Angel Velasco
Grégoire Marchal
Michael Adda
Maxime Sourdin
ING 4 CYB Gr02

TP1: DÉPLOIEMENT D'UN DOMAINE AD

Objectifs:

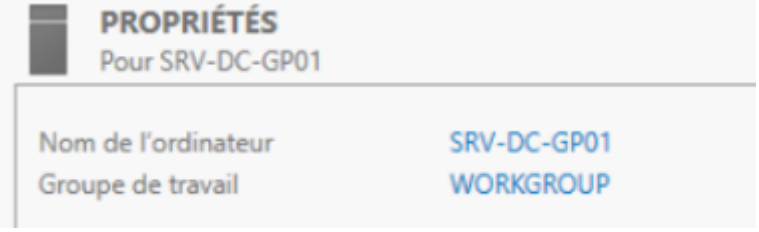
- Installer un contrôleur de domaine (AD DS + DNS) dans une nouvelle forêt
- Organiser l'annuaire : OU, utilisateurs, groupes, poste client
- Déployer des GPO de sécurité et de poste de travail
- Mettre en place un partage SMB avec droits NTFS et mapping par GPO
- Tester et valider le bon fonctionnement (DNS, authentification, journaux, gpresult)

Sommaire

Partie 1 - Installation du DC

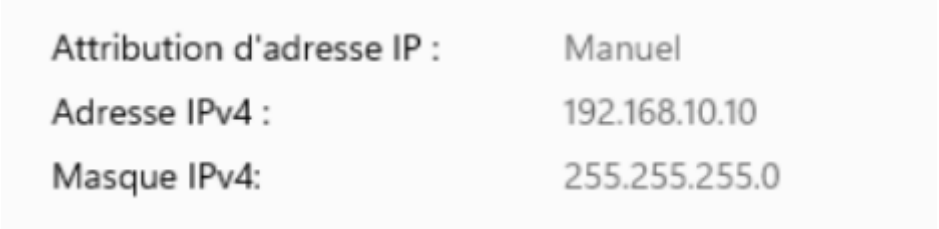
Le but de cette première partie est de montrer que l'installation du contrôleur de domaine s'est déroulée correctement et quelles options ont été choisies.

Pour ce faire, on a commencé par renommer le serveur avec le nom de notre groupe SRV-DC-GP01.



- **Figure** : Capture d'écran du bilan Serveur Local

Puis on a configuré une adresse IP statique et indiqué comme DNS l'adresse IP du Domain Controller.
On assigne d'abord une adresse privé IPv4:



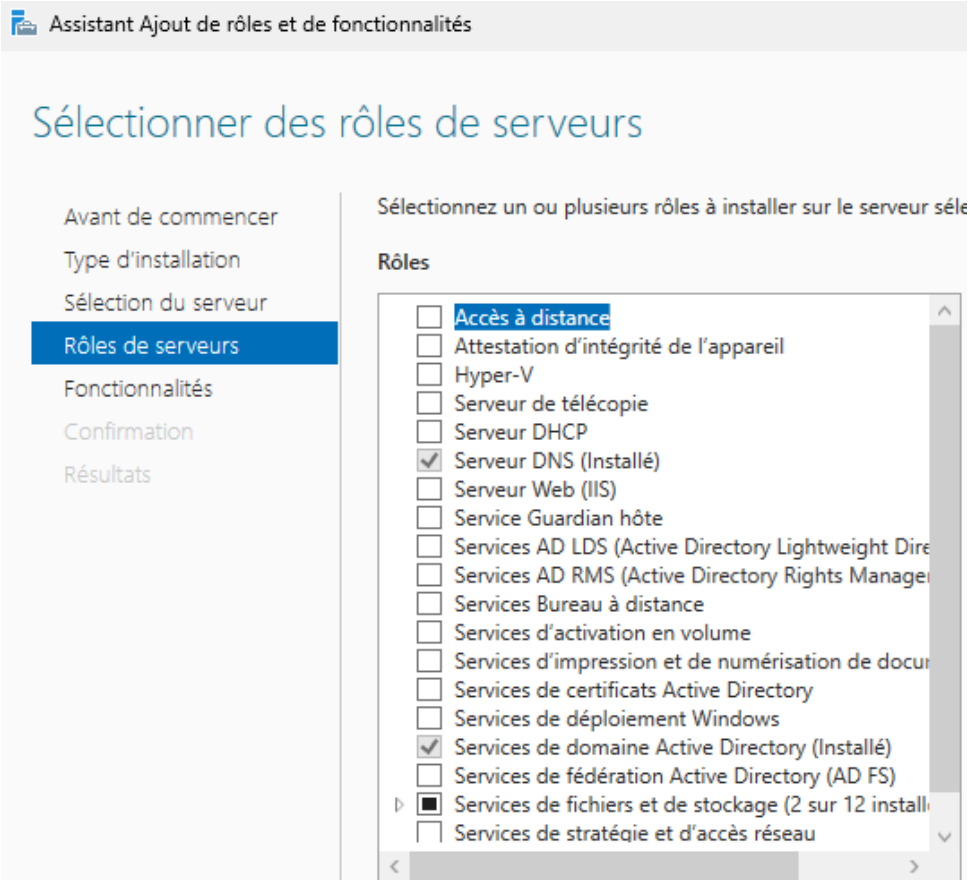
- **Figure** : Configuration de l'adresse IP

La zone DNS est l'espace de noms qui contient les enregistrements permettant de résoudre les noms d'hôtes en adresses IP et de localiser des services pour un domaine.
Dans l'Active Directory, la zone de recherche directe du domaine porte le nom du domaine DNS, dans notre cas gp01.lab.ece.

Le DNS fournit donc la résolution de noms qui permet aux clients et serveurs de localiser les services Active Directory. Sans DNS, les ordinateurs ne peuvent pas trouver les contrôleurs de domaine.

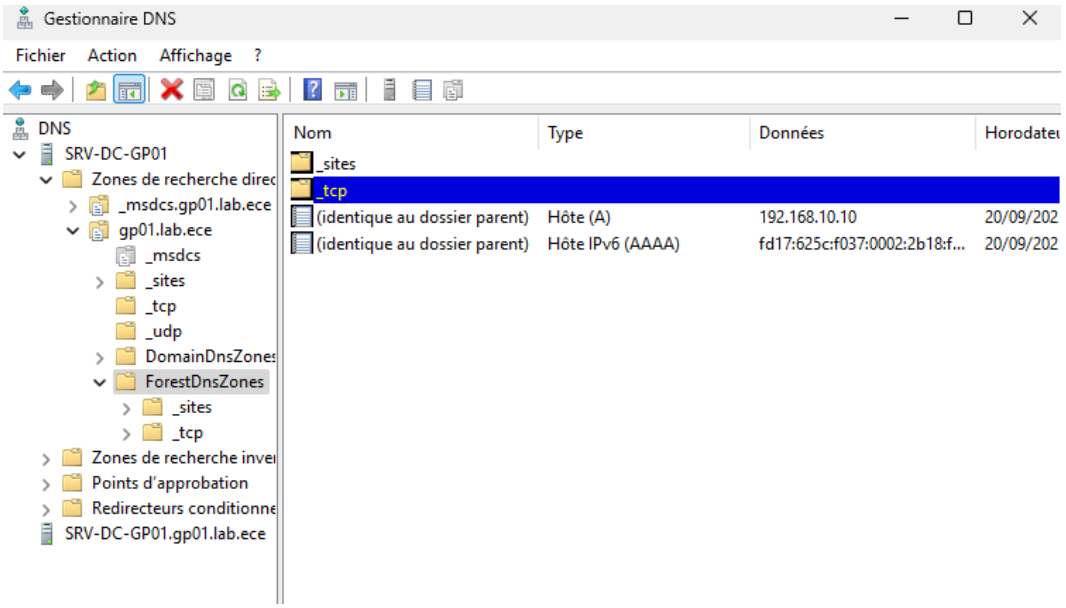
- **Figure** : Configuration du DNS

Voici les configurations apportées pour le choix des Rôles de serveurs en sélectionnant le Service de domaine Active Directrory.



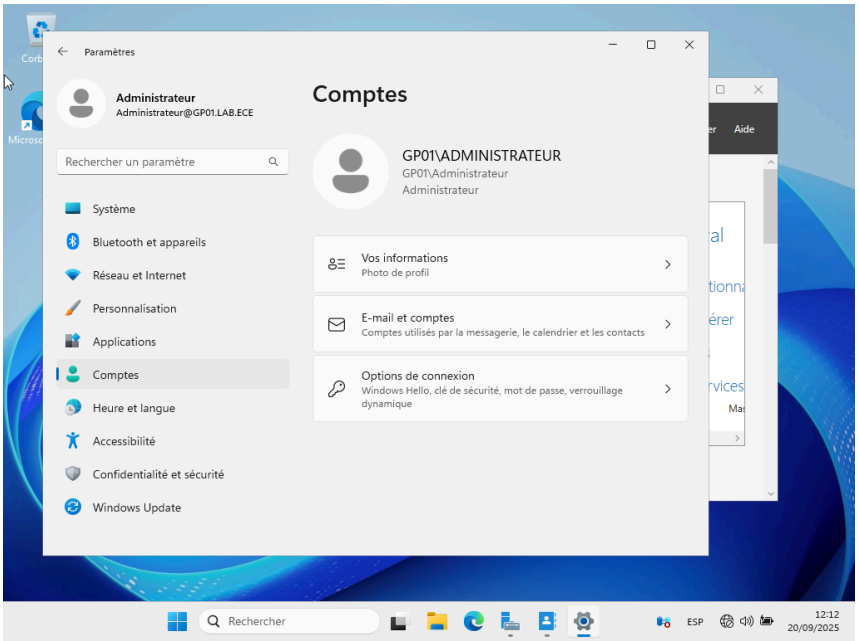
- **Figure** : Configuration de l'ajout de rôle

La console DNS (Gestionnaire de serveur et DNS) affiche la zone de recherche directe gp01.lab.ece et, dans son dossier ForestDnsZones, deux enregistrements de type A et AAAA nommés _tcp pointant respectivement vers 192.168.10.10 et son adresse IPv6.



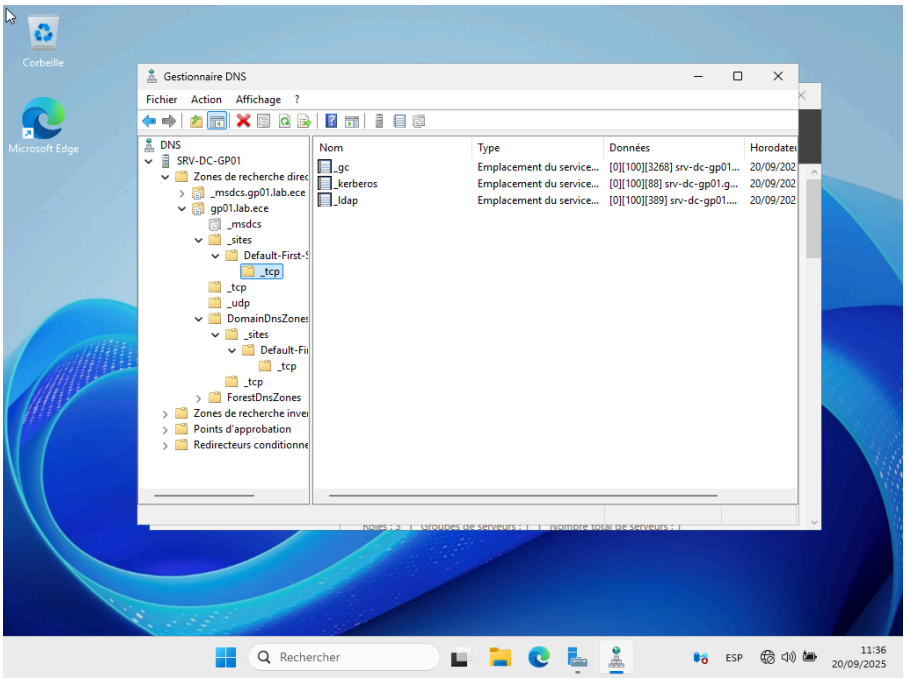
- **Figure** : Affichage Gestionnaire DNS

Nous avons ensuite redémarré la machine et nous nous sommes connectés avec le compte Administrateur@gp01.lab.ece.



- **Figure** : Connexion en tant qu'administrateur

Voici la vérification de la zone DNS gp01.lab.ece et les enregistrements SRV (_ldap , _kerberos).

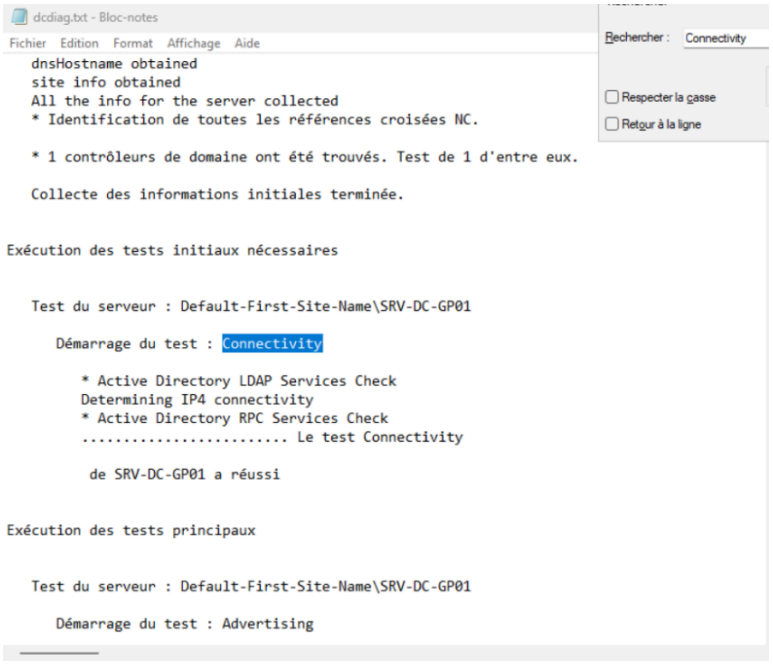


- **Figure** : Enregistrements SRV

Nous avons utilisé DCDiag afin de vérifier l'état et le bon fonctionnement du contrôleur de domaine.

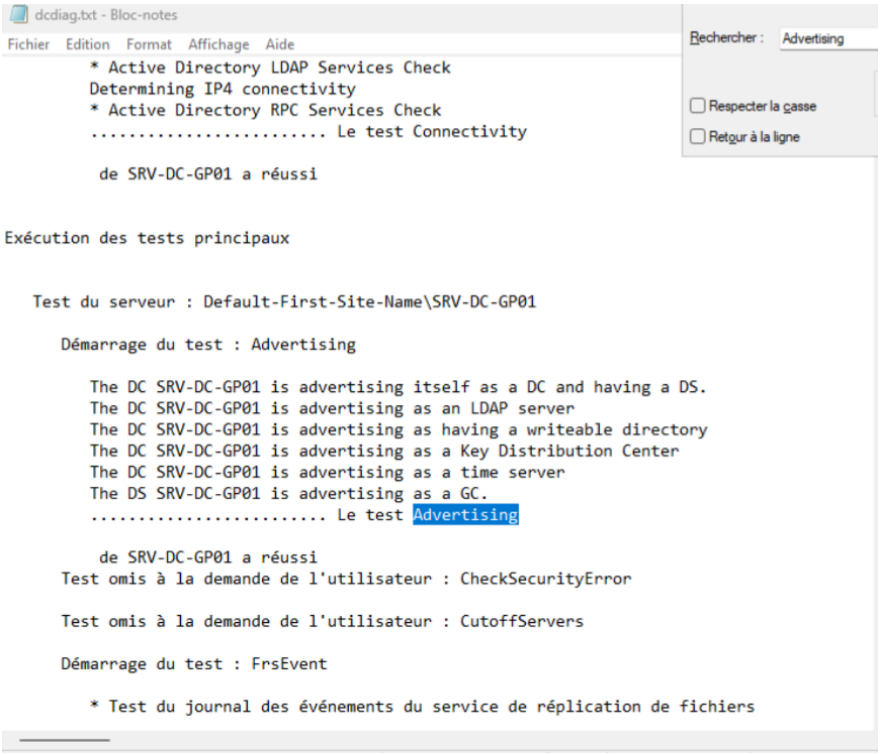
Tout d'abord, le test Connectivity a confirmé que le serveur était joignable et que les protocoles essentiels d'Active Directory répondaient correctement, en validant notamment la résolution d'adresses, la connectivité réseau et la disponibilité des services d'annuaire nécessaires aux clients et aux autres DC.

Voici une capture du résultat de la partie Connectivitée :



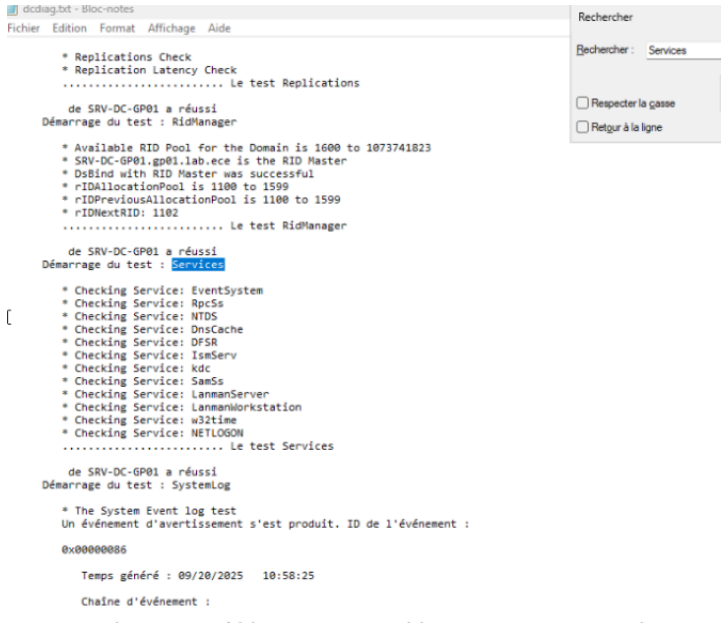
- **Figure** : Résultats de la partie Connectivity

Le test *Advertising* a ensuite permis de vérifier que le contrôleur de domaine s'annonçait correctement comme fournisseur de services Active Directory, afin que les clients puissent le découvrir via DNS. Voici une capture du résultat de la partie Advertising :



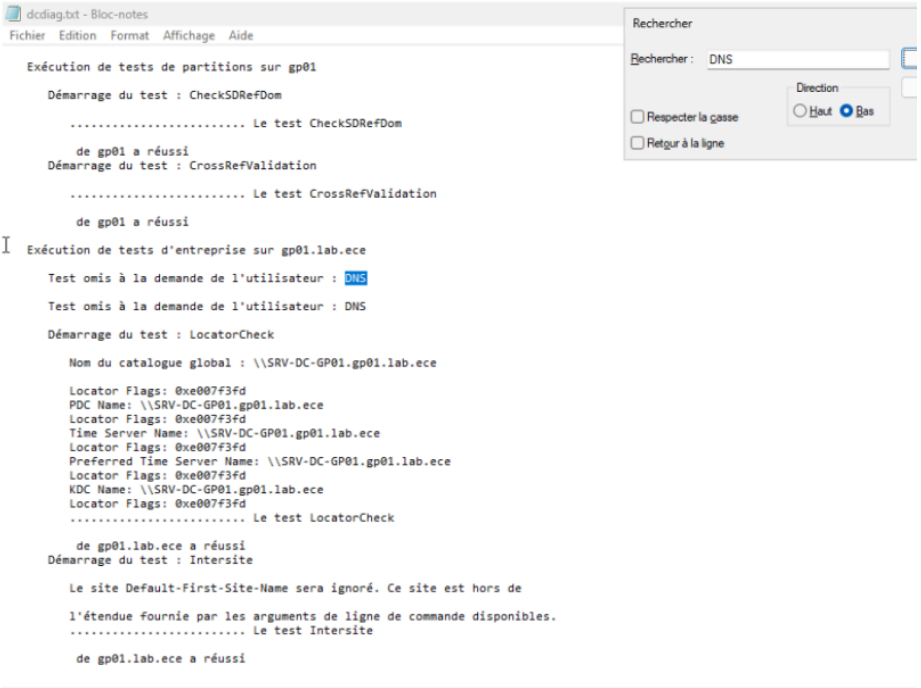
- **Figure** : Résultats de la partie Advertising

Le test *Services* a confirmé que les processus critiques, tels que Netlogon et Kerberos, étaient bien démarrés et opérationnels, garantissant ainsi l'authentification et la réplication. Voici une capture du résultat de la partie Services :



- **Figure** : Résultats de la partie Advertising

Enfin, le test *DNS* a contrôlé l'existence et l'exactitude des zones ainsi que des enregistrements indispensables (A/AAAA, SRV) pour la découverte et la résolution des noms Active Directory. Voici une capture du résultat de la partie DNS :



- **Figure** : Résultats de la partie DNS

Pour conclure, dans la première partie de ce TP, nous avons installé et configuré un serveur Windows nommé SRV-DC-GP01 en tant que contrôleur de domaine.
Nous avons attribué une adresse IP statique, installé les rôles AD DS et DNS. À L'aide de l'outil dcdiag, nous avons vérifié l'état du serveur en s'appuyant sur quatre parties Connectivity Advertising service et DNS. Les tests ont montré que les sévices sont actifs et que les enregistrements DNS sont présents.

Questions :

1. **Pourquoi gpXX.lab.ece est-il préférable à .local ?**

.local est réservé aux résolutions DNS Multicast, ce qui peut créer des conflits avec les systèmes Windows. En utilisant un domaine comme gp01.lab.ece, on respecte les standards DNS, on évite les erreurs de résolution et on peut intégrer plus facilement des services externes.

2. **À quoi servent les enregistrements SRV _ldap._tcp et _kerberos._tcp ?**

Ces enregistrements sont essentiels pour qu'un client puisse localiser les services Active Directory. Le _ldap._tcp permet de trouver les serveurs LDAP pour interroger l'annuaire, et le _kerberos._tcp sert à localiser les serveurs Kerberos pour l'authentification. Sans eux, les connexions ne fonctionnent pas correctement.

3. **Que vérifier en priorité si dcdiag remonte une erreur DNS ?**

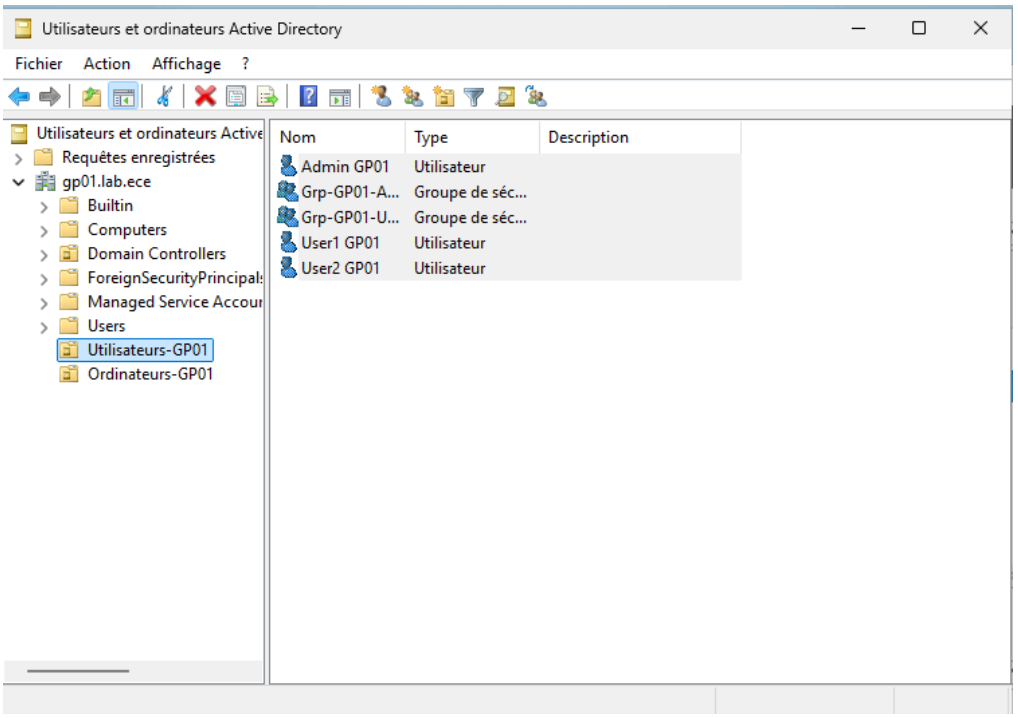
La première chose qu'on vérifie, c'est que le contrôleur de domaine pointe bien vers lui-même en DNS dans sa configuration réseau. Ensuite, on regarde si la zone DNS du domaine existe, si les enregistrements SRV sont présents, et si les cibles des SRV ont bien un enregistrement A.

4. **Quel est l'intérêt de configurer des redirecteurs DNS (forwarders)?**

Les redirecteurs DNS permettent au serveur DNS interne de transmettre les requêtes qu'il ne peut pas résoudre (comme les sites web externes) vers des serveurs DNS publics (exemple 8.8.8.8). Ça évite de faire sortir chaque client directement sur Internet, ça accélère les résolutions, et ça centralise la gestion DNS dans l'entreprise.

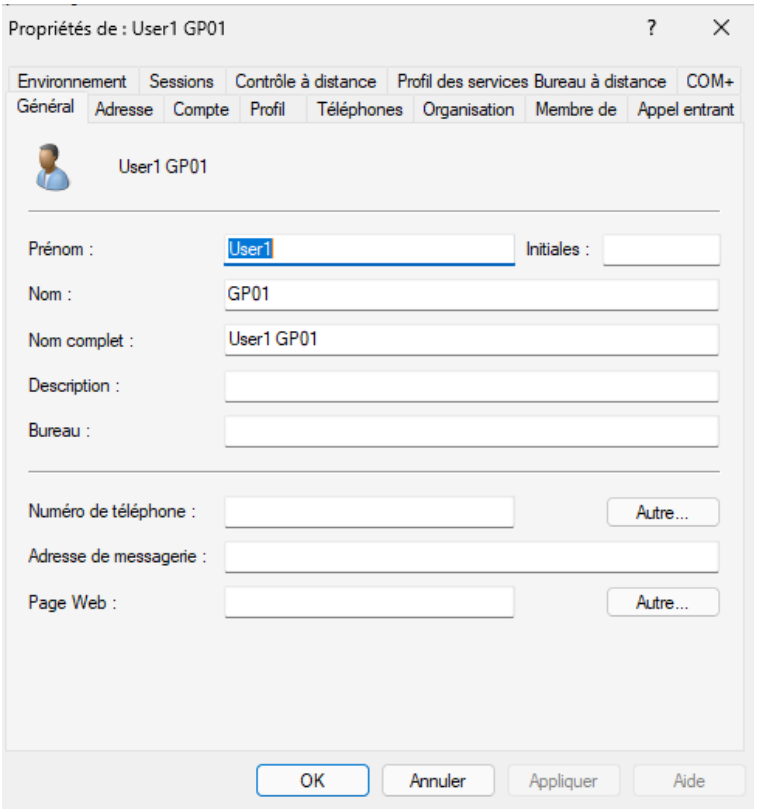
Partie 2 - Organisation de l’annuaire

Dans cette partie, l’objectif est de mettre en place une structure d’unités d’organisation (OU) adaptée, puis de créer et configurer des utilisateurs ainsi que des groupes de sécurité afin de préparer la gestion des droits et des stratégies de groupe.



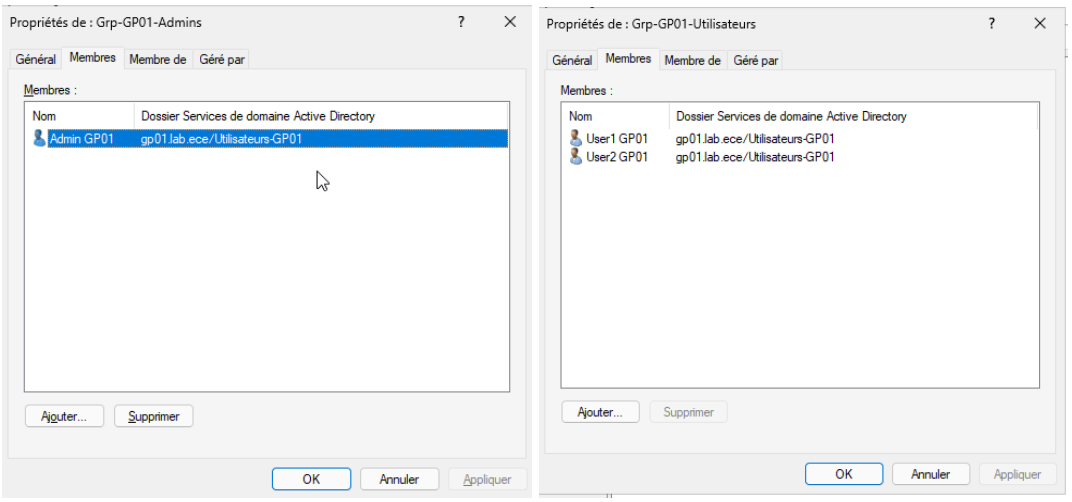
- **Figure :** Structure des OU

Comme on peut l’observer sur la figure de structure des OU, nous avons organisé le domaine en créant 2 unités d’organisation, Ordinateurs-GP01 et Utilisateurs-GP01. Cette hiérarchie permet de séparer clairement les objets selon leur rôle et de faciliter l’application ciblée des GPO.



- **Figure :** Propriétés de l'utilisateur "User1 GP01"

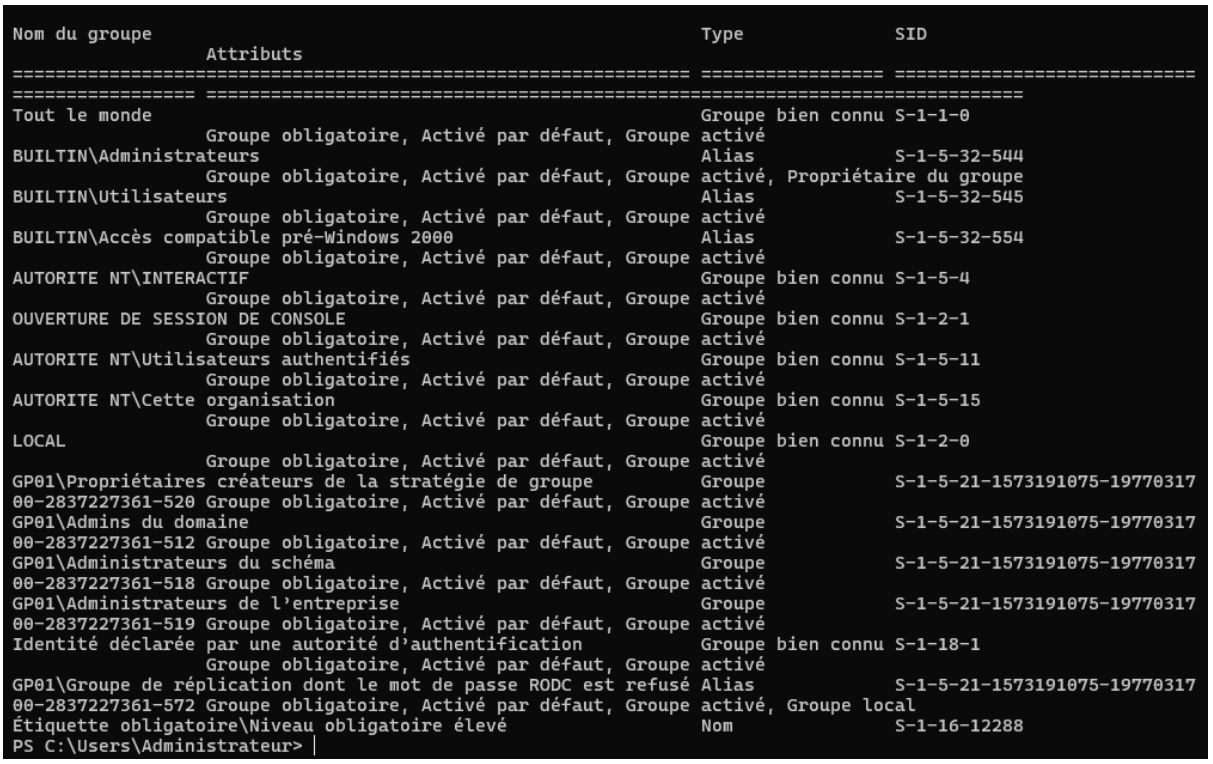
Ensuite, nous avons créé plusieurs comptes utilisateurs, dont User1 GP01 et User2 GP01. La figure ci-dessus illustre la configuration de base d'un compte utilisateur, comprenant le prénom, le nom, le nom complet et les informations associées. Cette étape est essentielle pour disposer d'identités distinctes sur lesquelles appliquer des stratégies et des droits spécifiques.



- **Figure :** Membres des groupes Grp-GP01-Admins et Grp-GP01-Utilisateurs

Nous avons également mis en place deux groupes de sécurité, Grp-GP01-Admins et Grp-GP01-Utilisateurs. Comme montré dans la figure, le premier regroupe les

administrateurs du domaine, tandis que le second rassemble les utilisateurs standards. Cette séparation permet de gérer plus efficacement les permissions et de limiter les droits selon les rôles.



- **Figure :** Vérification de l'appartenance aux groupes via whoami /groups

Enfin, nous avons vérifié l'appartenance des comptes aux groupes à l'aide de la commande whoami /groups. La figure confirme que les utilisateurs héritent bien des droits associés à leurs groupes respectifs. Cette étape de validation est indispensable pour s'assurer que la configuration est correcte avant de déployer des stratégies ou des restrictions supplémentaires.

Questions :

1. **Pourquoi organiser les objets dans des OU avant de déployer des GPO ?**

Organiser les objets dans des unités d'organisation avant de déployer des stratégies de groupe est essentiel pour garantir une administration claire et efficace. Les OU permettent de regrouper logiquement les utilisateurs et les ordinateurs selon des critères précis. Cette organisation permet d'appliquer les GPO de manière ciblée uniquement aux objets concernés, évitant qu'une règle trop générale ne s'applique à tout le domaine. Cette hiérarchisation améliore la lisibilité de l'annuaire et facilite la maintenance à long terme, car chaque OU peut recevoir des stratégies adaptées à son rôle.

2. **Quel est l’intérêt d’utiliser des groupes plutôt que d’attribuer des droits aux utilisateurs directement ?**

L’utilisation de groupes pour attribuer des droits est pratique, puisqu’ils permettent de simplifier l’administration, car au lieu de gérer les permissions utilisateur par utilisateur, ce qui est chronophage et source d’erreurs, on attribue les droits une seule fois au groupe. Tous les membres héritent automatiquement de ces droits, ce qui rend la gestion plus cohérente et évolutive. Lorsqu’un nouvel utilisateur rejoint l’organisation, il suffit de l’ajouter au groupe approprié pour qu’il bénéficie immédiatement des mêmes accès que ses collègues. Cette approche renforce également la sécurité, car elle évite les oublis et permet un contrôle centralisé des autorisations.

3. **Proposez une organisation OU adaptée à une entreprise ayant 2 sites (Paris, Lyon) et 3 services (RH, IT, Finance)**.

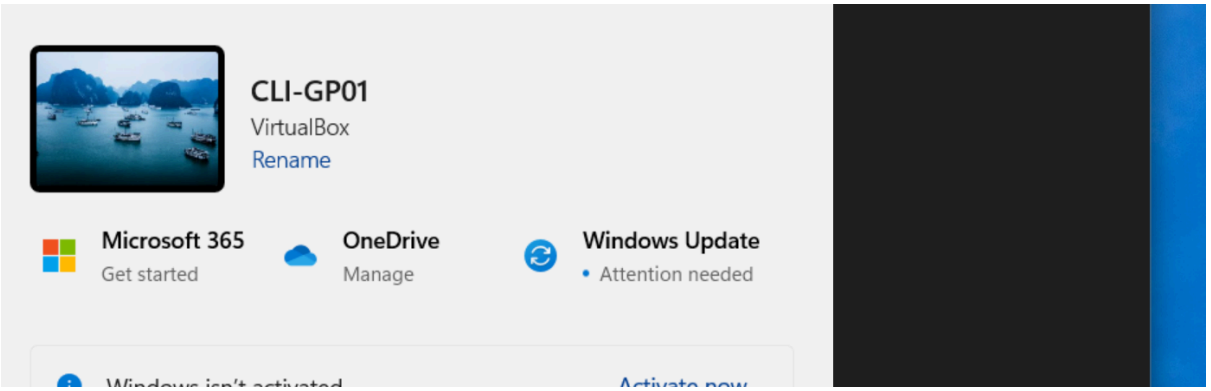
Pour une entreprise répartie sur deux sites, Paris et Lyon, et comprenant trois services (RH, IT et Finance), on pourrait créer une OU principale par site, puis à l’intérieur de chacune, trois sous-OU correspondant aux services. Par exemple : Paris → RH, IT, Finance et Lyon → RH, IT, Finance. Cette organisation rend possible l’application de GPO spécifiques à un site (par exemple des règles réseau propres à Paris) ou à un service (par exemple des restrictions logicielles pour le service Finance).

4. **Quels risques si tous les objets sont laissés à la racine du domaine ?**

Laisser tous les objets à la racine du domaine entraîne plusieurs risques. D’abord, cela nuit à la lisibilité de l’annuaire, car il devient rapidement difficile de distinguer les utilisateurs, ordinateurs et groupes dans une longue liste non structurée. Ensuite, cela complique l’application des GPO, car les stratégies appliquées à la racine affectent indistinctement tous les objets, sans possibilité de cibler des populations spécifiques. Enfin, cela fragilise la sécurité et la gestion des droits, car il n’existe plus de séparation claire entre les différents rôles ou services. En cas de mauvaise configuration, une règle pourrait impacter l’ensemble du domaine, ce qui est dangereux dans un environnement de production.

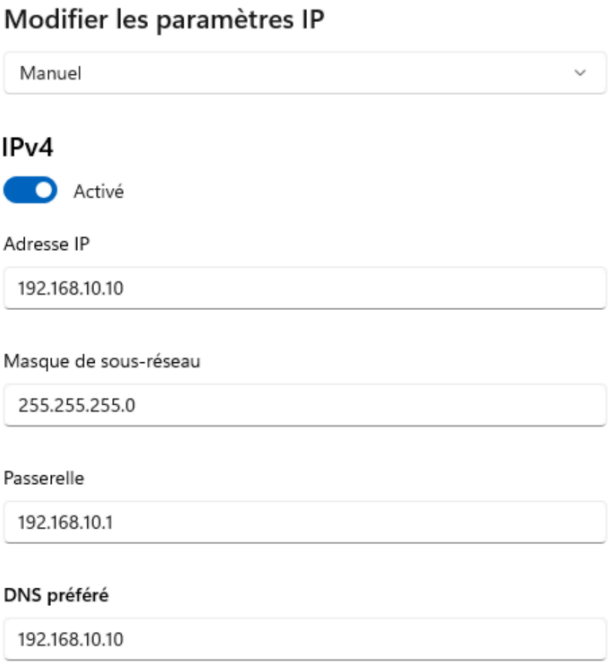
Partie 3 - Intégration du poste client (Michael)

Dans cette partie, il faut lancer la deuxième machine virtuelle qui est une Windows 11. Il faut alors modifier le nom en CLI-GP01 comme ci-dessous:



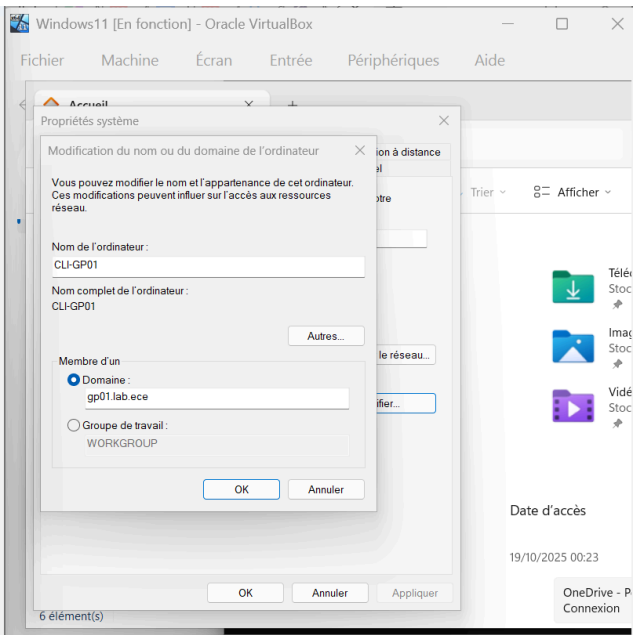
- **Figure :** Nouveau nom du poste client

Il faut également modifier l'adresse DNS. La nouvelle adresse à inscrire est l'adresse IP du DC, dans notre cas c'est 192.168.10.10. Il est également possible de mettre une passerelle dans le cas où nous voudrions utiliser internet.



- **Figure :** Changement de l'adresse DNS préférée

Comme nous pouvons le voir sur cette capture d'écran, c'est grâce au DNS que nous allons pouvoir connecter le client au serveur.



- **Figure :** Connexion du client au domaine

Afin de connecter le client au domaine, il faut accéder aux propriétés système et modifier le paramètre de domaine pour y inscrire gp01.lab.ece.

Dans ce TP, nous n'avons pas réussi à connecter un client au domaine, même si les étapes précédentes ont été réalisées correctement et que la configuration réseau des VM était identique.

Normalement, une fois le poste intégré au domaine, nous aurions dû nous connecter à la fois avec un compte utilisateur et avec le compte administrateur, afin de comparer les droits d'accès. En effet, le compte administrateur dispose de nombreuses fonctionnalités supplémentaires qui ne sont pas accessibles aux utilisateurs standards.

Nous aurions également dû vérifier les stratégies appliquées grâce à la commande gpresult /R, ainsi que consulter l'Observateur d'événements dans Journaux Windows > Sécurité. Cet outil permet d'analyser les événements liés à l'authentification, de tracer les connexions réussies ou échouées, et de repérer d'éventuelles tentatives d'intrusion ou des erreurs de mot de passe.

Questions :

1. **Pourquoi le client doit-il utiliser le DNS du DC avant de rejoindre le domaine ?**

Le client doit utiliser le DNS du DC car il est le seul qui contient les enregistrements (_ldap, _kerberos) nécessaires pour localiser le contrôleur de domaine. Sans ce DNS, le client ne peut pas trouver le domaine.

2. **Que se passe-t-il si vous configurez 8.8.8.8 comme DNS du client ?**

Dans le cas où nous configurons le DNS du client à 8.8.8.8, le client ne trouvera pas le domaine, il sera donc impossible de le rejoindre.

3. **Que prouvent les événements 4624 et 4625 dans les journaux de sécurité ?**

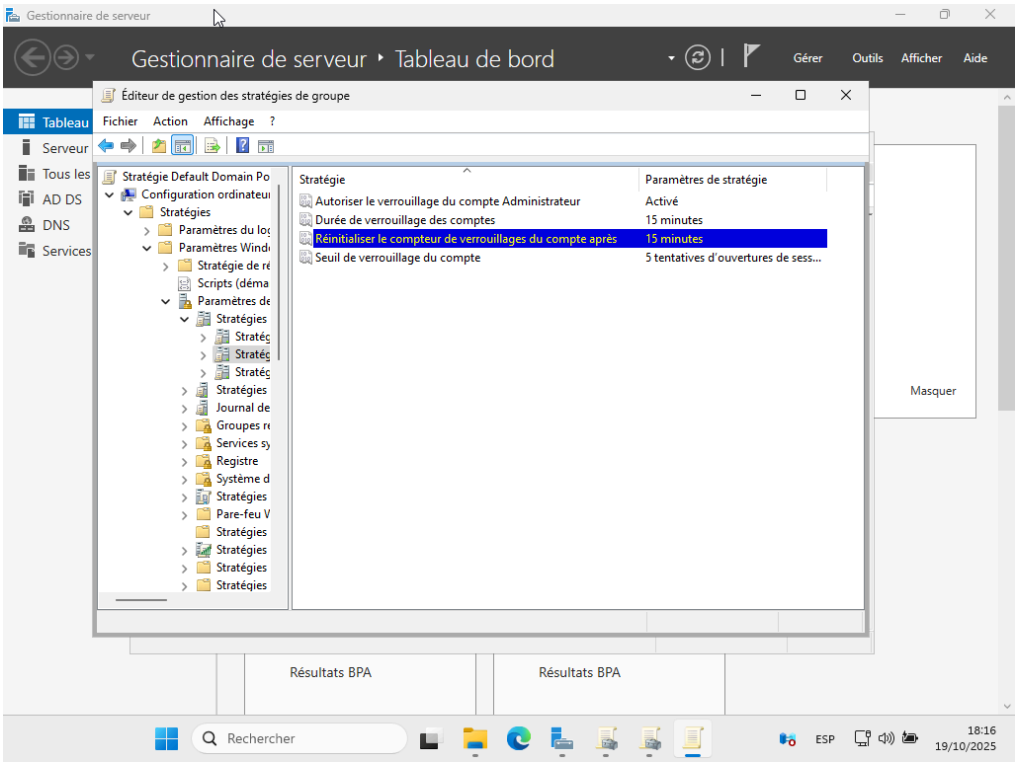
4624 signifie qu'une authentification est réussie, c'est-à-dire qu'un utilisateur a pu se connecter.
4625 signifie un échec, cela peut être dû à plusieurs raisons comme le mauvais mot de passe ou un refus d'accès.

4. **Quelles différences avez-vous constaté entre user1.gpXX et admin.gpXX ?**

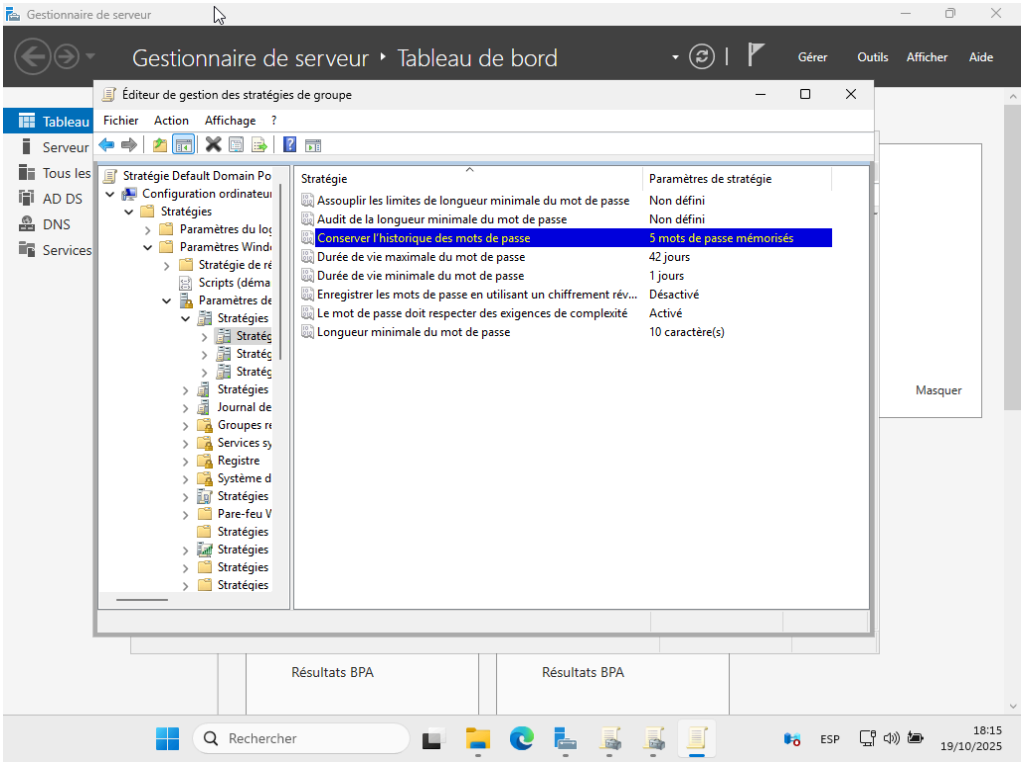
L'utilisateur user1 est un utilisateur standard qui n'a pas accès aux zones et outils administrateur.
L'utilisateur admin est par définition un administrateur qui a un accès complet à la gestion du domaine, des groupes et des utilisateurs.

Partie 4 - GPO

Dans cette partie, l'objectif est de mettre en place et de tester plusieurs GPO afin d'appliquer des règles de sécurité et des paramètres personnalisés aux utilisateurs et aux ordinateurs du domaine.



- **Figure :** Paramètre de verrouillage de compte avec une durée fixée à 15 minutes



- **Figure :** Paramètres de mot de passe et de verrouillage de compte

Comme on peut observer sur les figures au-dessus, la première étape consiste à modifier la “Default Domain Policy” pour renforcer la sécurité des mots de passe. Dans cette GPO, on a configuré une longueur minimale de 10 caractères, activé la complexité, imposé l’historique des 5 derniers mots de passe, et défini un verrouillage de compte après 5 tentatives échouées pendant 15 minutes. Ces paramètres permettent d’éviter les mots de passe faibles et les tentatives de connexion par force brute.

Ensuite, nous avons créé une nouvelle GPO nommée GPO-Securite-GP01 et l’avons appliquée à l’unité d’organisation Ordinateurs-GP01. Cette stratégie regroupe plusieurs paramètres destinés à renforcer la sécurité et à personnaliser les postes clients.
Nous avons configuré un message d’accueil personnalisé à la connexion, interdit l’accès au Panneau de configuration et défini un fond d’écran d’entreprise commun stocké dans un dossier partagé sur le contrôleur de domaine. La GPO a ensuite été paramétrée pour appliquer ce fond d’écran à tous les postes clients via un chemin réseau. Enfin, nous avons bloqué l’exécution des fichiers .exe dans le dossier Téléchargements en utilisant les SRP, plus simples à mettre en place et compatibles avec la plupart des éditions de Windows.

Comme nous avons rencontré un problème pour joindre le domaine gp01.lab.ece avec la VM client, nous n’avons pas pu tester le bon fonctionnement des paramètres sur le poste client.

Questions :

1. **Pourquoi faut-il tester une GPO avant un déploiement global ?**

Il faut tester une GPO avant de la déployer sur l'ensemble du domaine, car une mauvaise configuration peut avoir des effets négatifs sur tous les utilisateurs et ordinateurs. Par exemple, une GPO mal paramétrée peut bloquer l'accès à des outils essentiels ou modifier des paramètres réseau cruciaux. En testant d'abord sur une OU de test ou sur un poste isolé, on s'assure que les paramètres appliqués ont bien l'effet souhaité.

2. **Quelles sont les différences majeures entre SRP et AppLocker ? Quel choix avez-vous fait ici ?**

Les SRP (Software Restriction Policies) sont une ancienne méthode pour contrôler les programmes autorisés à s'exécuter. Ils sont simples mais moins flexibles. Alors que AppLocker, permet un contrôle plus précis selon l'éditeur, le chemin ou le hachage du fichier.
Dans ce TP, on a choisi SRP, car il est compatible avec toutes les éditions de Windows et plus rapide à mettre en place.

3. **Où serait-il préférable de stocker le fond d'écran pour plus de robustesse et pourquoi ?**

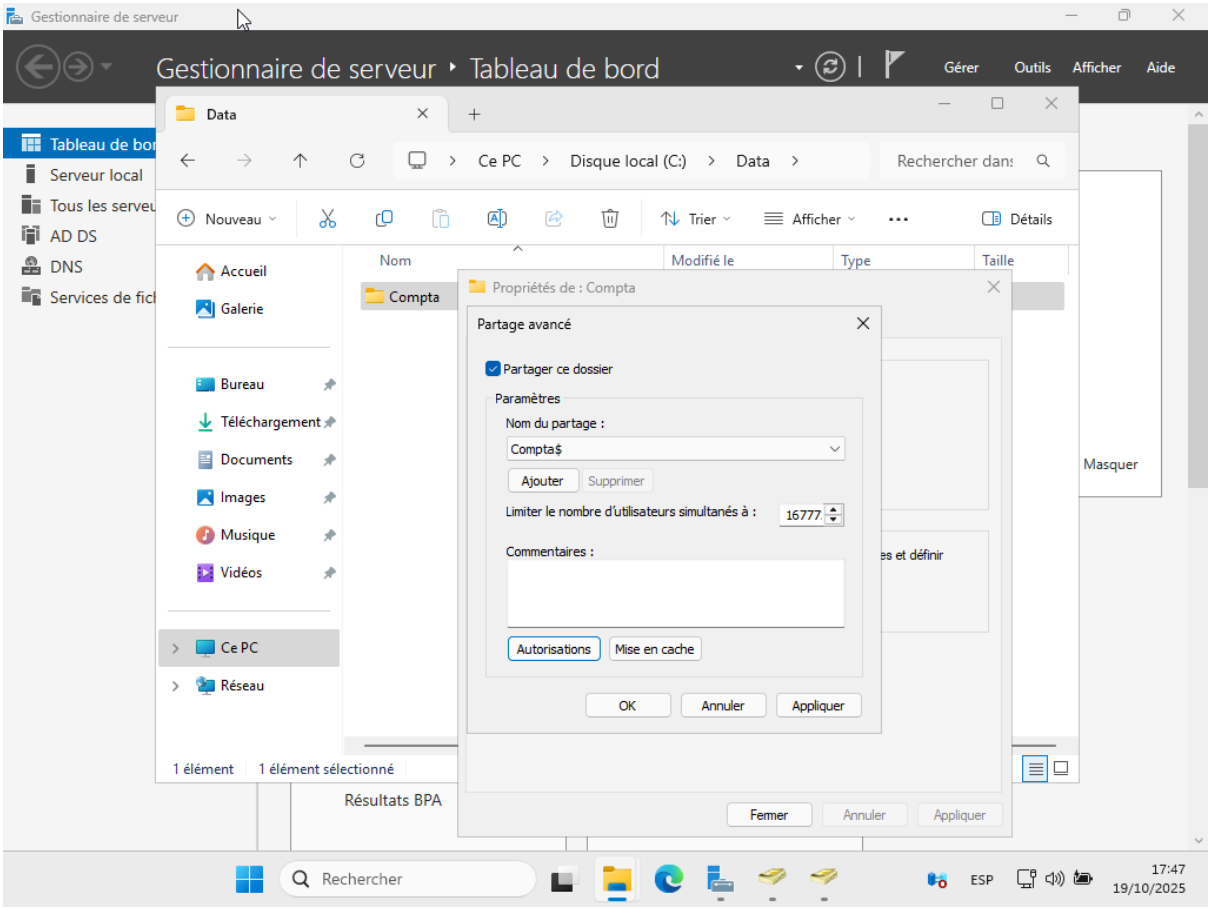
Le fond d'écran devrait être stocké dans un dossier partagé et accessible en lecture seule à tous les utilisateurs. Ce type de partage est plus robuste car il est répliqué automatiquement entre les contrôleurs de domaine, contrairement à un simple dossier sur le disque local du DC. Cela garantit que le fond d'écran reste disponible même en cas de panne du serveur principal.

4. **Donnez un exemple de mauvaise GPO et ses conséquences possibles.**

Par exemple, une GPO qui désactive l'accès à l'invite de commande ou au Panneau de configuration pour tous les utilisateurs, y compris les administrateurs. Cela empêcherait toute maintenance ou modification de configuration. Une autre erreur serait de forcer un proxy ou un script de logon erroné, ce qui bloquerait toutes les connexions réseau.

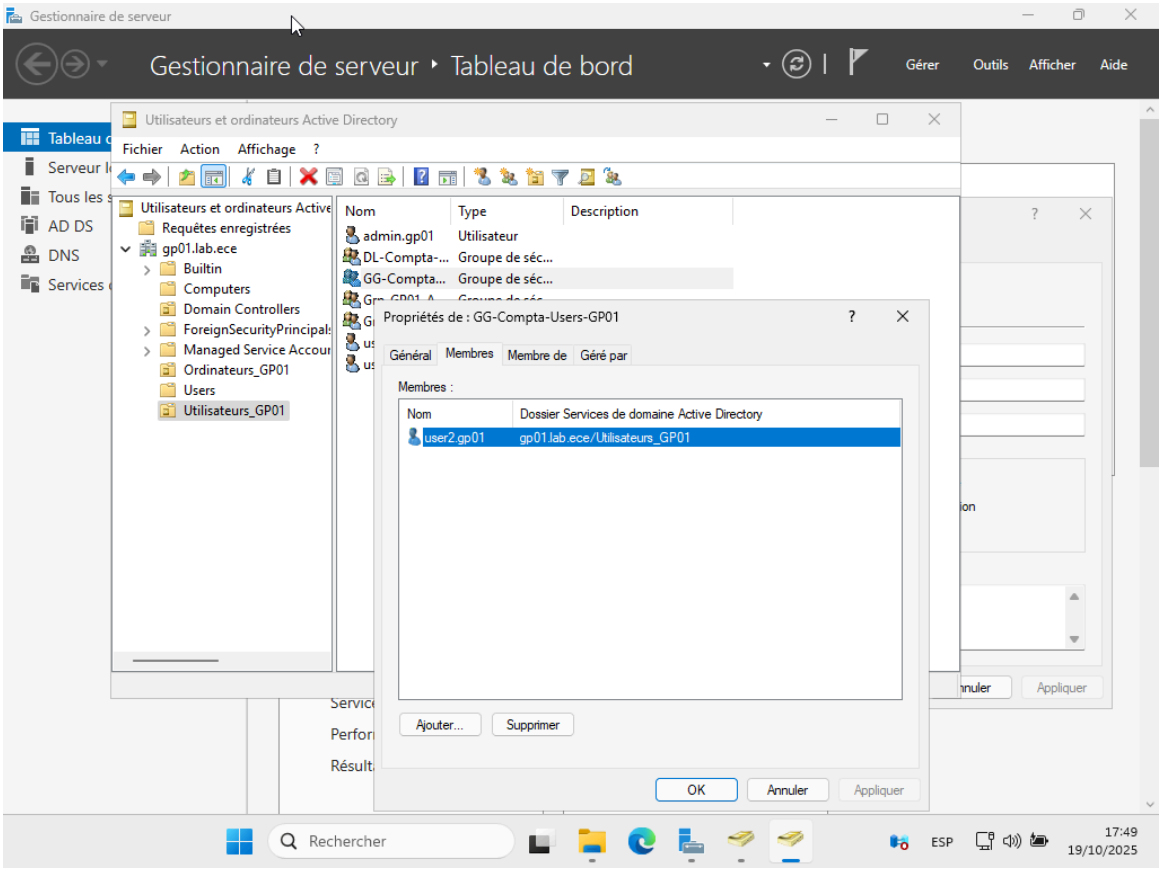
Partie 5 - Partage SMB et droits NTFS

La dernière partie du TP porte sur la gestion des partages réseau et l'application des droits NTFS dans un domaine Active Directory.
L'objectif est de créer un dossier partagé de manière sécurisée, avec des droits adaptés à chaque groupe d'utilisateurs, en respectant le modèle AGDLP.

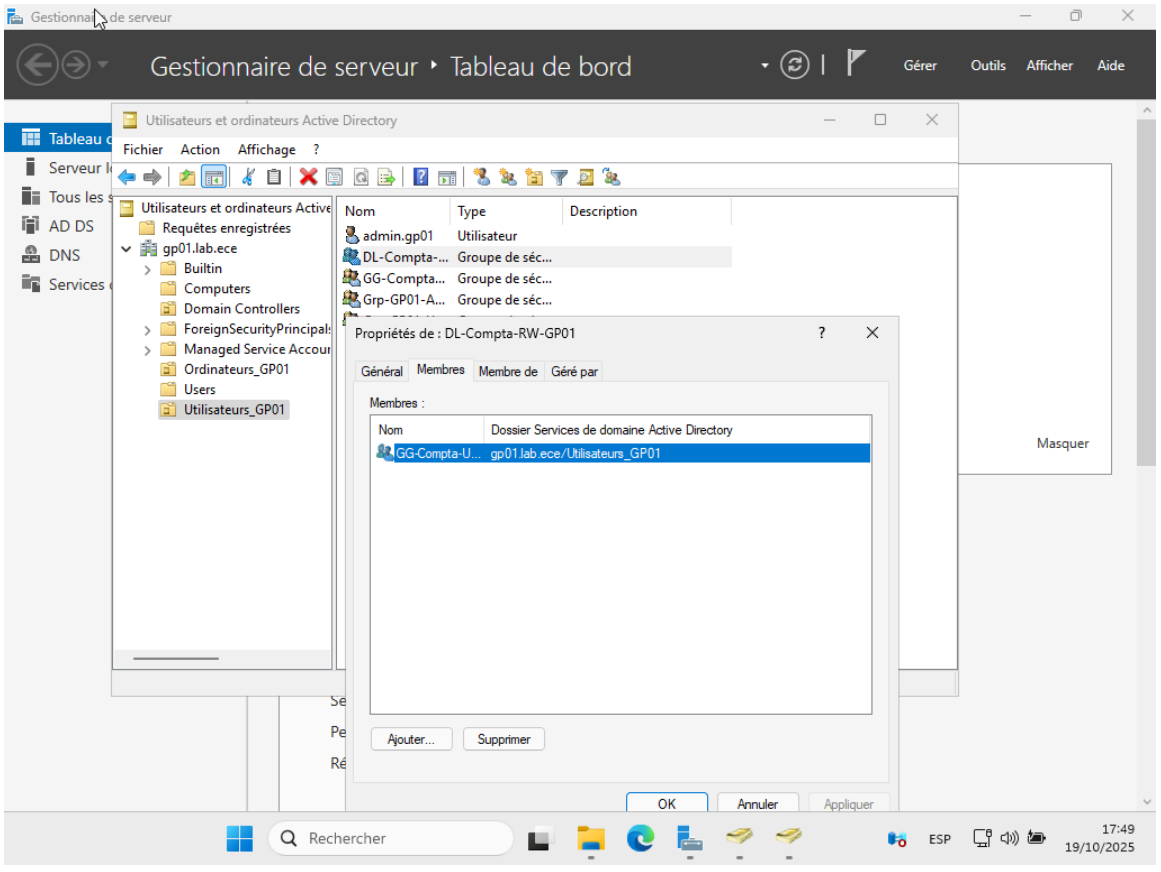


- **Figure :** Création et partage du dossier C:\Data\Compta en Compta$ sur le DC

Comme on peut le voir sur la figure ci-dessus, on a d'abord créé le dossier C:\Data\Compta sur le contrôleur de domaine, puis après on la partagé sous le nom Compta$.

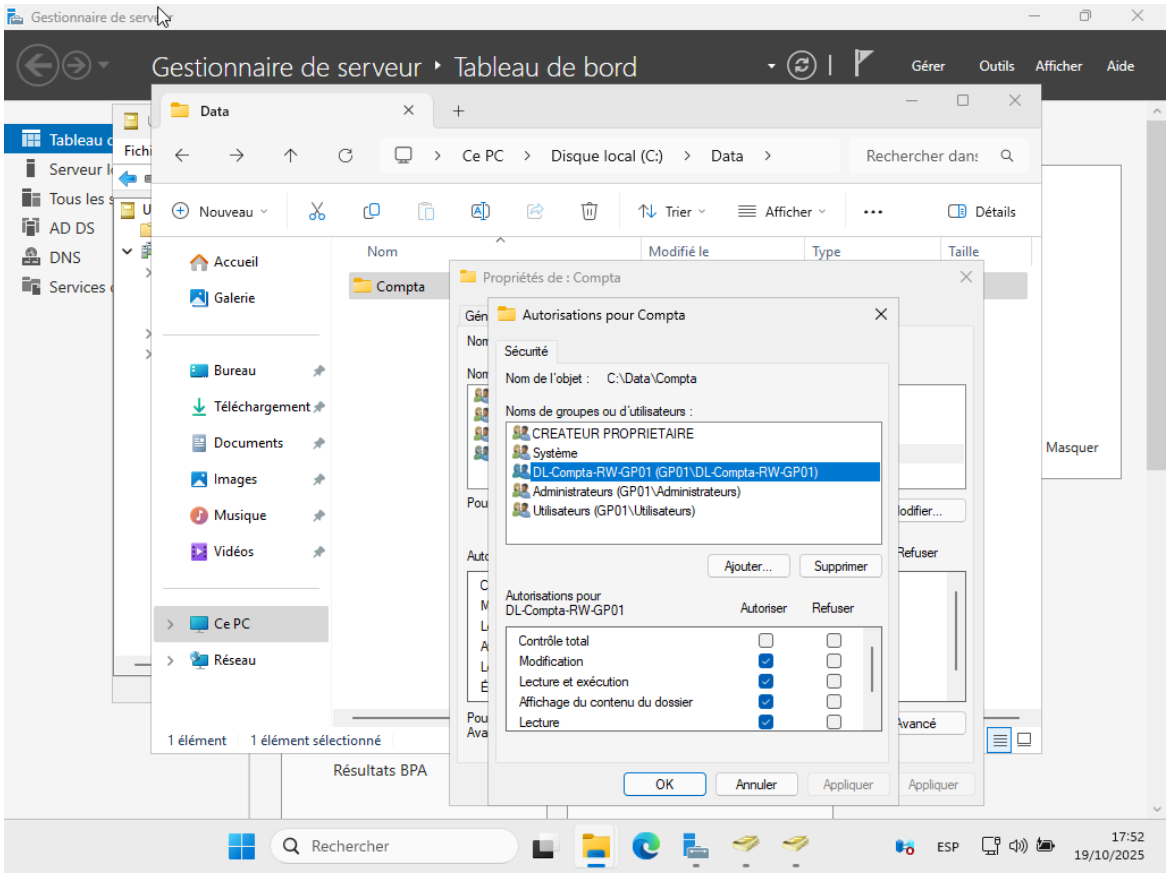


- **Figure :** Propriétés du groupe GG-Compta-Users-GP01



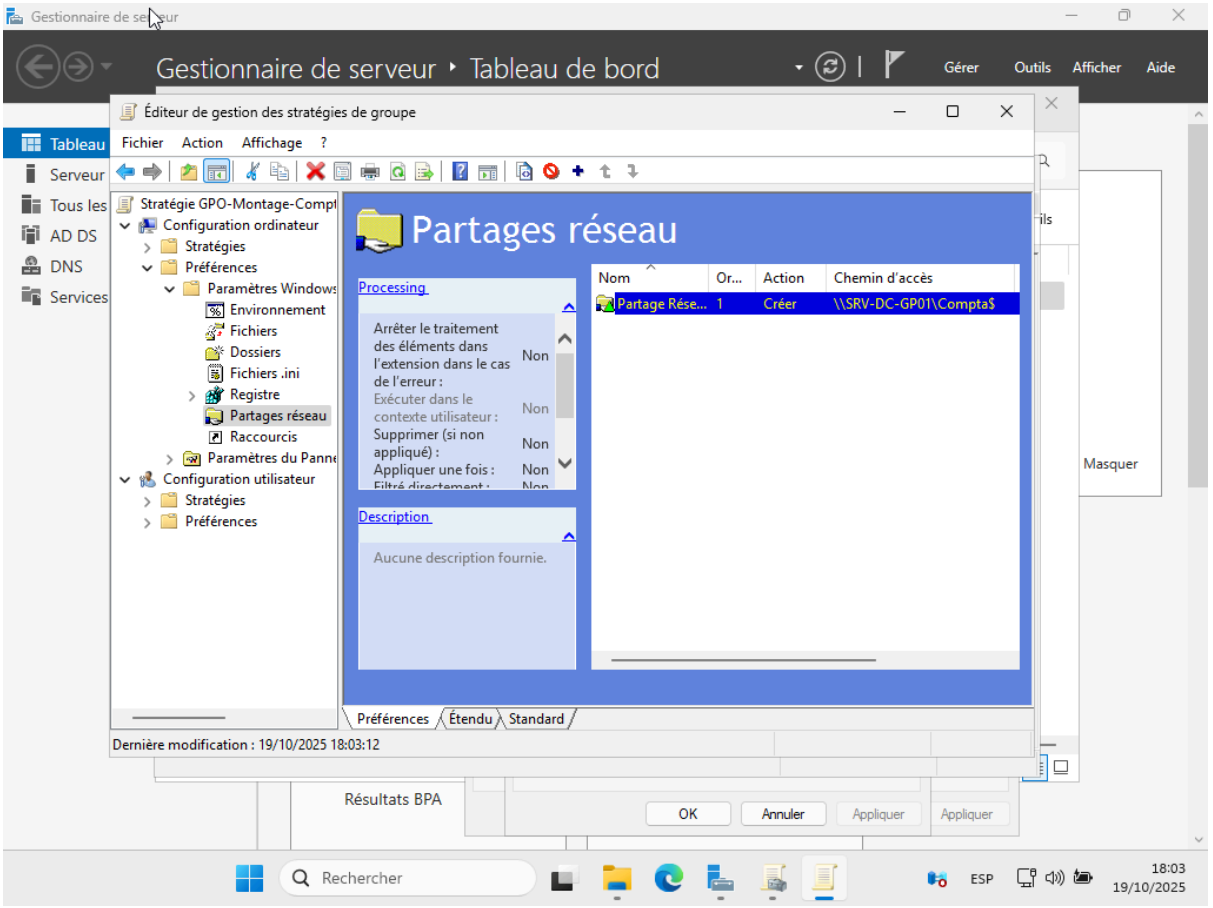
- **Figure :** Propriétés du groupe DL-Compta-RW-GP01

Ensuite, on a créé deux groupes dont un groupe global GG-Compta-Users-GP01, contenant les utilisateurs du service comptabilité, et un groupe local de domaine DL-Compta-RW-GP01 contenant comme membre le groupe global précédemment créé.



- Figure : Application les droits NTFS sur C:\Data\Compta

Sur le dossier C:\Data\Compta, nous avons ensuite configuré les droits NTFS de manière à ce que le groupe DL-Compta-RW-GP01 dispose de l'autorisation Modify, tandis que les administrateurs et le système conservent le Full Control. Pour tous les autres groupes ou utilisateurs, nous avons défini qu'ils n'aient aucun accès.



- **Figure :** Configuration d'une GPO pour monter le partage Compta$ en lecteur H pour le groupe Utilisateurs-GP01

Une fois les permissions en place, nous avons créé une GPO pour mapper le partage réseau en tant que lecteur H sur les postes du groupe Utilisateurs-GP01. Au prochain démarrage ou après un gpupdate /force, les utilisateurs devaient voir apparaître automatiquement le lecteur H pointant vers \\SRV-DC-GP01\Compta$.

Comme nous avons rencontré un problème pour rejoindre le domaine gp01.lab.ece avec la VM client, nous n'avons pas pu réaliser les tests avec user1 et user2. En théorie, user2.gp01 aurait dû pouvoir créer et modifier des fichiers dans le dossier, tandis que user1.gp01 aurait dû obtenir un accès refusé.

Questions :

1. **Expliquez le principe AGDLP utilisé ici**

L'acronyme AGDLP signifie Account, Global Group, Domain Local Group, Permission.
Ce modèle de gestion des droits permet de simplifier et structurer l'administration des accès.

Concrètement, les utilisateurs (Accounts) sont ajoutés dans un groupe global (Global Group), ce groupe global devient ensuite membre d'un groupe local de domaine (Domain Local Group), et enfin, ce groupe local se voit attribuer les droits NTFS (Permissions) sur la ressource concernée, comme un dossier partagé.
Cette méthode permet de modifier facilement les membres ou les droits sans avoir à modifier directement les listes de contrôle d'accès (ACL), ce qui rend la gestion plus claire, plus sûre et plus évolutive.

2. Pourquoi séparer Groupes Globaux (utilisateurs) et Domain Local (droits) ?

Cette séparation permet de distinguer les rôles fonctionnels des autorisations.
Les groupes globaux représentent des ensembles logiques d'utilisateurs (par exemple, dans une entreprise les services Comptabilité ou Ressources Humaines), tandis que les groupes locaux de domaine correspondent aux ressources partagées accessibles à ces ensembles (comme des dossiers, imprimantes ou applications).
Ainsi, en cas de changement de personnel ou de réorganisation, il suffit simplement d'ajouter ou de retirer un utilisateur du groupe global, sans avoir à modifier directement les droits sur les ressources.
Cette méthode offre une meilleure flexibilité et facilite la maintenance de la sécurité à long terme.

3. Quelle est la différence entre droits NTFS et droits de partage (et lequel prime) ?

Les droits NTFS s'appliquent directement au système de fichiers local, et permettent de définir des permissions précises comme la lecture, la modification ou l'exécution d'un fichier ou dossier.
Les droits de partage, quant à eux, s'appliquent uniquement lorsqu'un dossier est accédé via le réseau, et offrent un niveau de contrôle plus général, avec des options telles que lecture, modification ou contrôle total.
Lorsqu'un utilisateur accède à une ressource partagée sur le réseau, le niveau d'accès effectif est déterminé par la combinaison des deux jeux de permissions, et c'est toujours le plus restrictif qui prime.

4. Quelle preuve avez-vous produit pour montrer que la configuration fonctionne ?

On aurait dû générer un rapport à l'aide de la commande gpresult /R afin de vérifier que la GPO de montage du lecteur H a bien été appliquée sur le poste client. Ce rapport affiche l'ensemble des stratégies effectivement reçues par l'utilisateur et par l'ordinateur, ce qui constitue une preuve claire du bon fonctionnement de la configuration.