

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

Historique des versions :

Révision	Date	Objet
1.0.1	02/01/2025	Création du document
1.0.2	04/01/2025	Corrections et mise en forme du document

Auteurs et Intervenants :

Initiales	Nom	Fonction	Organisation - Rôle
YK	Youssef KEITA	Apprenti	BTS-SIO IIA LAVAL

Identification du document :

Document applicable	à compter du 02/02/2025		
Identification du document			
Direction:	IIA Saint-Berthevin / BTS 2eme année		
Objet:	Installation serveur AD sous Windows serveur 2022		
Domaine:	Architecture technique		
Nature:	Procédure d'installation		
N° d'ordre:	0001	Version:	1.0.1
Durée installation	Environ 2 heures.		
Nb pages:	33		
Nom fichier:	Procedure_Installation_SRV-AD_V-1.odt		
Format document:	ODT réalisé avec Libre Office		

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

Table des matières :

I. Objectif du document :.....	3
II. Caractéristique générale :.....	3
III. Pré-requis :.....	3
IV. À qui s'adresse ce document ?.....	3
V. Qu'est ce que Windows server 2022 ?.....	4
VI. Qu'est ce qu'un Active Directory ?.....	4
VII. Installation d'Active Directory :.....	5
1. Nommer le serveur :.....	5
2.....	5
paramétrage de la carte réseau :.....	5
3. Installation :.....	6
VIII. Configuration Active Directory :.....	11
1. Promouvoir le serveur en contrôleur de domaine :.....	11
2. Configuration de la zone DNS :.....	15
2.1 Configuration de la Zone Directe :.....	15
2.2 Configuration de la Zone Indirecte :.....	18
IX. Gestion des Utilisateurs et Ordinateurs dans Active Directory :.....	26
1. Créer une Unité d'Organisation (UO) :.....	27
1. Créer un Utilisateur :.....	29
3. Créer un groupe :.....	32
X. Configuration des GPO :.....	34
Que ce qu'un GPO ?.....	34
GPO 1 : Connecter un lecteur réseau en GPO :.....	35
1-) Créer la GPO :.....	35
2-) Tester la GPO :.....	41
GPO 2 : Déployer les applications (Chrome et Libre office) :.....	41
Étape 1 :Préparer les fichier d'installation.....	41
Étape 2 : Partager le dossier (DEPLOIEM-APPLI-LOGICIEL).....	41
Étape 3 : Créer l'OU pour stocker les PC :.....	46
Étape 4 : Créer la stratégie de groupe pour déployer (Chrome et libre Office).....	46
Étape 5 : Modifier La GPO.....	47
GPO 3 : Déployer l'Agent GLPI sur les postes Utilisateur Windows :.....	49
Étape 1 :Préparer les fichier d'installation.....	49
Étape 2 : Créer la stratégie de groupe pour déployer l'agent GLPI.....	50
Étape 3 : Modifier la GPO pour créer un script de démarrage.....	51
Étape 4 : Activer L'inventaire dans GLPI :.....	54
Phase de test : Test du déploiement des GPO.....	55

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

I. Objectif du document :

Fournir un guide clair et structuré pour installer, configurer et sécuriser un serveur Active Directory (AD) sur Windows Server 2022. l'objectif est de centraliser la gestion des ressources réseau, des comptes utilisateurs et des politiques de sécurité tout en facilitant son utilisation, sa maintenance et le transfert de compétences à d'autres administrateurs.

II. Caractéristique générale :

Expression des besoins :

Mettre en place une solution interne permettant de centraliser la gestion des utilisateurs, des groupes, et des ressources réseau grâce à un environnement Active Directory. Cela inclut la sécurisation des échanges, l'intégration avec les services réseau existants (DNS, DHCP, etc.), et la définition de politiques de sécurité cohérentes.

1. Gestion centralisée des identités et des accès :

- Installer et configurer un domaine Active Directory permettant de gérer les utilisateurs, groupes, et machines via une architecture centralisée.

2. Sécurisation et résilience :

- Mettre en place des politiques de mots de passe, des audits de sécurité, et des sauvegardes régulières pour protéger les données et garantir la continuité des services.

3. Personnalisation et extension :

- Configurer des GPO (Group Policy Objects) pour définir des règles spécifiques (accès aux ressources, paramètres de sécurité, etc.) et permettre une compatibilité avec des services tels que les VPN, serveurs de fichiers, ou applications métier.

III. Pré-requis :

- Un serveur Windows Server 2022 avec accès administrateur.
- Une configuration réseau fonctionnelle avec une adresse IP statique.

IV. À qui s'adresse ce document ?

Ce guide s'adresse aux administrateurs systèmes et réseaux ayant des compétences solides en environnement Microsoft Windows Server. Une maîtrise des principes liés aux domaines, aux rôles serveur (DNS, DHCP, etc.) et aux stratégies de groupe est essentielle.

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

V. Qu'est ce que Windows server 2022 ?

Windows Server 2022 est la dernière version du système d'exploitation pour serveurs de Microsoft, conçu pour offrir des services réseau et des fonctionnalités avancées aux entreprises. Cette version est basée sur Windows 10, avec des améliorations en matière de sécurité, de performance, et de prise en charge des environnements Cloud hybrides.

Principales fonctionnalités pour l'entreprise :

- **Réseau** : Serveur DHCP et DNS pour la gestion des adresses IP et des noms de domaine.
- **Gestion des utilisateurs et des accès** : Serveur Active Directory pour la gestion centralisée des utilisateurs, groupes, et permissions.
- **Accès distant** : Serveur de connexion RDS (Remote Desktop Services) pour les connexions de bureau à distance.
- **Gestion des fichiers et des impressions** : Serveur de fichiers DFS pour le partage et la réplication de données, ainsi qu'un serveur d'impression centralisé.

Windows Server 2022 se distingue par ses améliorations de sécurité intégrées, comme la protection avancée contre les menaces (Secured-core server) et les fonctionnalités de chiffrement avancées, notamment dans les environnements de virtualisation. Conçu exclusivement pour les serveurs, il n'est ni recommandé ni rentable pour une station de travail classique, car le coût de la licence est nettement plus élevé que celui de Windows pour postes de travail (professionnel ou familial) et il est optimisé pour la gestion des services réseau et Cloud pour les entreprises. agit comme un relais, transmettant tous les emails via Office 365 avant qu'ils n'atteignent leur destination finale.

VI. Qu'est ce qu'un Active Directory ?

Active Directory (AD) est un annuaire LDAP propriétaire de Microsoft utilisé pour centraliser la gestion des comptes utilisateurs et des ressources au sein d'un réseau. Il s'agit d'un contrôleur de domaine qui combine les services LDAP (pour la gestion des utilisateurs et des ressources) et DNS (pour la résolution de noms).

Fonctionnalités principales :

- **Gestion centralisée des comptes utilisateurs** : Active Directory permet de créer et de gérer les comptes des utilisateurs de manière centralisée, leur donnant accès aux ressources du réseau avec un seul identifiant.
- **Connexion unifiée** : Une fois qu'un utilisateur est inscrit dans l'Active Directory, il peut se connecter à tout ordinateur faisant partie du domaine en utilisant ses identifiants (nom et prénom).

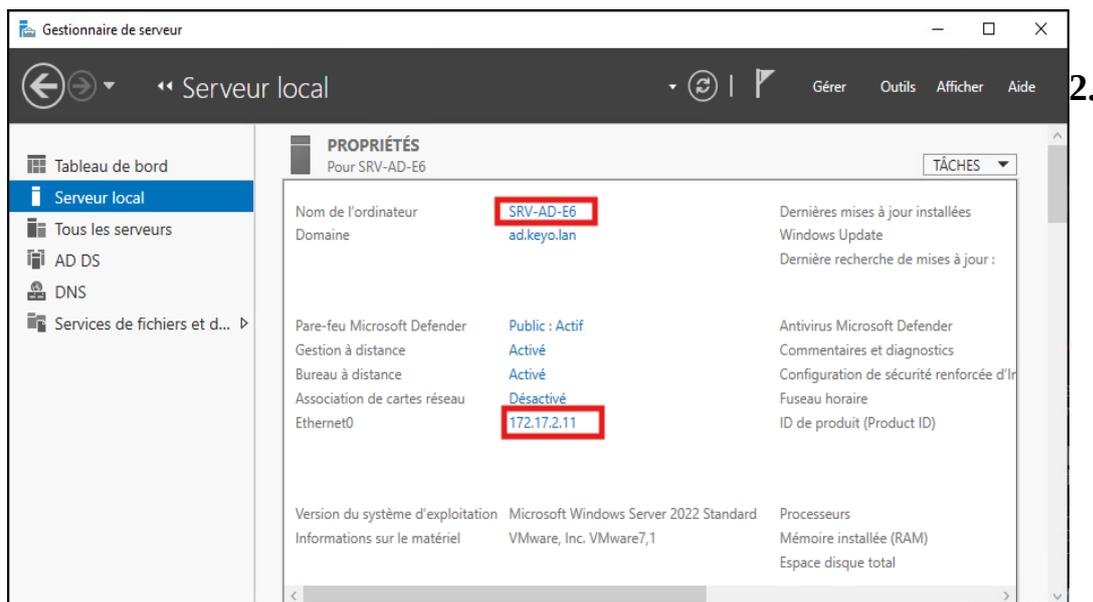
- **Group Policy Objects (GPO)** : AD permet également de mettre en place des règles de sécurité appelées GPO, qui peuvent être appliquées aux utilisateurs ou aux ordinateurs. Ces règles permettent d'administrer la sécurité et les paramètres du réseau de manière cohérente et contrôlée.

En résumé, Active Directory simplifie la gestion des utilisateurs, des permissions et des règles de sécurité dans un réseau d'entreprise.

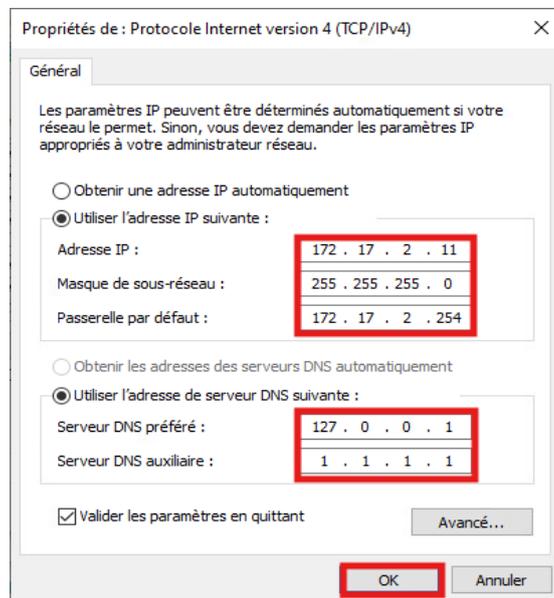
VII. Installation d'Active Directory :

1. Nommer le serveur :

- Allez dans « Serveur local », cliquer sur le nom de l'ordinateur, puis « Modifier » et faites « **OK** » pour valider.



paramétrage de la carte réseau :

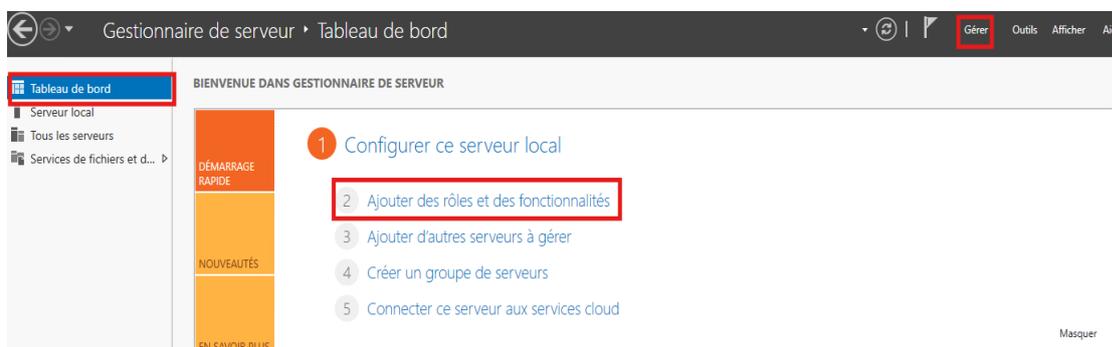


3. Installation :

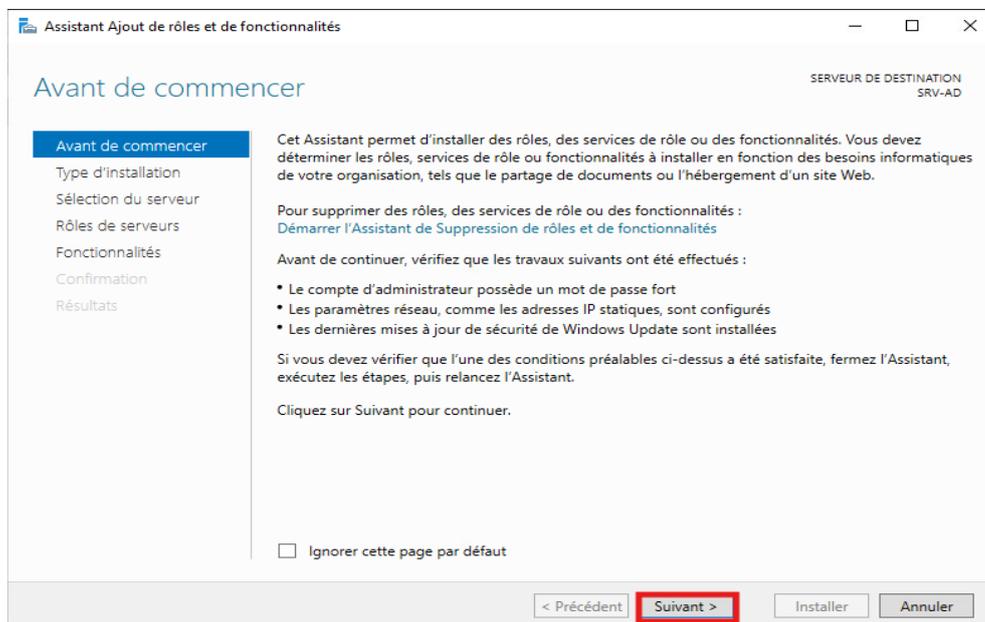
Pour installer Active Directory, il faut ajouter les rôles et des fonctionnalités correspondant.

Pour ce faire :

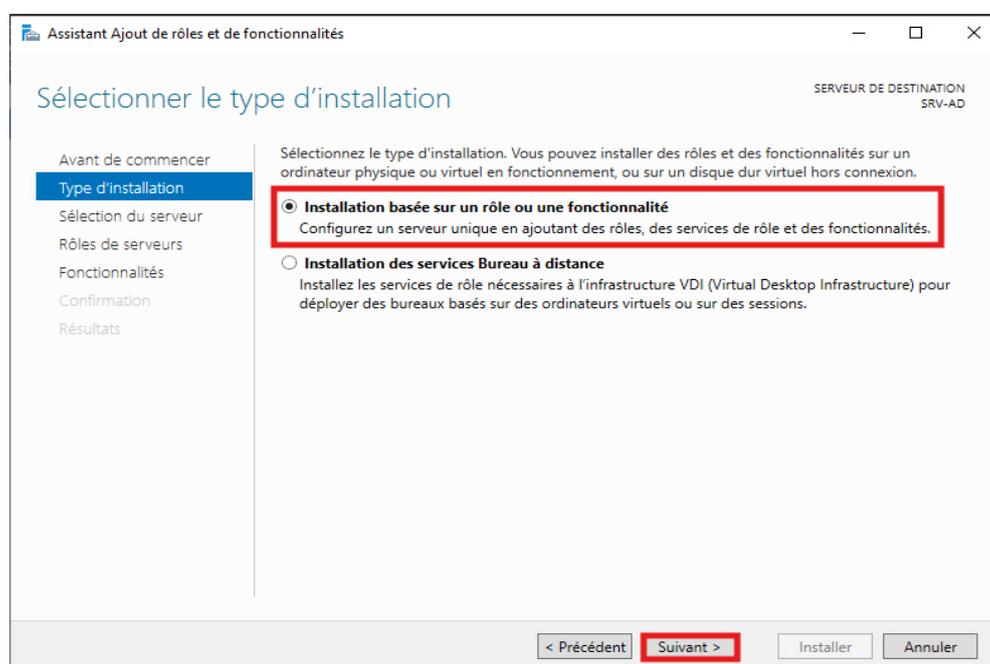
- Ouvrez le Gestionnaire de serveur et accédez aux options d'ajout de rôles, soit (en cliquant sur « **Ajouter des rôles et des fonctionnalités** » ou dans l'option « **Gérer** », puis « **Ajouter des rôles et des fonctionnalités** ») .



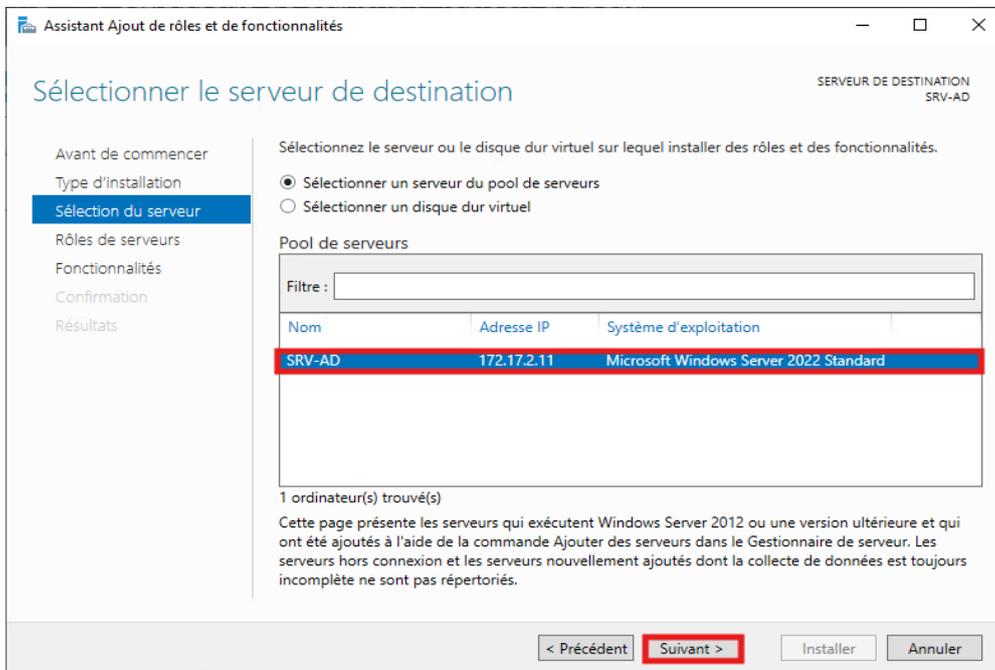
La page « **Assistant Ajout de rôles et de fonctionnalités** » s'affiche, faites « **Suivant** »



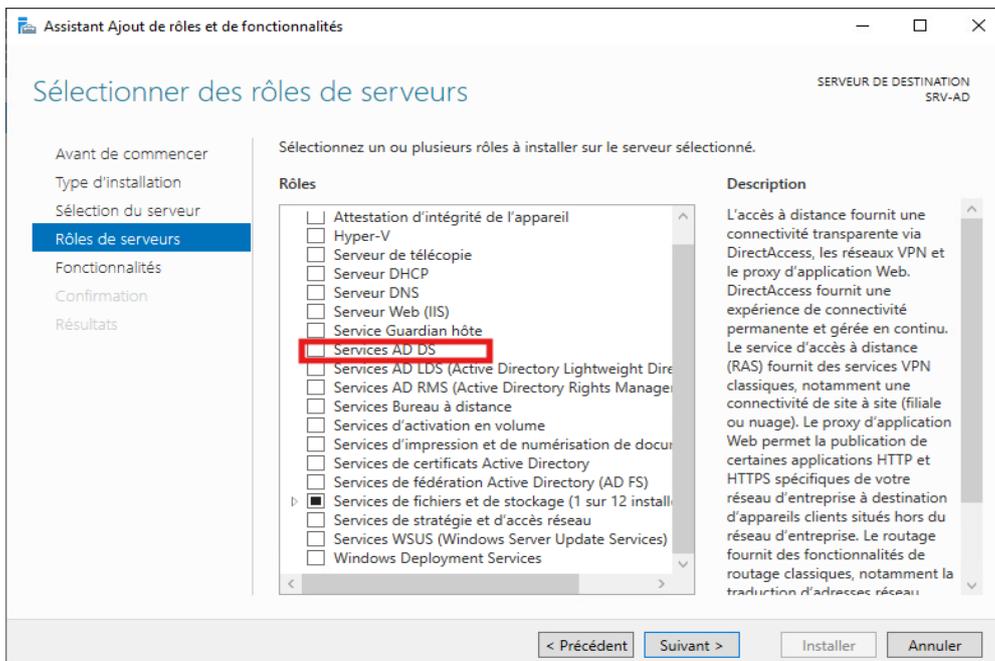
- À l'étape « **Type d'installation** », laisser l'option « **Installation basés sur un rôle ou une fonctionnalité** » par défaut et faites « **Suivant** ».



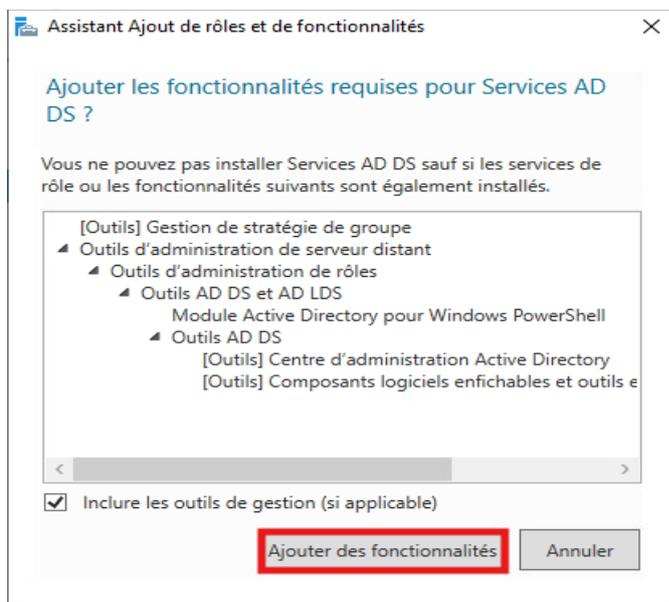
À l'étape « **Sélection du serveur** », sélectionner votre serveur s'il y'en a plusieurs.



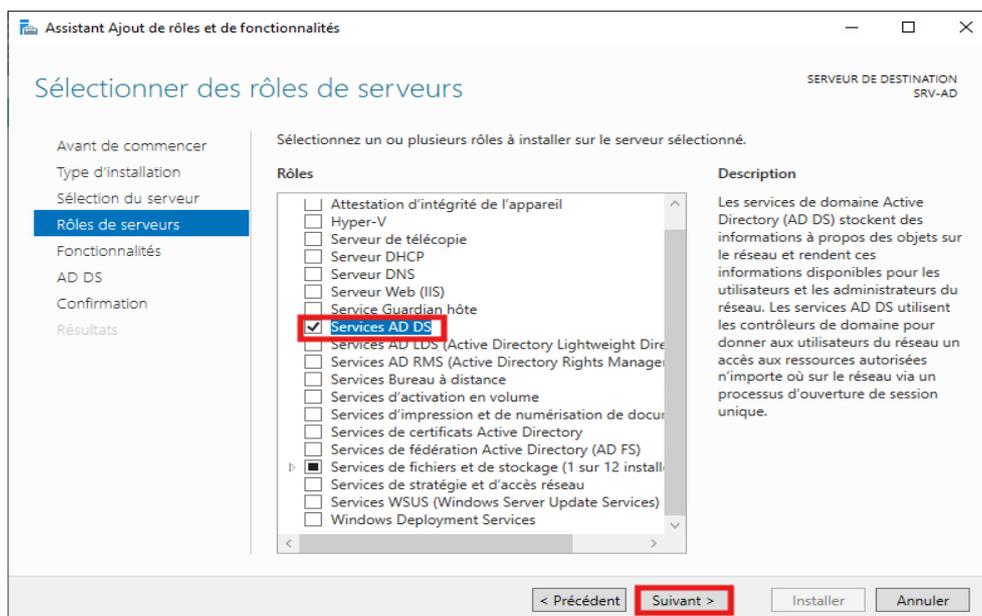
- Dans la page « **Rôles de serveurs** », On sélectionne uniquement le service "AD DS", car le DNS est installé automatiquement avec, une fois cliquer dessus,



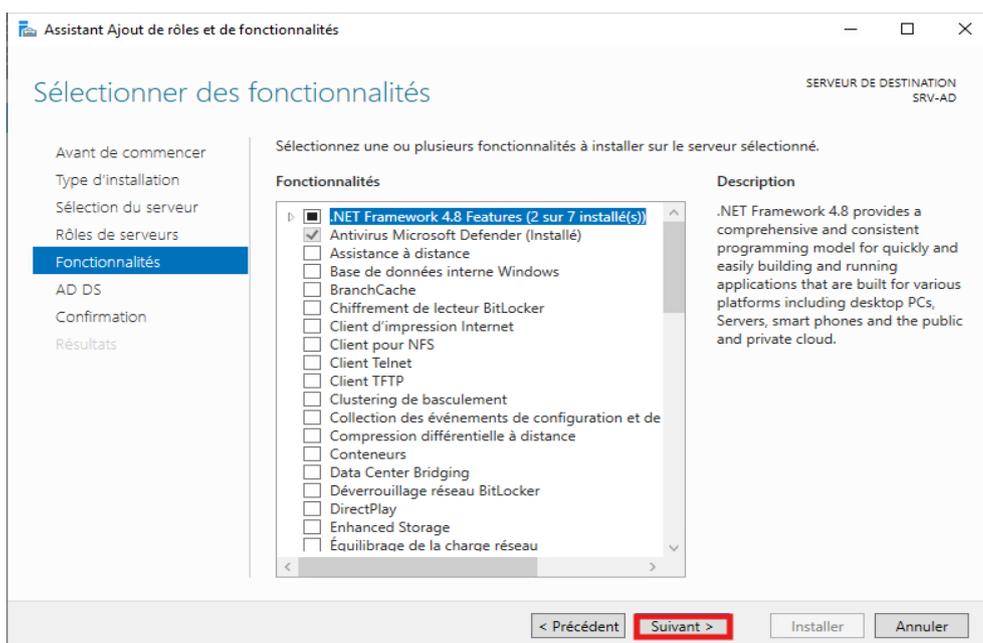
- Ensuite, les détails des fonctionnalités requises pour Services « **AD DS** » qui seront installés s'affiche faites "**Ajouter des fonctionnalités**".



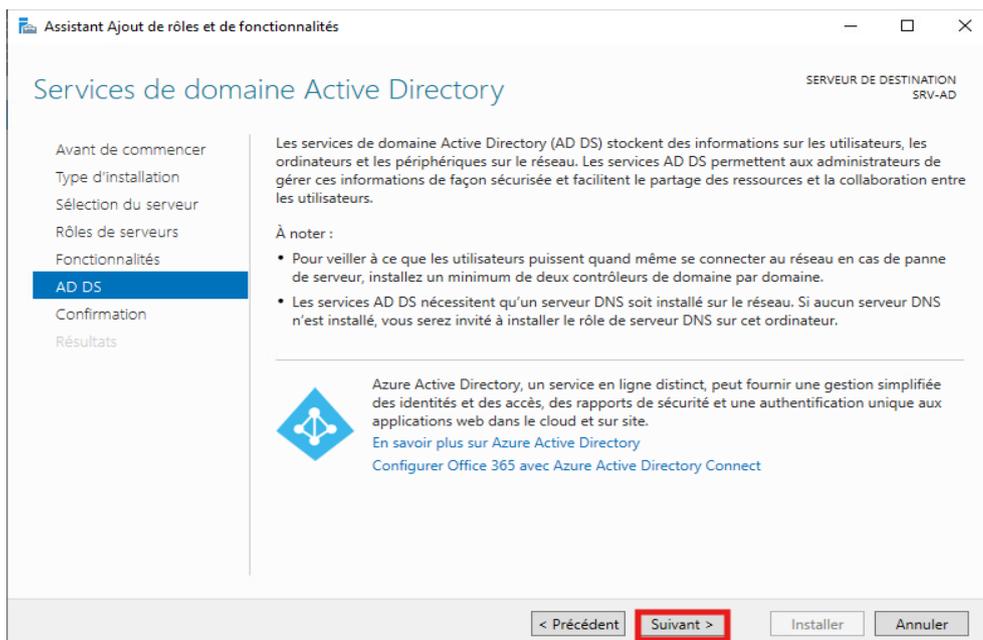
- Toujours dans « Rôles de serveurs », vous verrez que le rôle de **Services AD DS** est coché, faites « **Suivant** ».



- À l'étape « **Fonctionnalités** », ayant aucune fonctionnalité à ajouter, on peut faire "Suivant".



- À l'étape « **AD DS** », On a une description du service et des recommandations, faites "Suivant".



	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

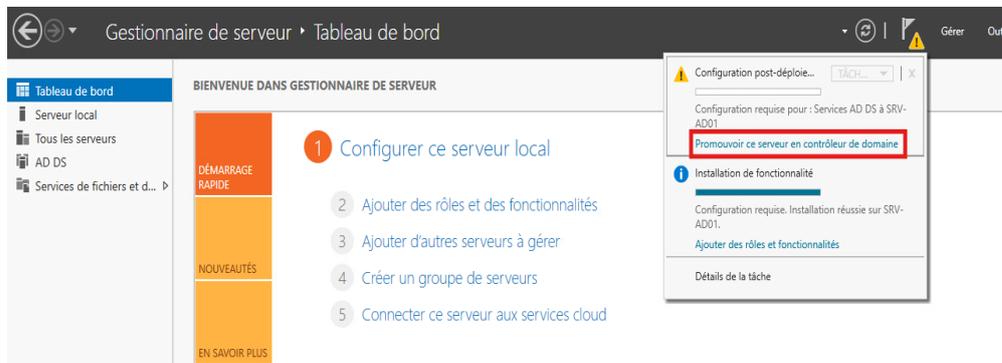
- Dans la page de « **Confirmation** », on voit le récapitulatif de ce qui va être installé, cliquer sur "**Installer**" et attendre la fin de l'installation.

VIII. Configuration Active Directory :

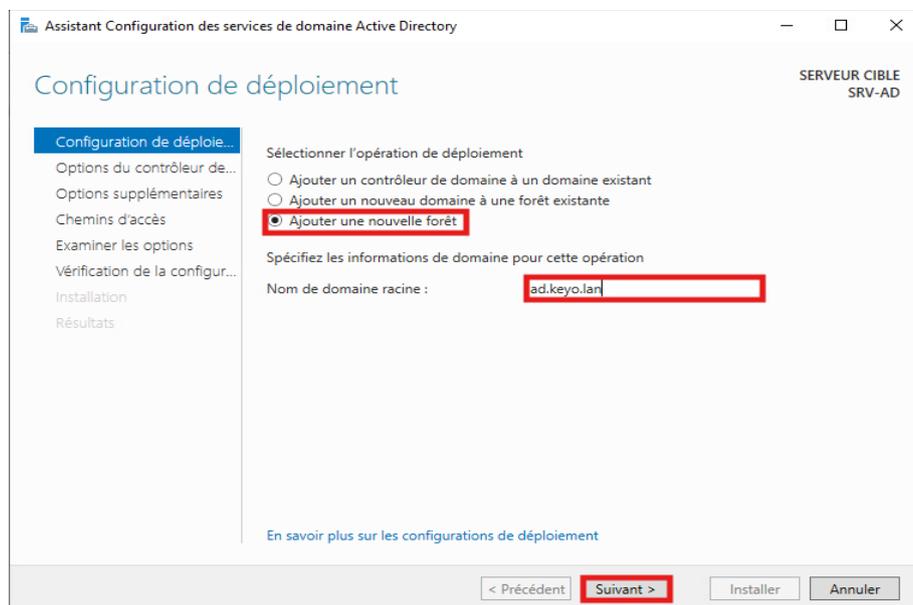
1. Promouvoir le serveur en contrôleur de domaine :

Une fois le service installé, il faut promouvoir le serveur en contrôleur de domaine.

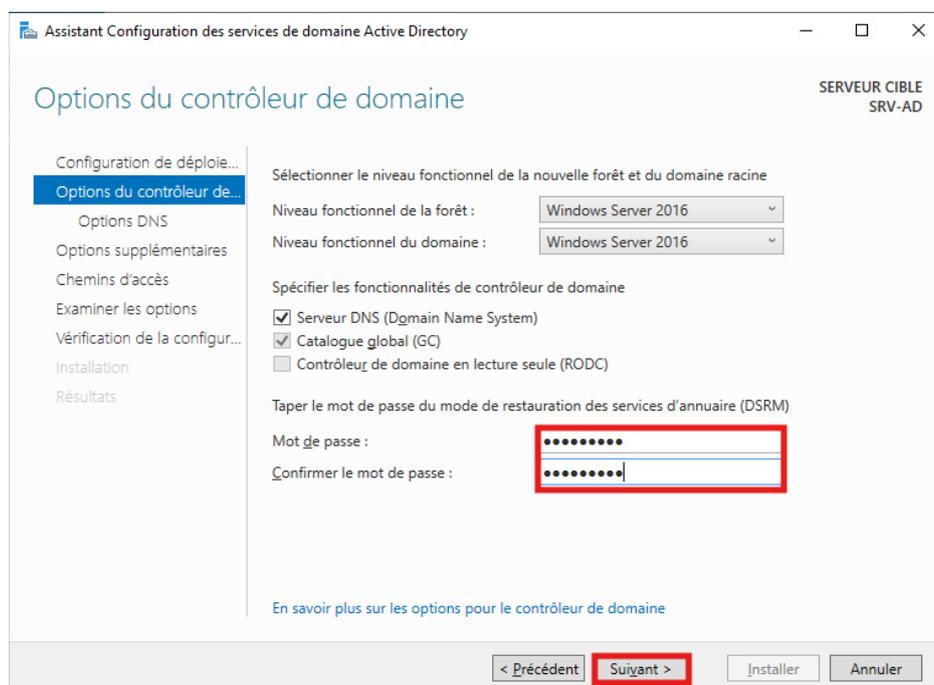
- Cette option est dans le gestionnaire de serveur en haut à gauche dans notifications.



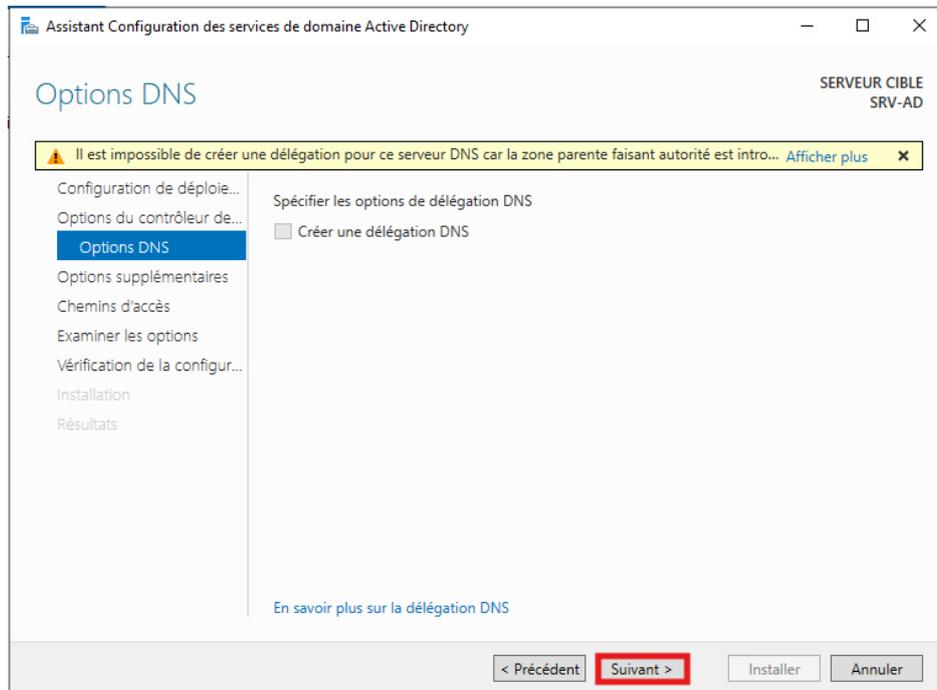
- Cliquer sur « **Promouvoir ce serveur en contrôleur de domaine**»,
- Ensuite, la page « **Assistant Configuration des services de domaine Active Directory** » s'affiche.
- À l'étape « **Configuration de déploiement** », sélectionner « **Ajouter une nouvelle forêt** », puis dans la case « **Nom de domaine racine** », taper votre nom de domaine et faites « **Suivant** ».



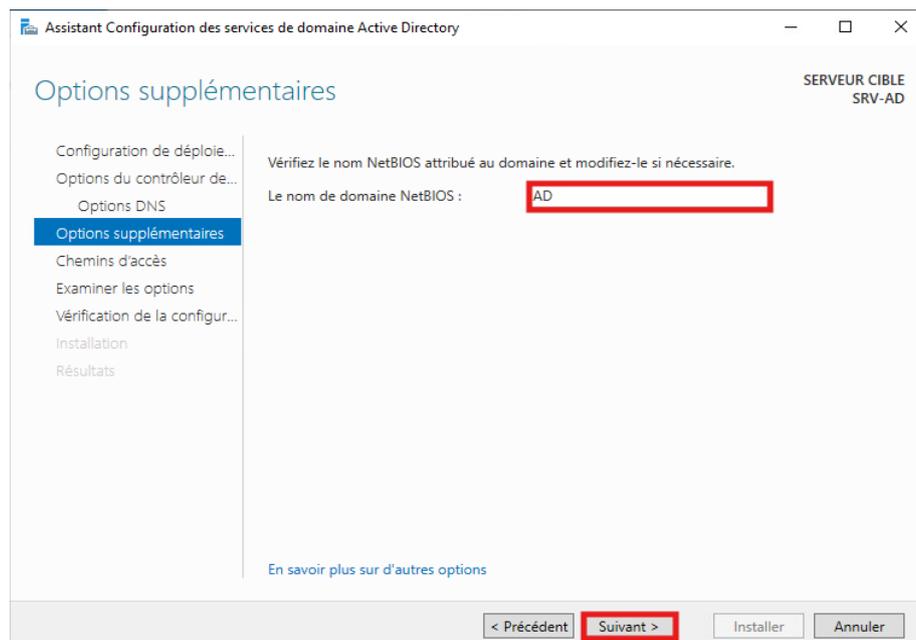
- À l'étape « Options du contrôleur de ... », saisissez le mot de passe du mode de restauration des services d'annuaire ici (!Keita@53», puis faites « Suivant ».



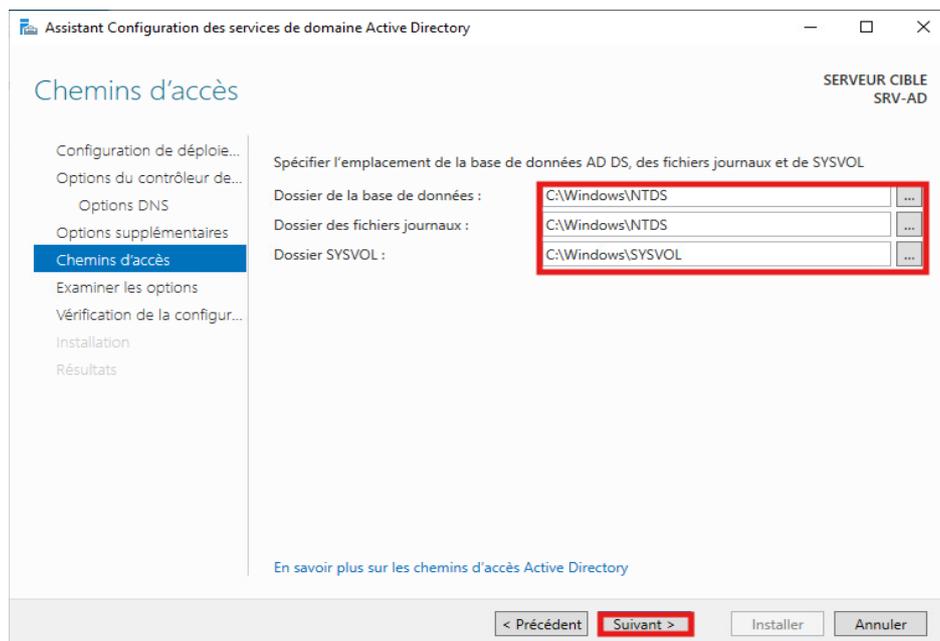
- À l'étape « **Options DNS** », aucune zone de délégation n'existe, faites "**Suivant**".



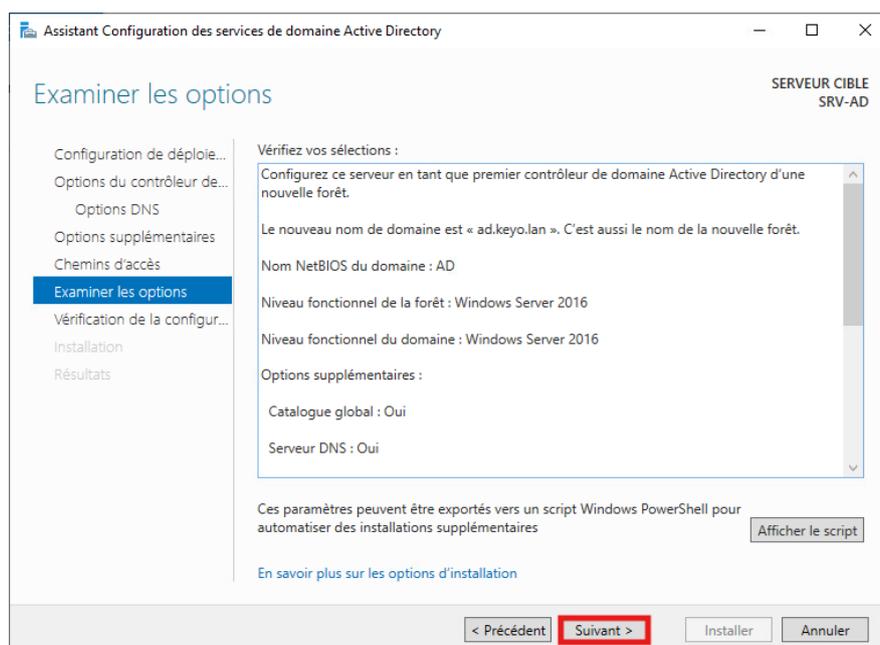
- À l'étape « **Options Supplémentaires** », On vérifie que le nom NetBIOS correspond à notre DNS, faites « **Suivant** ».



- À l'étape « **Chemins d'accès** », les choix des emplacements peuvent être laissés par défaut et cliquer sur « **Suivant** ».

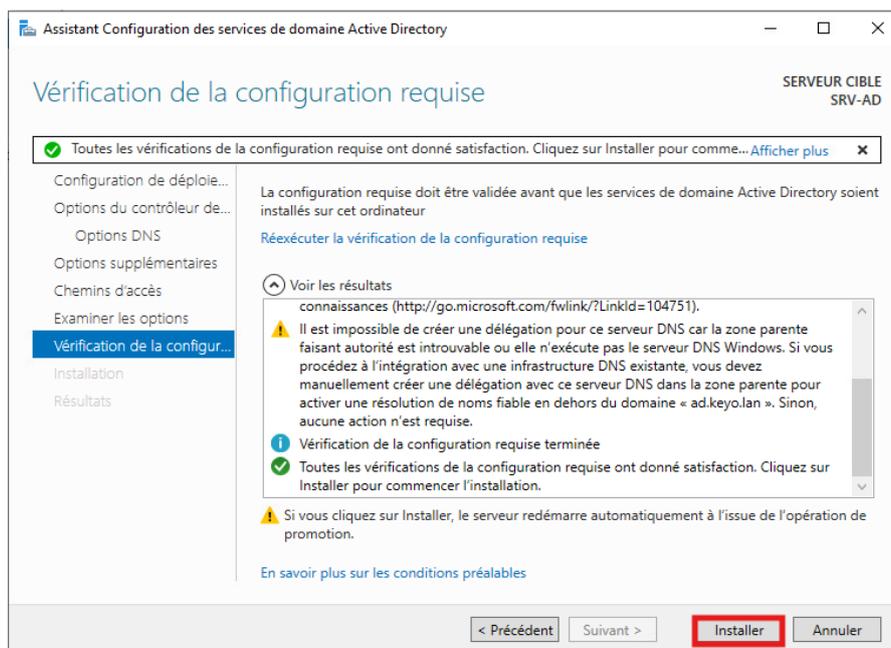


- À l'étape « **Examiner les options** », nous avons le récapitulatif de la configuration de notre AD et faites « **Suivant** ».



	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

- À l'étape « **Vérification de la configuration** » nous pouvons donc installer notre Active Directory avec le bouton "Installer". Le serveur va redémarrer.



2. Configuration de la zone DNS :

2.1 Configuration de la Zone Directe :

La zone directe d'un DNS permet de convertir un nom de domaine en adresse IP.

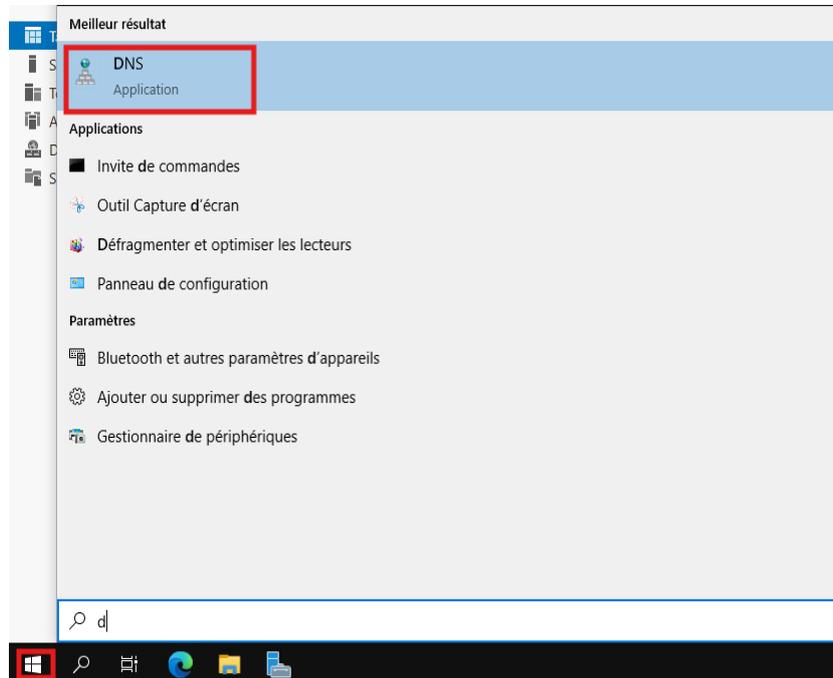
Exemple :

www.google.fr = 172.217.19.35

Grâce à cette correspondance, il est plus simple de retenir un nom de site web qu'une suite de chiffres.

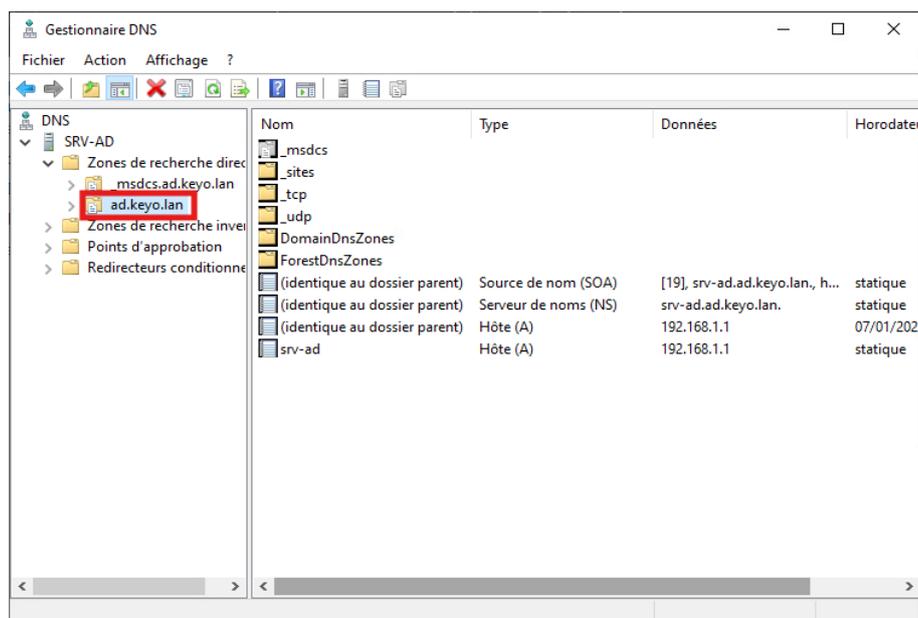
Pour configurer la zone Directe de notre DNS :

- Cliquez sur le menu « **Démarrer** », taper DNS pour accéder aux paramètres de votre serveur DNS et cliquez dessus.



Voici à quoi ressemble la zone DNS principal, qui a été créé automatiquement grâce au contrôleur de domaine.

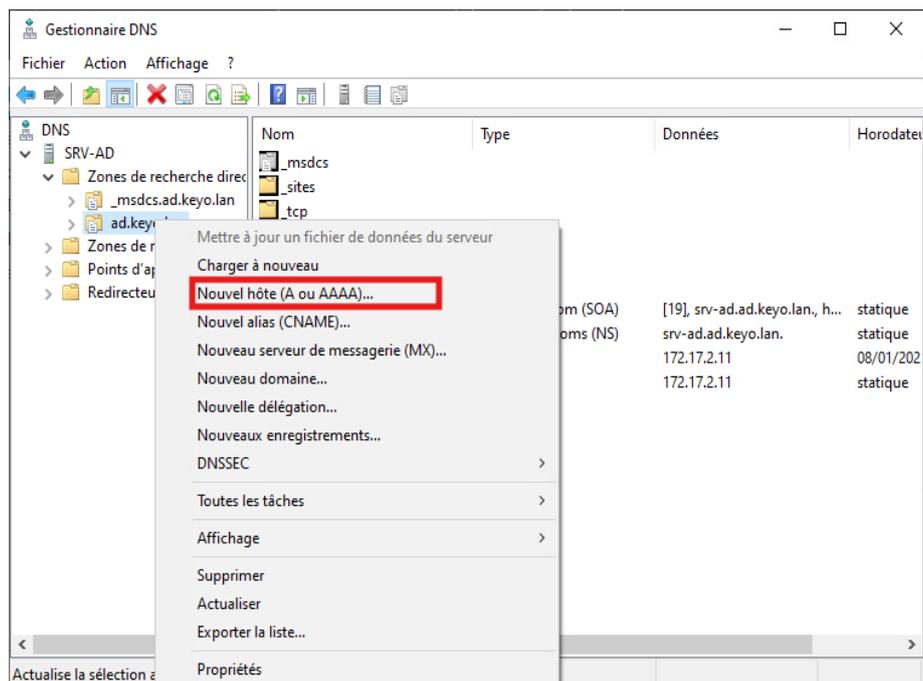
Info : Il faut d'abord configurer la Zone de recherche indirect pour pouvoir configurer la Zone de recherche direct, si non cela affiche un message d'erreur.



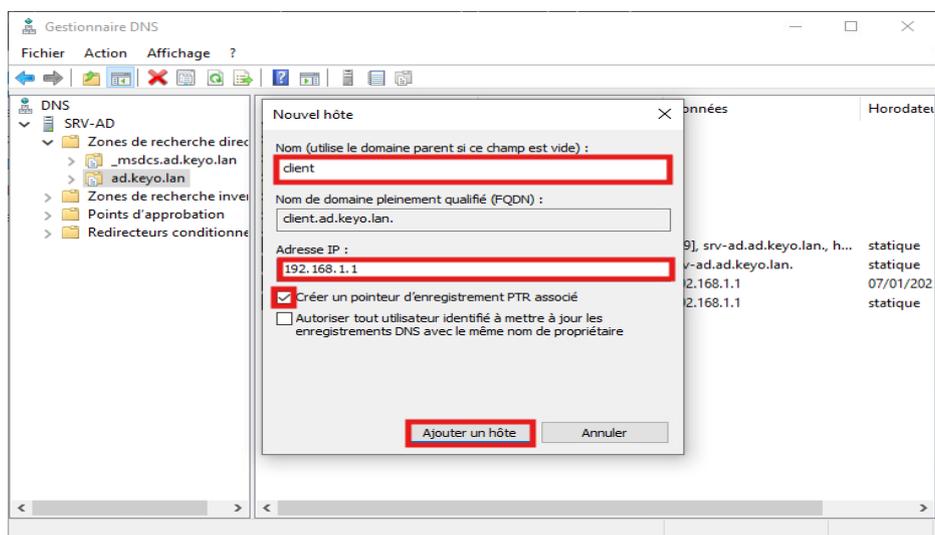
Nous allons ajouter de nouvelles entrées dans notre zone directe de notre DNS :

Pour ajouter une nouvelle entrée :

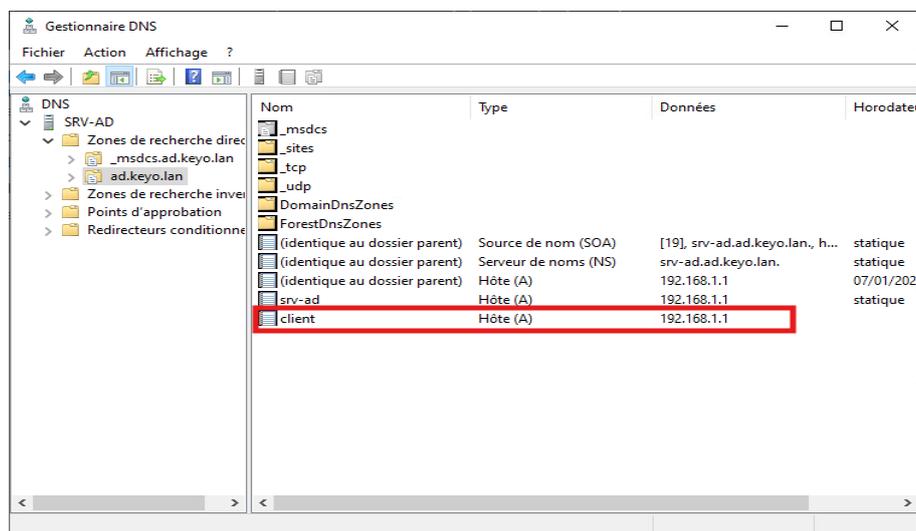
- Faites un clic droit dans la zone, puis cliquer sur « **Nouvelle hôte (A ou AAAA)...** » ou A : IPv4 et AAAA : IPv6.



Dans le champ "Nom" taper le nom, ensuite entrer "IP" du serveur AD dans le champ « Adresse IP » et il est recommandé de cocher la création du pointeur PTR, puis cliquer sur "Ajouter un hôte"



Comme nous pouvons le voir l'hôte client est bien créer.



2.2 Configuration de la Zone Indirecte :

La zone indirecte (ou zone inverse) d'un DNS permet de convertir une adresse IP en nom de domaine.

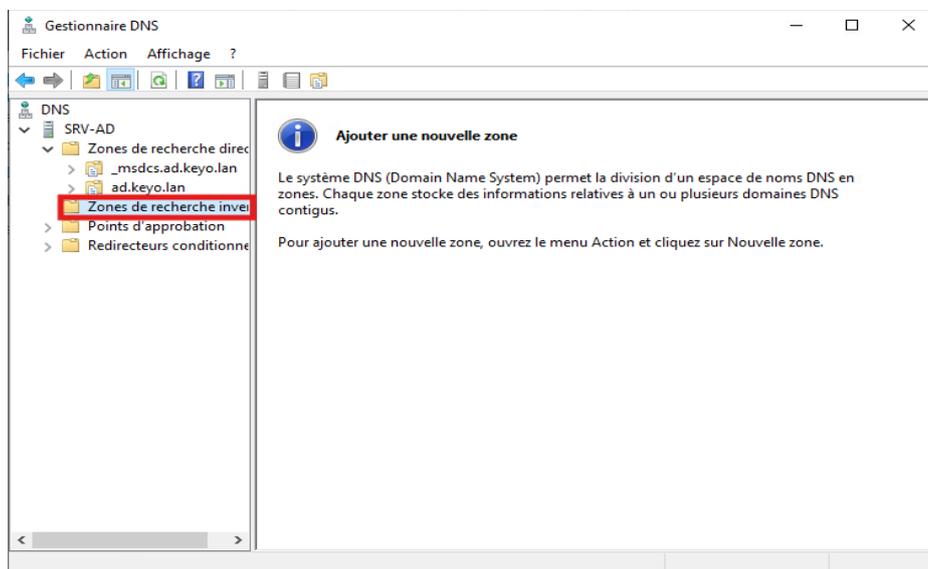
Par exemple :

172.217.19.35 = www.google.fr

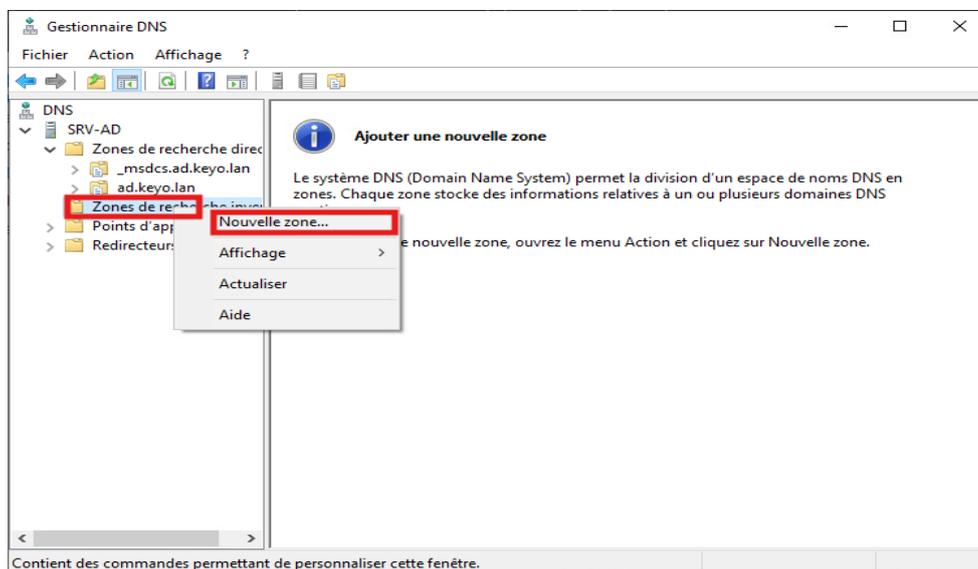
Cette configuration est utile pour certaines applications ou pour que d'autres serveurs DNS puissent identifier le nom de domaine associé à une IP. Pour configurer la Zone Indirecte dans notre DNS, accédez aux paramètres de votre serveur DNS.

Pour ce faire :

- On clique sur « **Zones de recherche inverser** », par défaut la zone n'existe pas nous devons la créer.



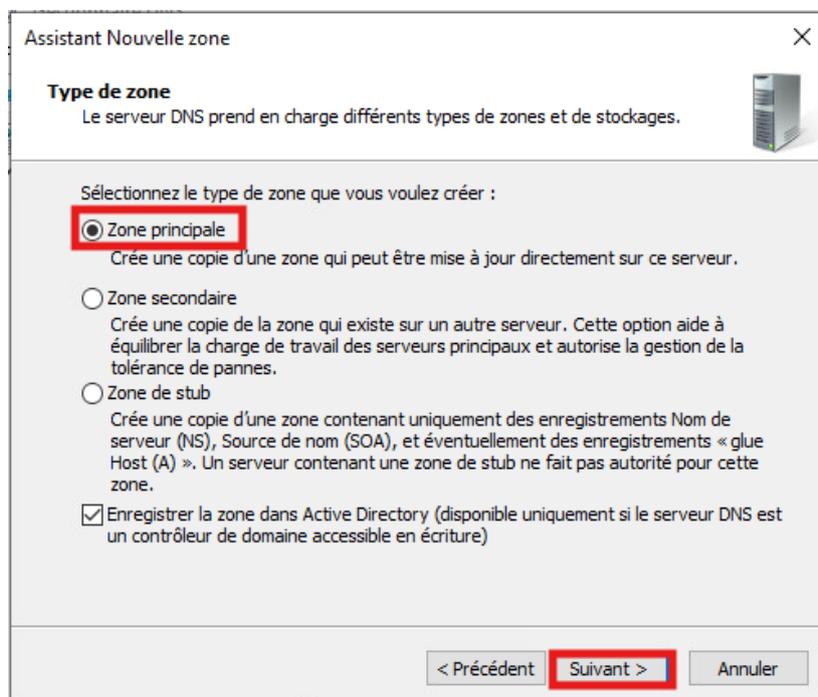
- Faites un clic droit sur « **Zones de recherche inverser** », puis cliquez sur « **Nouvelle zone...** »



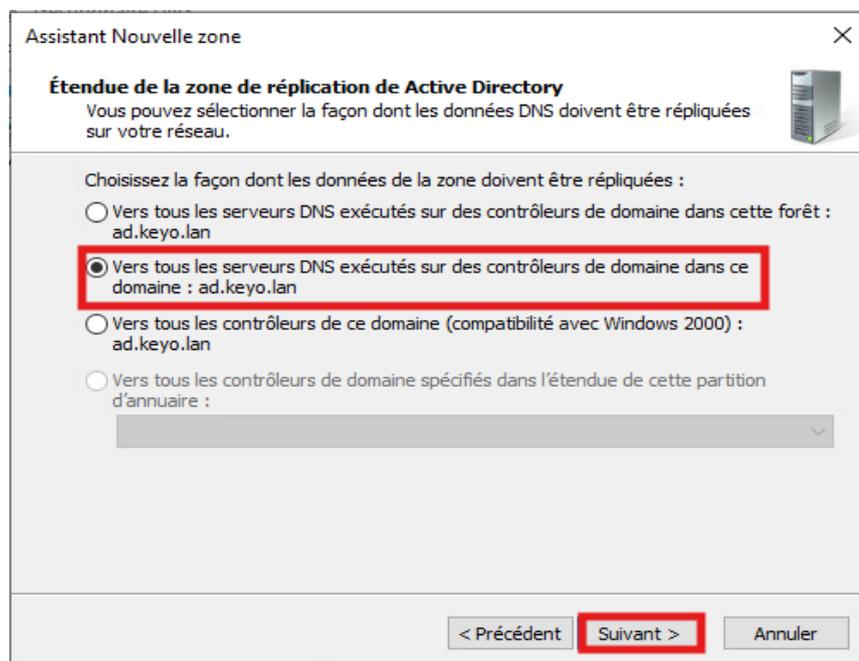
- Une assistance se lance afin de créer notre Zone, faites « **Suivant** ».



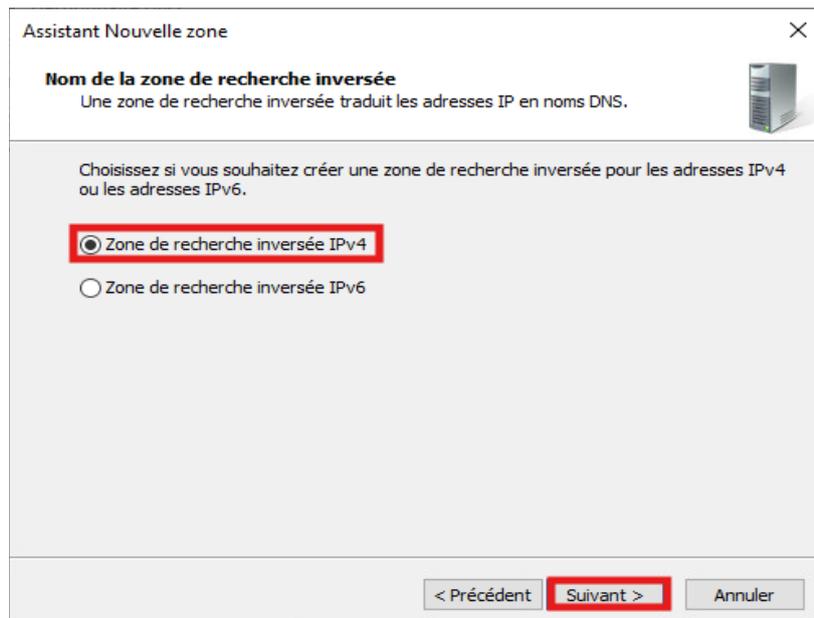
- Dans la page « **Type de zone** », sélectionner "**Zone Principale**", puis "**Suivant**".



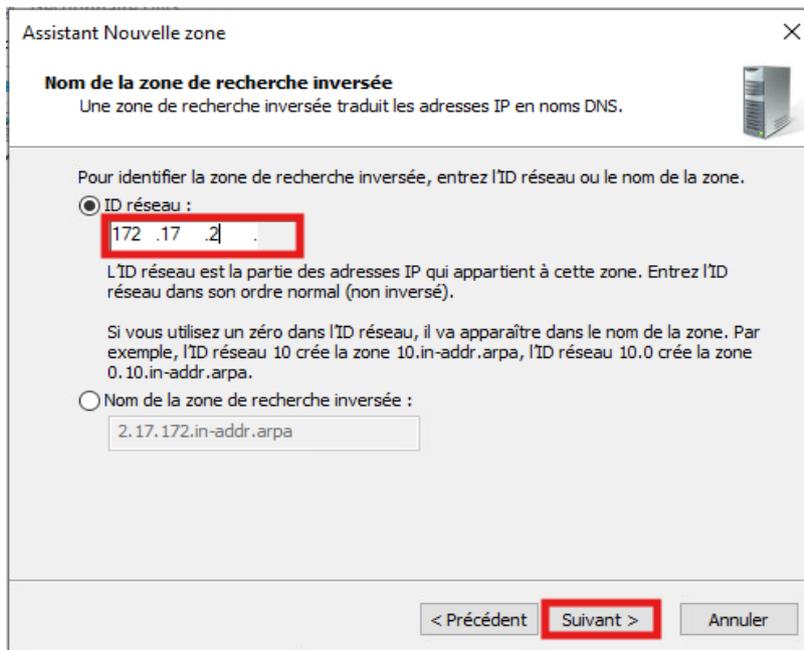
- À l'étape suivant « **Étendu de la zone...** », laisser le choix par défaut qui est la seconde option, puis cliquez sur "**Suivant**".



- Dans la page « **Nom de la zone de recherche inversée** » Notre zone de recherche inversée est en IPv4, laisser l'option IPv4 par défaut, puis faire "**Suivant**".



- Ensuite nous devons mettre notre ID réseau qui va créer automatiquement notre nom de zone inversée, puis "**Suivant**".



Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

172 .17 .2

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

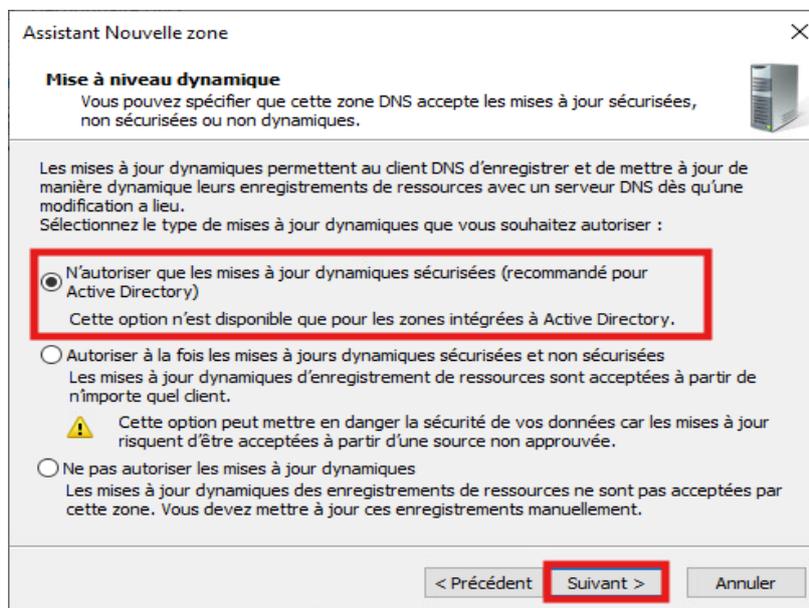
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

2.17.172.in-addr.arpa

< Précédent **Suivant >** Annuler

- Puis laisser la première option par défaut et cliquer sur "**Suivant**".



Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

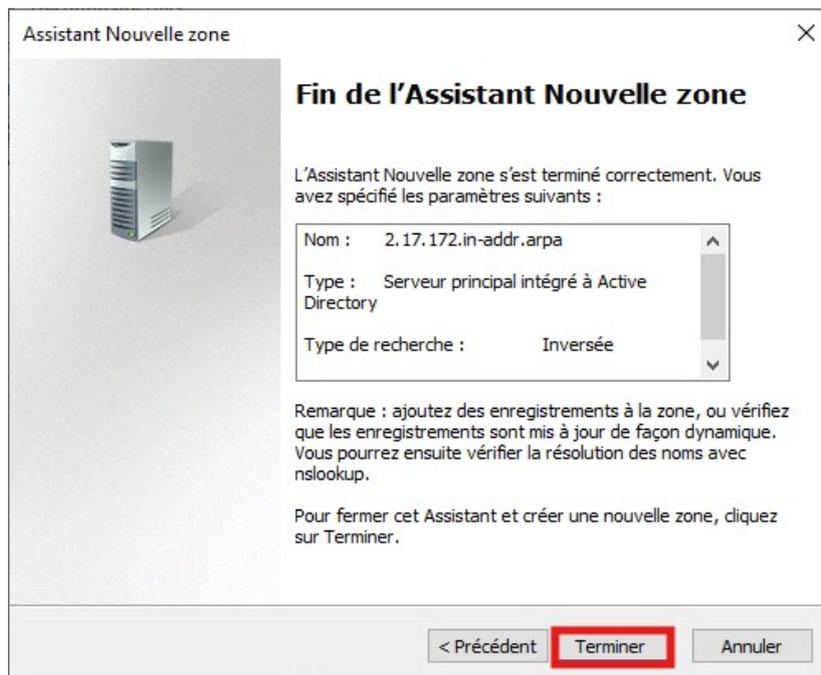
N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

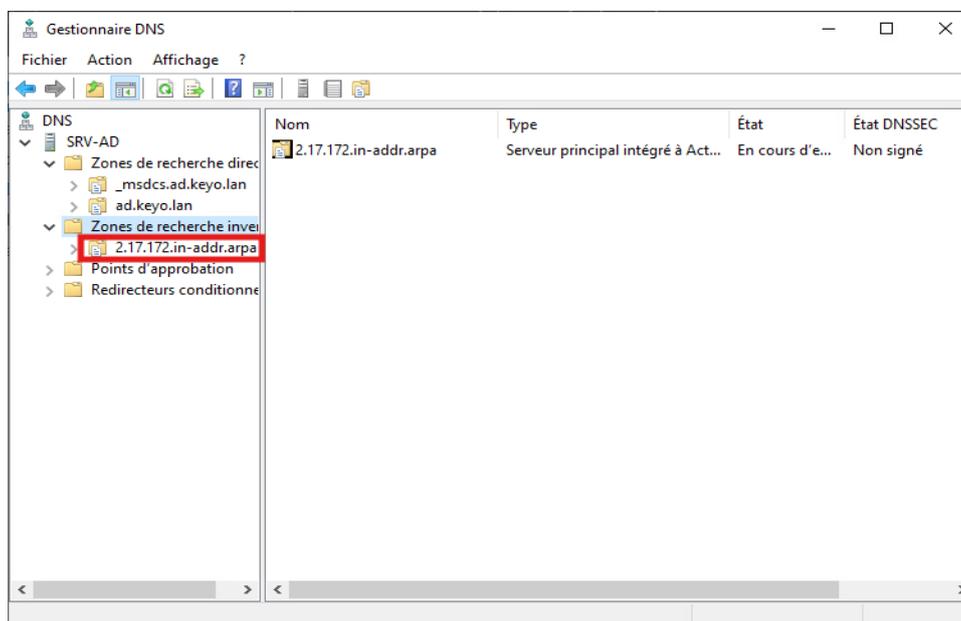
Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent **Suivant >** Annuler

- Une fois fini, nous avons un récapitulatif. Pour terminer cliquer sur "**Terminer**".

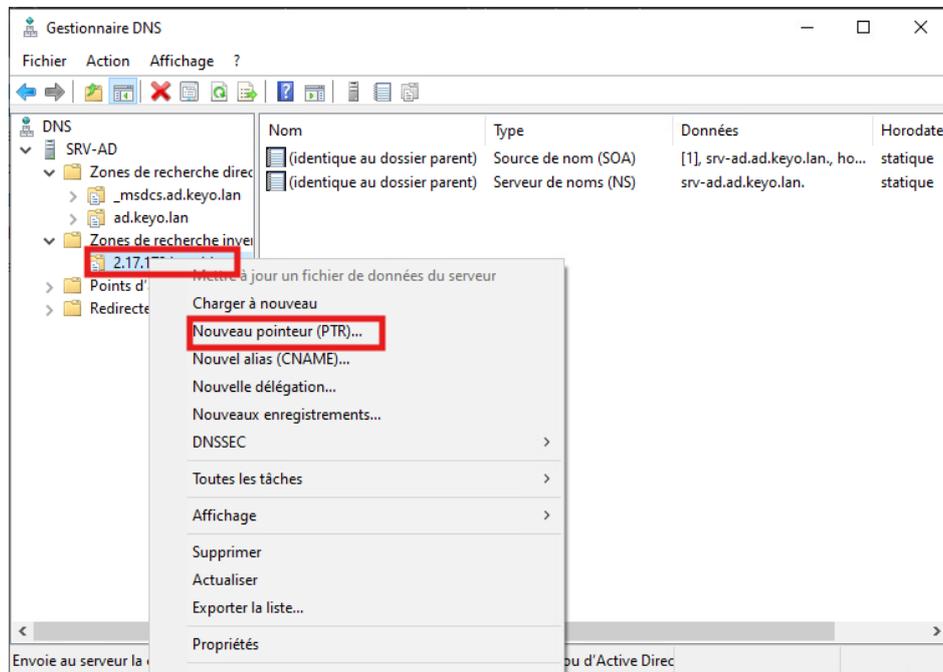


Comme on peut le voir notre zone est créer, mais elle est vide et ne contient aucun pointeur PTR.

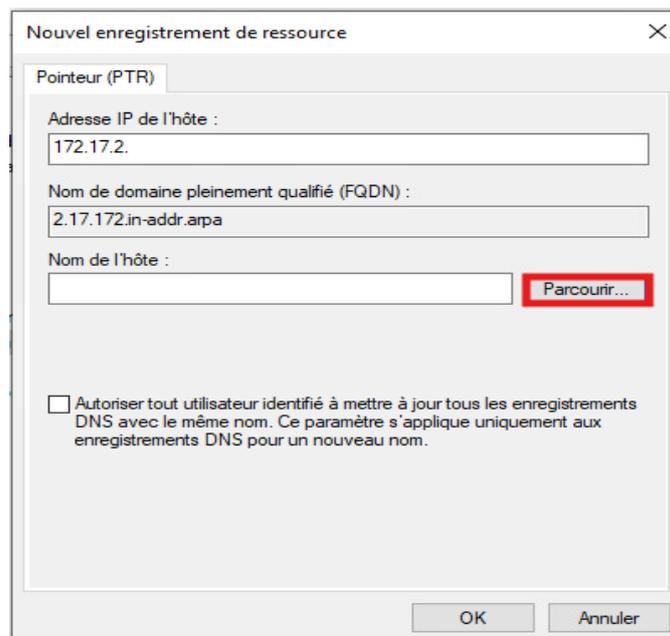


Nous allons ajouter un nouveau pointeur PTR :

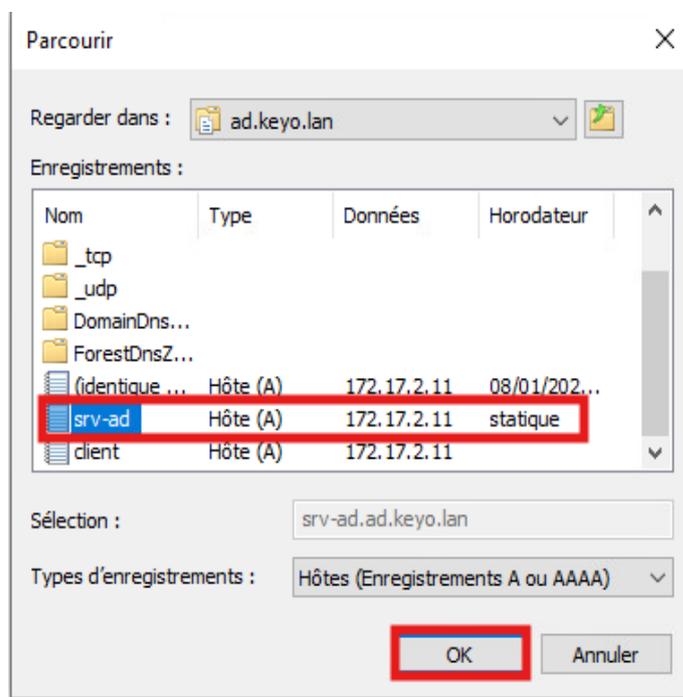
- Faites un clic droit dans la zone, puis cliquer sur « **Nouveau pointeur (PTR)...** »



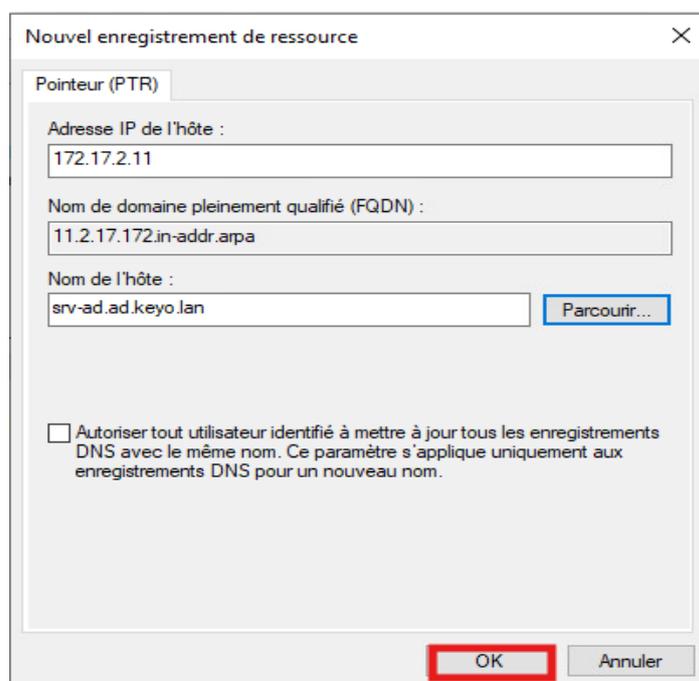
- Pour remplir automatiquement les informations, cliquer sur "**Parcourir**".



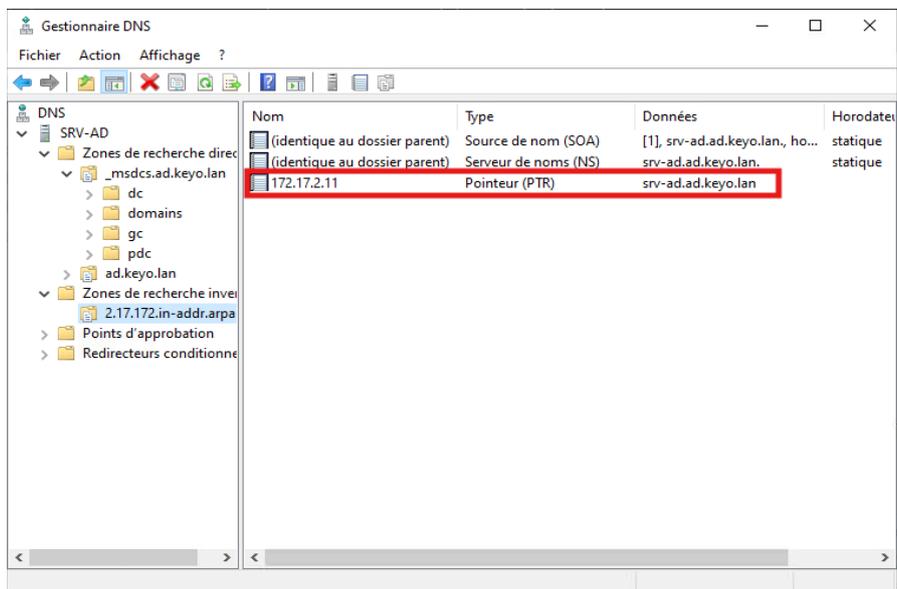
- Ensuite sélectionnons notre hôte.



- Comme on peut le voir les informations ont été saisies automatiquement. Pour valider cliquer sur "OK".



- Notre pointeur est créer, nous pouvons faire cela pour tous les autres hôtes.

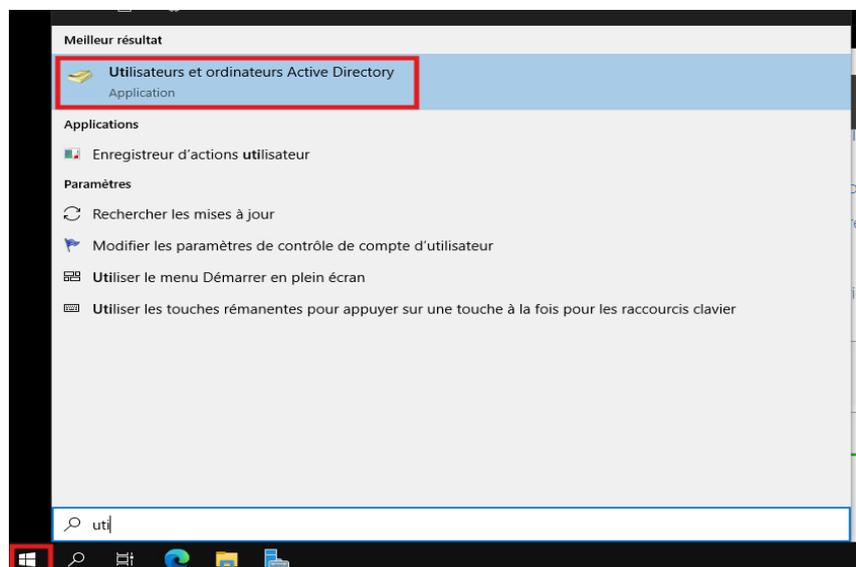


IX. Gestion des Utilisateurs et Ordinateurs dans Active Directory :

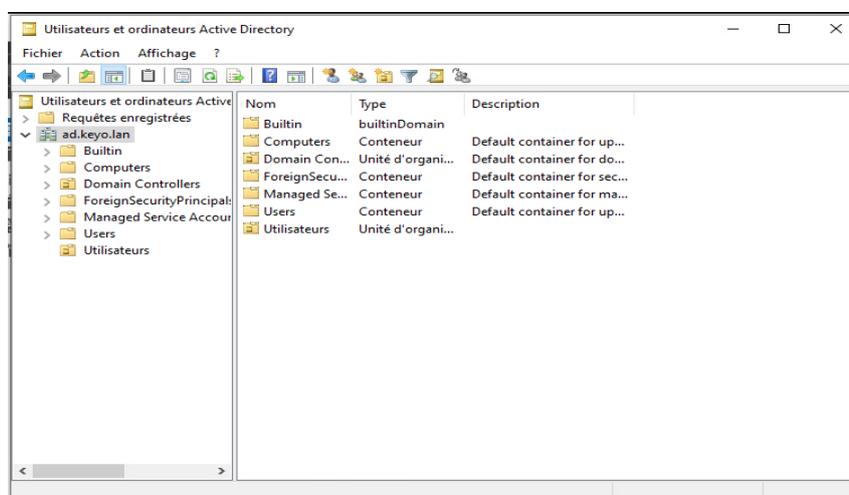
Pour gérer les utilisateurs et les ordinateurs du domaine, il suffit de lancer l'outil dédié à cette administration dans Active Directory. Ils est possible de l'accéder via au menu démarrer ou dans le tableau de bord de « **Gestionnaire de serveur** », puis dans « **Outils** »

Pour ce faire :

- Cliquer sur le menu démarrer,
- Ensuite taper « **Utilisateurs et ordinateurs Active Directory** » et cliquer dessus pour l'ouvrir.



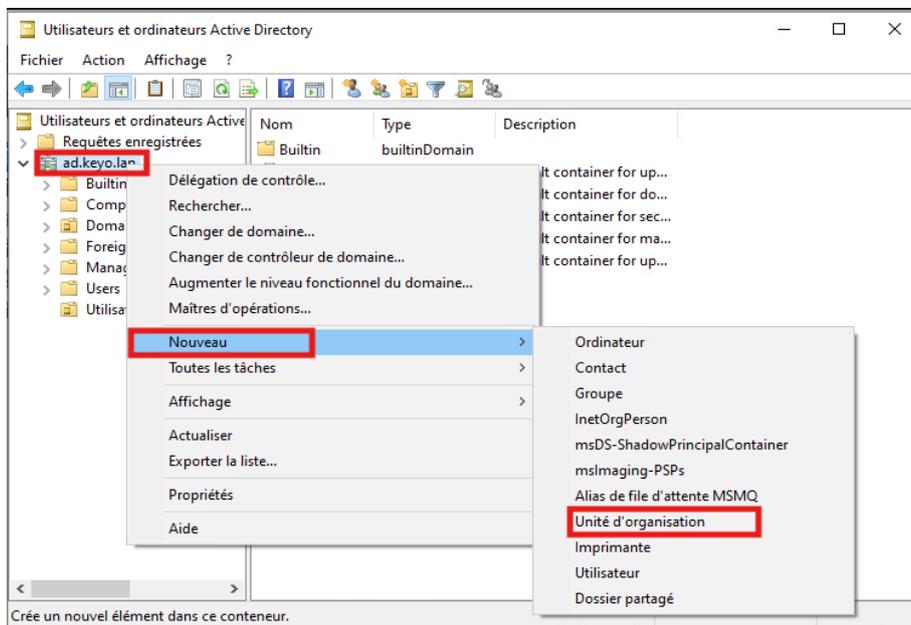
Voici le gestionnaire qui nous permet une gestion de notre domaine :



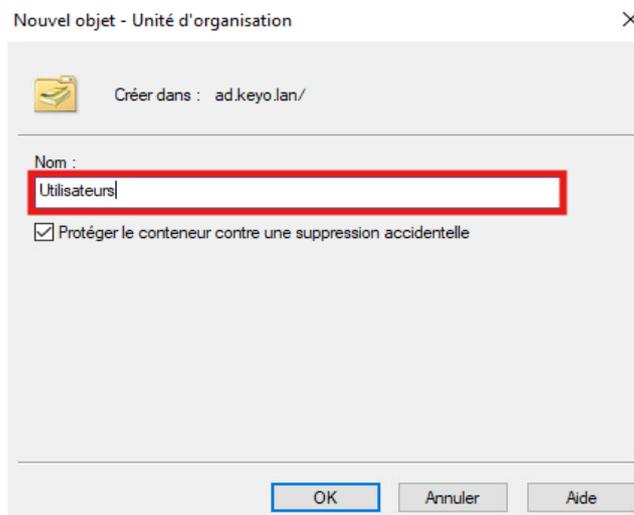
1. Créer une Unité d'Organisation (UO) :

Nous allons créer une Unité d'Organisation (UO), qui permet de structurer notre domaine en organisant les utilisateurs, les ordinateurs, les partages, etc., dans une hiérarchie claire. Cette étape consiste donc à créer notre UO pour faciliter la gestion et le classement des ressources du domaine.

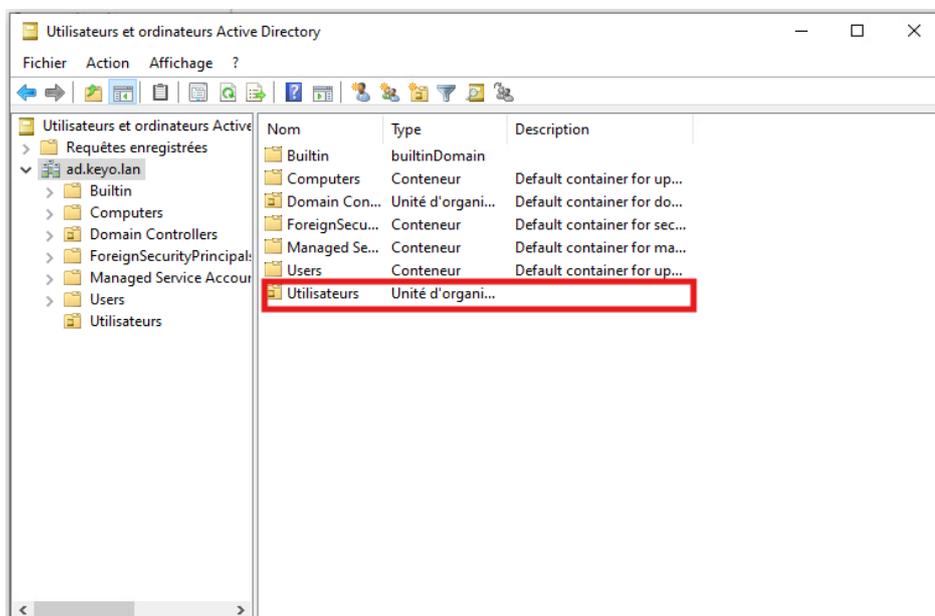
- Faites un clique droit à la racine de notre domaine, puis "**Nouveau**" et ensuite aller dans "**Unité d'organisation**".



- Ensuite la fenêtre de création de nouvelle objet "**Unité d'organisation**" s'affiche à l'écran, taper le nom de l'OU que vous souhaitez créer et faites « **OK** ».



Ici on peut le voir notre UO a été créer.

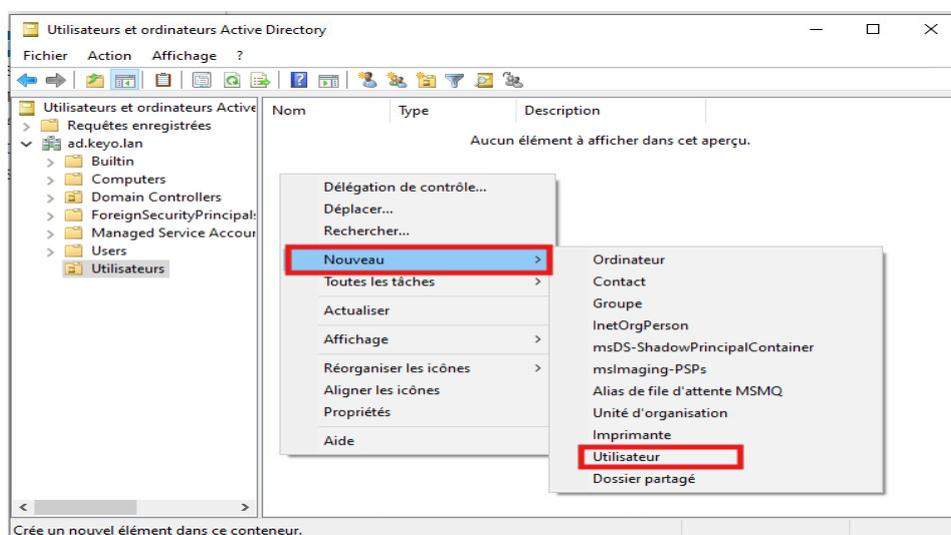


1. Créer un Utilisateur :

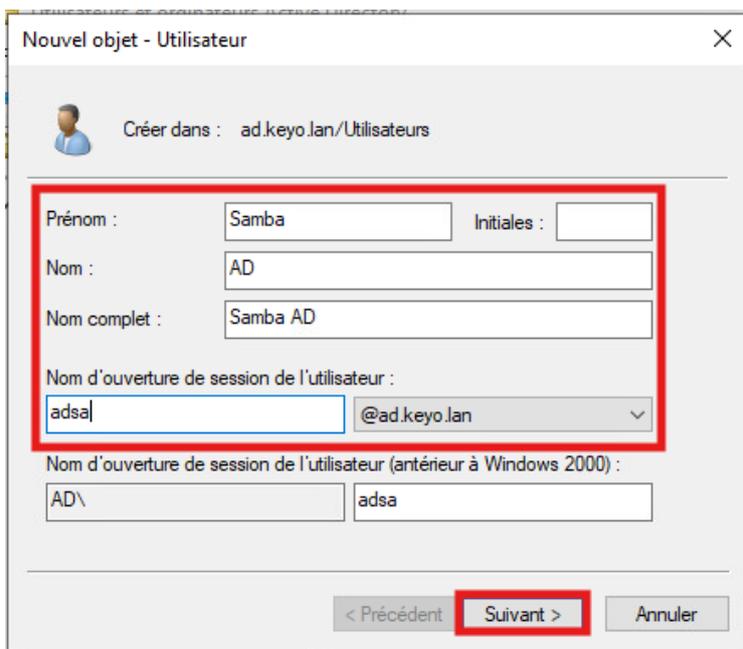
Nous allons créer un compte utilisateur, permettant à cet utilisateur de se connecter sur n'importe quel ordinateur du domaine avec une session personnalisée et identique sur chaque poste. Il n'est donc pas nécessaire de configurer manuellement le profil sur chaque ordinateur : le contrôleur de domaine gère la création et la mise à jour de la session automatiquement.

Pour ce faire :

- Faites un clic droit dans l'UO où vous souhaitez créer l'utilisateur, puis **"Nouveau"** et ensuite cliquer sur **"Utilisateur"**.



- Nous devons saisir "**prénom**", "**Nom**", et le "**nom d'ouverture de session**". Puis cliquer sur "**Suivant**".



Nouvel objet - Utilisateur

Créer dans : ad.keyo.lan/Utilisateurs

Prénom : Samba Initiales :

Nom : AD

Nom complet : Samba AD

Nom d'ouverture de session de l'utilisateur :

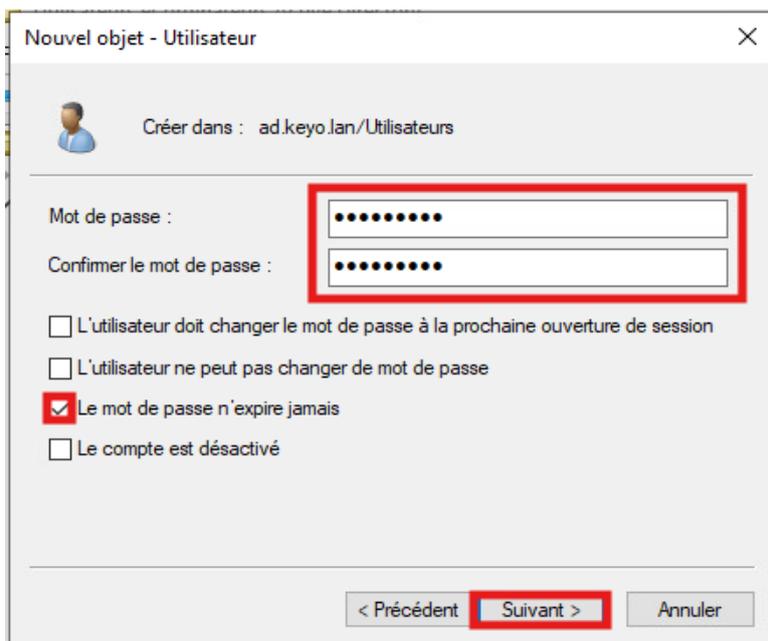
adsa @ad.keyo.lan

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

AD\ adsa

< Précédent **Suivant >** Annuler

- Ensuite on saisit le mot de passe de notre utilisateur et choisissez votre option ici, "**Le mot de passe n'expire jamais**". Puis cliquer sur "**Suivant**".



Nouvel objet - Utilisateur

Créer dans : ad.keyo.lan/Utilisateurs

Mot de passe :

Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

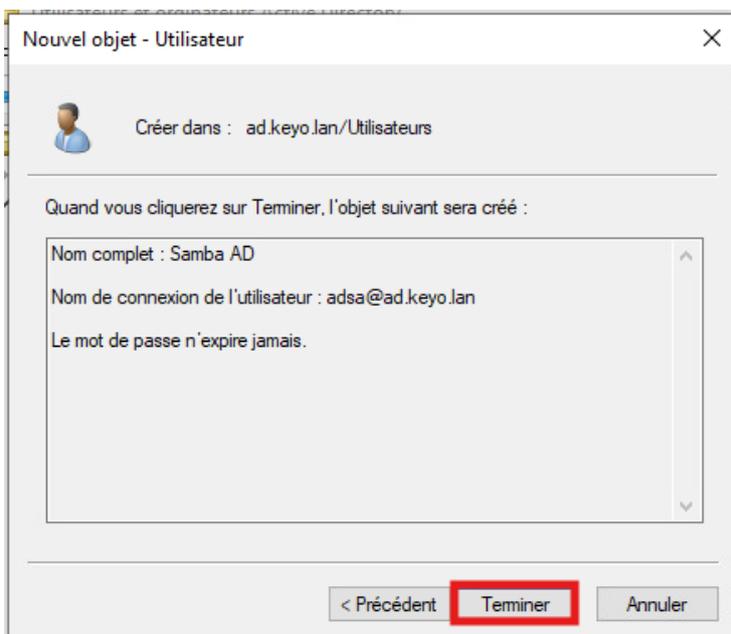
L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

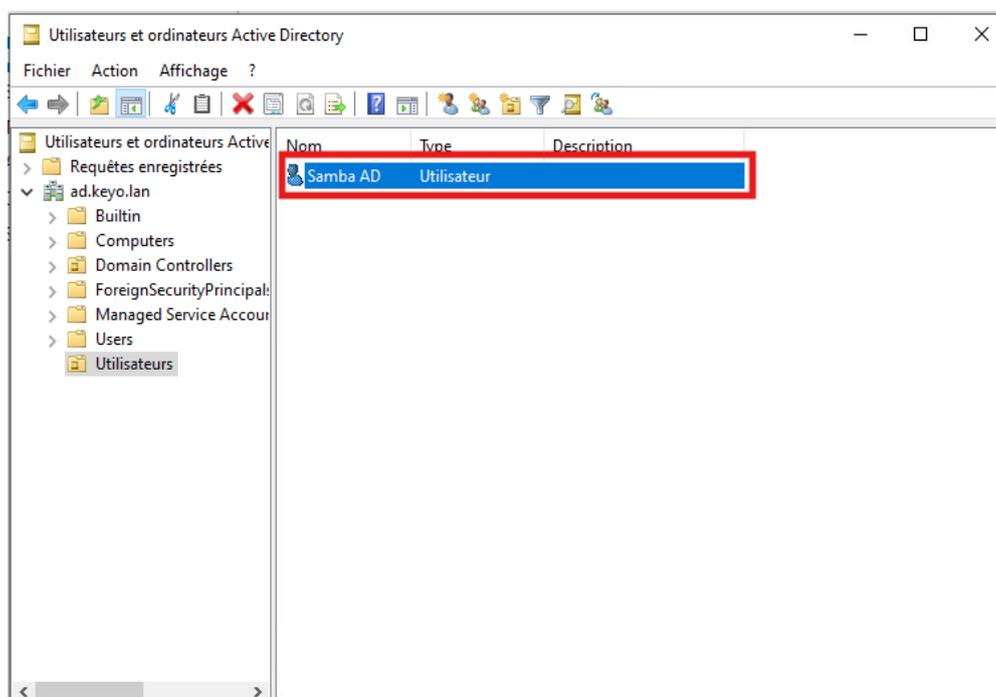
Le compte est désactivé

< Précédent **Suivant >** Annuler

- Nous avons un récapitulatif de notre utilisateur. Nous pouvons quitter en cliquant sur "**Terminer**".



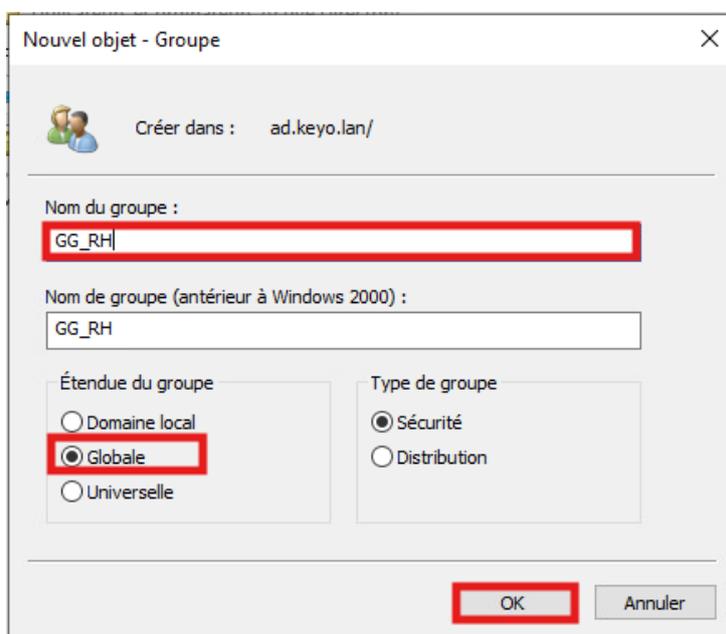
Notre utilisateur est bien créer dans l'UO.



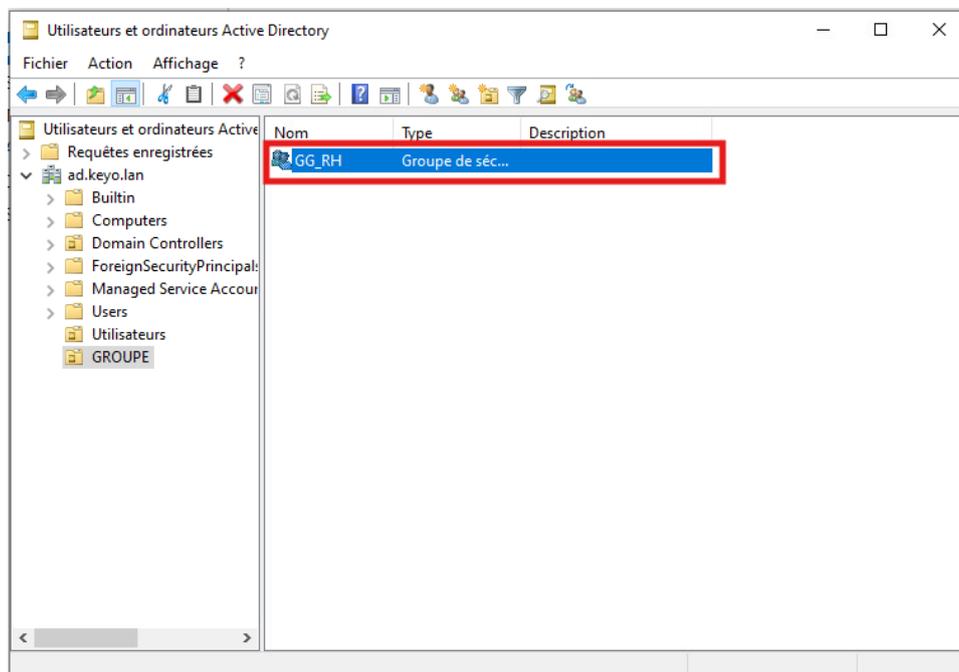
3. Créer un groupe :

Nous allons créer un groupe, qui est un ensemble d'utilisateurs pouvant être utilisé pour appliquer des stratégies de groupe (GPO) ou pour gérer des autorisations, comme les droits d'écriture DFS. Passons donc à la création de ce groupe.

- Faites un clic droit dans l'UO souhaité, puis "**Nouveau**" et ensuite cliquer sur "**Groupe**",
- Nous saisissons "**Nom du groupe**", choisissez l'étendue de groupe pour ensuite cliquer sur "**OK**".

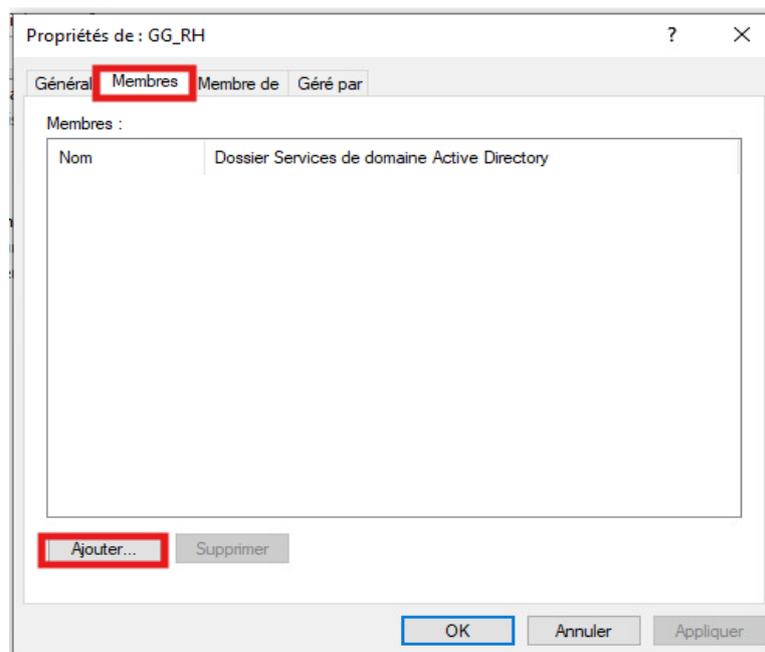


On peut voir que notre groupe a bien été créé.

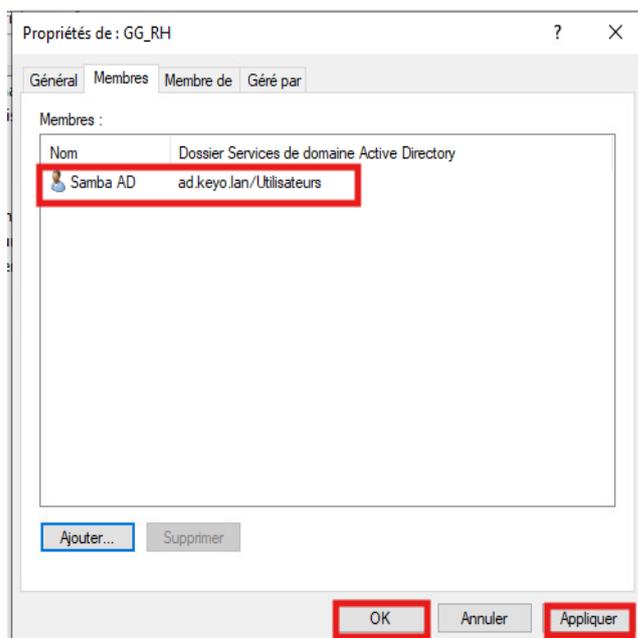


Il est possible d'ajouter des membres à ce groupe, dans l'onglet "**Membres**" de l'élément.

- Allez dans propriété de l'élément en faisant un clique droit dessus,
- Ensuite dans "**Membres**", faites "**Ajouter**";



- Taper le nom de l'utilisateur que vous souhaitez ajouter, puis " **Entrer** ",
- L'utilisateur apparaîtra dans champ membre, faites " **Appliquer** ", puis " **OK** ".



X. Configuration des GPO :

Que ce qu'un GPO ?

Les GPO (Group Policy Objects ou Stratégies de Groupe) sont des règles permettant d'appliquer des configurations spécifiques à des utilisateurs, des groupes ou des Unités d'Organisation (OU) au sein d'un annuaire Active Directory. Elles nécessitent donc la présence d'un domaine configuré sur le serveur.

Exemples d'utilisation des GPO :

- Masquer des icônes sur le bureau,
- Restreindre certaines actions (ex. : interdiction de modifier le fond d'écran, d'installer des logiciels ou d'ajouter des imprimantes),
- Définir une politique de mot de passe (ex. : longueur minimale, complexité, etc.),
- Modifier des permissions et droits d'accès,
- Déployer des logiciels automatiquement,
- Mapper des lecteurs réseau (ce que nous allons détailler ici).

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

GPO 1 : Connecter un lecteur réseau en GPO :

1-) Créer la GPO :

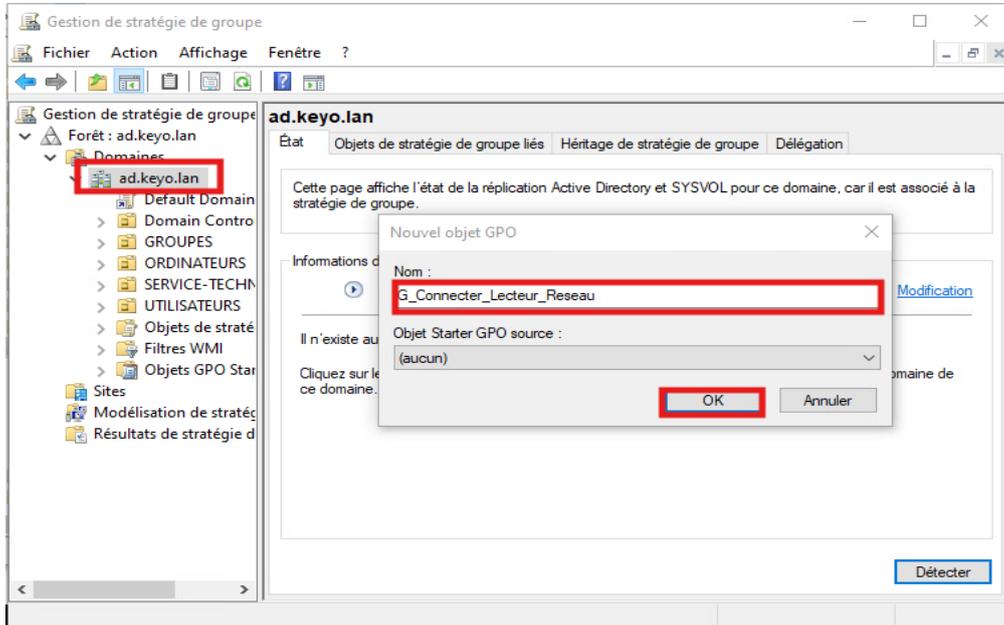
La GPO "Éléments de préférence - **Mappage de lecteur**" permet de gérer automatiquement les lecteurs réseau en offrant les actions suivantes : création, remplacement, mise à jour et suppression des mappages ainsi que de leurs propriétés associées.

Grâce à cette stratégie, un dossier partagé sera monté automatiquement en tant que lecteur réseau sur les postes de travail d'utilisateurs concerné.

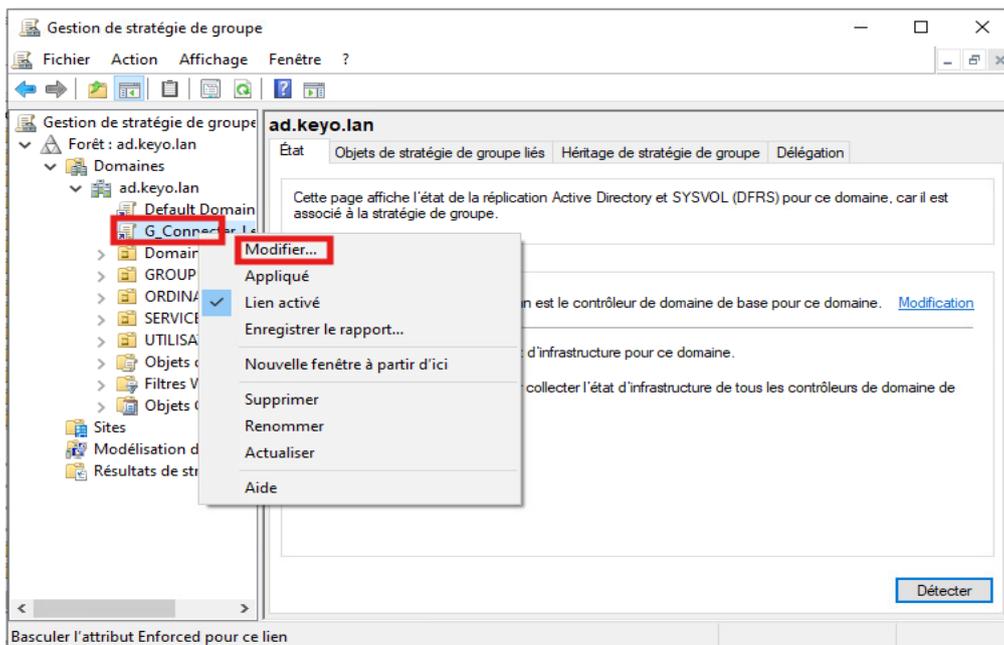
À l'aide de la console GPMC (Group Policy Management Console ou Console de Gestion des Stratégies de Groupe), créez une nouvelle GPO avec un nom explicite, par exemple ici "**G_Connecter_Lecteur_Reseau**". Cette stratégie sera exclusivement dédiée aux paramètres utilisateurs.

Pour ce faire :

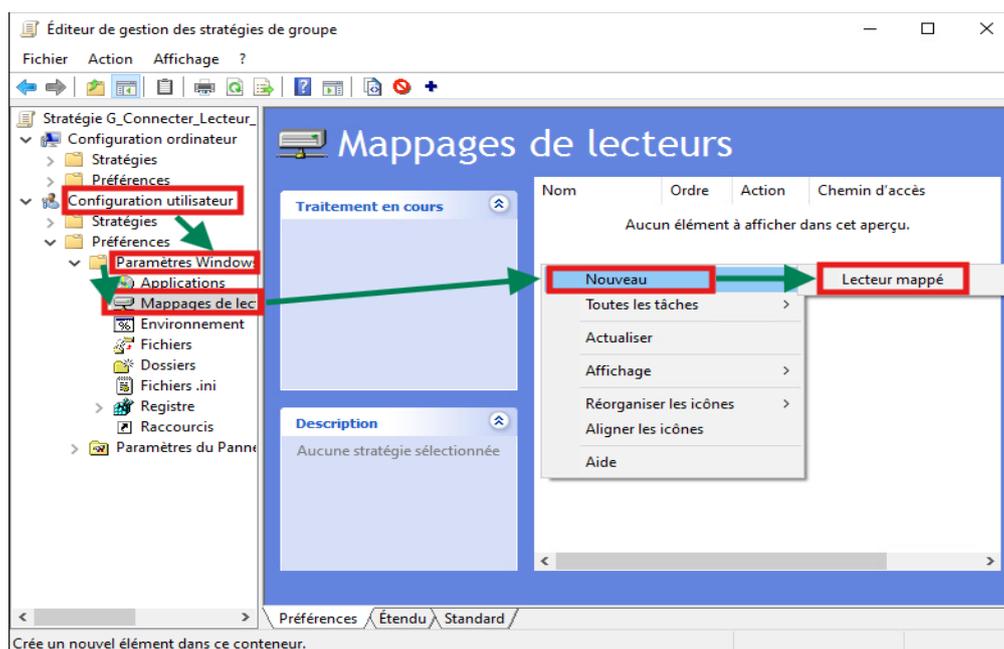
- Sur le serveur AD, ouvrez le Gestionnaire de serveur, puis allez dans : **Outils > Gestion des stratégies de groupe**.
- Une nouvelle fenêtre s'ouvre. Dans le volet de gauche, développez les sections.
- Ensuite un clic droit sur votre domaine (ici ad.keyo.lan) et sélectionnez l'option "**Créer un objet GPO dans ce domaine et le lier ici...**".
- Donnez un nom à votre GPO ici "**G_Connecter_Lecteur_Reseau**" puis faites "**OK**".



- Une nouvelle GPO devrait alors apparaître sous "Default Domain Policy" avec le nom que vous lui avez attribué.
- Une fois la GPO créée, faites un clic droit dessus et sélectionnez "**Modifier**".



- Allez dans **Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs**.
- La section droite de la fenêtre affiche alors "**Mappages de lecteurs**". Faites un clic droit dans cette zone, sélectionnez "**Nouveau**", puis choisissez "**Lecteur mappé**".



Maintenant, la partie la plus complexe reste à faire : renseigner les informations nécessaires pour connecter le lecteur réseau. Voici les différents champs disponibles :

- ◆ **Action** : choisir parmi les options suivantes : créer, mettre à jour, remplacer, supprimer (voir les détails ci-dessous).
- ◆ **Emplacement** : indiquer le chemin UNC vers le partage réseau que vous souhaitez connecter au poste client.
- ◆ **Reconnecter** : cochez cette option si vous souhaitez rendre le lecteur réseau persistant, ce qui signifie qu'il se reconnectera automatiquement à chaque ouverture de session.
- ◆ **Libeller en tant que** : attribuer un nom personnalisé au lecteur réseau.
- ◆ **Lettre de lecteur** : spécifier la lettre à assigner au lecteur. Veillez à éviter tout conflit avec les lecteurs locaux.

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

- ◆ L'option "**Se connecter en tant que**" est désactivée par Microsoft pour des raisons de sécurité, car elle exposait les identifiants dans les fichiers GPO accessibles via le dossier SYSVOL, ce qui représentait un risque.

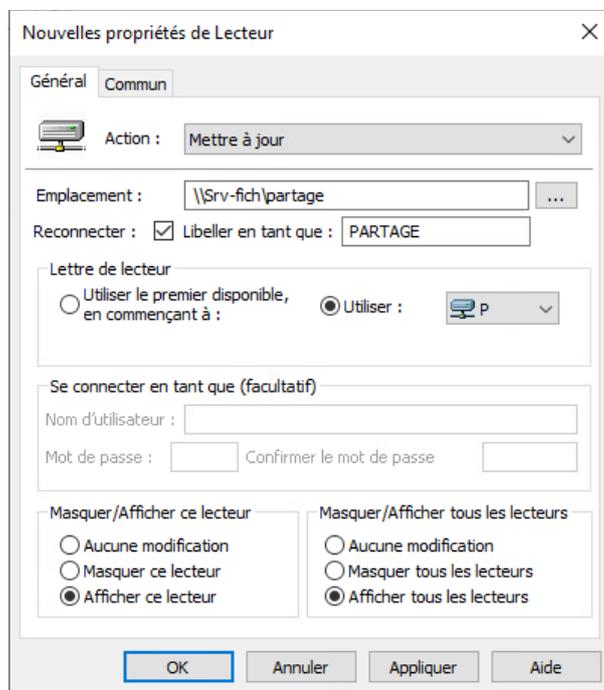
Détaillons maintenant l'option "**Action**", qui est très importante et mérite une explication détaillée. Les différentes actions sont les suivantes :

- ◆ **Créer** : permet de connecter un nouveau lecteur réseau pour l'utilisateur. Attention, la lettre choisie ne doit pas être déjà utilisée, sinon la connexion échouera.
- ◆ **Supprimer** : déconnecte un lecteur réseau existant. Si le lecteur n'existe pas, aucune action n'est effectuée.
- ◆ **Remplacer** : supprime le lecteur réseau ciblé, puis le recrée pour l'utilisateur.
- ◆ **Mettre à jour** : connecte le lecteur réseau s'il ne l'est pas déjà, ou met à jour sa configuration si le lecteur est déjà connecté. Contrairement à l'action "Remplacer", cette option ne supprime pas le lecteur avant de le recréer, ce qui la rend plus flexible.

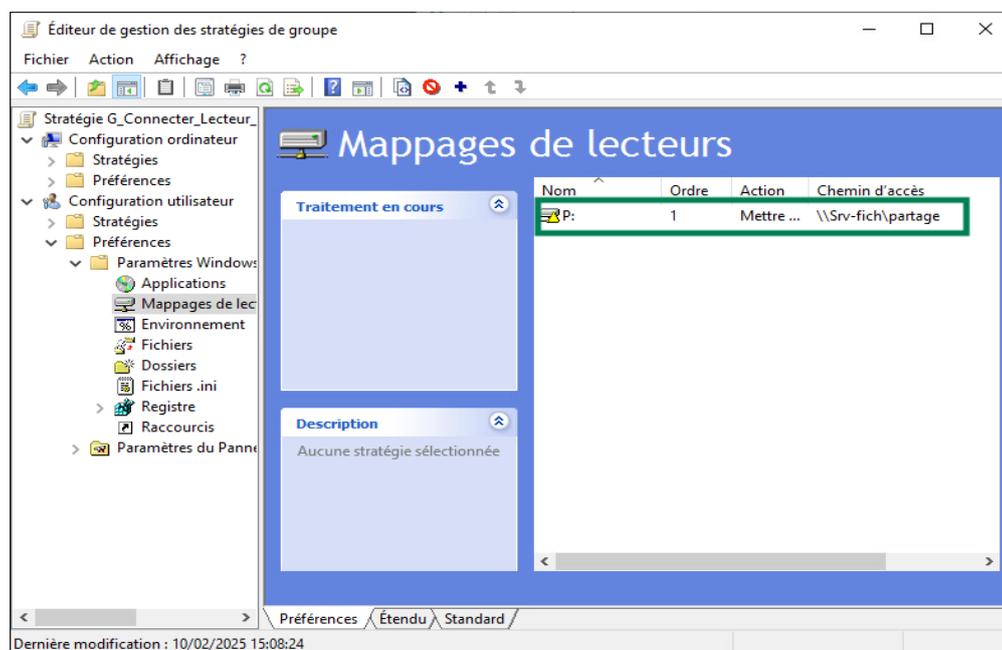
Info : Lors d'une migration, il peut être judicieux d'utiliser l'action "Remplacer" pour s'assurer que le lecteur réseau sera supprimé puis recréé vers le nouveau partage. Une fois la migration terminée et la situation stabilisée, il est préférable d'opter pour l'option "Mettre à jour".

Parmi les options disponibles, sélectionnez :

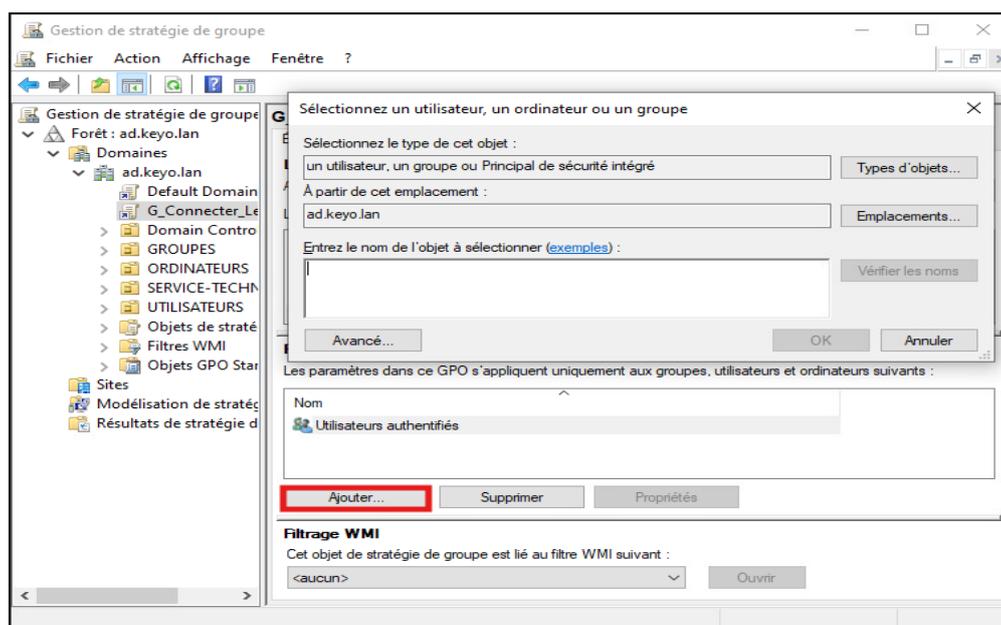
- l'Action : "**Mettre à jour**".
- Dans le champ "**Emplacement**", entrez le chemin réseau de votre partage.
- Cochez la case "**Reconnecter**" et attribuez un nom au libellé du lecteur.
- Choisissez ensuite la lettre du lecteur à assigner ici "**P**".
- Enfin, cochez les options "**Afficher ce lecteur**" et "**Afficher tous les lecteurs**".
- Cliquez sur "**Appliquer**", puis sur "**OK**" pour valide, (voir image ci dessous).



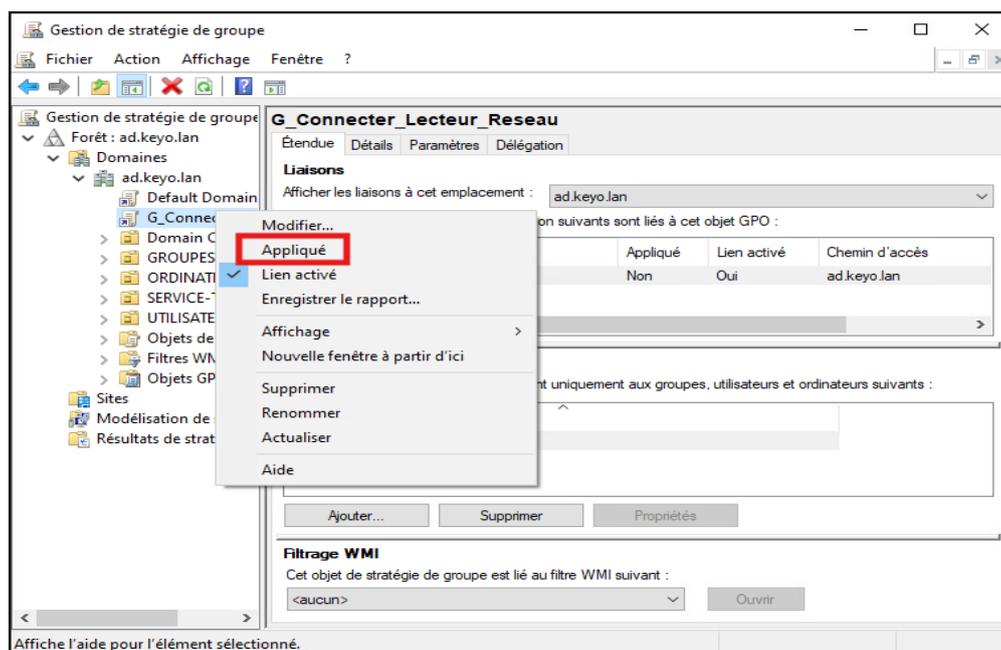
- Une nouvelle ligne apparaîtra alors dans la section "**Mappages de lecteurs**", vous pouvez maintenant fermer cette fenêtre et revenir à la liste de vos GPO.



- Dans la partie droite, en bas, vous pouvez définir les utilisateurs, groupes ou unités organisationnelles (OU) concernés par cette GPO.
- Cliquez sur "**Ajouter**", saisissez les noms souhaités, puis validez en cliquant sur "**OK**".

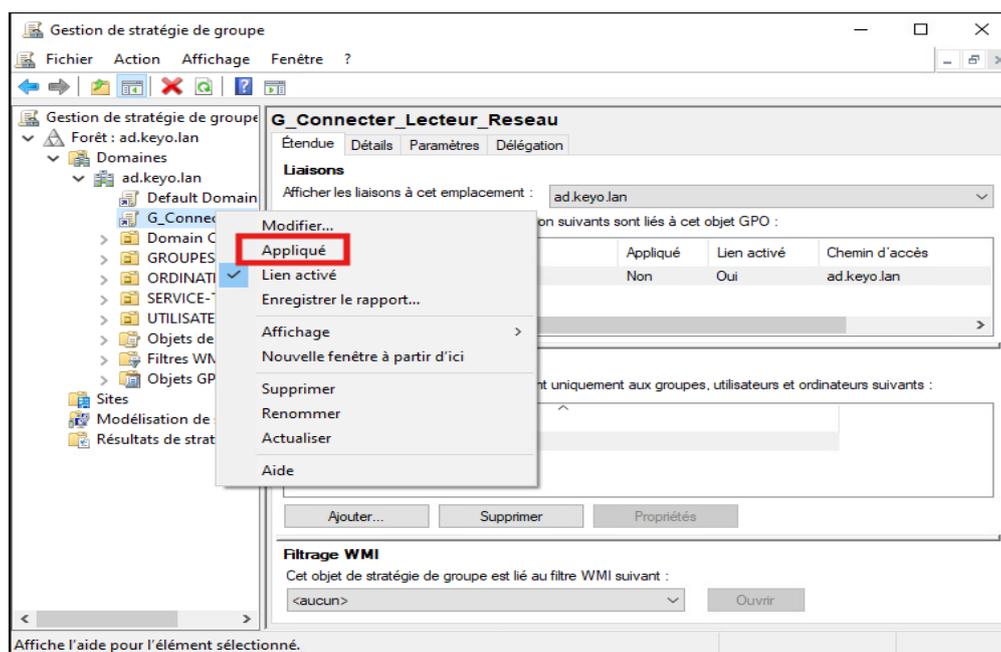


- Faites un clic droit sur votre GPO, puis cochez "Appliqué". Cette étape est essentielle pour activer la GPO, sans quoi elle ne sera pas exécutée.



2-) Tester la GPO :

Une fois la GPO configurée, il est temps de la tester ! Pour cela, connectez-vous à un poste du domaine en utilisant un compte concerné par la GPO et disposant des autorisations nécessaires pour accéder au partage via un lecteur réseau.



GPO 2 : Déployer les applications (Chrome et Libre office) :

Étape 1 : Préparer les fichiers d'installation

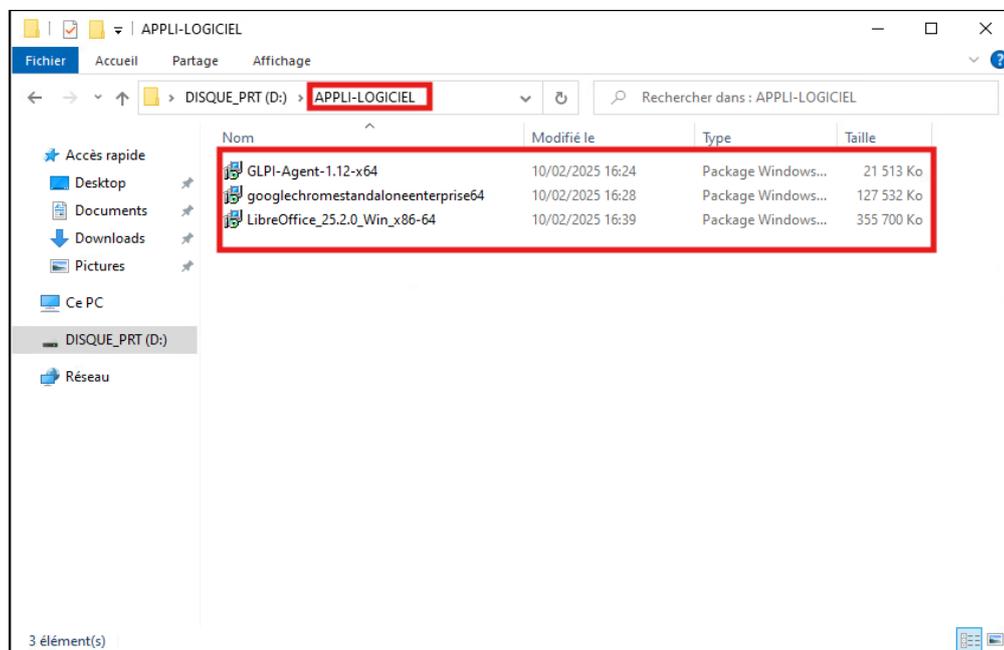
Avant de créer la GPO, vous devez disposer des fichiers d'installation :

- ◆ Google Chrome MSI : Téléchargez la version MSI depuis le site Google Entreprise.
- ◆ Téléchargez la dernière version de LibreOffice MSI depuis le site officiel.

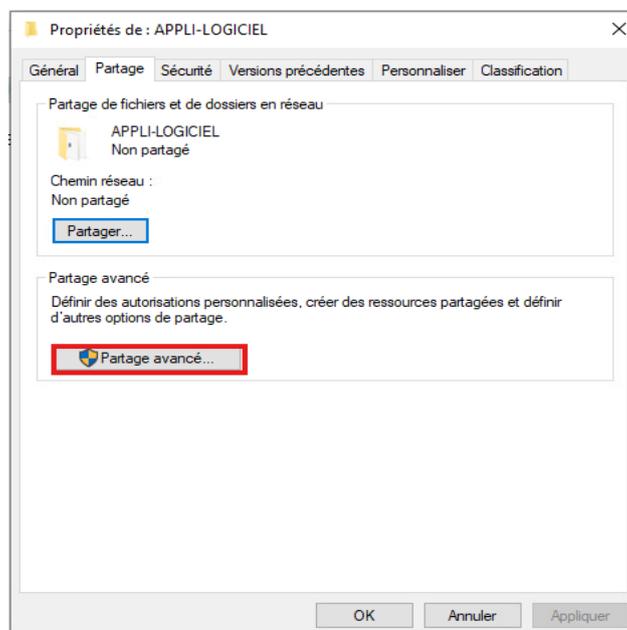
Stockez ces fichiers sur un partage réseau accessible par tous les postes (exemple : <\\srv-fich\DEPLOIEM-APPLI-LOGICIEL>).

Étape 2 : Partager le dossier (DEPLOIEM-APPLI-LOGICIEL)

- Sur la machine Windows Server il faut créer un dossier partagé qui contient le fichier **.msi** des applications précédemment télécharger.

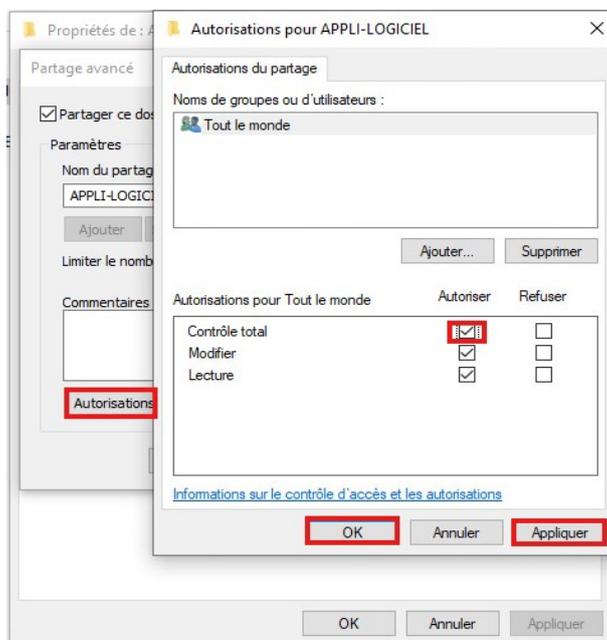


- Faites un clic droit sur le dossier, puis accédez aux "Propriétés".
- Dans l'onglet "Partage", cliquez sur "Partage avancé".

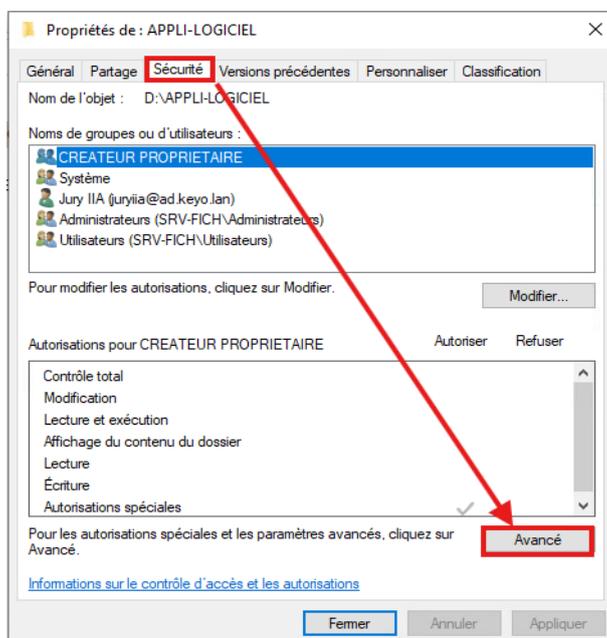


- Cliquez sur "**Autorisations**", puis accordez le contrôle total à "**Tout le monde**".

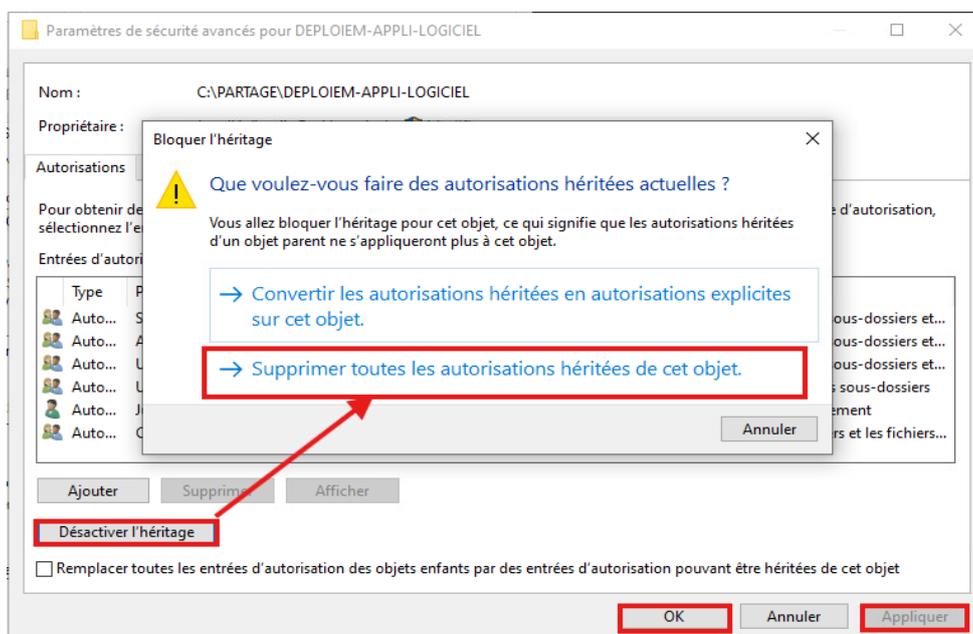
- Ensuite, cliquez sur "**Appliquer**", puis sur "**OK**".



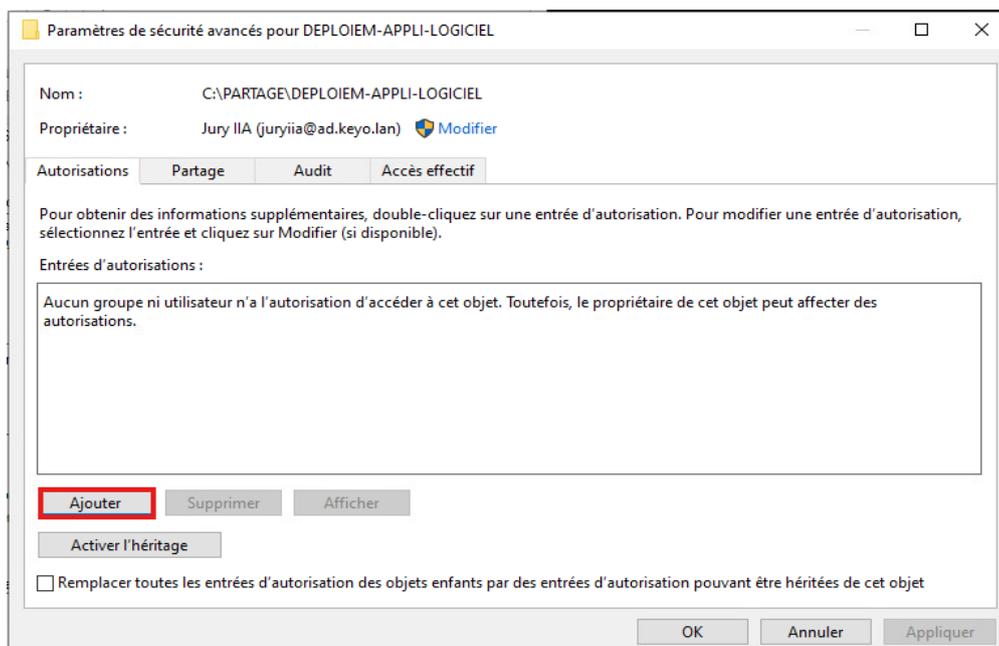
- Ensuite allez dans l'onglet "**Sécurité**" puis dans la partie "**Avancé**".



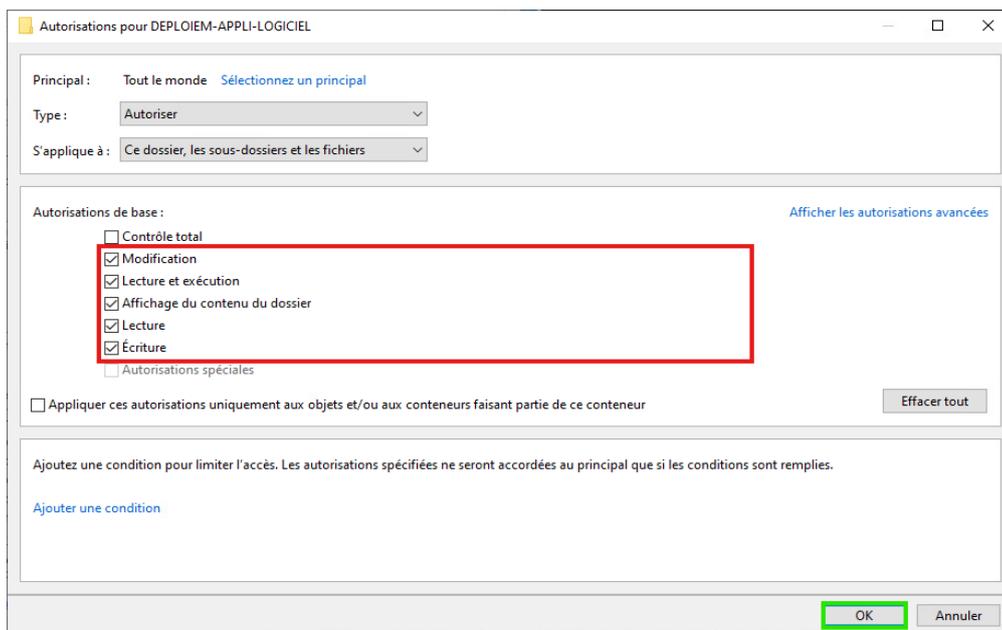
- Dans l'onglet "Sécurité", désactivez l'héritage, puis faites "**Supprimer toutes les autorisations héritées de cet objet**".



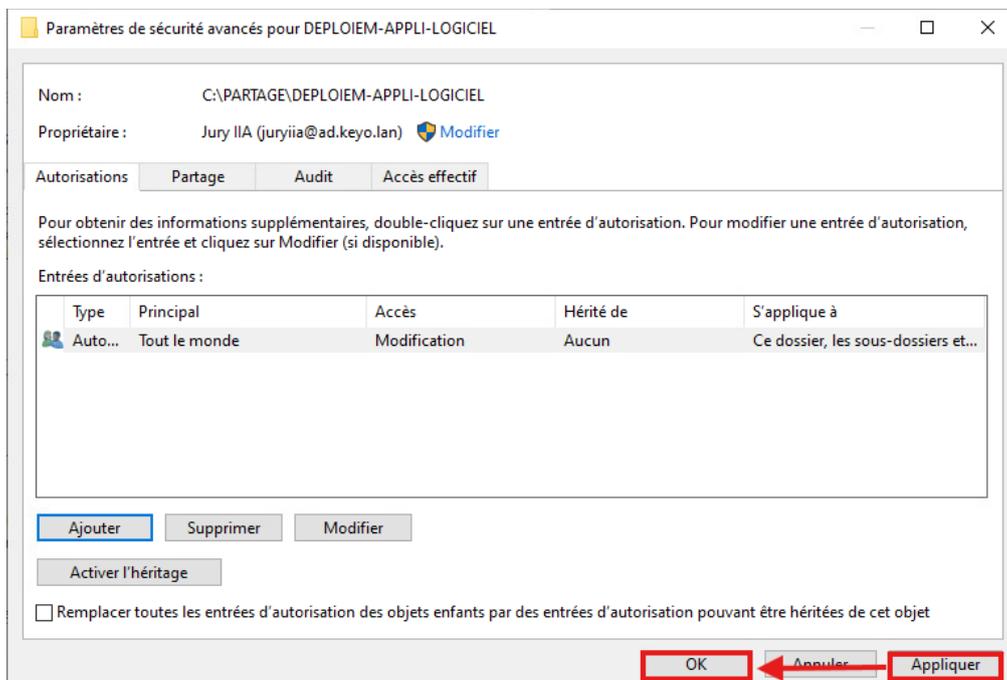
- Puis cliquer sur "**Ajouter**".



- Puis cliquer sur "**Sélectionner un principal**", ajouter le groupe "**Tout le monde**" puis coché la casse "**Modifier**" et faites "**OK**".

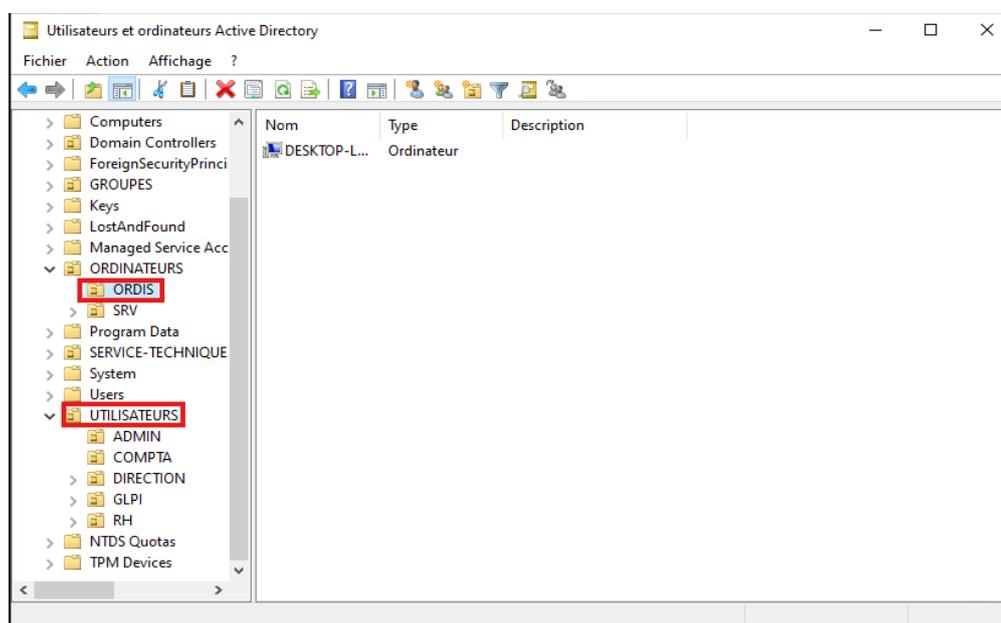


- "**Appliquer**" et puis "**OK**"



Étape 3 : Créer l'OU pour stocker les PC :

- Créez une nouvelle Unité d'Organisation (OU) sur le domaine et ajoutez-y les PC concernés par la GPO.
- Vous pouvez également y inclure les utilisateurs concernés ici j'appliquerais aux ordinateurs et les utilisateurs, ici je vais l'appli sur **OU ORDIS** .

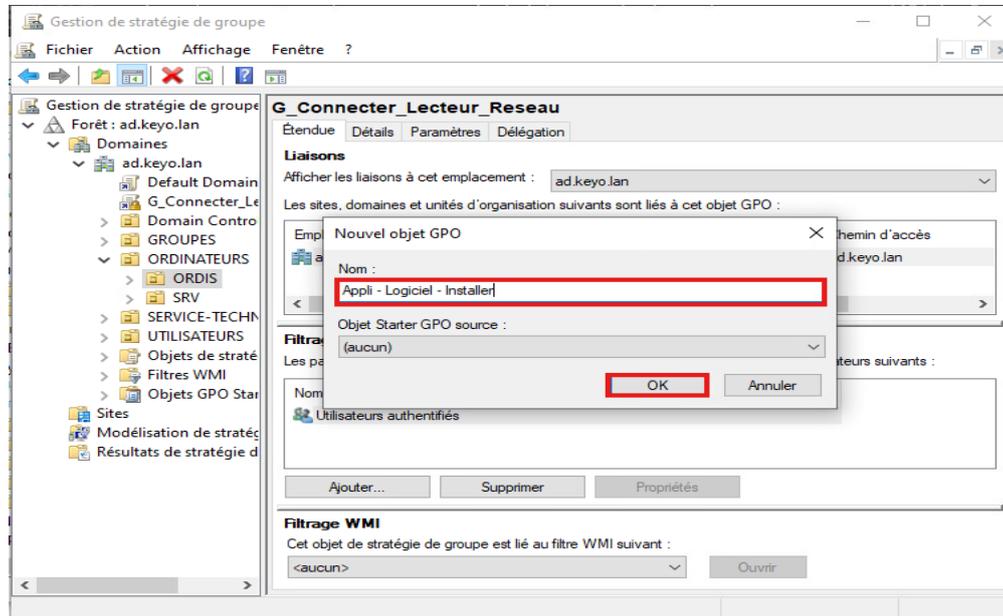


Étape 4 : Créer la stratégie de groupe pour déployer (Chrome et libre Office)

Ouvrez la console "Gestion de stratégie de groupe" et créez une nouvelle GPO.

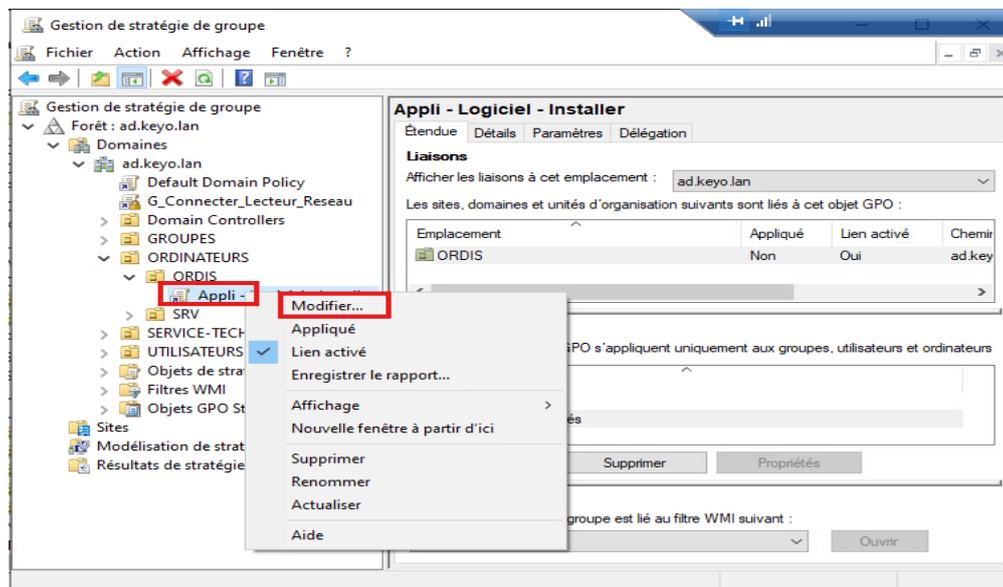
Dans cet exemple, la **GPO** est nommée "**Appli - Logiciel - Installer**" et est liée à l'Unité ORDIS (OU), qui contient les postes de travail Windows.

Attention : Si vous liez cette **GPO** à la racine de votre domaine Active Directory, les applications seront déployés sur toutes les machines, y compris les postes de travail et les serveurs.

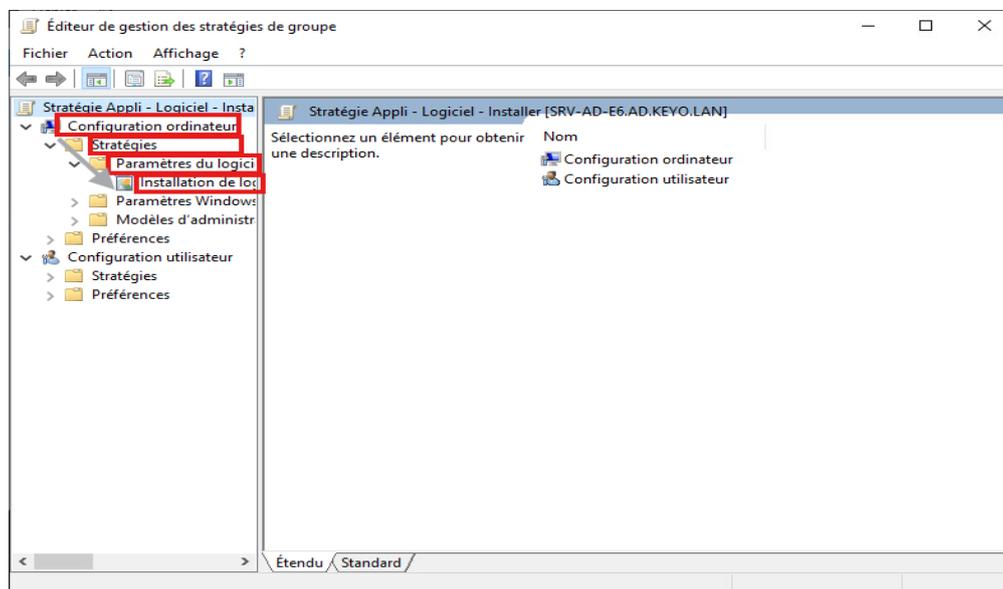


Étape 5 : Modifier La GPO

- Faites clic droit sur la GPO → "Modifier".



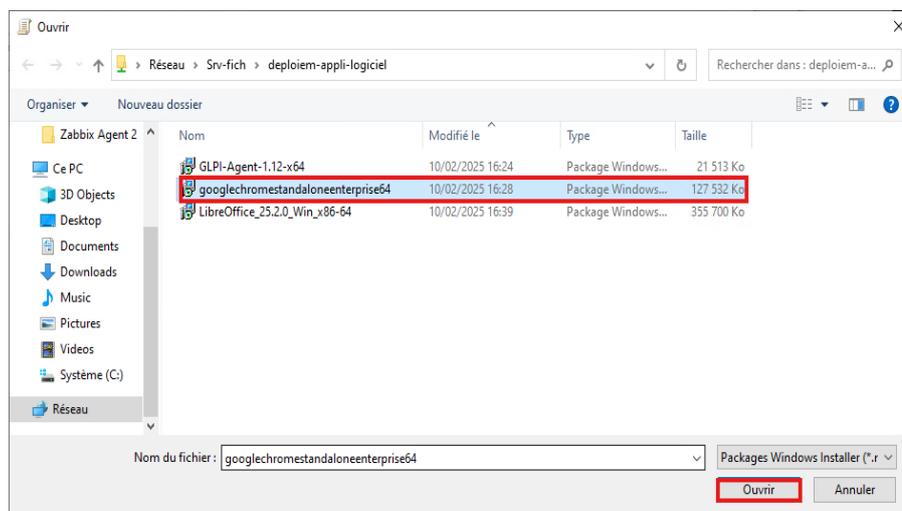
- Allez dans **Configuration ordinateur** → **Stratégies** → **Paramètres logiciels** → **Installation de logiciels**.



Ajouter les packages MSI :

Pour Chrome :

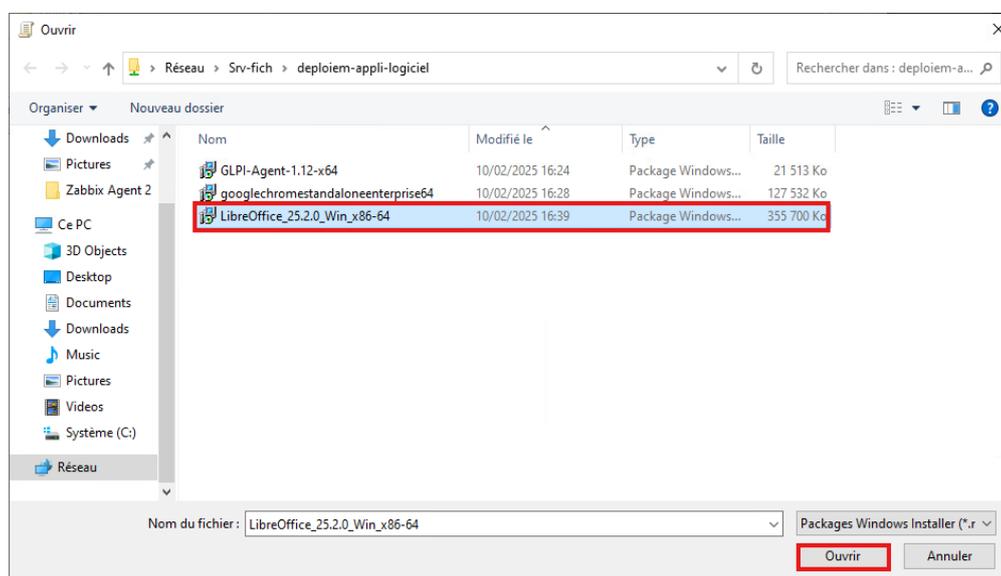
- Faites un clic droit sur "**Installation de logiciel**" → "**Nouveau**" → "**Package**".
- Ensuite une fenêtre va s'ouvrir afin de vous permettre de sélectionner le package MSI à déployer. Vous devez préciser le chemin réseau (chemin UNC) vers le package MSI.
- Sélectionnez le package Chrome depuis \\srv-fich\Déploiement-appli-logiciel\
- Faites "**Ouvrir**".



- A la question "Sélectionnez le type de déploiement", choisissez "**Attribué**" et puis "**OK**".

Pour Libre Office :

- Faites un clic droit sur "**Installation de logiciel**" → "**Nouveau**" → "**Package**".
- Ensuite une fenêtre va s'ouvrir afin de vous permettre de sélectionner le package MSI à déployer. Vous devez préciser le chemin réseau (chemin UNC) vers le package MSI.
- Sélectionnez le package Libre Office depuis \\srv-fich\Déploiement-appli-logiciel\
- Faites "**Ouvrir**".



- A la question "Sélectionnez le type de déploiement", choisissez "**Attribué**" et puis "**OK**" à voir impossible d'ajouter ce package.

GPO 3 : Déployer l'Agent GLPI sur les postes Utilisateur Windows :

Etape 1 :Préparer les fichier d'installation

Avant de créer la GPO, vous devez disposer des fichiers d'installation :

- ◆ Agent GLPI MSI: Téléchargez l'agent GLPI depuis le site officiel.

Stockez ces fichiers sur un partage réseau accessible par tous les postes (ici j'ai ajouter ce fichier .msi dans : \\srv-fich\DEPLOIEM-APPLI-LOGICIEL) déjà partagé.

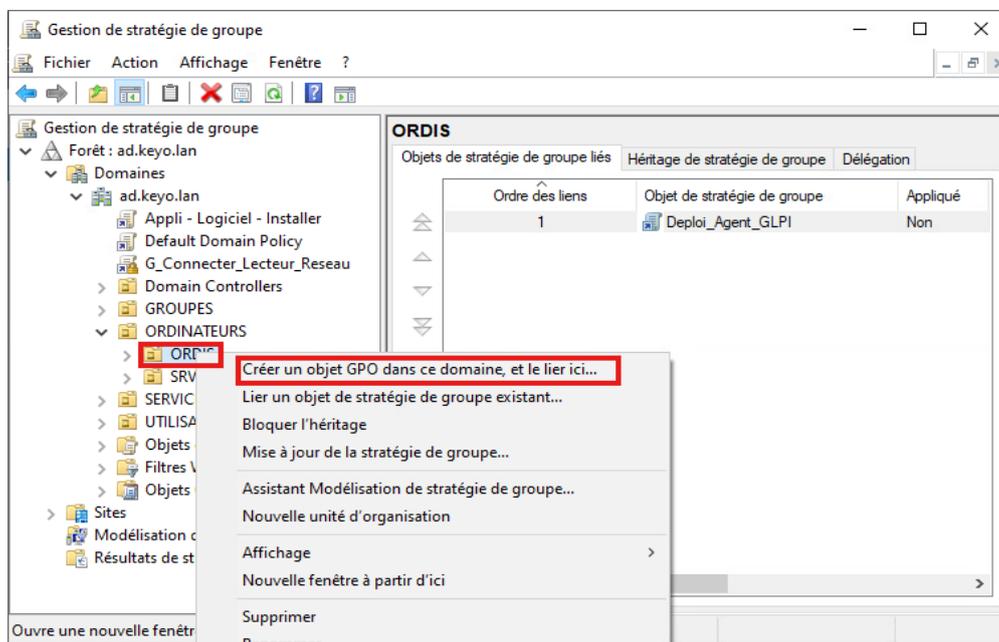
Étape 2 : Créer la stratégie de groupe pour déployer l'agent GLPI

Ouvrez la console "Gestion de stratégie de groupe" et créez une nouvelle GPO.

Dans cet exemple, la **GPO** est nommée "**Deploi_Agent_GLPI**" et est liée à l'Unité **ORDIS** (OU), qui contient les postes de travail Windows.

Pour ce faire :

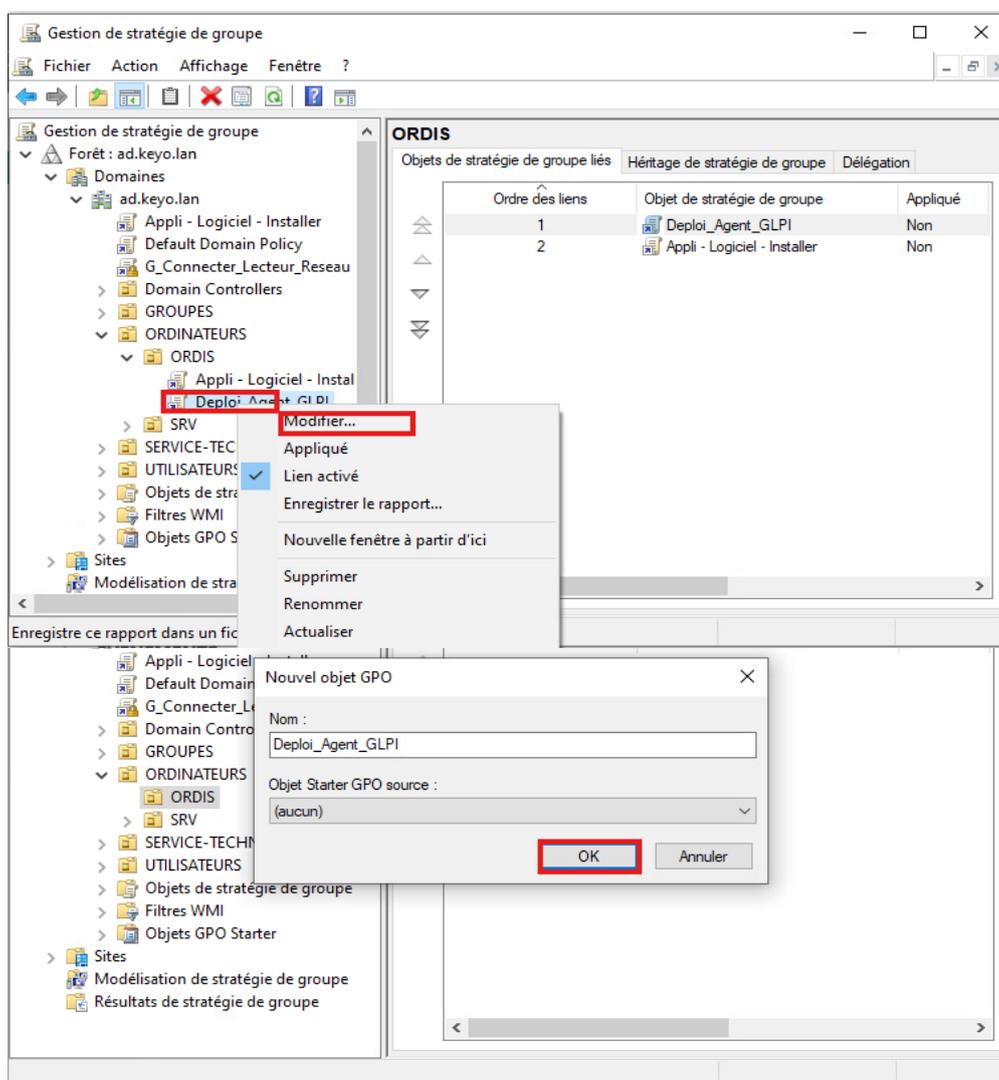
- Faites un clic droit sur OU **ORDIS**, et cliquez sur "**Créer un objet GPO dans ce domaine, et liez ici...**".



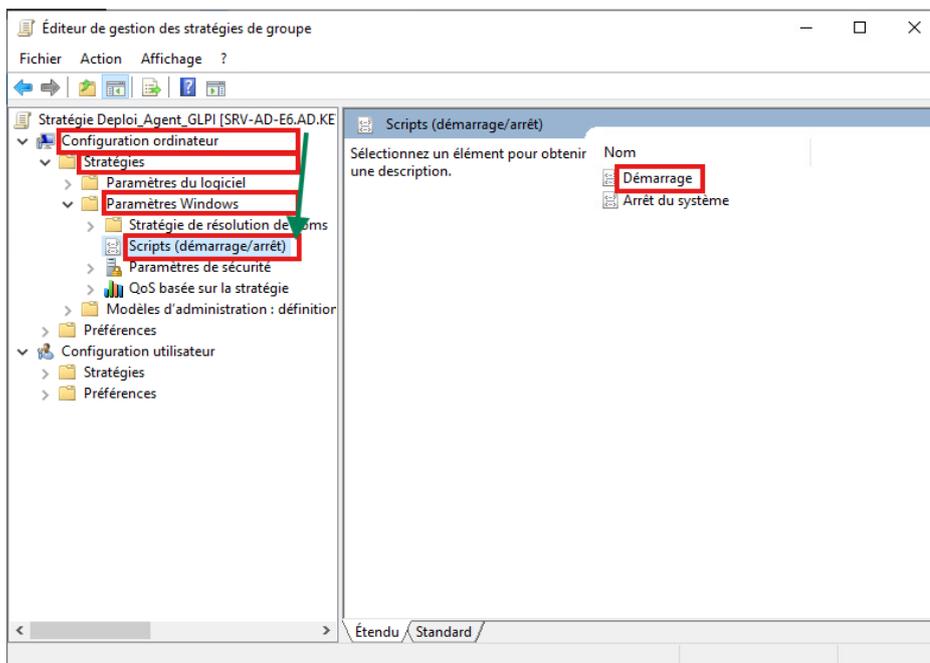
- le nom de la GPO, puis faites "**OK**".

Étape 3 : Modifier la GPO pour créer un script de démarrage

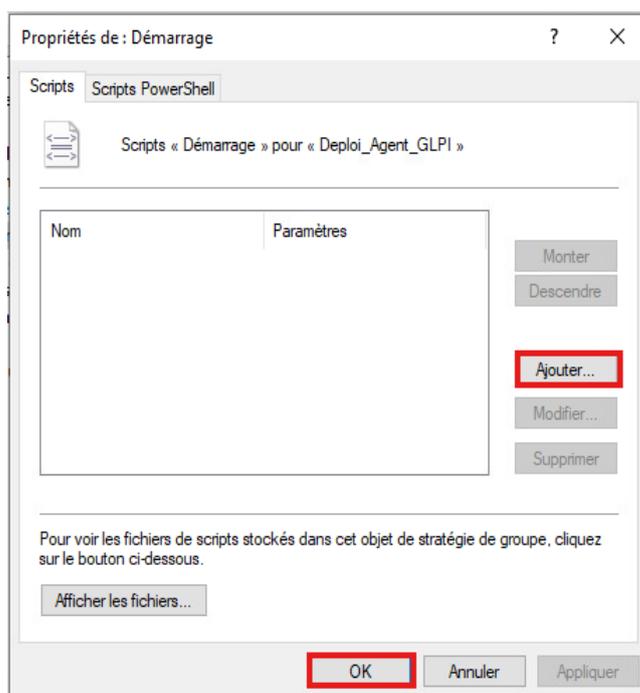
- Faites un clic droit sur la GPO, puis "Modifier"



- Allez dans **Configuration ordinateur** → **Stratégies** → **Paramètres Windows** → **Scripts (démarrage/ Arrêt)**.



- Ensuite double cliquer sur démarrage, faites **Ajouter**



	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	

Et c'est ici que nous allons créer le script de démarrage pour l'installation de l'agent GLPI :

Le script doit contenir le chemin du fichier Agent-GLPI ainsi que les options d'installation. Veillez à respecter scrupuleusement la syntaxe :

- ◆ Espaces entre les différentes options, mais pas avant ou après un signe "="
- ◆ Guillemets autour du chemin réseau et de l'URL du serveur GLPI
- ◆ Adapter l'URL en fonction de votre infrastructure (nom/IP du serveur, domaine, emplacement de GLPI...)

Commande du script :

```
/quiet /i "\\srv-fich\deploiem-appli-logiciel\GLPI-Agent-1.12-x64.msi" runnow=1
Add_Firewall_Exception=1 Server="http://172.17.2.14/glpi/front/inventory.php"
```

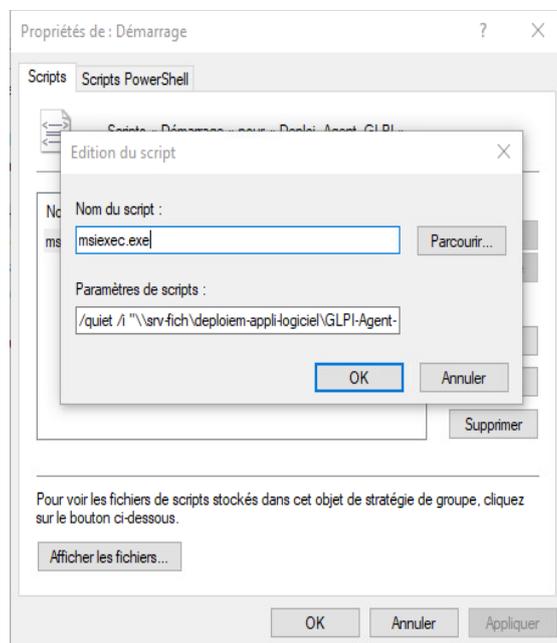
Explications des paramètres de script:

Paramètre	Explication
/quiet	Exécute l'installation en mode silencieux (aucune fenêtre affichée).
/i "\\srv-fich\deploiem-appli-logiciel\GLPI-Agent-1.12-x64.msi"	Spécifie le chemin réseau du fichier .msi à installer.
runnow=1	Exécute immédiatement un inventaire après l'installation.
Add_Firewall_Exception=1	Ajoute une exception au pare-feu Windows pour permettre la communication de l'agent.
Server="http://172.17.2.14/glpi/front/inventory.php"	Définit l'URL du serveur GLPI où l'agent enverra l'inventaire.

Dans la nouvelle page de formulaire de création du script :

1. **Nom du script** : msi.exec.exe
2. **Paramètre du script** : adapter le script à votre configuration et le mettre ici, voir (le script et le tableau d'explication pour ajuster vos paramètres).

	Architecture Système	Ref : DOC_procedure_AD Version 1.0.0 Date:02/01/2025 Page:1/33
	Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022	



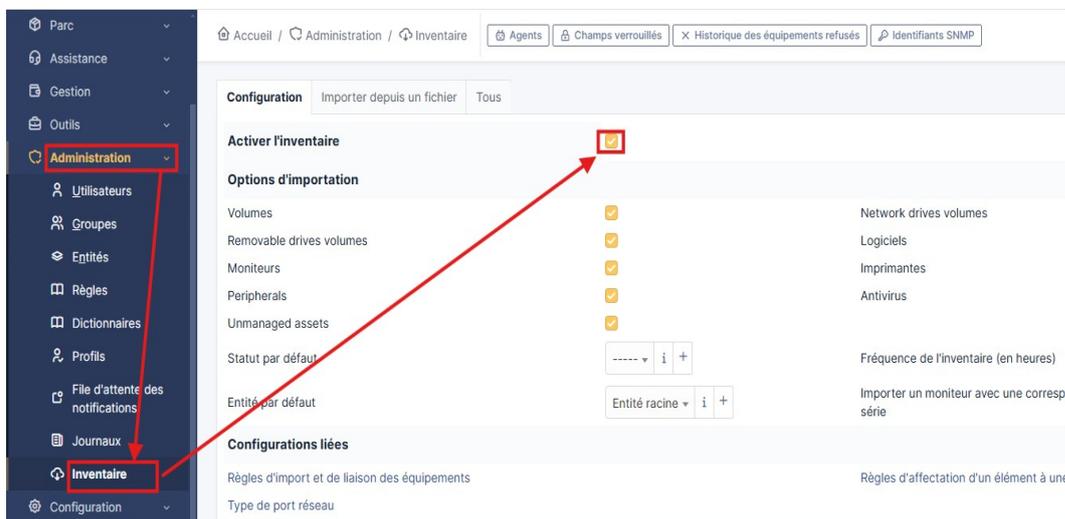
Exécution détaillée :

- ◆ L'agent GLPI est installé depuis le chemin réseau spécifié.
- ◆ Un inventaire est immédiatement lancé après l'installation (runnow=1).
- ◆ Une règle de pare-feu est ajoutée pour éviter que Windows bloque l'agent (Add_Firewall_Exception=1).
- ◆ L'agent est configuré pour envoyer l'inventaire à GLPI à l'URL donnée

Voilà, l'agent GLPI est prêt à être déployé par GPO :

Étape 4 : Activer L'inventaire dans GLPI :

- Se connecter sur GLPI,
- Allez dans **Administration** → **Inventaire**, ensuite cocher la case "**Activer l'inventaire**".



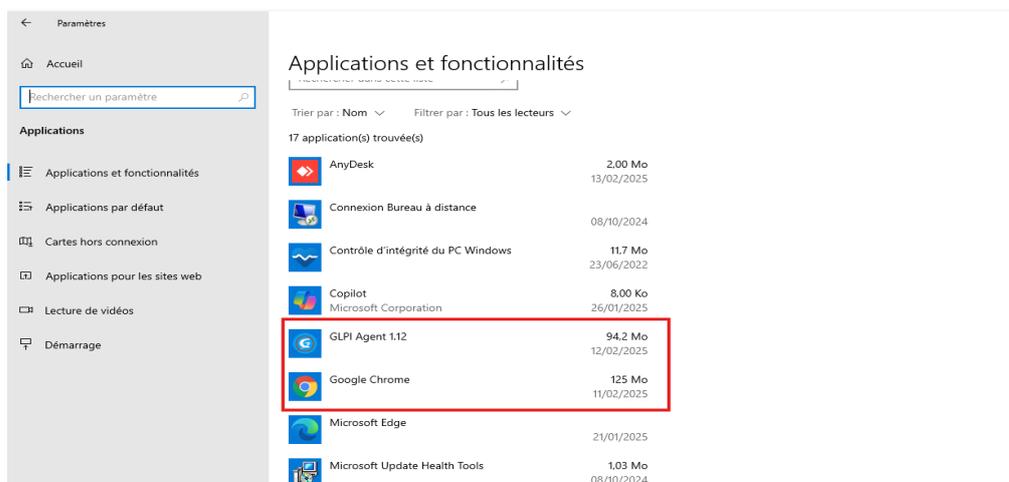
Phase de test : Test du déploiement des GPO

1. Redémarrer l'ensemble des PC concernés par les GPO.
2. Vérifier l'installation de Google Chrome et de l'Agent GLPI.

Après le redémarrage, l'installation des applications se lancera automatiquement.

Une fois terminée, vous pourrez retrouver les logiciels installés en accédant à :

Paramètres → **Applications**. Dans cet exemple, nous utiliserons "PCADM02".



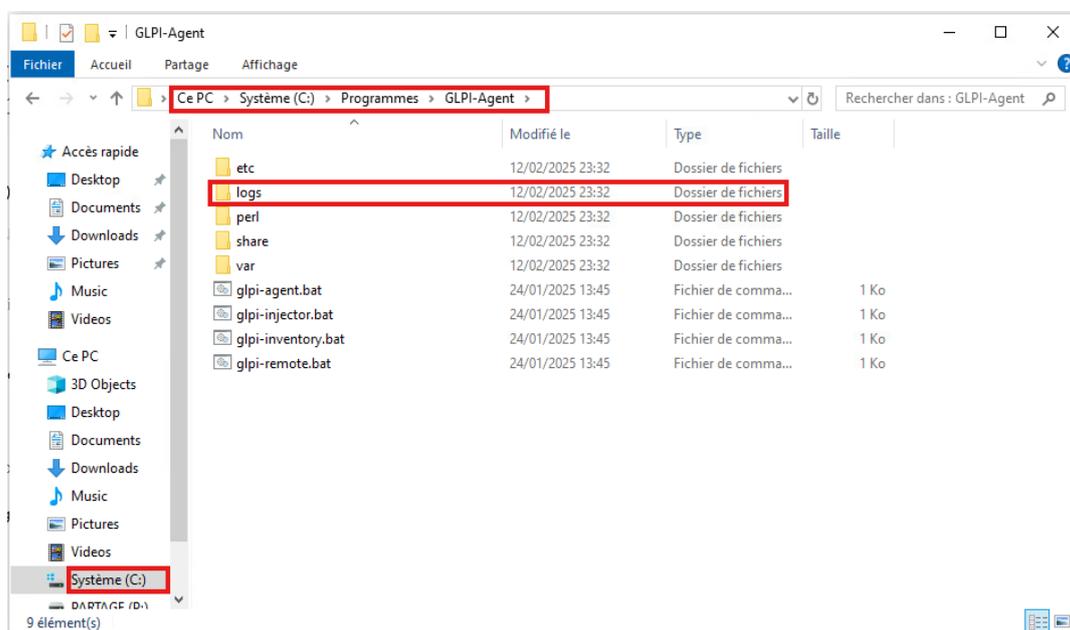
Ensuite vous trouverez les dossier de configuration et le dossier logs

- Sur le poste client, accéder au répertoire d'installation de l'agent :

C:\Programmes\GLPI-Agent

Astuce : Vous pouvez également consulter les fichiers de logs situés dans :

C:\Programmes\GLPI-Agent\log\glpi-agent.log pour vérifier si l'agent communique correctement avec le serveur GLPI.



Validation de la remontée des inventaires dans GLPI :

- Se connecter à l'interface GLPI.
- Vérifier la présence des nouveaux équipements dans l'inventaire.



Architecture Système

Procédure techniques Déploiement de serveur Active Directory AD sous Windows 2022

Ref : DOC_procedure_AD
Version 1.0.0
Date:02/01/2025
Page:1/33

Chercher dans le menu

- Parc
- Tableau de bord
- Ordinateurs**
- Moniteurs
- Logiciels
- Matériels réseau
- Peripherals
- Imprimantes
- Cartouches
- Consommables

Accueil / Parc / Ordinateurs

+ Ajouter Rechercher Listes Gabarits

Rechercher

Super-Admin
Entité racine (Arborescence)

Éléments visualisés contient

régle règle globale (+) groupe Rechercher

Actions

NOM	STATUT	FABRICANT	NUMÉRO DE SÉRIE	TYPE	MODÈLE	SYSTÈME D'EXPLOITATION - NOM	LIEU	DERNIÈRE MODIFICATION	COMPOSANTS - PROCESSEUR
DESKTOP-LOQH2PH		VMware, Inc.	VMware-72 81 7d d0 48 eb 43 71-b5 bd 37 f2 21 43 0a	VMware	VMware7,1	Microsoft Windows 10 Professionnel		2025-02-12 23:47	Intel Xeon Silver 4210 CPU @ 2.20GHz

20 lignes / page De 1 à 1 sur 1 lignes