Projet 1 :

Sommaire

Contexte:

Dans le cadre de mon travail au sein de Carrefour, un établissement spécialisé dans l'aggroalimentaire, j'ai participé à la mise en place d'une infrastructure réseau complète virtualisée sous Proxmox. Cette infrastructure vise à simuler un environnement professionnel avec des besoins en gestion centralisée des utilisateurs, des postes clients et des services réseaux.
Le projet 1 consiste à déployer un contrôleur de domaine Active Directory (AD DS), intégrant également les rôles DNS et DHCP, afin de gérer efficacement les utilisateurs, les ordinateurs, les groupes et les stratégies de sécurité dans un domaine nommé "ief2i.lan".
Ce projet est réalisé dans un objectif pédagogique, mais en suivant les standards et bonnes pratiques des environnements d'entreprise.

Prérequis :

- Une plateforme Proxmox avec plusieurs machines virtuelles
- Un serveur Windows Server 2022 destiné à accueillir les rôles AD DS, DNS et DHCP
- Un poste client sous Windows 10
- Un routeur/firewall pfSense pour la gestion réseau

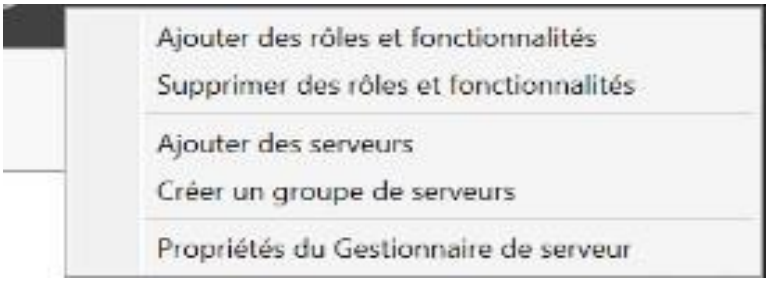
I) Mise en place d'un Contrôleur de Domaine Active Directory (AD DS)

Dans le cadre de ma formation, j'ai installé et configuré un Contrôleur de Domaine Active Directory (AD DS) sur Windows Server 2022. Ce serveur sera intégré dans une infrastructure virtuelle via Proxmox. Le domaine crée portera le nom suivant : ief2i.lan.

Cette étape est cruciale car elle permet de centraliser l'authentification des utilisateurs, de gérer les ressources réseau, et d'appliquer des stratégies de groupe (GPO). Voici les étapes nécessaires :

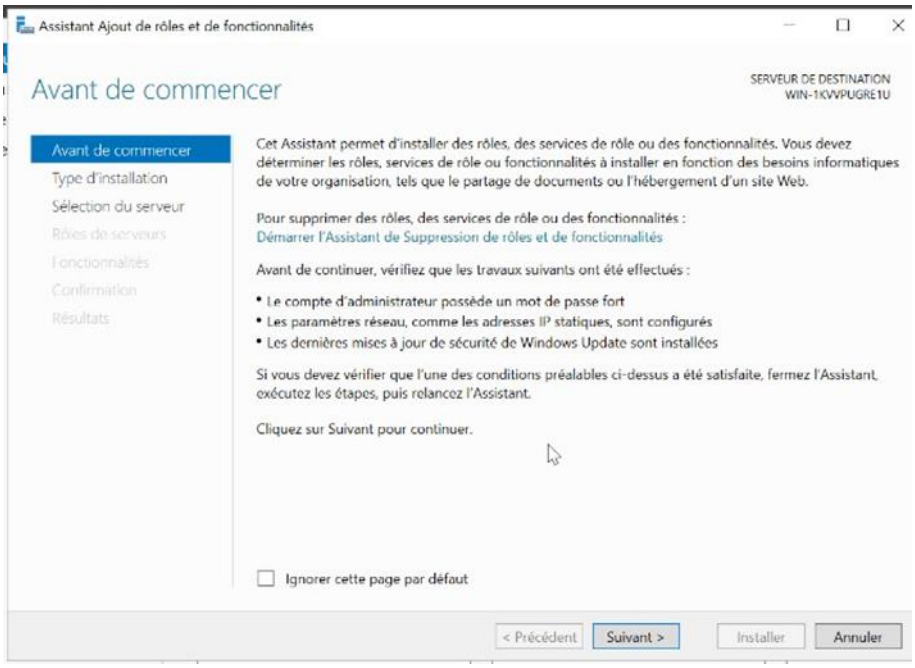
1. Accès au gestionnaire de serveur

Il faut tout d'abord lancer le Gestionnaire de serveur et cliquer sur « Gérer », puis « ajouter des rôles « et fonctionnalités ».



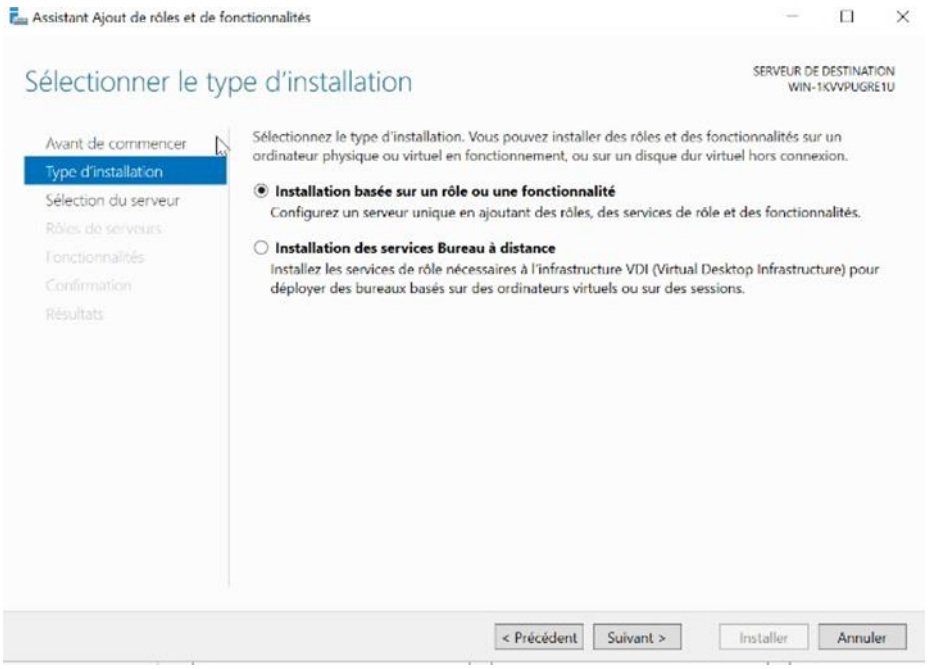
2. Assistant d'installation

Il important de vérifier que tous les prérequis sont remplis et ainsi cliquer sur « Suivant » pour continuer.



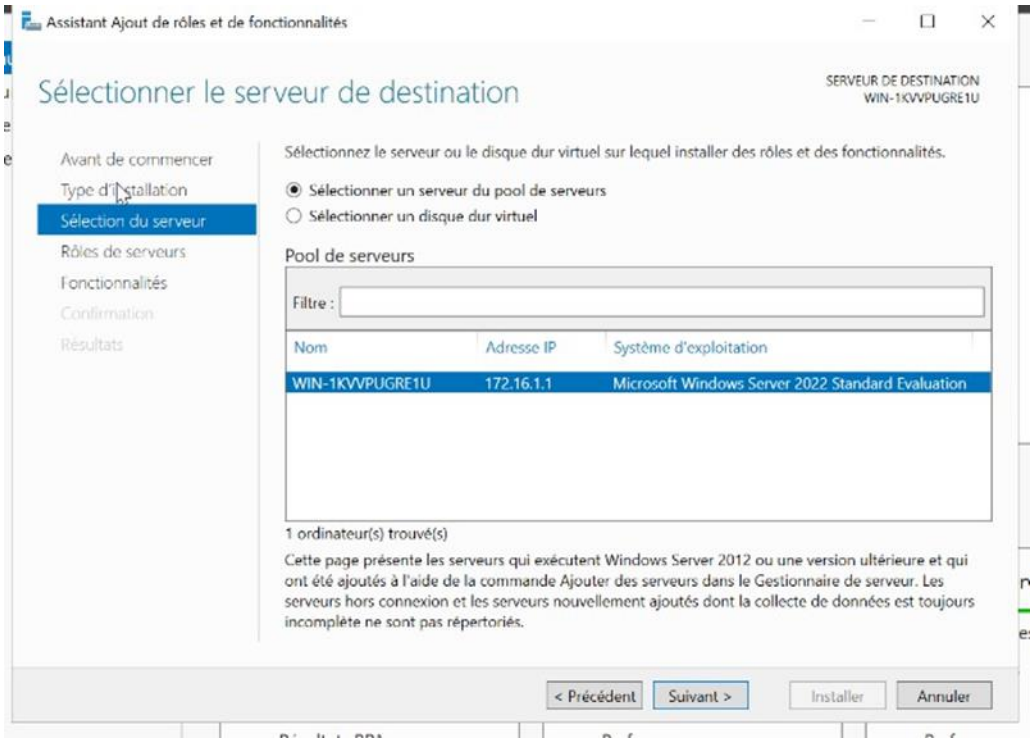
3. Type d'installation

Il faut ensuite choisir « Installation basée sur un rôle ou une fonctionnalité » et cliquer sur « Suivant».



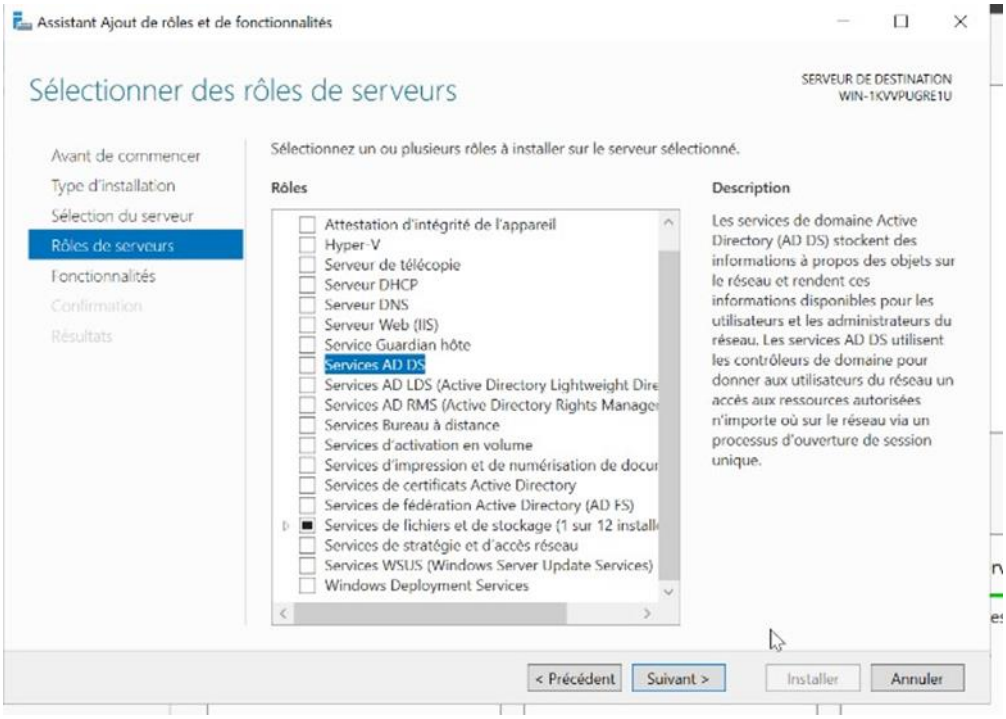
4. Sélection du serveur

La quatrième étape est de sélectionner le serveur cible de l'installation et valider avec « Suivant ».



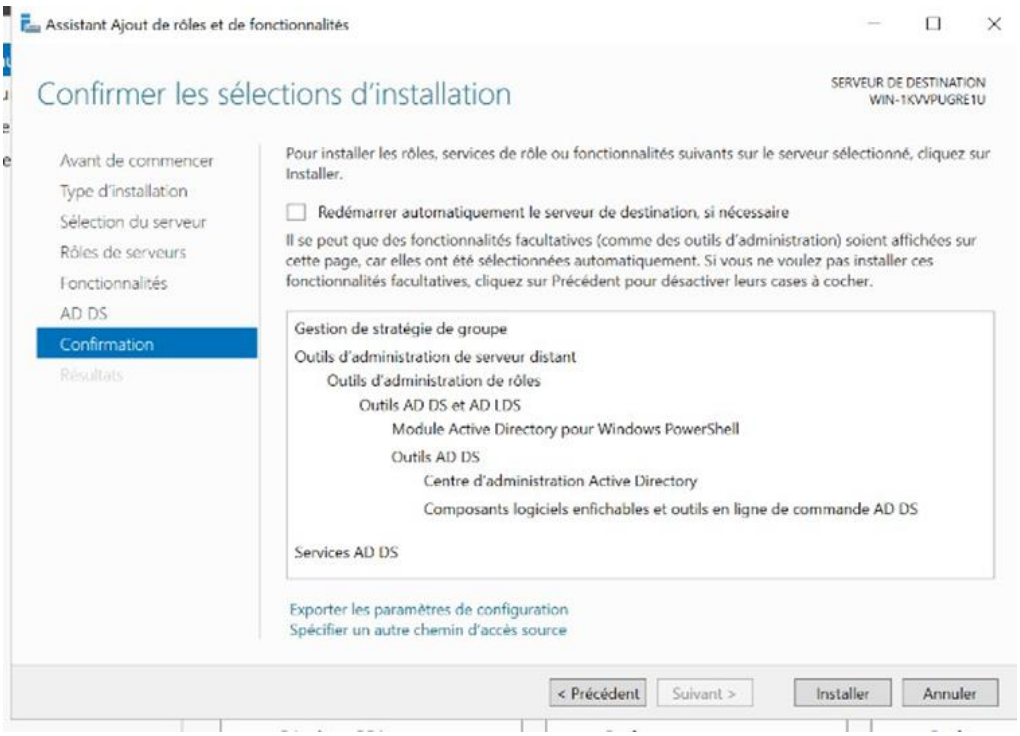
5. Sélection du rôle AD DS

Il faut ensuite cocher la case « Services AD DS ». Une fenêtre contextuelle proposera d'ajouter les fonctionnalités requises (Accepter), puis cliquer sur « Suivant ».



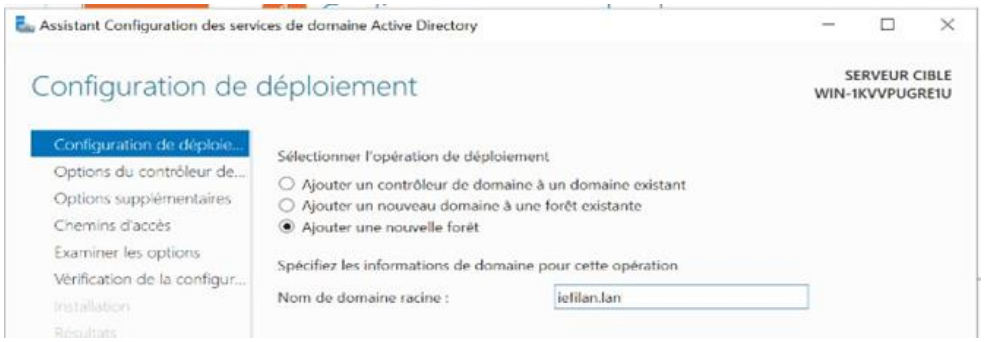
6. Confirmation d'installation

Tous les éléments doivent être corrects ainsi il faut cliquer sur « Installer ». L'installation peut prendre quelques minutes.



7. Configuration du déploiement

Après avoir sélectionner « Ajouter une nouvelle forêt », nous pouvons saisir le nom du domaine racine : ief2i.lan



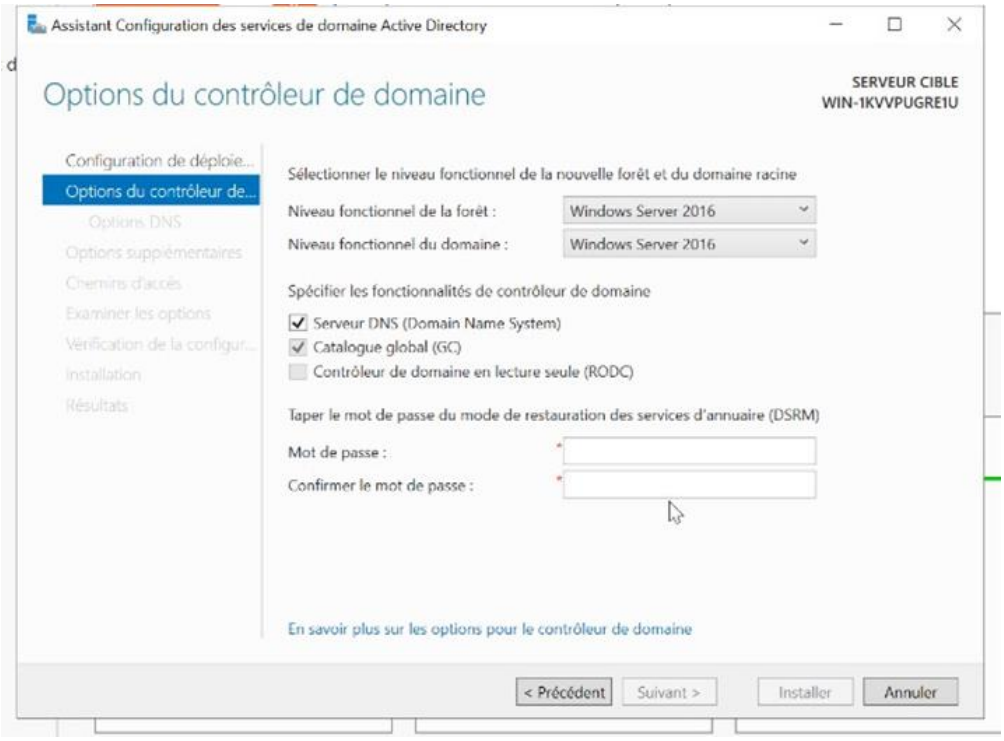
8. Options du contrôleur de domaine

Niveau fonctionnel de la forêt et du domaine : Windows Server 2016.

Les options suivantes doivent être cochées :

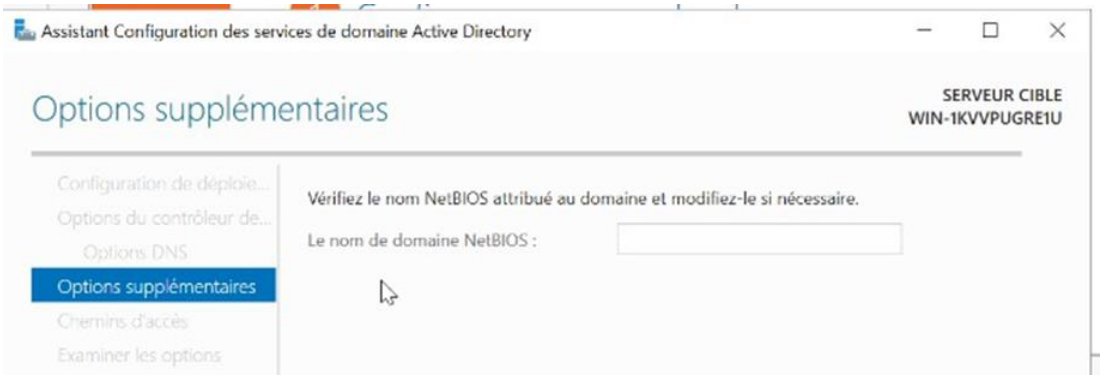
- Contrôleur de domaine DNS
- Catalogue global

En cas de panne de l'Active Directory il est indispensable de définir un mot de passe pour le mode de restauration DSRM.



9. Options supplémentaires

- Vérifier et, si besoin, modifier le nom NetBIOS (généralement proposé automatiquement).
- Cliquer sur Suivant, valider les chemins de base de données, fichiers journaux et SYSVOL.
- L'assistant réalise ensuite une vérification de la configuration.
- Cliquer sur Installer après validation.



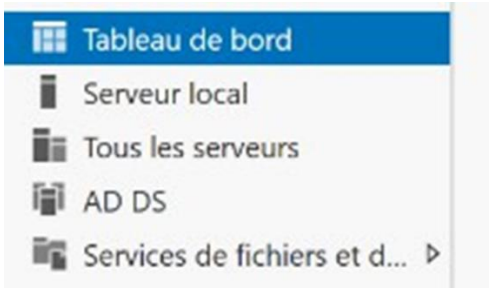
10. Configuration post-déploiement

Promotion du serveur en contrôleur de domaine

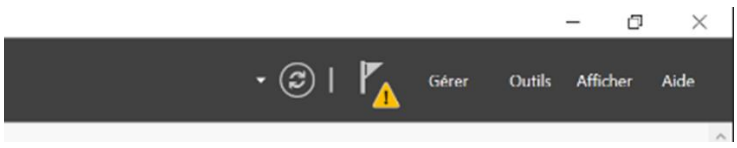
Une fois l'installation terminée, un message s'affiche dans le gestionnaire de serveur : « Ce serveur n'est pas encore un contrôleur de domaine Active Directory », il faut alors cliquer sur « Promouvoir ce serveur en contrôleur de domaine ».

11. Vérifications finales

Pour la vérification du rôle AD DS il faut retourner dans le Gestionnaire de serveur. Le rôle AD DS est désormais visible dans le tableau de bord.



Pour la vérification des événements il faut accéder à la section Événements du Gestionnaire de serveur puis vérifier qu'il n'y a pas d'erreurs liées au déploiement de l'AD DS. En cas d'erreur, consulter les journaux et redémarrer le serveur si nécessaire.



Conclusion : Le Contrôleur de Domaine Active Directory est maintenant configuré et fonctionnel. Il est désormais possible de :

- Créer et gérer des utilisateurs et groupes,
- Déployer des stratégies de groupe (GPO)
- Intégrer des postes clients dans le domaine
- Mettre en place les rôles DHCP et DNS si ce n'est pas déjà fait.

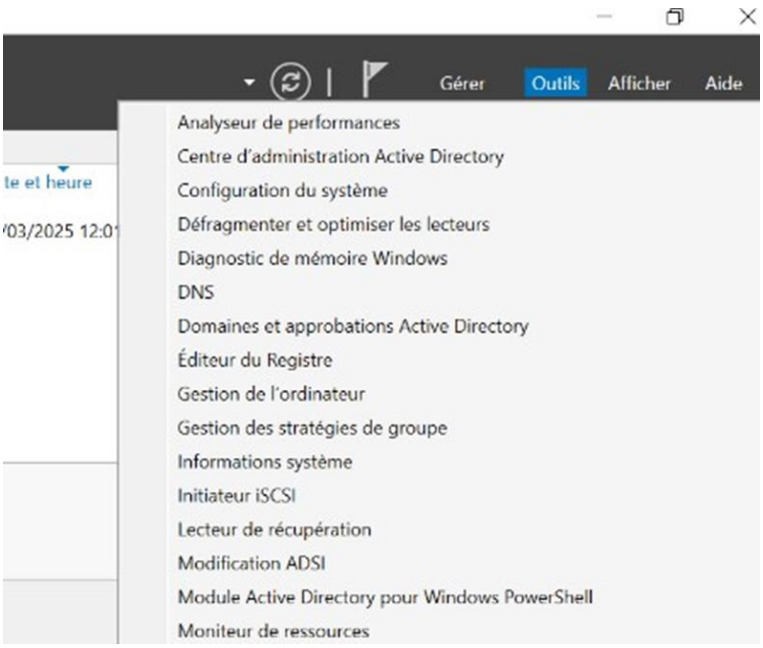
II) Configuration et vérification du service DNS

Lors de l'installation du rôle AD DS (Active Directory Domain Services) sur le serveur Windows, le rôle DNS est automatiquement installé. Ce service est essentiel pour permettre la résolution de noms au sein du domaine (traduction des noms de machines en adresses IP).

Ainsi, une fois la promotion du serveur en contrôleur de domaine terminée, une zone DNS est automatiquement créée et configurée avec le nom de domaine défini lors de la promotion (ici : ief2i.lan).

1. Accès au Gestionnaire DNS

Pour accéder à la console de gestion DNS il faut ouvrir le Gestionnaire de serveur et cliquer sur "Outils", puis sélectionner "DNS".

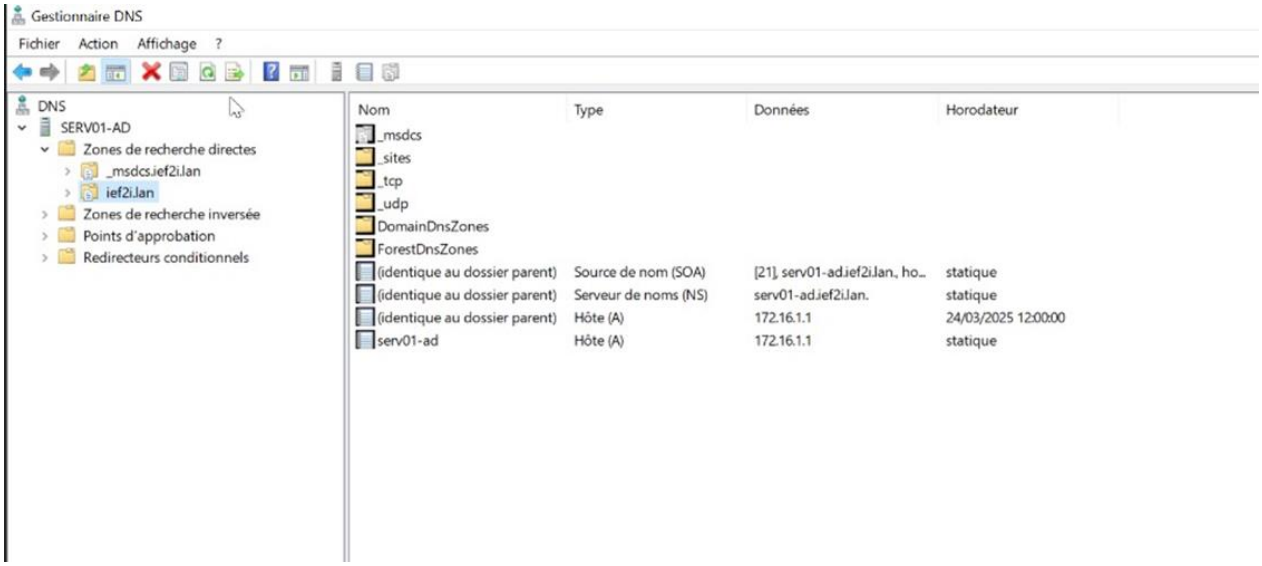


2. Structure de la zone DNS

Dans le gestionnaire DNS, on retrouve :

- Une zone de recherche directe pour le domaine ief2i.lan convertit en 172.16.1.1 par le DNS.
- Le client interroge le serveur DNS.
- Le serveur DNS cherche dans sa zone (ief2i.lan) un enregistrement de type A.
- Il trouve que serv01-ad correspond à 172.16.1.1.

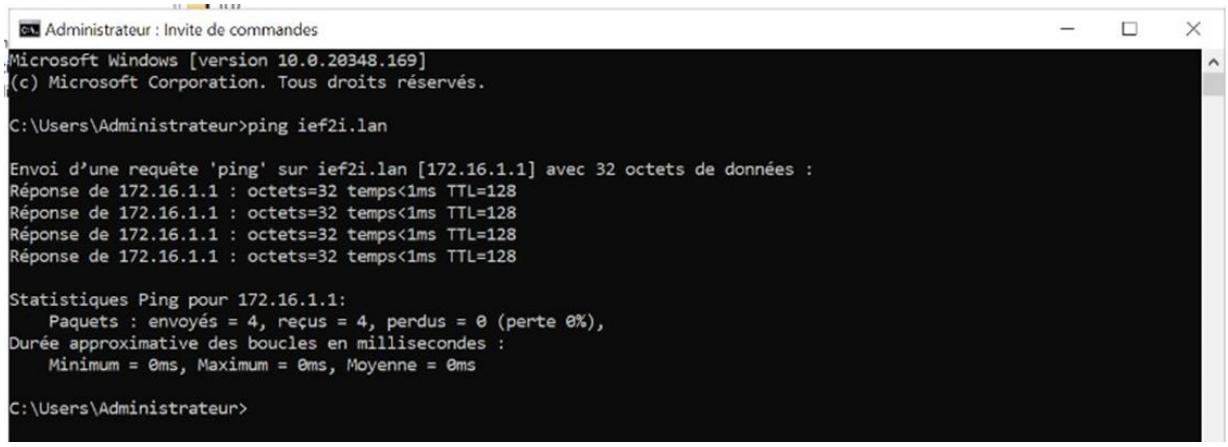
- Il retourne l'adresse IP au client → résolution faite



Cela permet aux machines du domaine de retrouver l'adresse IP du contrôleur de domaine à partir de son nom.

3. Test de résolution DNS

Un test de résolution DNS peut être effectué via l'invite de commandes, avec la commande suivante : "ping ief2i.lan"



Ce test vérifie que le nom de domaine est bien associé à l'adresse IP du serveur (172.16.1.1) et que le serveur DNS répond correctement.

Le résultat montre une résolution réussie sans perte de paquets, preuve que le service DNS fonctionne correctement.

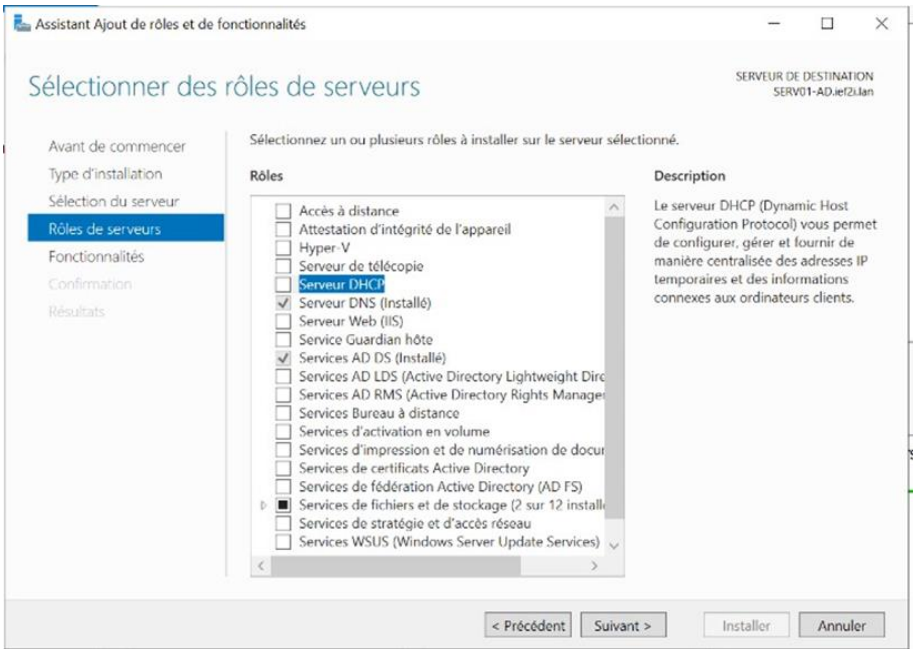
III) Déploiement du rôle DHCP sur Windows Server 2022

Dans le cadre de la mise en place d'un environnement réseau virtualisé à l'Institut F2I, nous avons intégré un serveur Windows Server 2022 dans une infrastructure Proxmox. Ce serveur héberge les rôles Active Directory, DNS et DHCP, nécessaires pour assurer une gestion centralisée des équipements. Le service DHCP (Dynamic Host Configuration Protocol) permet d'attribuer automatiquement des adresses IP aux postes clients, évitant ainsi la configuration manuelle de chaque machine.

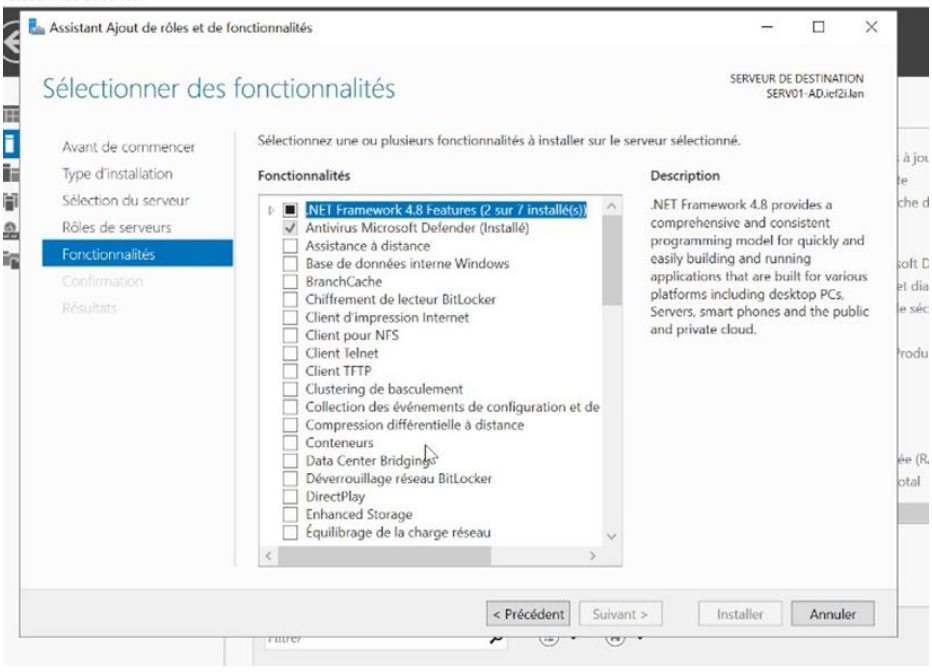
1. Installation du rôle DHCP

1.1 Lancement de l'assistant

Depuis le Gestionnaire de serveur, l'installation débute par l'ajout de rôles et fonctionnalités.



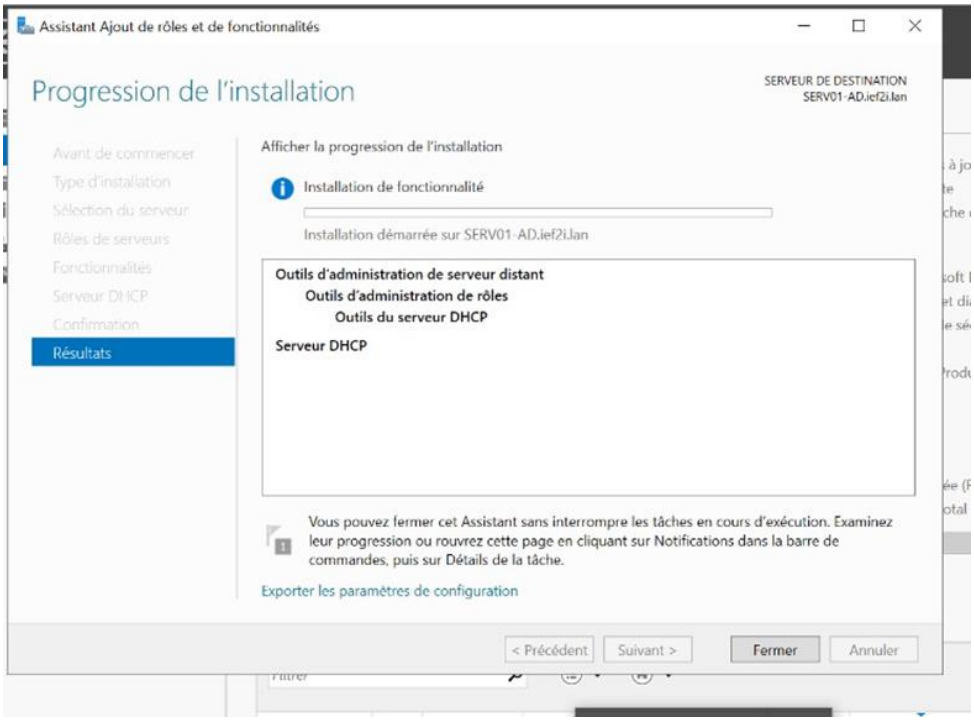
1.2 Sélection du rôle DHCP



Le rôle "Serveur DHCP" est sélectionné pour installation.

1.3 Installation du rôle

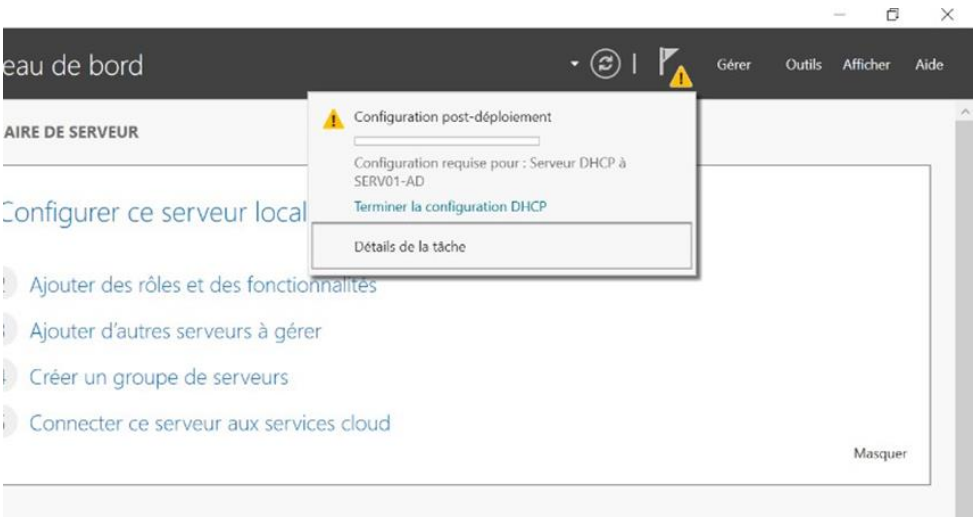
Après validation, l'installation est lancée et progresse automatiquement.



2. Configuration post-installation

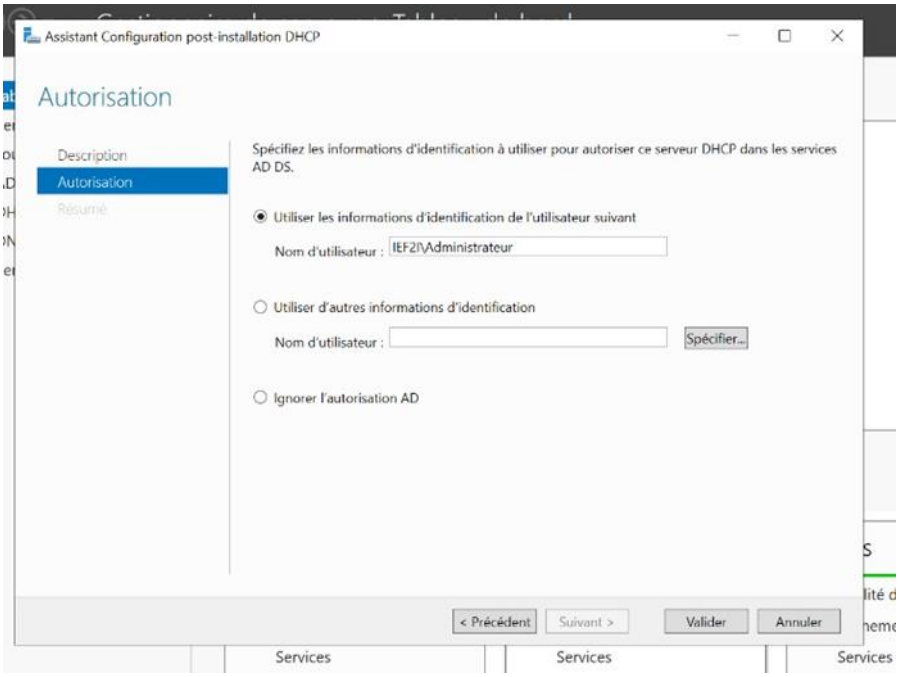
Une fois le rôle installé, une configuration post-déploiement est requise pour intégrer le DHCP à l'Active Directory.

2.1 Lancement de la configuration

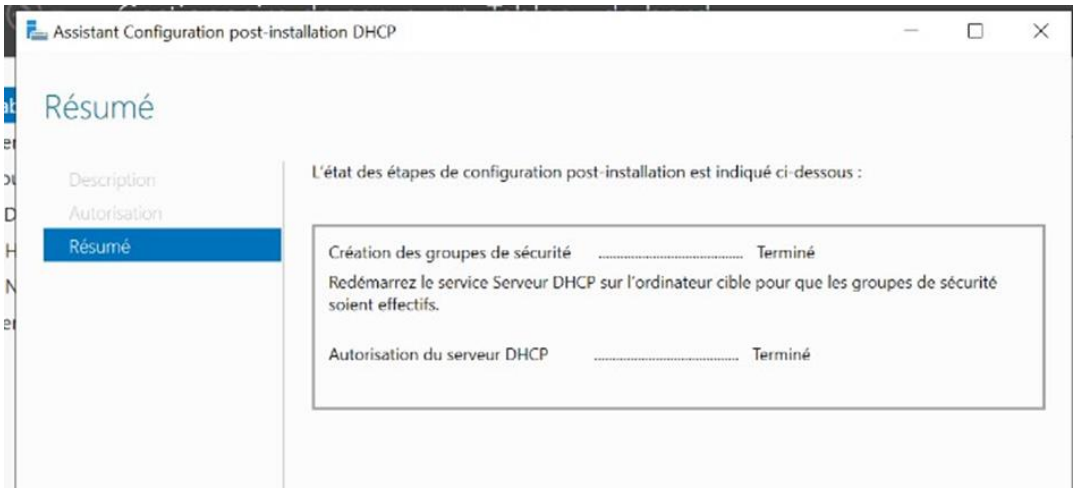


2.2 Autorisation dans l'AD

L'assistant demande de valider l'autorisation du serveur DHCP dans l'AD via le compte administrateur du domaine.



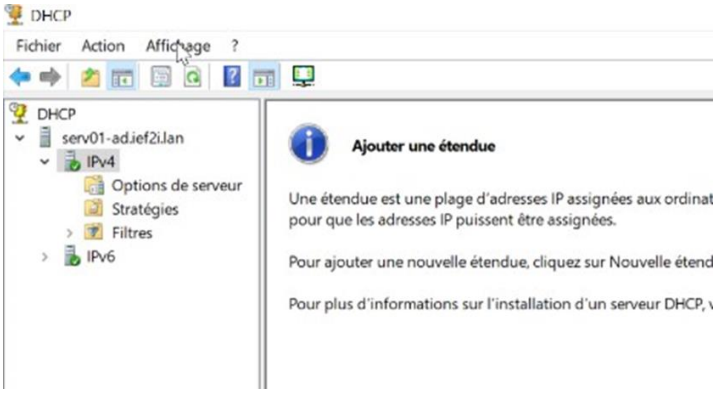
2.3 Résumé



3. Création de l'étendue DHCP

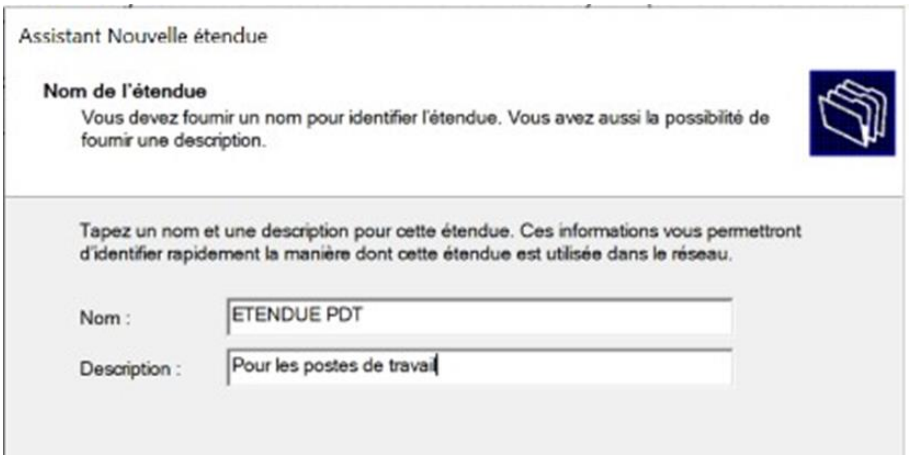
Une étendue définit la plage d'adresses IP que le serveur DHCP pourra attribuer aux clients.

3.1 Accès à la console DHCP

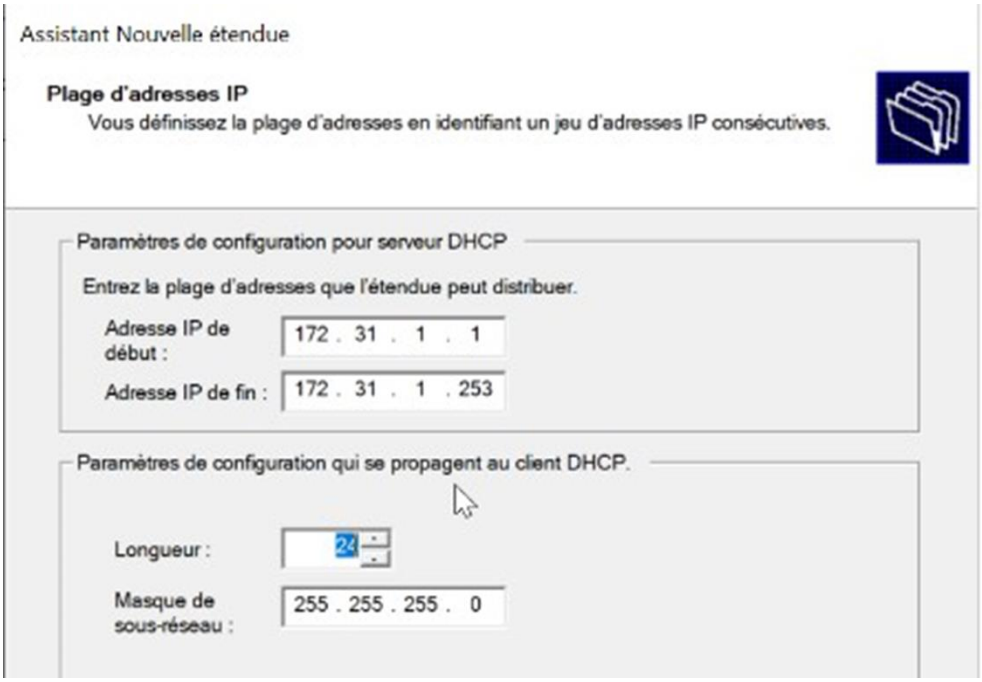


3.2 Nom et description

L'étendue est nommée "ÉTENDUE PDT", destinée aux postes de travail.



3.3 Définition de la plage IP

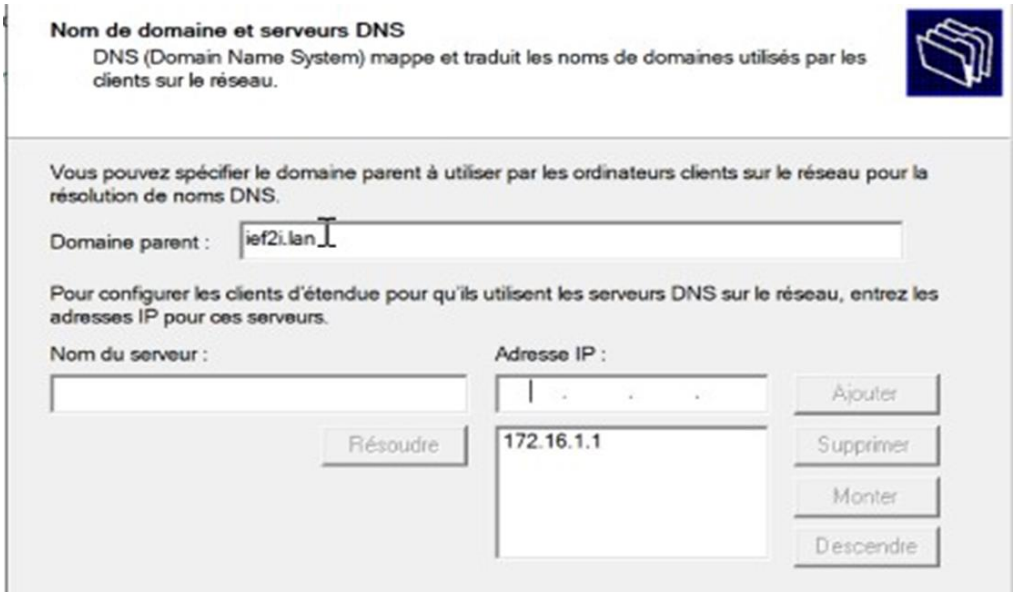


3.4 Passerelle par défaut

La passerelle 172.31.1.254 utilisée redirige vers le pfSence qui permet d'accéder au LAN et à Internet.

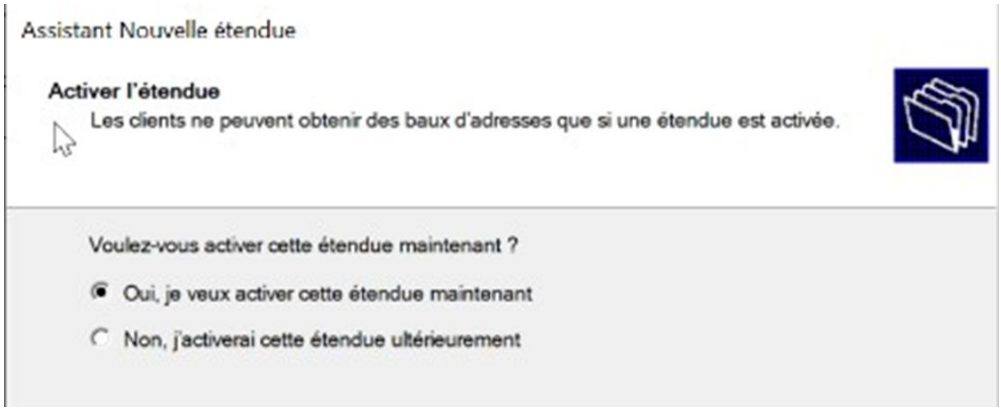
3.5 DNS

Les paramètres DNS permettent aux clients de résoudre le nom du domaine



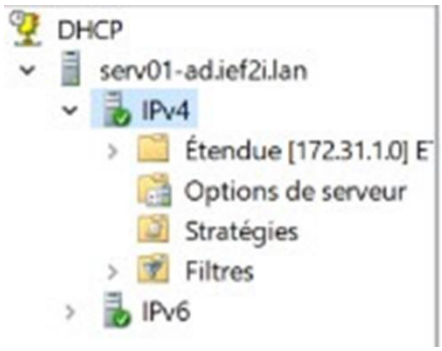
3.6 Activation de l'étendue

L'étendue est activée pour devenir immédiatement fonctionnelle.



4. Vérification de la configuration

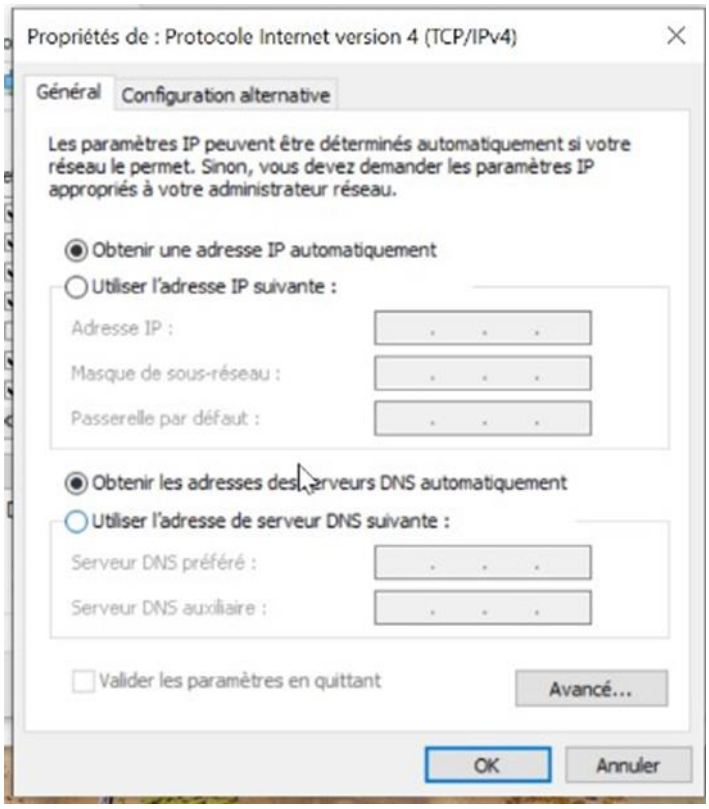
Dans la console DHCP, on vérifie que l'étendue a bien été créée et activée.



5. Test côté poste client

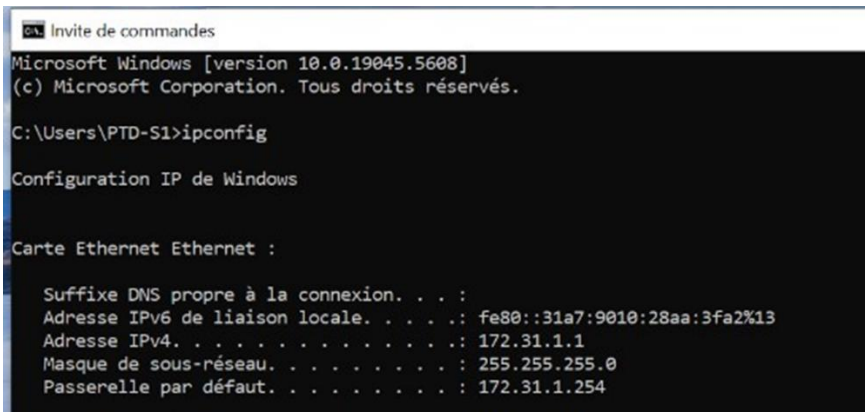
5.1 Configuration automatique

Le poste client Windows 10 est configuré pour obtenir automatiquement une adresse IP via DHCP.



5.2 Résultat de la commande ipconfig

Le client reçoit bien une IP dans la plage : 172.31.1.11, ainsi que la passerelle et le DNS définis.



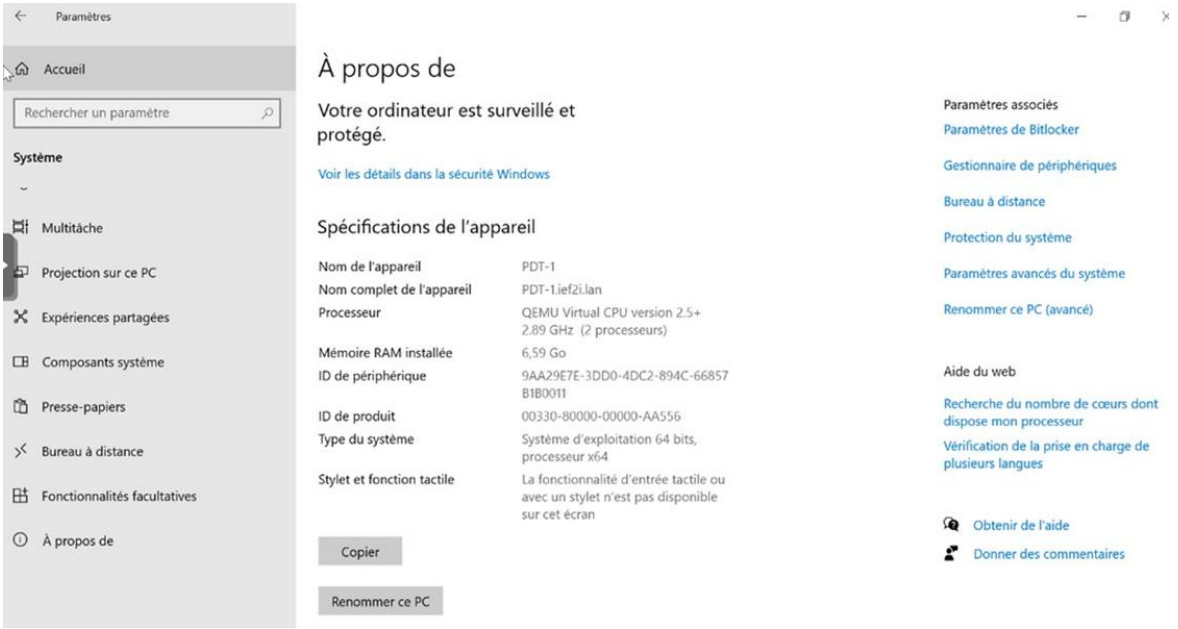
Conclusion : Le rôle DHCP est désormais pleinement fonctionnel et intégré au sein de l'infrastructure AD/DNS. Les clients reçoivent automatiquement une configuration IP valide. Le tout permet une gestion simplifiée et centralisée du réseau.

IV) Ajouter un poste de travail à un domaine Active Directory

Cette documentation explique comment configurer un poste client Windows pour qu'il rejoigne un domaine Active Directory.

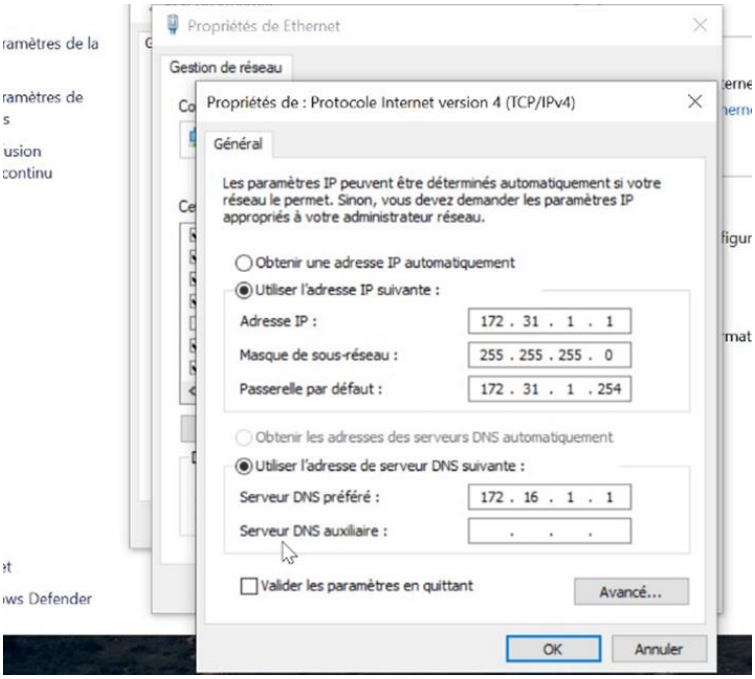
1. Vérifier les informations système du poste

Tout d'abord, il faut aller dans les paramètres de Windows > Système > À propos puis vérifier le nom de l'appareil et le nom complet de l'ordinateur.



2. Configurer l'adresse IP manuellement (ou par DHCP)

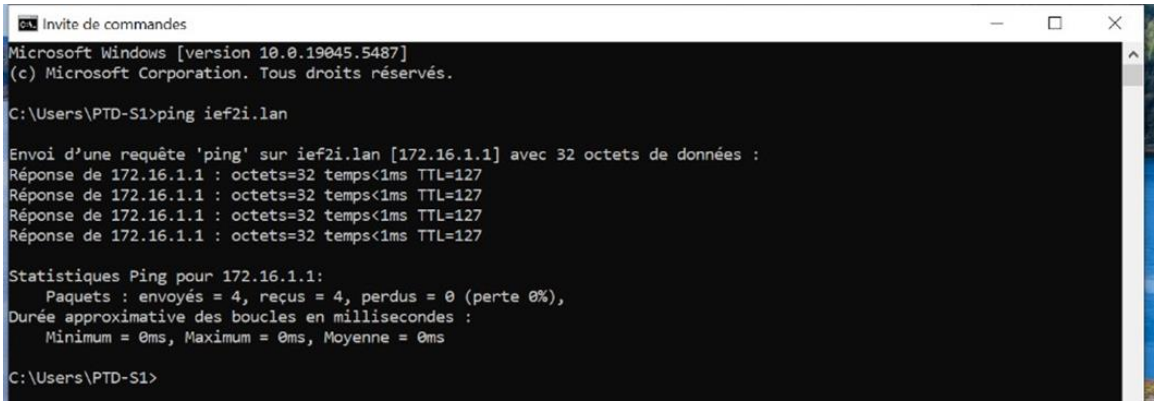
Pour configurer l'adresse IP il faut aller dans le Panneau de configuration > Réseau et Internet > Centre Réseau et partage > et modifier les paramètres de la carte. Il est maintenant possible de configurer manuellement une adresse IP dans le même sous-réseau que le serveur Active Directory et de renseigner l'adresse IP du serveur comme passerelle et serveur DNS.



3. Tester la connectivité avec le domaine

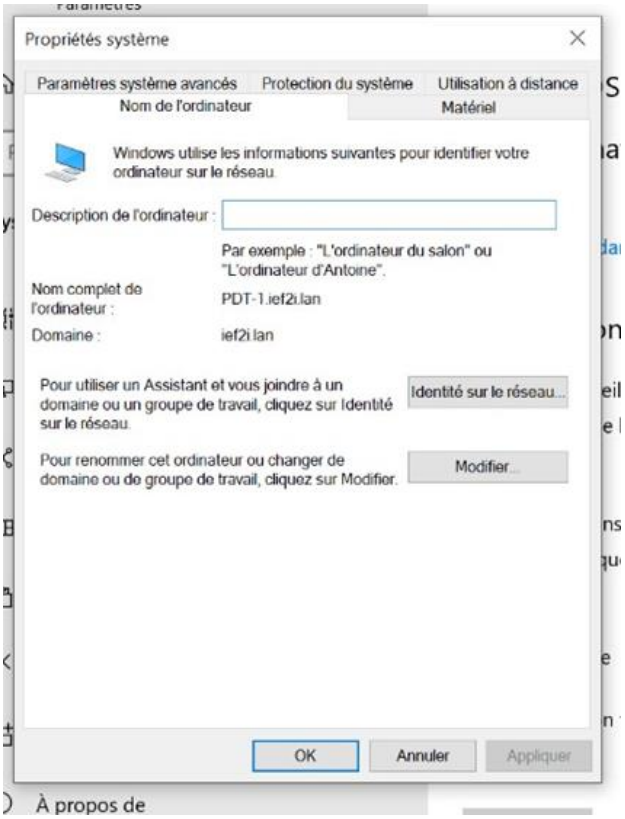
Il faut maintenant ouvrir l'invite de commandes (cmd) et lancer un test ping vers le domaine. La commande à utiliser est la suivante : ping ief2i.lan

Si le domaine répond, la connectivité est correcte.



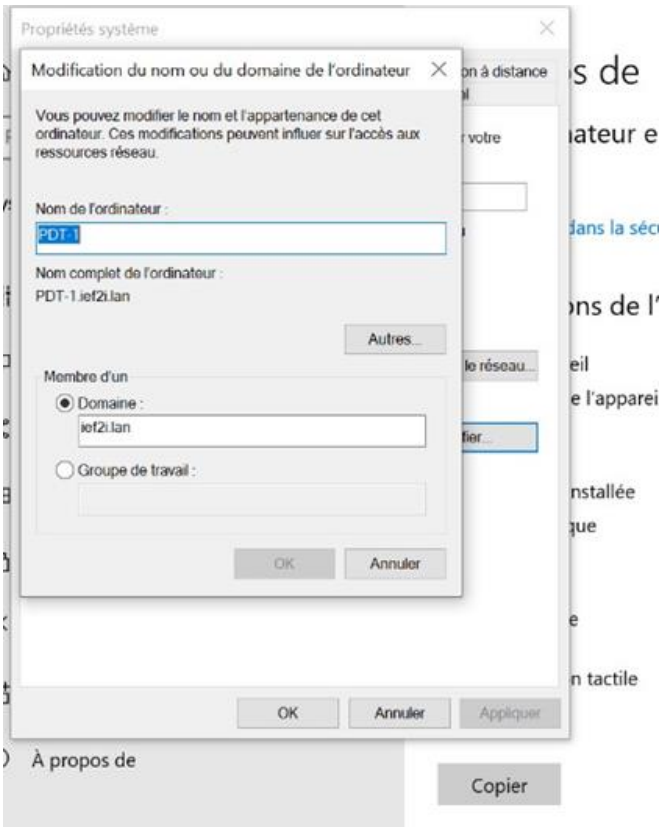
4. Rejoindre le domaine

Pour rejoindre le domaine, nous devons ouvrir les paramètres système avancés > Nom de l'ordinateur > Modifier et sélectionner "Domaine" et ainsi entrer le nom du domaine (exemple : ief2i.lan).



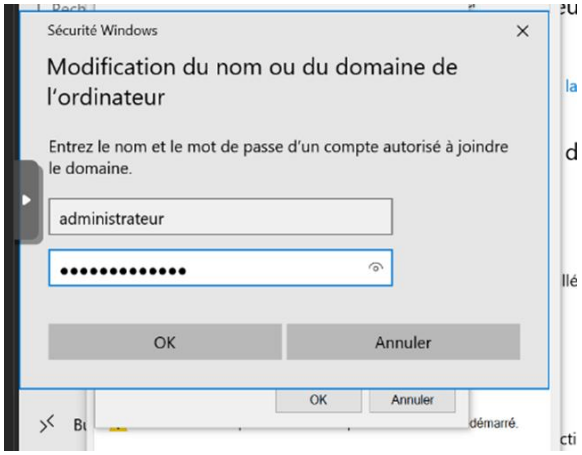
5. Authentifier l'ajout au domaine

Un écran s'affiche désormais pour entrer les identifiants. Ensuite il faut entrer les identifiants d'un compte autorisé à joindre des machines au domaine (ex : administrateur).



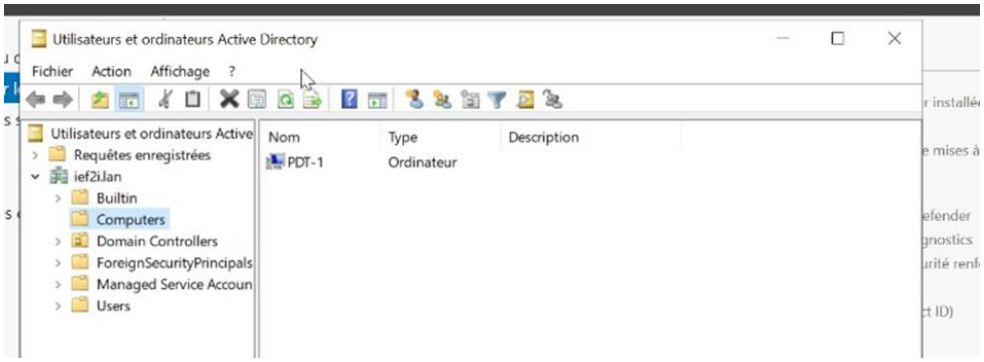
6. Confirmation d'intégration

Après validation, un message confirme que l'ordinateur a rejoint le domaine. Un redémarrage est demandé.



7. Vérification dans Active Directory

Sur le contrôleur de domaine, ouvrir la console "Utilisateurs et ordinateurs Active Directory". Aller dans le dossier "Computers" et vérifier que le poste apparaît.



V) Créer un utilisateur dans active directory

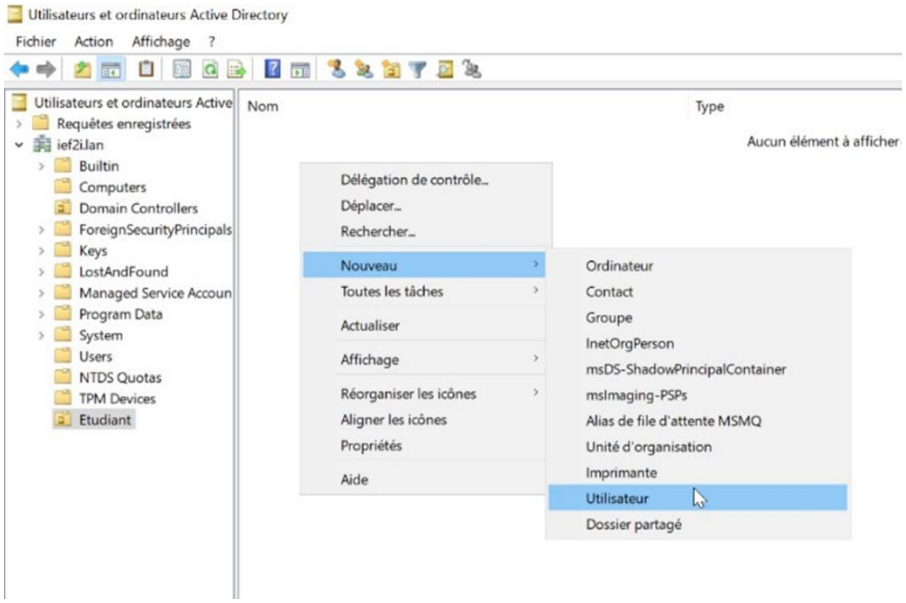
1. Accès à la console "Utilisateurs et ordinateurs Active Directory"

Avant toute manipulation, il est primordial d'ouvrir la console "Utilisateurs et ordinateurs Active Directory". Celle-ci permet de gérer les comptes utilisateurs, groupes et unités d'organisation (OU) dans le domaine.

2. Clic droit sur l'OU cible > Nouveau > Utilisateur

Dans l'arborescence à gauche, il faut créer un nouvel utilisateur dans l'OU puis clic droit pour choisir :

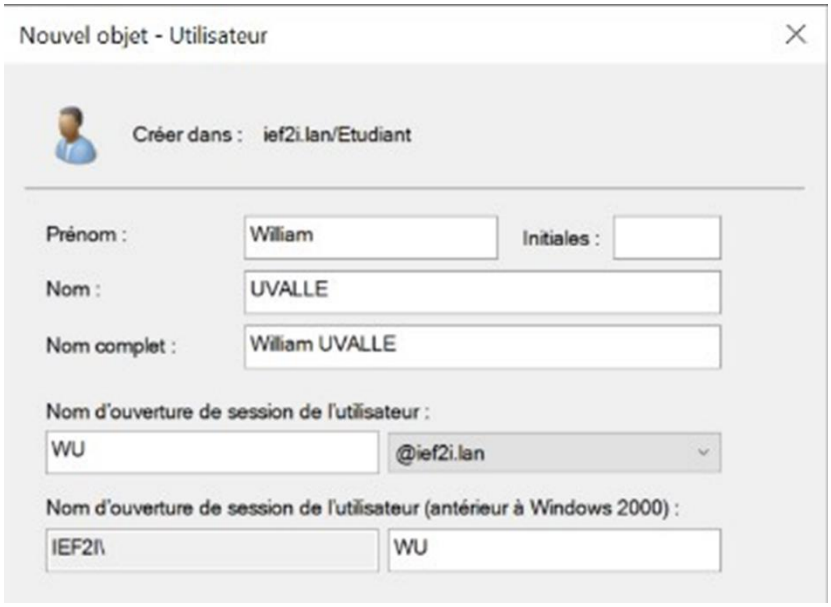
Nouveau > Utilisateur



3. Renseignement des informations de base de l'utilisateur

Dans la fenêtre qui s'ouvre, les informations suivantes sont nécessaires :

- Prénom
- Nom
- Nom d'ouverture de session (identifiant utilisateur)

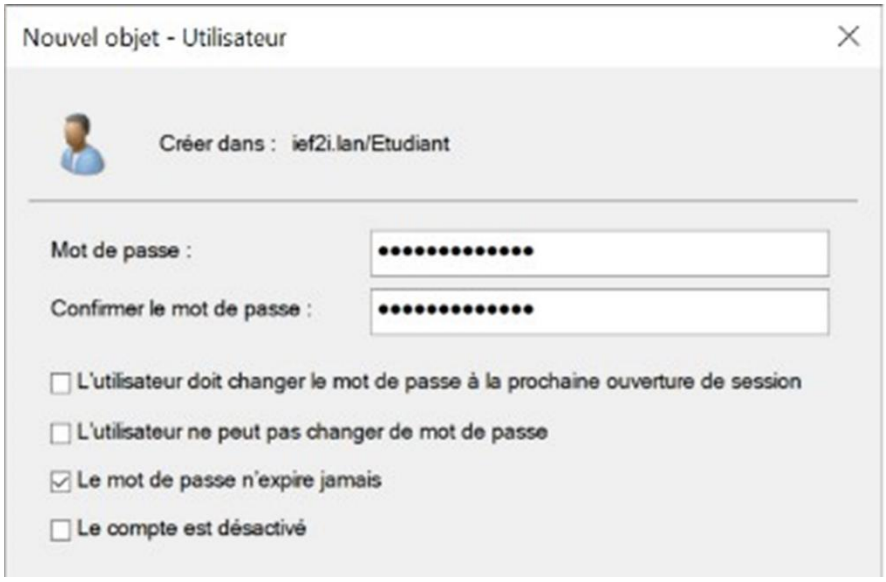


4. Définir le mot de passe du compte

À l'étape suivante, un mot de passe sécurisé pour le compte est nécessaire. Il est possible de choisir de forcer l'utilisateur à le modifier à sa première connexion, ou de le rendre permanent.

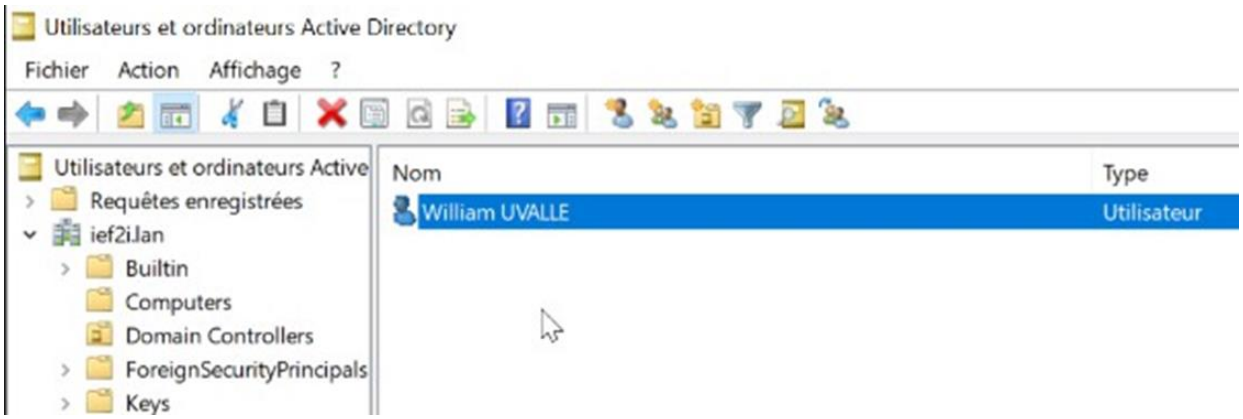
Options disponibles :

- L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
- L'utilisateur ne peut pas changer le mot de passe.
- Le mot de passe n'expire jamais



5. Vérifier le compte dans l'OU

Une fois validé, le compte apparaît dans l'OU sélectionnée. Il est maintenant possible de double-cliquer pour modifier ses propriétés si nécessaire.



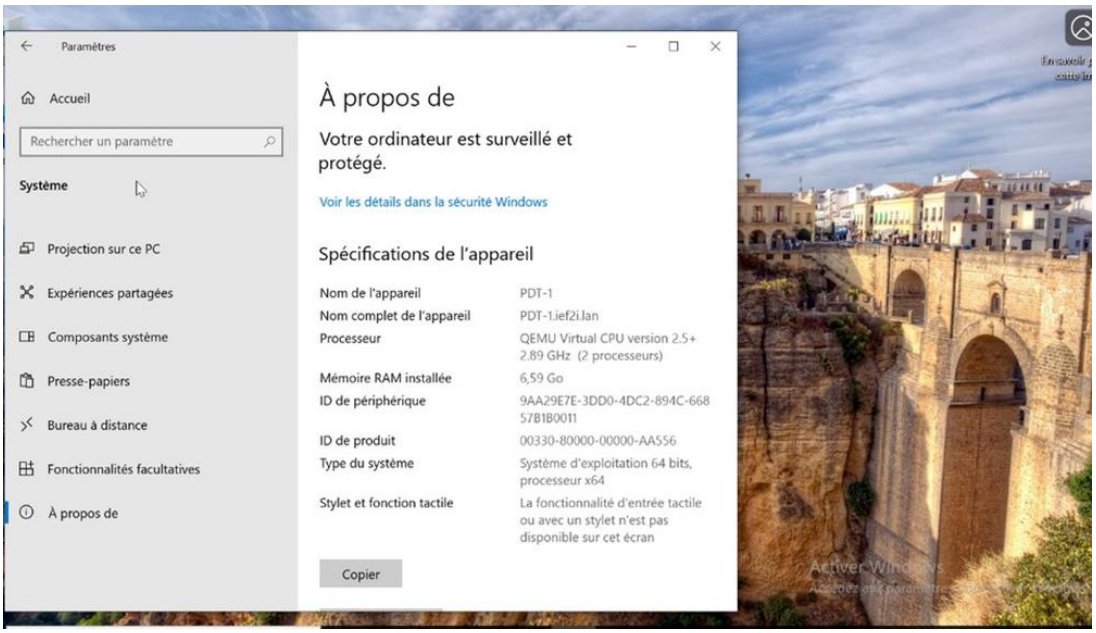
6. Connexion sur un poste de test

Sur un poste client connecté au domaine, il faut cliquer sur "Autre utilisateur" à l'écran de connexion.

Pour tester la connexion, il faut entrez l'identifiant utilisateur et le mot de passe définis précédemment.

7. Vérification de la session

Une fois connecté, il est important de vérifier si la session s'ouvre correctement et que le profil est bien créé. Cela confirme que le compte Active Directory est fonctionnel.

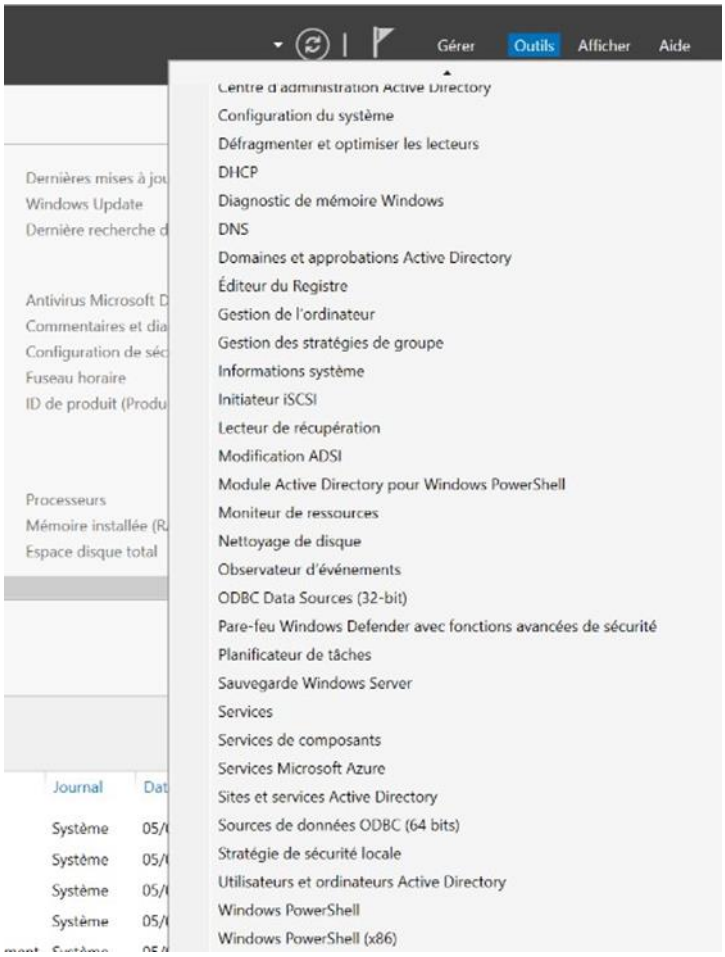


Conclusion : L'utilisateur a bien été créé, affecté à l'OU choisie, et a pu se connecter avec succès à une machine du domaine. Cette méthode permet de créer manuellement un utilisateur prêt à l'emploi dans un environnement Active Directory.

VI) Création d'une unité d'organisation (OU) – Guide pas à pas

1. Accès à l'outil de gestion Active Directory

Pour commencer, il faut ouvrir "Utilisateurs et ordinateurs Active Directory" depuis le menu démarrer ou la console d'administration.

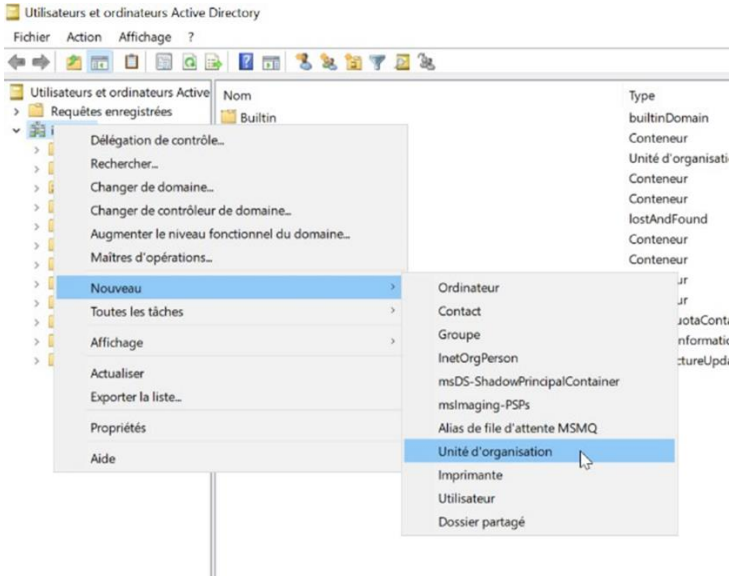


2. Navigation dans l'arborescence

Une fois arriver jusqu'au domaine cible dans le panneau gauche, nous pouvons créer l'unité d'organisation.

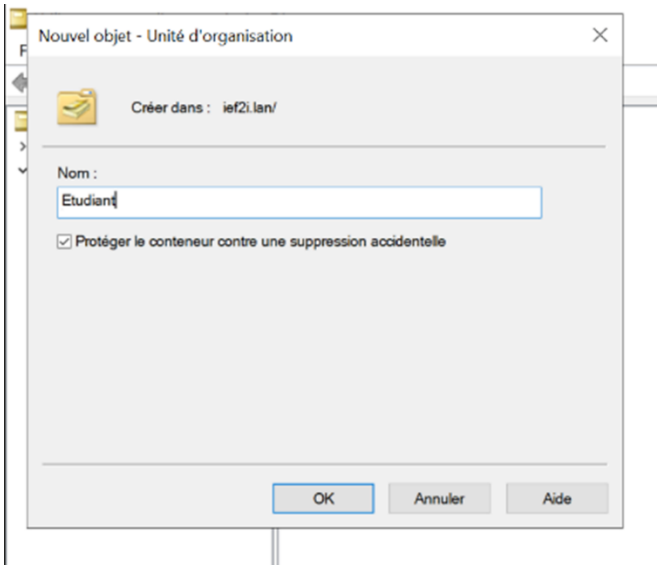
3. Création de l'OU

Un clic droit sur le conteneur ou le domaine est nécessaire afin de sélectionner "Nouveau" > "Unité d'organisation".



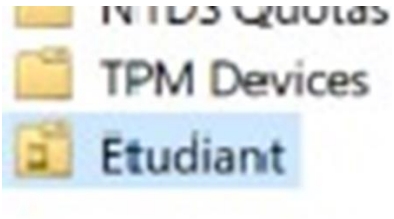
4. Définition du nom de l'OU

On peut désormais renseigner le nom de l'unité d'organisation souhaitée. Ce nom doit être explicite et en lien avec son usage (ex : Étudiants, Support, RH...).



5. Validation de la création

La validation de la création s'effectue en cliquant sur "OK". L'unité d'organisation s'affiche alors dans la structure du domaine.



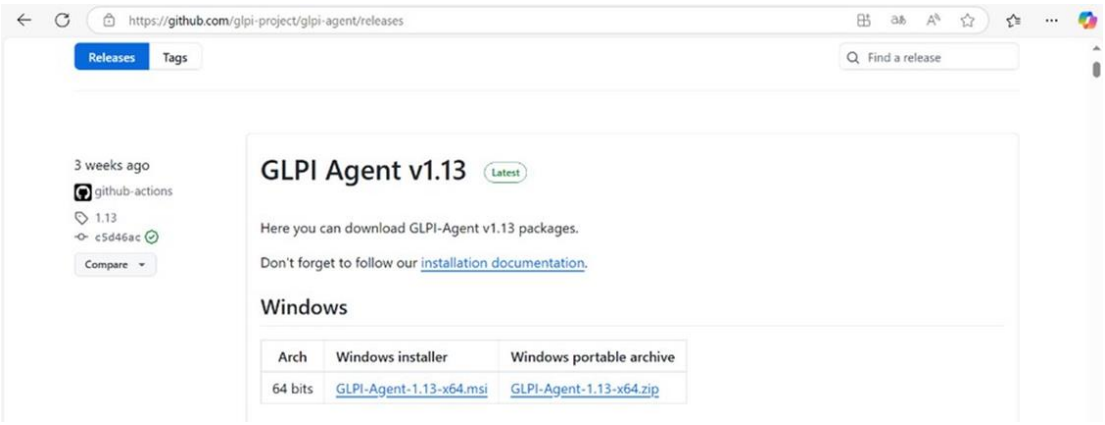
Conclusion : L'unité d'organisation est désormais créée. Il est possible maintenant d'y ajouter des utilisateurs, groupes ou ordinateurs, ou encore appliquer des stratégies de groupe (GPO) spécifiques. Les captures d'écran mentionnées ci-dessus peuvent être insérées pour illustrer chaque étape de façon claire et professionnelle.

VII) Déploiement de l'agent GLPI via GPO – Guide détaillé

1. Téléchargement de l'agent GLPI

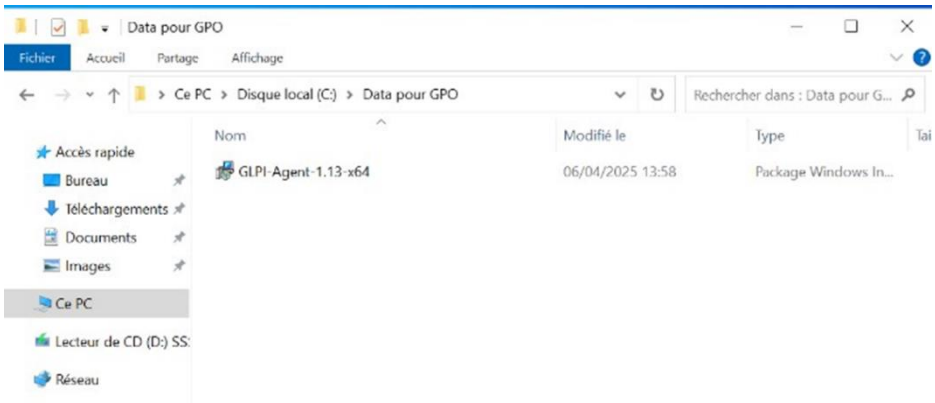
Tout d'abord, il faut télécharger l'agent GLPI sous forme de fichier.msi, depuis le site officiel ou la page GitHub du projet.

Ce fichier sera utilisé pour le déploiement via la GPO.



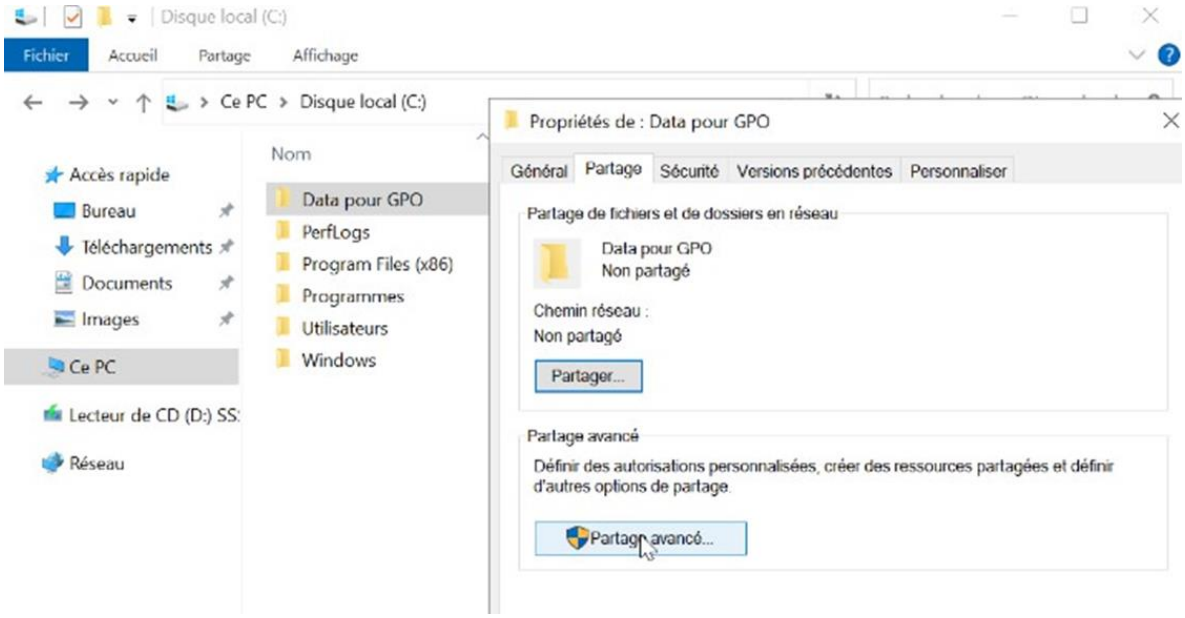
2. Préparation d'un dossier de partage contenant le MSI

Un dossier dédié à la GPO doit être crée sur le disque local (par exemple C:\GPO\GLPI-Agent\) afin d'être placé dans le fichier .msi de l'agent.



3. Partage du dossier en réseau

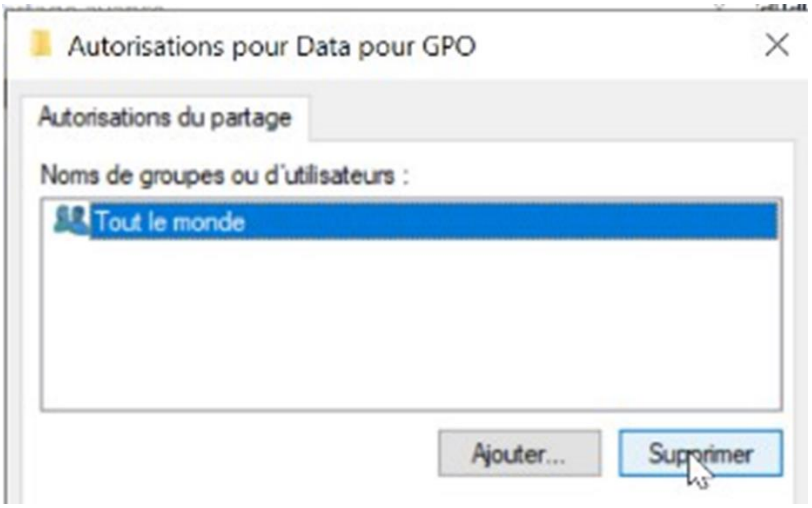
Il faut ensuite cliquer droit sur le dossier, puis "Propriétés" > "Partage avancé". Le partage du dossier doit être activer et doit posséder un nom reconnaissable.



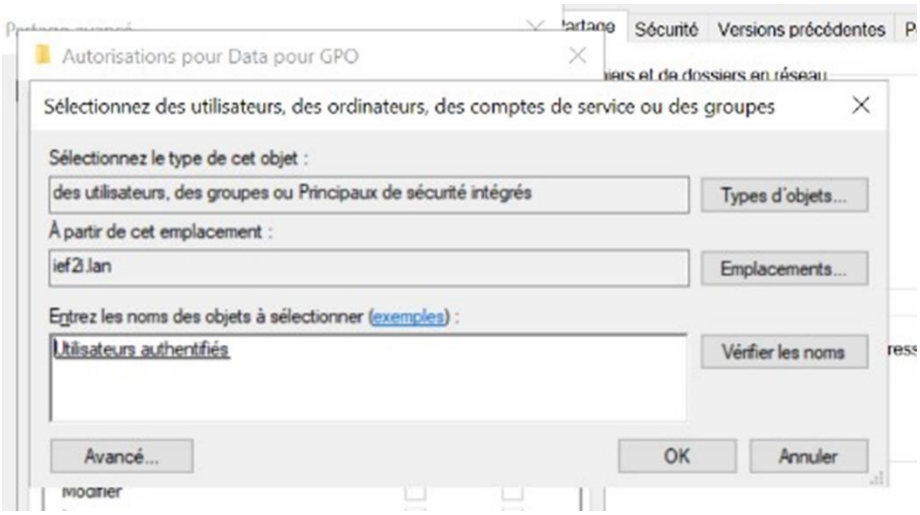
4. Définition des autorisations de sécurité du dossier partagé

Le groupe "Utilisateurs authentifiés" doit être ajouté aux autorisations de sécurité pour que tous les postes puissent accéder au MSI via le réseau.

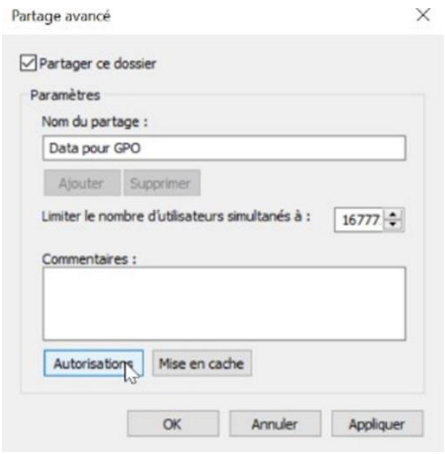
1.



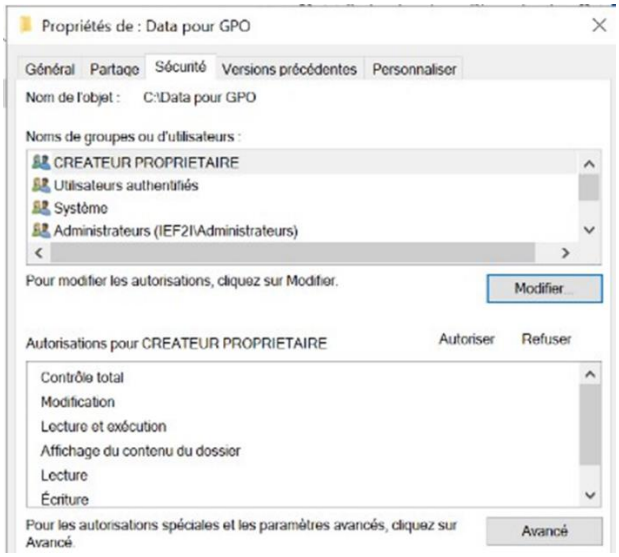
2.



3.

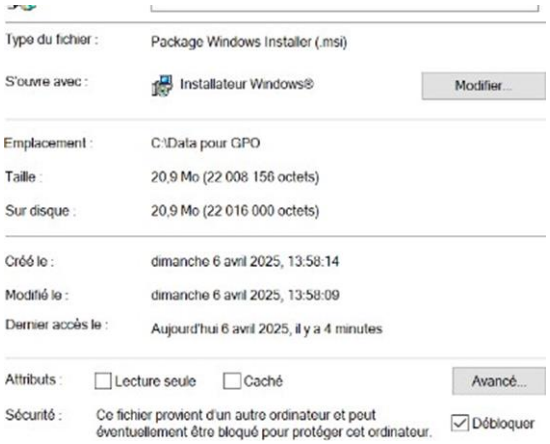


4.



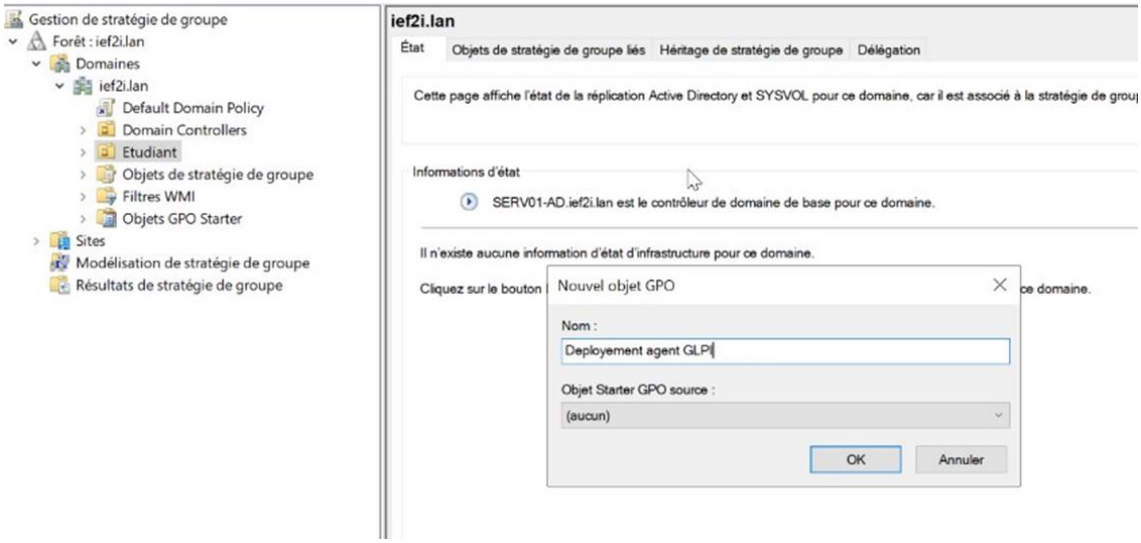
5. Déblocage du fichier MSI (si besoin)

Il faut ensuite cliquer droit sur le fichier MSI > Propriétés > et cocher "Débloquer" si cette option apparaît.



6. Création de la GPO

Dans la console GPMC, il faut créer une nouvelle GPO liée à l'OU contenant les postes concernés.



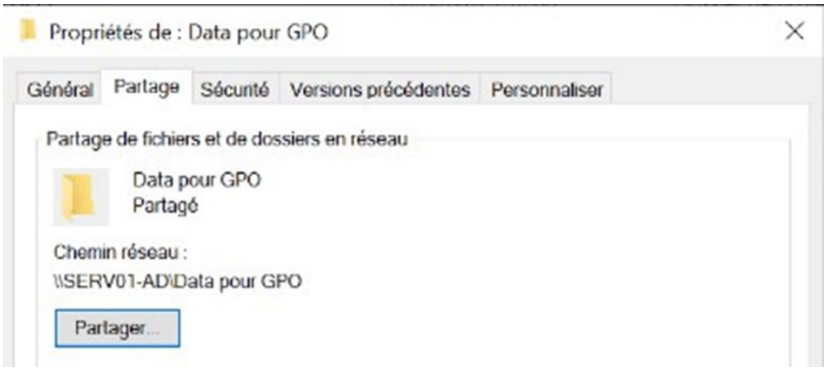
7. Configuration de l'installation du logiciel via GPO

Dans la GPO, il faut suivre les informations suivantes :

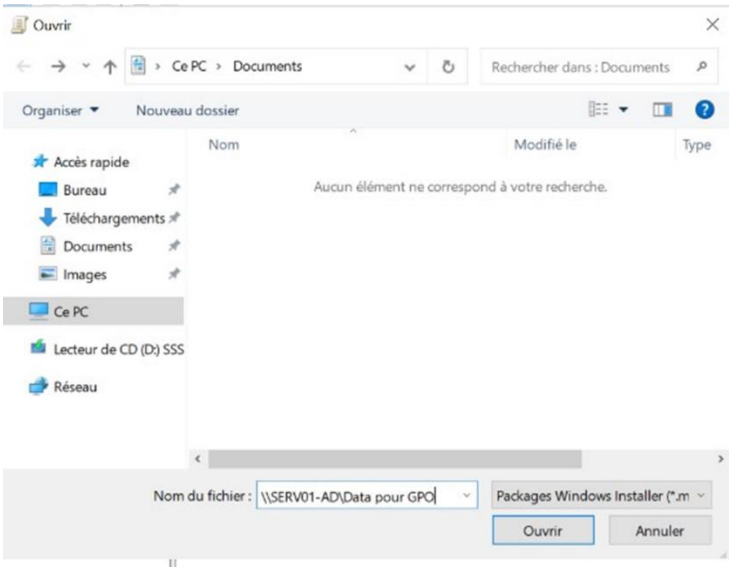
- Aller dans Configuration utilisateur > Paramètres logiciels > Installation de logiciels.
- Ajouter un nouveau package

Il est important d'utiliser un chemin réseau UNC (ex : \\serveur\GPO\GLPI-Agent\glpi-agent.msi), pas un chemin local.

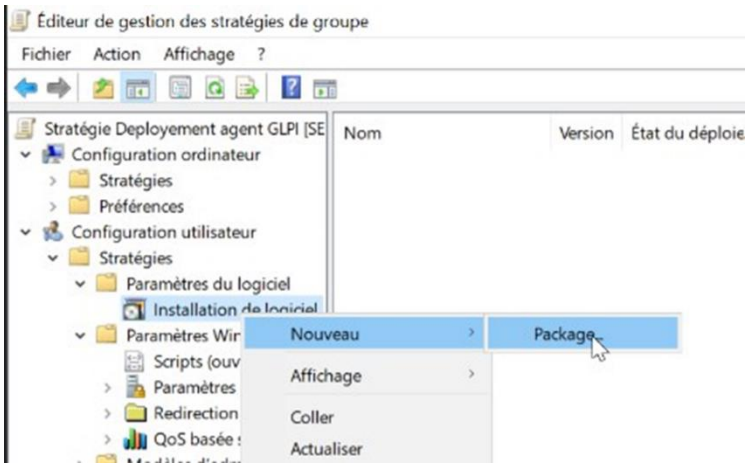
1.



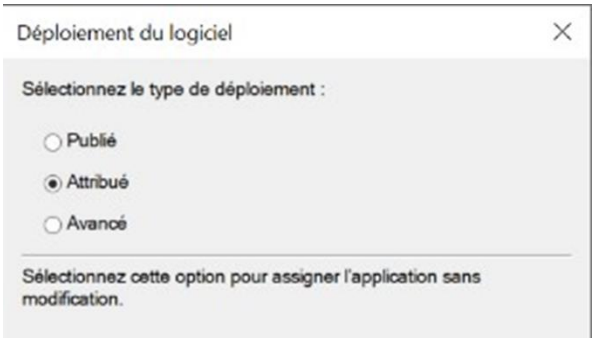
2.



3.



4.

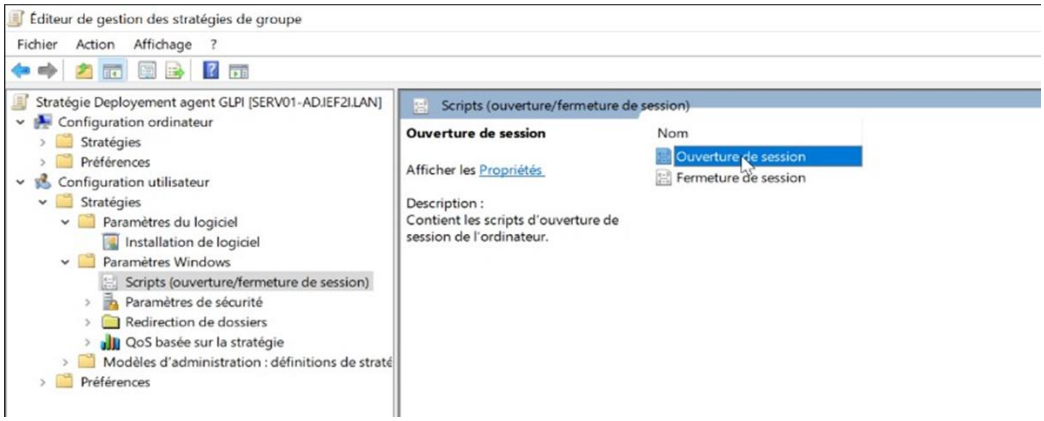


8. Ajout un script d'ouverture de session (si besoin)

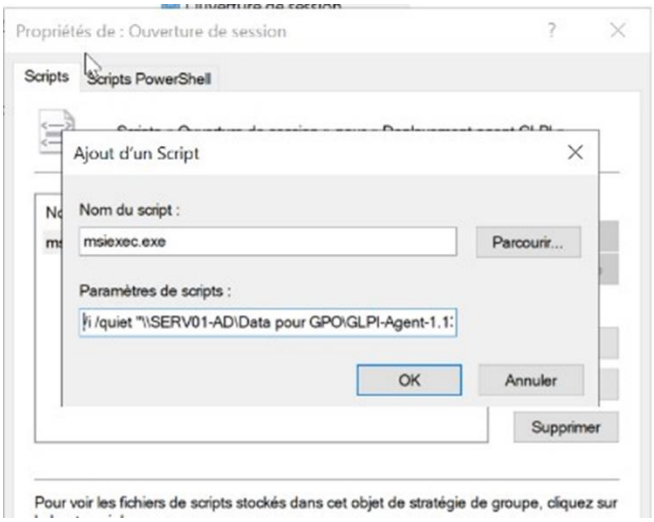
Dans la GPO, il est possible également d'ajouter un script d'ouverture de session pour lancer l'installation si elle ne se fait pas automatiquement.

1.

Paramètre: /quiet /i “\win2022\agentglpi\GLPI-Agent-1.4-x64.msi’’ RUNNOW=1 ADD_FIREWALL_EXCEPTION=1EXECMODE=1 SERVER= ‘’http://192.168.4.11/glpi”

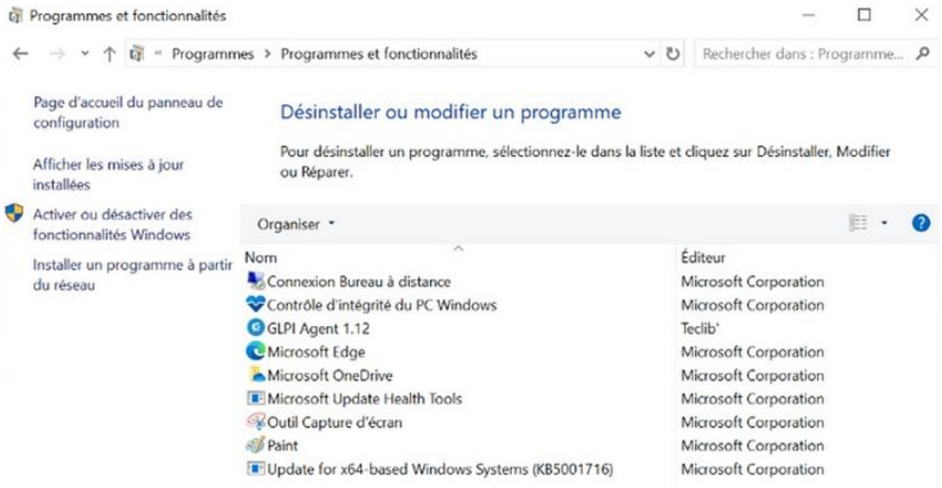


2.



9. Vérification sur un poste client

Après avoir appliqué la GPO et redémarré un poste, l’agent GLPI est doit être bien installé dans "Programmes et fonctionnalités".

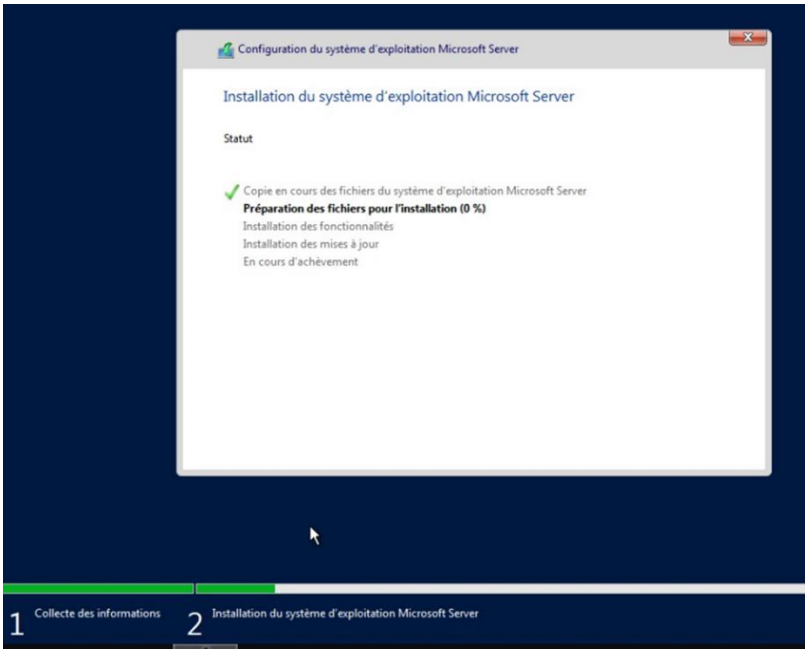


Conclusion : En suivant ces étapes, il est désormais possible de déployer l'agent GLPI de manière centralisée via une GPO, ce qui permet d'uniformiser et d'automatiser son installation sur tous les postes d'un domaine.

VIII) Ajout d'un contrôleur de domaine secondaire

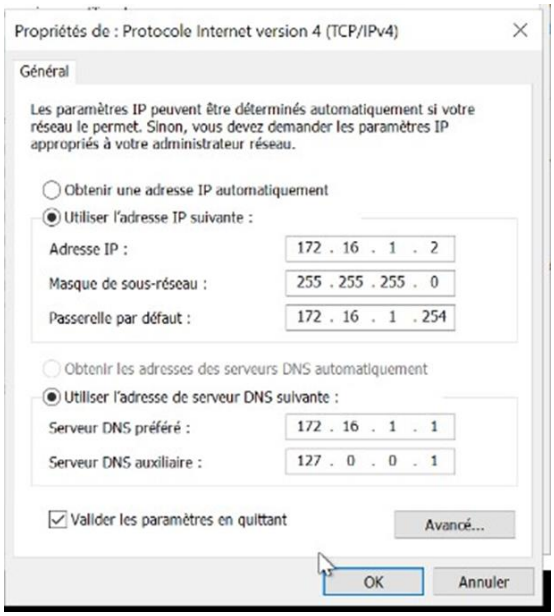
1. Création d'une machine virtuelle dédiée

Avant d'installer un second contrôleur de domaine, il est recommandé de le déployer sur une machine distincte. Pour commencer, il faut donc créer une nouvelle machine virtuelle (par exemple sur Proxmox) avec une image de Windows Server 2022.



2. Configuration réseau

Affectation d'une adresse IP fixe à la carte réseau de la VM. Il faut faire attention que le serveur secondaire est bien sur le même réseau que le serveur principal.

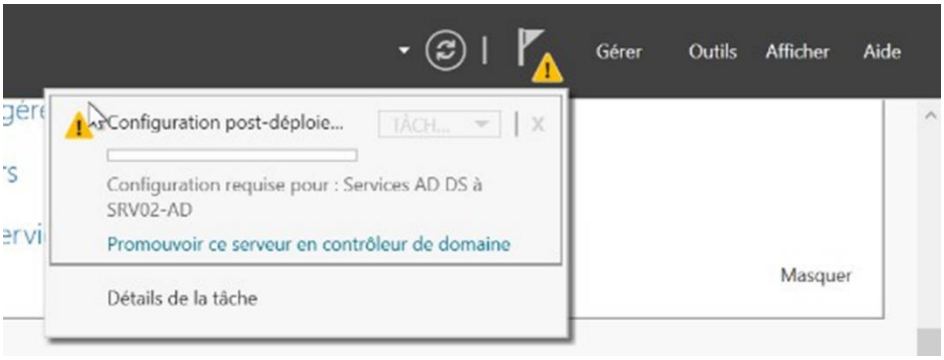


3. Ajout du rôle "Services de domaine Active Directory"

Sur le serveur fraîchement installé, il faut suivre les étapes suivantes :

- Ouvrir le Server Manager
- Cliquer sur "Ajouter des rôles et fonctionnalités"
- Sélectionner le rôle AD DS (Active Directory Domain Services)

Puis on assigne la fonction contrôleur de domaine au serveur secondaire



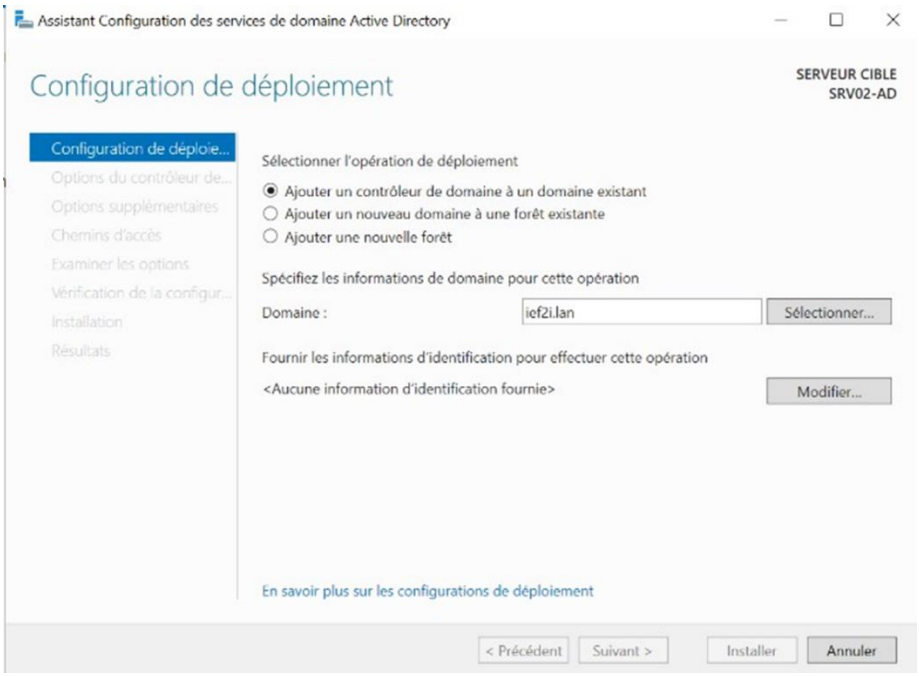
4. Promotion en tant que contrôleur de domaine

Une fois le rôle installé, il faut cliquer sur "Promouvoir ce serveur en contrôleur de domaine" et choisir l'option "Ajouter un contrôleur de domaine à un domaine existant".

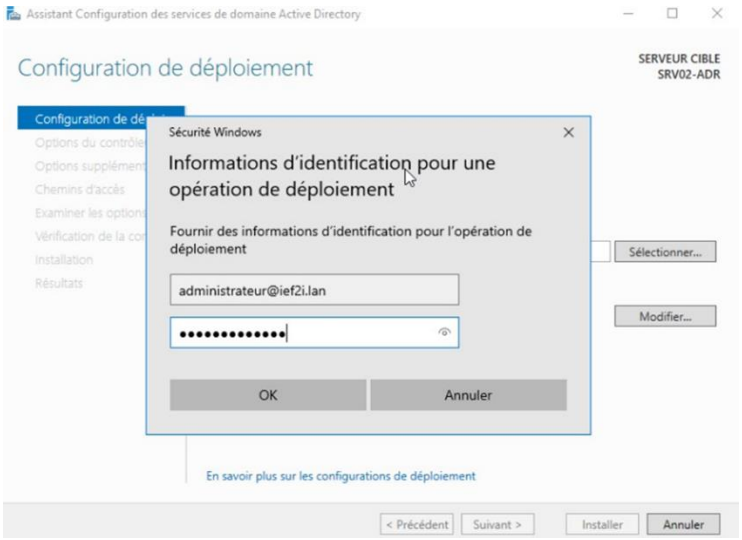
On peut donc enseigner :

- Le nom du domaine principal
- Le compte administrateur du domaine (avec les droits nécessaires)

1.



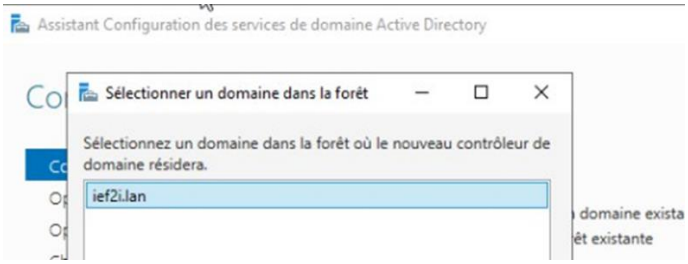
2.



- On renseigne le nom du domaine principal
- On renseigne le admin du domaine

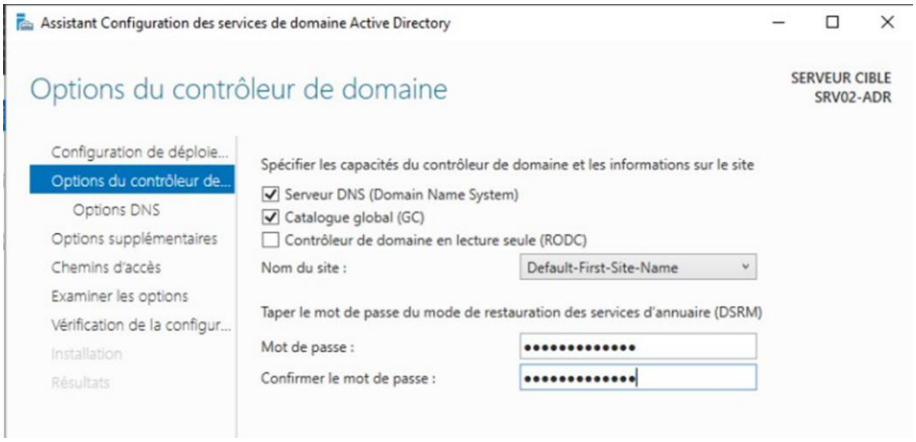
5. Sélection du domaine

L'assistant va détecter automatiquement le domaine existant, il faut donc le sélectionner dans la liste proposée pour poursuivre l'installation.



6. Configuration du mot de passe DSRM

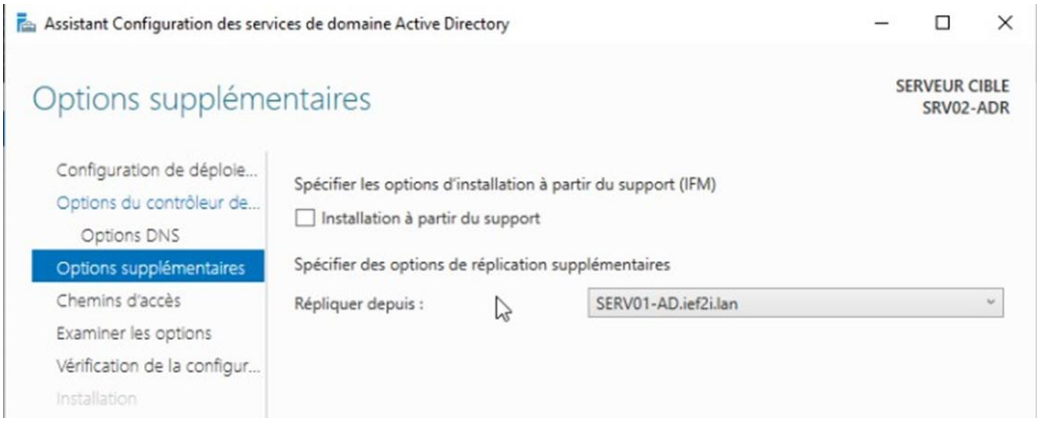
L'étape suivante est de définir un mot de passe pour le mode de restauration des services d'annuaire (DSRM). Ce mot de passe est utilisé en cas de récupération d'urgence de l'annuaire.



7. Lancer la réplication et finaliser l'installation

Une fois la configuration terminée, le serveur commencera la réplication depuis le contrôleur de domaine principal.

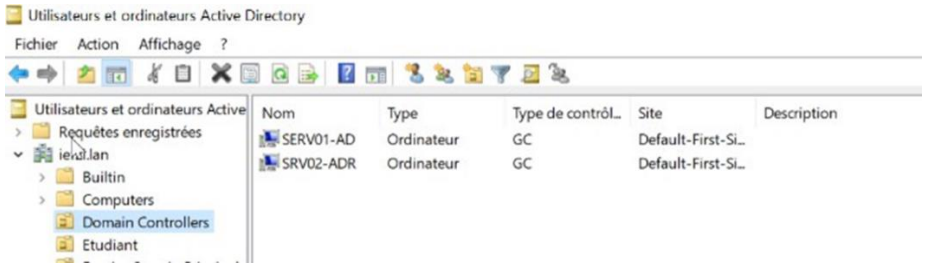
Ceci permet de synchroniser toutes les informations du domaine sur le second DC.



8. Vérification de l'ajout du contrôleur secondaire

Une fois le redémarrage effectué, il est nécessaire de vérifier que le contrôleur secondaire a bien été ajouté au domaine.

Il faut ensuite ouvrir la console "Utilisateurs et ordinateurs Active Directory" ou "Sites et services AD" pour confirmation.



Conclusion : Le contrôleur de domaine secondaire opérationnel est désormais crée, prêt à prendre le relais en cas de panne du serveur principal. Cela renforce la résilience et la haute disponibilité de votre infrastructure Active Directory.

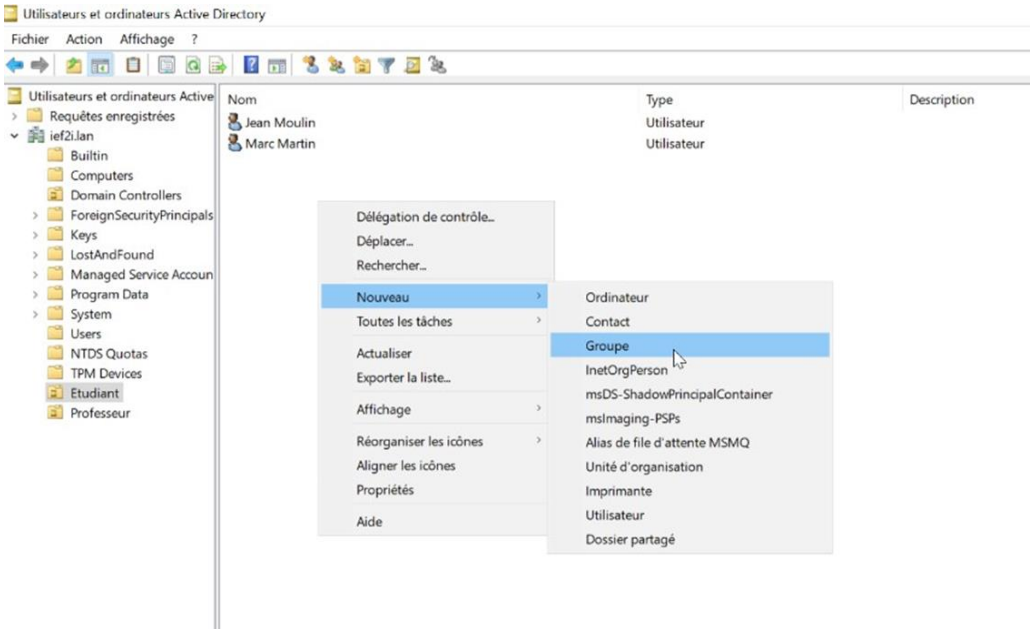
IX) Créer et gérer un groupe de sécurité

1. Création d'un groupe de sécurité dans Active Directory

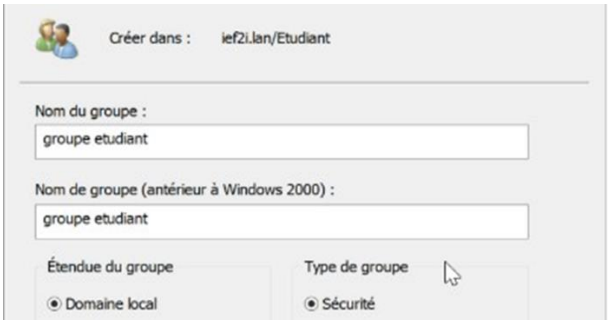
Depuis la console Utilisateurs et ordinateurs Active Directory, il faut :

- Naviguer vers l'OU souhaitée (par exemple : Étudiants ou Professeurs)
- Effectuer un clic droit > Nouveau > Groupe
- Donner un nom clair au groupe, puis sélectionner : Type : Sécurité et Étendue : Global

1.



2.



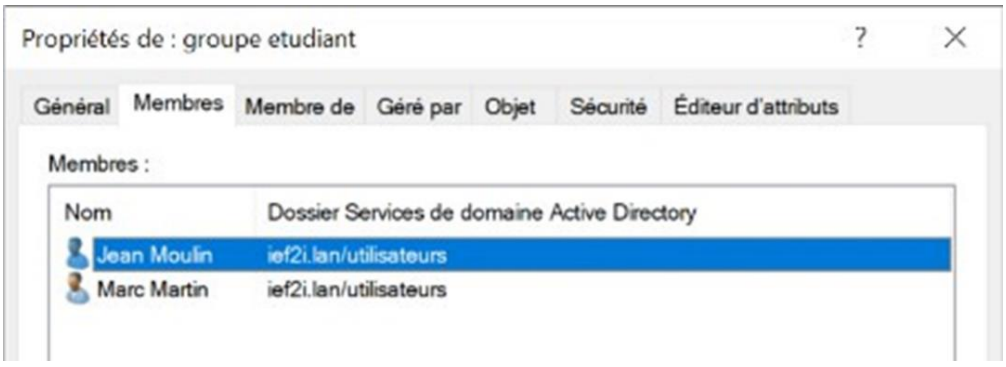
3.

2. Ajout des utilisateurs aux groupes créés

Une fois les groupes créés, il faut :

- Double-cliquer sur le groupe
- Aller dans l'onglet "Membres"
- Cliquer sur "Ajouter" et sélectionner les utilisateurs concernés

1.



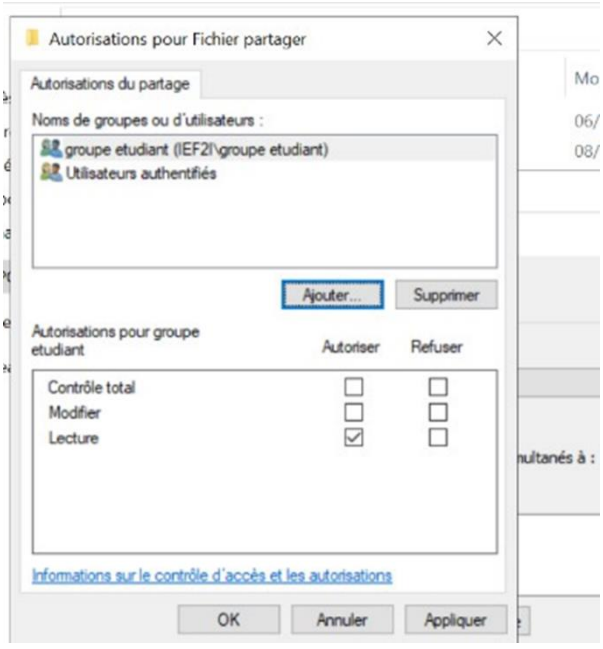
2.

3. Création d'un dossier partagé selon les groupes

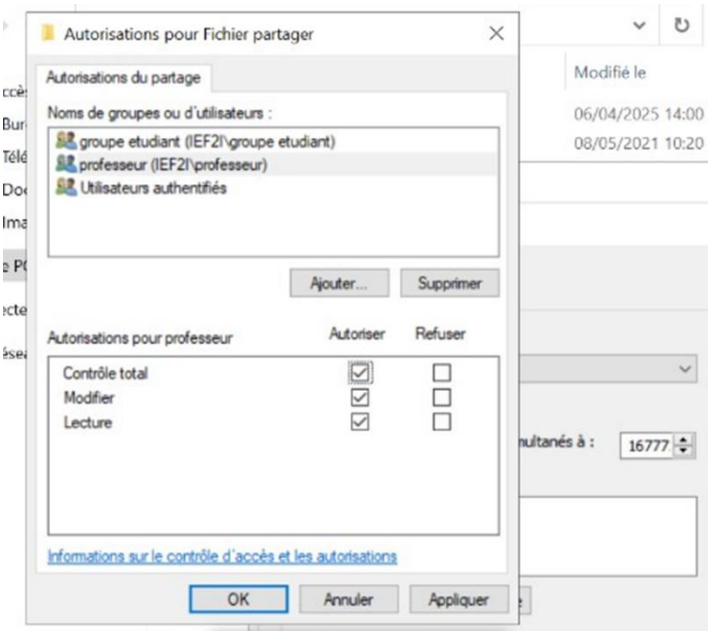
Sur un serveur de fichiers ou une machine dédiée, il faut ensuite créer un dossier partagé. Il faut alors :

- Cliquer droit > Propriétés
- Aller dans l'onglet Partage > Partage avancé
- Activer le partage et cliquez sur Autorisations
- Ajouter les groupes précédemment créés (Étudiants, Professeurs)

1.



2.

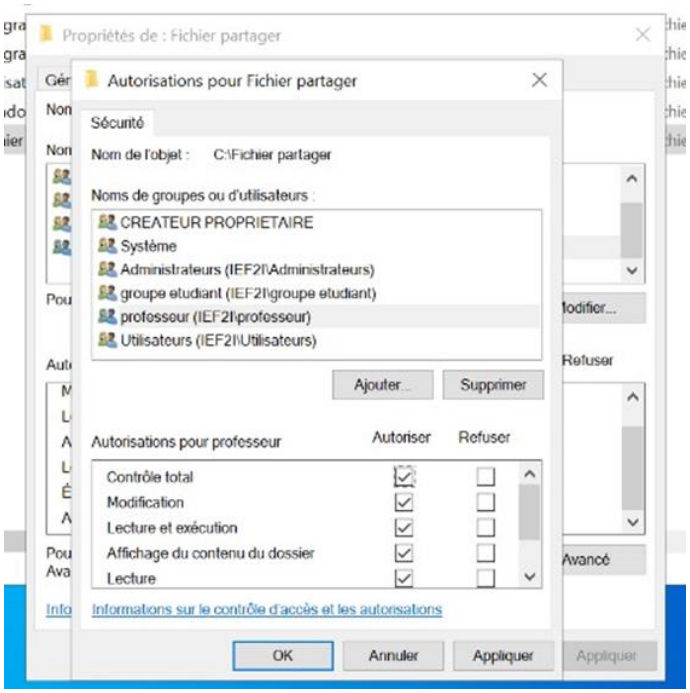


4. Configuration des autorisations de sécurité

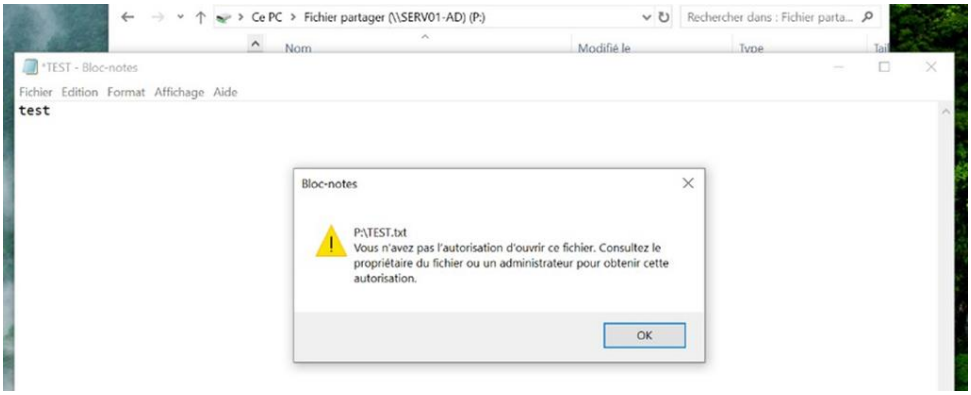
Dans l'onglet Sécurité du dossier, il faut :

- Retirer "Tout le monde" si nécessaire
- Ajouter les groupes un par un
- Donner les bons niveaux de droit : Lecture seule pour les étudiants et contrôle total pour les professeurs

1.



2.



Conclusion : Les groupes de sécurité permettent de gérer efficacement les droits d'accès aux dossiers partagés dans un environnement Active Directory. En associant des groupes à des ressources, il est facile de simplifier l'administration et d'éviter les erreurs de configuration individuelle.