



# PROJET DE STAGE

## LICENCE PROFESSIONNELLE

### Filière : Cybersécurité

#### THEME

**Mise en œuvre d'une infrastructure sécurisée et managée  
avec Active Directory, LAPS et WSUS**

Présenté par : **ABAKTA Haana Camille**

Maitre de stage :

**Florent ADADE**

Senior Manager IT – Cyber Security

# SOMMAIRE

<b>1. Contexte général du projet .....</b>	<b>7</b>
<b>2. Objectifs du projet.....</b>	<b>7</b>
<b>3. Architecture du système.....</b>	<b>8</b>
<b>4. Manuel de déploiement .....</b>	<b>9</b>
<b>4.1. Installation des fonctionnalités sur le serveur principale .....</b>	<b>9</b>
<b>4.1.1. AD DS .....</b>	<b>16</b>
<b>4.1.2. DNS .....</b>	<b>18</b>
<b>4.1.3. Création des Unités d'organisation .....</b>	<b>21</b>
<b>4.1.4. Installation de LAPS .....</b>	<b>23</b>
<b>4.2. Installation du serveur WSUS.....</b>	<b>27</b>
<b>4.2.1. Configuration des stratégies de groupe pour les mises à jour .....</b>	<b>40</b>
<b>4.3. Configuration de LAPS .....</b>	<b>49</b>
<b>4.3.1. Installation de LAPS sur le contrôleur de domaine .....</b>	<b>49</b>
<b>4.3.2. Configuration de la GPO LAPS.....</b>	<b>52</b>
<b>4.3.3. Déploiement de LAPS par GPO.....</b>	<b>57</b>
<b>5. Perspectives et améliorations futures .....</b>	<b>61</b>
<b>6. Conclusion.....</b>	<b>62</b>

## LISTE DES FIGURES

Figure 1 Informations système .....	9
Figure 2 Paramètres système avancés .....	10
Figure 3 Modification du nom .....	10
Figure 4 Vérification des configurations réseau.....	11
Figure 5 Paramètres de la carte réseau .....	11
Figure 6 Sélection de la carte réseau.....	12
Figure 7 Propriétés de la carte réseau.....	12
Figure 8 Sélection du protocole TCP/IPv4.....	13
Figure 9 Modification des paramètres réseau .....	13
Figure 10 Ajout de rôles et fonctionnalités .....	14
Figure 11 Sélection des rôles.....	14
Figure 12 Fin de l'installation.....	15
Figure 13 Vérification des rôles .....	15
Figure 14 Promotion en contrôleur de domaine.....	16
Figure 15 Nom du domaine.....	16
Figure 16 Mot de passe de l'annuaire .....	17
Figure 17 Sélection du DNS.....	18
Figure 18 Vérification de la zone de recherche directe.....	18
Figure 19 Zone de recherche inversée.....	19
Figure 20 ID réseau .....	19
Figure 21 Nouveau pointeur.....	20
Figure 22 Vérification du DNS .....	20
Figure 23 Sélection du menu.....	21
Figure 24 Création de l'unité d'organisation.....	21
Figure 25 Nom de l'unité d'organisation .....	22
Figure 26 Unité d'organisation créé.....	22
Figure 27 Téléchargement de LAPS .....	23
Figure 28 Sélection de la langue .....	23
Figure 29 Sélection de la version .....	24
Figure 30 Assistant d'installation de LAPS .....	24
Figure 31 Condition d'utilisation de LAPS .....	25
Figure 32 Sélection des fonctionnalités .....	25

Figure 33 Début de l'installation de LAPS .....	26
Figure 34 Fin de l'installation de LAPS .....	26
Figure 35 Modification du DNS.....	27
Figure 36 Intégration au domaine .....	27
Figure 37 Connexion au compte dédié dans le domaine.....	28
Figure 38 Sélection du rôle WSUS .....	28
Figure 39 Emplacement des mises à jour.....	29
Figure 40 Configuration post-déploiement .....	29
Figure 41 Sélection des services WSUS .....	30
Figure 42 Assistant d'installation.....	30
Figure 43 Programme d'amélioration de WSUS .....	31
Figure 44 Choix d'un serveur en amont .....	31
Figure 45 Choix du serveur proxy.....	32
Figure 46 Téléchargement des informations via Microsoft Update .....	32
Figure 47 Fin du téléchargement des informations de mise à jour .....	33
Figure 48 Choix des langues .....	33
Figure 49 Choix des produits .....	34
Figure 50 Choix du type de mises à jour.....	34
Figure 51 Planification de la synchronisation .....	35
Figure 52 Lancement de la synchronisation initiale.....	35
Figure 53 Vérification de l'état de synchronisation.....	36
Figure 54 Ajout de groupe d'ordinateurs .....	36
Figure 55 Création de groupes d'ordinateurs.....	37
Figure 56 Visualisation des mises à jour .....	37
Figure 57 Sélection et approbation des mises à jour .....	38
Figure 58 Approuver les mises à jour.....	38
Figure 59 Héritage de l'installation .....	39
Figure 60 Fin de l'approbation des mises à jour .....	39
Figure 61 Avancement des mises à jour .....	40
Figure 62 Sélection des stratégies de groupe .....	40
Figure 63 Création de la GPO .....	41
Figure 64 Nom de la GPO.....	41
Figure 65 Modification de la GPO .....	42
Figure 66 Modification de la GPO .....	42

Figure 67 Sélection de Windows Update .....	43
Figure 68 Emplacement du serveur WSUS.....	43
Figure 69 Configuration du paramètre .....	44
Figure 70 Configuration du service Mises à jour automatique .....	44
Figure 71 Configuration du paramètre .....	45
Figure 72 Application de la GPO .....	45
Figure 73 Machines enregistrées sur le serveur .....	46
Figure 74 Création d'utilisateur .....	46
Figure 75 Nom d'utilisateur.....	47
Figure 76 Cr éation du mot de passe .....	47
Figure 77 Connexion à l'utilisateur cr éer .....	48
Figure 78 Import du module LAPS dans PowerShell .....	49
Figure 79 Ajout des attributs .....	49
Figure 80 Acc ès au mot de passe .....	50
Figure 81 Permission de lecture du mot de passe .....	50
Figure 82 Permission de r éinitialisation du mot de passe .....	51
Figure 83 Copie du Template d'administration de LAPS .....	52
Figure 84 Collage du Template d'administration de LAPS .....	52
Figure 85 Cr éation de la GPO .....	53
Figure 86 Nom de la GPO.....	53
Figure 87 Modification de la GPO .....	54
Figure 88 S élection du dossier LAPS .....	54
Figure 89 S élection du param ètre Password Settings .....	55
Figure 90 Password Settings .....	55
Figure 91 Activation du param ètre d'expiration .....	56
Figure 92 Activation du param ètre de mot de passe local.....	56
Figure 93 PArtage du package LAPS.....	57
Figure 94 Nouveau package d'installation .....	58
Figure 95 S élection du package d'installation .....	58
Figure 96 Validation de la GPO .....	59
Figure 97 Application de la GPO sur la machine cliente .....	59
Figure 98 V érification de l'installation de LAPS sur machine cliente .....	60
Figure 99 Ex cution de l'interface utilisateur de LAPS .....	60
Figure 100 Interface utilisateur de LAPS.....	61

## GLOSSAIRE

- **AD** (Active Directory) : Service d'annuaire développé par Microsoft pour les réseaux Windows. Il permet de centraliser la gestion des utilisateurs, des ordinateurs et des stratégies de sécurité.
- **AD DS** (Active Directory Domain Services) : Le rôle serveur principal qui exécute Active Directory, gérant les informations de l'annuaire et l'authentification des utilisateurs.
- **DNS** (Domain Name System) : Service qui traduit les noms de domaine (comme entreprise.local) en adresses IP compréhensibles par les machines.
- **DSRM** (Directory Services Restore Mode) : Mode de démarrage sécurisé d'un contrôleur de domaine utilisé pour la maintenance et la restauration.
- **GPO** (Group Policy Object / Objet de Stratégie de Groupe) : Un ensemble de paramètres de configuration qui sont appliqués de manière centralisée à des utilisateurs ou des ordinateurs dans un domaine Active Directory.
- **LAPS** (Local Administrator Password Solution) : Solution Microsoft qui gère et sécurise automatiquement les mots de passe des comptes administrateur locaux sur les machines jointes au domaine.
- **OU** (Organizational Unit / Unité d'Organisation) : Conteneur dans Active Directory utilisé pour organiser les objets (utilisateurs, groupes, ordinateurs) et leur appliquer des GPO de manière granulaire.
- **PTR** (Pointer Record) : Un type d'enregistrement DNS utilisé dans les zones de recherche inversée pour associer une adresse IP à un nom d'hôte.
- **WSUS** (Windows Server Update Services) : Service de mise à jour de Microsoft qui permet aux administrateurs de gérer et de déployer les correctifs de manière centralisée.

## 1. Contexte général du projet

Un parc informatique désigne l'ensemble des équipements, logiciels et réseaux qu'une organisation utilise pour fonctionner : ordinateurs, serveurs, routeurs, etc. Pour qu'il soit considéré comme sécurisé, il doit reposer sur plusieurs piliers : une gestion centralisée des identités (via Active Directory), une politique stricte de mots de passe, des mises à jour régulières et contrôlées des systèmes, une surveillance des accès privilégiés, et des sauvegardes fiables. Or, dans de nombreuses PME, on observe une : la persistance de mots de passe administrateur locaux identiques et statiques sur l'ensemble des machines, combinée à une absence de contrôle des correctifs de sécurité. Cette double vulnérabilité permet à un attaquant, après avoir compromis un seul poste, de se propager facilement à travers tout le réseau.

Pour remédier à cette situation, ce projet vise à construire les fondations d'une infrastructure moderne, sécurisée et centralisée en déployant les technologies Microsoft core : un domaine **Active Directory** pour la gestion des identités, **LAPS** (Local Administrator Password Solution) pour sécuriser les accès privilégiés locaux, et **WSUS** (Windows Server Update Services) pour maîtriser le cycle de vie des correctifs. L'ensemble sera orchestré de manière cohérente et automatisée via les **Stratégies de Groupe** (GPO).

Face à ce constat, la mise en œuvre d'une solution adaptée s'imposait, guidée par des objectifs opérationnels clairs.

## 2. Objectifs du projet

Pour concrétiser cette vision, le projet poursuit un objectif principal, décliné en plusieurs objectifs spécifiques :

- **L'objectif principal**

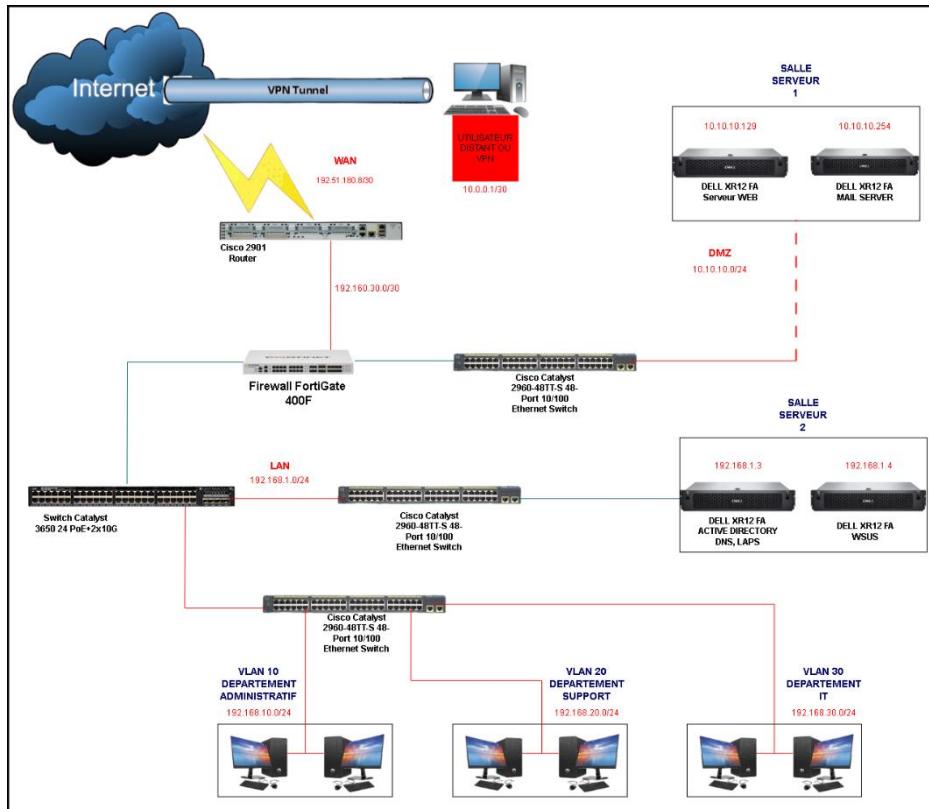
Il est de concevoir et déployer une infrastructure centralisée, sécurisée et automatisée pour répondre aux enjeux de gouvernance et de cybersécurité.

- **Objectifs spécifiques :**

1. **Centraliser la gestion** en installant et configurant un domaine Active Directory.
2. **Sécuriser les accès privilégiés** en déployant LAPS pour automatiser la rotation des mots de passe administrateur locaux.
3. **Contrôler la maintenance corrective** en mettant en place un serveur WSUS et en configurant les postes clients pour qu'ils s'y approvisionnent via des GPO.

4. Documenter l'architecture et les procédures pour assurer la reprise et la pérennité de la solution.

### 3. Architecture du système



L'architecture mise en œuvre repose sur une topologie centralisée autour d'un **contrôleur de domaine (AD / DNS)** qui assure la gestion des identités, des stratégies de groupe et la solution **LAPS** pour la rotation automatique des mots de passe administrateur locaux. Un **serveur WSUS** est dédié à la gestion et à la distribution des mises à jour Windows au sein du réseau interne.

Le projet a été déployé sur une infrastructure reposant sur **Windows Server 2019**, avec une répartition claire et cohérente des rôles. Le serveur **DC01** joue le rôle de **contrôleur de domaine (AD DS)**, de **serveur DNS**, et d'hôte de la solution **LAPS**, tandis que le serveur **WSUS** est exclusivement dédié à la gestion centralisée des mises à jour.

Les postes de travail, répartis par département, fonctionnent sous **Windows 10 Professionnel version 22H2** et sont tous rejoints au domaine, leur permettant d'hériter automatiquement des stratégies de groupe configurant les paramètres LAPS et WSUS.

L'ensemble des serveurs et des postes clients sont connectés via un **switch Cisco Catalyst 2960**, lui-même protégé par un **pare-feu FortiGate 400F** qui assure la sécurité périphérique et le filtrage du trafic entre Internet et le réseau local (192.168.1.0/24).

Les **postes clients**, répartis par département (Support, IT, Sécurité, Secrétariat), communiquent avec le contrôleur de domaine pour l'authentification et appliquent automatiquement les mises à jour et politiques configurées via les **GPO**.

Cette architecture garantit à la fois **centralisation, sécurité et automatisation** dans la gestion du parc informatique.

## 4. Manuel de déploiement

Dans cette partie, nous allons détailler le processus d'installation et de mise en place de ce projet.

### 4.1. Installation des fonctionnalités sur le serveur principale

Nous allons commencer par changer le nom de la machine et son adresse IP. Commençons par le nom.

Allons dans **Paramètres > Système** et tout en bas de la partie gauche, cliquons sur « **Informations système** » puis sur **Paramètre avancés du système**

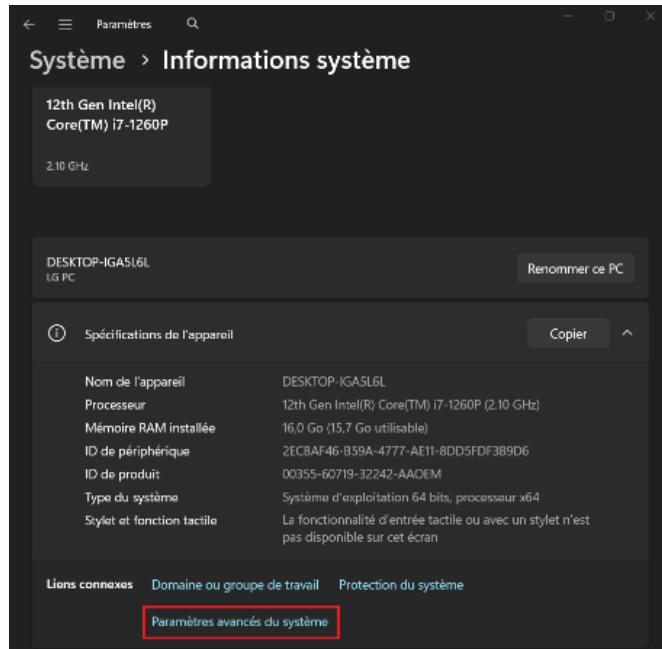


Figure 1 Informations système

Dans la liste des onglets, cliquons sur **Nom de l'ordinateur** puis sur **Modifier**. On pourra alors renseigner le nom de l'appareil dans la partie correspondante.

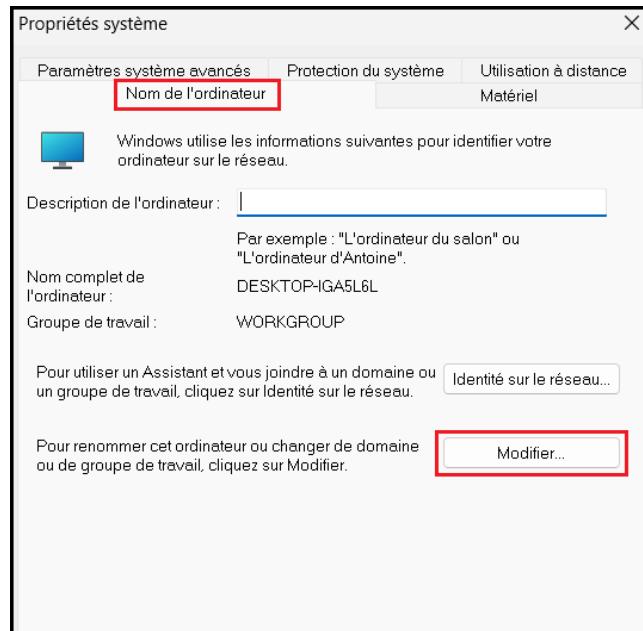


Figure 2 Paramètres système avancés

Dans la partie correspondante, renseignons le nom de l'ordinateur

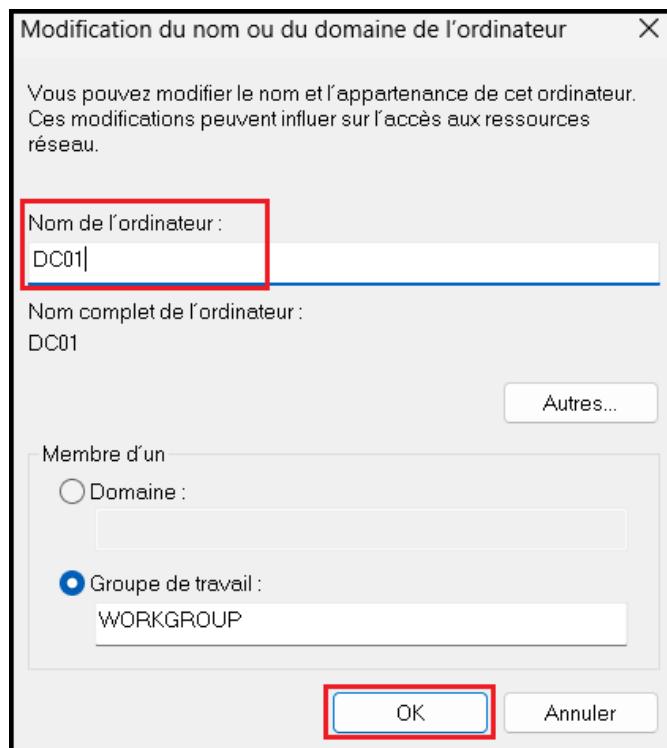


Figure 3 Modification du nom

Après redémarrage nous allons adresser statiquement le serveur. Dans l'invite de commande, tapons la commande « **ipconfig** ». Ça nous permettra de voir l'adresse IP attribuée et de la rendre statique.

```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.17763.7792]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 192.168.1.3
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.2

C:\Users\Administrateur>
```

Figure 4 Vérification des configurations réseau

Rendons-nous dans le **Panneau de configuration** et cliquons sur **Réseau et Internet**. Dans la page qui s'ouvre cliquons sur **Modifier les paramètres de la carte**

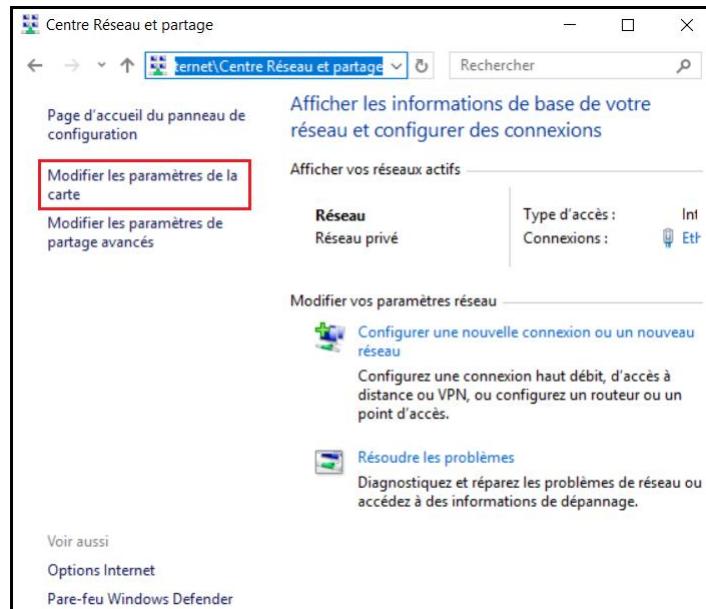


Figure 5 Paramètres de la carte réseau

Cliquons sur la carte réseau qui nous intéresse, ici la carte **Ethernet**

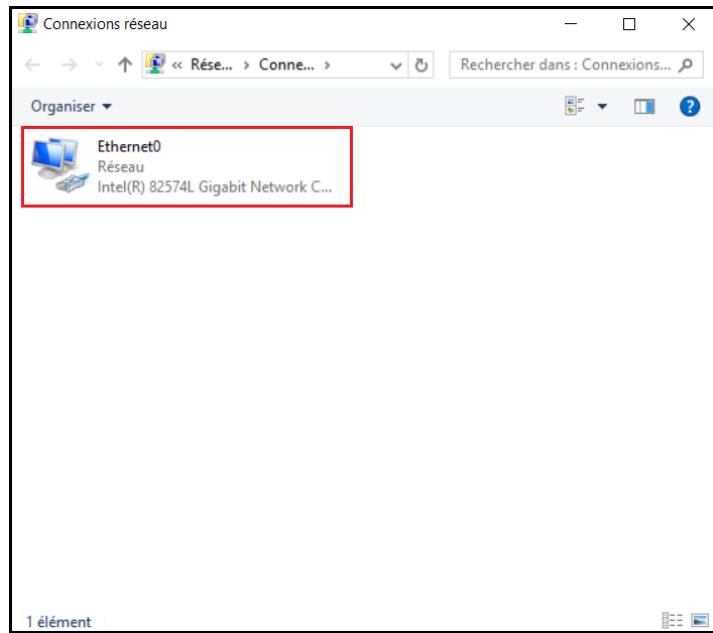


Figure 6 Sélection de la carte réseau

Ensuite cliquons sur **Propriétés**

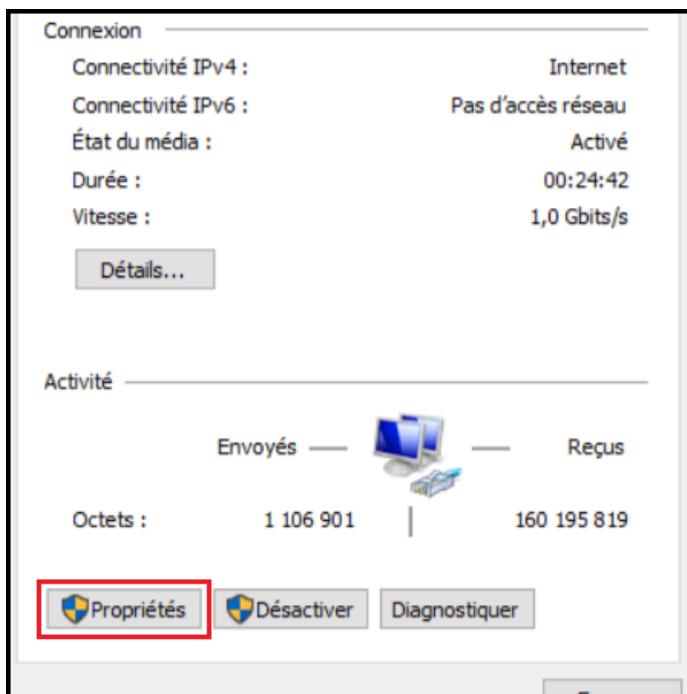


Figure 7 Propriétés de la carte réseau

Sélectionnons **Protocole Internet version 4 (TCP/IPv4)**

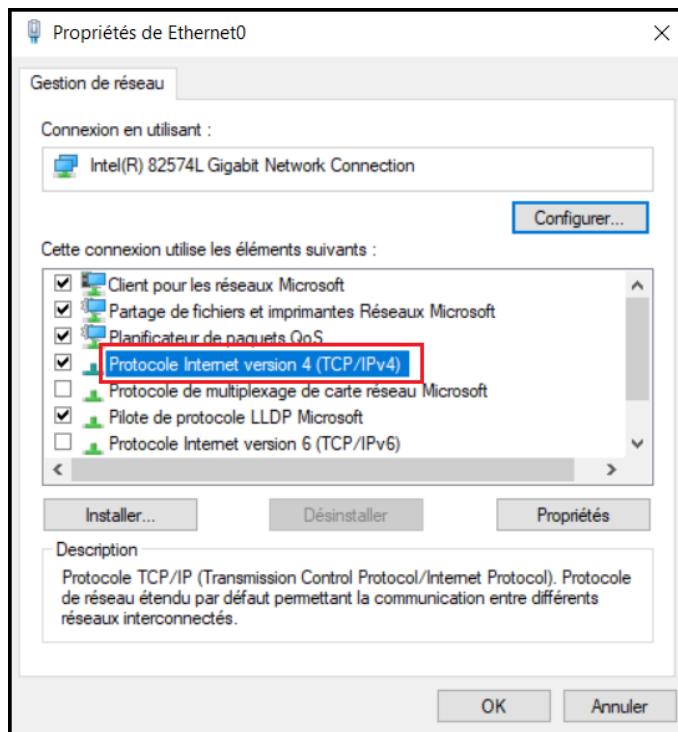


Figure 8 Sélection du protocole TCP/IPv4

On sélectionne **Utiliser l'adresse IP suivante** et on renseigne les informations correspondantes

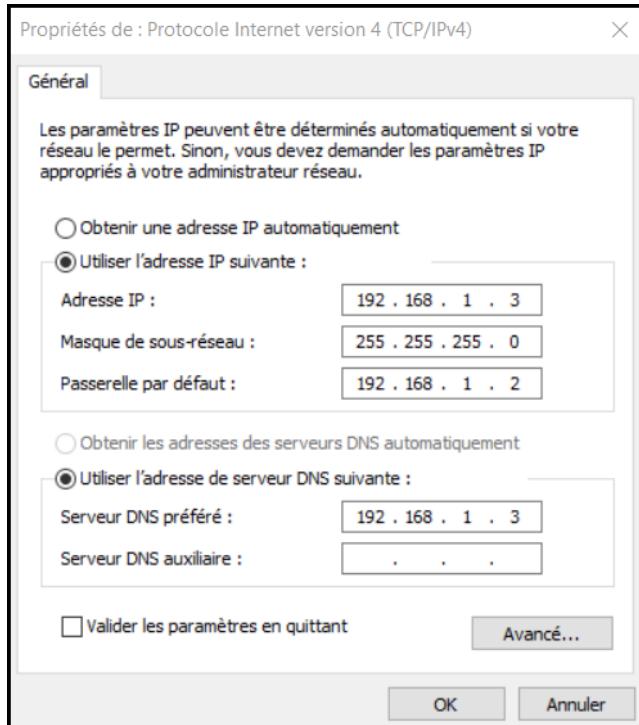


Figure 9 Modification des paramètres réseau

Nous pouvons maintenant commencer l'installation des rôles et des fonctionnalités du serveur, notamment **AD DS** et **DNS**.

Dans le gestionnaire de serveur, tout en haut, cliquons sur **Gérer** puis sur **Ajouter des rôles et fonctionnalités**.

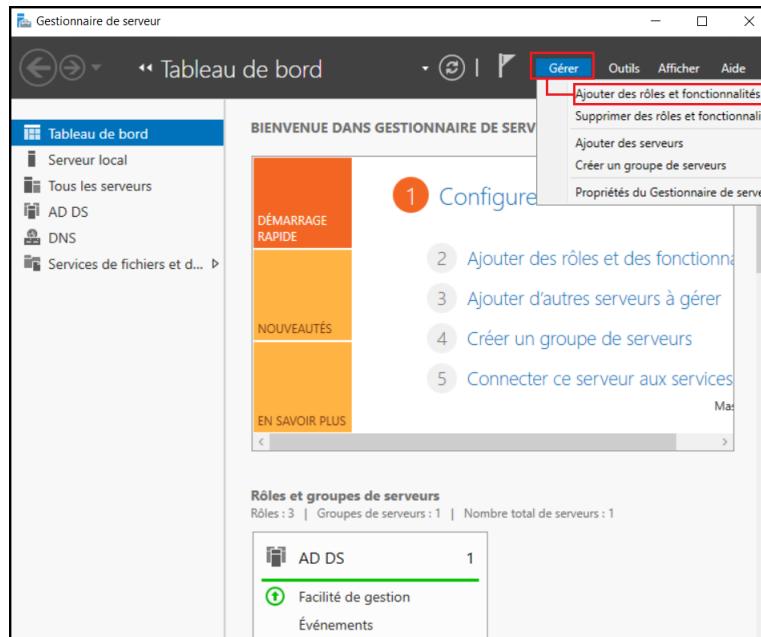


Figure 10 Ajout de rôles et fonctionnalités

Dans la fenêtre qui s'ouvre cliquons sur suivant jusqu'à la sélection des fonctionnalités ou des rôles qu'on veut sur le serveur, en l'occurrence ici **AD DS** et **DNS** puis **Suivant**.

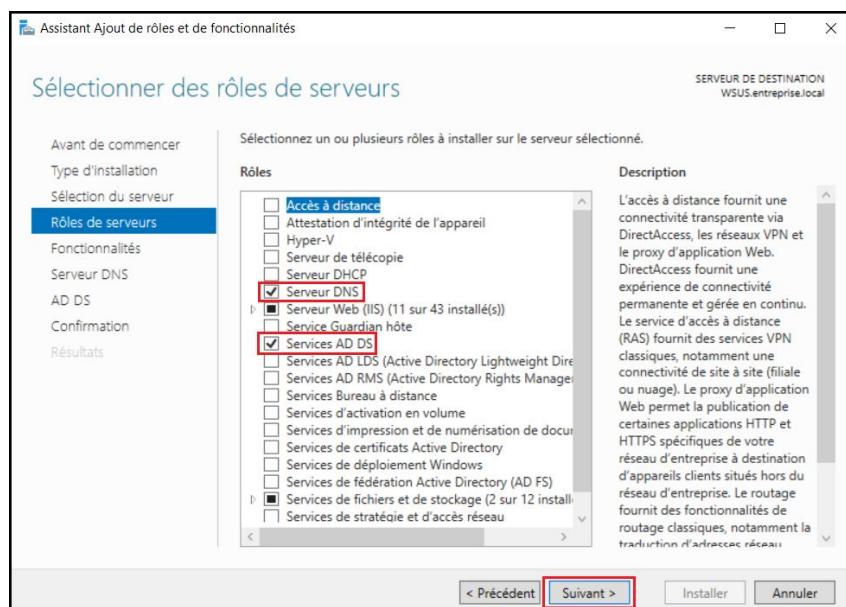


Figure 11 Sélection des rôles

Cliquons ensuite sur suivant jusqu'à l'installation et une fois cette dernière terminée, nous pouvons fermer la fenêtre.

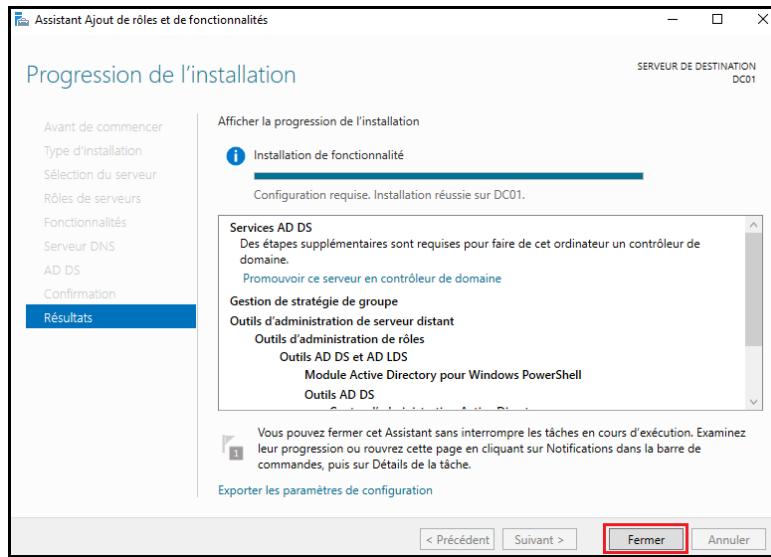


Figure 12 Fin de l'installation

Nous pouvons voir dans le tableau de bord que les rôles ont été correctement installer.

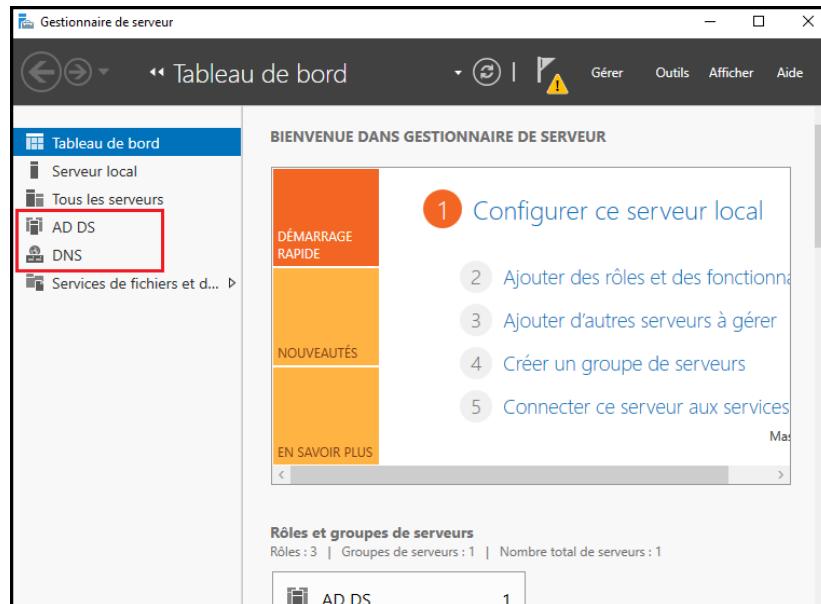


Figure 13 Vérification des rôles

### 4.1.1. AD DS

Nous allons maintenant promouvoir le serveur en contrôleur de domaine ce qui va nous permettre de gérer efficacement les utilisateurs et leurs postes clients.

Un drapeau avec un panneau jaune devrait apparaître. Cliquons dessus puis sur **Promouvoir ce serveur en contrôleur de domaine**

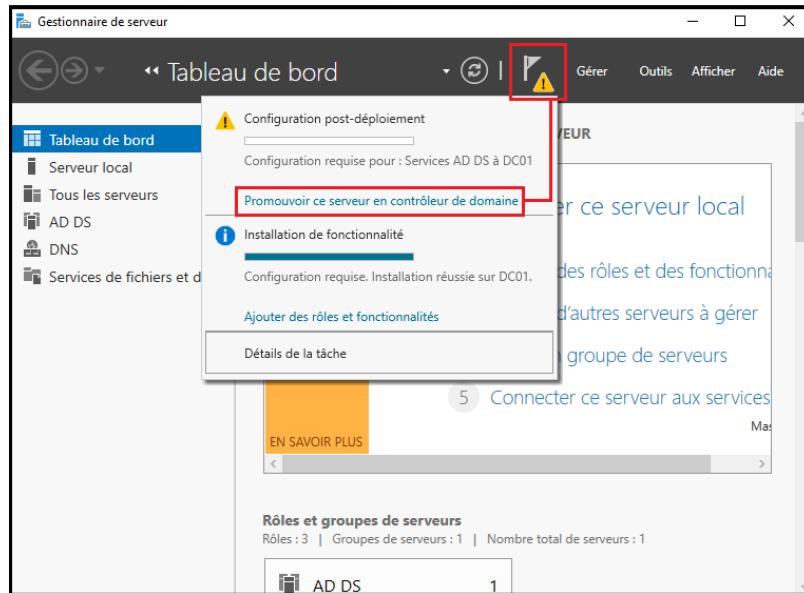


Figure 14 Promotion en contrôleur de domaine

Dans la fenêtre qui s'ouvre, sélectionnons **Ajouter une nouvelle forêt** et entrons le nom de notre domaine, ici « **entreprise.local** » puis sur **suivant**.

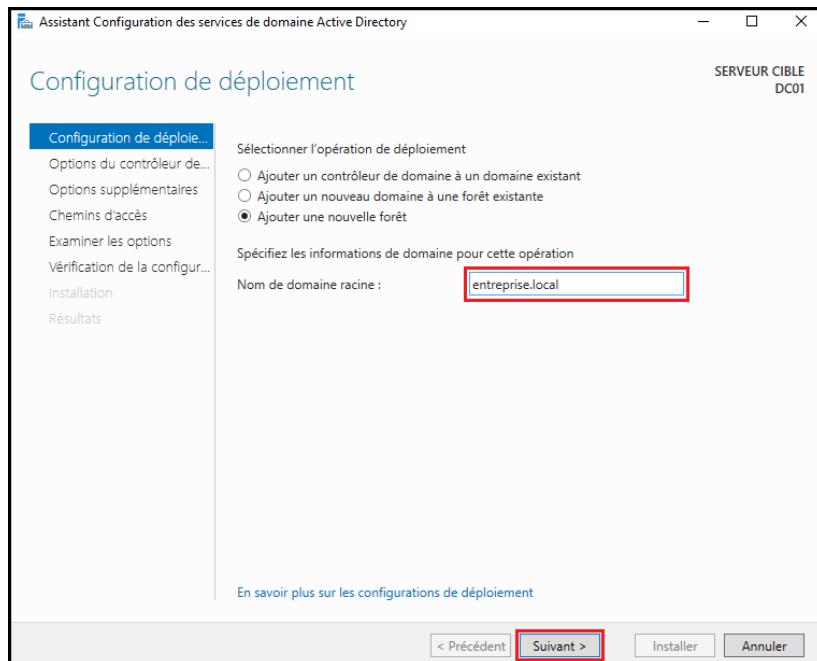


Figure 15 Nom du domaine

Nous allons maintenant mettre un mot de passe fort pour le mode de restauration des services d'annuaire. les critères sont :

- Une lettre majuscule (A-Z)
- Une lettre minuscule (a-z)
- Un chiffre (1-9)
- Un caractère spécial (@, &, ~)

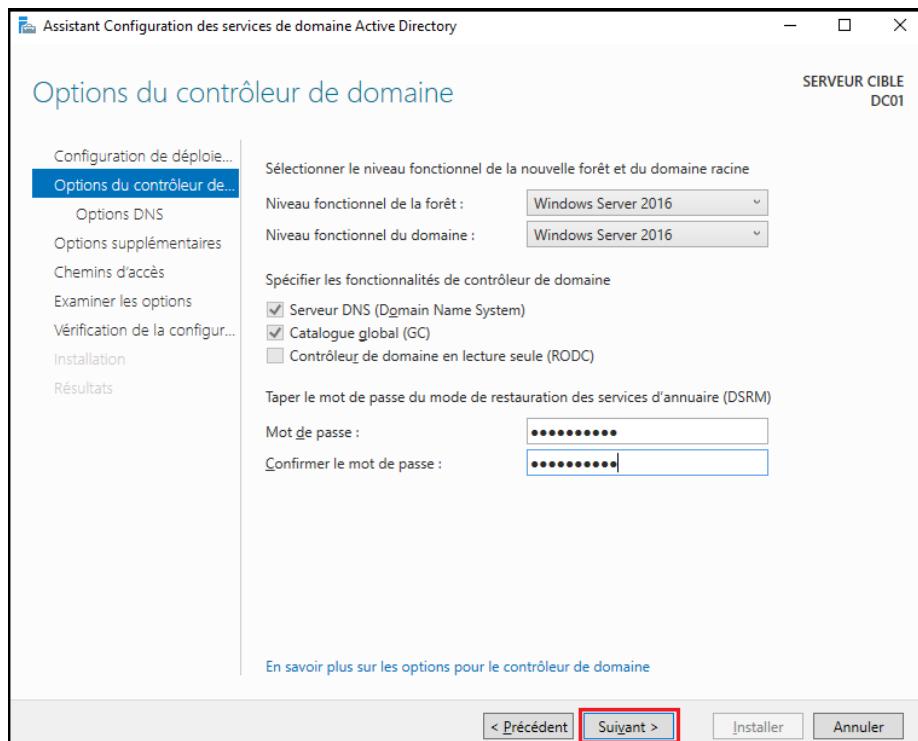


Figure 16 Mot de passe de l'annuaire

On clique ensuite sur **Suivant** jusqu'à ce que l'installation ne se termine.

## 4.1.2. DNS

Nous allons maintenant configurer le serveur DNS

Dans **Outils** cliquons sur **DNS**

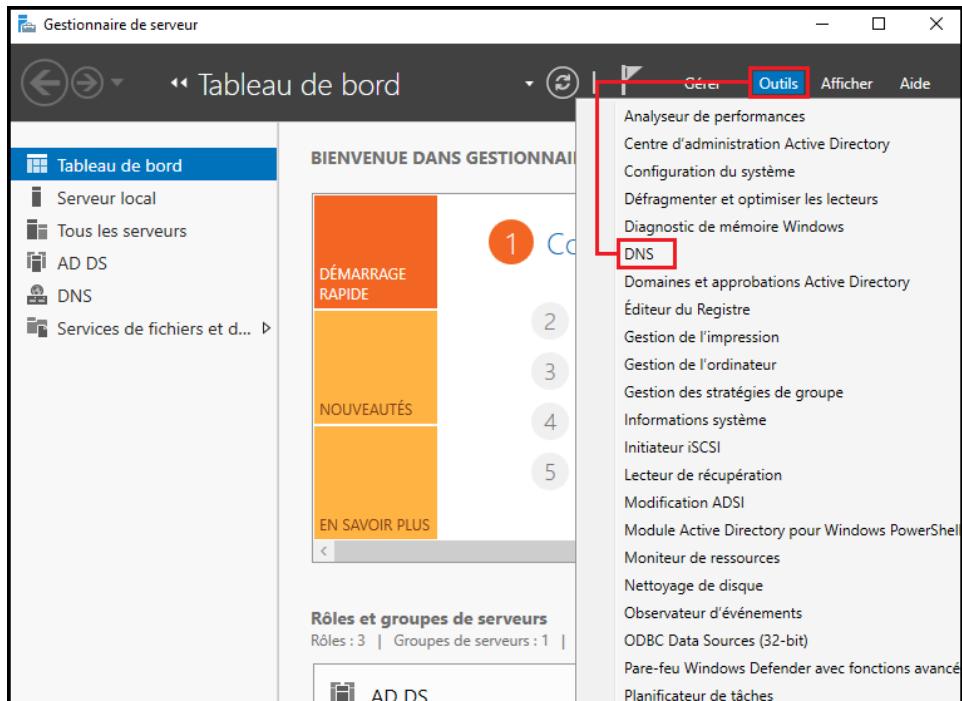


Figure 17 Sélection du DNS

Nous allons vérifier si le rôle à bien été pris en compte. En développant l'arborescence, allons dans **Zones de recherches directe** puis sur le nom de notre forêt qu'on a créé précédemment ici c'est **entreprise.local**. Nous voyons ici le nom de notre machine ce qui prouve que ça a marché.

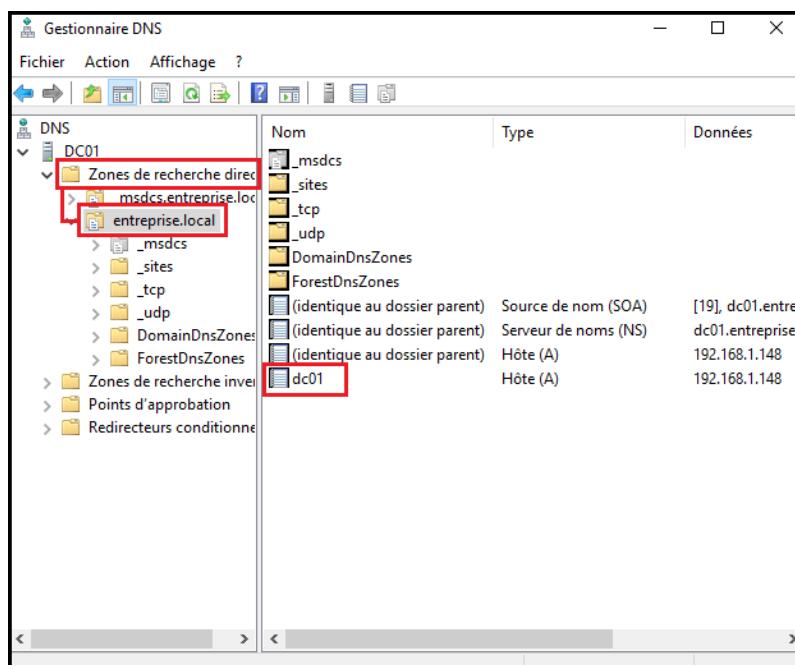


Figure 18 Vérification de la zone de recherche directe

Vérifications faites, nous allons donc commencer à configurer le serveur DNS.

Faisons un clic droit sur **Zone de recherche inversée** et sélectionnons **Nouvelle zone** et suivons l'assistant d'installation. Sélectionnons **Zone principale** et ensuite suivant.

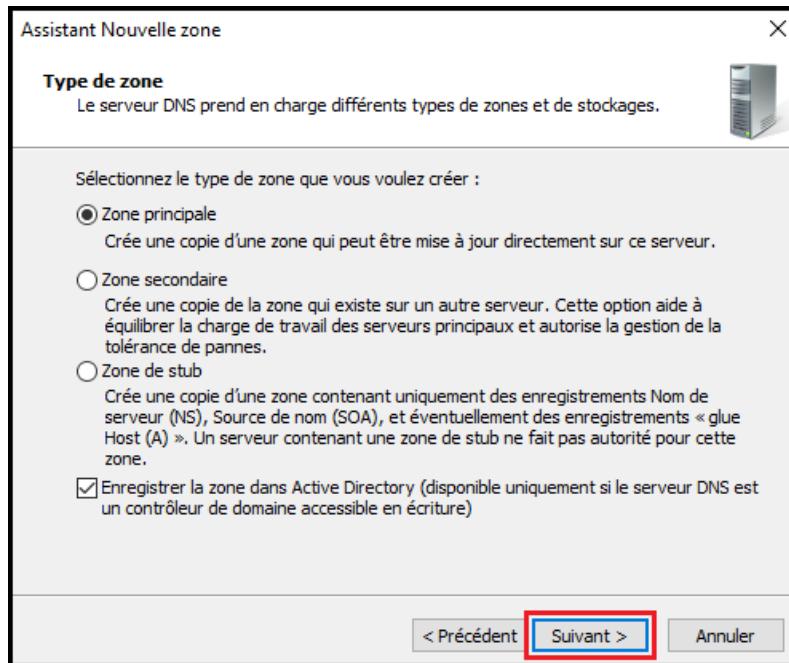


Figure 19 Zone de recherche inversée

Mettons la partie réseau de l'adresse IP de notre serveur et cliquons sur suivant jusqu'à la fin de l'ajout de la nouvelle zone.

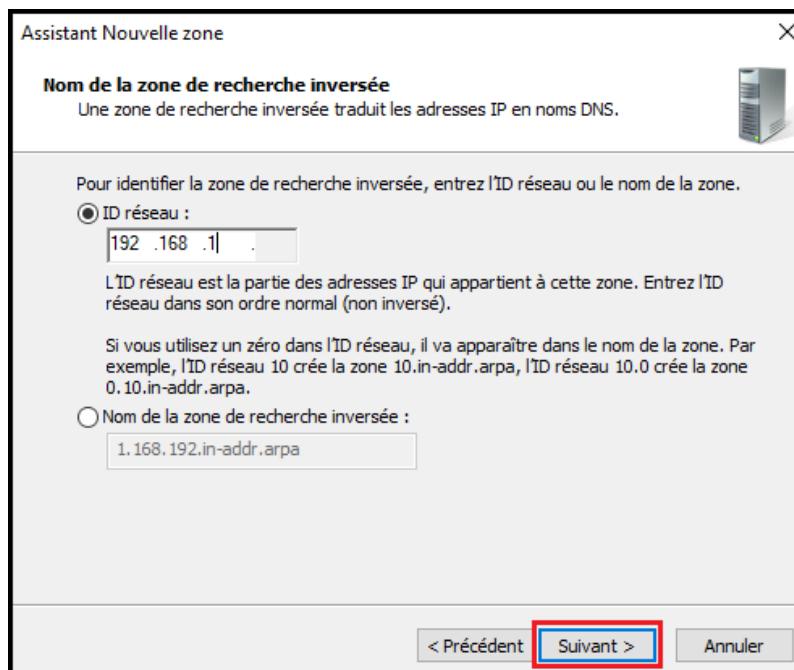


Figure 20 ID réseau

Dans la nouvelle zone de recherche inversée, nous allons définir un enregistrement PTR (pointeur) afin d'associer l'adresse IP au nom d'hôte. **Clic droit** sur la nouvelle zone et on sélectionne **nouveau pointeur**. On renseigne l'adresse IP et le nom du serveur DNS et ensuite sur OK.

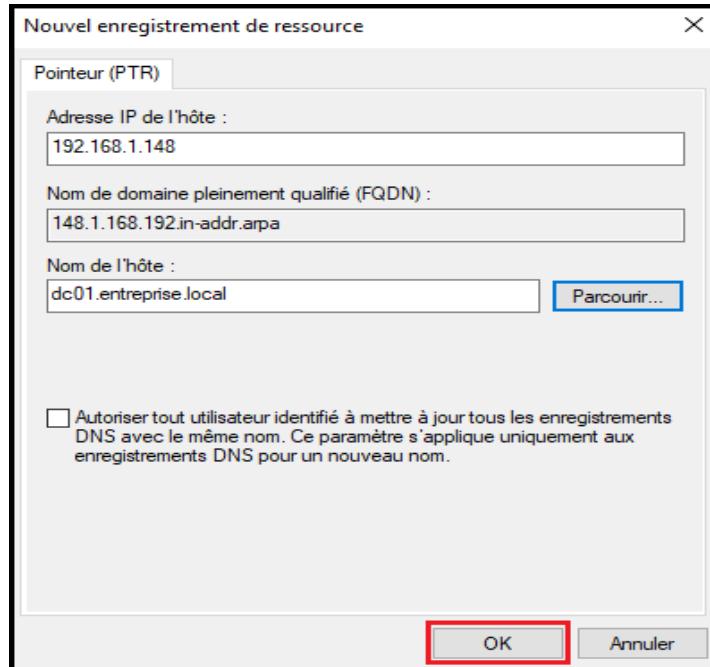


Figure 21 Nouveau pointeur

Pour vérifier que les configurations ont bien été prises en compte et que le serveur DNS est accessible, on va taper dans **l'Invite de commande** la commande « **nslookup** » qui devrait nous retourner le nom du serveur comme suit :

```
Administrator : Invite de commandes - nslookup
Microsoft Windows [version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>nslookup
Serveur par défaut : DC01.entreprise.local
Address: 192.168.1.148

>
```

Figure 22 Vérification du DNS

C'est bon, le DNS est correctement configuré.

### 4.1.3. Création des Unités d'organisation

Créons des Unités d'organisation pour différencier le différents utilisateurs.

Dans le gestionnaire de serveur, cliquons sur **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**

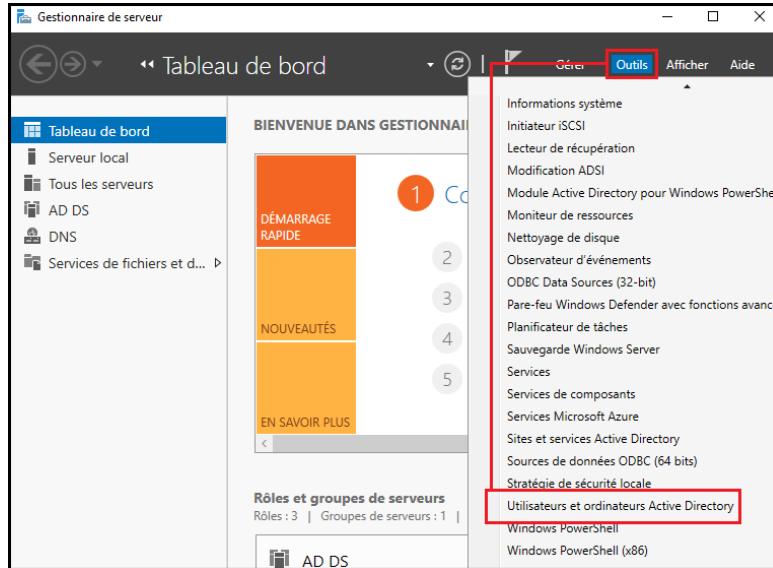


Figure 23 Sélection du menu

Faisons clic droit sur le nom de notre domaine, ensuite sur **Nouveau** et sur **Unité d'organisation**

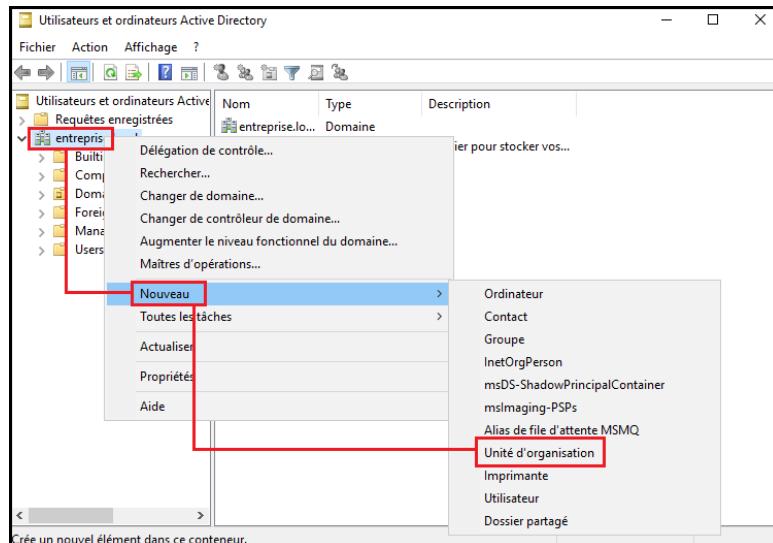


Figure 24 Création de l'unité d'organisation

Renseignons le nom de l'unité d'organisation et validons.

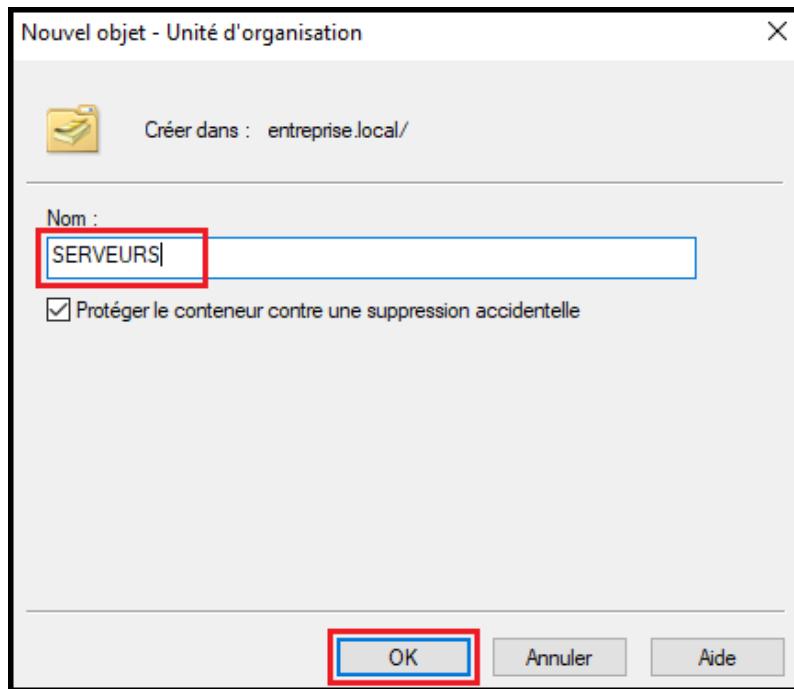


Figure 25 Nom de l'unité d'organisation

Nous avons créé trois unités d'organisation et des utilisateurs dans chaque unité d'organisation.

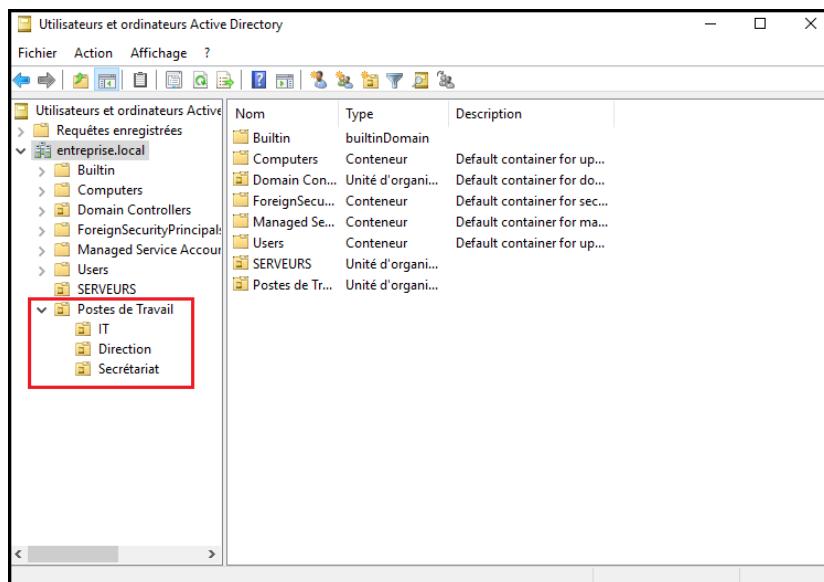


Figure 26 Unité d'organisation créé

#### 4.1.4. Installation de LAPS

Dans notre navigateur, entrons ce lien pour [Télécharger LAPS](#).

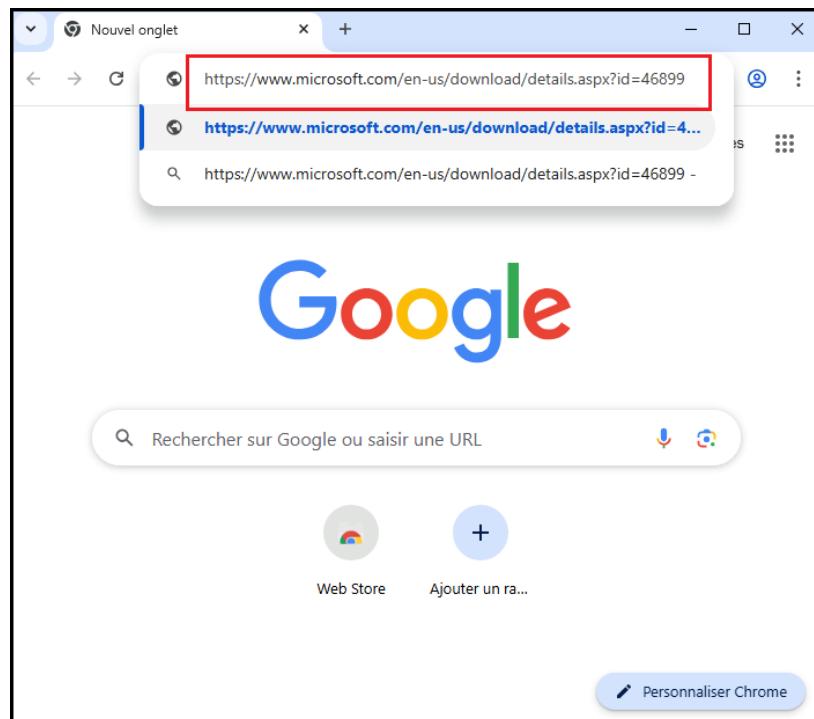


Figure 27 Téléchargement de LAPS

Sélectionnons la langue et cliquons sur le bouton **Download**

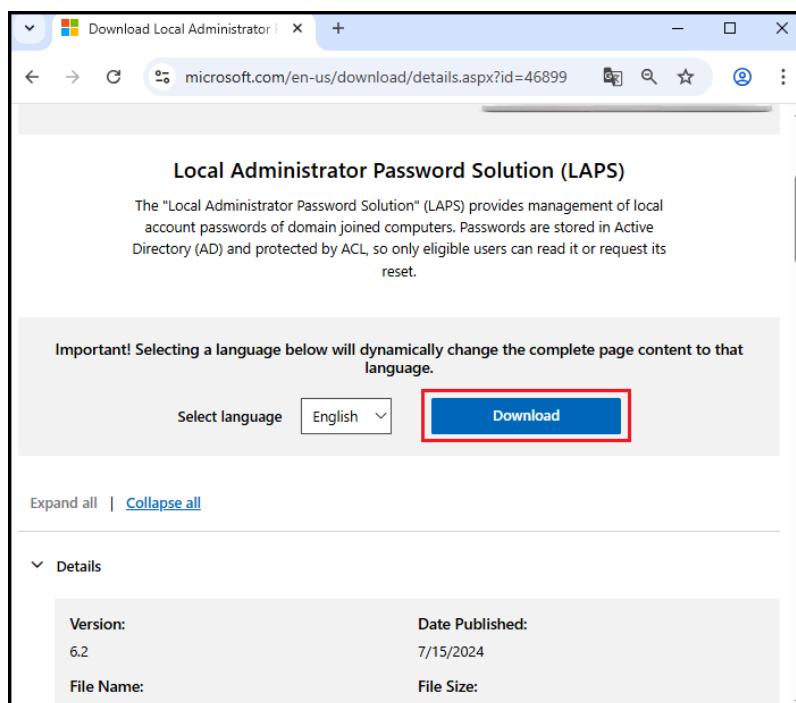


Figure 28 Sélection de la langue

Choisissons la version qui nous intéresse. **LAPS.x64.msi** pour les systèmes de version 64 bits et **LAPS.x86.msi** pour les 32 bits. La version qui nous intéresse ici c'est la version **LAPS.x64.msi**. Lançons donc l'installation.

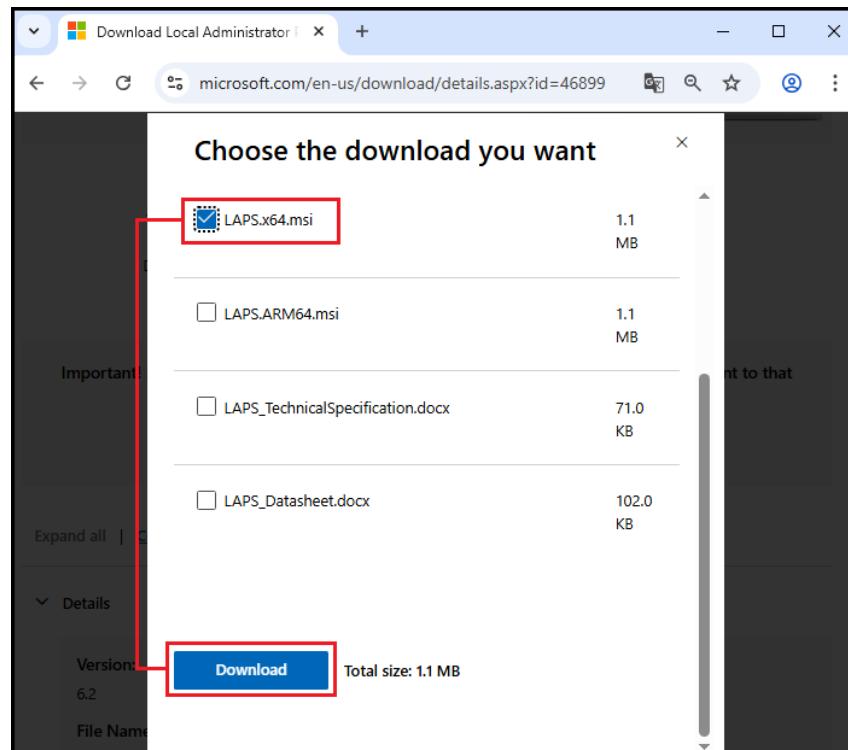


Figure 29 Sélection de la version

Lançons l'assistant d'installation.

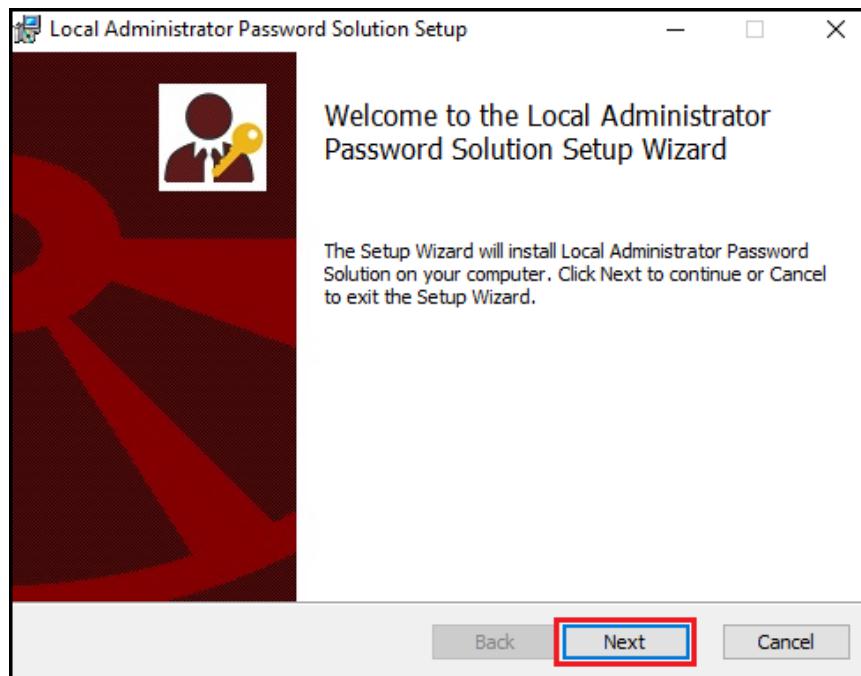


Figure 30 Assistant d'installation de LAPS

Après avoir lu les conditions d'utilisation, cochons la case et avançons.

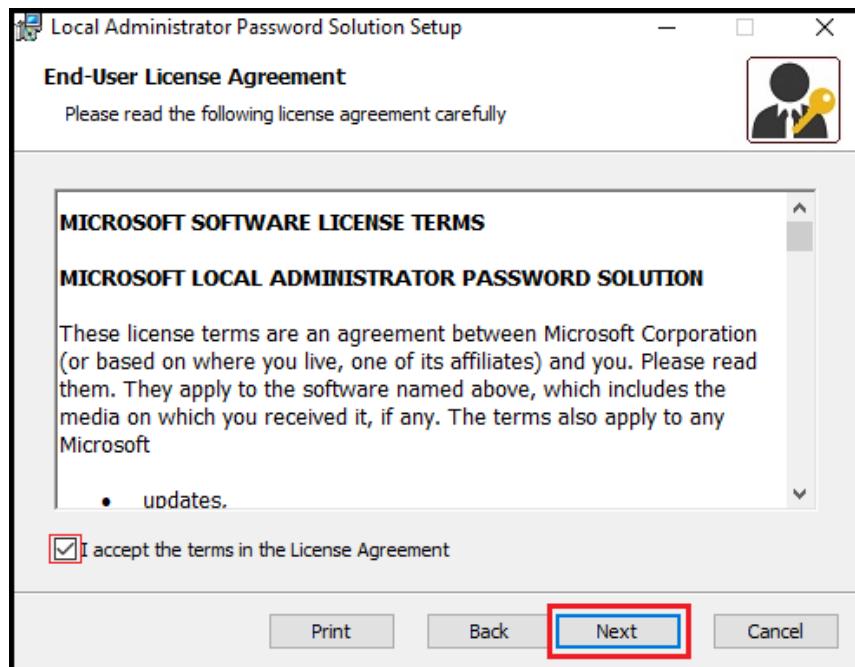


Figure 31 Condition d'utilisation de LAPS

Nous allons maintenant sélectionner ce que l'installateur va installer .

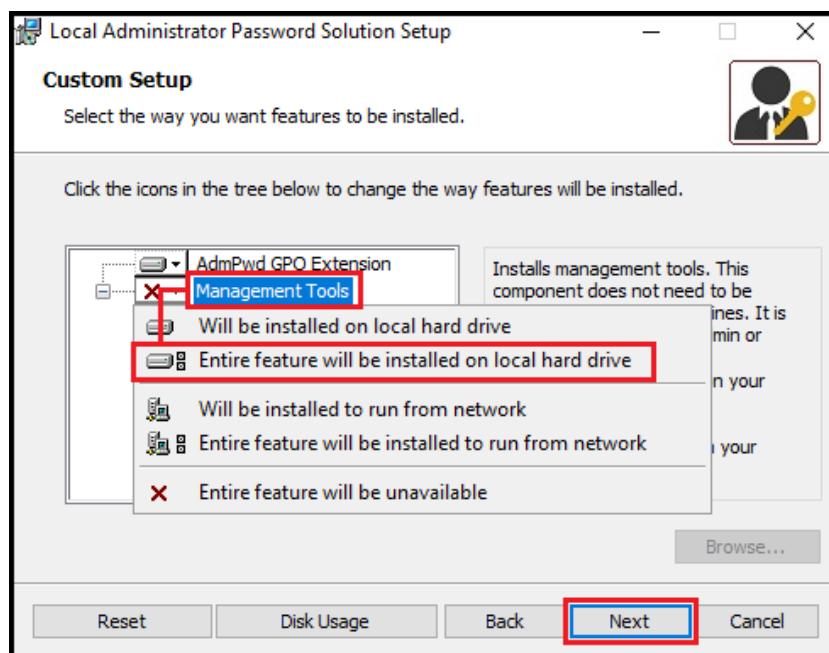


Figure 32 Sélection des fonctionnalités

Lançons l'installation

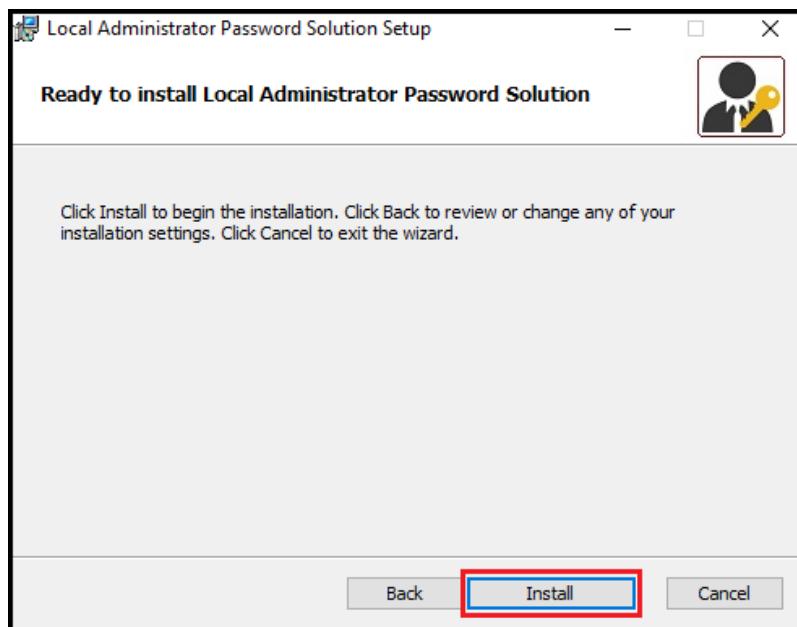


Figure 33 Début de l'installation de LAPS

Une fois l'installation terminée, fermons l'assistant.

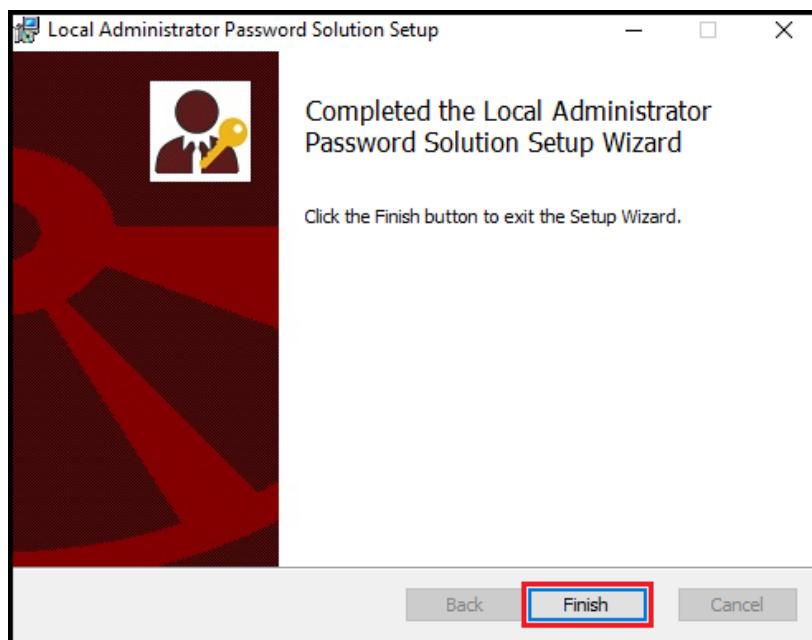


Figure 34 Fin de l'installation de LAPS

Nous allons revenir sur ce serveur pour configurer les stratégies de groupes mais pour l'instant passons au second serveur.

## 4.2. Installation du serveur WSUS

Avant d'ajouter le serveur au domaine, nous allons lui attribuer une adresse IP statique pointant vers notre serveur DNS. Dans **Panneau de configuration** cliquons sur **Réseau et Internet** puis sur **Centre réseau et partage**. Ensuite cliquons sur **Modifier les paramètres de la carte** et sélectionnons la carte correspondante. Ensuite cliquons sur **Propriété>TCP/IPv4** et dans la partie **DNS** et mettons l'adresse de notre serveur.

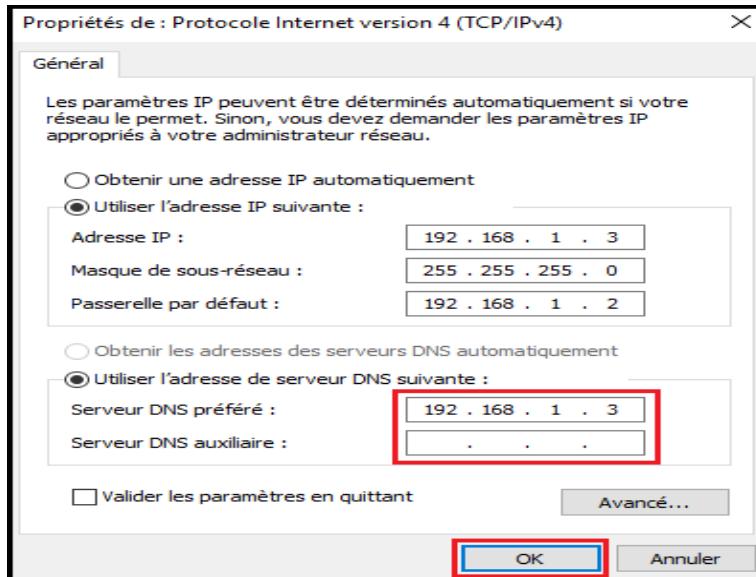


Figure 35 Modification du DNS

Nous pouvons maintenant ajouter cette machine au domaine et pour se faire nous allons suivre la même procédure que précédemment c'est-à-dire **Paramètre>Système>Information système>Paramètre système avancé>Nom de l'ordinateur>Modifier** et renseignons le nom de notre domaine, ici « **entreprise.local** »

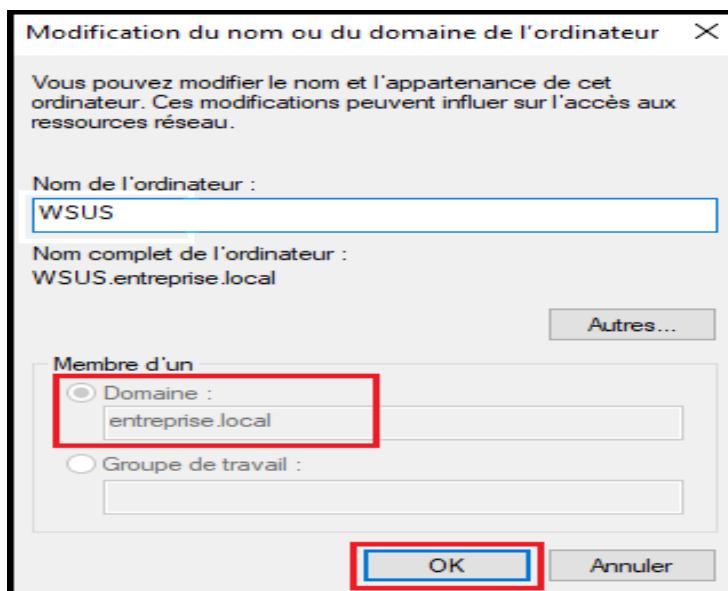


Figure 36 Intégration au domaine

Après redémarrage entrons les identifiant d'un compte autoriser à rejoindre le domaine.

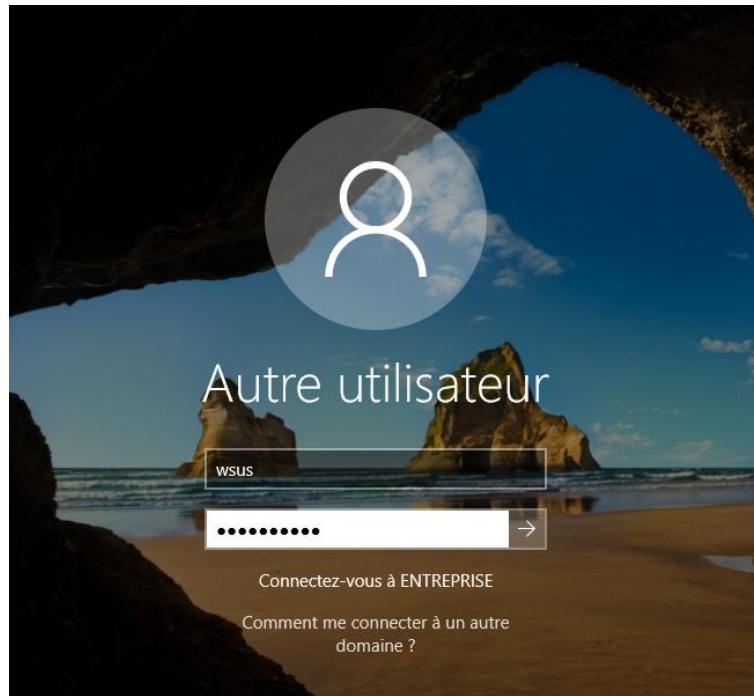


Figure 37 Connexion au compte dédié dans le domaine

Lançons le gestionnaire de serveurs. Dans **Gérer, Ajouter des rôles et des fonctionnalités** puis lors de la sélection du serveur choisissons le rôle **Services WSUS (Windows Server Update Services)**

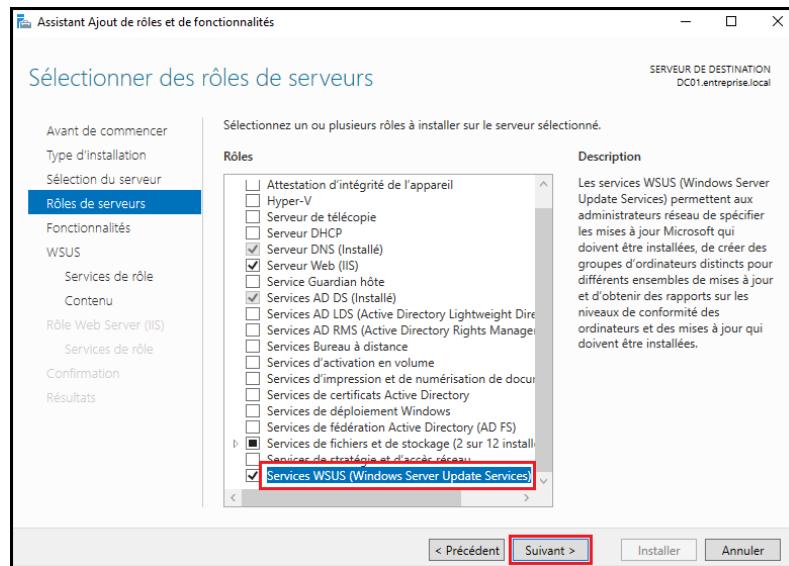


Figure 38 Sélection du rôle WSUS

Entrons l'emplacement où nous souhaitons que les mises à jour soient stockées puis installons le rôle.

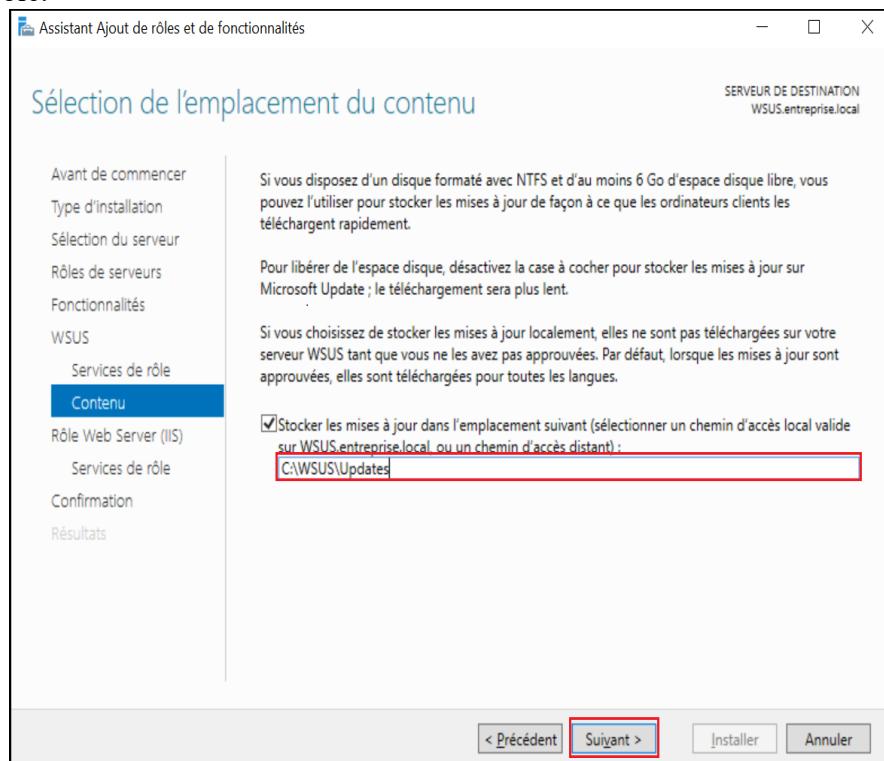


Figure 39 Emplacement des mises à jour

Après l'installation, lançons la configuration post-déploiement.

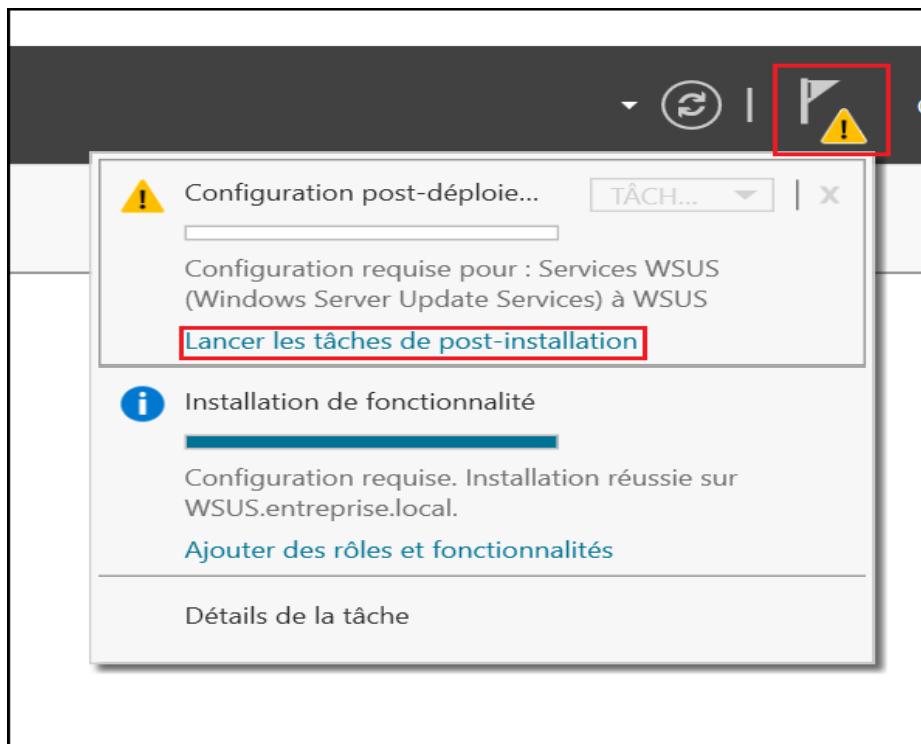


Figure 40 Configuration post-déploiement

Une fois la configuration terminée, rendons-nous-en haut à droite dans **Outils** puis en bas de liste cliquons sur **Services WSUS (Windows Server Update Services)**

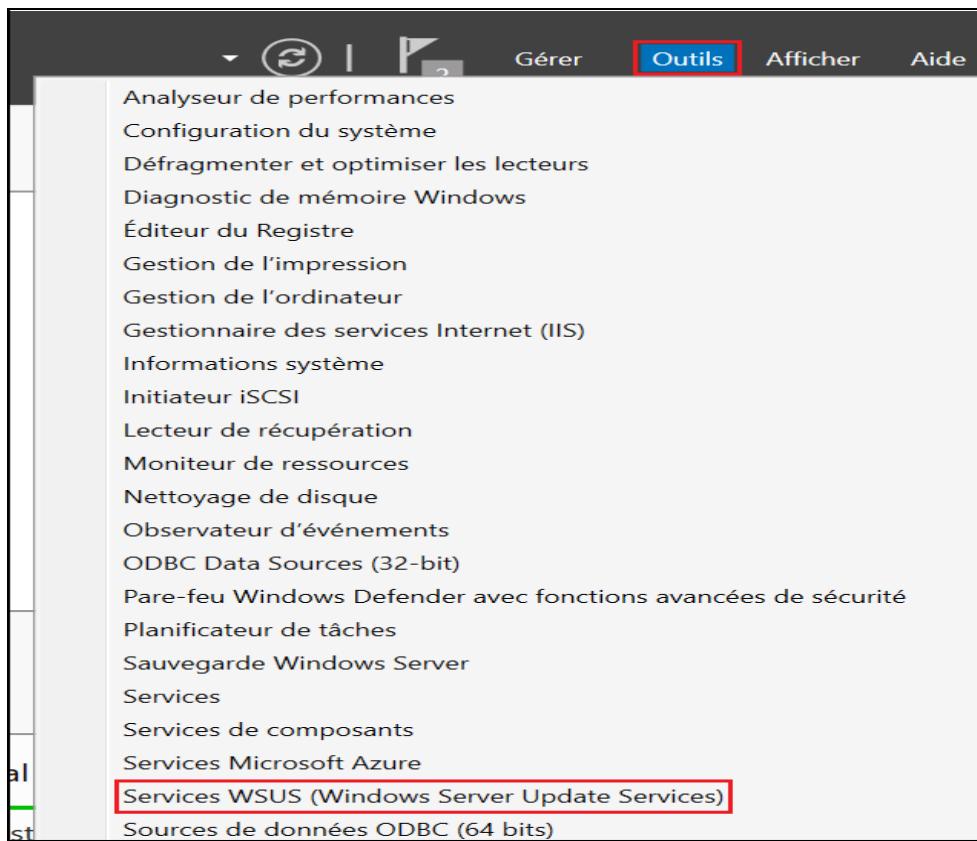


Figure 41 Sélection des services WSUS

Lançons l'assistant d'installation

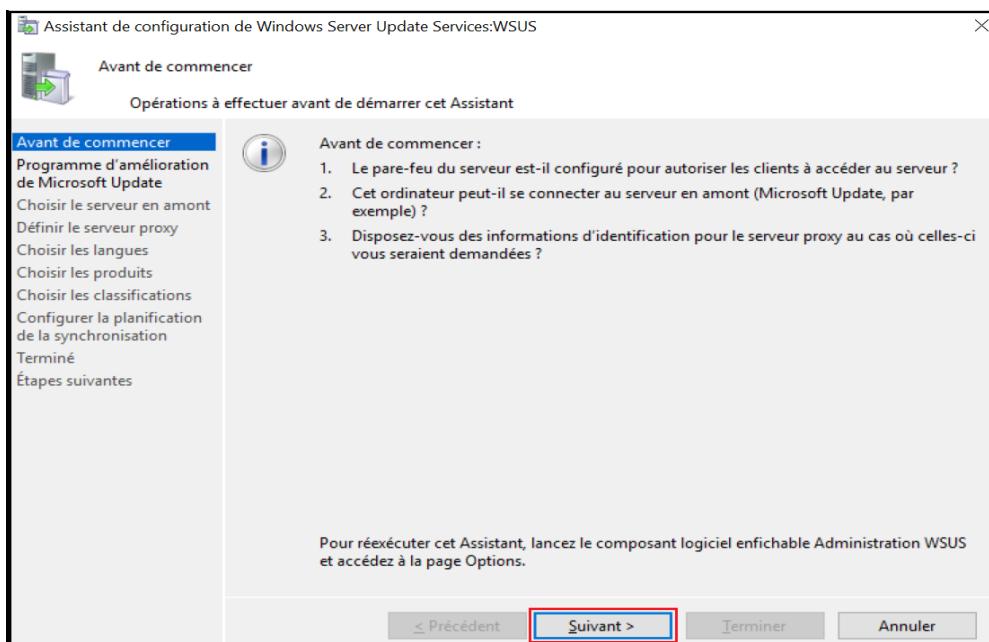


Figure 42 Assistant d'installation

Si vous voulez participer à l'amélioration de WSUS cochez la case et cliquons sur suivant

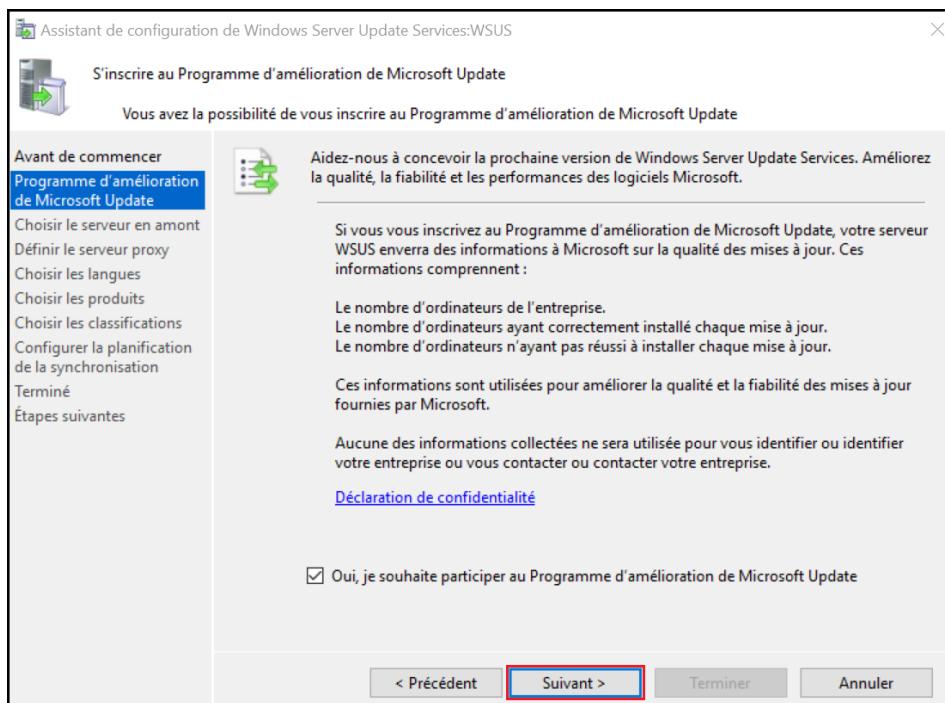


Figure 43 Programme d'amélioration de WSUS

Ici vu que c'est notre seul serveur WSUS nous allons sélectionner la première option

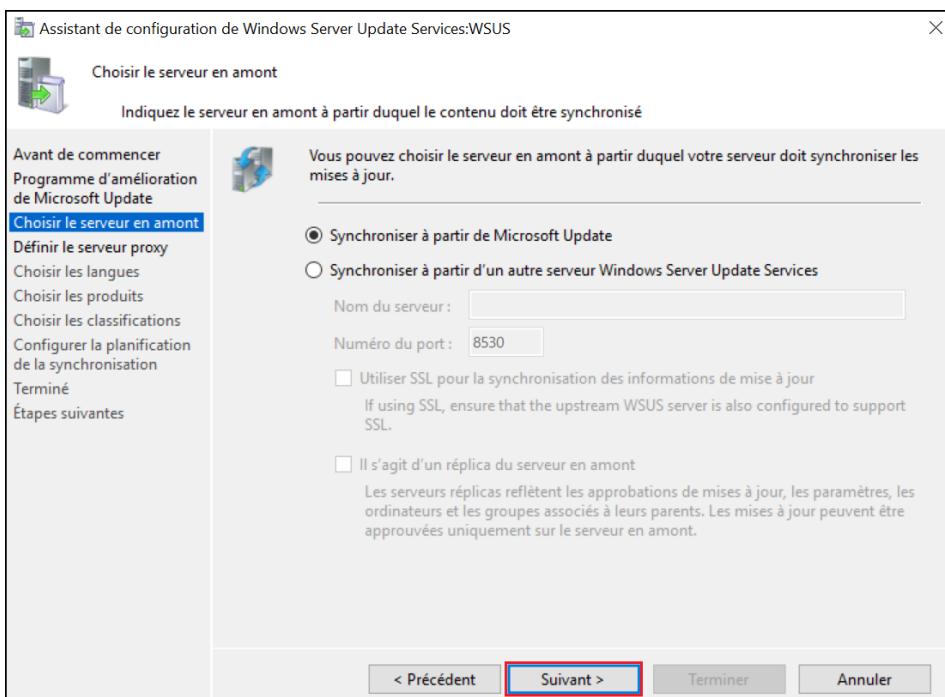


Figure 44 Choix d'un serveur en amont

Si nous avons un serveur proxy à utiliser lors de la synchronisation nous entrons ses coordonnées dans cette partie, au cas contraire cliquons juste sur suivant, c'est ce que nous faisons dans notre cas

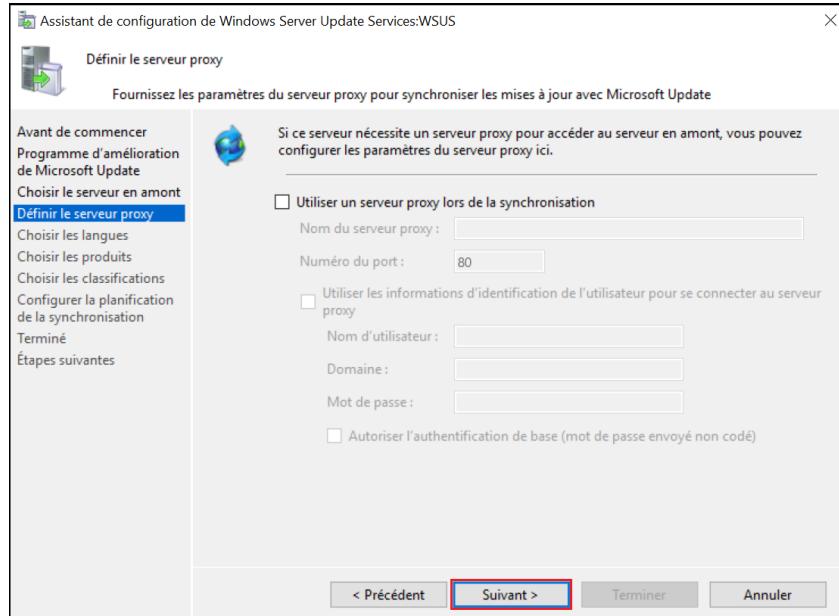


Figure 45 Choix du serveur proxy

Nous allons maintenant démarrer la connexion de notre serveur WSUS à Microsoft Update en cliquant sur **Démarrer la connexion**

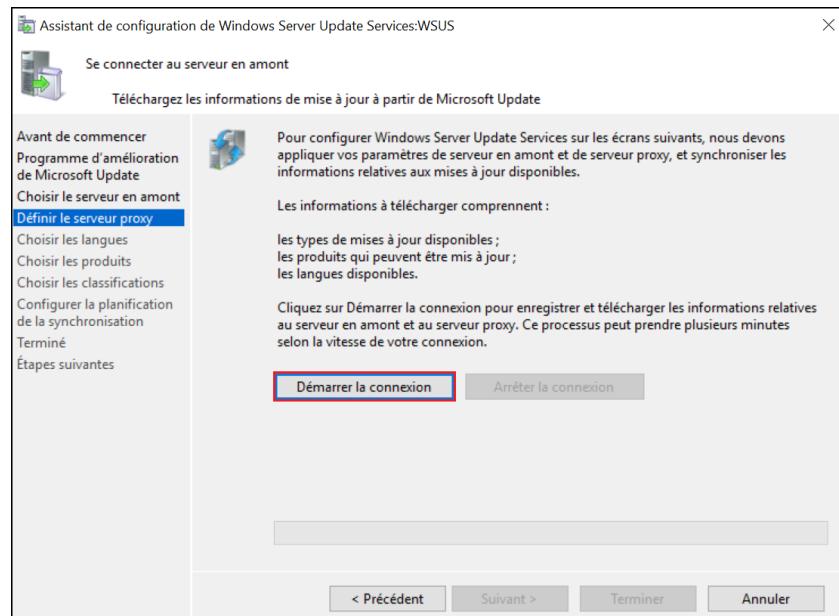


Figure 46 T2lechargement des information via Microsoft Update

Une fois le téléchargement terminer, cliquons sur suivant

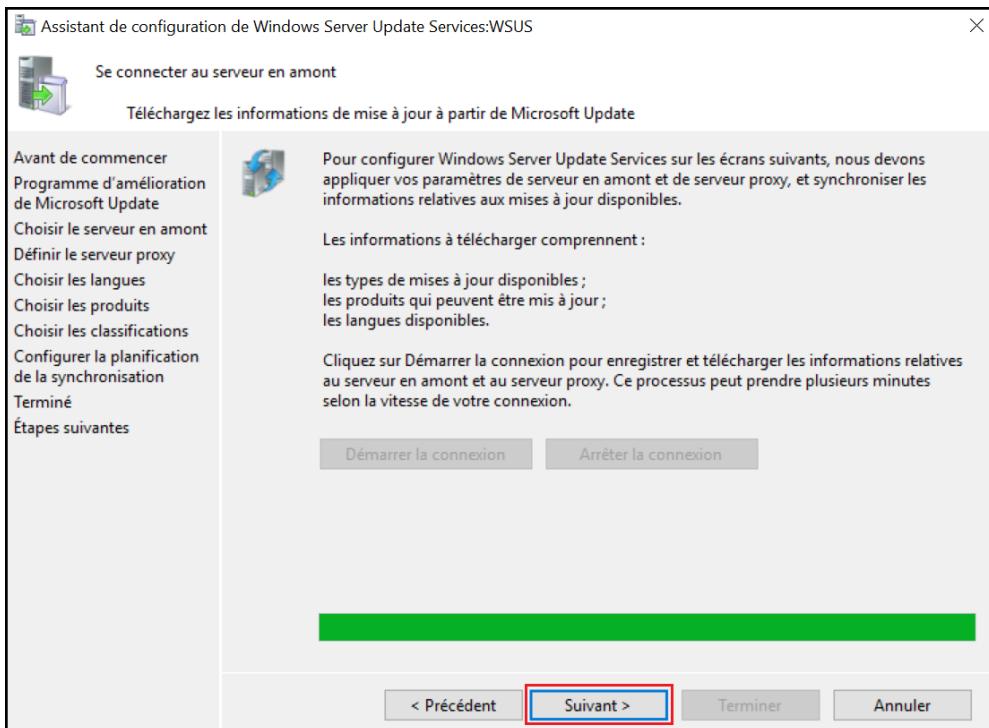


Figure 47 Fin du téléchargement des information de mise à jour

Choisissons les langues dans lesquelles nous souhaitons télécharger nos mises à jour et cliquons sur suivant

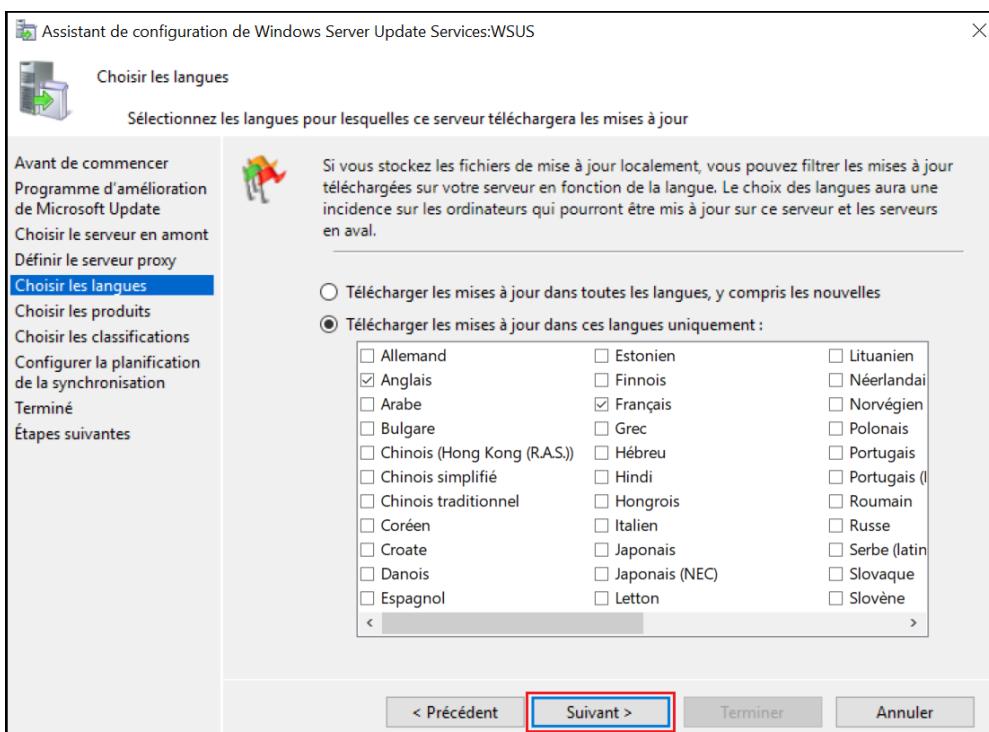


Figure 48 Choix des langues

Dans la fenêtre suivante nous allons sélectionner les produits pour lesquels nous souhaitons télécharger les mises à jour.

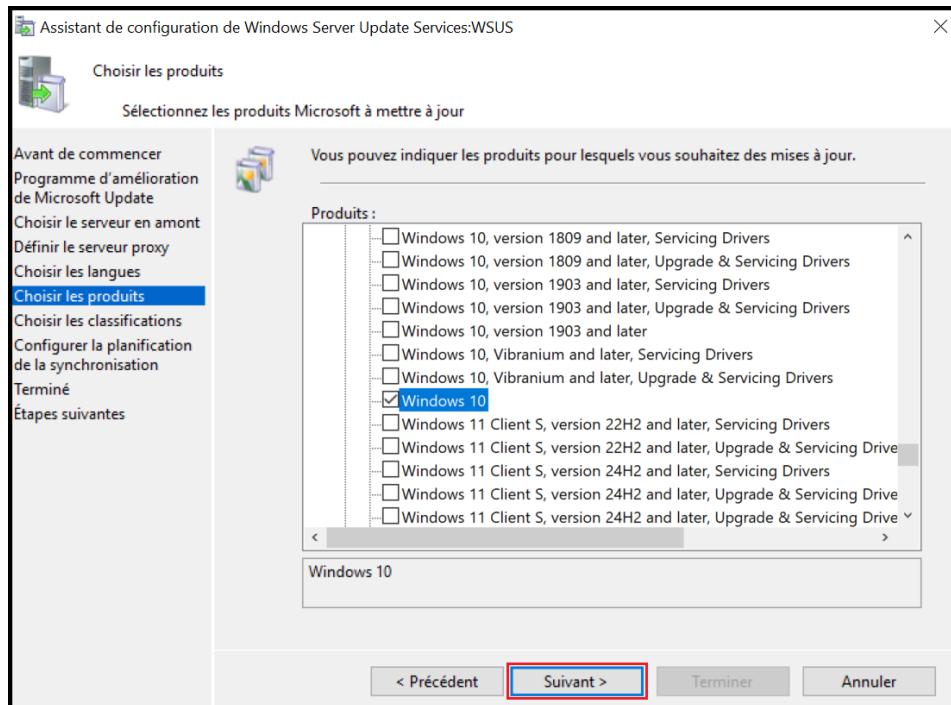


Figure 49 Choix des produits

Ensuite nous allons choisir le type de mises à jour qu'on veut télécharger. Une fois cela fait cliquons sur suivant

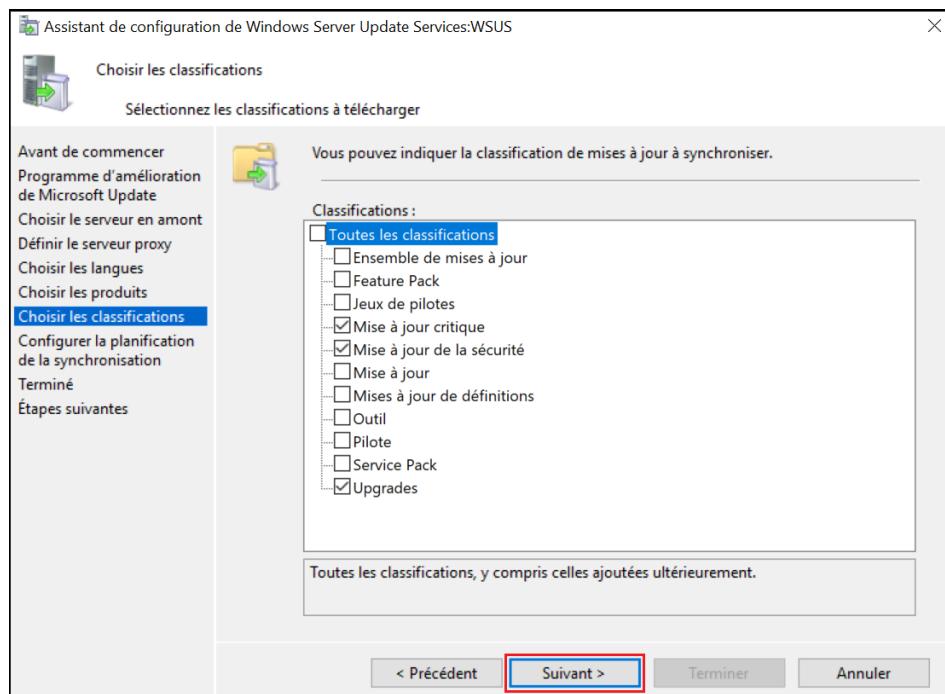


Figure 50 Choix du type de mises à jour

La synchronisation correspond à la communication entre notre serveur WSUS et Microsoft Update pour voir s'il n'y a pas de nouvelle mises à jour disponibles. Elle peut se faire de façon manuelle ou de façon automatique. Nous avons choisi la synchronisation automatique à raison d'une synchronisation par jour qui se fait à des heures d'inactivité pour éviter tout problèmes.

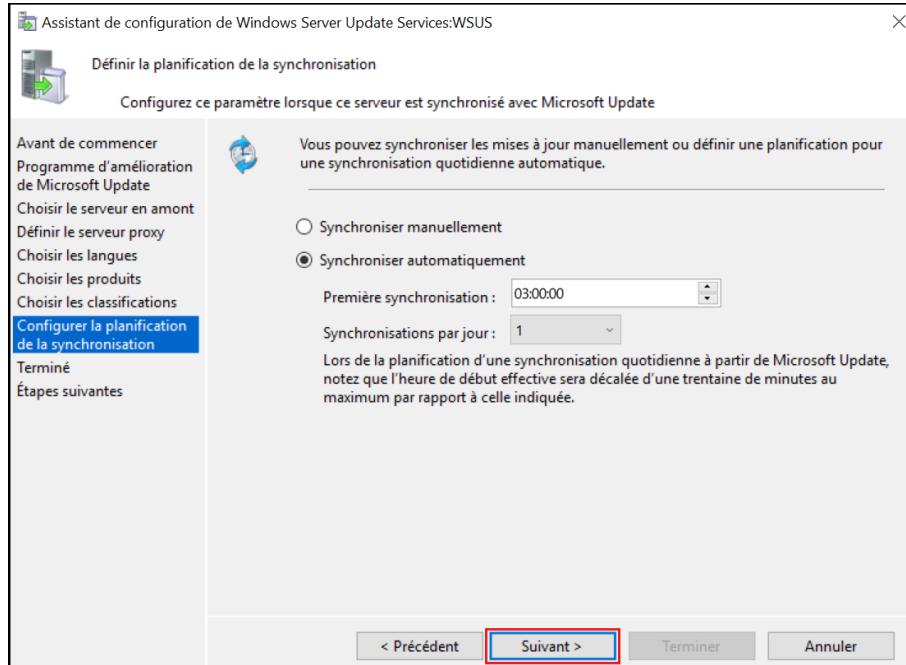


Figure 51 Planification de la synchronisation

Les configurations de bases effectuées nous pouvons lancer la première synchronisation et cliquer sur suivant.

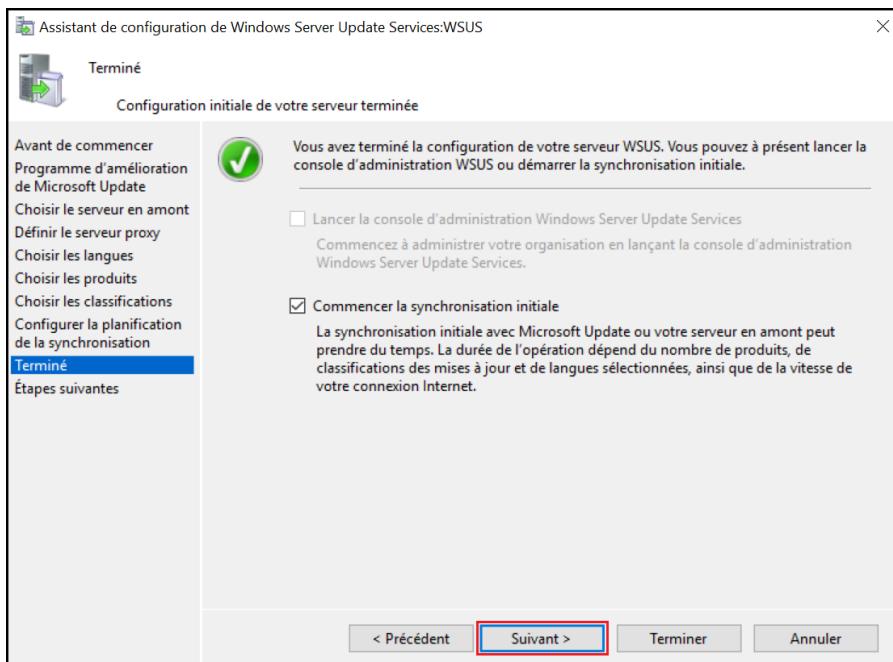


Figure 52 Lancement de la synchronisation initiale

Dans la fenêtre qui s'ouvre cliquons sur **WSUS**, nous pourrons voir l'état d'avancement de la synchronisation

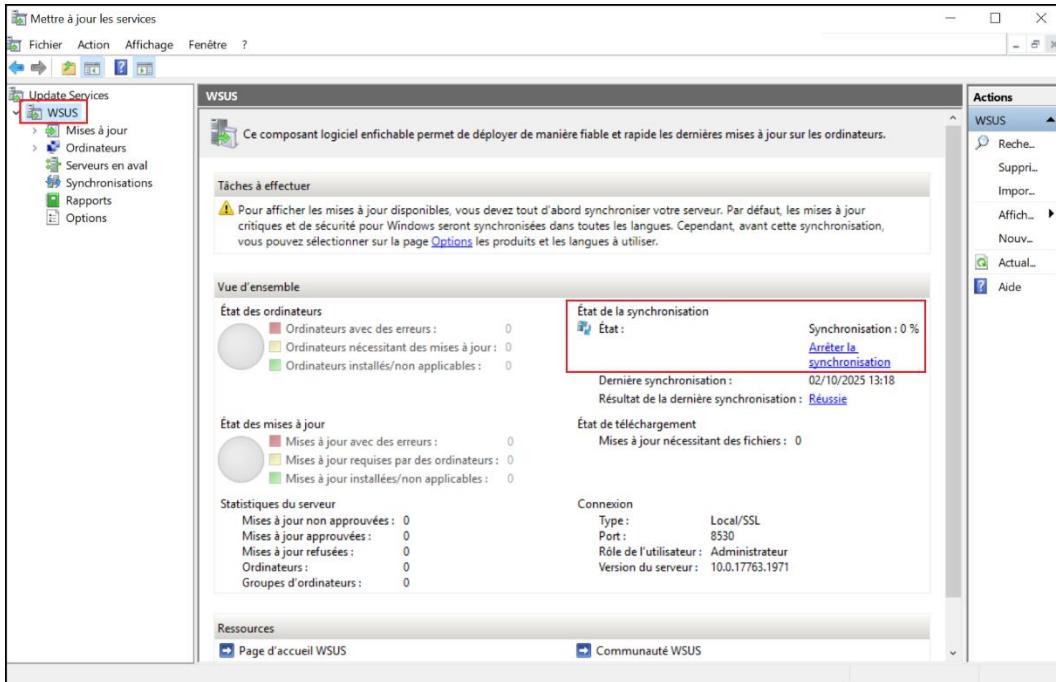


Figure 53 Vérification de l'état de synchronisation

En attendant la fin de la synchronisation créons des groupes d'ordinateurs pour séparer nos machines.

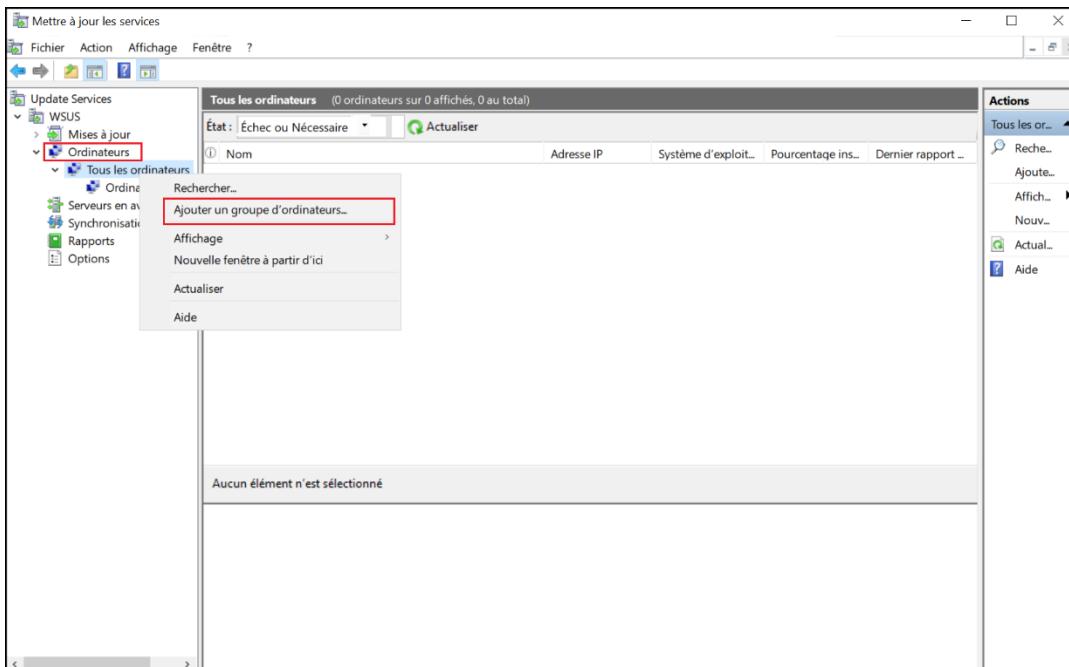


Figure 54 Ajout de groupe d'ordinateurs

Nous en avons donc créé deux : un groupe pour nos **Serveurs** et un autre pour les **Postes de travail**

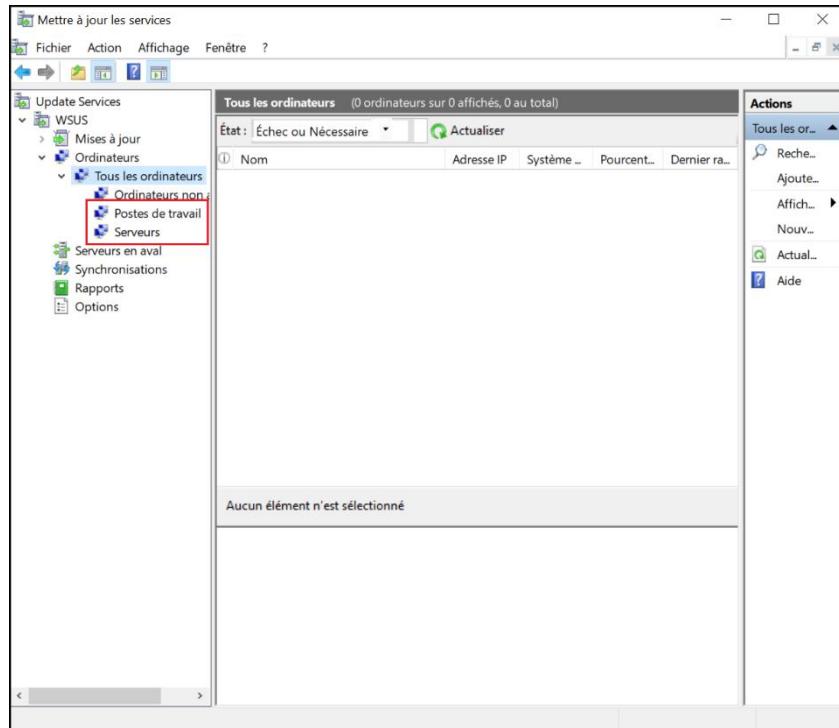


Figure 55 Création de groupes d'ordinateurs

En développant la section **Mises à Jour** dans l'arborescence, on peut voir toutes les mises à jour disponibles après la synchronisation initiale

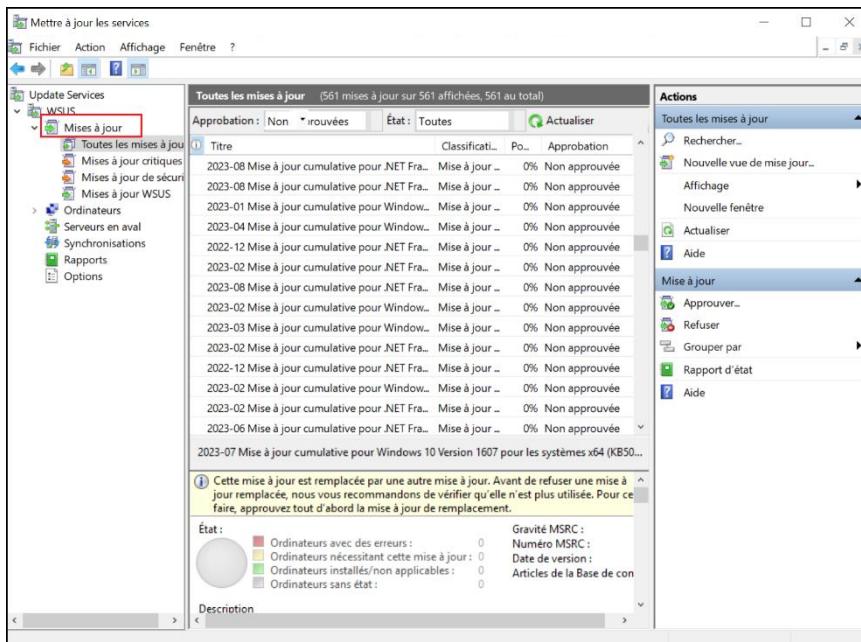


Figure 56 Visualisation des mises à jour

On peut sélectionner et approuver les mises à jour comme montrer dans la capture

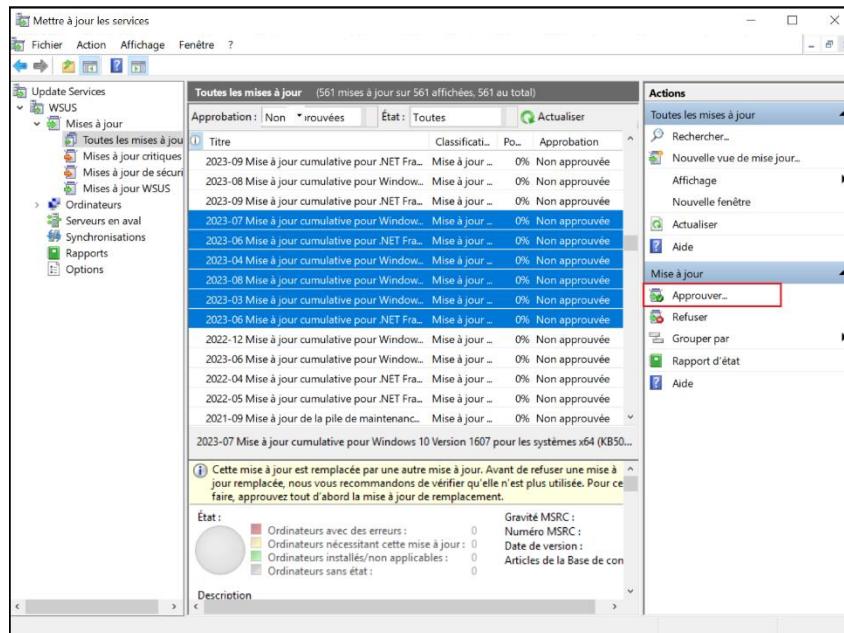


Figure 57 Sélection et approbation des mises à jour

Faisons un clic droit sur **Tous les ordinateurs** et cliquons sur **Approuvée pour l'installation**

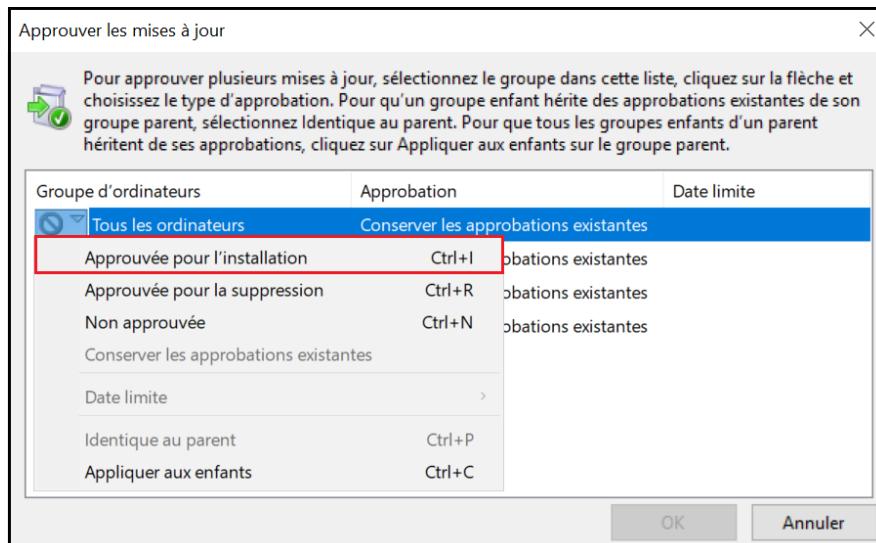


Figure 58 Approuver les mises à jour

Faisons **Ctrl+C** pour faire hériter l'installation à tous les groupes

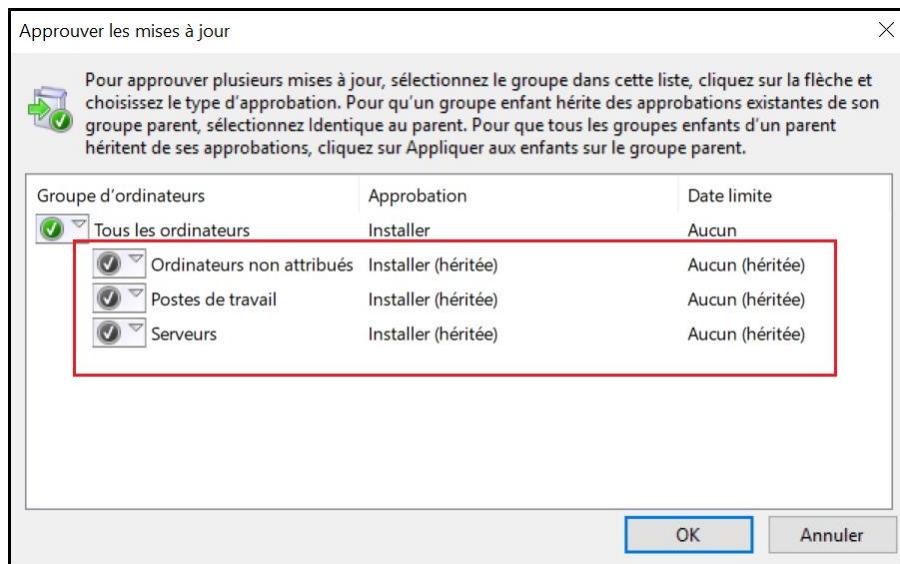


Figure 59 Héritage de l'installation

Après approbation des mises à jour, nous pouvons fermer la fenêtre

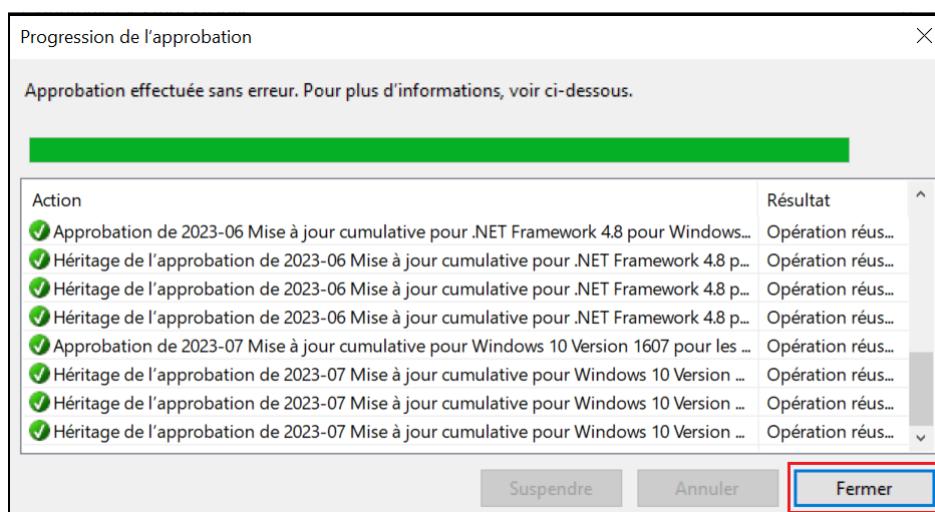


Figure 60 Fin de l'approbation des mises à jour

Dans la section **WSUS** dans l'arborescence, nous pouvons voir l'état d'avancement du téléchargement des mises à jour

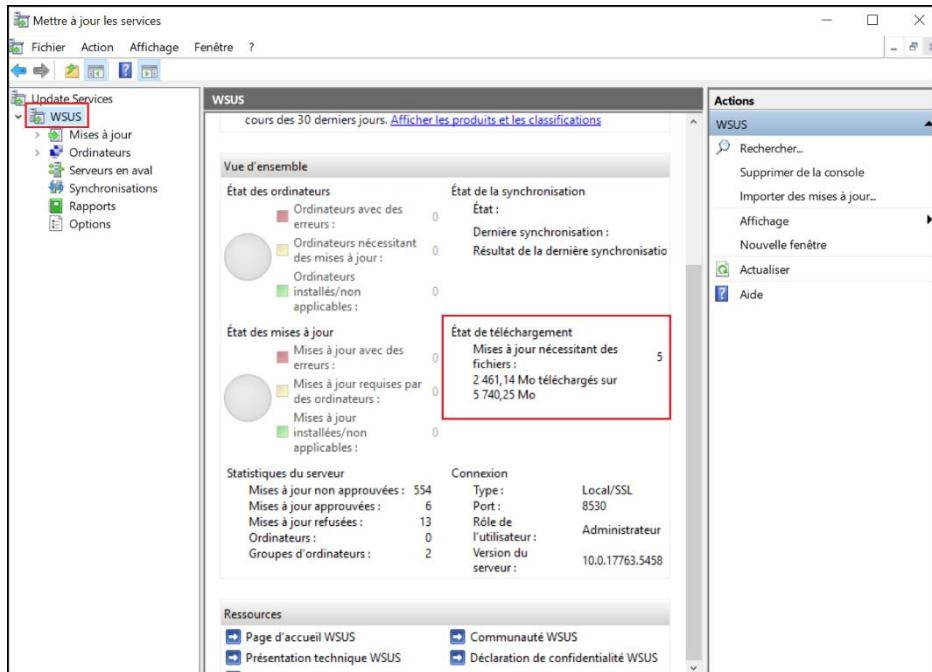


Figure 61 Avancement des mises à jour

#### 4.2.1. Configuration des stratégies de groupe pour les mises à jour

Commençons la configuration sur le contrôleur de domaine. Dans le gestionnaire de serveurs, cliquons sur **Outils** et ensuite sur **Gestion des stratégies de groupe**

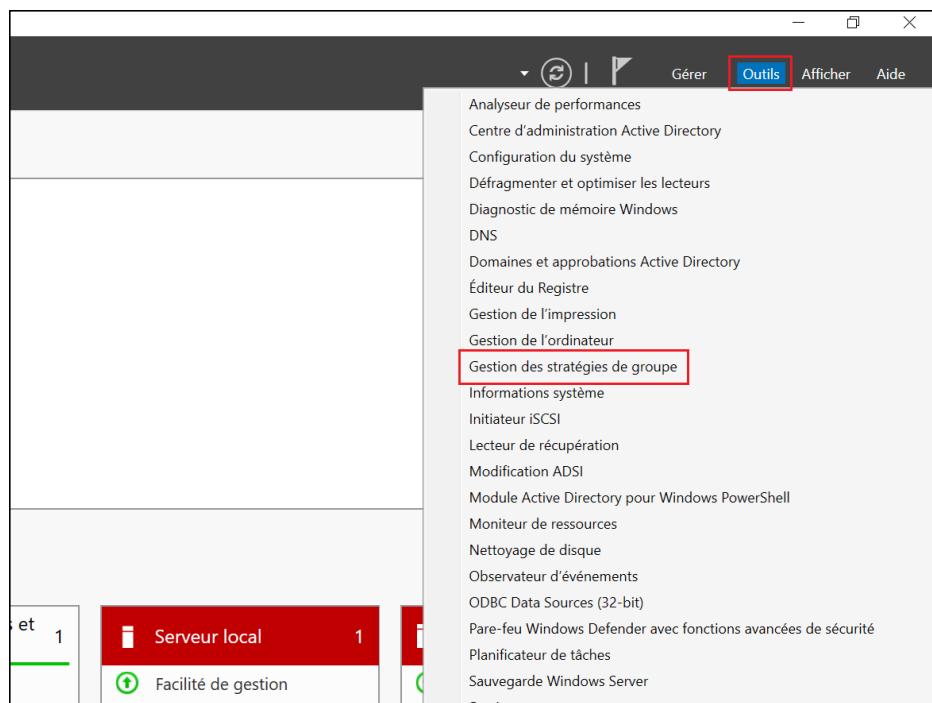


Figure 62 Sélection des stratégies de groupe

Dans la fenêtre qui s'ouvre, après avoir développé l'arborescence, faisons un **clic droit** sur le nom de notre domaine et sélectionnons **Créer un objet GPO dans ce domaine et le lier ici**

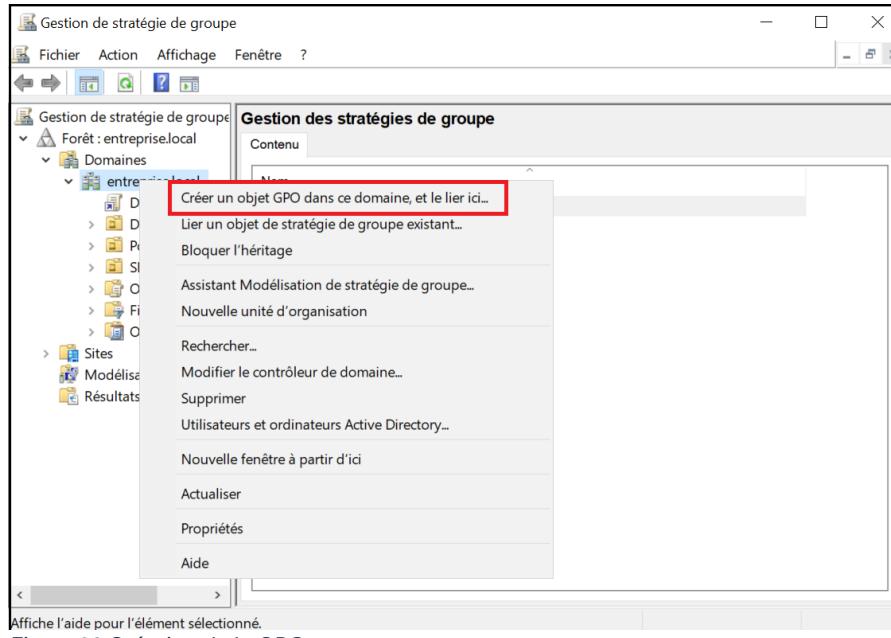


Figure 63 Création de la GPO

Dans la colonne **Nom** entrons le nom de notre stratégie de groupe

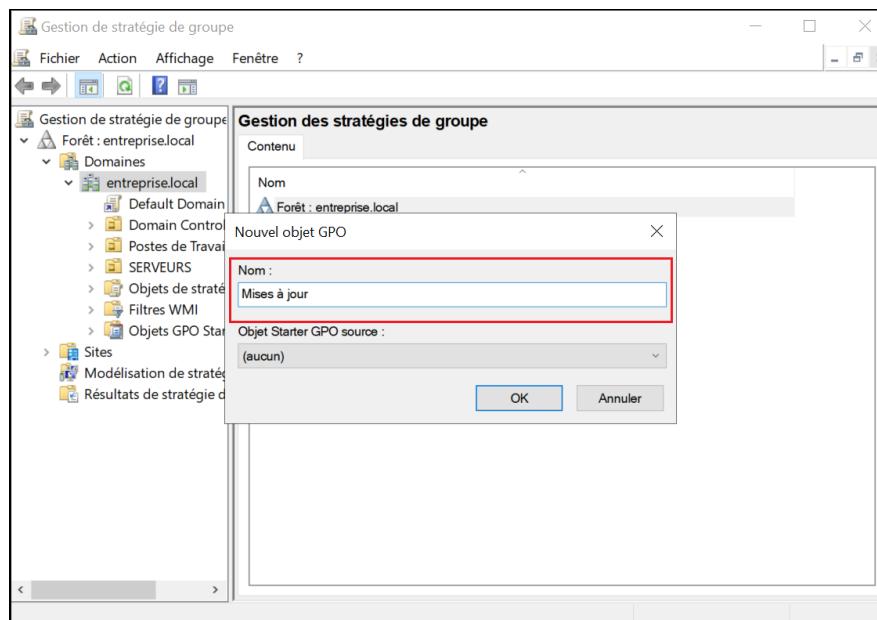


Figure 64 Nom de la GPO

Faisons un **Clic droit** sur la GPO qu'on vient de créer et cliquons sur **Modifier**

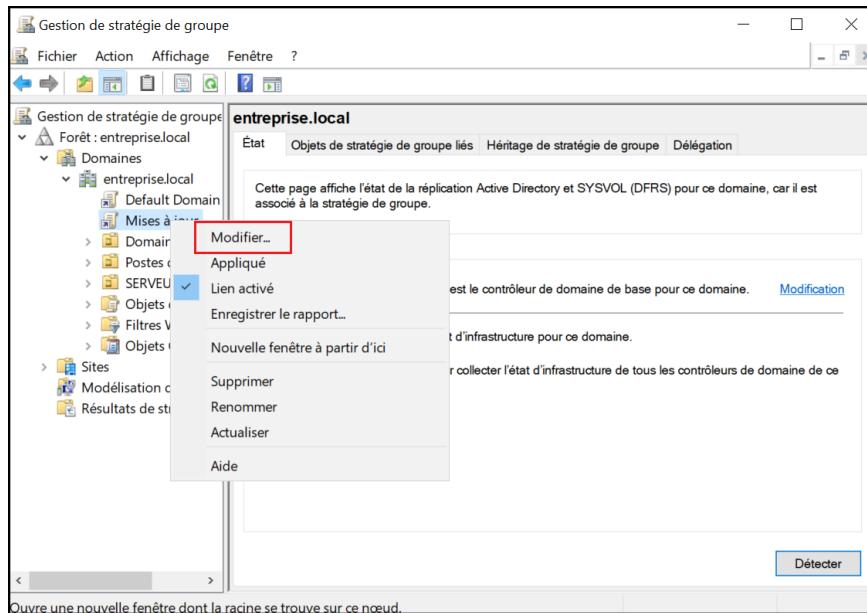


Figure 65 Modification de la GPO

Dans la fenêtre qui s'ouvre, développons **Configuration ordinateur** puis **Stratégies et Modèles d'administration**. Pour terminer sélectionnons **Composants Windows**

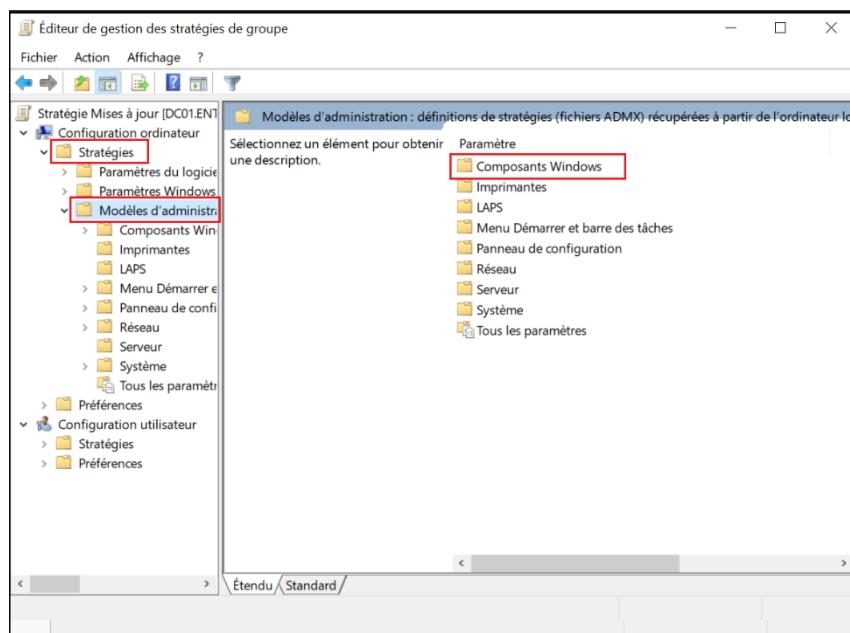


Figure 66 Modification de la GPO

Tout en bas cliquons sur Windows Update

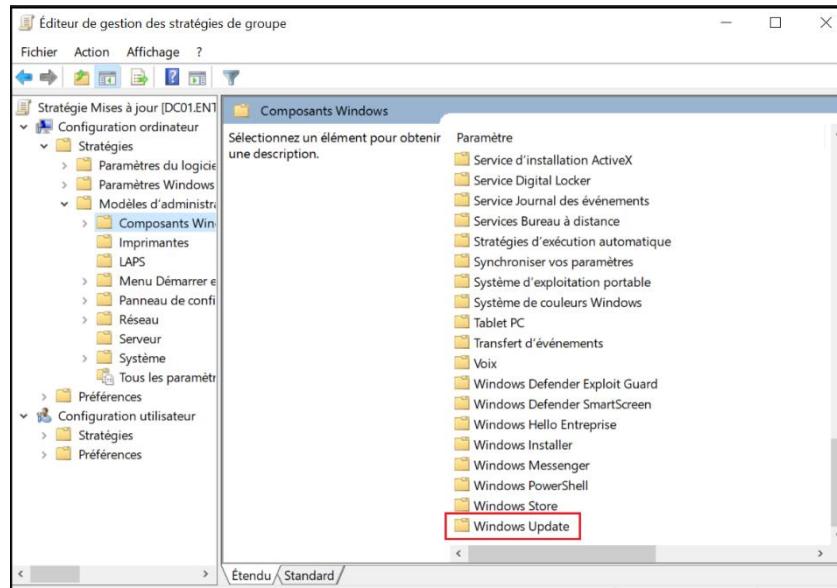


Figure 67 Sélection de Windows Update

Nous allons maintenant spécifier l'emplacement du serveur WSUS pour que les machines du domaine aillent chercher les mises à jour dessus

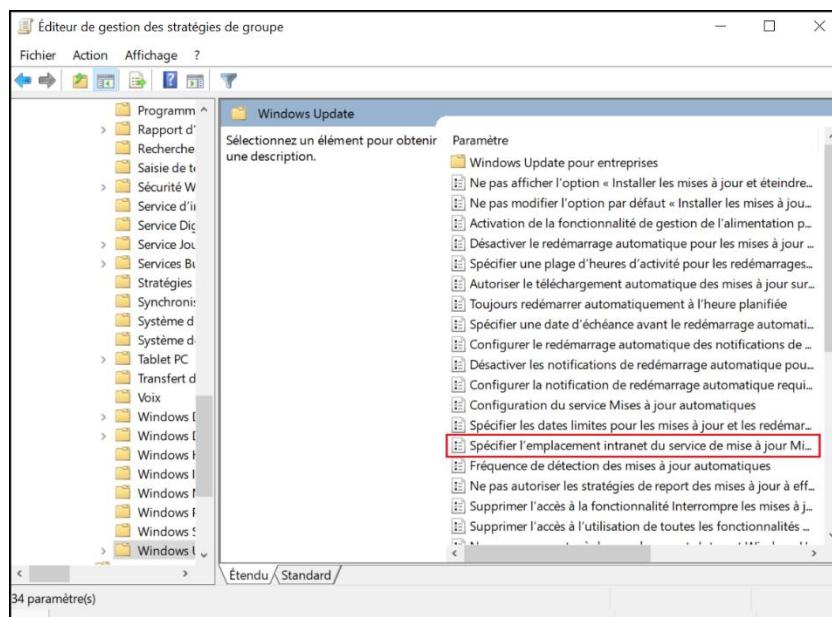


Figure 68 Emplacement du serveur WSUS

Activons ce paramètre et renseignons dans les deux premiers champ l'adresse de notre serveur WSUS

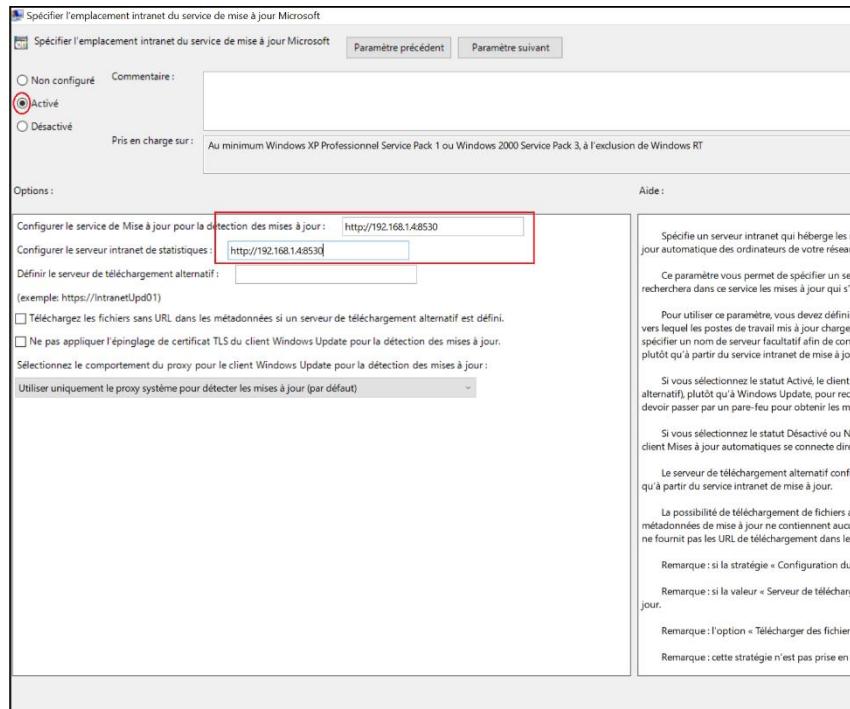


Figure 69 Configuration du paramètre

Passons au prochain paramètre : **Configuration du service Mises à jour automatique**

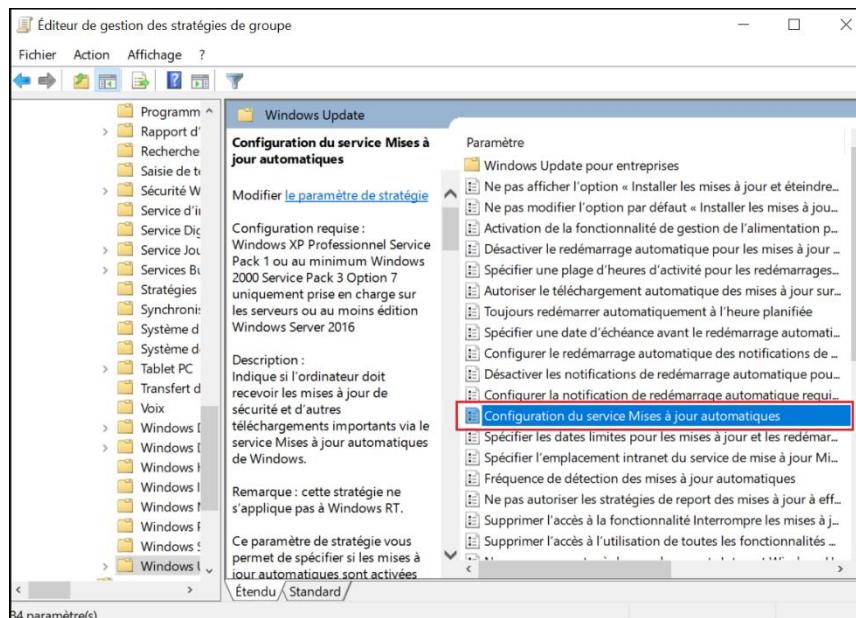


Figure 70 Configuration du service Mises à jour automatique

## Activons le paramètre et configurons-le

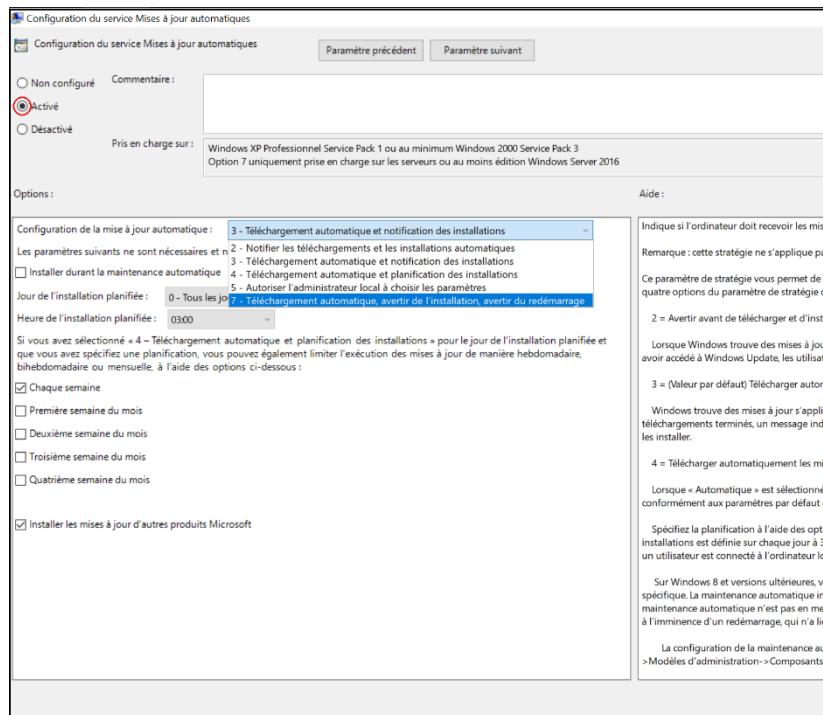


Figure 71 Configuration du paramètre

Pour forcer l'application de la GPO, dans l'invite de commande tapons « **gpupdate** »

```
C:\Users\Administrateur>gpupdate
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

C:\Users\Administrateur>
```

Figure 72 Application de la GPO

De retour sur notre serveur WSUS, dans la console de gestion puis dans tous les ordinateurs, nous constatons que les machines de notre domaine ont trouvé le serveur de mises à jour et y sont enregistrées

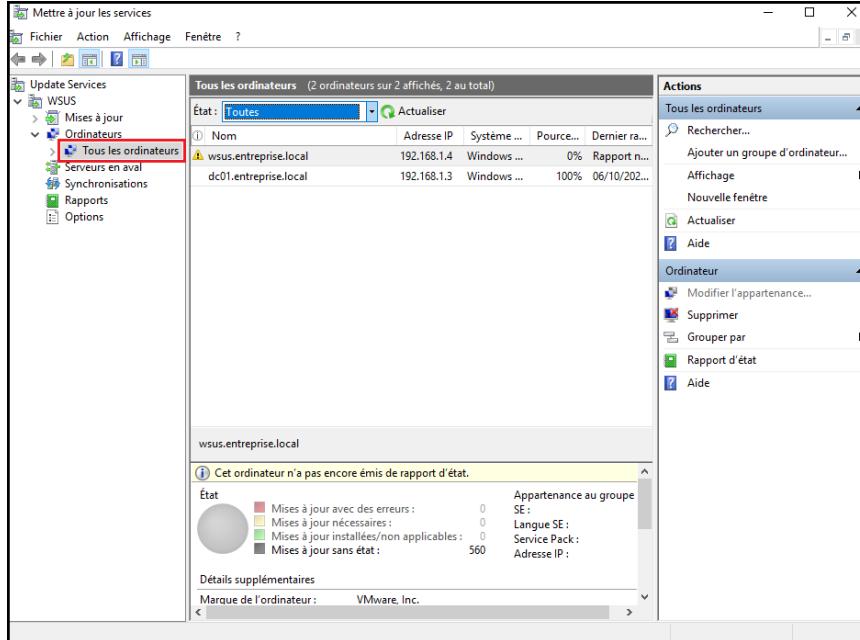


Figure 73 Machines enregistrées sur le serveur

Nous allons rapidement retourner sur le contrôleur de domaine pour créer des utilisateurs. Dans le **Gestionnaire de serveur** cliquons sur **Outils**, puis sur **Utilisateurs et ordinateurs Active Directory**. Dans la fenêtre qui s'ouvre, faisons un **clic droit** sur l'OU qui nous intéresse puis sur **Nouveau** et enfin sur **Utilisateur**

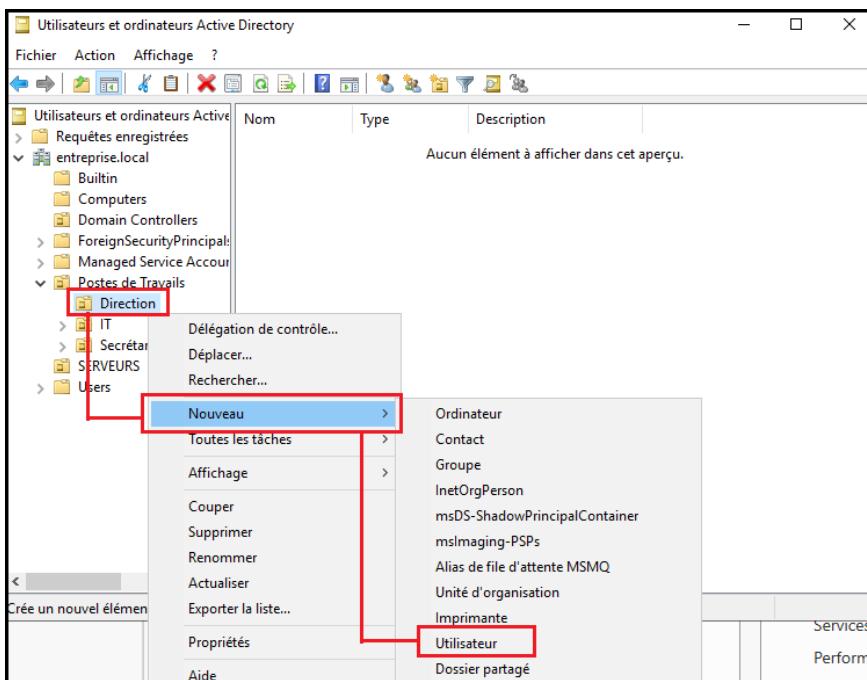


Figure 74 Création d'utilisateur

Renseignons dans les colonnes respectives le nom de l'utilisateur que nous voulons créer puis cliquons sur suivant

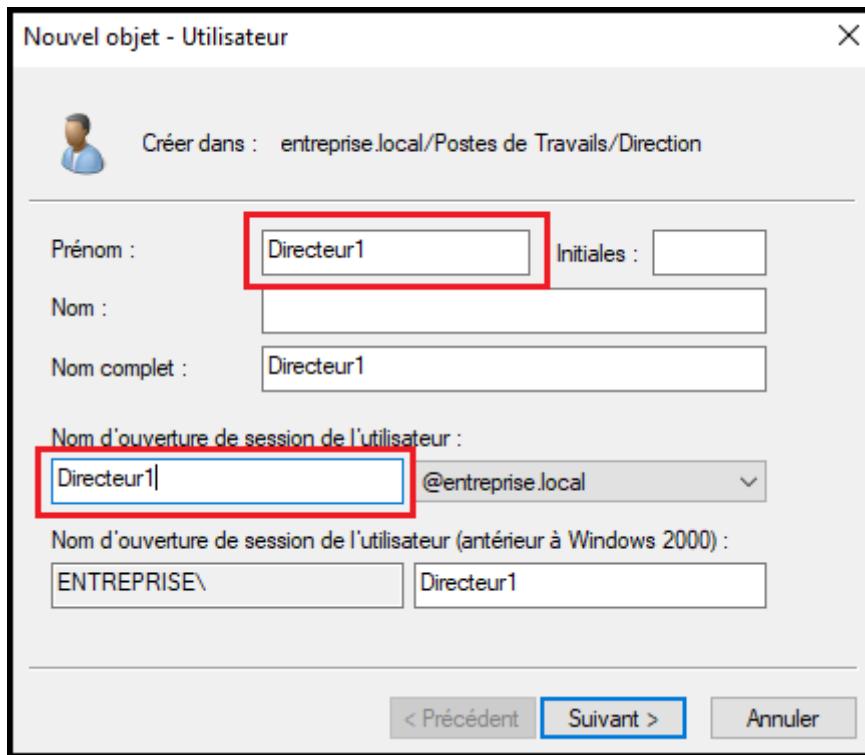


Figure 75 Nom d'utilisateur

Définissons le mot de passe de l'utilisateur et cliquons sur suivant. Comme dit précédemment, il doit être fort sinon vous ne pourrez pas continuer.

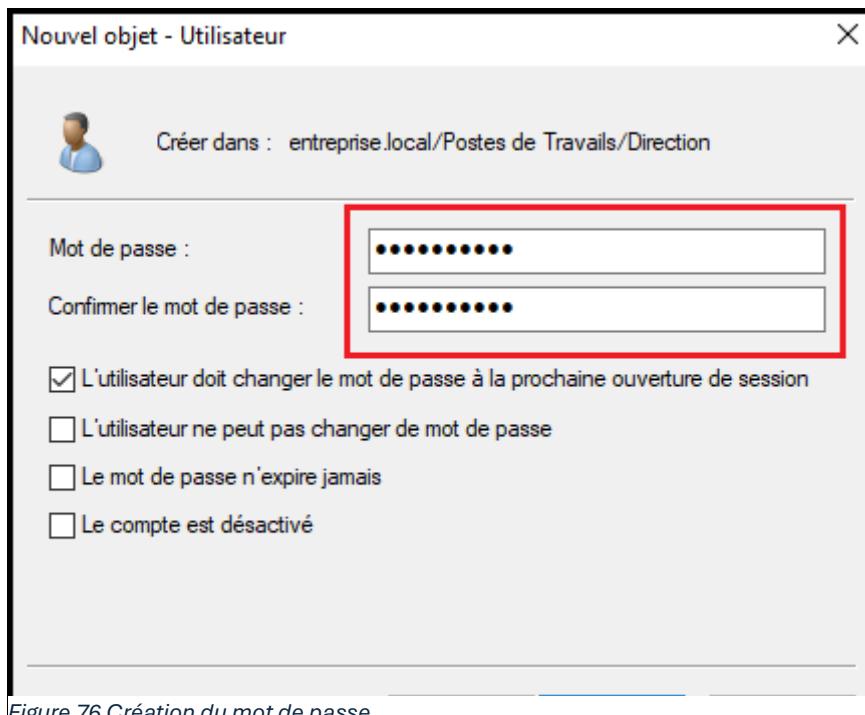
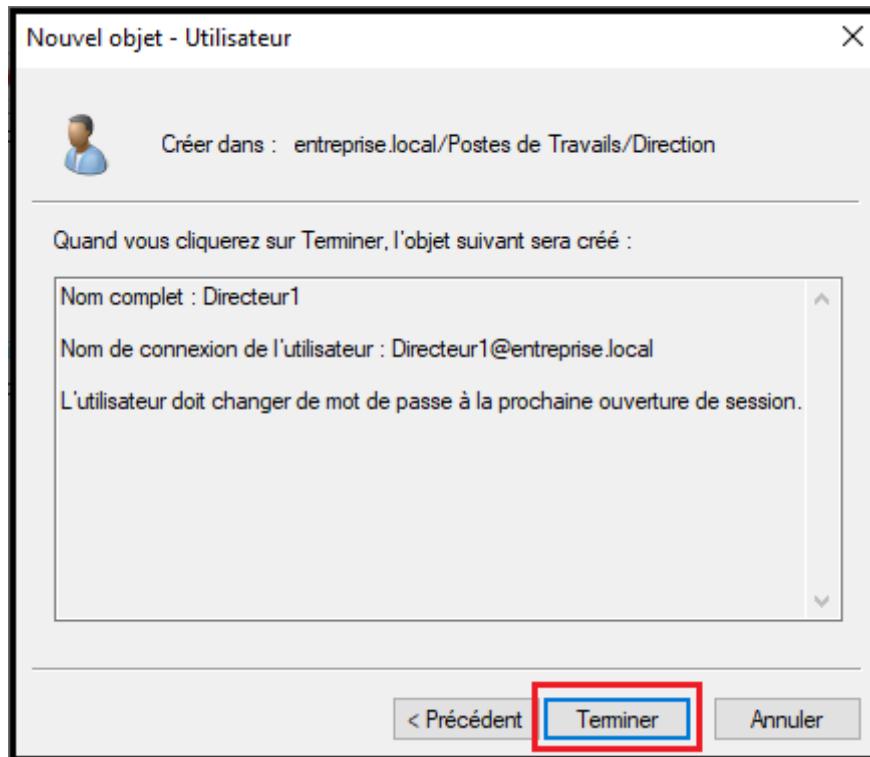


Figure 76 Création du mot de passe

Nous pouvons maintenant cliquer sur terminer et ça y est, notre utilisateur a été créé.



Ajoutons une machine à notre domaine. Nous procèderons comme pour le server WSUS c'est-à-dire **adresser statiquement la machine, changer son nom et mettre comme adresse DNS celle de notre server DNS**. Une fois tout ça fait, entrons le nom de notre domaine et connectons-nous.

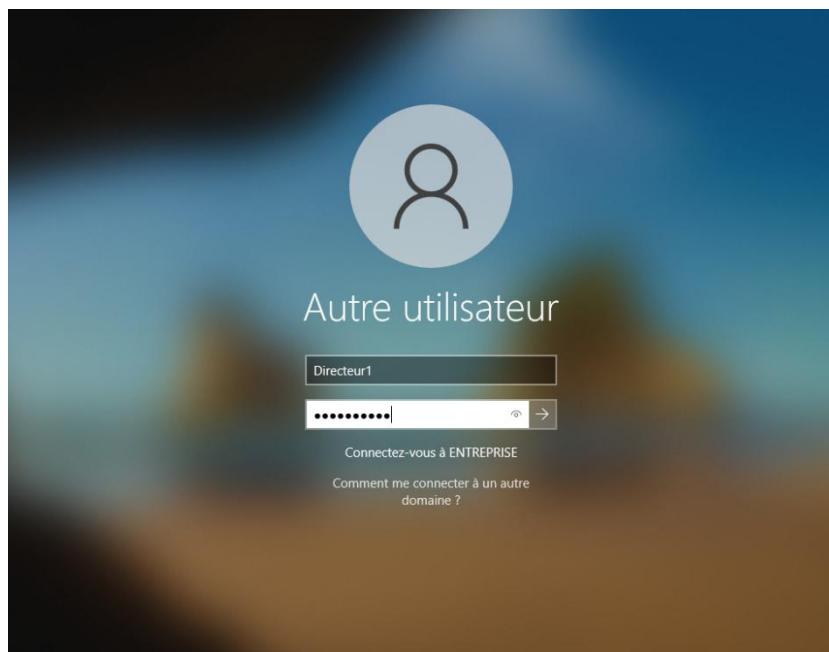
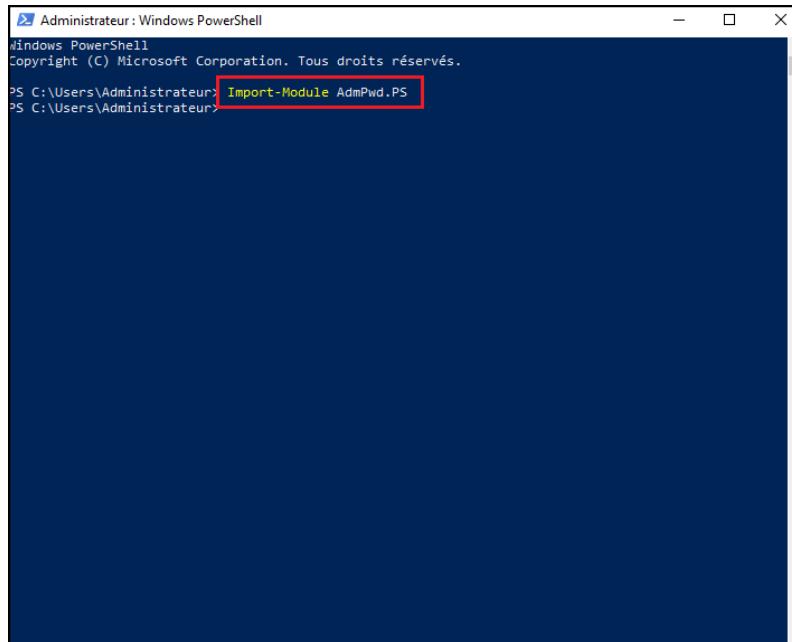


Figure 77 Connexion à l'utilisateur créé

## 4.3. Configuration de LAPS

### 4.3.1. Installation de LAPS sur le contrôleur de domaine

Nous allons commencer la configuration sur le contrôleur de domaine parce que c'est le maître de schéma. Commençons par importer le module LAPS de PowerShell. Pour ce faire, lançons PowerShell en mode administrateur et exécutons cette commande : « **Import-Module AdmPwd.PS** »

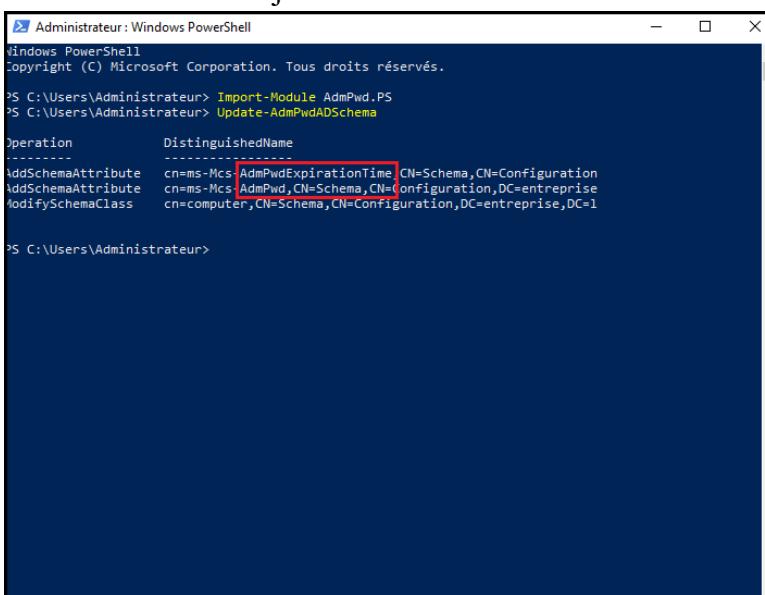


```
Administrator : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Import-Module AdmPwd.PS
```

Figure 78 Import du module LAPS dans PowerShell

Ensuite nous allons inscrire deux nouveaux attributs au schéma : **la date d'expiration du mot de passe et le mot de passe lui-même**. Pour se faire, nous allons entrer la commande « **Update-AdmPwdADSchema** » toujours dans la console PowerShell



```
Administrator : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Import-Module AdmPwd.PS
PS C:\Users\Administrateur> Update-AdmPwdADSchema

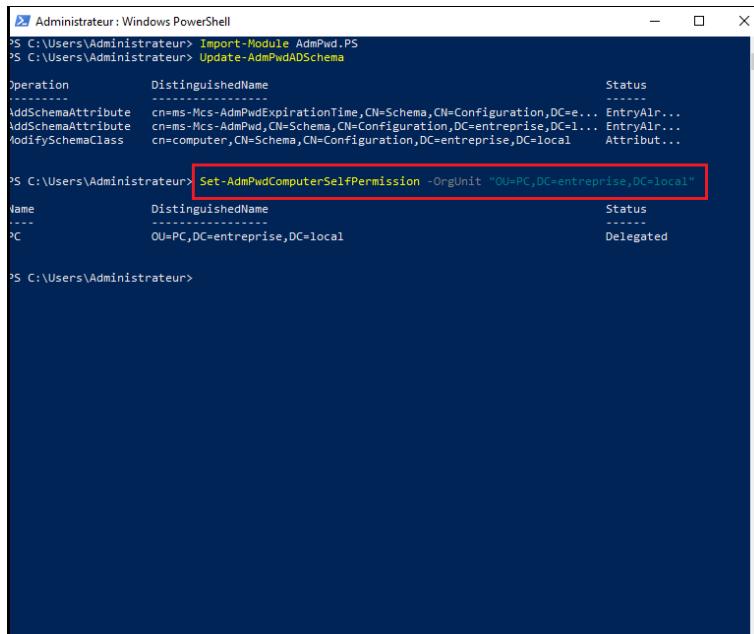
Operation          DistinguishedName
-----          -----
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=entreprise
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=entreprise,DC=1

PS C:\Users\Administrateur>
```

Figure 79 Ajout des attributs

Pour sécuriser LAPS, nous allons sécuriser l'accès au mot de passe dans l'AD et donner les droit d'accès aux machines de notre domaine. Tapons la commande « **Set-AdmPwdComputerSelfPermission -OrgUnit “OU=PC,DC=entreprise,DC=local”** »

**OU=PC** : C'est l'unité d'organisation qui a accès au mots de passe. **DC=entreprise** : c'est la première partie de notre nom de domaine et **DC=local** la seconde partie



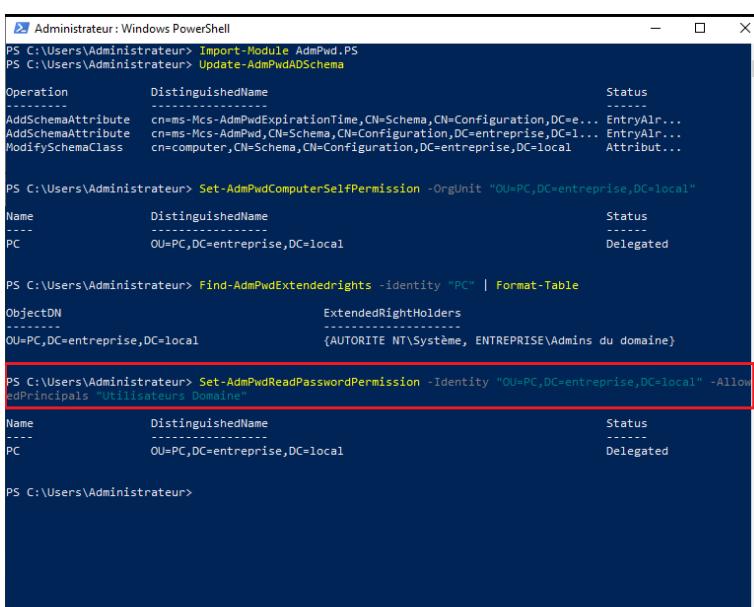
```

PS C:\Users\Administrateur> Import-Module AdmPwd.PS
PS C:\Users\Administrateur> Update-AdmPwdADSschema
Operation      DistinguishedName          Status
-----
AddSchemaAttribute cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=ent... EntryAlr...
AddSchemaAttribute cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=entreprise,DC=local... EntryAlr...
ModifySchemaClass cn=computer,CN=Schema,CN=Configuration,DC=entreprise,DC=local   Attribut...
PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=entreprise,DC=local"
Name      DistinguishedName          Status
-----
PC      OU=PC,DC=entreprise,DC=local   Delegated
PS C:\Users\Administrateur>

```

Figure 80 Accès au mot de passe

Nous allons maintenant spécifier le groupe d'utilisateur qui peut lire les mots de passe avec la commande « **Set-AdmPwdReadPasswordPermission -Identity “OU=PC,DC=entreprise,DC=local” -AllowedPrincipals “Utilisateurs Domaine”** »



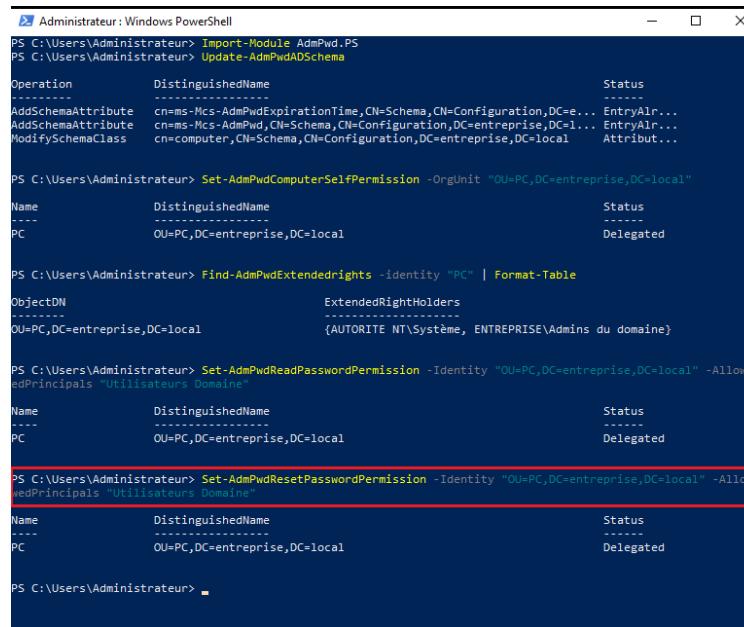
```

PS C:\Users\Administrateur> Import-Module AdmPwd.PS
PS C:\Users\Administrateur> Update-AdmPwdADSschema
Operation      DistinguishedName          Status
-----
AddSchemaAttribute cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=ent... EntryAlr...
AddSchemaAttribute cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=entreprise,DC=local... EntryAlr...
ModifySchemaClass cn=computer,CN=Schema,CN=Configuration,DC=entreprise,DC=local   Attribut...
PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=entreprise,DC=local"
Name      DistinguishedName          Status
-----
PC      OU=PC,DC=entreprise,DC=local   Delegated
PS C:\Users\Administrateur> Find-AdmPwdExtendedrights -identity "PC" | Format-Table
ObjectDN          ExtendedRightHolders
-----
OU=PC,DC=entreprise,DC=local   {AUTORITE NT\Système, ENTREPRISE\Admins du domaine}
PS C:\Users\Administrateur> Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=entreprise,DC=local" -AllowdPrincipals "Utilisateurs Domaine"
Name      DistinguishedName          Status
-----
PC      OU=PC,DC=entreprise,DC=local   Delegated
PS C:\Users\Administrateur>

```

Figure 81 Permission de lecture du mot de passe

Comme fait précédemment, nous allons autoriser un groupe d'utilisateur spécifique qui peut réinitialiser le mot de passe définit avec la commande : « **Set-AdmPwdResetPasswordPermission -Identity “OU=PC,DC=entreprise,DC=local” -AllowedPrincipals “Utilisateurs Domaine”** »



```

PS C:\Users\Administrateur> Import-Module AdmPwd.PS
PS C:\Users\Administrateur> Update-AdmPwdADSschema

Operation          DistinguishedName           Status
-----
AddSchemaAttribute cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=ent... EntryAlr...
AddSchemaAttribute cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=entreprise,DC=lo... EntryAlr...
ModifySchemaClass  cn=computer,CN=Schema,CN=Configuration,DC=entreprise,DC=local   Attribut...

PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=entreprise,DC=local"
Name          DistinguishedName           Status
-----
PC            OU=PC,DC=entreprise,DC=local       Delegated

PS C:\Users\Administrateur> Find-AdmPwdExtendedrights -identity "PC" | Format-Table
ObjectDN          ExtendedRightHolders
-----
OU=PC,DC=entreprise,DC=local      {AUTORITE NT\Système, ENTREPRISE\Admins du domaine}

PS C:\Users\Administrateur> Set-AdmPwdReadPasswordPermission -Identity "OU=PC,DC=entreprise,DC=local" -Allow... edPrincipals "Utilisateurs Domaine"
Name          DistinguishedName           Status
-----
PC            OU=PC,DC=entreprise,DC=local       Delegated

PS C:\Users\Administrateur> Set-AdmPwdResetPasswordPermission -Identity "OU=PC,DC=entreprise,DC=local" -Ali... wedPrincipals "Utilisateurs Domaine"
Name          DistinguishedName           Status
-----
PC            OU=PC,DC=entreprise,DC=local       Delegated

PS C:\Users\Administrateur>

```

Figure 82 Permission de réinitialisation du mot de passe

La première phase de la configuration de LAPS est terminée donc maintenant nous allons passer à la configuration de la GPO.

## 4.3.2.Configuration de la GPO LAPS

Afin d'effectuer la configuration de la GPO LAPS, nous allons devoir importer sur notre domaine Active Directory le **Template d'administration de LAPS**. Rendons-nous dans : **C:\Windows\PolicyDefinitions** et copions le fichier **AdmPwd.admx**

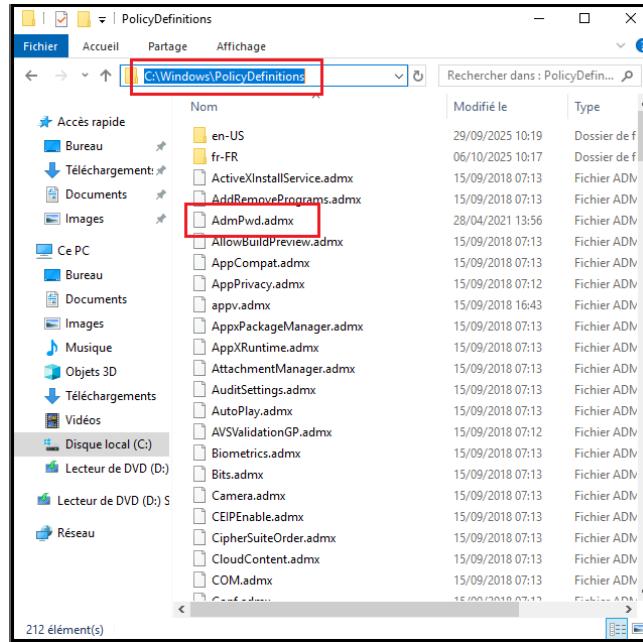


Figure 83 Copie du Template d'administration de LAPS

Collons le dans :

**C:\Windows\SYSVOL\sysvol\entreprise.local\Policies\PolicyDefinitions**

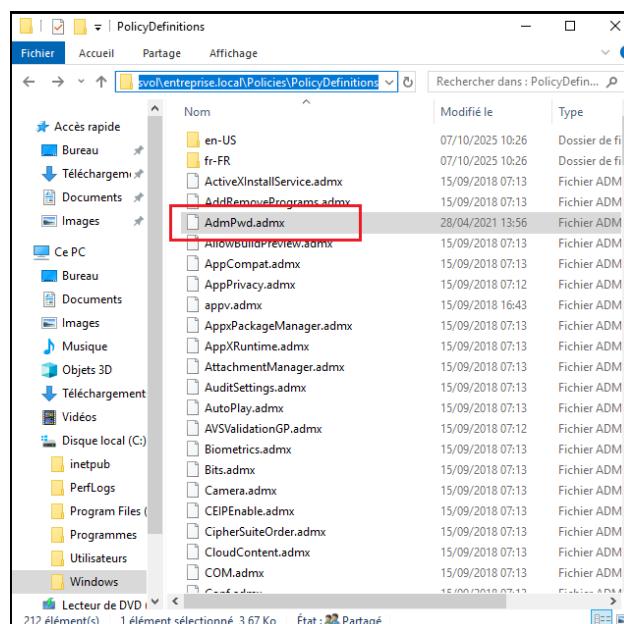


Figure 84 Collage du Template d'administration de LAPS

Nous pouvons maintenant créer la GPO. Comme fait précédemment, lançons la fenêtre de gestion de stratégie de groupe, faisons clic droit sur l'OU qui nous intéresse puis cliquons sur **Créer un objet GPO dans ce domaine, et le lier ici**

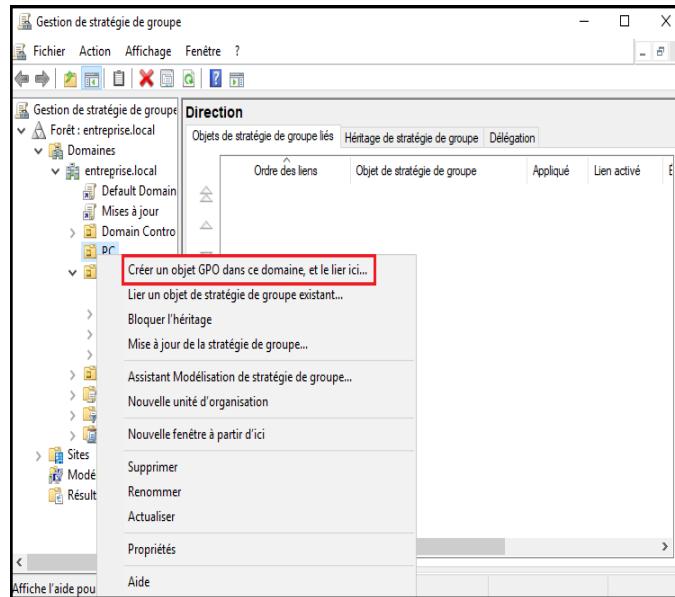


Figure 85 Création de la GPO

Nommons notre GPO **LAPS-Config** puis validons.

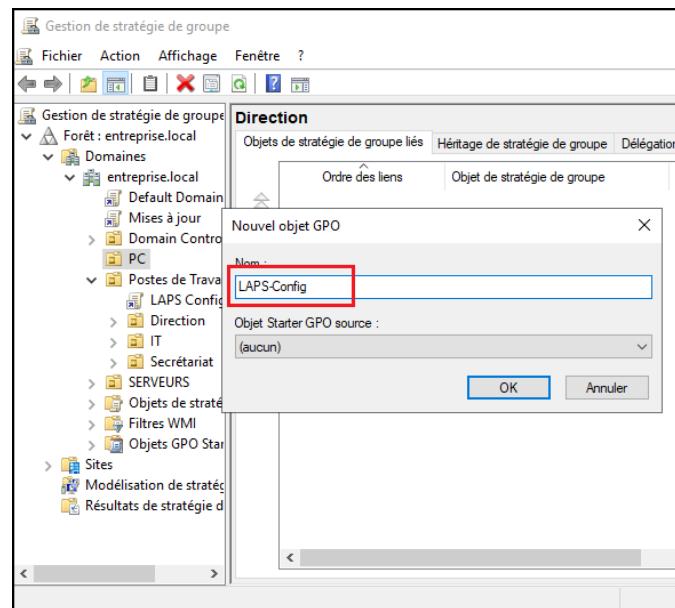


Figure 86 Nom de la GPO

Faisons un clic droit sur la GPO nouvellement créée puis sur **Modifier**

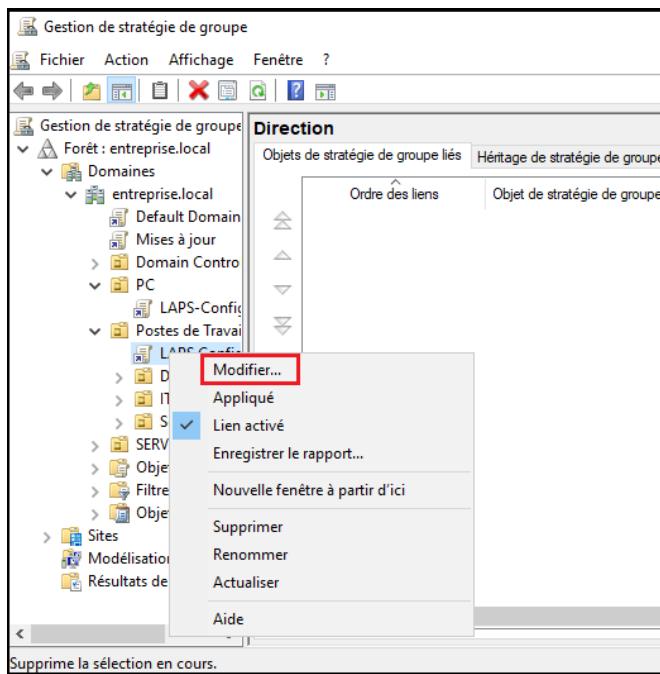


Figure 87 Modification de la GPO

Dans **Configuration ordinateur**, développons le dossier **Stratégies**, puis **Modèles d'administration**. Sélectionnons le dossier **LAPS**.

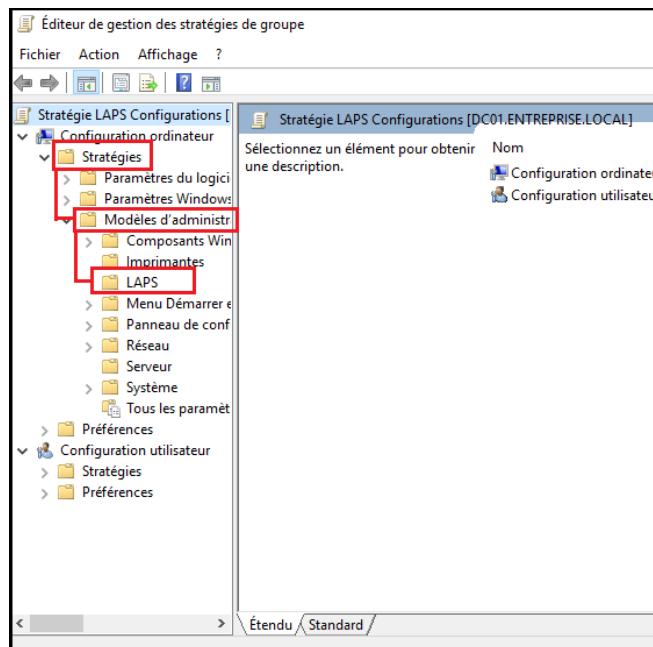


Figure 88 Sélection du dossier LAPS

Dans la fenêtre qui s'ouvre, sélectionnons le paramètre **Password Settings** qui va nous permettre de gérer les politiques de génération de mot de passe

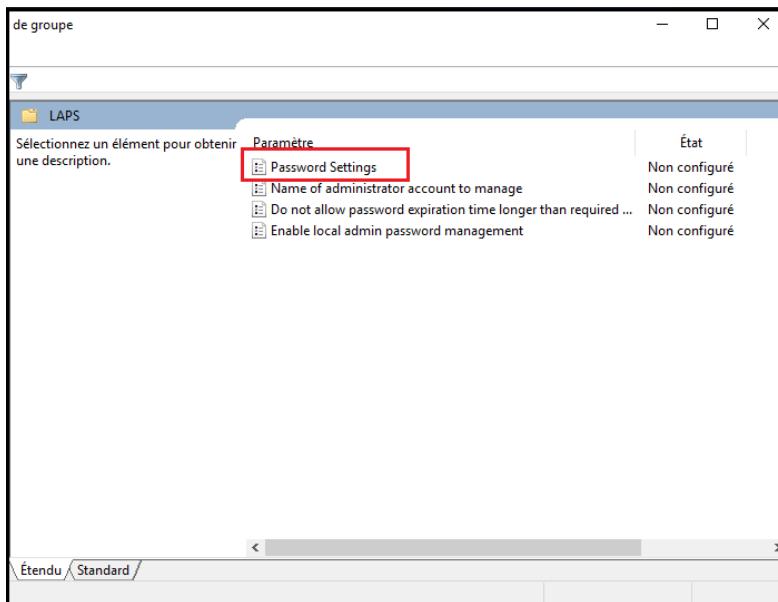


Figure 89 Sélection du paramètre Password Settings

Activons le paramètre et renseignons : la complexité du mot de passe, la longueur et la période de validité du mot de passe généré puis cliquons sur **Appliquer** puis sur **OK**

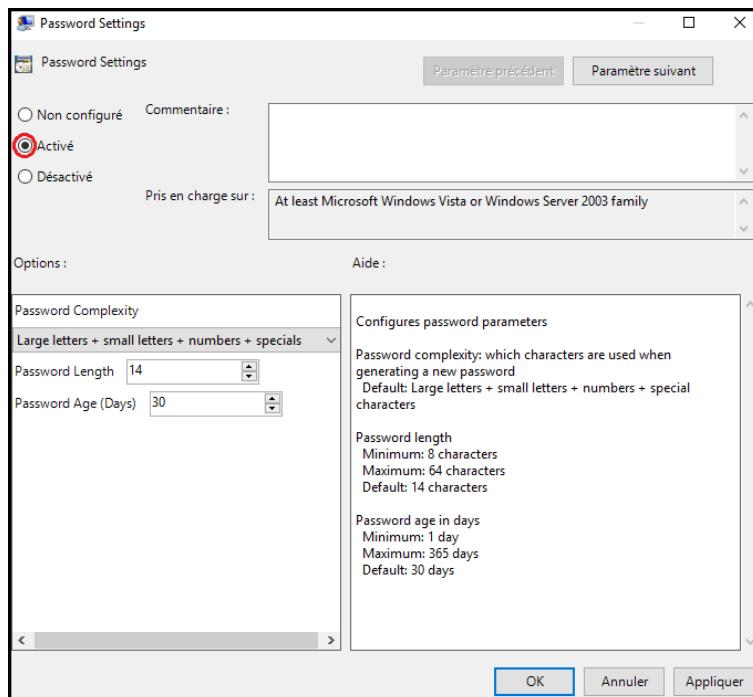


Figure 90 Password Settings

Ensuite activons le paramètre **Do not allow password expiration time longer than required by policy**

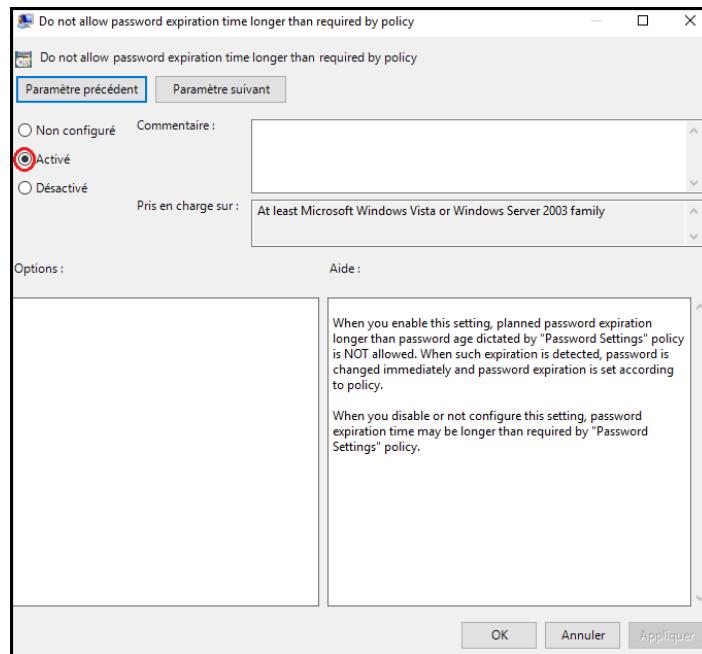


Figure 91 Activation du paramètre d'expiration

Pour terminer, activons le paramètre **Enable local password management** et validons

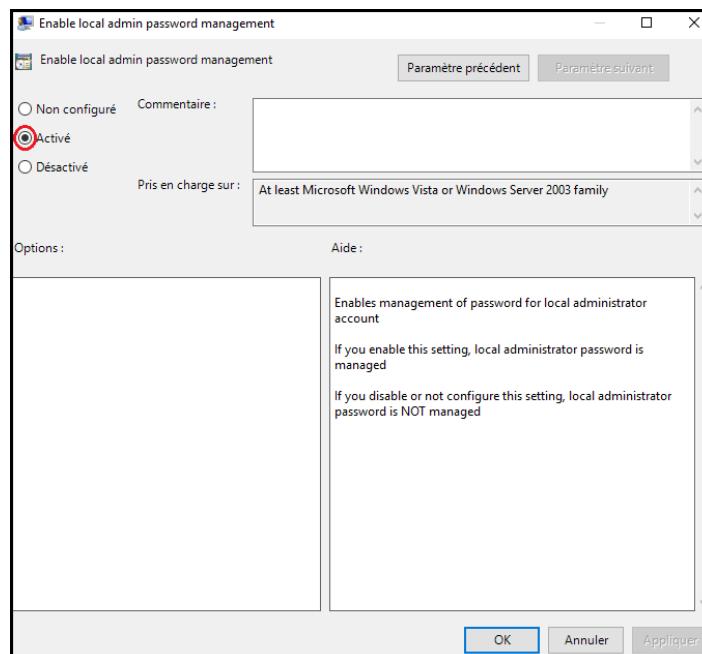


Figure 92 Activation du paramètre de mot de passe local

### 4.3.3.Déploiement de LAPS par GPO

Pour que nos configurations soient effectives, il faut que LAPS soit installé sur toutes les machines du domaine. Pour se faire, nous allons devoir définir une GPO pour l'installer automatiquement dès qu'une machine rejoint le domaine. Pour se faire nous devons partager en réseau le package d'installation de LAPS.

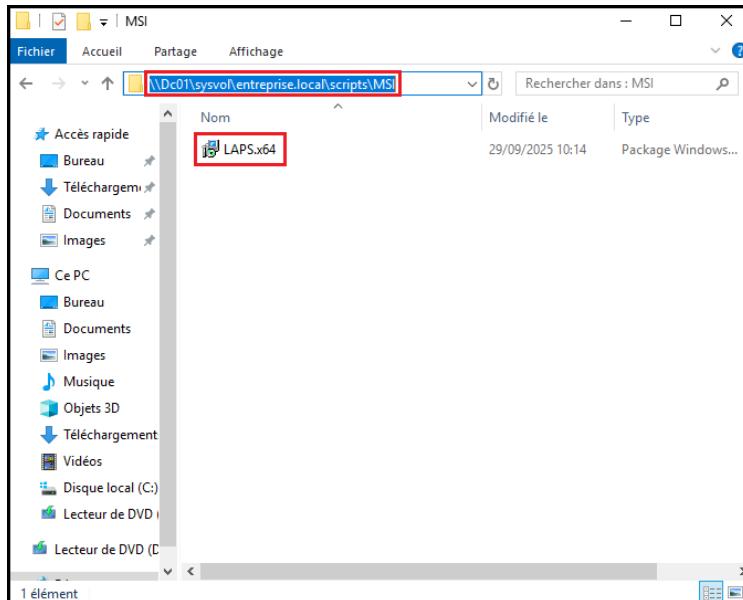
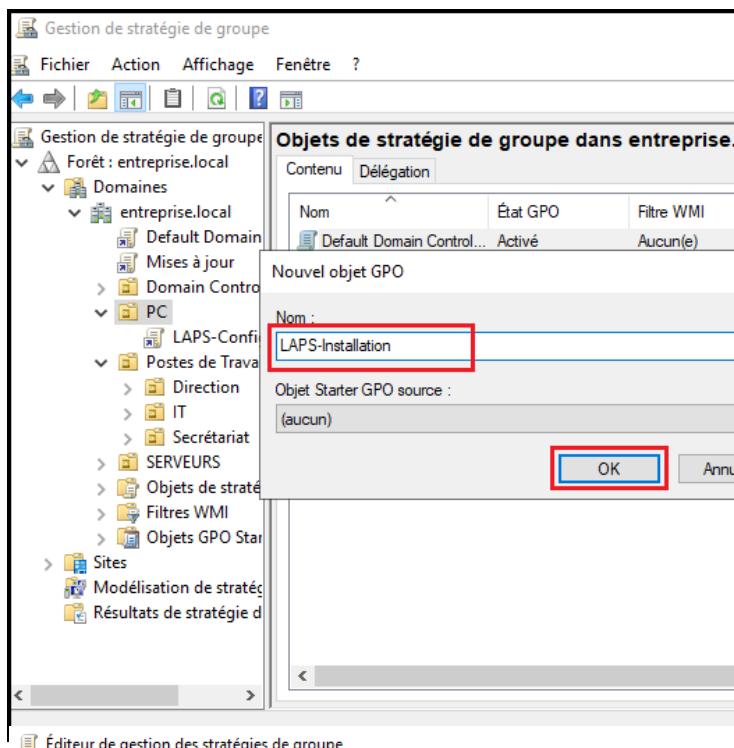


Figure 93 Partage du package LAPS

Comme fait précédemment, lançons la fenêtre de **gestion de stratégie de groupe**, faisons **clic droit** sur l'OU qui nous intéresse puis cliquons sur **Créer un objet GPO dans ce domaine, et le lier ici**. Nommons notre GPO **LAPS-Installation** puis validons.



Dans l'éditeur de gestion de stratégies de groupe, dans **Configurations ordinateur**, développons **Stratégies** puis **Paramètres du logiciel**. Faisons un clic droit sur **Installation de logiciel** puis sur **Nouveau** et enfin **Package**.

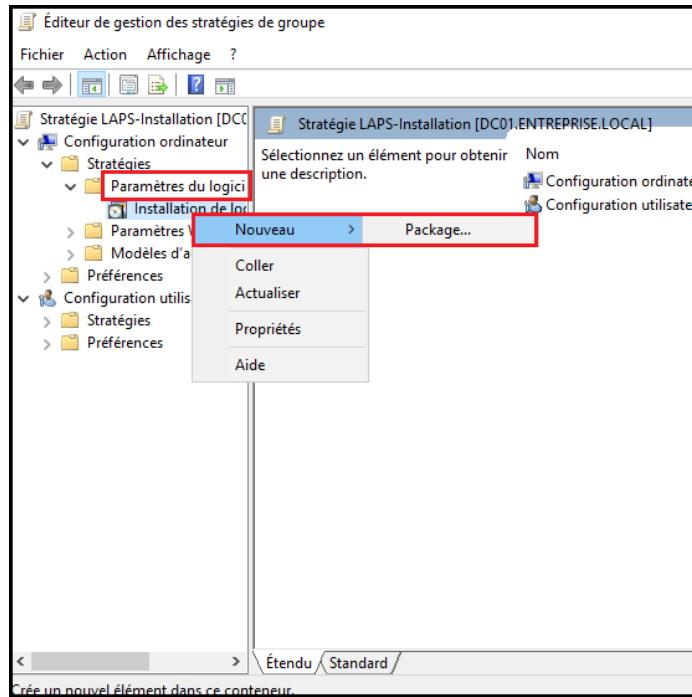


Figure 94 Nouveau package d'installation

Dans la fenêtre qui s'ouvre, naviguons jusqu'au dossier partager dans lequel il y a le package d'installation et sélectionnons-le.

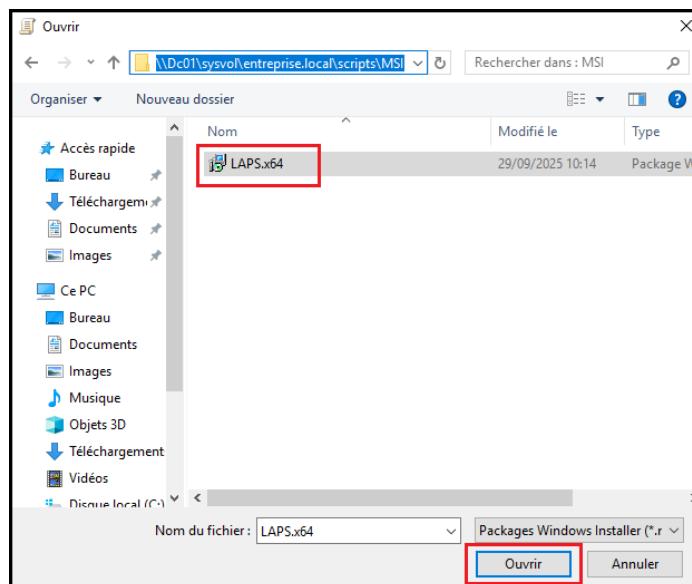


Figure 95 Sélection du package d'installation

Cliquons sur **OK** et nous en avons fini.

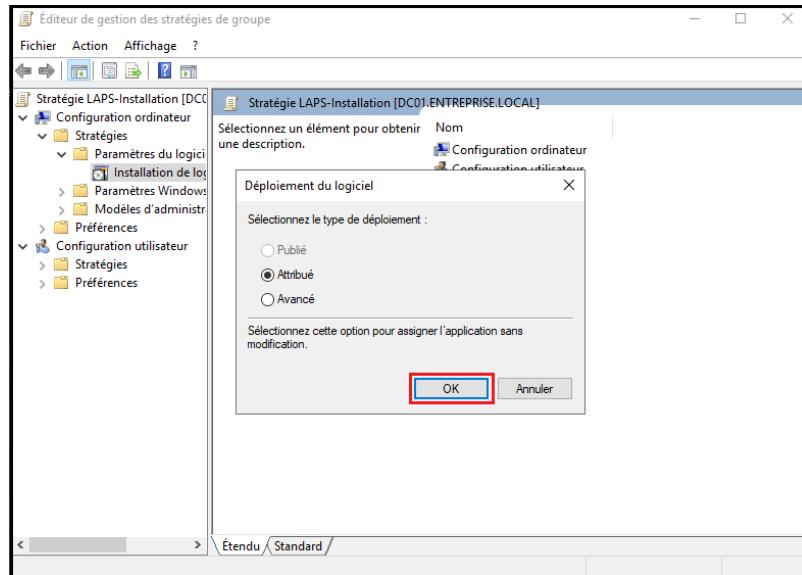


Figure 96 Validation de la GPO

Sur notre machine cliente, dans l'invite de commande, tapons la commande : **gpupdate /force**

```
Invité de commandes - gpupdate /force
Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Directeur1>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.

Les avertissements suivants ont été rencontrés lors du traitement de la stratégie de l'ordinateur :

L'extension côté client de la stratégie de groupe Software Installation n'a pas pu appliquer un ou plusieurs paramètres car les modifications doivent être traitées avant le démarrage système ou la connexion utilisateur. Le système attendra la fin complète du traitement de la stratégie de groupe avant de procéder au prochain démarrage ou à la prochaine connexion pour cet utilisateur. Ceci peut entraîner un ralentissement du démarrage et des performances de démarrage du système.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

Pour plus de détails, ouvrez le journal des événements ou exécutez GPRESULT /H GPReport.htm depuis la ligne de commande pour accéder aux résultats de la stratégie de groupe.

Certaines stratégies d'ordinateurs activées peuvent uniquement être exécutées pendant le démarrage.

OK pour redémarrer ? (O/N)
```

Figure 97 Application de la GPO sur la machine cliente

Après redémarrage, vérifions si LAPS a été correctement installé. Dans les **Paramètres** cliquons sur **Applications** puis sur **Applications installées** et recherchons « **Local** ». Nous constatons que ça a été correctement installé.

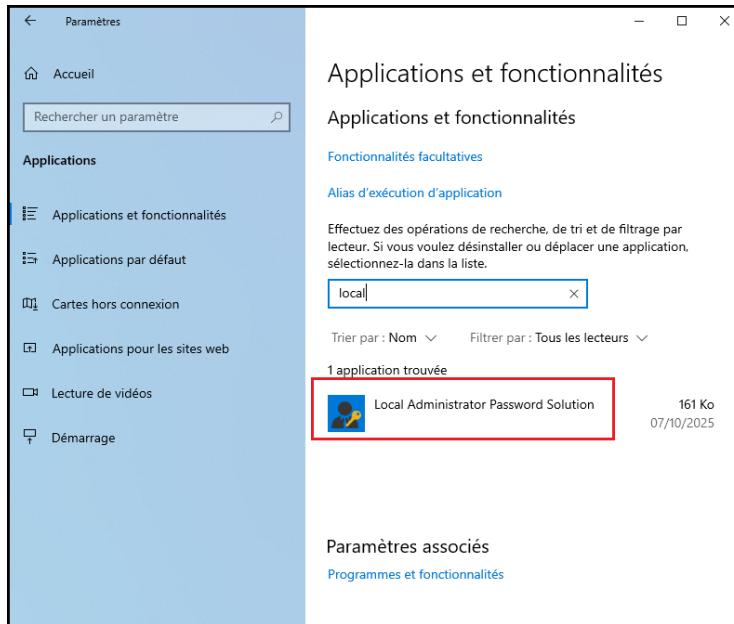


Figure 98 Vérification de l'installation de LAPS sur machine cliente

De retour sur le contrôleur de domaine, pour afficher le mot de passe générer, dans la fenêtre Windows, développons le dossier **LAPS** et exécutons **LAPS UI**

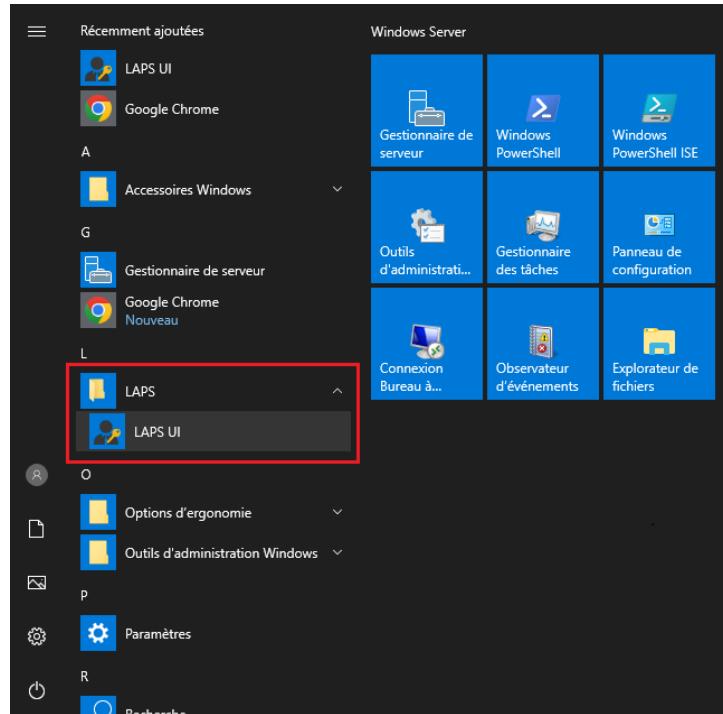


Figure 99 Exécution de l'interface utilisateur de LAPS

En entrant le nom d'un ordinateur du domaine, nous pouvons voir le mot de passe générer, la date d'expiration du mot de passe et nous avons la possibilité de réinitialiser le mot de passe

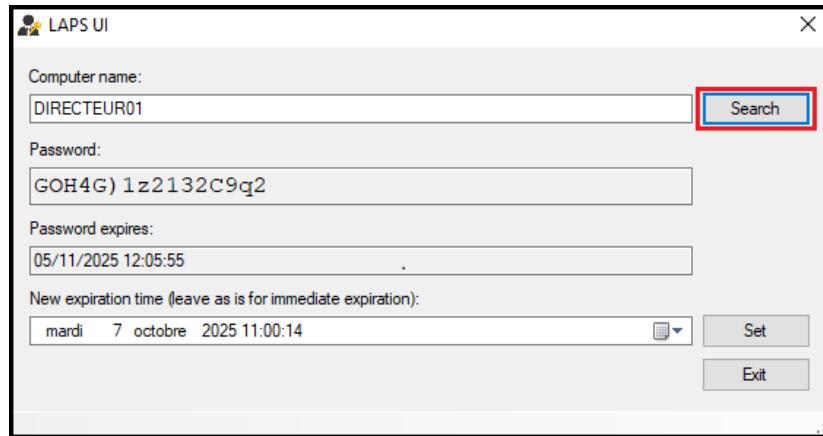


Figure 100 Interface utilisateur de LAPS

Nous venons de terminer nos configurations.

## 5. Perspectives et améliorations futures

Bien que l'infrastructure déployée réponde aux besoins actuels en matière de centralisation et de sécurité, plusieurs pistes d'amélioration peuvent être envisagées pour renforcer davantage la gouvernance du système d'information.

À moyen terme, l'intégration d'un **système de supervision** (tel que **Microsoft System Center ou Zabbix**) permettrait de surveiller en temps réel l'état des serveurs et des postes clients. De plus, la mise en place d'une **solution de sauvegarde centralisée** garantirait une meilleure résilience face aux sinistres.

À plus long terme, il serait intéressant d'étudier la **migration partielle vers des services cloud**, comme **Azure Active Directory** ou **Microsoft Intune**, afin d'étendre la gestion des identités et des mises à jour à des environnements hybrides.

Enfin, une **politique de sensibilisation des utilisateurs** autour de la cybersécurité compléterait la démarche technique, assurant ainsi une sécurité globale, tant humaine que technologique.

## **6. Conclusion**

Le déploiement de l'infrastructure intégrant Active Directory, LAPS et WSUS a été mené à bien avec succès. Cette solution permet désormais une gestion centralisée et sécurisée du parc informatique, éliminant les risques liés aux mots de passe administrateur statiques et offrant un contrôle total sur les mises à jour critiques.

L'automatisation des processus via les Stratégies de Groupe a considérablement renforcé la posture de sécurité tout en simplifiant l'administration quotidienne. Les objectifs initiaux de centralisation, de sécurisation des accès privilégiés et de maîtrise de la maintenance corrective sont ainsi pleinement atteints.

Ce projet constitue une base solide pour l'évolution future de l'infrastructure et démontre l'importance stratégique d'une approche intégrée pour la sécurisation des systèmes d'information.