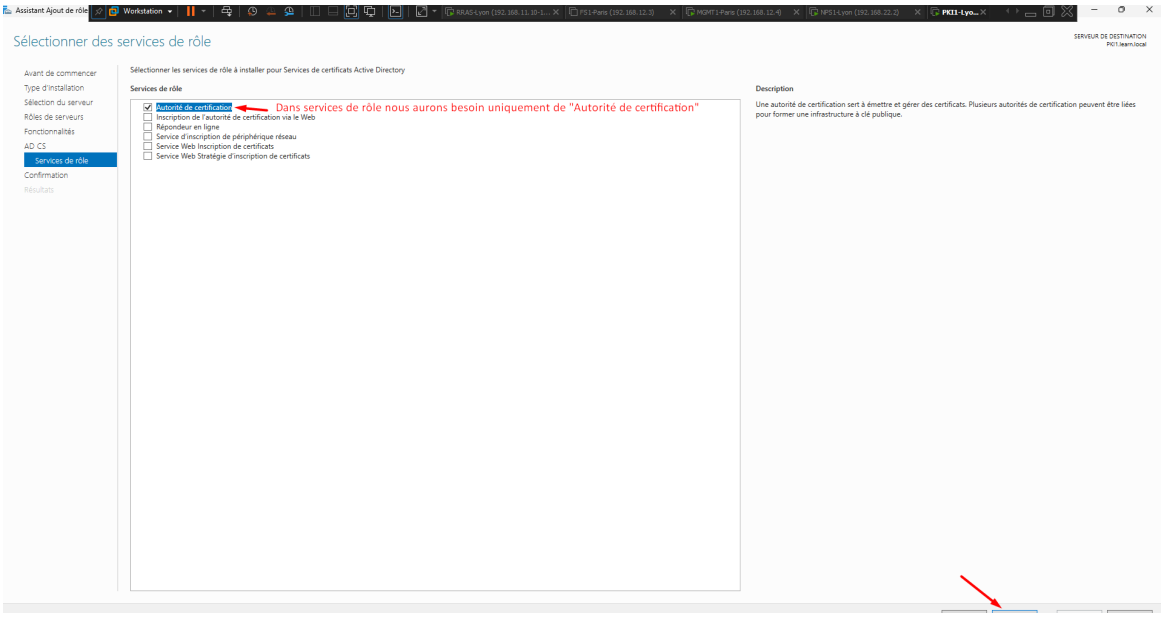

FIGURE 156 – Cochage du service de rôle Autorité de certification

13.7 Notification de post-déploiement

L'installation des binaires est terminée sur PKI1. Une notification avec un drapeau d'avertissement apparaît dans le Gestionnaire de serveur, nous invitant à cliquer sur le lien "Configurer les services de certificats Active Directory...".

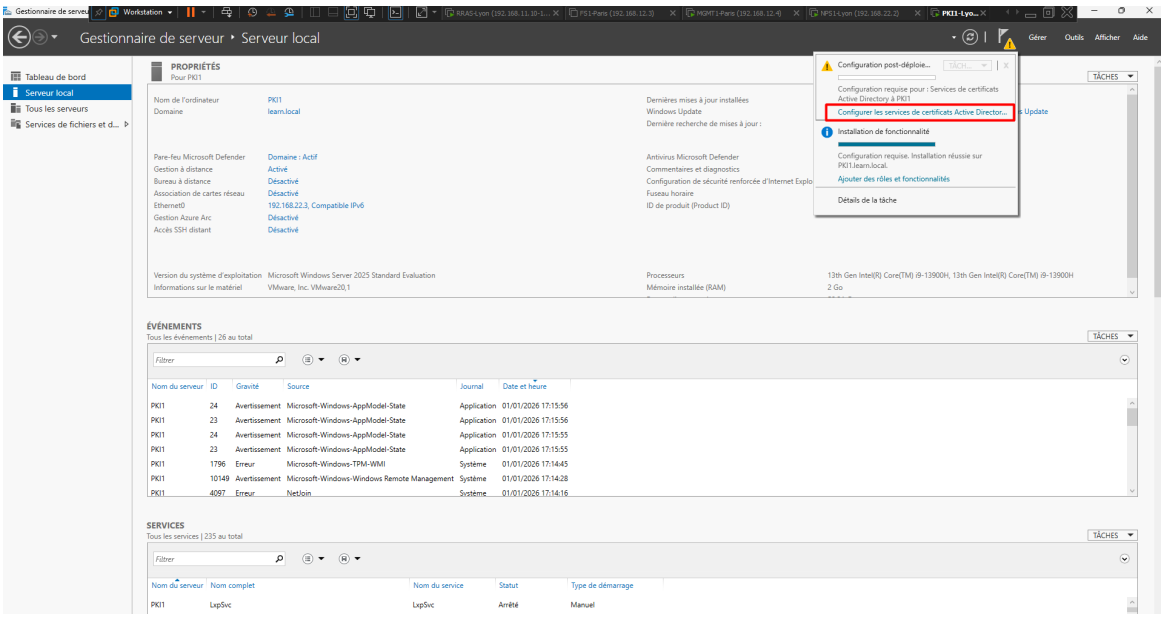

FIGURE 157 – Lien pour lancer la configuration de l'Autorité de Certification

13.8 Informations d'identification (PKI)

L'assistant de configuration s'ouvre. Pour configurer une autorité de certification d'entreprise (intégrée à l'annuaire), il est nécessaire de valider l'étape avec des droits d'administrateur de l'entreprise. Nous utilisons ici le compte `LEARN\administrateur`.

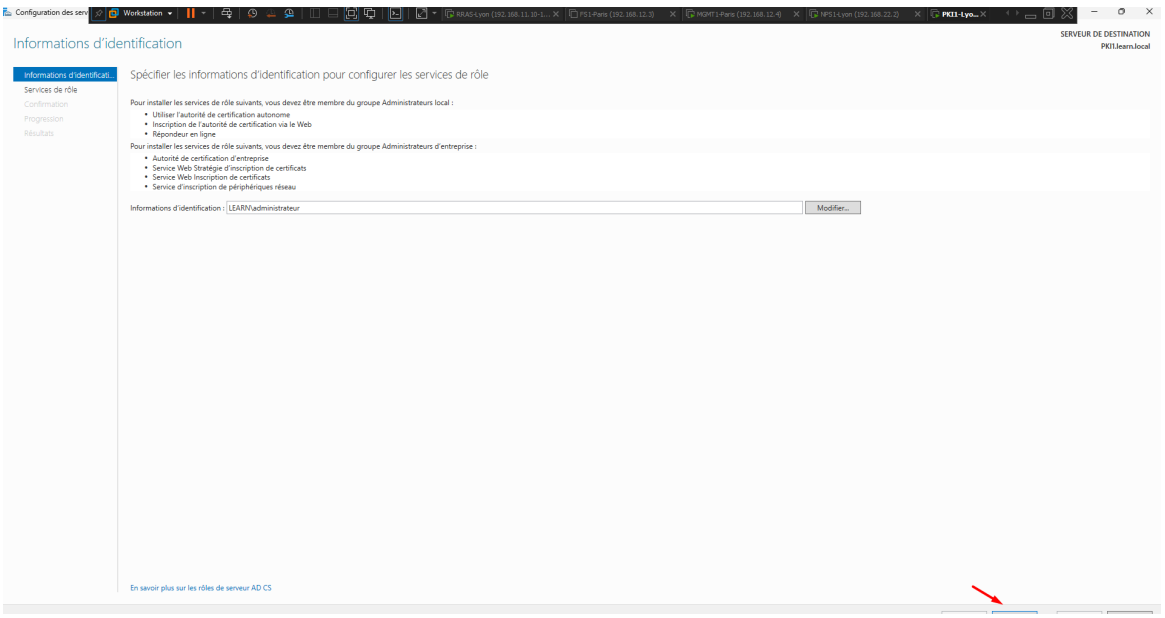

FIGURE 158 – Validation des informations d'identification d'entreprise

13.9 Sélection du service à configurer

À l'étape "Services de rôle", nous cochons "Autorité de certification" pour procéder à son paramétrage (choix du type, création de la clé privée, etc.) lors des prochaines étapes.

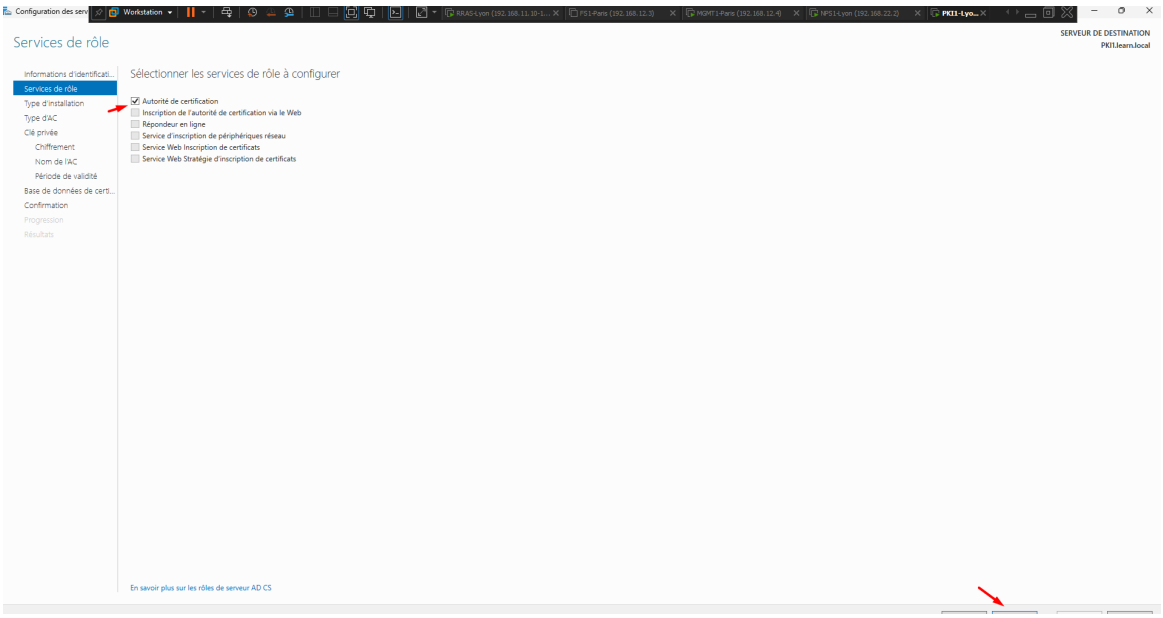

FIGURE 159 – Sélection du service Autorité de certification à configurer

13.10 Type d'installation de l'Autorité de Certification

Dans l'assistant de configuration AD CS, nous choisissons l'option "Autorité de certification d'entreprise" afin que notre PKI soit intégrée à l'Active Directory.

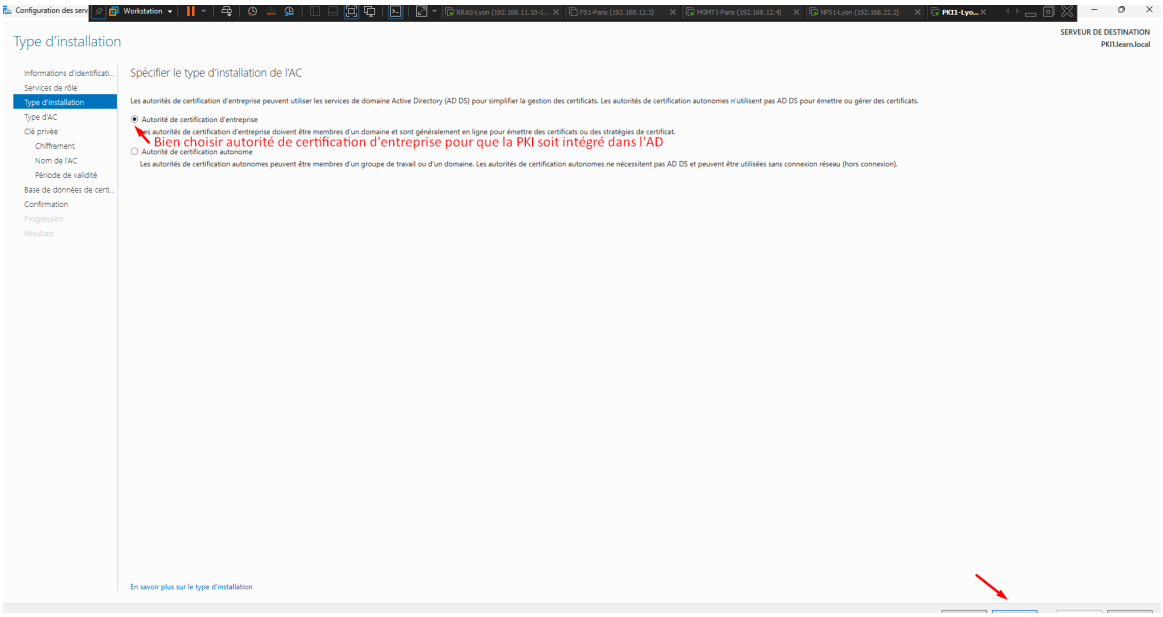

FIGURE 160 – Sélection de l'autorité de certification d'entreprise

13.11 Type d'Autorité de certification

Comme il s'agit de notre premier serveur de certificats, nous sélectionnons "Autorité de certification racine".

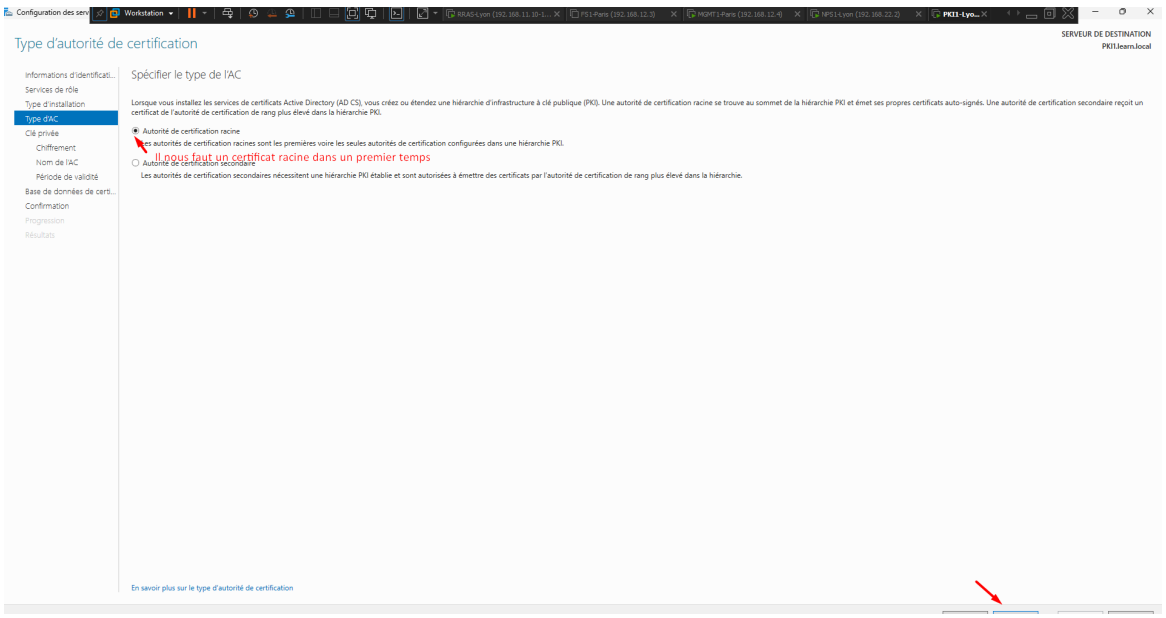

FIGURE 161 – Définition du serveur en tant qu'Autorité racine

13.12 Création de la clé privée

Nous n'avons pas encore de clé privée, nous choisissons donc l'option "Créer une clé privée" nouvelle.

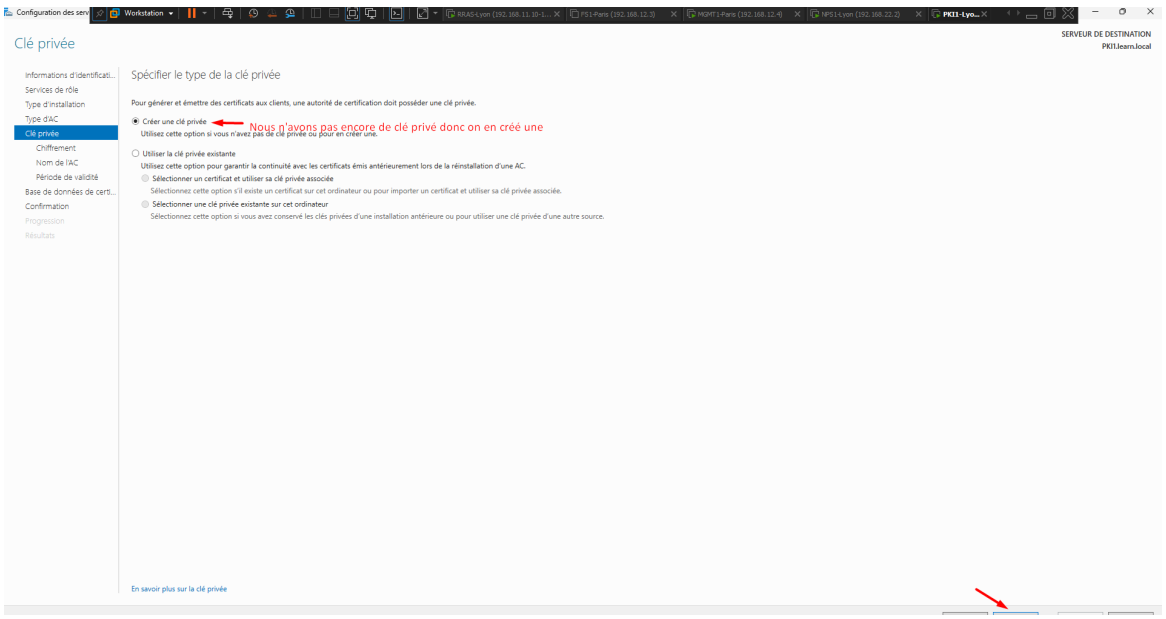

FIGURE 162 – Génération d'une nouvelle clé privée pour la PKI

13.13 Résultats de la configuration AD CS

Nous laissons tous les autres paramètres par défaut (chiffrement, validité...) et lançons la configuration. Le résultat affiche un succès avec un avertissement : nous devrons ajouter manuellement le serveur PKI1 au groupe de sécurité "Éditeurs de certificats" dans l'AD.

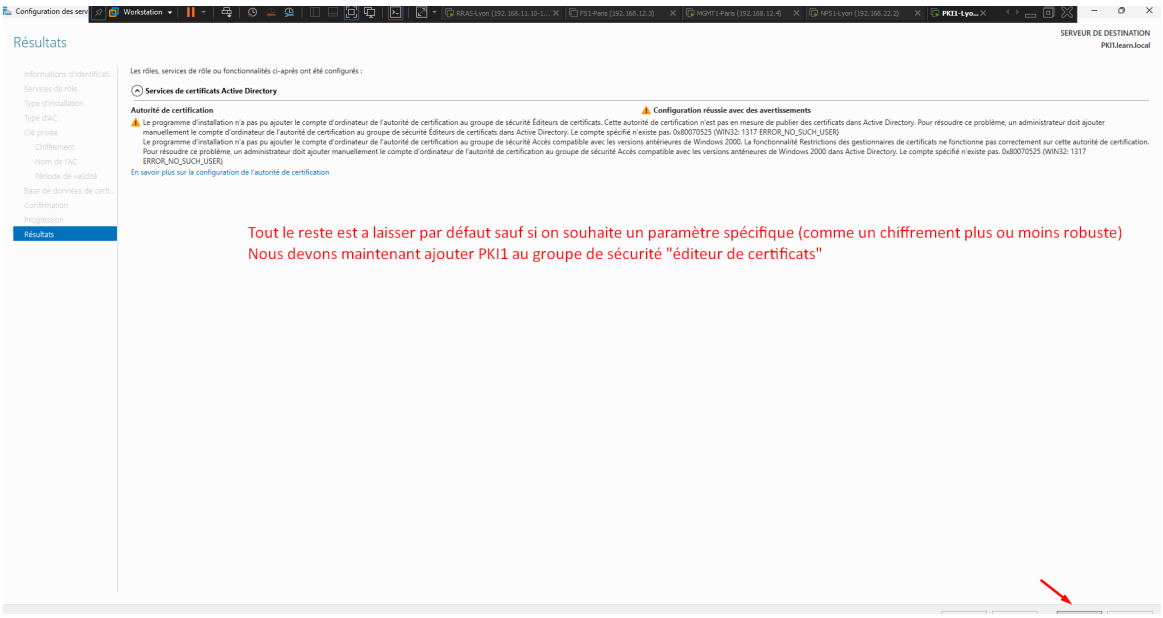

FIGURE 163 – Succès de la configuration avec un avertissement de groupe de sécurité

13.14 Préparation de l'auto-inscription (Tableau de bord PKI1)

De retour sur le tableau de bord, nous allons maintenant mettre en place un modèle d'auto-inscription pour que nos serveurs obtiennent leur certificat automatiquement.

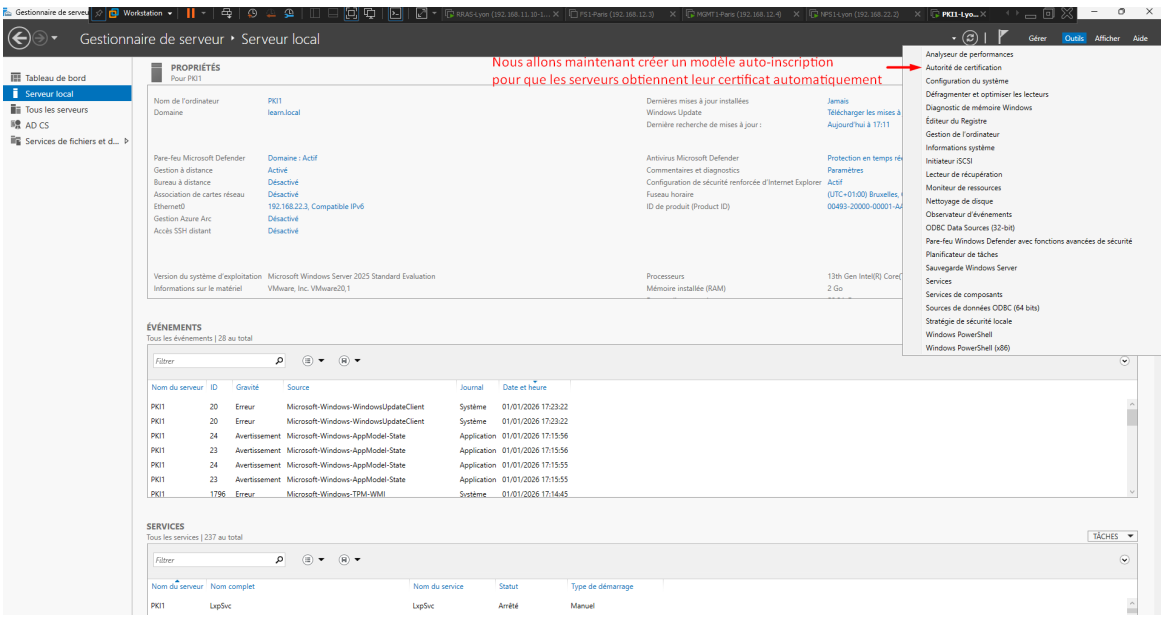

FIGURE 164 – Tableau de bord de PKI1 après la configuration AD CS

13.15 Console de l'Autorité de certification

Nous ouvrons la console "Autorité de certification" depuis les outils d'administration pour gérer notre nouvelle PKI (`learn-PKI1-CA`).

FIGURE 165 – Ouverture de la console de gestion de l'Autorité de certification

13.16 Duplication du modèle de certificat

Dans la gestion des modèles, nous sélectionnons le modèle "Ordinateur" et nous le dupliquons. Ce modèle nous servira de base pour que les machines du domaine reçoivent un certificat.

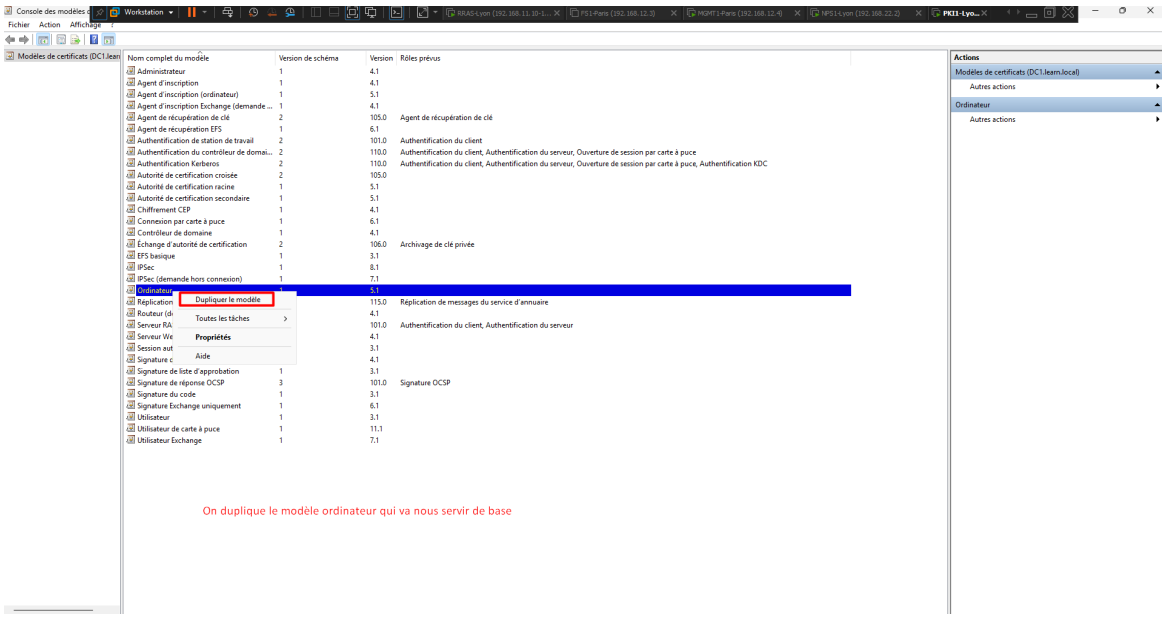

FIGURE 166 – Duplication du modèle de certificat Ordinateur

13.17 Création d'une GPO d'auto-inscription

Dans l'Éditeur de gestion des stratégies de groupe, nous créons une nouvelle GPO pour configurer les paramètres de sécurité et dire aux appareils de demander un certificat automatiquement.

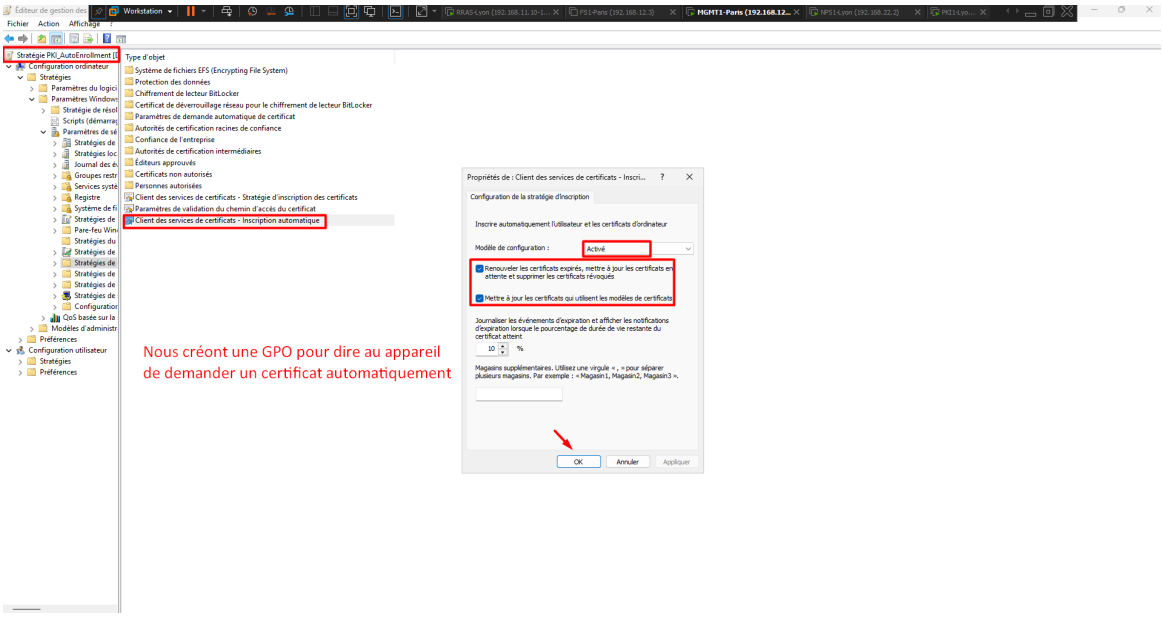

FIGURE 167 – Création de la GPO pour l'inscription automatique des certificats

13.18 Configuration de l'inscription automatique

Dans les propriétés de la stratégie "Client des services de certificats - Inscription automatique", nous définissons le modèle de configuration sur "Activé" et nous cochons les options pour renouveler et mettre à jour les certificats.

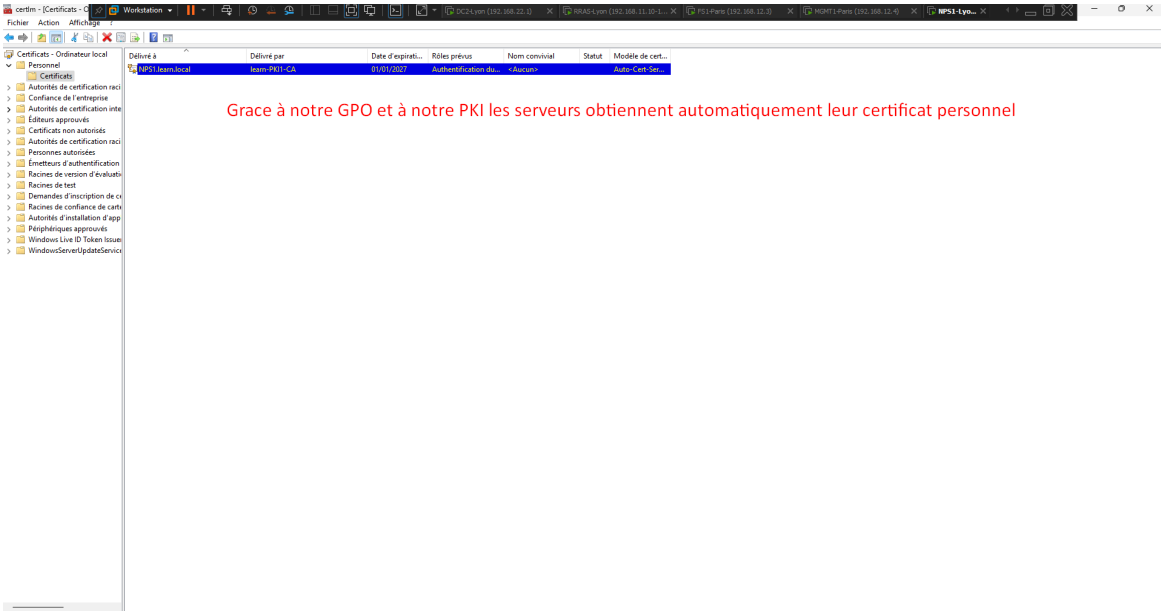

FIGURE 168 – Activation de l'inscription automatique dans la GPO

13.19 Vérification du certificat sur NPS1

Grâce à notre GPO et à la PKI, les serveurs obtiennent automatiquement leur certificat personnel. Nous le vérifions sur NPS1 en ouvrant la console des certificats (ordinateur local).

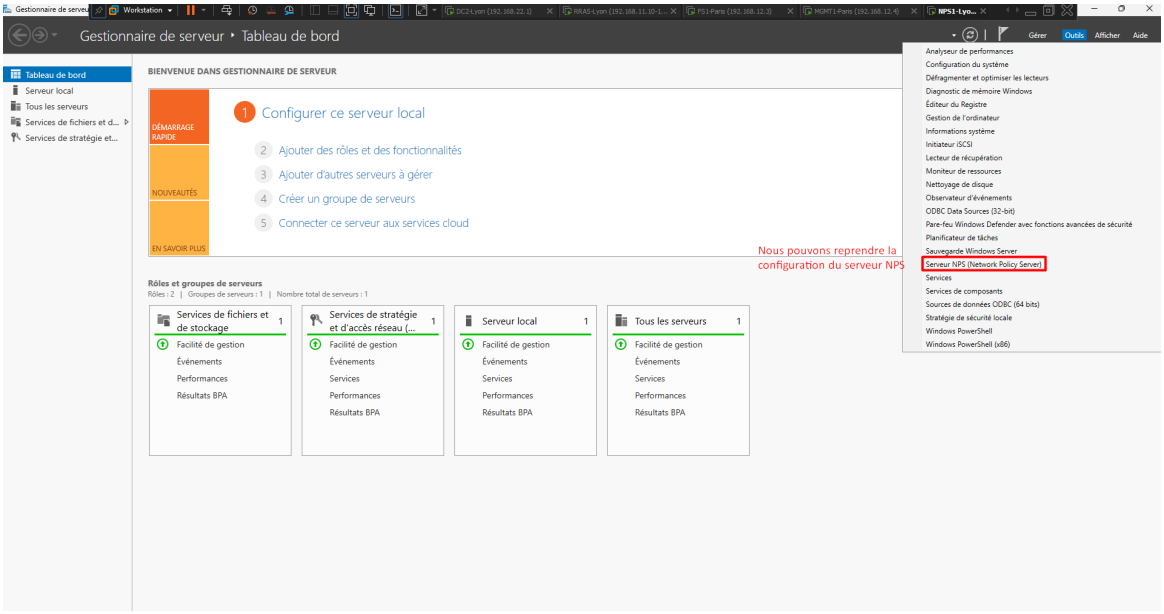

FIGURE 169 – Présence du certificat auto-généré dans le magasin personnel du serveur

14 SÉCURISATION DES ACCÈS (NPS ET RADIUS)

14.1 Reprise de la configuration sur NPS1

Maintenant que le serveur NPS1 dispose de son certificat, nous pouvons reprendre sa configuration depuis le Gestionnaire de serveur.

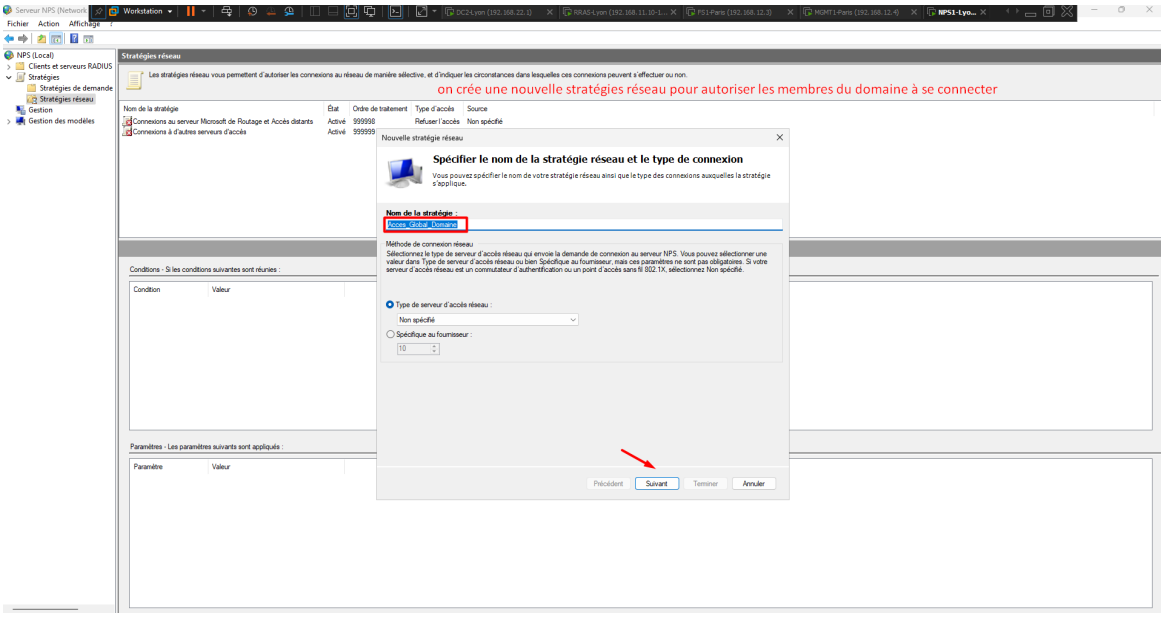

FIGURE 170 – Tableau de bord de NPS1 pour reprendre la configuration

14.2 Création d'une Stratégie réseau (NPS)

Dans la console Serveur NPS, nous créons une nouvelle stratégie réseau (nommée "Accès Global Domaine") pour autoriser les membres du domaine à se connecter via le réseau.

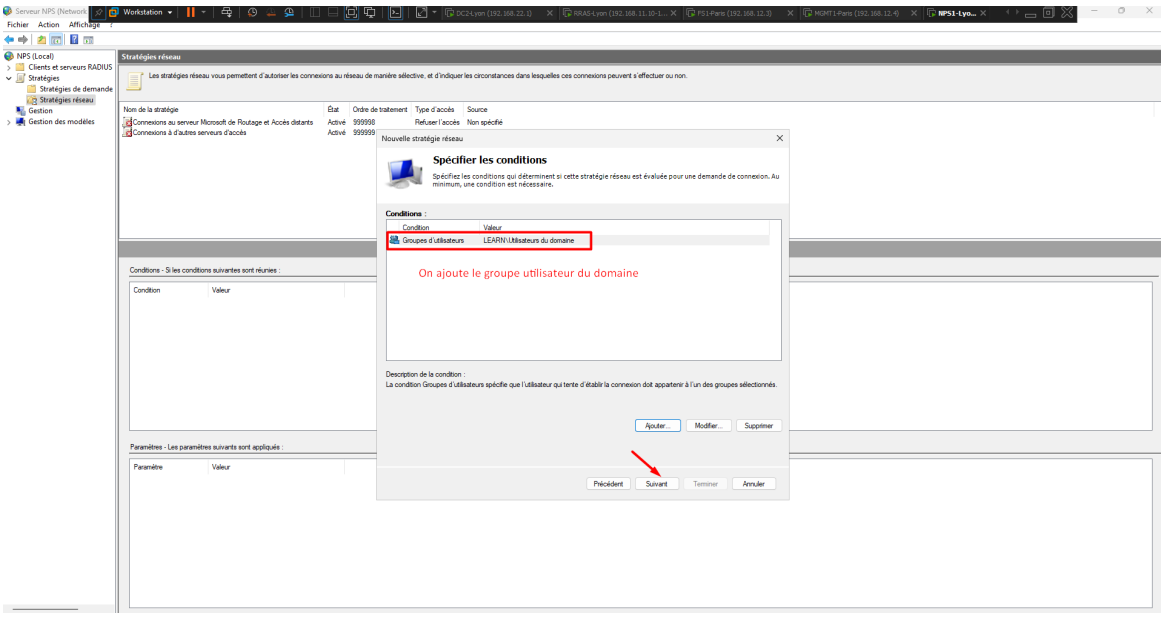

FIGURE 171 – Création d'une nouvelle stratégie réseau dans NPS

14.3 Conditions de la stratégie

À l'étape des conditions, nous ajoutons le groupe d'utilisateurs "Utilisateurs du domaine" (`LEARN\Utilisateurs du domaine`) pour restreindre l'accès à ce groupe.

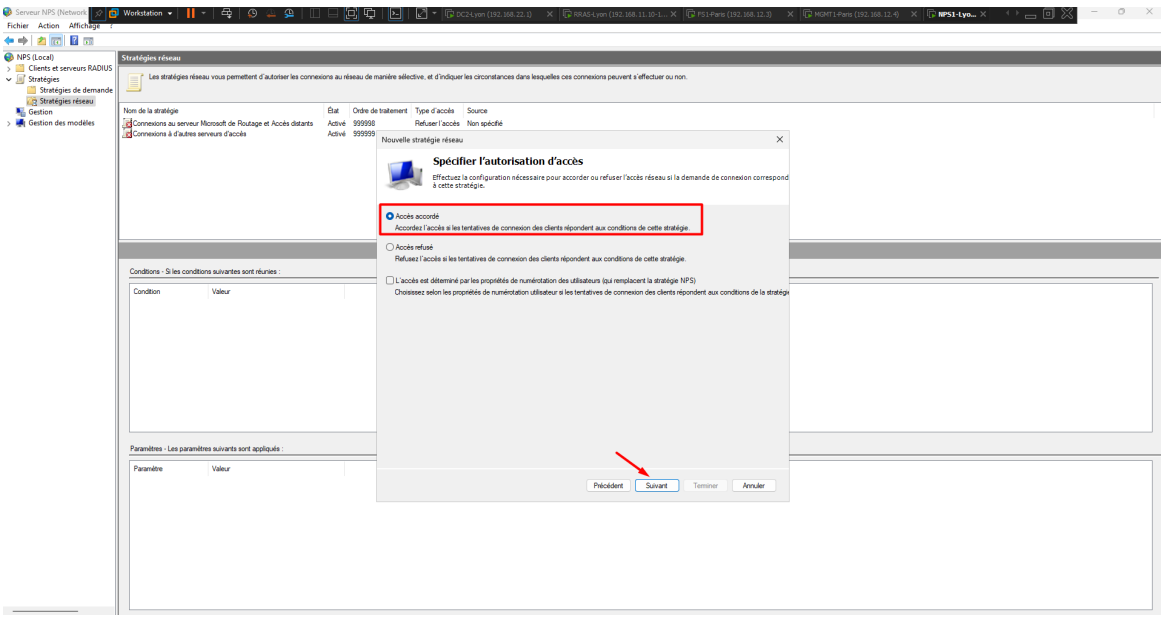

FIGURE 172 – Ajout de la condition d'appartenance au groupe Utilisateurs du domaine

14.4 Autorisation d'accès

Nous spécifions l'autorisation en choisissant "Accès accordé" si les tentatives de connexion répondent aux conditions de la stratégie.

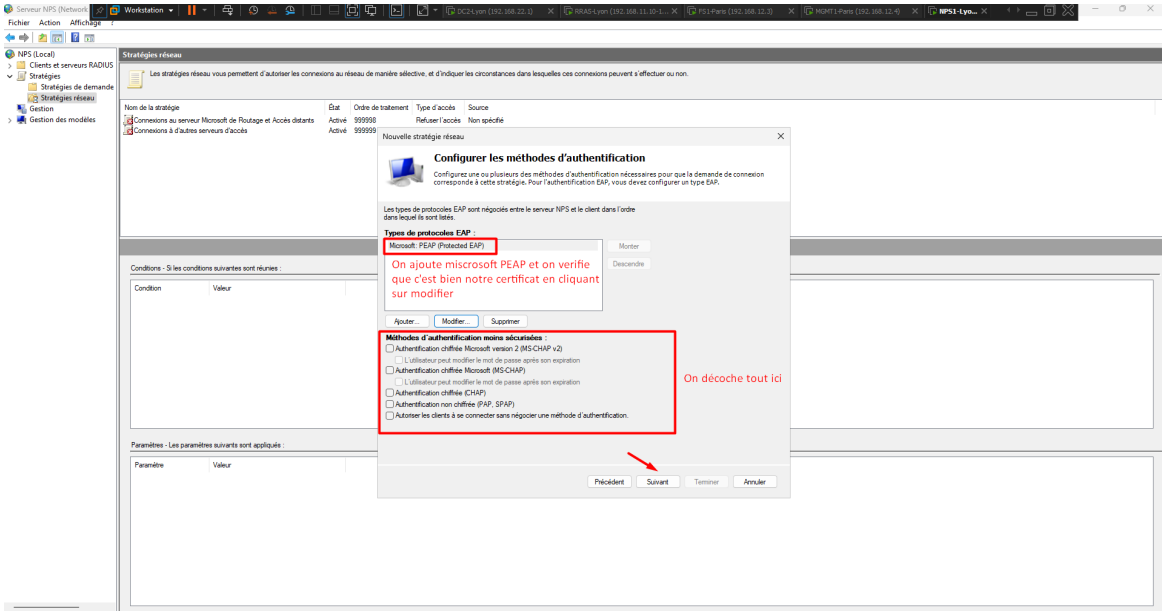

FIGURE 173 – Configuration de l'accès accordé pour la stratégie

14.5 Méthodes d'authentification

Dans les méthodes d'authentification, nous ajoutons le type EAP "Microsoft : PEAP". Nous cliquons sur "Modifier" pour nous assurer qu'il utilise bien le certificat de NPS1 obtenu précédemment. Enfin, nous décochons toutes les méthodes d'authentification moins sécurisées (MS-CHAP v2, CHAP, PAP).

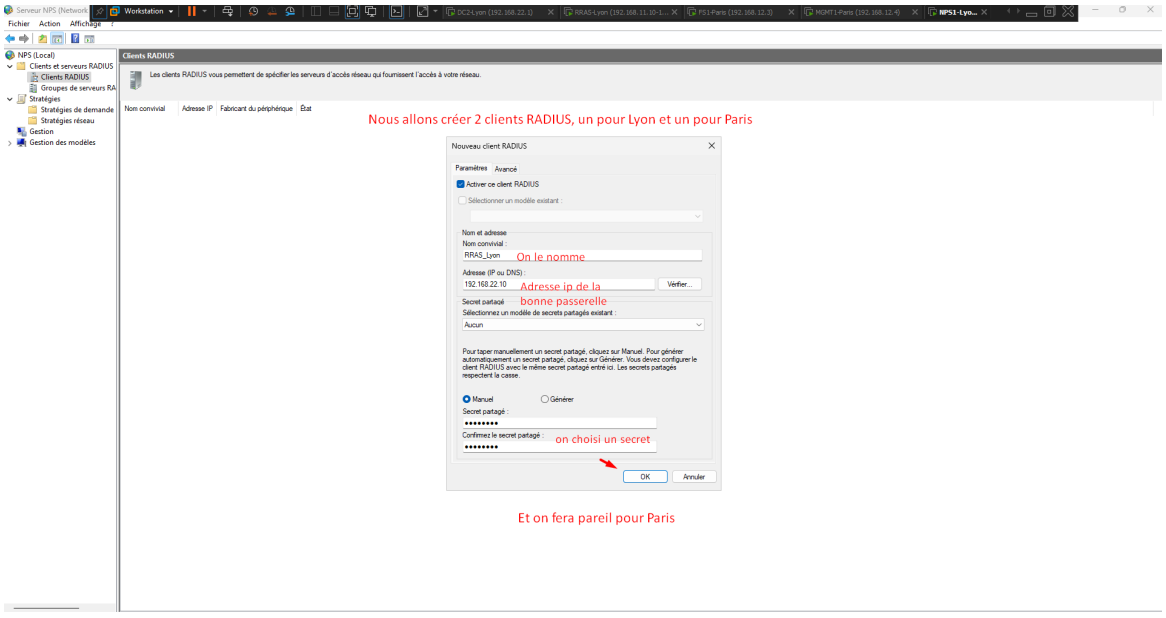

FIGURE 174 – Configuration du protocole PEAP et désactivation des méthodes obsolètes

14.6 Ajout des clients RADIUS (RRAS)

Dans le menu "Clients RADIUS", nous allons déclarer nos routeurs. Nous créons un nouveau client nommé "RRAS Lyon" avec l'adresse IP de sa passerelle (`192.168.22.10`) et nous définissons un secret partagé manuel. Nous répétons l'opération pour le RRAS de Paris.

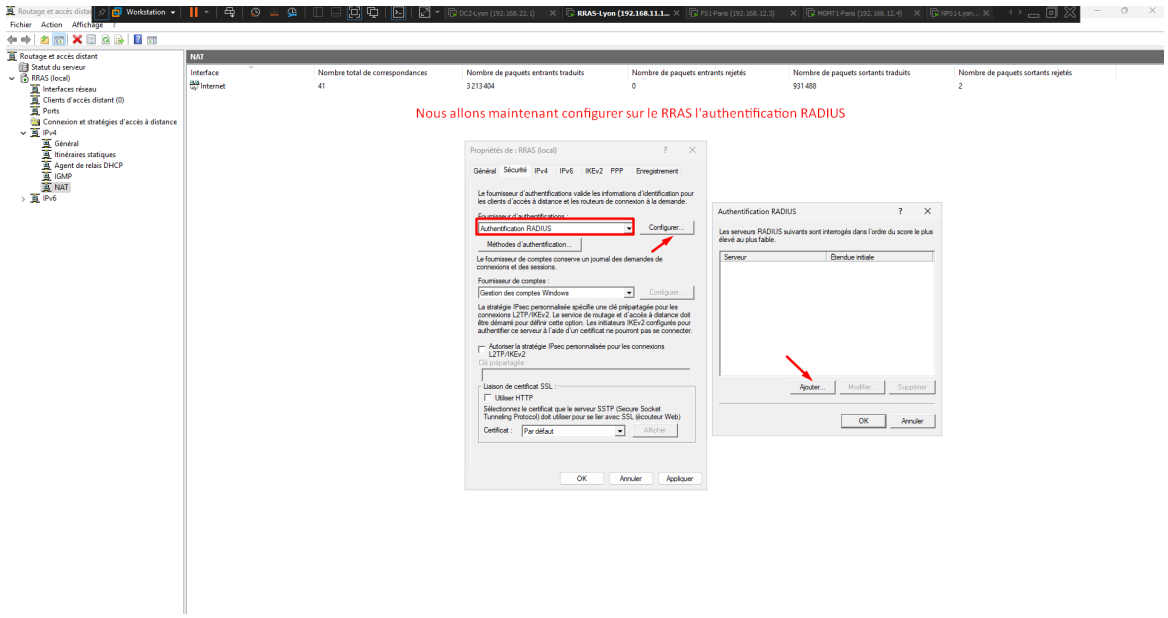

FIGURE 175 – Déclaration des routeurs RRAS en tant que clients RADIUS

14.7 Configuration de l'authentification RADIUS sur RRAS

Nous basculons sur le serveur RRAS. Dans les propriétés du serveur (onglet Sécurité), nous sélectionnons le fournisseur d'authentification "Authentification RADIUS" et nous cliquons sur Configurer pour y ajouter l'IP de notre serveur NPS (`192.168.22.2`) avec le même secret partagé.

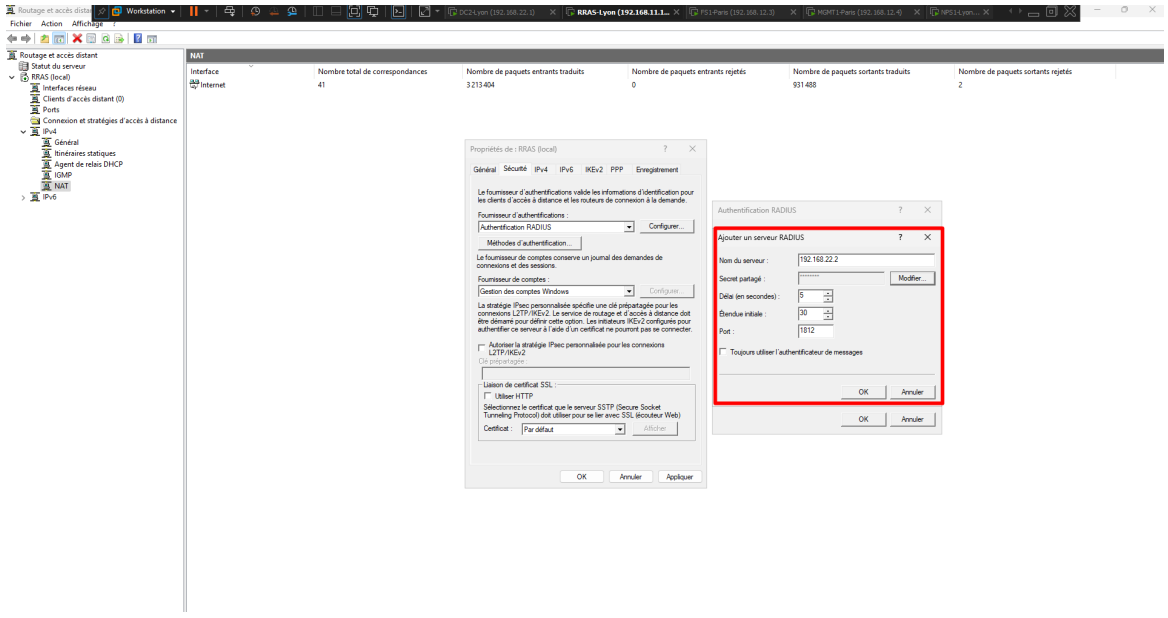

FIGURE 176 – Configuration du serveur RADIUS (NPS1) dans les propriétés du RRAS

15 CONCLUSION ET BILAN

15.1 1. État de l'Infrastructure (Lyon & Paris)

Nom de la machine	Site	Adresse IP	Rôle et Services
DC1	Paris	192.168.12.1	Contrôleur de domaine (AD DS), DNS
NPS1	Lyon	192.168.22.2	Serveur RADIUS (NPS), gère l'authentification
PKI1	Lyon	192.168.22.3	Autorité de Certification (AD CS)
RRAS	Lyon	192.168.11.10 192.168.12.10 192.168.21.10 192.168.22.10	Serveur VPN (SSTP), Routeur, Client RADIUS
CL1	Paris	192.168.11.DHCP	Poste client Windows 11 de test
CL2	Lyon	192.168.21.DHCP	Poste client Windows 11 de test
DC2	Lyon	192.168.22.1	Contrôleur de domaine secondaire
MGMT1	Paris	192.168.12.4	Serveur d'administration (WSUS, IPAM, WEF)
FS1	Paris	192.168.12.3	Serveur de fichiers (DFS)
WDS1	Paris	192.168.12.2	Serveur de déploiement (WDS, MDT)

15.2 2. Problèmes rencontrés et résolus

Lors de la mise en place de cette infrastructure complexe, plusieurs problématiques techniques ont été rencontrées et analysées :

Erreur de déploiement PXE (Pilotes réseau VMware)

Lors de la tentative d'amorçage PXE du client CL2, l'environnement WinPE se chargeait mais l'assistant MDT affichait une erreur empêchant la connexion au *Deployment Share*. Ce problème a été résolu en extrayant les pilotes réseau spécifiques à VMware (`vmxnet3.inf`) de l'hôte, en les importent dans les *Out-of-Box Drivers* du MDT, puis en régénérant et remplaçant l'image de démarrage dans WDS.

Anomalie liée à l'architecture x86 dans MDT

Un bug a été identifié lors de la génération des images de boot, l'architecture x86 n'étant plus correctement prise en charge avec Windows 11 et Server 2025. La résolution a nécessité la

modification du fichier `Settings.xml` (passage de la balise `<SupportX86>` à `False`) ainsi que la copie manuelle du dossier `WinPE_OCs` dans le répertoire d'installation de l'ADK.

Blocage IPAM (Accès au journal des événements)

Malgré une remontée fonctionnelle des données opérationnelles (étendues DHCP et zones DNS visibles), la console IPAM sur MGMT1 maintient les serveurs DC1 et DC2 dans un état global "Bloqué". L'erreur spécifique indique que le service IPAM ne parvient pas à lire à distance le journal de sécurité (Security Event Log), nécessaire pour la corrélation IP/Utilisateur (Audit). Ce blocage persiste probablement en raison du durcissement des ACL sur le canal RPC de Windows Server 2025. Les tentatives d'ajustement (désactivation du pare-feu, permissions WMI, ajout au groupe Lecteurs du journal d'événements) n'ont pas permis de contourner ce blocage système natif.

Erreur d'obtention de certificat sur le client (CL2)

Un problème bloquant a été rencontré concernant l'obtention de certificats depuis le poste client CL2. Plusieurs solutions ont été tentées : désactivation du pare-feu, désactivation de la vérification de la liste de révocation, régénération des certificats et bascule de l'identification sur le mode Windows à la place de RADIUS. Aucune de ces solutions n'a fonctionné. Ce même type d'erreur s'est également manifesté lors de la configuration de l'IPAM.

Fin du rapport technique.