ADMINISTRATION DE L'ACTIVE DIRECTORY

Cédric BAUDIMENT
AgroMousquetaires – Site d'Antartic 2

BTS SIO SISR
Greta Ardèche- Drôme
Session 2026

Table des matières

I/ Cahier des charges

1- Descriptif de l'existant

Dans le cadre de ce TP, l'objectif est de mettre en place une infrastructure réseau comprenant un Active Directory redondé, des services DNS associés, ainsi que des ressources partagées avec gestion des droits. Le nom de domaine choisi pour cette infrastructure est MySocCBt.fr.

Le réseau est structuré autour de six services répartis sur deux sites distincts. Le site A regroupe les services Technique et Recherche & Développement (R&D) et est connecté au sous-réseau SR2. Le site B regroupe les services Comptabilité, Commerciale, Administration et Ressources humaines, connectés au sous-réseau SR3. Entre le routeur et le pare-feu, un sous-réseau SR1 a également été défini pour assurer la liaison avec l'extérieur.

Cette infrastructure tournera sur quatre VM installées sur une machine physique :

- Une VM PFSense en guise de pare-feu faisant lien entre l'infrastructure réseau et le réseau physique.
- Une VM sous Debian 13 servant de routeur et de serveur DHCP
- Deux VM sous Windows server 2022 où seront installés un serveur DNS et Active Directory (un DNS et Active Directory redondants pour le second).

Nous pouvons prévoir une ou deux VM supplémentaires sous Windows 10 ou 11 qui feront office de poste client où nous effectuerons nos tests.

2- Besoins

Les besoins principaux identifiés pour ce TP sont la mise en place d'un Active Directory avec redondance, la configuration d'un DNS intégré pour la résolution interne, la création et l'organisation des utilisateurs et des groupes selon le modèle AGDLP, ainsi que la gestion des dossiers partagés avec attribution correcte des droits NTFS. Il était également nécessaire de déployer des GPO permettant de restreindre certains paramètres utilisateurs, d'installer Firefox pour le service Technique et de supprimer l'icône de la corbeille pour l'ensemble des utilisateurs sauf R&D. Enfin, l'ensemble de l'infrastructure devait être testé pour s'assurer de sa cohérence et de son fonctionnement conforme aux exigences du TP.

3- Contraintes

L'adresse réseau de base utilisée pour ce TP est 172.28.0.0/16. Trois sous-réseaux distincts ont été créés : SR1 entre le routeur et le pare-feu, SR2 pour le site A et SR3 pour le site B. Chaque service devait disposer d'une capacité suffisante pour ses six utilisateurs avec une marge pour les évolutions futures. La redondance de l'Active Directory était obligatoire, et deux politiques de mots de passe différentes devaient être appliquées : une pour le service R&D et une autre pour le reste des services. De plus, une convention de nommage claire devait être adoptée pour tous les utilisateurs, groupes et ressources.

II/ Ressources

1- Ressources mises à disposition

Pour la réalisation de ce TP, l'ensemble de l'infrastructure a été déployé dans un environnement virtualisé à l'aide du logiciel VMware Workstation. Chaque composant du réseau a ainsi été créé sous

forme de Machine Virtuelle (VM), ce qui a permis de simuler un environnement complet tout en conservant une grande souplesse de configuration.

Les systèmes d'exploitation utilisés pour ces machines virtuelles sont les suivants :

- **Debian 13** : utilisée pour le routeur, permettant la gestion des sous-réseaux, du routage et du DHCP.
- **Windows Server 2022** : utilisé pour les serveurs Active Directory, DNS et les services associés. Deux serveurs distincts ont été configurés pour assurer la redondance de l'AD.
- **PF Sense** : utilisé comme pare-feu afin d'assurer la sécurité et le filtrage du trafic entre le réseau interne et Internet.
- **Windows 10** : utilisé pour les postes clients, permettant de tester l'authentification sur le domaine, les partages réseau et l'application des stratégies GPO.

Les images ISO de chaque OS ont été fournies afin de mettre en place chacune des VMs.

L'utilisation d'un environnement virtualisé a présenté plusieurs avantages : la possibilité de restaurer rapidement un état antérieur grâce aux instantanés, la simplification des tests réseau entre machines virtuelles, et la réduction des risques liés à la manipulation d'un réseau réel.

2- Ressources nécessaires à la mise en place

La mise en place de l'infrastructure a nécessité l'utilisation de logiciels et services tels que DHCP, DNS, Active Directory et les outils de gestion GPO. Des outils de test réseau, notamment ping et nslookup, ont été employés pour vérifier la configuration. Chaque client devait pouvoir se connecter au réseau avec une adresse IP correcte, et le navigateur Mozilla Firefox a été installé pour le service Technique. Le matériel réseau était également indispensable pour établir les connexions entre les sous-réseaux.

3- Gestion des ressources

Les ressources ont été gérées de manière centralisée afin d'assurer la cohérence et la disponibilité. Les serveurs ont reçu des adresses IP statiques adaptées à leur rôle, tandis que les clients ont été configurés pour recevoir leurs adresses automatiquement via DHCP. La documentation et les conventions de nommage ont été respectées afin de garantir une organisation claire et de faciliter la maintenance future.

III/ Analyse

1- Descriptifs des solutions

Pour répondre aux besoins du TP, il a été décidé d'installer l'Active Directory sur un serveur primaire et de configurer un serveur secondaire pour assurer la redondance. Le DNS a été intégré à l'AD afin de simplifier la résolution interne. Le modèle AGDLP a été choisi pour organiser les utilisateurs et les groupes et pour attribuer les permissions aux ressources partagées. Les dossiers de services, les dossiers personnels et le dossier commun ont été créés avec des droits NTFS adaptés. Enfin, des GPO ont été configurées pour appliquer les restrictions spécifiques aux différents services.

2- Comparaison des solutions

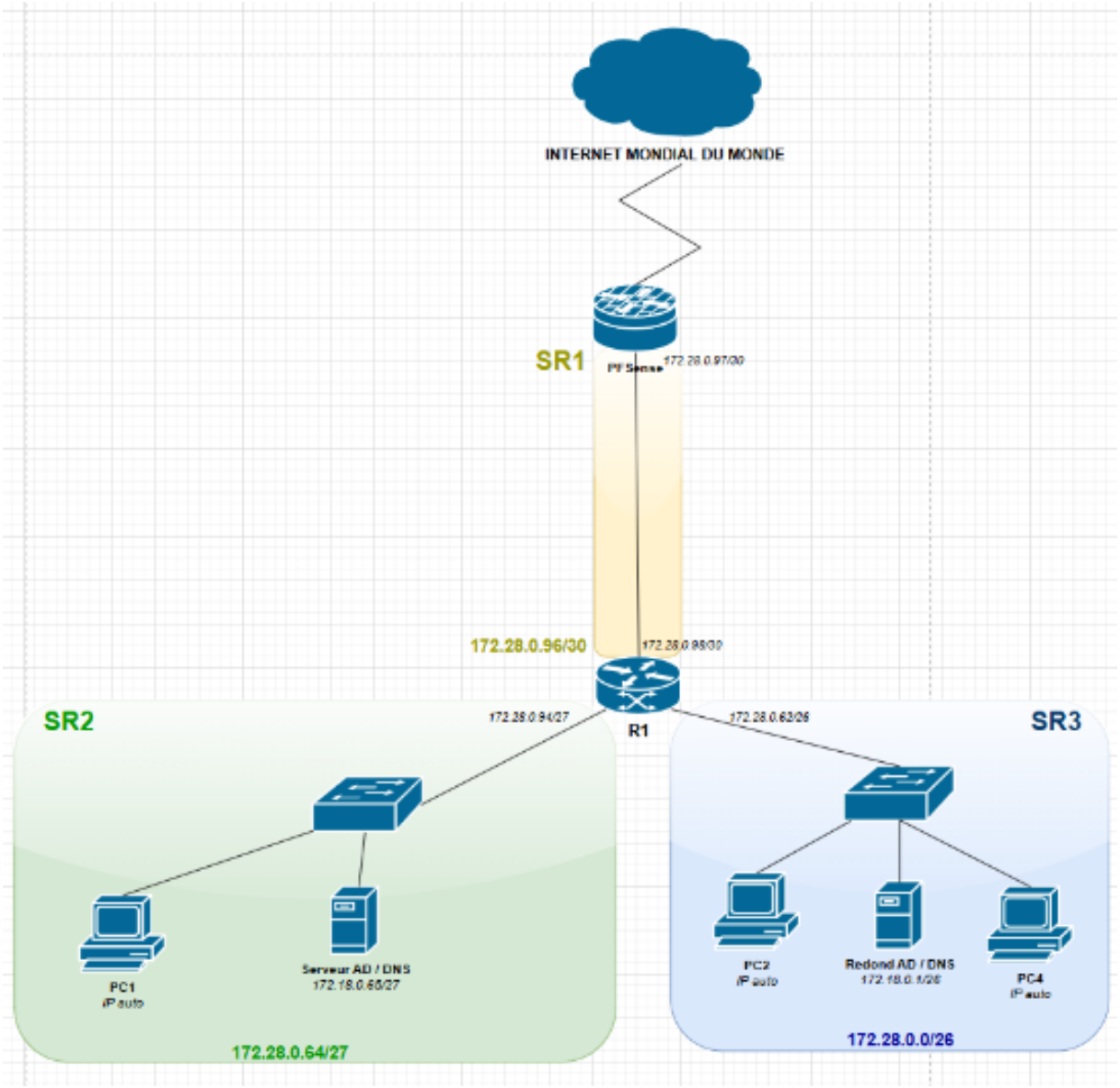
L'option d'un AD redondé présente l'avantage de garantir une haute disponibilité et une réplication automatique des données, mais elle nécessite une configuration correcte du DNS et de la réplication. L'utilisation des dossiers partagés avec le modèle AGDLP permet une gestion centralisée et sécurisée des droits, mais demande une organisation initiale rigoureuse. Enfin, l'application de GPO standardise les configurations et sécurise l'environnement de travail, bien qu'un mauvais paramétrage puisse générer des conflits.

3- Choix d'une solution

La solution retenue combine un AD redondé avec DNS intégré, l'application du modèle AGDLP pour la gestion des groupes et des ressources, ainsi que l'utilisation de GPO pour imposer les restrictions et installer Firefox pour le service Technique. Cette approche répond à l'ensemble des besoins identifiés dans le TP tout en respectant les contraintes techniques.

4- Cartographie du réseau

a) Schéma



b) Plan d'adressage

Pour réaliser cette infrastructure je vais utiliser l'adresse réseau **172.28.0.0/16**.

Cette infrastructure est composée de **6 services** de **6 utilisateurs** chacun répartis comme suit :

- **Comptabilité** **SR3**
- **Technique** **SR2**
- **Commerciale** **SR3**
- **Administration** **SR3**
- **R&D** **SR2**
- **Ressources humaines** **SR3**

Ces services seront déployés sur deux sites correspondant au deux sous réseaux : **SR2** et **SR3**. **SR1** correspondant au sous réseau situé entre le pare-feu et le routeur.

Je vais donc avoir besoin de calculer trois sous réseaux et de définir le nombre d'hôte pour chaque sous réseau :

- **SR1** : **2 hôtes** suffiront => le routeur et le pare-feu.
- **SR2** : deux services intégreront ce sous réseau soit 12 hôtes minimum. Je vais doubler le nombre d'hôtes afin d'avoir de la marge en cas de recrutement ou d'arrivé d'intervenant. Nous allons retenir un maximum de **24 hôtes**.

SR3 : 4 services intègreront ce sous réseau, soit un total de 24 utilisateurs. Comme précédemment, je vais laisser de la marge en doublant le nombre d'hôte, soit un maximum de **48 hôtes**.

- **SR3 : 48 hôtes**

Sous-Réseau	172.28.0.0/26
Masque	*255.255.255.192*
1ère adresse	172.28.0.1/26
Dernière adresse	172.28.0.62/26
Broadcast	172.28.0.63/26

- **SR2 : 24 hôtes**

Sous-Réseau	172.28.0.64/27
Masque	*255.255.255.224*
1ère adresse	172.28.0.65/27
Dernière adresse	172.28.0.94/27
Broadcast	172.28.0.95/27

- **SR1 : 2 hôtes**

Sous-Réseau	172.28.0.96/30
Masque	*255.255.255.252*
1ère adresse	172.28.0.97/30
Dernière adresse	172.28.0.98/30
Broadcast	172.28.0.99/30

c) Tables de routage

- **Routeur :**

Sous-réseau	Adresse	Interface	Passerelle
SR1	172.28.0.96/30	172.28.0.98/30	172.28.0.97/30
SR2	172.28.0.64/30	172.28.0.94/27	172.28.0.94/27
SR3	172.28.0.0/26	172.28.0.62/26	172.28.0.62/26
Défaut	0.0.0.0/0	172.28.0.98/30	172.28.0.97/30

- **PF Sense :**

Sous-réseau	Adresse	Interface	Passerelle
SR1	172.28.0.96/30	172.28.0.97/30	172.28.0.97/30
SR2	172.28.0.64/30	172.28.0.97/30	172.28.0.98/30
SR3	172.28.0.0/25	172.28.0.97/30	172.28.0.98/30
Défaut	0.0.0.0/0	WAN	FAI

5- Etude de l'impact sur le SI existant

L'intégration de cette infrastructure implique que tous les clients du réseau devront utiliser le nouveau domaine pour s'authentifier. Les ressources partagées sont centralisées sur les serveurs AD, et les droits d'accès sont appliqués via les groupes et GPO. Les utilisateurs voient leur environnement de travail standardisé, et les restrictions empêchent certaines modifications non autorisées sur les postes clients.

6- Phasage de l'intervention

L'intervention a été planifiée en plusieurs étapes successives. Tout d'abord, le réseau et les sous-réseaux ont été configurés. Ensuite, le serveur AD primaire et le DNS ont été installés. Le serveur AD secondaire a ensuite été configuré pour assurer la redondance et la réplication des données. Les unités organisationnelles, utilisateurs et groupes ont été créés, suivis de la mise en place des dossiers partagés et de l'attribution des droits. Enfin, les GPO ont été déployées et les tests de validation ont été réalisés.

7- Prévision des tests de validation

Les tests de validation comprenaient la vérification de la connectivité réseau et de la résolution DNS à l'aide des commandes ping et nslookup. La réplication AD a été vérifiée via la commande repadmin /replsummary. Les droits sur les dossiers partagés ont été testés pour s'assurer de la conformité avec le modèle AGDLP. Enfin, les GPO ont été contrôlées pour valider les restrictions et l'installation du logiciel Firefox.

8- Déploiement

Le déploiement a consisté à installer et configurer les serveurs et les clients conformément au plan, à configurer le DHCP sur le routeur pour l'attribution automatique des IP, et à vérifier que chaque serveur disposait d'une IP statique correcte.

IV/ Mise en place

1- Configuration de PFSense

Je vais utiliser PF Sense comme pare feu principale de notre réseau. Il sera le lien entre le web et le sous réseau SR1.

L'interface WAN, qui donne sur le net sera configuré automatiquement. Je vais donc configurer l'interface LAN, porte d'entrée de notre réseau, les règles de pare feu et la table de routage vers les autres sous réseau.

- Installer et configurer PFSense

2- Configuration du routeur

- Installation d'une machine sous debian
- Installer et configurer un routeur sous Debian

3- Configuration du serveur DHCP au sein du routeur

- Installation d'une machine sous debian
- Installer et configurer un serveur DHCP sous Debian

4- Mise en place du premier serveur Windows Server 2022

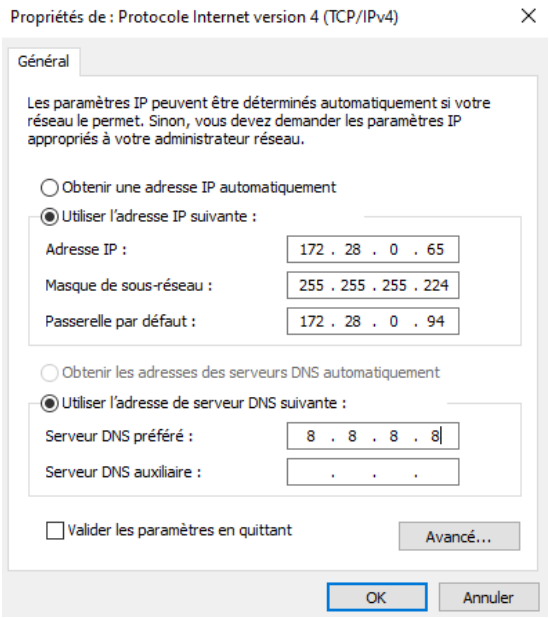
Ce serveur sera connecté au réseau SR2.

- Installation de windows server 2022

Dans un premier temps je vais donner un nom au serveur : Serveur_AD01

Paramètres > système > à propos > renommer le PC puis redémarrer.

Ensuite je vais attribuer une configuration réseau statique avec une adresse IPv4 de 172.28.0.65.



a) Configuration du serveur DNS

- Installer et configurer un serveur DNS sous Windows

b) Configuration du serveur Active Directory

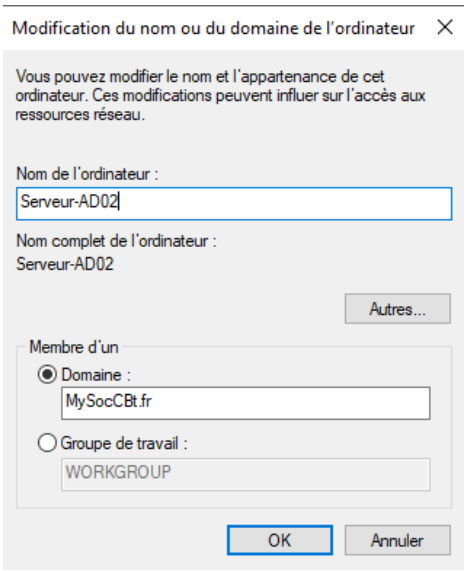
- Installer et configurer un serveur Active Directory

5- Mise en place du second serveur de redondance Windows Server 2022

Dans un premier temps je vais connecter ce serveur au réseau SR3 et configurer son adresse IP avec 172.28.0.1. Je vais ensuite nommer ce serveur Serveur-AD02 et l'intégrer au domaine.

Paramètres > système > à propos > paramètres avancés du Système. Aller dans l'onglet Nom de l'ordinateur puis modifier.

Changer le nom de l'ordinateur, cocher domaine puis inscrire le nom de domaine MySocCBt.fr et valider. Rentrer le nom d'admin et le mot de passe admin enregistrer dans l'AD puis redémarrer la machine.



a) Configuration du serveur DNS de redondance

- Mise en place d'un serveur DNS de redondance sous windows

b) Configuration du serveur Active Directory de redondance

- Mise en place d'un serveur AD redondant

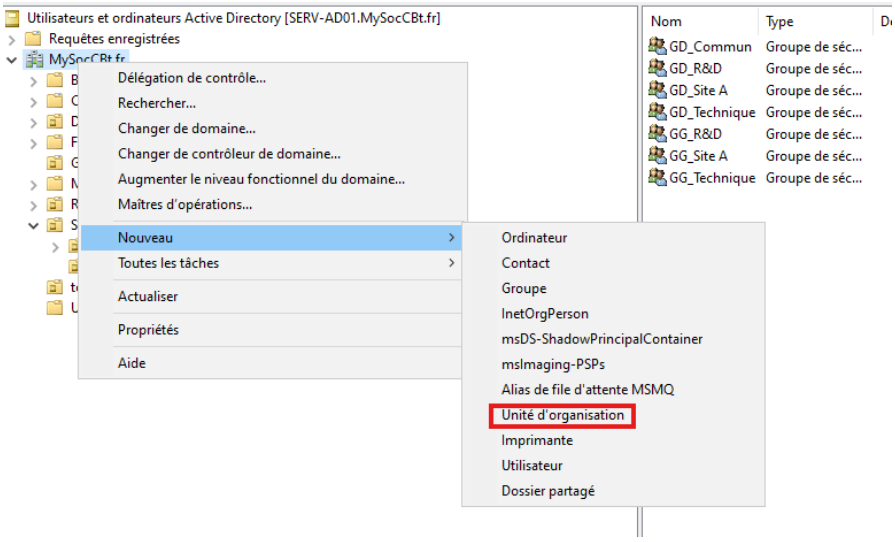
V/ Gestion de l'Active Directory

1- Création des groupes et des utilisateurs

Dans **Utilisateurs et Ordinateurs de l'Active Directory** je vais créer des Unités Organisationnels pour plus d'organisation :

- Une OU Groupes où nous y ajouterons les groupes globaux et les groupes de domaines locaux
- Une OU Services où nous y ajouterons une OU par services et les utilisateurs.

Pour cela : *clic droit sur le nom de domaine > Nouveau > Unité d'Organisation*



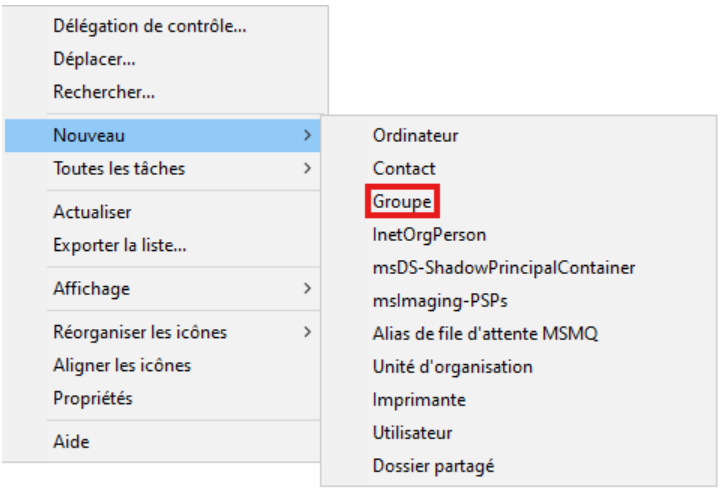
Ajouter le nom du groupe puis valider.

a) Ajout des groupes globaux

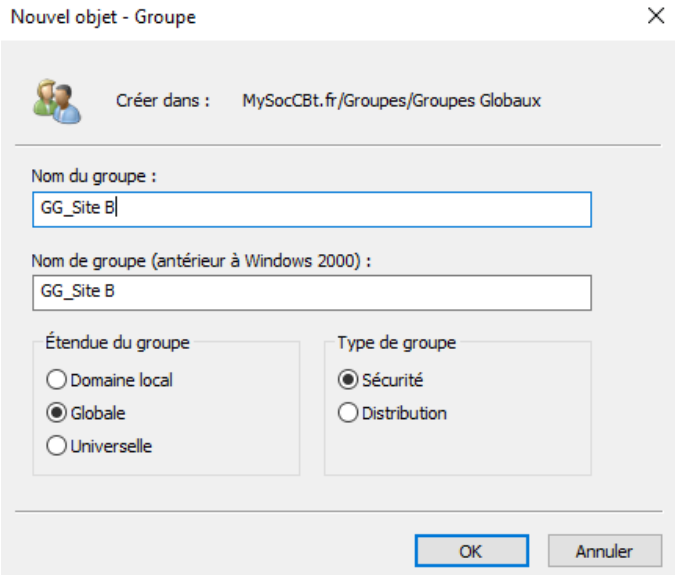
Je vais ajouter nos groupes locaux qui seront organisés ainsi : site > service > utilisateurs

Créer notre Site B :

- Dans l'OU groupes, clic droit > Nouveau > Groupe



Inscrire le nom souhaité, dans l'étendue du groupe sélectionner Globale puis valider.



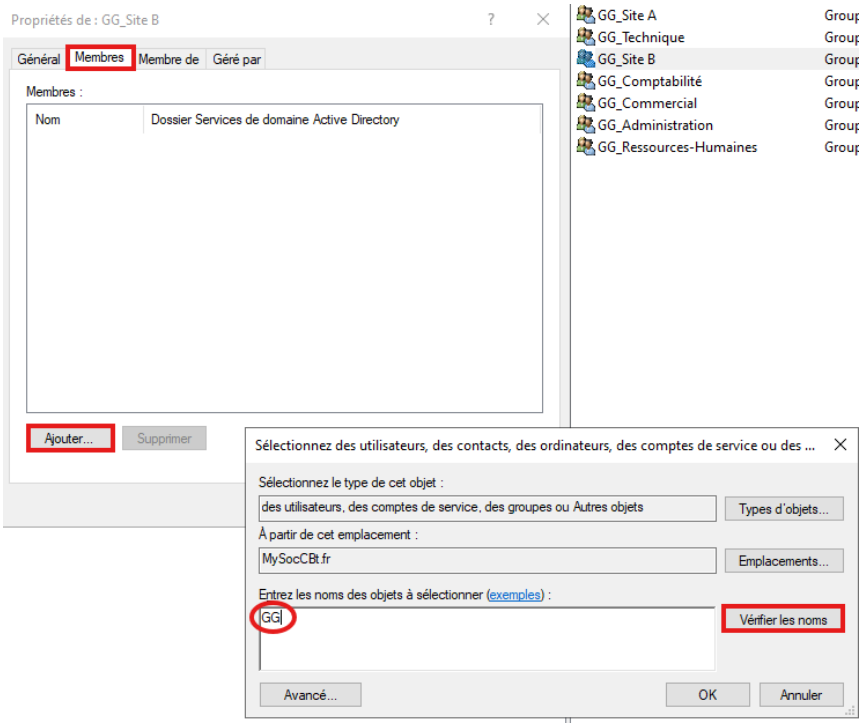
Faire ceci pour tous les groupes globaux souhaités.

Pour plus de praticité nous nommerons les groupes globaux GG_Nom.

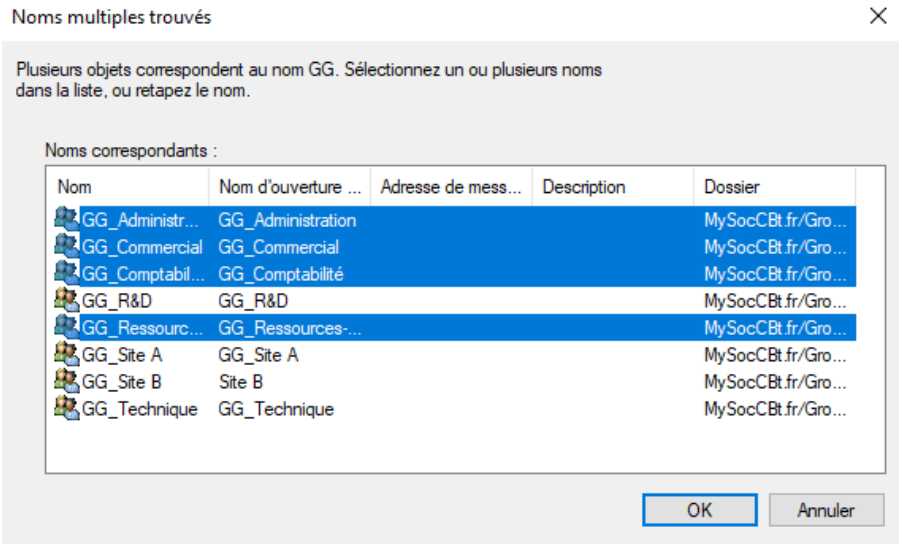
Une fois que les groupes sont créés, nous allons ajouter les groupes services aux groupes sites :

- Clic droit sur le groupe global site B puis propriété
- Onglet Membres > Ajouter

Inscrire le nom (ou les premières lettres) du groupe souhaité puis Vérifier :



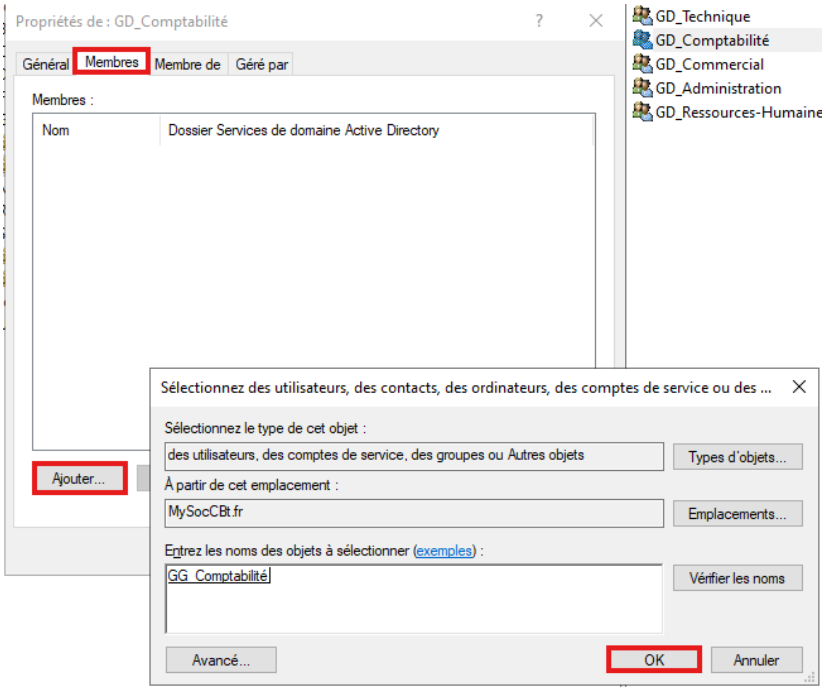
Sélectionner ensuite les groupes qui feront parties du site B puis valider :



b) Ajout des groupes de domaine local

Pour créer les groupes de domaine local, nous allons utiliser la même méthode que précédemment. A la seule différence que dans l'étendue du groupe je sélectionnerais Domaine Locale. Chaque groupe local sera nommé sous cette forme : GD_Nom.

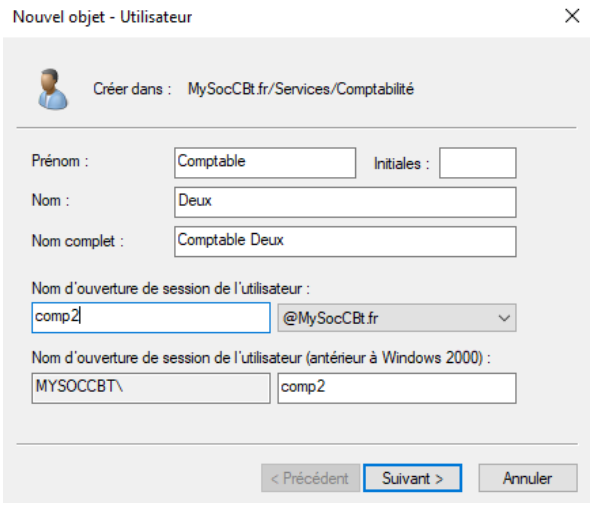
Chaque groupe de domaine local sera membre du groupe global lui correspondant : GG_Nom > GD_Nom.

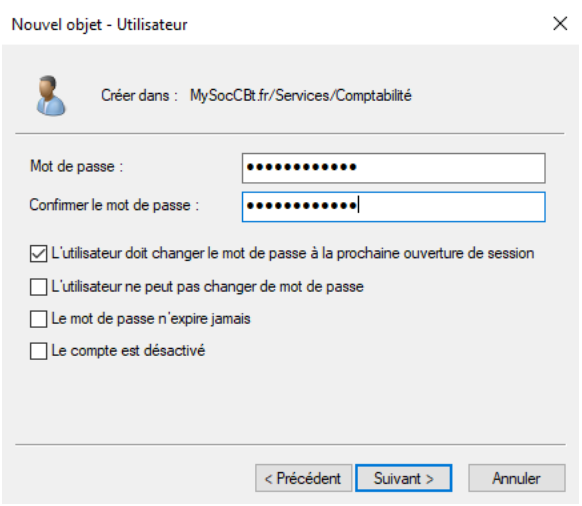


Ajout des utilisateurs

Pour créer un nouvel utilisateur je vais me positionner dans l'OU Services > nom_service. Puis clic droit > Nouveau > Utilisateur.

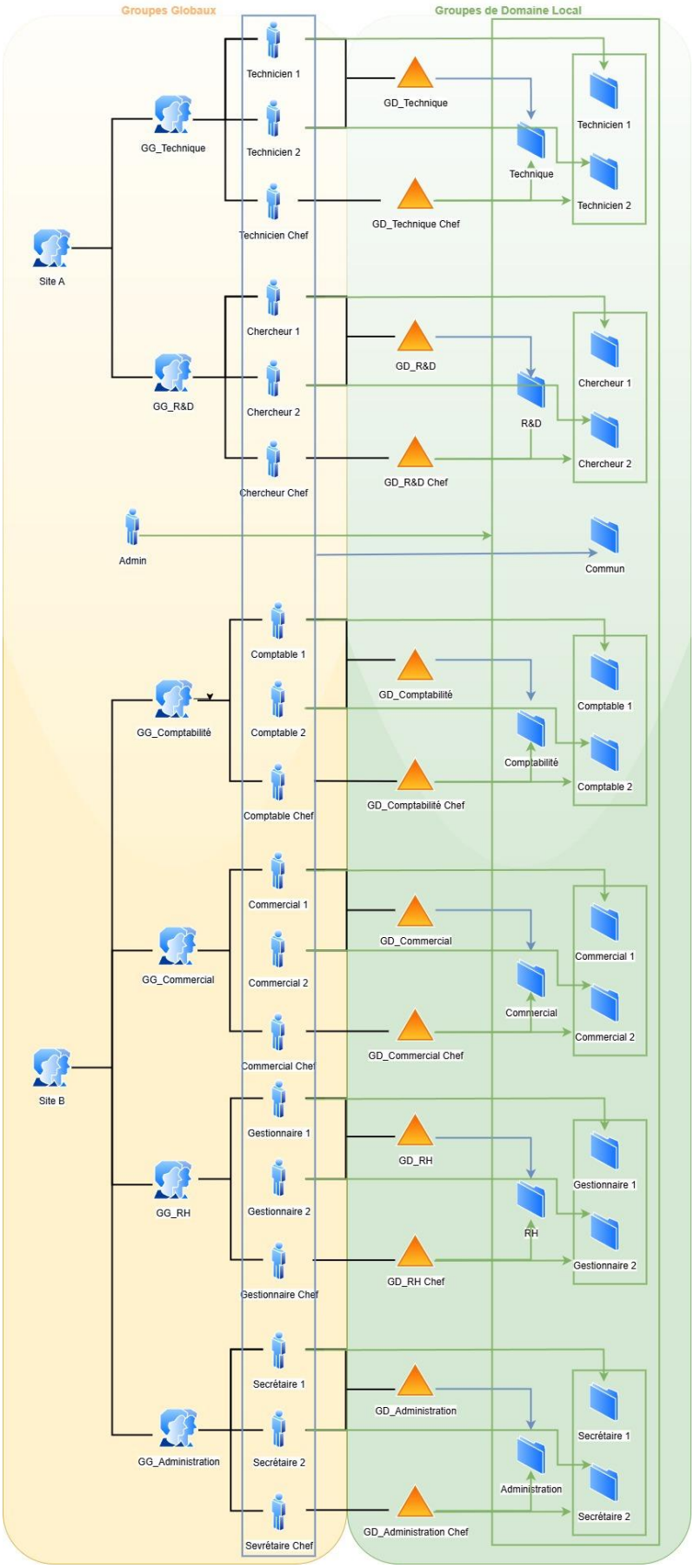
Inscrire les informations concernant l'utilisateur puis lui définir un mot de passe :





Pour une bonne pratique je laisserai l'option « l'utilisateur doit changer le mot de passe » cocher. Mais pour des soucis pratiques, je le décocherai et cocherai « le mot de passe n'expire jamais ».

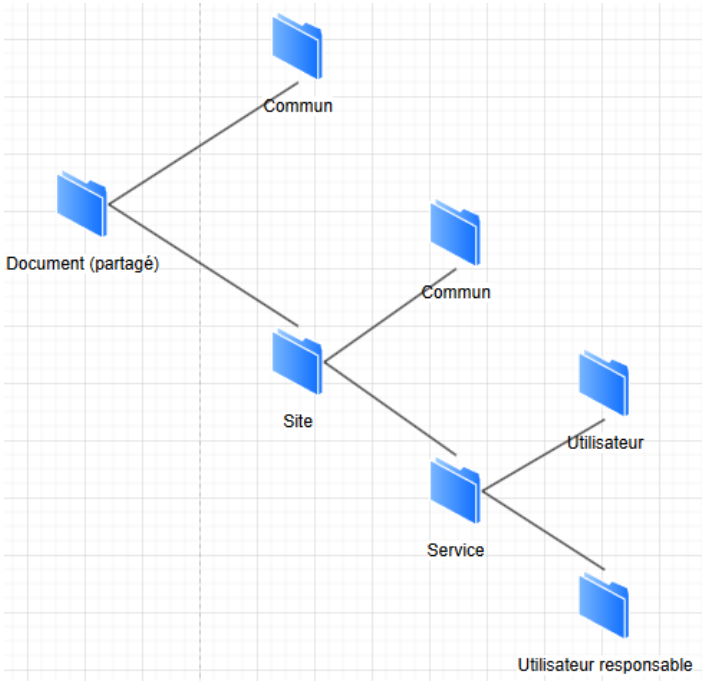
c) Arborescence des groupes utilisateurs



2- Création des dossiers utilisateurs et autorisation accès

a) Création des dossiers

Les dossiers seront créés dans cette arborescence : Site > services > utilisateur (dossier perso).



Je créerai cette arborescence dans le dossier Document qui me mettra en partage sur le réseau de cette manière :

Clic droit > propriété > onglet partage > partage avancé > cocher Partager ce dossier.

L'arborescence sera accessible sur n'importe quelle machine du réseau en allant dans le dossier Réseau ou en cherchant dans la barre de recherche d'un explorateur de dossier : \\SRV01-SR2\Documents.

b) Politique d'autorisation

Je vais mettre en place deux politiques d'autorisations au sein des dossiers :

- **Une politique de lecture et exécution (L.E) :** l'utilisateur pourra consulter les dossiers et les fichiers concernés mais ne pourra pas les modifier ni les supprimer. Il pourra cependant copier le fichier ou le dossier qu'il souhaite dans son dossier pour le modifier.
- **Une politique de lecture, écriture, suppression (L.E.S) :** l'utilisateur pourra modifier et supprimer à sa guise les documents et les fichiers.

Tout d'abord l'utilisateur admin aura des droits L.E.S sur tous les dossiers et leur contenant.

Les dossiers Site sera accessible en L.E par tous les membres de GD_Site.

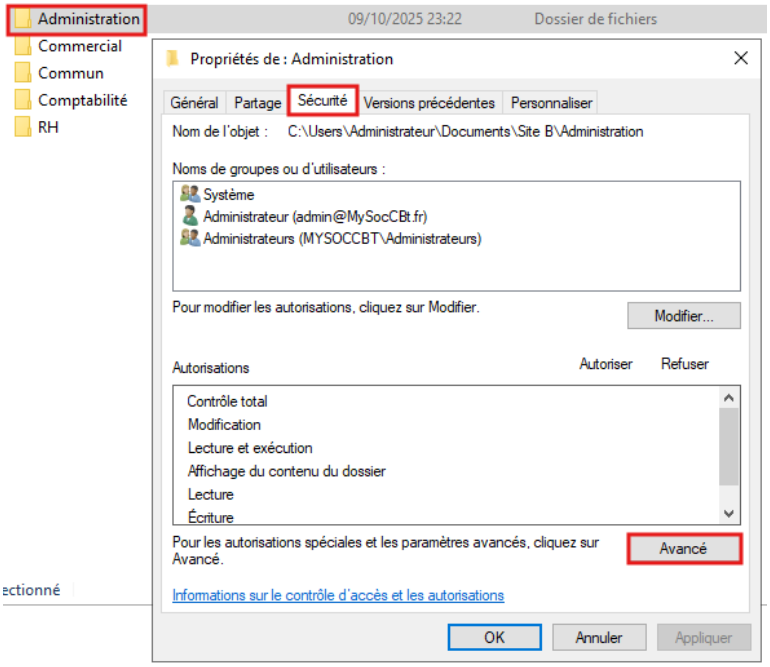
Les dossiers services seront accessible en L.E par les membres de GD_Service. Cependant ils seront accessibles dans son intégralité en L.E.S par les membres de GD_Service_Chef soit les responsables du service.

Les dossiers persos d'utilisateurs seront accessibles en L.E.S par les utilisateurs concernés ainsi que par les membres de GD_Service_Chef.

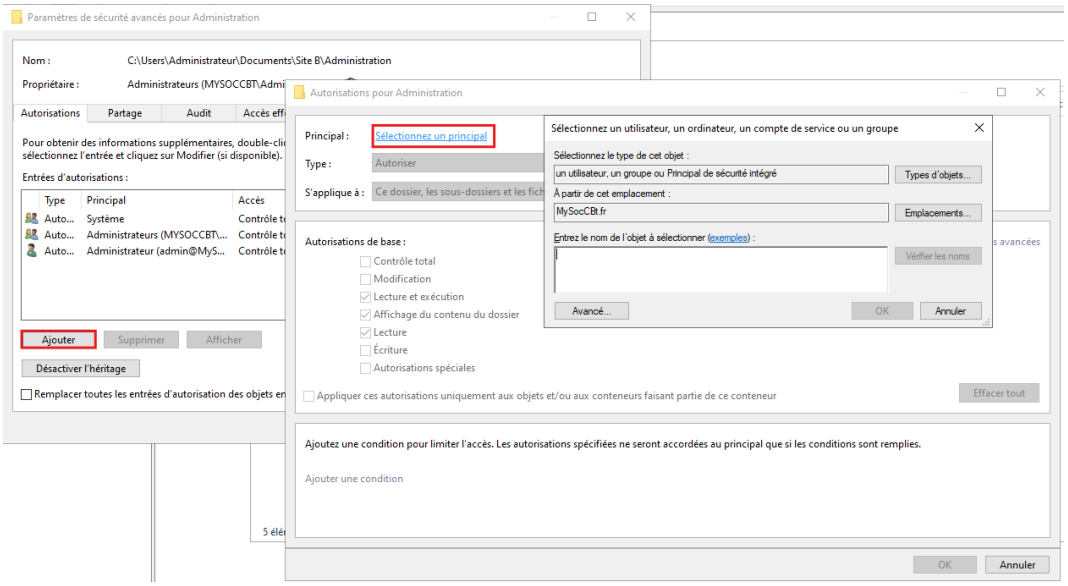
NB : Un dossier faisant partie d'un groupe particulier ne pourra pas être accessible par un utilisateur ne faisant pas partie de ce groupe.

Pour donner des droits à un dossier je vais procéder comme suit :

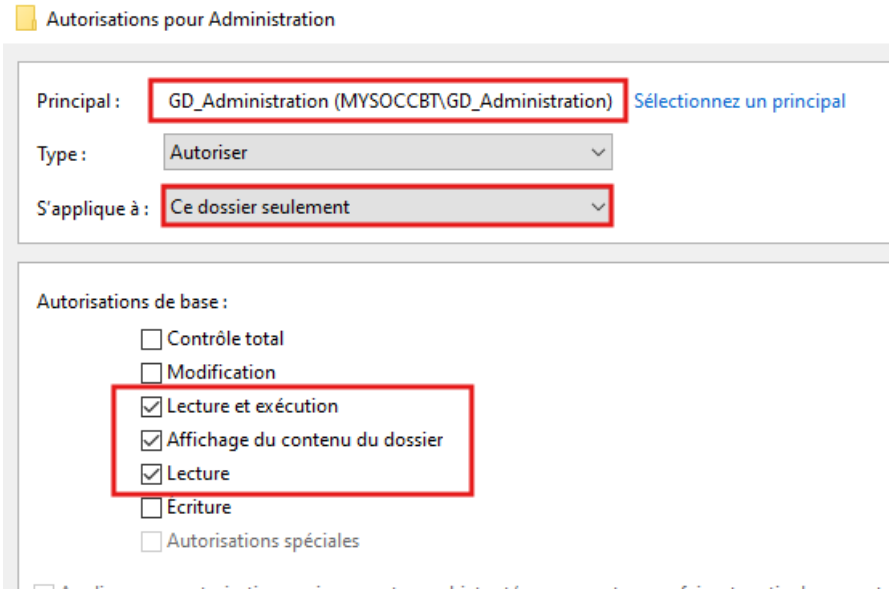
Clic droit sur un dossier > Propriété > Sécurité



Ensuite sélectionner ajouter puis Sélectionner un principal. A ce stade, dans l'encadré Entrez le nom de l'objet à sélectionner, entré le nom du groupe ou de l'utilisateur qui pourra accéder à ce dossier.



Je vais prendre pour exemple le dossier Administration qui sera accessible par les membres de ce service et leurs responsables.

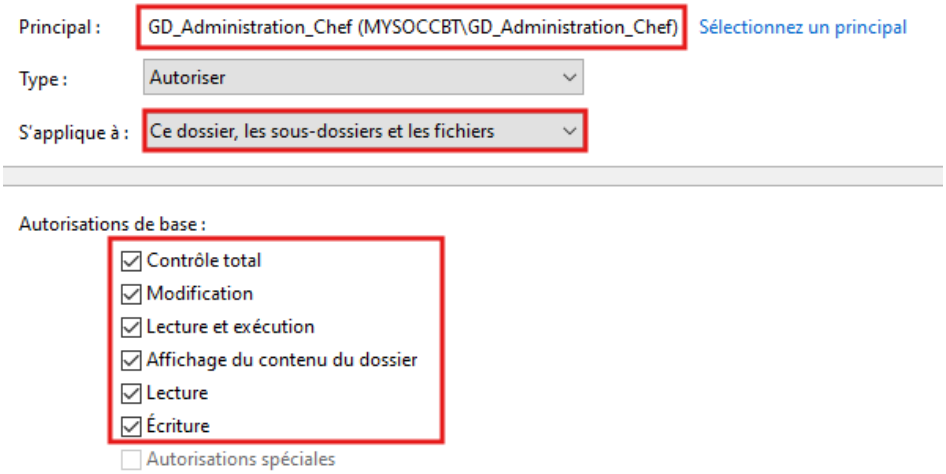


Le groupe concerné est bien le groupe de domaine local Administration. Il s'applique seulement à ce dossier. Les dossiers à l'intérieur étant les dossiers des utilisateurs qui seront accessible par eux et par leurs responsables.

Dans autorisation de base j'ai les droits que je leur donnerai. C'est-à-dire :

- Lecture et exécution
- Affichage du contenu du dossier
- Lecture

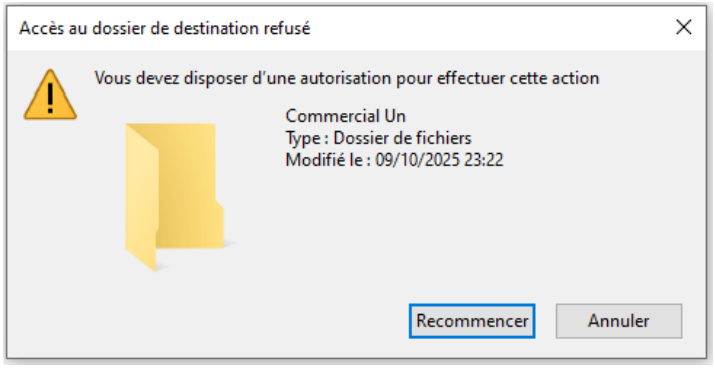
Ils peuvent ainsi consulter le dossier et les fichiers contenu mais pas les modifier ni les supprimer.



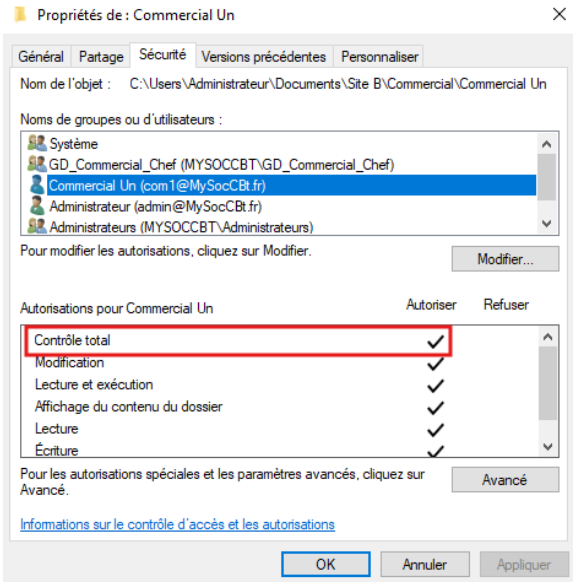
Dans ce second cas, je donne les droits au groupe de responsable du service administration. Je leur donne accès au dossier et tous les sous-dossiers qui le compose. Enfin, je leur donne tous les droits dessus soit la lecture, l'exécution et la suppression du contenu.

A ce stade, lorsque je me connecte à une machine avec les identifiants d'un utilisateur, je peux observer qu'il est possible d'accéder aux dossiers dont il a les droits d'accès. Cependant, je peux m'apercevoir qu'il ne peut pas modifier son dossier perso (celui où il a le contrôle total).

Lorsque l'on va, par exemple, créer un dossier j'aurais ce message d'erreur :



Je vais pourtant donner tous les droits à cet utilisateur :



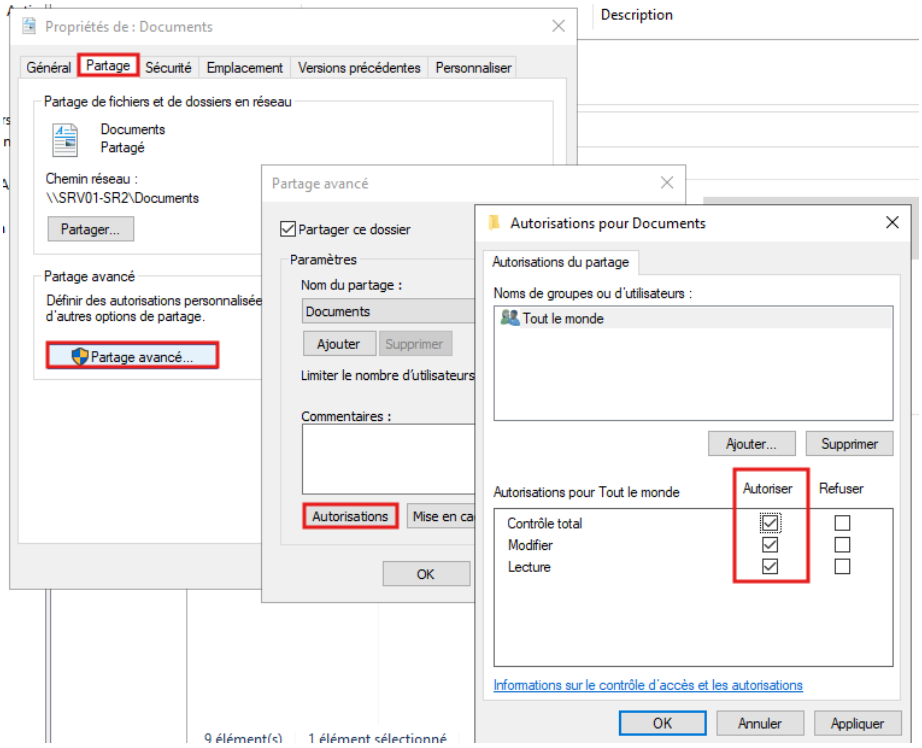
En effet, tant que le partage réseau n'accorde pas "Contrôle total" à Tout le monde, la machine bloque toute écriture via le réseau, même si le NTFS lui donne les droits choisis. Les autorisations de partage et NTFS ne se remplacent pas : elles se cumulent. En réalité, Windows applique les deux, et le résultat final correspond au niveau le plus restrictif. Autrement dit : L'accès effectif = le plus restrictif entre les droits de partage et les droits NTFS.

En résumé :

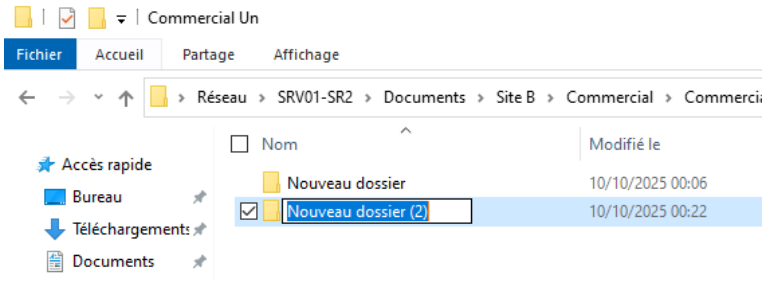
Situation	Résultat effectif
Partage = Lecture / NTFS = Écriture	Lecture seule
Partage = Contrôle total / NTFS = Lecture	Lecture seule
Partage = Contrôle total / NTFS = Écriture	Écriture
Partage = Contrôle total / NTFS = Contrôle total	Contrôle total

En pratique, il suffit de modifier les autorisations de partage dans le dossier racine :

Clic droit sur le dossier Document > propriété > onglet Partage > Partage avancé > Autorisation



Désormais, lorsque je retourne sur la session de mon utilisateur, il peut désormais avoir le contrôle total de son dossier et dans mon cas créer un dossier.



VI/ Gestion des objets de stratégie de groupe (GPO)

L'utilisation des GPO permet d'administrer et de contrôler le comportement des postes clients du domaine depuis les serveurs Active Directory. Les GPO ont été créées et appliquées depuis la console "Gestion des stratégies de groupe" sur le serveur principal (Serveur-AD01), puis répliquées automatiquement sur le serveur secondaire (Serveur-AD02).

Pour accéder à la console : Gestionnaire de serveur > Outils > Gestion des stratégies de Groupe.

1- Politique de mot de passe

Afin de répondre aux exigences du cahier des charges, deux politiques de mots de passe distinctes ont été mises en place :

- une politique générale appliquée à l'ensemble des utilisateurs du domaine ;

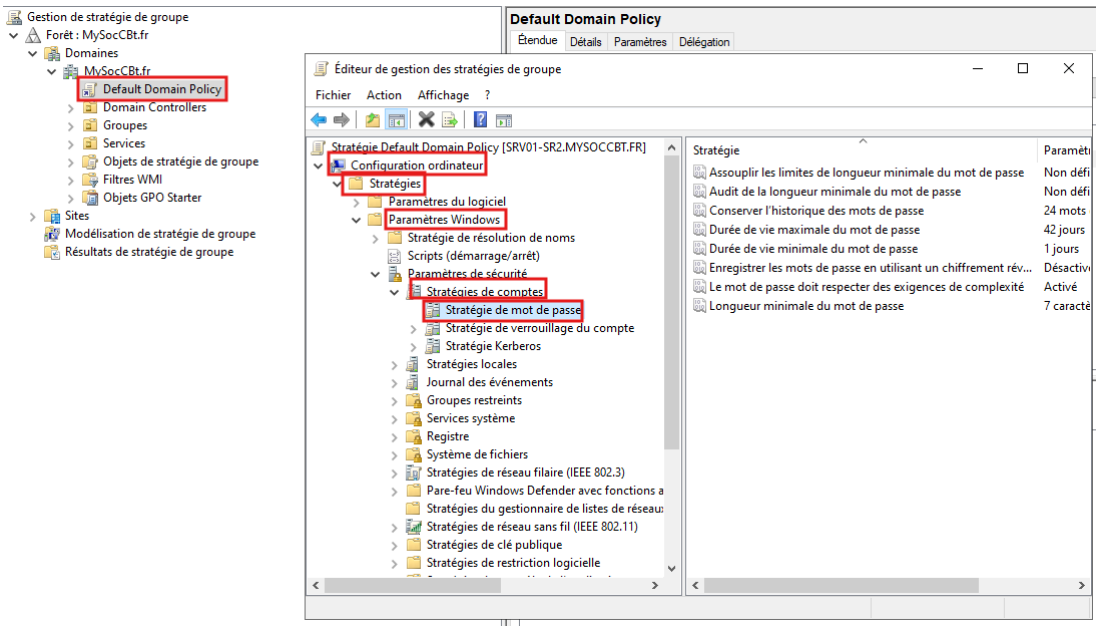
- une politique spécifique au service **R&D**, plus restrictive.

a) Politique générale à l'ensemble des utilisateurs

Pour le reste des utilisateurs du domaine, la stratégie par défaut a été conservée avec une longueur minimale de 8 caractères et une complexité activée.

1. Développer :
   Forêt → Domaines → MySocPNm.fr → Stratégie de domaine par défaut (Default Domain Policy)
2. Clic droit → Modifier.
3. Dans l'éditeur de stratégie :
   - Aller dans Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de compte → Stratégie de mot de passe.
4. Modifier les valeurs suivantes :
   - Longueur minimale du mot de passe : 8 caractères
   - Le mot de passe doit respecter les exigences de complexité : Activé
   - Durée de vie maximale du mot de passe : 90 jours
   - Nombre de mots de passe mémorisés : 5

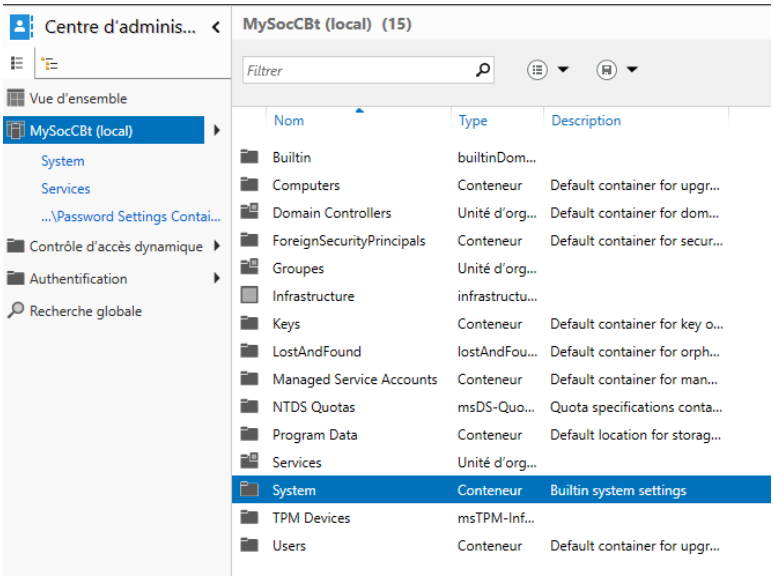
Cette configuration s'applique à tous les utilisateurs du domaine sauf ceux pour le service R&D.



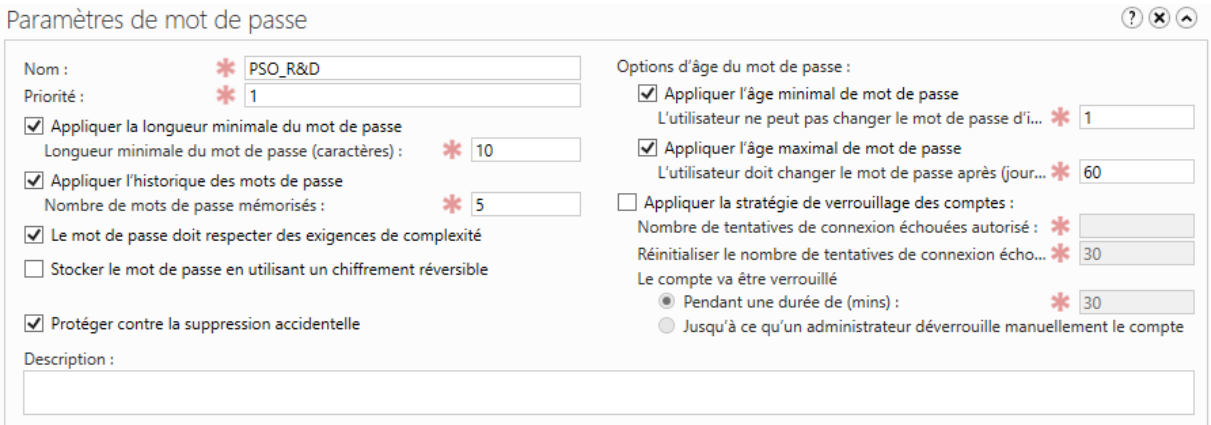
Stratégie	Paramètres de stratégie
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	5 mots de passe mémorisés
Durée de vie maximale du mot de passe	90 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	8 caractère(s)

b) Politique spécifique au service R&D

Ouvrir Centre d'administration Active Directory. Sélectionner le nom de notre domaine puis sélectionner System.



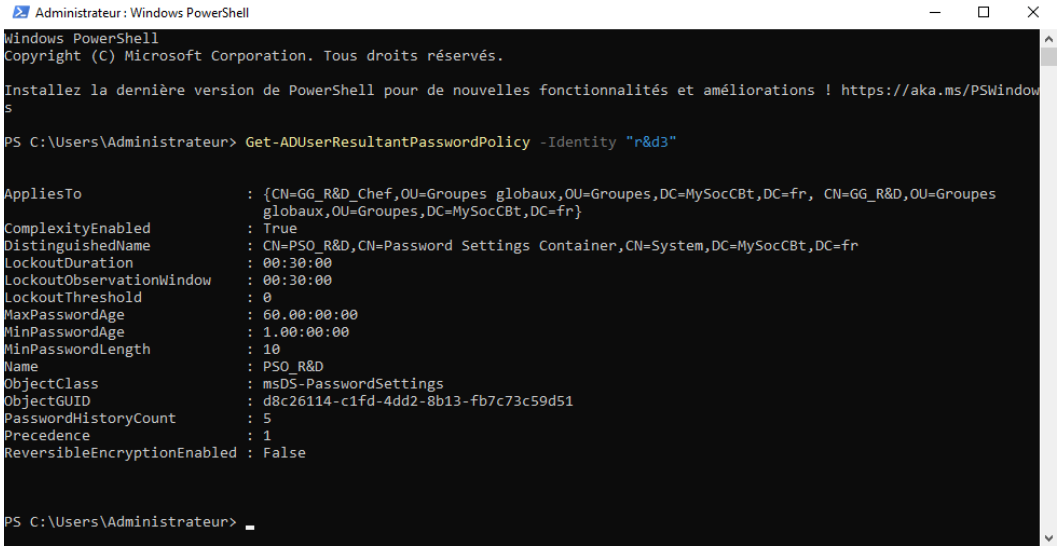
Sélectionner ensuite Password Setting Container. Clic droit puis Nouveau > paramètre de mot de passe.



Cliquer ensuite sur ajouter afin d'ajouter les groupe globaux R&D et R&D_Chef.

c) Vérification et test

Pour tester si la politique de mot de passe est fonctionnelle, he vais ouvrir un terminal powershell en admin et taper la commande suivante : `Get-ADUserResultantPasswordPolicy -Identity "r&d3"`. Cette commande retourne la police de mot de *passe* effective sur l'utilisateur.



Le compte r&d3 est membre du groupe global GG_R&D et hérite de la politique de mot de passe spécifique R&D (PSO_R&D). La commande PowerShell Get-ADUserResultantPasswordPolicy -Identity "r&d3" confirme que la politique est appliquée, incluant complexité obligatoire, longueur minimale de 10 caractères et historique de 5 mots de passe.

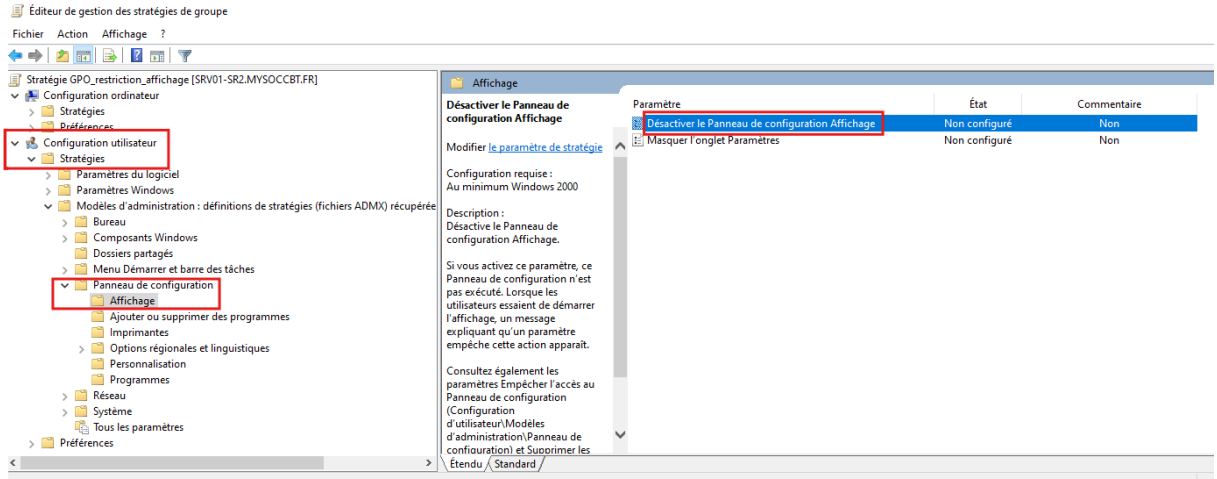
2- Modification des paramètres d'affichage du bureau

Pour répondre aux contraintes du TP, il a été demandé de restreindre la modification des paramètres d'affichage du bureau pour tous les services sauf le service R&D. Cette configuration est réalisée via les Objets de Stratégie de Groupe (GPO) dans l'Active Directory.

a) Restriction des paramètres d'affichages

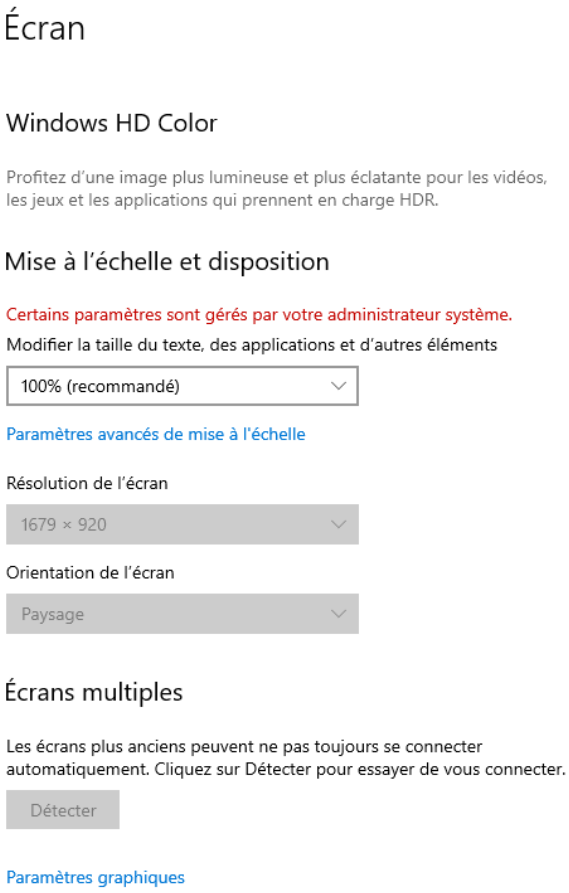
Dans gestion des stratégies de groupe, sur l'OU Services qui contient les OU de tous les services, faites un clic droit puis *Créer un objet GPO dans ce domaine et le lier ici*.

Je nommeraicette GPO GPO_restriction_affichage. Une fois créé, faire clic droit sur la GPO puis modifier. Sélectionner Configuration utilisateur > Stratégie > Modèles d'administration > Panneau de configuration > Affichage.



Ouvrir Désactiver le panneau de configuration Affichage et activer le.

Pour tester si la GPO à fonctionner je vais me connecter avec un utilisateur sur un poste client. Une fois connecter je vais faire un clic droit sur le bureau puis ouvrir Paramètres d'affichage. Je peux voir que certains paramètres sont grisés et inaccessible :



b) Règle d'exception pour le service R&D

Je vais créer une exception pour le service R&D afin qu'eux seuls puissent modifier les paramètres d'affichage.

Dans la GPO précédemment créé, aller dans l'onglet Délégation et ajouter les groupes GD_R&D et GD_R&D_Chef. Cliquer sur Avancé et sélectionner les groupes ajoutés. Pour chacun d'eux, cocher la case refuser à la ligne Appliquer la stratégie de groupe.

Maintenant, je vais le connecter sur le poste client avec un compte R&D. Lorsque je vais dans les paramètres d'affichage, je peux les modifier.

3- Installation de Mozilla Firefox sur les PCs du technique

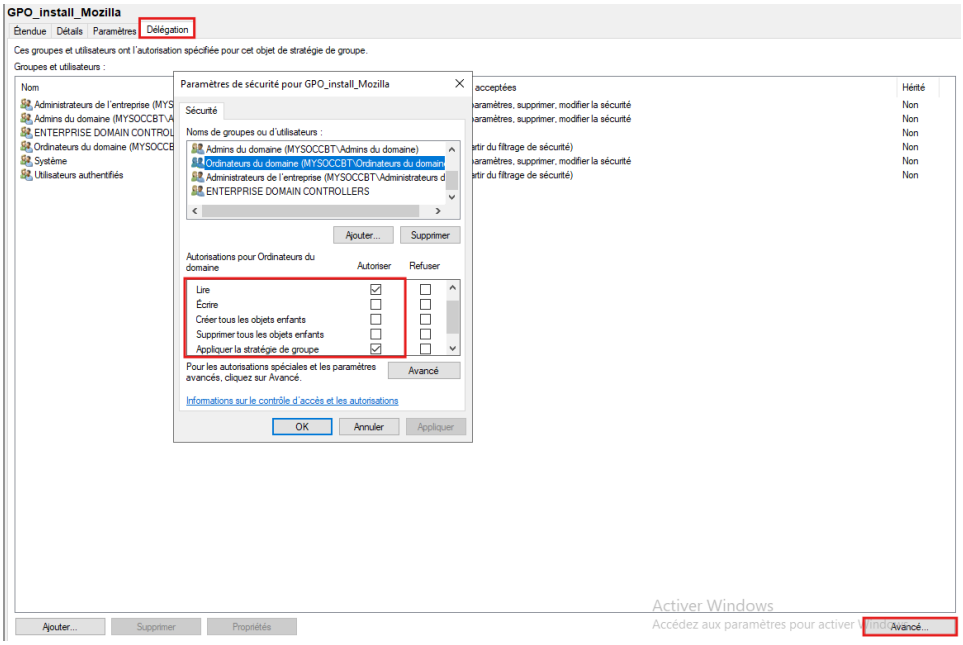
Afin d'installer Mozilla Firefox sur tous les postes du service technique je vais d'abord télécharger le logiciel sur le serveur via ce lien. Je déplace ensuite le fichier téléchargé dans un dossier partagé en lecture par tout le monde (a noté qu'il est important que le fichier d'installation soit en .msi).

Je créé une nouvelle OU Ordinateur / Technique où j'y glisse le poste client. Je vais ensuite créer une nouvelle GPO comme précédemment, dans l'OU Technique.

Clic droit > Créer un objet GPO dans ce domaine. J'appellerai GPO_install_mozilla. Clic droit sur la GPO puis chercher : Configuration ordinateur / Stratégie / Paramètres du logiciel / Installation de logiciel. Faire clic droit sur ce dernier puis Nouveau > Package. Pointer dans le dossier partagé précédemment créer et sélectionner le fichier d'installation.

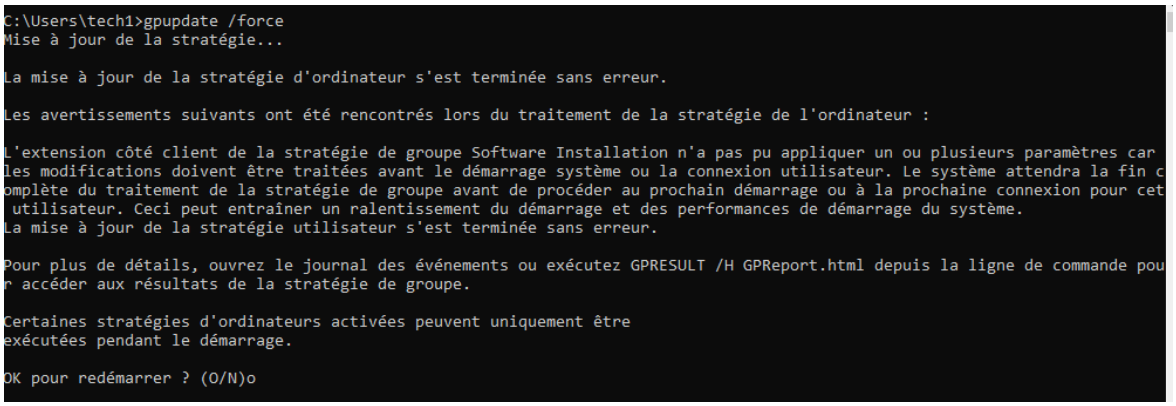
Faire bien attention au chemin d'accès au fichier : préférer "\\SRV01-SR2\Documents\Admin" à "C:\Users\Administrateur\Documents\Admin" pour que le poste client puisse y accéder.

Sur la GPO Je vais donner les autorisations nécessaires aux ordinateurs du domaine. Pour cela sélectionner la GPO puis aller dans l'onglet délégation et enfin avancé. Ajouter ordinateurs du domaine puis donner lui les autorisations de lectures et Appliquer les stratégies de groupes.



Je peux maintenant tester sur le poste client :

- Ouvrer une invite de commande et taper gpupdate /force.
- Lorsque cela vous est invité, répondre oui à l'invitation de redémarrer la machine.



- Une fois redémarré et connecté au compte utilisateur, nous pouvons apercevoir qu'un raccourci vers mozilla se trouve sur le bureau. Mozilla Firefox a été installé au démarrage.

Je peux également instaurer une option pour désinstaller le logiciel lorsque le PC est placé dans une autre OU que technique :

- Clic droit sur la GPO et Modifier. Clic droit sur Installation de logiciel puis Propriétés. Aller sur l'onglet Options avancées et cocher Désinstaller les applications lorsqu'elles se trouvent en dehors de l'étendue de la gestion.

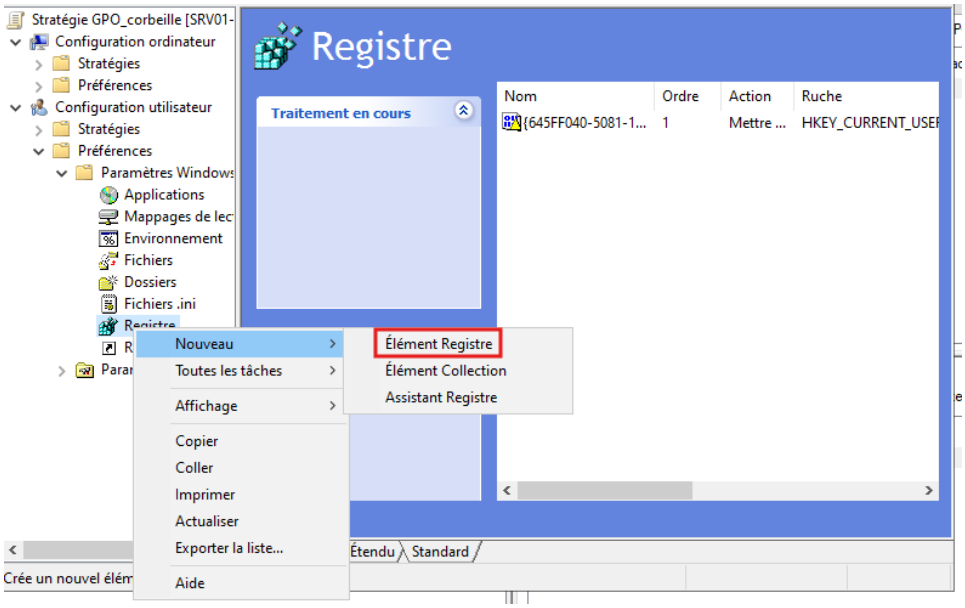
4- Suppression de l'icône de la corbeille

L'objectif de cette étape est de supprimer l'icône de la Corbeille sur le bureau de l'ensemble des utilisateurs, à l'exception du service R&D, conformément au cahier des charges. Cette action vise à uniformiser l'environnement de travail tout en maintenant une différenciation fonctionnelle pour le service de recherche et développement.

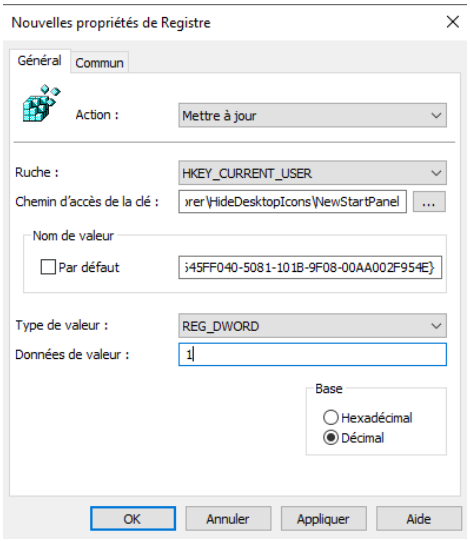
a) Création de la GPO

Une nouvelle stratégie de groupe a été créée dans la console de gestion des stratégies sous le nom GPO_corbeille. Elle a ensuite été liée à l'OU Services.

La configuration a été réalisé dans Configuration utilisateur > Préférence > Paramètres Windows > Registre.



Clic droit sur registre > Nouveau > élément registre. Remplir de cette manière.



Pour le chemin d'accès :

Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel

Pour tester son fonctionnement, je vais sur le poste client et sur une invite de commande faire gpupdate /force puis redémarrer. A la réouverture de session la corbeille aura disparu.

b) Exclusion du service R&D

Afin d'exclure le service R&D de cette GPO, je peux sélectionner la GPO puis aller dans l'onglet délégation.

Cliquer sur Avancé puis ajouter les groupes GD_R&D et GD_R&D_Chef. Je cocherai ensuite refuser d'appliquer les stratégies de groupe.

Si je me connecte à la session d'un utilisateur R&D sur le poste client, Je peux apercevoir la corbeille sur le bureau.

VII/ Bilan

1- Conclusion

Le TP a été mené à bien. L'Active Directory a été mis en place avec succès, avec redondance et DNS intégré. Les utilisateurs et groupes ont été créés et organisés selon le modèle AGDLP. Les dossiers partagés sont accessibles avec les droits adéquats, et les GPO ont permis d'appliquer les restrictions et logiciels spécifiques aux services. Les tests de validation ont confirmé la cohérence et la fonctionnalité complète de l'infrastructure.

2- Auto-évaluation

Le travail a été réalisé en respectant les contraintes et les besoins définis. La planification méthodique et l'organisation du déploiement m'ont permis de maintenir une cohérence dans la gestion des utilisateurs, des groupes et des ressources. La documentation complète permet de comprendre chaque étape et d'assurer une traçabilité efficace pour les futurs tests ou interventions.