Mr ROTH

08/11/2023

Compte rendu TP4

Active Directory - Serveur de fichier - Droits NTFS - GPO

TEWES Arnaud
BTS SIO SISR 1ÈRE ANNÉE

1. Introduction

Dans ce TP, j'ai procédé à la mise en place d'un domaine Active Directory avec création d'unités d'organisation, d'utilisateurs, de groupes et j'ai mis en place un serveur de fichier avec droits NTFS sur mes groupes d'utilisateurs. J'ai ensuite établi une stratégie de groupe pour que mes utilisateurs puissent avoir accès à mon partage de fichier en passant par un lecteur réseau sans avoir à taper le chemin UNC.

Dans un premier temps, j'ai installé les rôles Active Directory (AD DS) et DNS sur mon serveur, et je l'ai ensuite promu en contrôleur de domaine. J'ai ensuite pu spécifier un nom à mon domaine (étant donné que j'ai créé un tout nouveau domaine dans une toute nouvelle forêt).
J'ai ensuite configuré DNS pour qu'il fasse la résolution entre mon nom de domaine et l'adresse IP de mon contrôleur de domaine et inversement. En créant dans un premier temps une zone de recherche inversée, qui elle fera la résolution entre adresse IP et nom de domaine, puis en configurant les propriétés du serveur DNS pour qu'il écoute seulement sur IPv4 (comme je fonctionne en IPv4 dans mon cas).

Dans un second temps, j'ai organisé mes utilisateurs, groupes et ordinateurs dans différentes unités d'organisations que j'ai créées : une principale sur le domaine avec le nom de l'organisation (pour laquelle je travaille virtuellement), et dans celle-ci j'en ai créé trois autres pour les ordinateurs, utilisateurs et groupes. Cela me permet d'avoir une base de travail plus claire pour la création de mes utilisateurs et de mieux m'y retrouver lorsque je voudrais appliquer des stratégies de groupes sur mes UOs.

Enfin, j'ai ajouté le rôle serveur de fichiers à mon serveur, créé des dossiers à partager entre les utilisateurs ou groupes d'utilisateurs, puis géré leurs droits NTFS respectivement pour chaque groupe, avec un groupe « direction » ayant un peu plus de droit que les autres.

Dans mon cas, j'ai utilisé le même serveur pour AD et pour le serveur de fichier car je suis en test. Mais dans un cas réel, il est important d'utiliser un serveur dédié pour chaque rôle que l'on souhaite installer pour des raisons de sécurité.

Prérequis

- **Installation sur Windows Server**

- **Adresse IP fixe et serveur DNS** : Active Directory a besoin de DNS pour fonctionner car il permet aux clients de localiser les contrôleurs de domaine, ou aux contrôleurs de domaine de se localiser entre eux. Sans DNS, les clients ne pourraient pas trouver les contrôleurs de domaine et donc ne pourraient pas être identifiés. DNS permet de faire la conversion du nom de domaine vers IP et inversement. Sans une adresse IP fixe et DNS, il serait impossible de se connecter au domaine

- **Matériel** : Un processeur 1,4 GHz 64 bits ou plus rapide, 512 Mo de RAM ou plus, 32 Go d'espace disque ou plus, et un adaptateur réseau Ethernet sont recommandés.

Pourquoi installe-t-on Active Directory ?

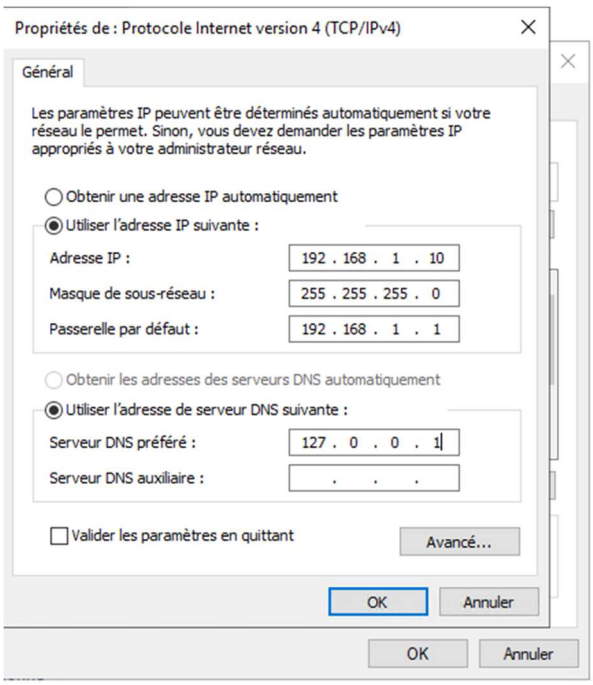
Active Directory est un service d'annuaire qui utilise le protocole LDAP (Lightweight Directory Access Protocol). Il est utilisé pour centraliser, référencer, identifier et authentifier les utilisateurs, les ordinateurs ou tout objet dans un domaine Active Directory. Il permet de simplifier l'administration des utilisateurs, de sécuriser l'accès aux ressources et de mettre en place des stratégies de groupe pour appliquer un paramétrage sur des unités d'organisation (une UO est un dossier dans lequel on range nos objets AD). On l'installe pour faciliter la gestion des utilisateurs et des ressources au sein d'un réseau d'entreprise.

Un serveur de fichiers est un serveur qui permet de centraliser un partage de fichiers/dossiers dans un réseau. Grâce à lui, nous pouvons stocker les ressources à un seul et même endroit et pouvons gérer les droits d'accès de manière centralisée grâce à l'annuaire Active Directory.

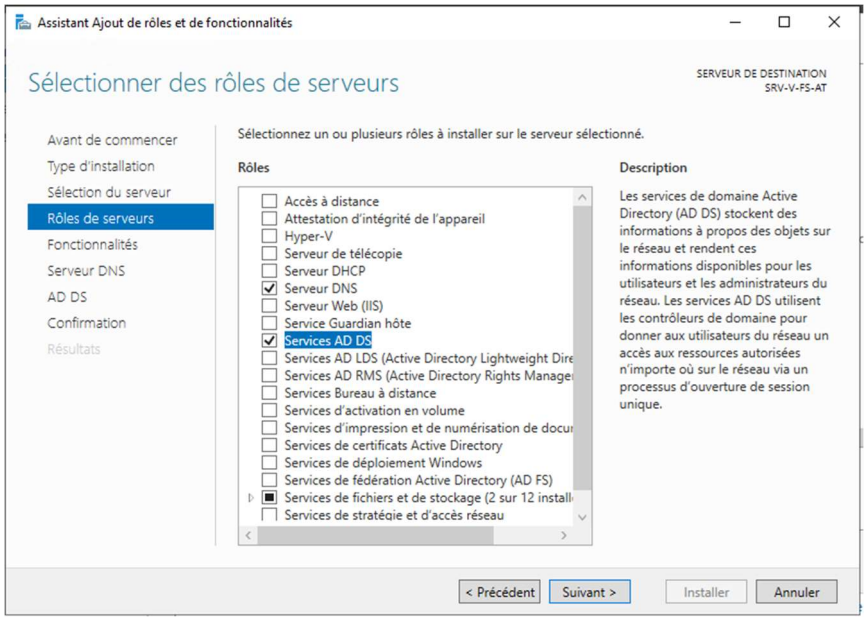
Une stratégie de groupe permet quant à elle, de créer un paramétrage sur nos unités d'organisations (Nous pouvons créer des UOs dans des UOs si on veut des paramétrages pour certains utilisateurs seulement). Nous pouvons par exemple, définir le même fond d'écran pour tout le monde, configurer un lecteur réseau, déployer un logiciel, forcer les MAJ Windows update, etc…

2. Mise en place et procédé pas à pas

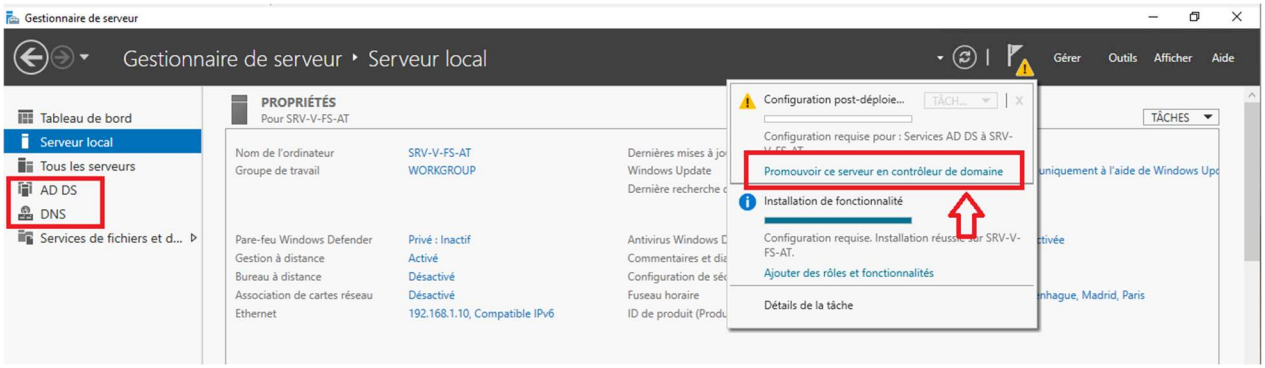
Dans un premier temps il faut définir un adresse IP fixe sur notre serveur ou l'on va installer AD qui deviendra le contrôleur de domaine. Dans mon cas, j'ai défini 192.168.1.10/24, puis définir en serveur DNS préféré nous-même, qui peut aussi se noter 127.0.0.1 (car notre contrôleur de domaine fera aussi serveur DNS, car AD en a besoin pour fonctionner comme je l'ai mentionné plus haut).



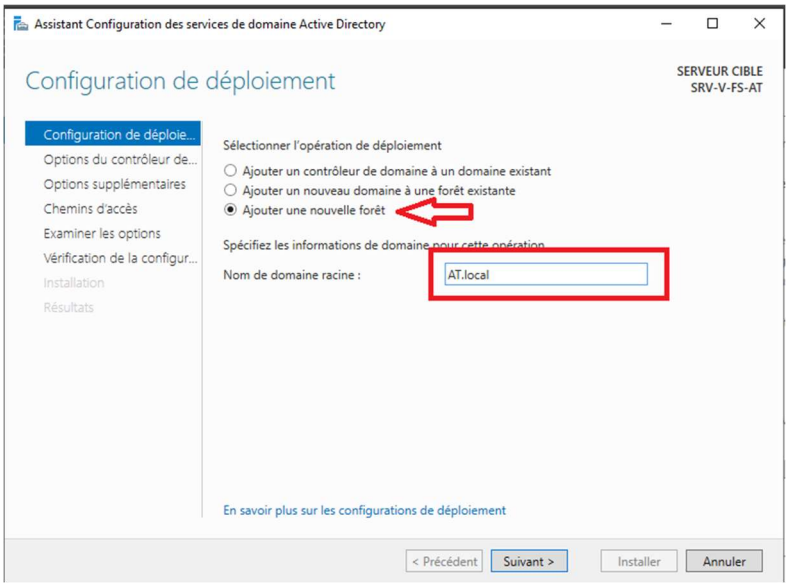
Ensuite, nous pouvons passer à l'installation des rôles en passant par le gestionnaire de serveur, ajout de rôles et fonctionnalités, et cocher les rôles « serveur DNS » et « Services AD DS », nous pouvons ensuite valider et faire suivant pour terminer l'installation.



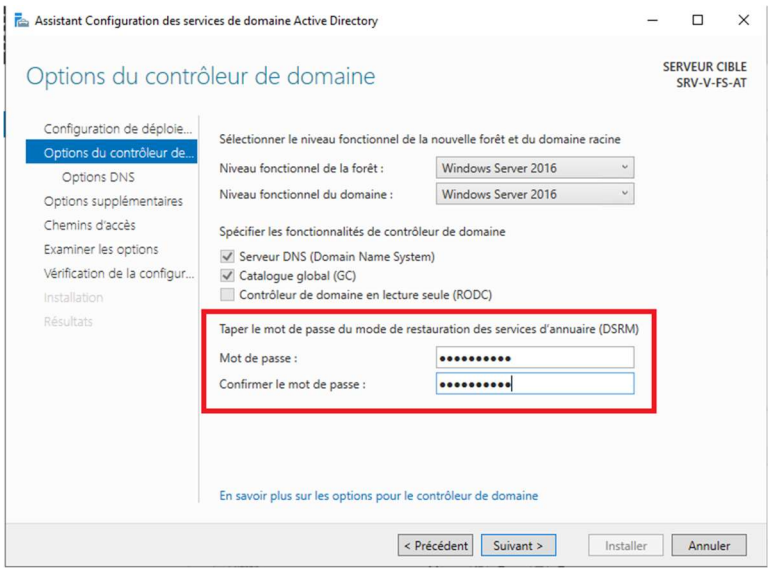
Une fois les rôles installer, nous avons deux nouveaux onglets à gauche sur notre gestionnaire de serveur « AD DS » et « DNS », qui certifient que les rôles sont bien installés. Et nous avons un petit symbole jaune « attention » en haut à droite qui nous avertit qu'il faut finir la configuration d'Active Directory (nous devons le passer en tant que contrôleur de domaine). Il faut donc cliquer dessus et cliquer sur « promouvoir ce serveur en contrôleur de domaine ».



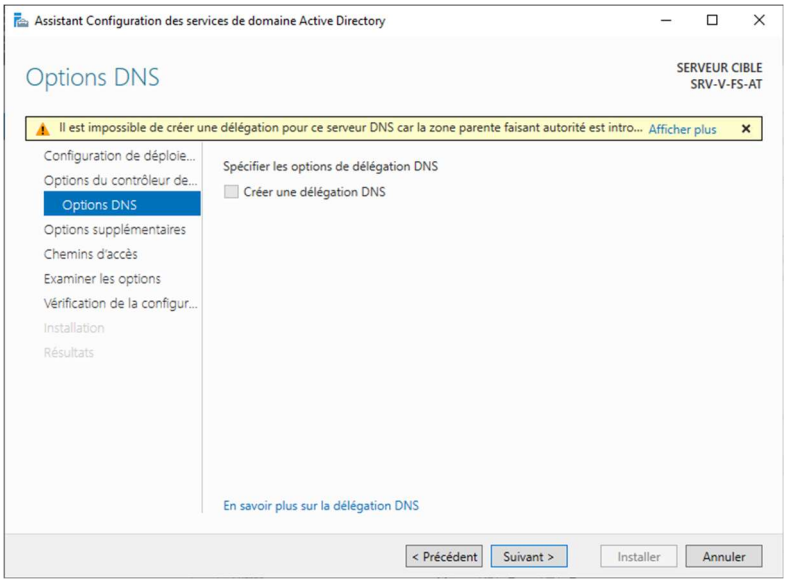
Maintenant le configurateur nous demande si l'on veut ajouter le contrôleur de domaine à un domaine existant, si l'on veut ajouter un nouveau domaine à un foret existant, ou si l'on veut créer une toute nouvelle forêt. Dans notre cas, c'est une toute nouvelle foret étant donné que c'est notre premier domaine, nous prenons donc la dernière option. Il faut maintenant définir un nom à notre domaine, étant donné que c'est un domaine local, il ne faut pas mettre un nom trop compliqué ni trop long, et finir par « .local » ou « .lan » pour ne pas le confondre avec un nom de domaine publique.



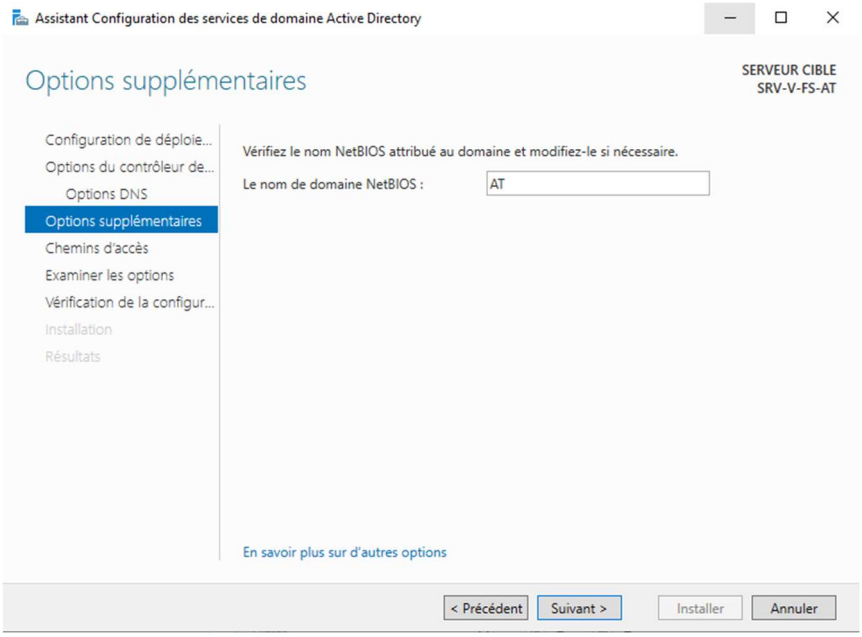
L'installeur nous demande si l'on veut que le contrôleur de domaine soit rétro compatible avec d'anciennes versions de Windows Server, dans notre cas nous n'en avons pas d'autres donc nous laissons les options par défaut. Nous pouvons aussi spécifier si nous voulons qu'il soit aussi serveur DNS, dans notre cas vu que c'est le premier il doit obligatoirement être serveur DNS aussi, si on veut qu'il soit catalogue global (qu'il stock tous les objet de mon annuaire), pareil que pour DNS vu que c'est notre premier il doit être CG, et l'option « contrôleur de domaine en lecture seule » permet d'avoir un contrôleur de domaine où l'on ne peut faire aucune modification, il répondra seulement au demande d'authentification ou autres des clients (utiles si l'on veut le mettre dans un site distant). Nous devons ensuite définir un mot de passe qui nous servira à la restauration en cas de panne d'Active Directory, seul ce mot de passe pourra être utilisé. (Il permet d'accéder en admin au serveur)



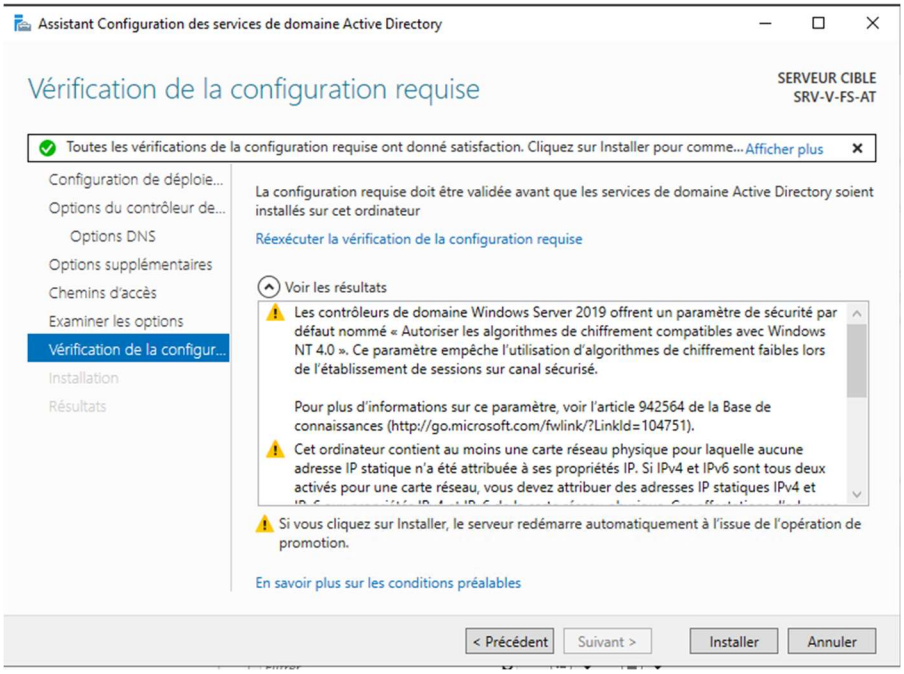
Il nous est ensuite possible de créer une délégation DNS (Si l'on veut qu'un autre serveur gère DNS), ce n'est pas notre cas, on peut donc cliquer sur suivant



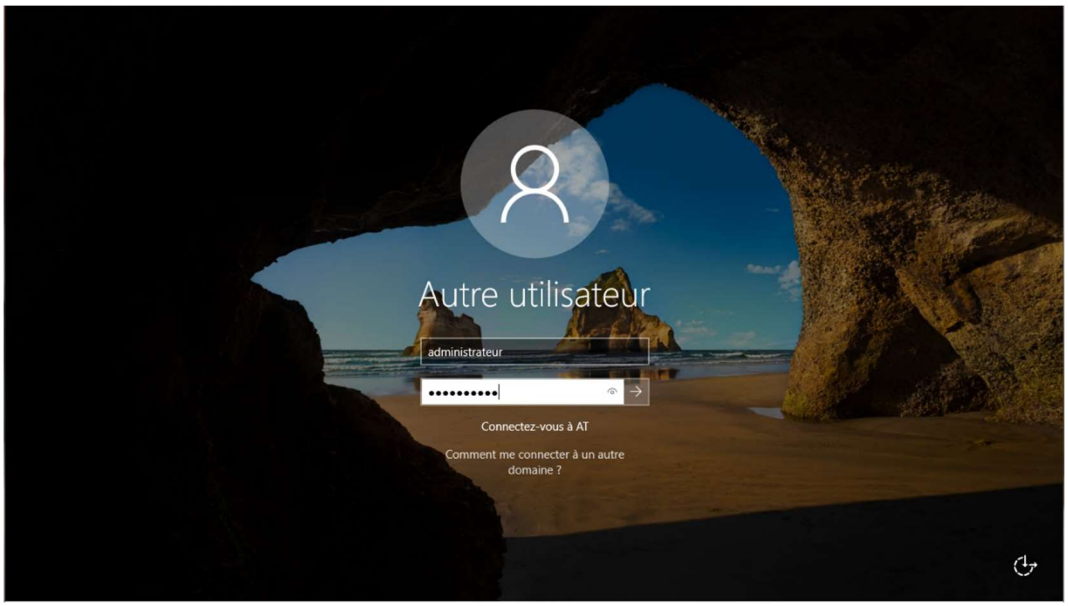
Il faut ensuite attendre que l'installateur définisse le nom de domaine NetBIOS (alternative à DNS plutôt ancienne)



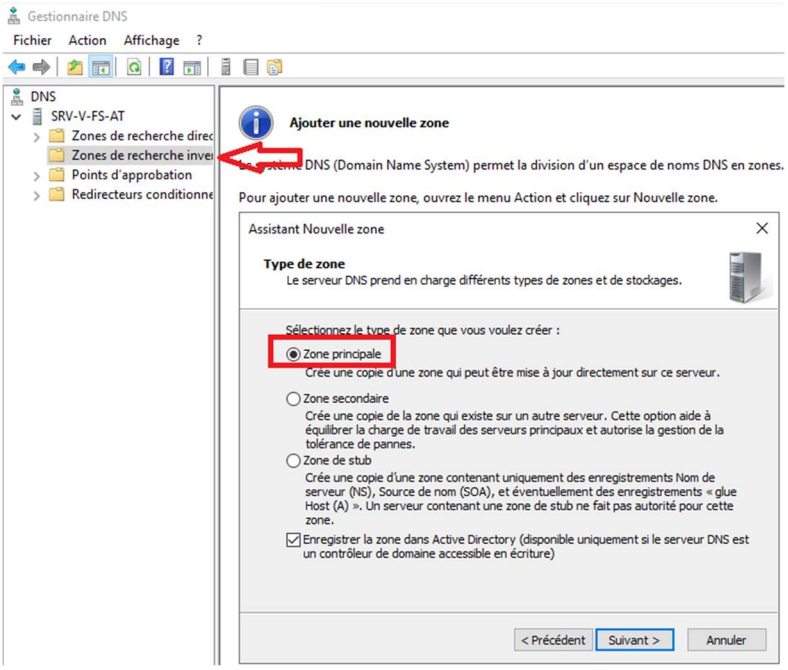
Maintenant, le configurateur nous avertit que nous n'avons pas défini de délégation DNS, et que nous n'aurons pas de rétrocompatibilité avec les anciens OS Windows Server.



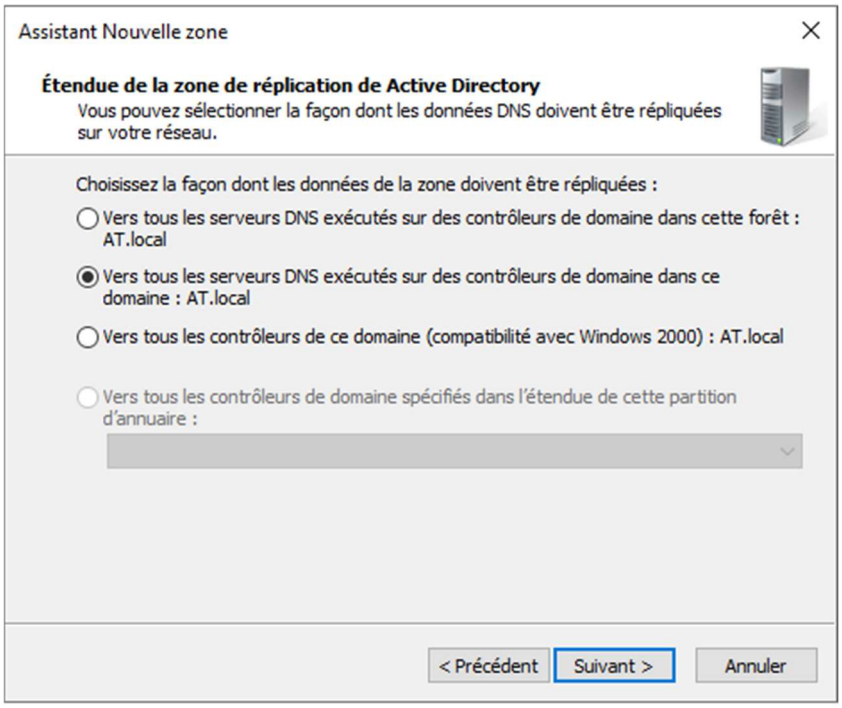
Le serveur redémarre, applique les modifications que l'on a effectué et nous pouvons maintenant nous connecter en tant qu'administrateur sur le domaine



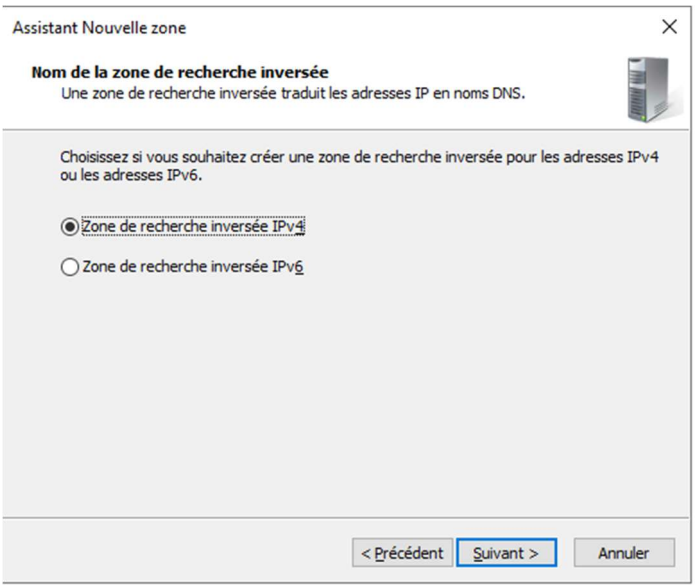
Nous passons à la configuration du DNS, il faut dans un premier temps définir une zone de recherche inversée, qui fera la liaison entre l'adresse IP et le nom de domaine pour tous les objets de notre domaine. Il faut donc aller dans les paramètres DNS, clic droit sur « zone de recherche inversé » et crée une nouvelle zone « zone principale »

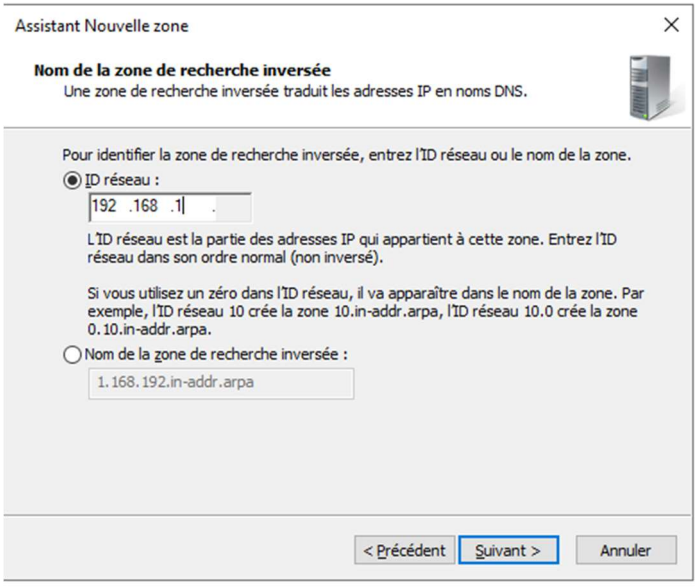


Nous pouvons définir si l'on veut que la zone de recherche inversée soit répliqué sur le domaine ou sur la forêt, nous pouvons laisser l'option par défaut et cliquer sur suivant.

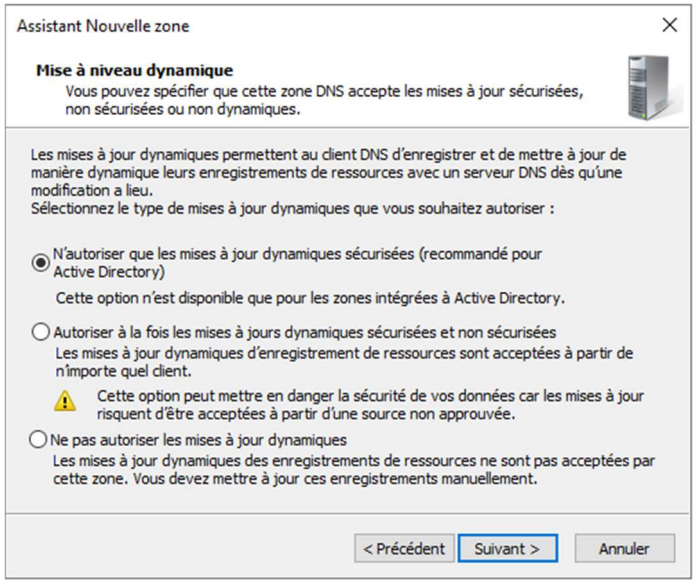


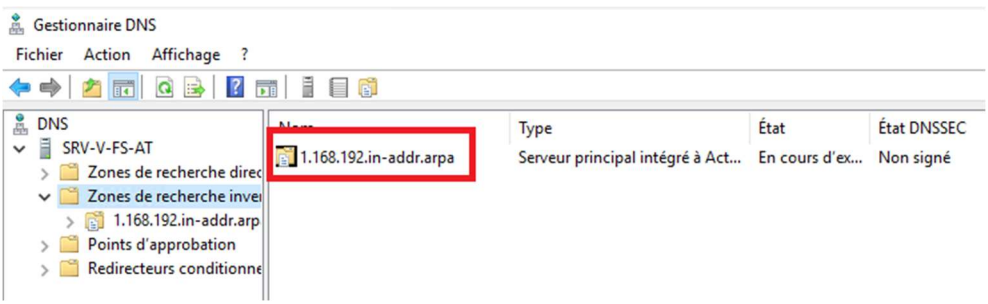
Nous indiquons sur quel type d'IP nous travaillons (IPv4) dans notre cas et spécifions dans la fenêtre d'après l'adresse réseau de l'IP de votre serveur (dans notre cas 192.168.1).



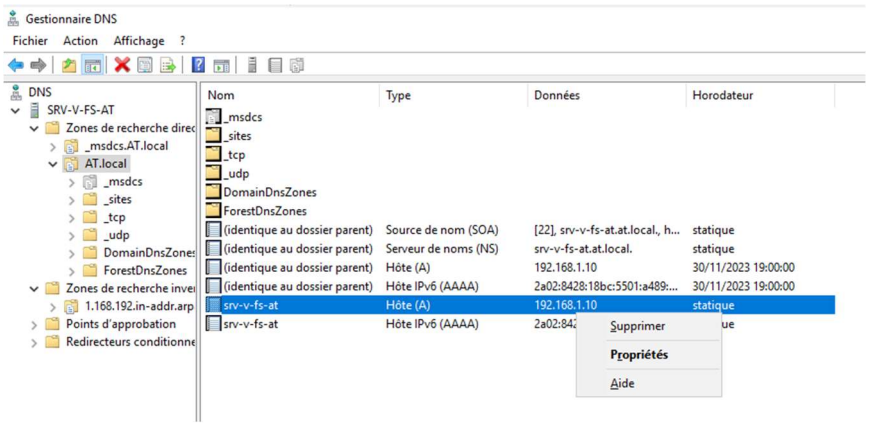


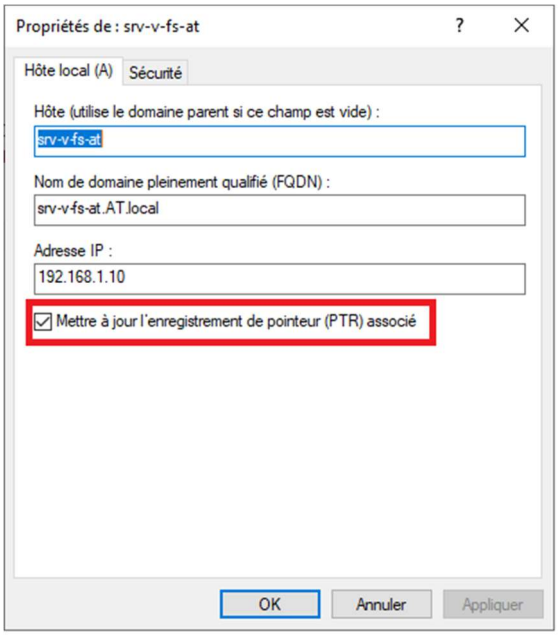
Nous pouvons laisser cocher la case par défaut qui est recommandé pour Active Directory et qui permettra que le serveur DNS mette à jour les enregistrements de ressources dès qu'une modification à lieu sur le domaine, puis nous terminons la configuration. La zone de recherche inversée est correctement paramétrée et nous le voyons dans la zone avec notez l'IP du réseau à l'envers.



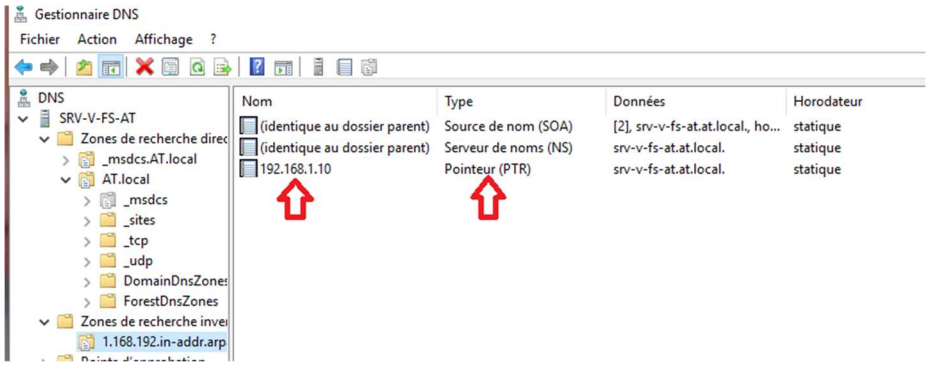


Nous devons maintenant aller dans la zone de recherche direct, faire un clic droit sur notre serveur est cocher la case « Mettre à jour l'enregistrement de pointeur PTR associé » qui permettra à notre zone de recherche inversé de retourner le nom DNS d'un hôte à partir de son adresse IP.

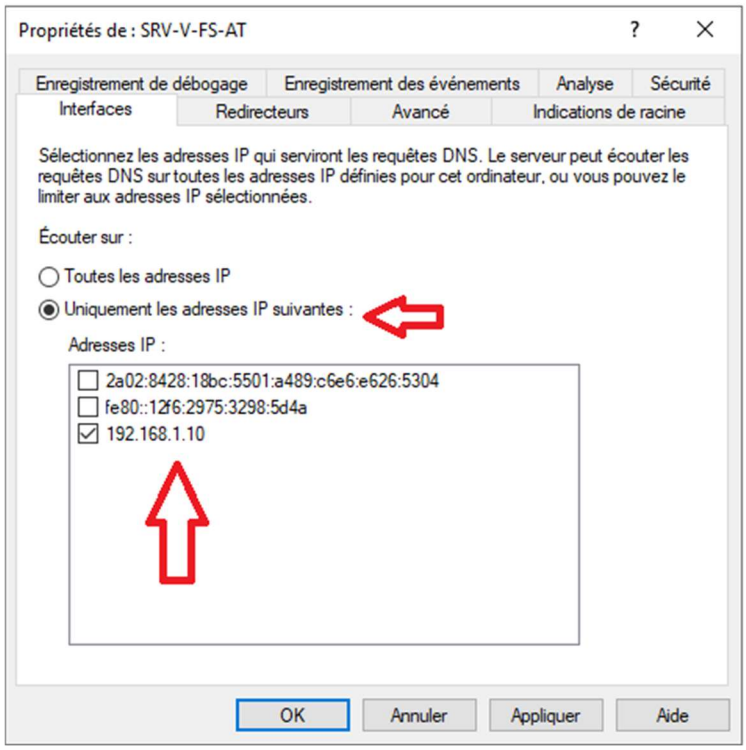




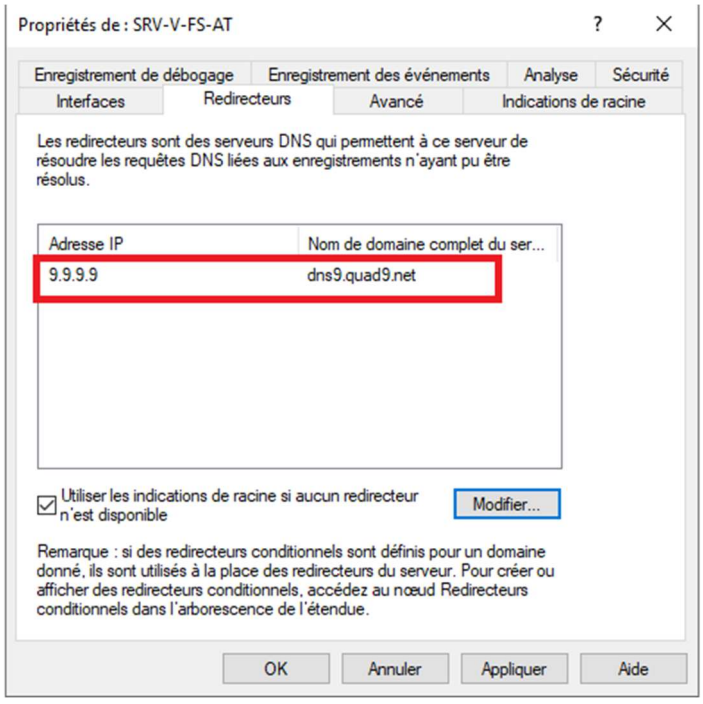
Et lorsque l'on retourne dans la liste de zone de recherche inversé, on voit bien que le PTR a été pris en compte



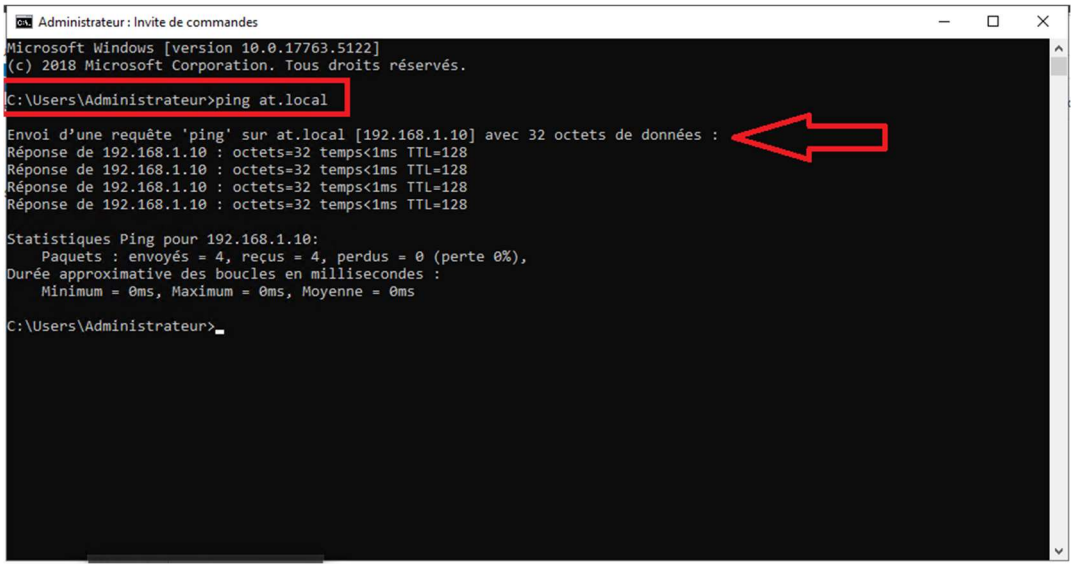
Nous pouvons maintenant terminer la configuration du serveur DNS en allant dans les propriétés du serveur DNS, dans l'onglet « Interface » cocher la case « Uniquement les adresses IP suivantes » et ne laisser cocher que les cases qui nous intéressent avec l'IP de notre serveur, ce qui permettra au serveur DNS de n'écouter que les requêtes provenant des adresses IP spécifié.



Ensuite, nous pouvons définir un redirecteur, c'est un autre serveur DNS qui se trouve coté internet cette fois, que notre serveur DNS interrogera s'il ne connaît pas les noms de domaine que nous lui demandons.



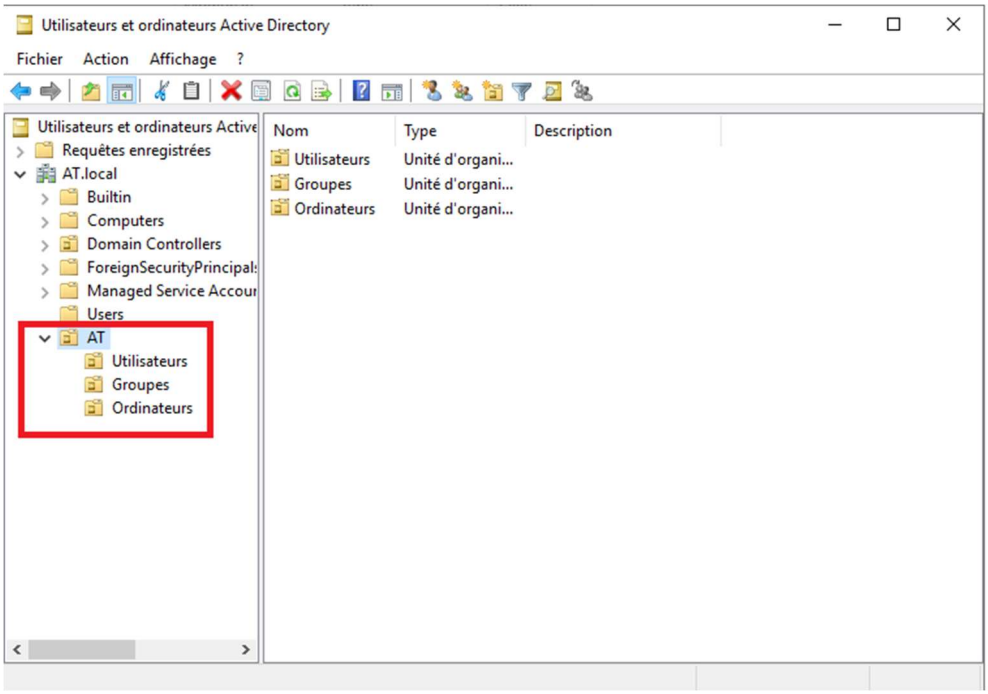
La configuration DNS est maintenant terminée, nous pouvons tester un ping vers notre nom de domaine pour vérifier que le serveur DNS répond bien aux requêtes et fait bien la conversion vers la bonne adresse IP



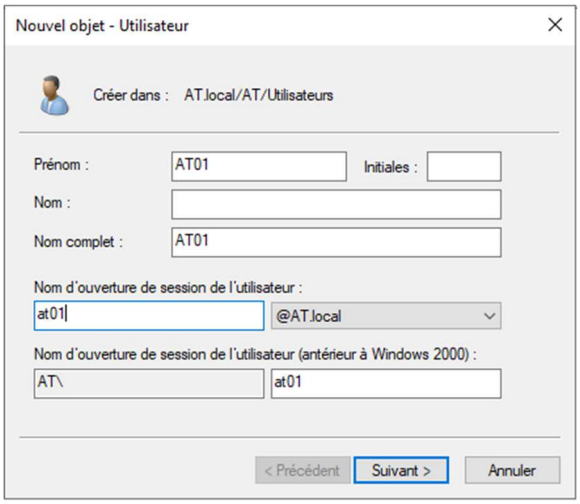
Le serveur DNS fait bien la conversion nom de domaine vers IP, tout fonctionne correctement.

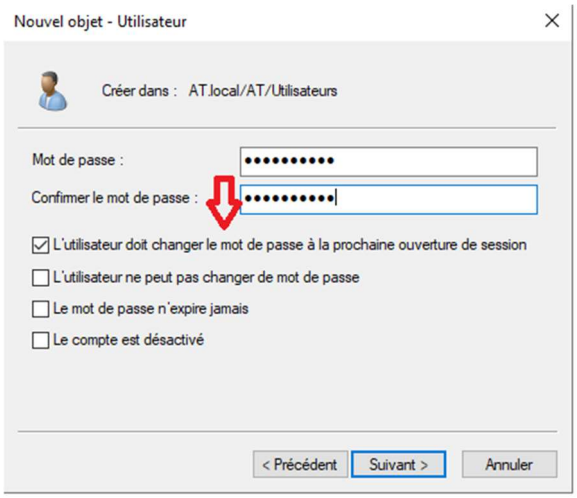
Active Directory

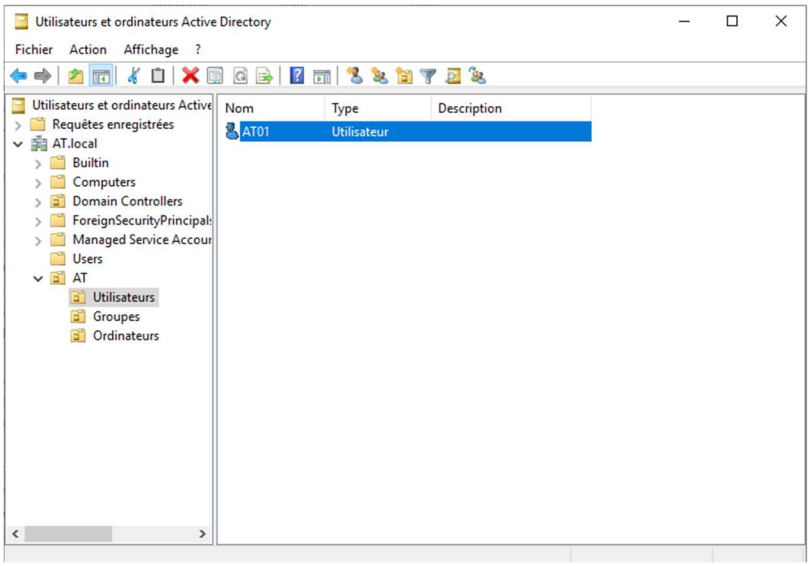
Nous pouvons donc passer maintenant à la configuration de nos premiers objets (utilisateurs, groupes, UO) sur Active Directory. Dans un premier temps, nous allons créer des unités d'organisation propre et claire pour mieux nous y retrouver.



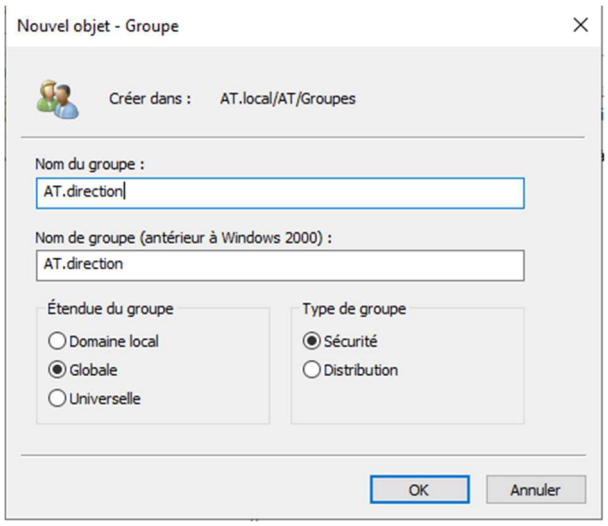
Ensuite, nous pouvons créer notre premier utilisateur du domaine. Nous créons l'utilisateur AT01, et spécifions qu'il doit changer son mot de passe à la première connexion (pour qu'il puisse définir son propre mot de passe).

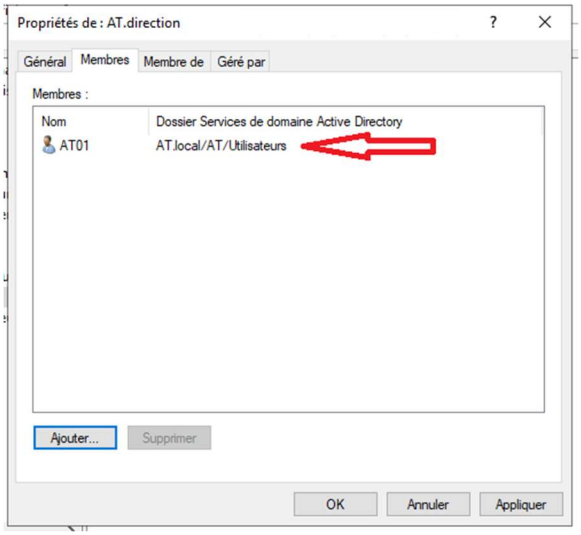






Nous allons créer un groupe, on peut imaginer que AT01 fait partie de la direction, nous créons donc le groupe AT.direction (les groupes permettent de gérer les droits). Nous ajoutons donc AT01 au groupe AT.direction (chacun sont dans leurs UO respective)



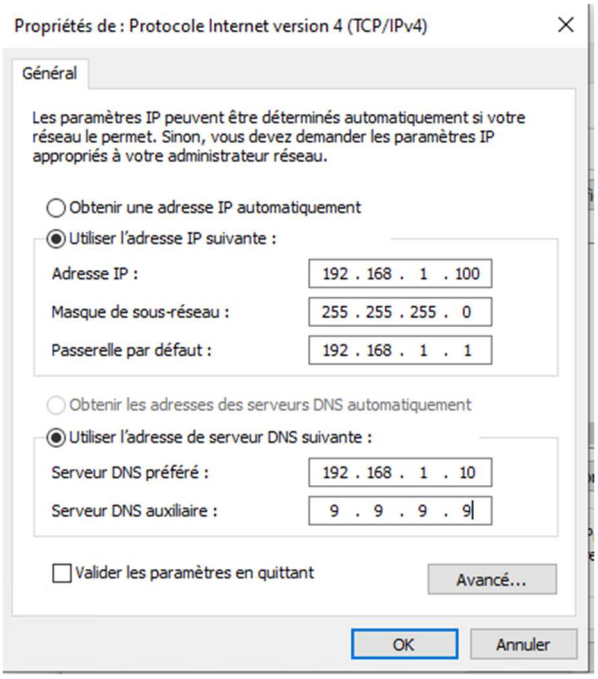


Notre utilisateur et notre groupe sont maintenant bien créer un sein de notre domaine Active Directory.

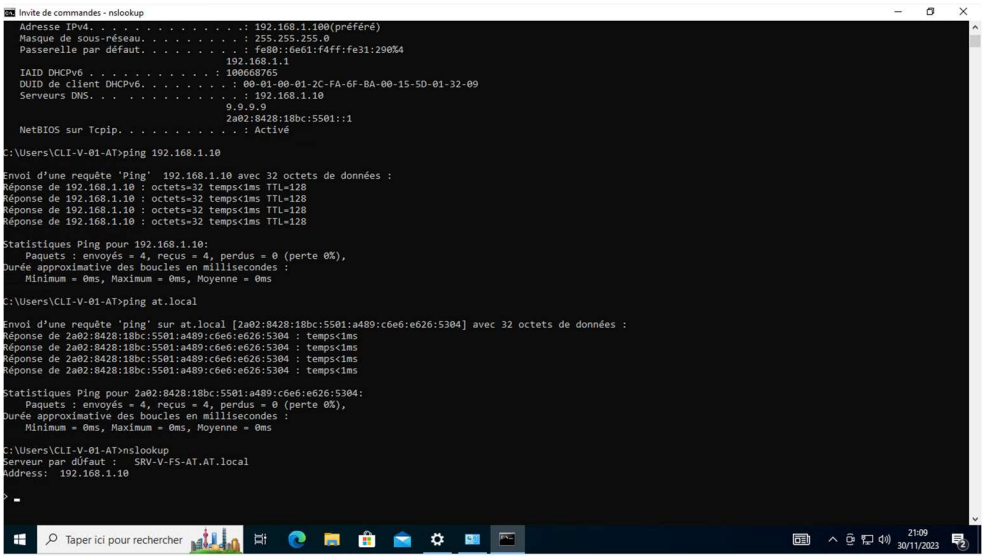
Client pour tests

Nous passons maintenant sur une machine cliente pour l'intégrer au domaine et vérifier qu'elle peut se connecter avec l'utilisateur que nous venons de créer.

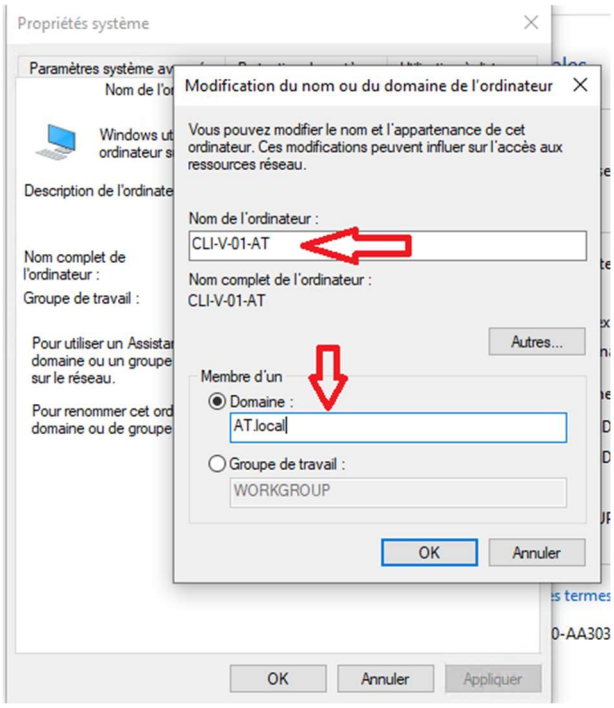
Dans un premier temps, il faudra de nouveau spécifier une adresse IPv4 fixe pour notre machine cliente qui fait partie de la même adresse réseau que notre serveur contrôleur de domaine (pour qu'ils puissent communiquer), et dans la partie « DNS préféré », nous pouvons maintenant définir l'adresse IP de notre contrôleur de domaine (192.168.1.10) qui fait aussi serveur DNS maintenant et peut donc répondre aux requête concernant notre domaine, et dans DNS secondaire, un serveur DNS public tel que 9.9.9.9.



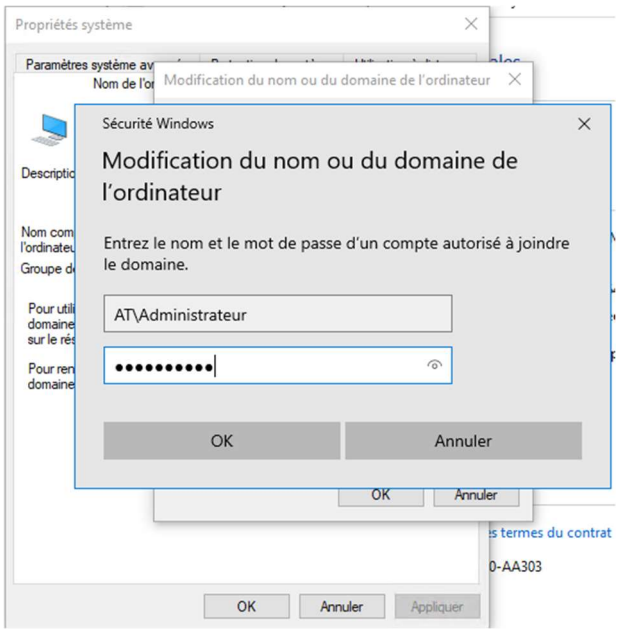
Une fois cela valider, nous pouvons tester si le serveur répond et si le DNS fonctionne correctement en faisant un ping sur le nom de domaine que nous avons créé. Et vérifier avec la commande « nslookup » qui interroge notre serveur DNS et nous fait le rapprochement entre l'IP du contrôleur de domaine et le nom de domaine.

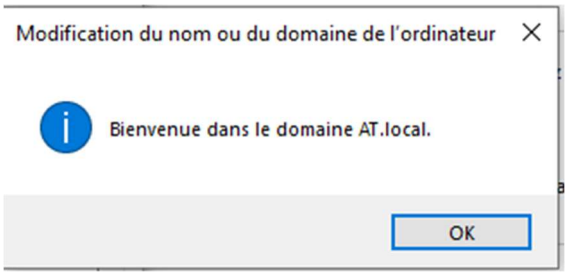


Le serveur répondant correctement à nos requêtes, nous pouvons maintenant ajouter l'ordinateur client au domaine. Il faut tout d'abord allez dans le gestionnaire de fichier Windows ou l'on a le disque local C:, clic droit et allez dans les propriété. Sur cette page, nous avons la possibilité de changer le nom du PC (ce que nous allons faire pour mieux le retrouver ensuite dans Active Directory, il faut qu'il ait un nom unique et reconnaissable au sein du domaine, pour une meilleure gestion), et dans la case juste en dessous cocher « membre d'un domaine » et spécifier le nom du domaine que l'on veut rejoindre.

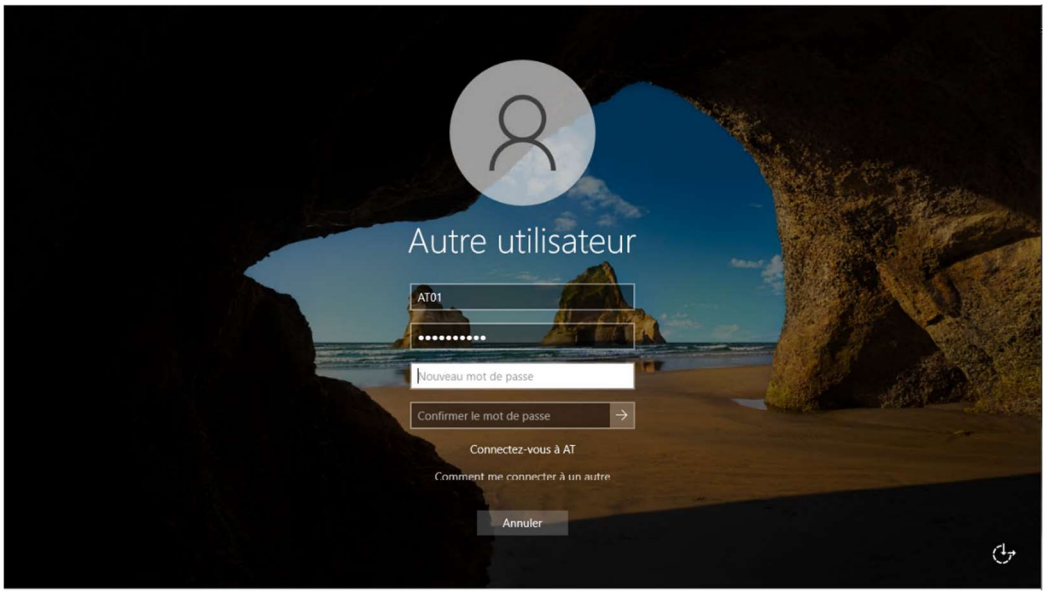


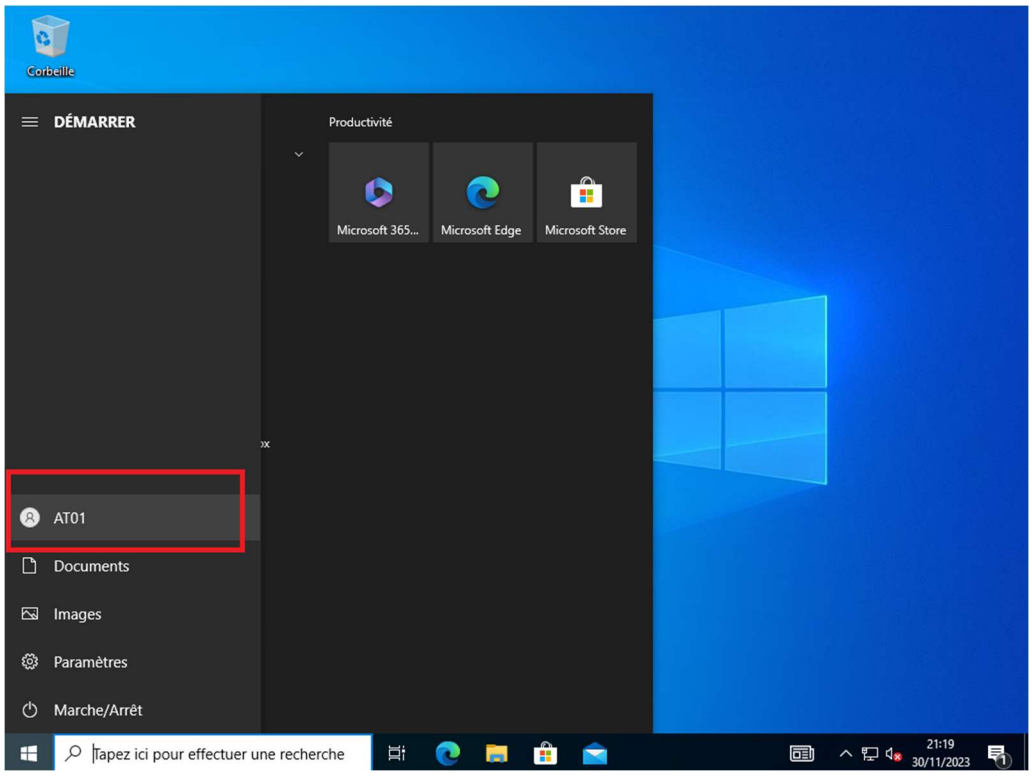
Le domaine nous demande un utilisateur autorisé à nous faire intégrer le domaine, typiquement le compte administrateur du domaine et sur Windows cela se note « AT\Administrateur » qui veut dire l'administrateur du domaine « AT ». Nous validons et rejoignons donc notre domaine !





Le PC client redémarre, et nous pouvons essayer de nous connecter avec l'utilisateur AT01 que nous avons créé juste avant.

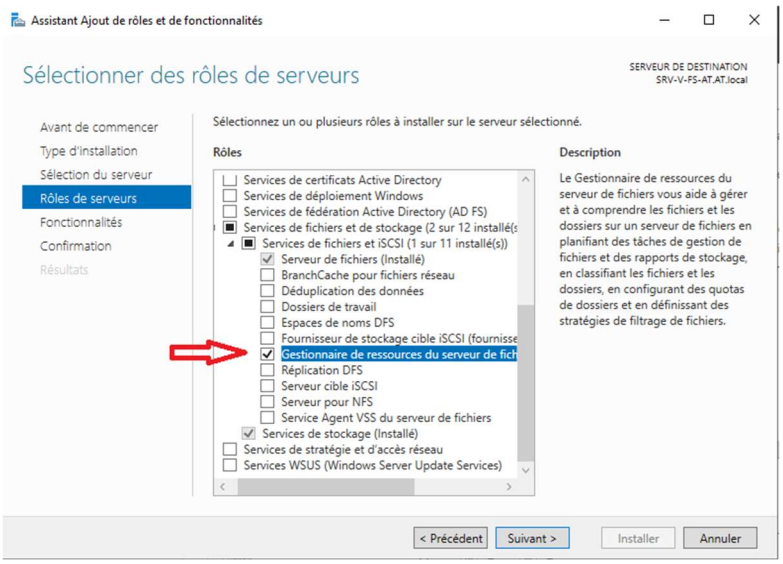




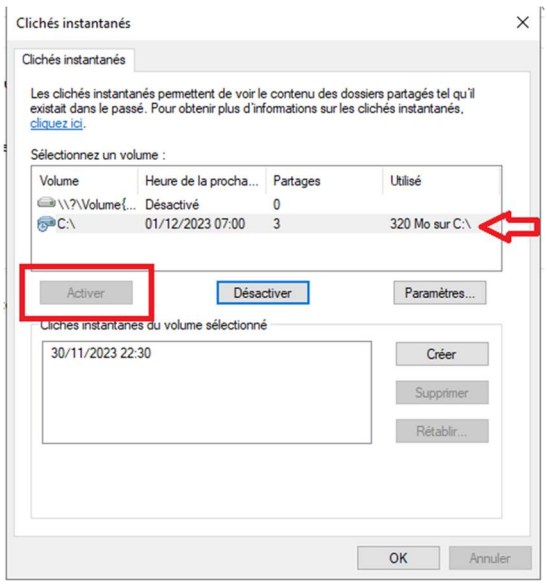
Le PC client à bien rejoint le domaine et nous pouvons nous connecter sur ce PC avec l'utilisateur du domaine que nous avions créé préalablement sur Active Directory. Nous avons toujours la possibilité de nous connecter en local avec le compte local du PC si nécessaire.

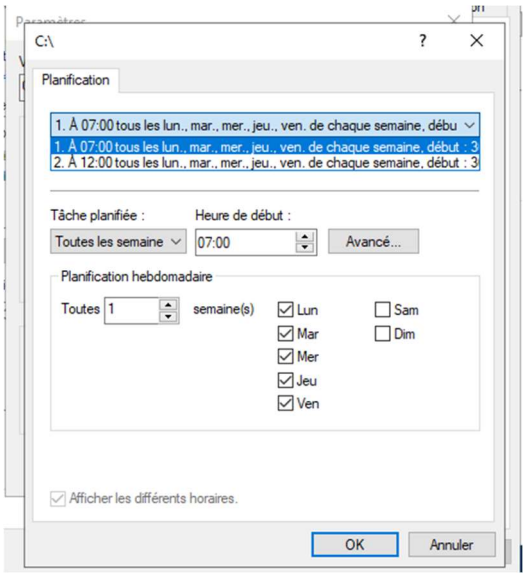
Serveur de fichier + droit NTFS

Le PC client ayant bien rejoint le domaine, nous allons maintenant ajouter le rôle serveur de fichier à notre serveur Active Directory (Encore une fois, dans un cas réel il est important de créer un serveur dédié pour chaque rôle que nous installons, mais dans notre cas comme nous sommes en test, nous faisons tout sur le même serveur).
Comme pour les rôles Active Directory, nous nous rendons sur le gestionnaire de serveur, ajout de fonctionnalité. Le rôles serveur de fichier étant déjà installé de base, nous avons simplement besoin de rajouter le gestionnaire de ressource du serveur de fichier pour ce serveur-là.

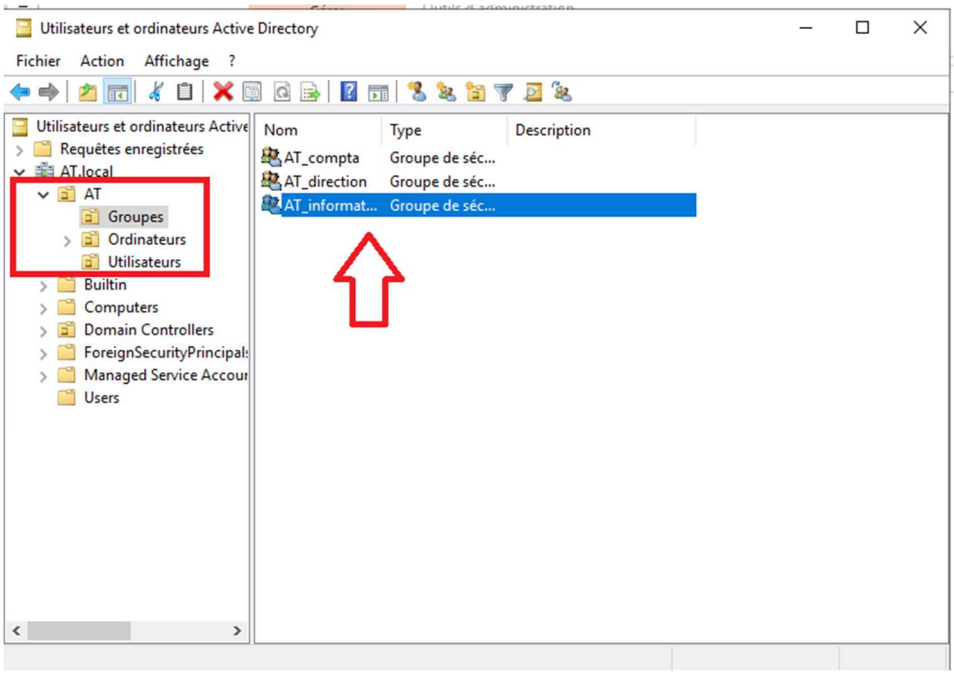


Une fois cela fait, nous devons nous rendre dans le gestionnaire de fichier, et en faisant un clic droit sur le « disque local C: », nous avons la possibilité d'activer les clichés instantanée. Les clichés instantanés est une technologie Windows qui nous permettent d'avoir un retour en arrière possible sur l'ensemble du disque dur, ou sur l'ensemble de la machine. Cela crée une sauvegarde du système au moment où le cliché est pris. En les activant, nous avons un nouvel onglet dans les propriétés de chaque dossier et sous dossier d'où son activé les clichés instantanée « version antérieur ». Très utile lorsqu'on fait des modifications et que l'on souhaite revenir en arrière. Nous avons également la possibilité de planifier à quelles fréquences sont pris les clichés.

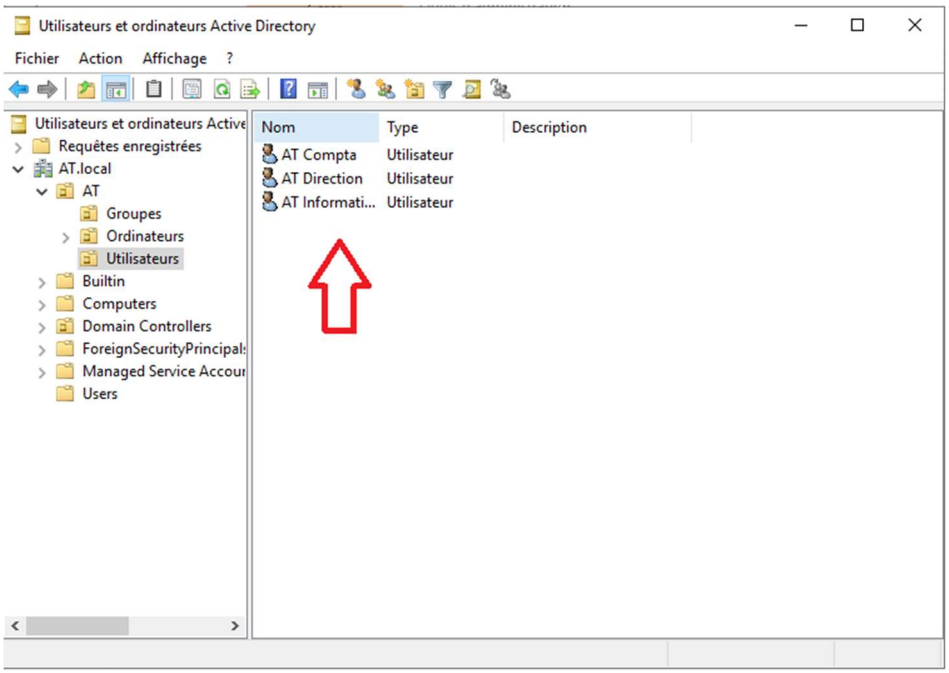




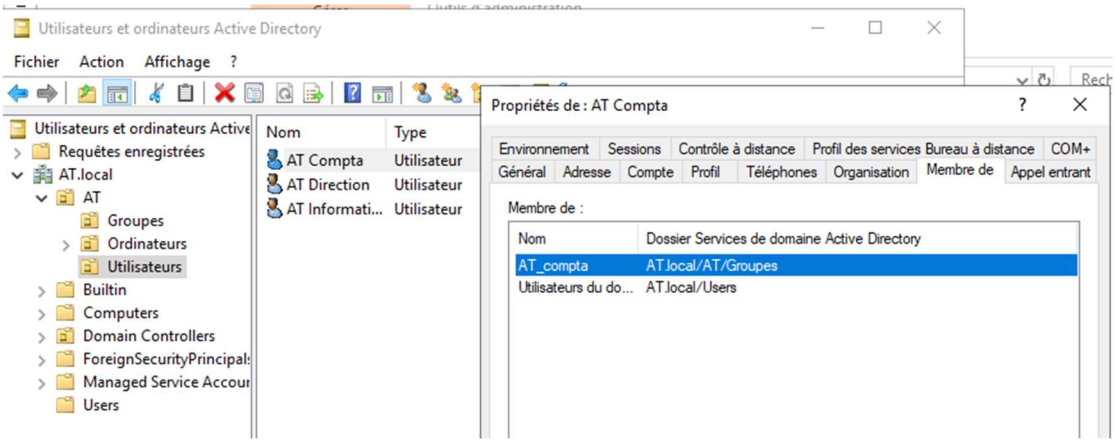
Nous pouvons maintenant aller dans les paramètres Active Directory, retrouver la configuration des unités d'organisation précédente que nous avions créé (quelques étapes au-dessus). J'ai décidé de supprimer l'utilisateur « AT01 » et de reprendre sur une base saine, en créant de nouveaux utilisateurs et groupes, pour pouvoir gérer leurs droits de manière plus compréhensible. Dans un premier temps, j'ai créé trois groupes (un par service).



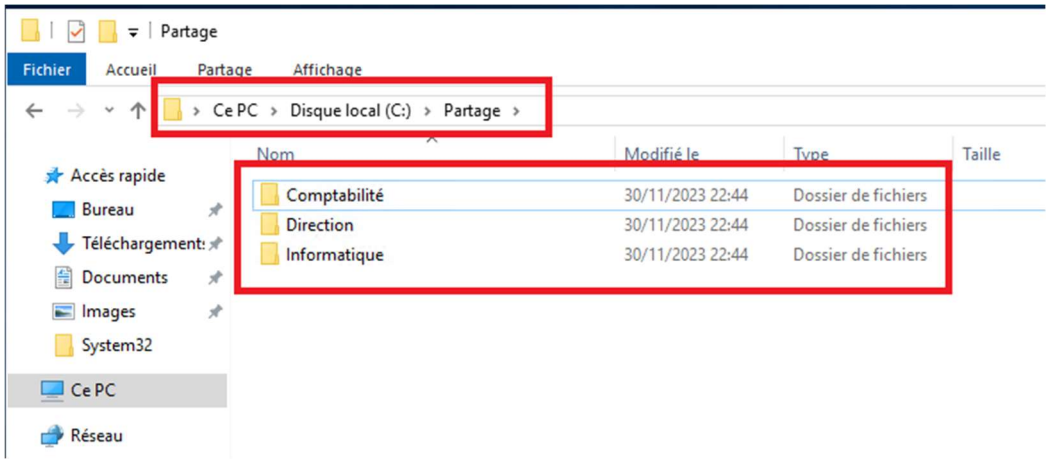
Puis, j'ai créé trois nouveaux utilisateurs (un par groupe).



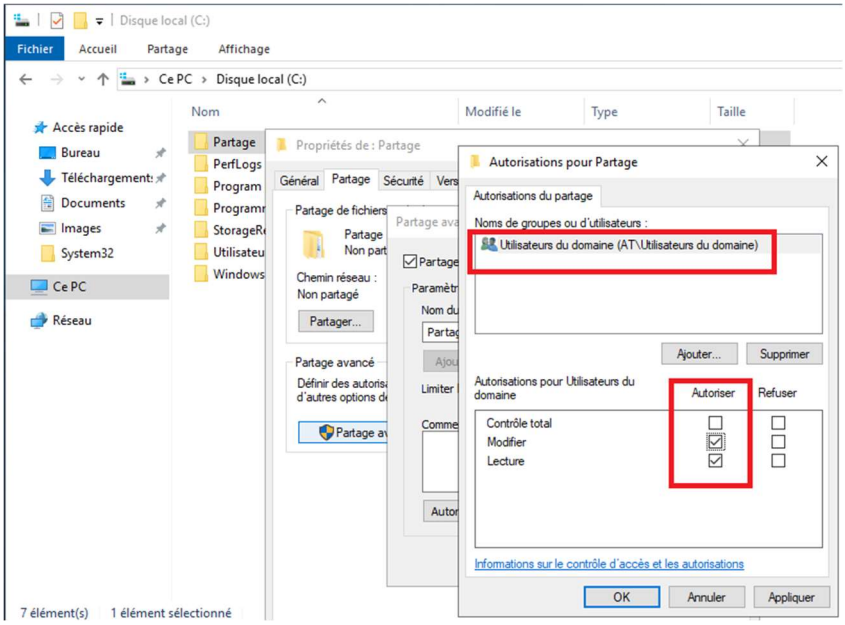
J’ai ensuite ajouté les utilisateurs à leurs groupes respectifs (les groupes nous permettent de gérer les droits de manière plus simple, sans avoir à gérer les droits pour chaque utilisateur un par un, alors qu’une stratégie de groupe s’applique uniquement sur des unités d’organisation).



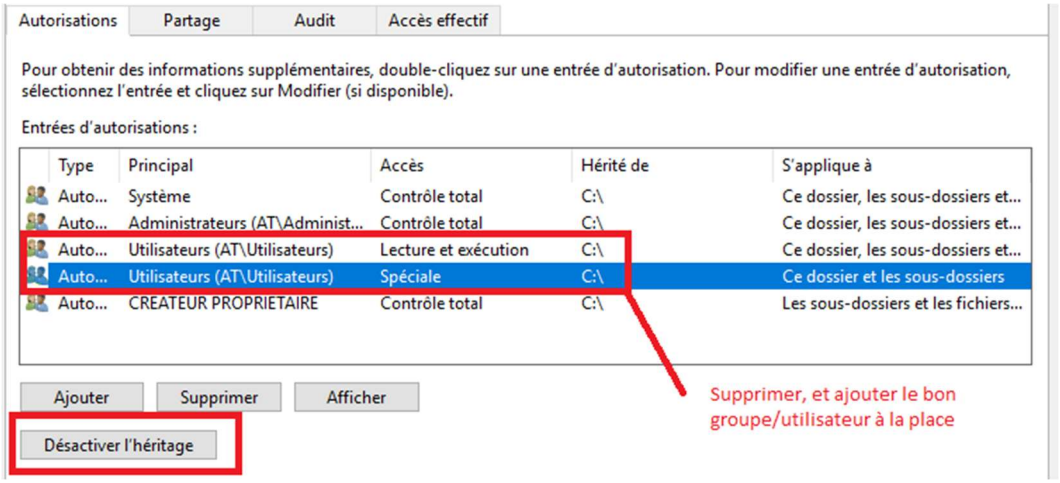
Nous pouvons maintenant créer les dossiers à partager. Il est recommandé de créer les dossiers à partager à la racine d’un disque dur pour éviter les chemins d'accès trop long et d’atteindre la limite de caractère imposée par Windows lorsqu’on voudra y accéder. Nous créons donc le dossier partage à la racine de notre disque dur, puis dans le dossier “partage”, nous pouvons créer un dossier pour chaque groupe d’utilisateur que nous avons créé (un pour compta, un pour direction, un pour informatique).

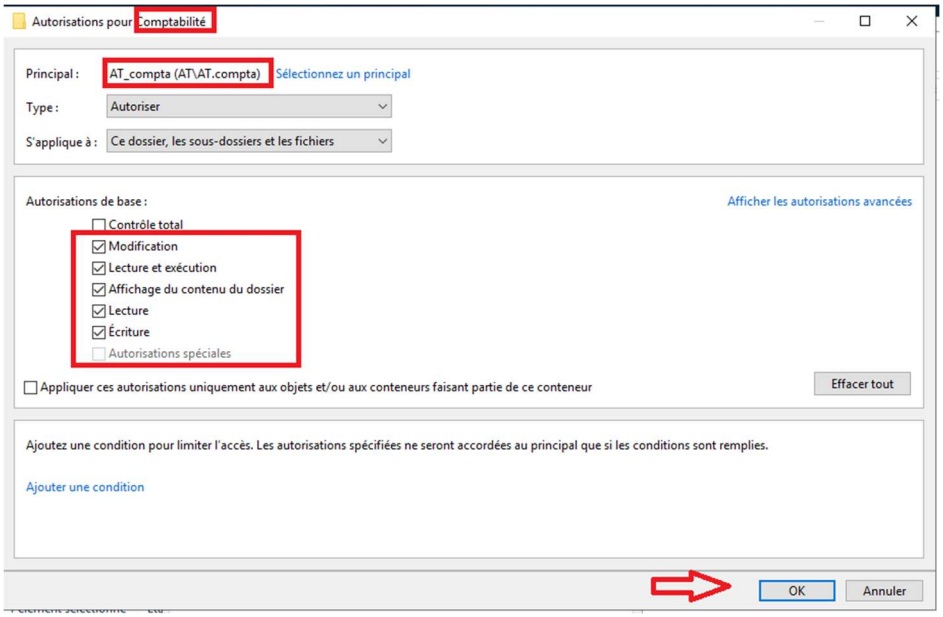


Dans un premier temps, nous devons partager le dossier « parent » de notre partage, dans notre cas, le dossier partage. Nous nous rendons donc sur ce dossier, clic droit, propriété, partage, partage avancé. Nous voyons que le groupe « tout le monde » à accès au partage par défaut. Tout le monde veut dire que n'importe quelle personne connectée au réseau même si elle n'est pas identifiée pourra voir le partage (ce que n'est pas très sécurisé). Nous supprimons donc « tout le monde » et ajoutons à la place « utilisateurs du domaine », et leur laissons le droit en modification et en lecture. (Les droits dans partage avancée ne concerne seulement qui a le droit de voir le dossier via le réseau, et non qui peut faire quoi. On gèrera les vrais droits à l'étape suivant)

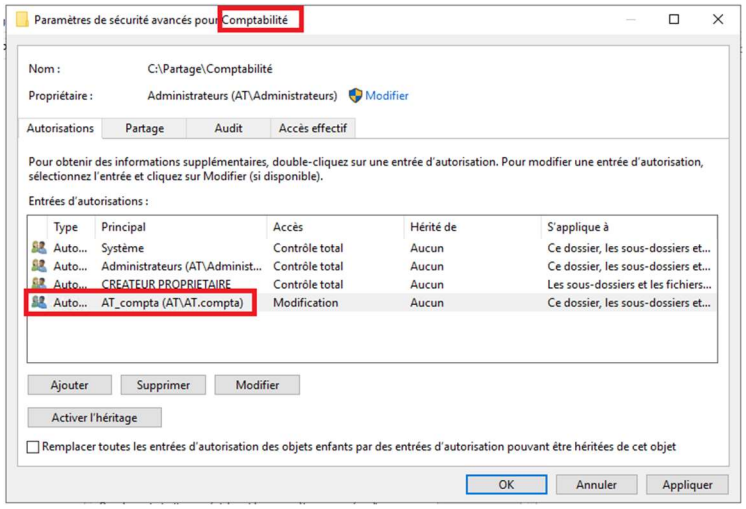


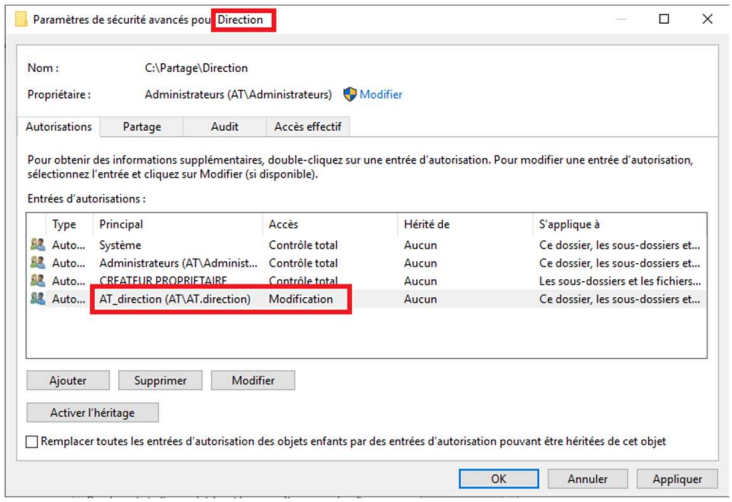
Nous pouvons maintenant gérer les droits d'accès au dossier, nous nous rendons donc dans le dossier partage, et sur chaque dossier respectif, nous avons la possibilité de gérer les droits d'accès au dossier en question. Pour cela, il faut clic droit sur le dossier, propriété, onglet « sécurité », « Avancé ». Il faut tout d'abord désactiver l'héritage pour que notre dossier n'hérite plus des droits de son dossier parent (dans notre cas le dossier « partage »), puis supprimer les groupes utilisateurs (il faut cependant bien laisser les groupes « administrateur » et « système »). Nous pouvons maintenant ajouter les groupes ou les utilisateurs qui auront accès au dossier. Ensuite, nous devons configurer ce que ce groupe pourra faire sur le dossier. Dans notre cas, nous voulons que chaque groupe puisse avoir les accès en lecture et modification/écriture sur leurs dossiers respectifs.

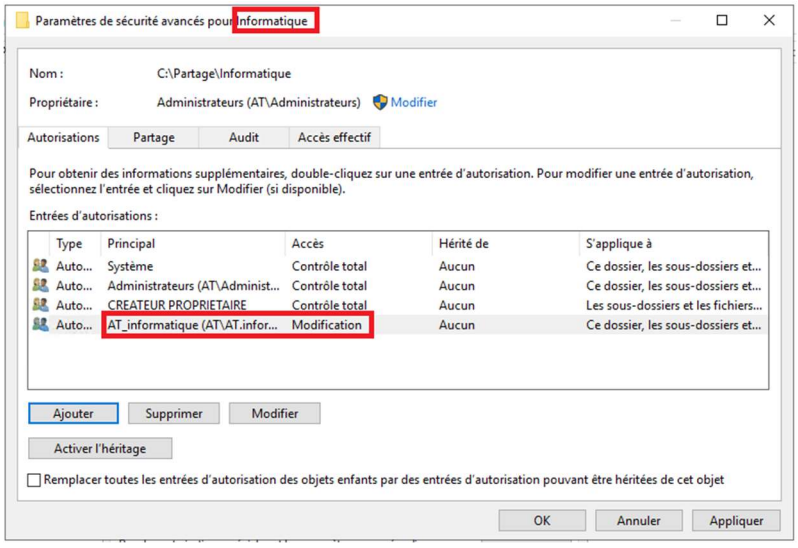




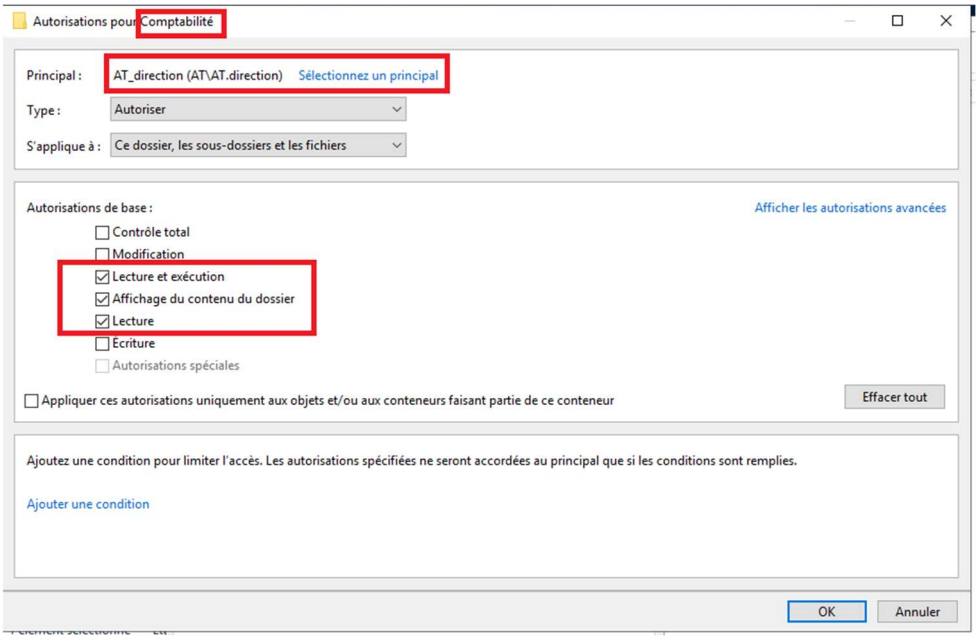
Nous vérifions que chaque groupe a accès à son dossier en Modification.

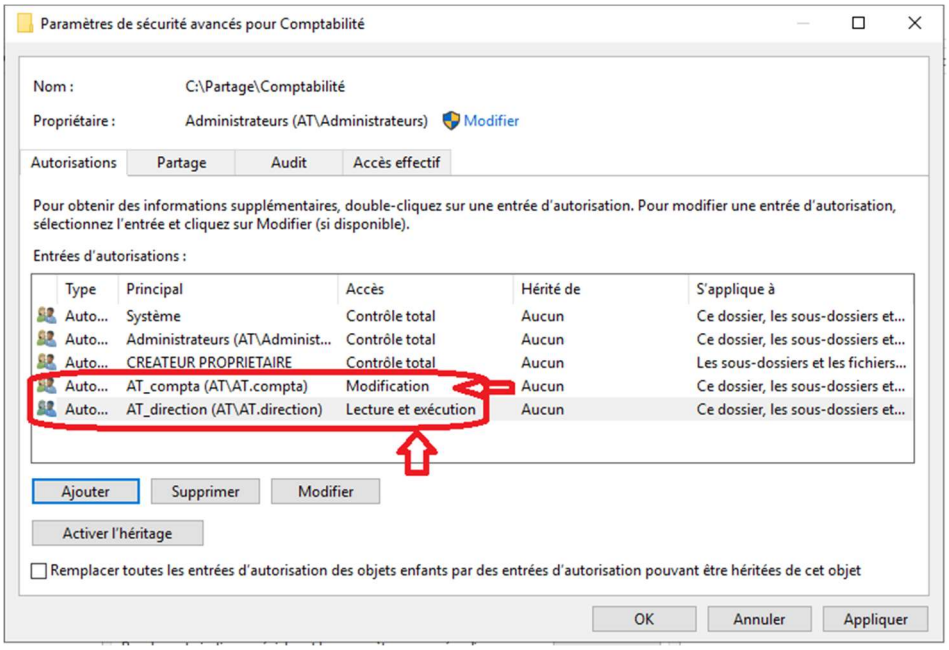




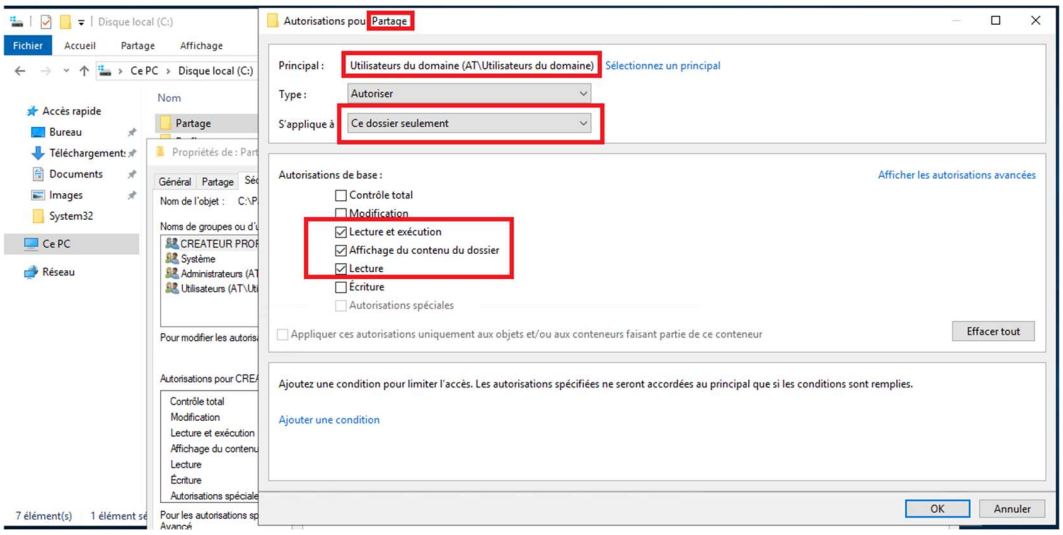


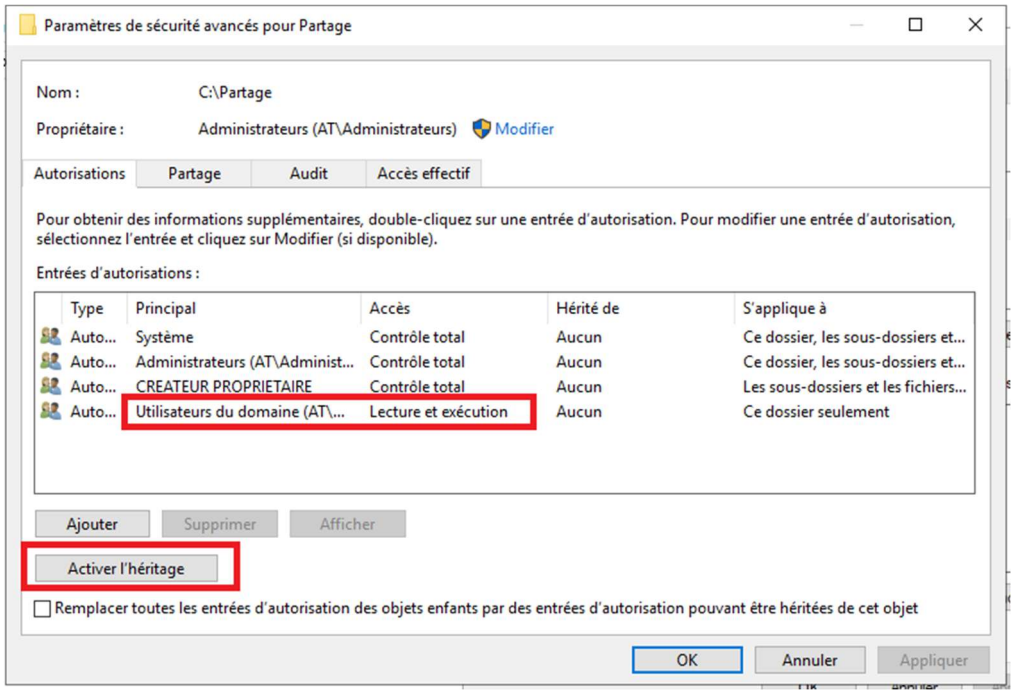
Nous pouvons aussi vouloir que, par exemple, le groupe « direction » ait des accès en lecture seulement sur les dossiers d'un autre service. Nous pouvons le faire en retournant dans les paramètres de sécurité avancés pour « Compta » par exemple, et en ajoutant le groupe « direction » en laissant les paramètres par défaut (Lecture et exécution, affichage du contenu du dossier, Lecture)



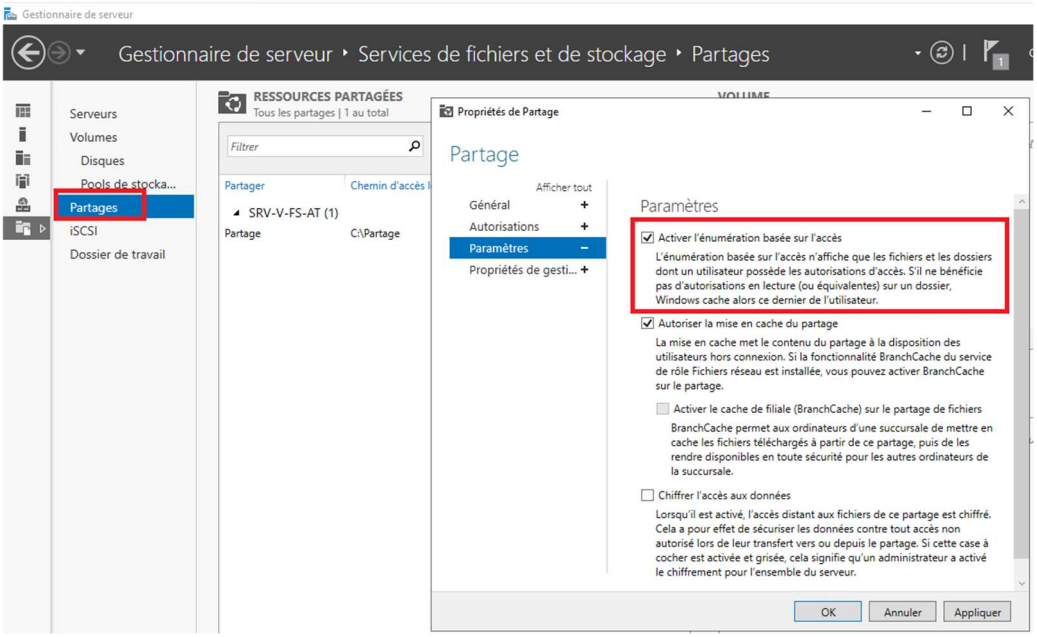


Nous avons bien géré les droits d'accès de chaque groupe sur leurs dossier respectif, avec direction qui a un peu plus de droit que les autres. Il faut maintenant gérer les droits du dossier « partage » (le dossier parent qui contient tous les autres dossiers que l'on partage). Nous retournons donc dans les paramètres de sécurité avancés du dossier « Partage », désactivons l'héritage, et supprimons également « utilisateurs » pour ajouter « utilisateurs du domaine ». Nous ne voulons cependant pas que n'importe quels utilisateurs puissent modifier ou créer des dossiers dans notre dossier « Partage », on peut donc laisser les droits en lecture, affichage du contenu du dossier, et lecture pour ce dossier.

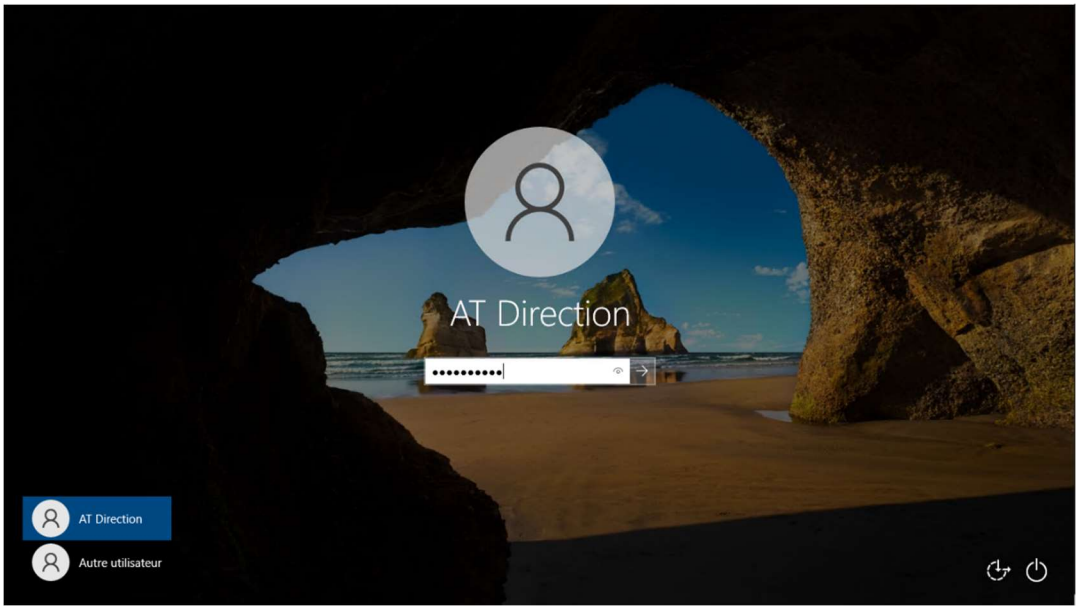




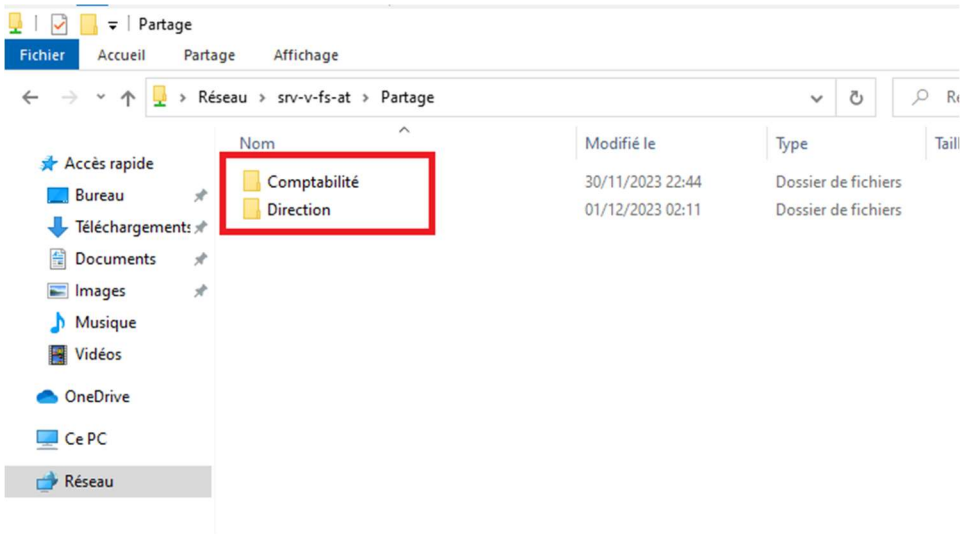
Nous pouvons aussi vouloir que chaque groupe voit seulement les dossiers où ils ont au moins des droits en lecture et qu'ils ne voient pas les autres dossiers partagés. C'est possible grâce à l'option ABE (énumération basée sur l'accès) qui cache les dossiers où l'on n'a pas au minimum un droit de lecture ou équivalent. Il s'active dans le gestionnaire de serveur, onglet « partage », clic droit sur le dossier partagé et dans l'onglet « paramètres » nous pouvons cocher l'ABE



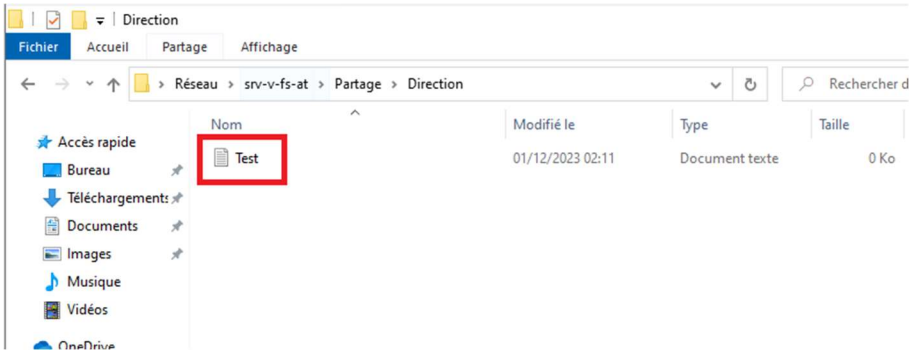
Nous allons nous connecter avec l'utilisateur AT Direction » (étant donné qu'il a un peu plus de droits que les autres) pour vérifier que tout ce que l'on à appliquer fonctionne correctement.



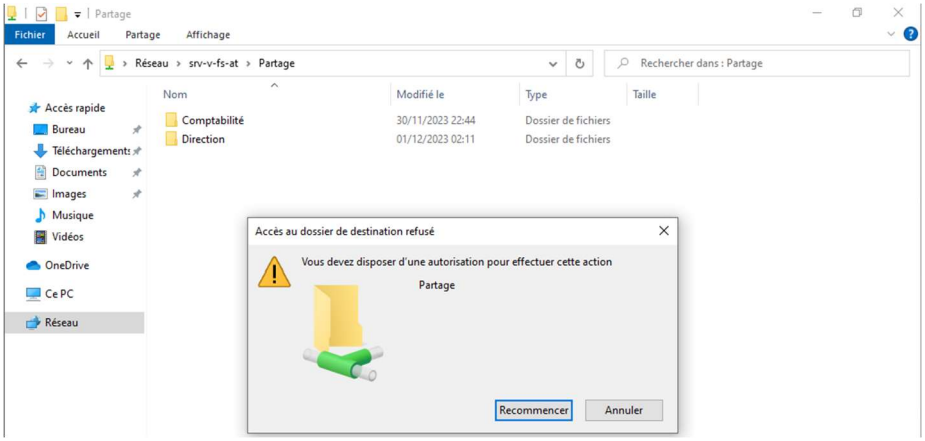
AT direction ne voit que les dossiers ou-il à les droits grâce à l'option ABE.



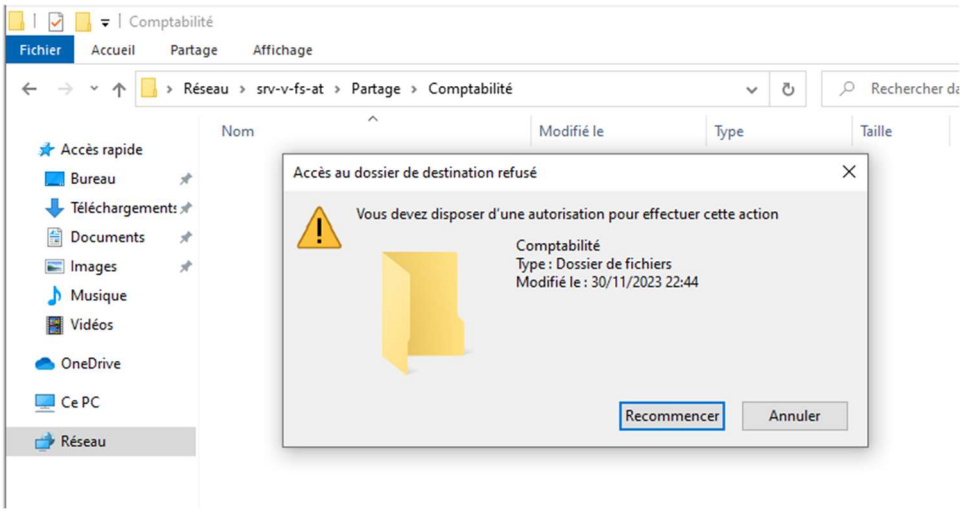
Il peut créer un document texte dans son propre dossier



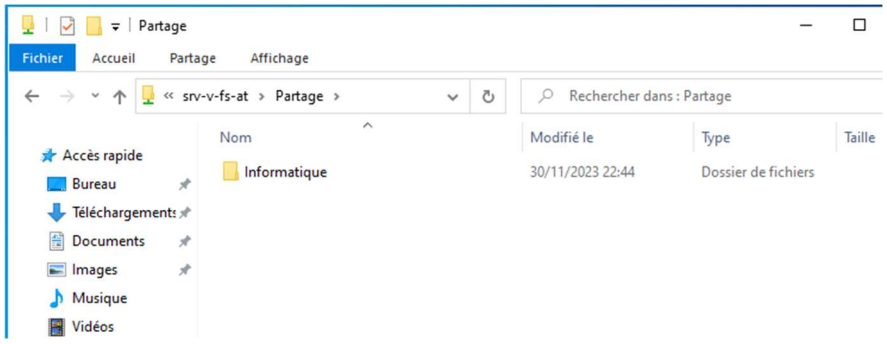
Il ne peut pas créer de dossiers dans le dossier parent « Partage »

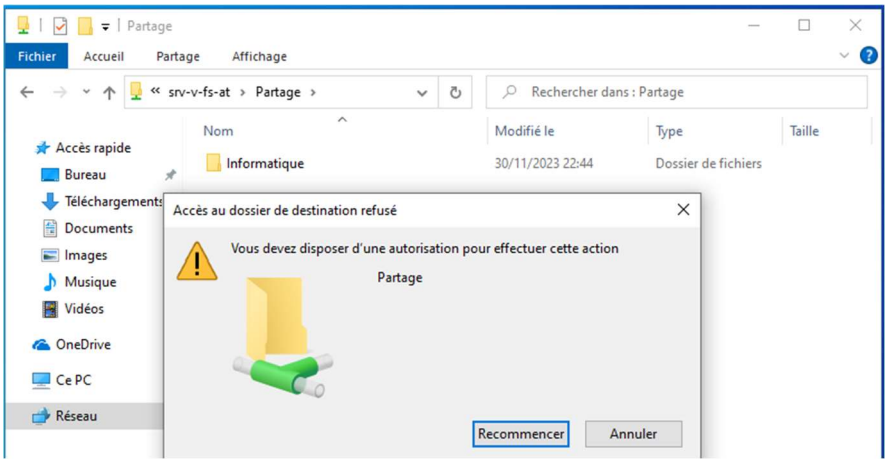


Il ne peut pas créer de dossier dans le dossier « Comptabilité »



Je me suis connecté avec l'utilisateur « AT Informatique » pour vérifier ses droits, et il ne voit bien que le dossier où il a des droits, et ne peut pas créer de dossiers dans le dossier parent « Partage ».

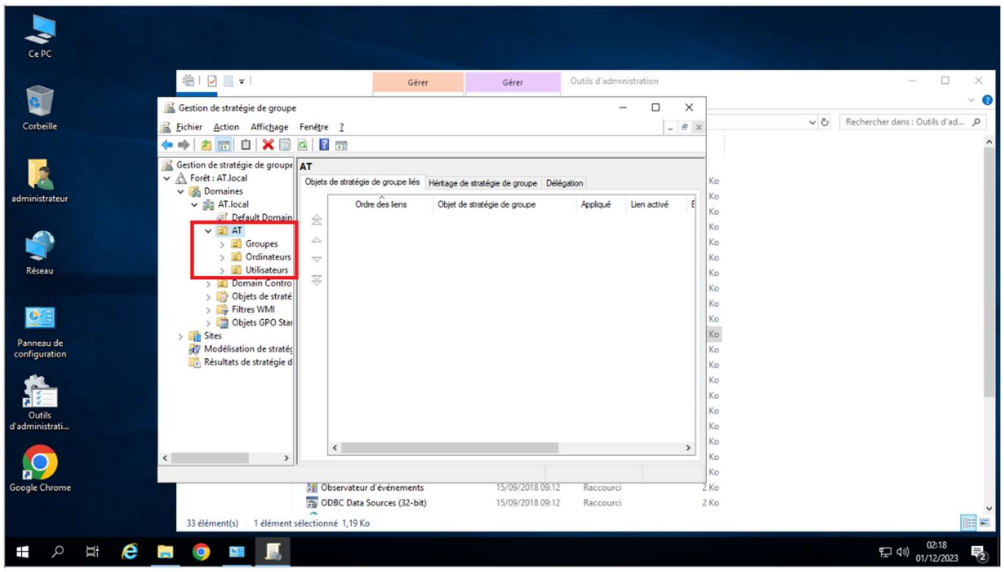




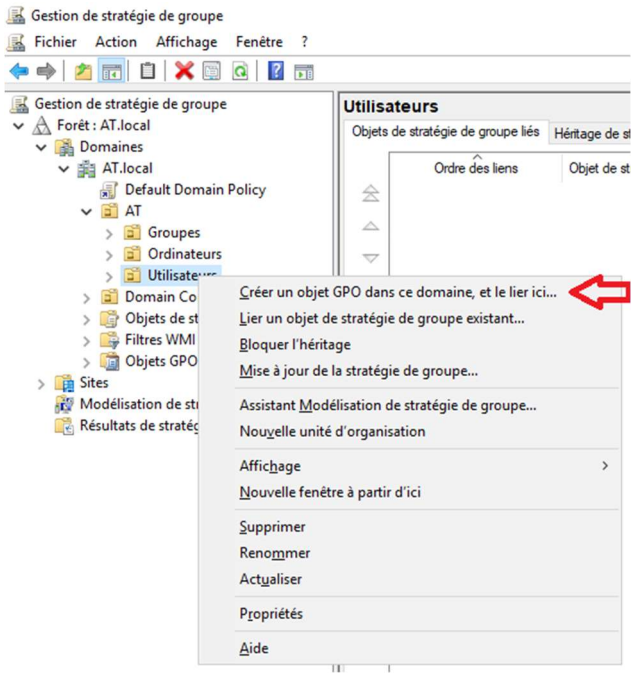
Tous les droits que l'on a attribués sont correctement configurés !

Mise en place d'une stratégie de groupe (GPO)

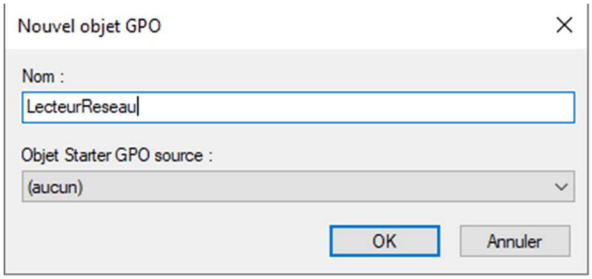
Nous allons maintenant ajouter une stratégie de groupe pour que les utilisateurs puissent avoir accès à notre partage de fichiers directement via un lecteur réseau de manière beaucoup plus simple (qui se trouvera directement dans le gestionnaire de fichiers en dessous du « Disque local C: »).
Pour ce faire, il faudra aller dans les outils d'administration, et dans « Gestion de stratégie de groupe ». Dans cette console, nous allons retrouver nos unités d'organisation (je rappelle qu'une GPO s'applique seulement sur une unité d'organisation, et non sur un groupe ou un utilisateur).
Nous retrouvons nos unités d'organisation créées précédemment.



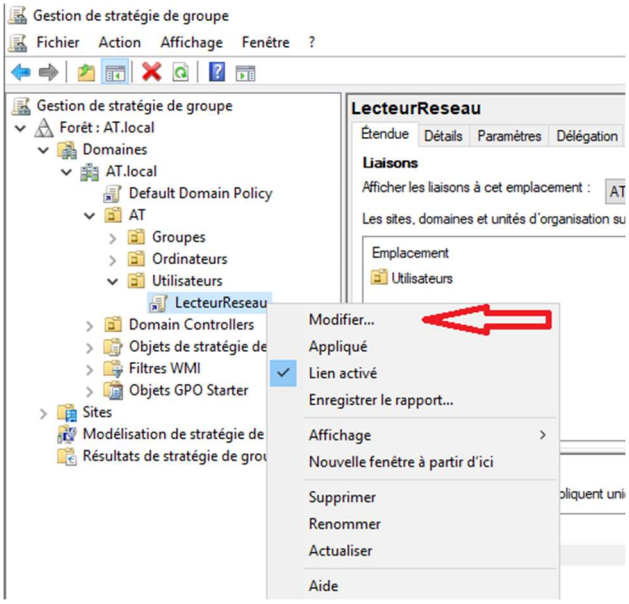
Nous décidons d'appliquer cette GPO sur l'unité d'organisation « Utilisateurs », qui s'appliquera donc à tous les objets se trouvant dans cette UO. Il faut faire un clic droit sur l'UO voulu, « Créer un objet GPO dans ce domaine, et le lier ici… »



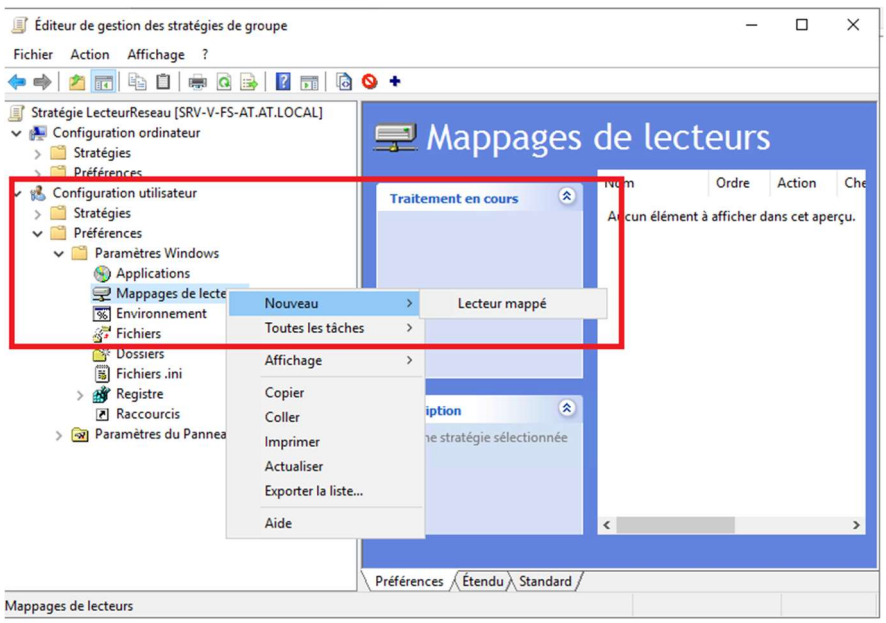
Nous devons lui ajouter un nom, vu que ce sera un lecteur réseau, nous pouvons l'appeler « LecteurReseau ».



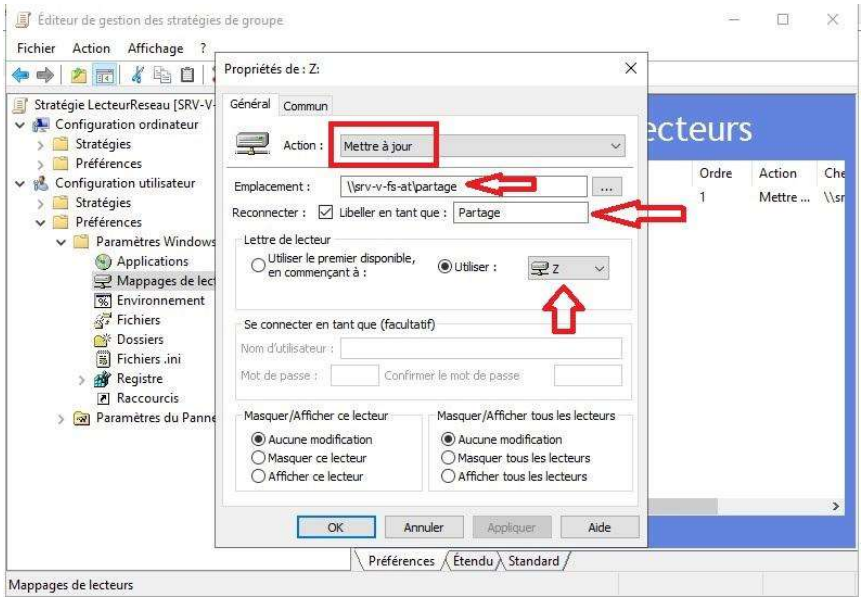
Il apparaîtra ensuite dans l'UO ou nous l'avons créé. Il faut faire un clic droit sur la GPO, et modifier.



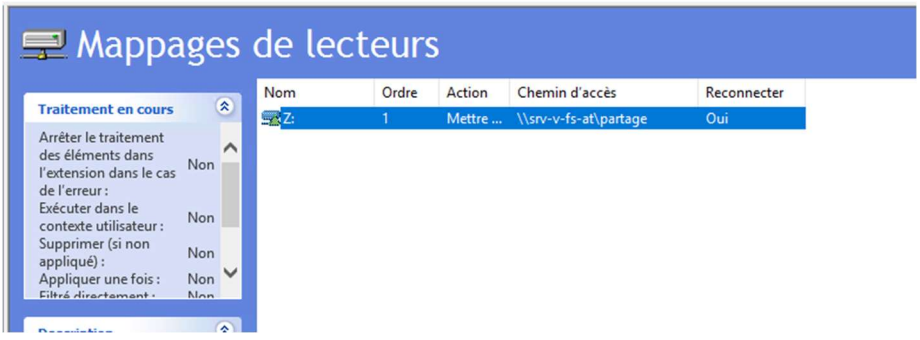
Dans « Configuration des utilisateurs », « Préférences » (Préférence qui permet de réaliser un paramétrage rapide, une nouvelle fonctionnalité de Windows Server), « Paramètres Windows », « Nouveau > Lecteur mappé », nous pouvons créer notre lecteur réseau.



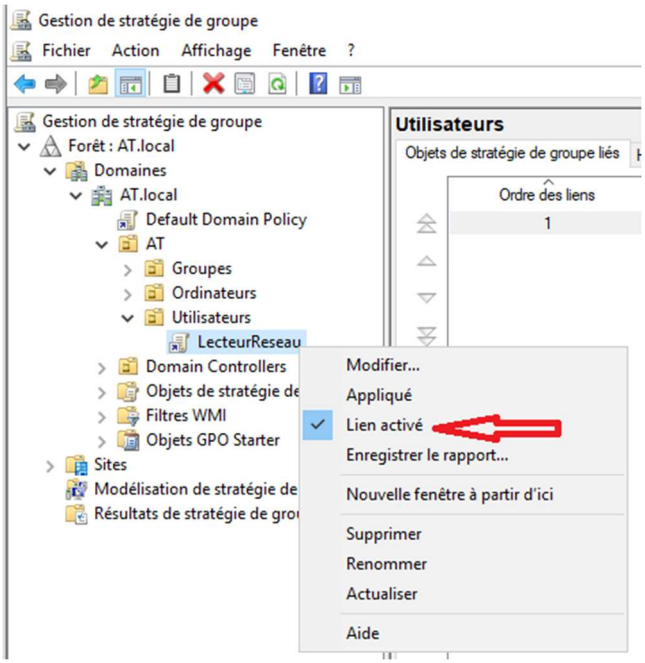
Dans la configuration du lecteur mappé, il est recommandé de laisser l'option « Mettre à jour » activée. Cette option permet de remplacer le lecteur s'il existe déjà, sinon de le créer. Ensuite, nous indiquons le chemin de notre partage (\\srv-v-fs-at\partage\). Nous avons ensuite la possibilité de donner un nom à notre lecteur, ce qui nous évite d'afficher tout le chemin (je conseille donc de le faire). De plus, nous avons la possibilité de choisir une lettre pour notre lecteur réseau. Pour éviter de choisir une lettre déjà utilisée par une clé USB ou autre, il est préférable de commencer par la fin de l'alphabet, ce qui permet d'éviter les problèmes.



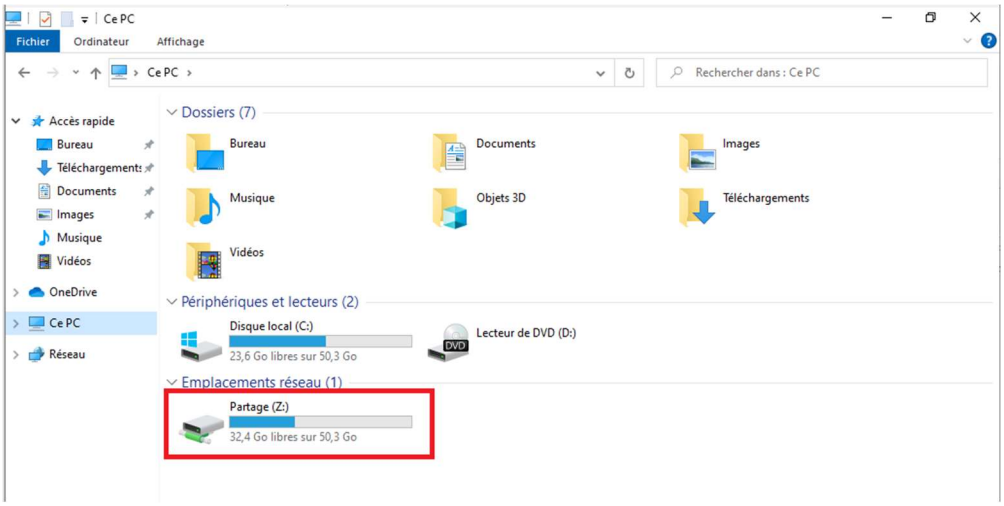
Nous pouvons ensuite choisir l'ordre de lancement des GPOs, dans notre cas nous n'en avons qu'une.

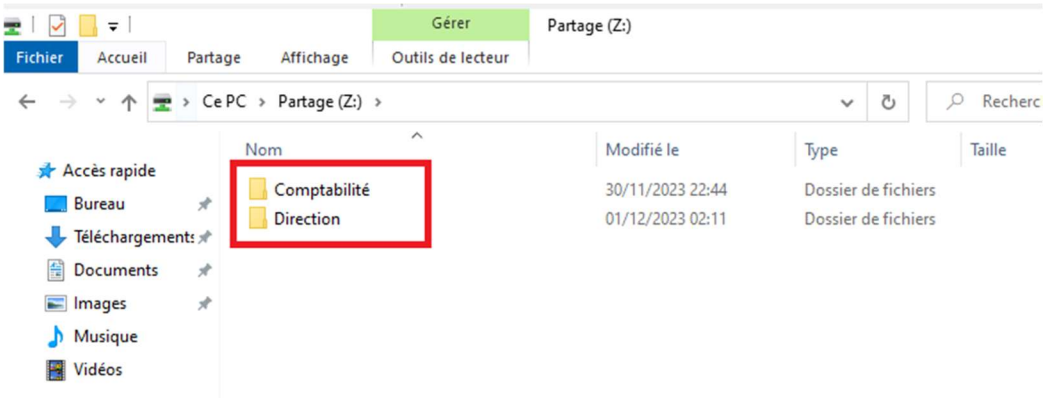


Pour que notre stratégie de groupe s'applique, il est nécessaire de laisser la case « Lien activé » cochée. La case située au-dessus, « Appliquer », ne sert pas à appliquer la stratégie de groupe, mais à la forcer. On l'utilise dans le cas où nous aurions une deuxième stratégie de groupe qui serait contraire à celle que nous paramétrons (comme un fond d'écran, par exemple)



Notre lecteur réseau est correctement configuré et nous avons appliqué la stratégie de groupe sur l'ensemble de notre unité d'organisation « Utilisateurs ». Nous pouvons vérifier qu'elle s'est bien appliquée et que nous avons toujours accès au dossier respectif de chaque groupe en nous connectant avec un utilisateur et en allant dans « PC ». Le lecteur réseau apparaît bien, et l'utilisateur « AT Direction » a bien accès au dossier pour lequel il a les droits, et ne voit que ceux-ci grâce à l'option ABE.



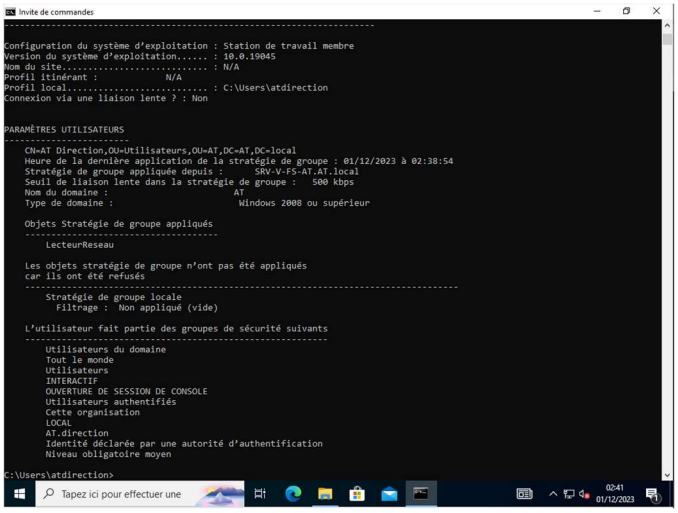


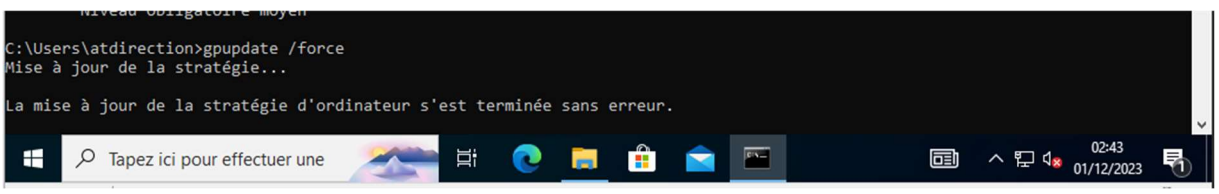
Nous avons deux commandes intéressantes sur les stratégies de groupe :

- gpresult /r : nous donne le résultats des GPOs appliquée à notre utilisateur et de voir les groupes/OU auxquels il appartient. Très utile si la GPO ne s'applique pas, nous pouvons vérifier plusieurs paramètres différents.
- gpupdate /force qui force l'ordinateur et l'utilisateur a interroger le serveur pour voir si une mise à jour de la GPO a eu lieu

A noter qu'une stratégie de groupe ne s'applique sur :

- Un ordinateur que si on le redémarre
- Un utilisateur : à la fermeture/ouverture de session.





3. Conclusion

Et voilà, nous avons procédé à la mise en place d'un domaine avec Active Directory, promu notre serveur AD en contrôleur de domaine et créé des utilisateurs dans ce domaine. Nous avons ensuite mis en place un partage de fichier avec des droits d'accès NTFS pour chaque utilisateur, avons laissé afficher les dossiers partagés qu'aux personnes ayant au minimum des droits en lecture sur ces derniers grâce à l'option ABE et avons déployé ce partage sous forme de lecteur réseau grâce à une GPO.

Test de bon fonctionnement :

Pour le test, il suffit de tenter d'entrer un ordinateur au domaine précédemment créé, de créer un utilisateur et d'essayer de se connecter avec ce dernier sur un poste client. Ensuite, nous pouvons vérifier que les GPOs s'appliquent bien en vérifiant dans « Ce PC » leurs droits d'accès à ce même endroit. Si nous arrivons à accéder avec un utilisateur à un dossier auquel il n'a pas accès ou qu'il le voit alors que l'option ABE est activée, c'est qu'il faut revoir ces points directement sur le serveur.

Point de vigilances

- Dans ce TP, j'ai rencontré un souci avec DNS qui ne faisait la résolution de mon nom de domaine uniquement vers mon adresse en IPv6 et non en IPv4. Pour pallier ce souci, il faut bien penser à décocher l'IPv6 dans les propriétés du serveur DNS pour n'avoir que des adresses en IPv4

- Bien vérifier le DNS sur le poste client si nous n'arrivons pas à l'entrer dans le domaine, le souci peut venir d'un DNS mal renseigné

- Un nom de domaine local, par convention, doit toujours se terminer par « .local » ou « .lan » pour ne pas le confondre avec un nom de domaine public.

- Il faut bien faire attention : les stratégies de groupes peuvent uniquement être mises en place sur des unités d'organisation. Les groupes quant à eux, servent à gérer les droits NTFS (accès aux dossiers ou ressources). A ne pas confondre !

- Pour se connecter au domaine, il faut utiliser cette façon d'écrire sur la page de connexion : AT\administrateur (qui veut dire l'administrateur du domaine AT). Ajouter un poste à un domaine n'empêche pas de se connecter en local, en écrivant le login de cette façon : .\UtilisateurduPC (qui veut dire l'utilisateur du poste en local)

- Lorsque l'on met en place une stratégie de groupe, pour l'appliquer il faut bien laisser la case « lien activé » cochée qui veut simplement dire que cette dernière est activée, et ne pas utiliser « appliqué » (qui se traduit « forced » sur un Windows Server anglais) et qui forcerait la GPO. On utilise « appliqué » dans le cas où on a une stratégie de groupe « parente » à celle

qu'on paramètre (comme un fond d'écran différent par exemple).

- Dans la configuration d'un lecteur mappé, il faut bien laisser l'option « mettre à jour » qui fait que si le lecteur existe déjà, on le remplace, sinon on le crée.

- Lorsqu'on paramètre un lecteur réseau, il faut bien penser à lui attribuer une lettre et de plutôt commencer par la fin, ce qui évite de tomber sur la même lettre qu'une clé USB ou autre par exemple.

- La commande « nslookup » est intéressante car elle interroge notre serveur DNS et nous fait le rapprochement entre l'IP du contrôleur de domaine et le nom de domaine.

- Les dossiers à partager sont à créer uniquement à la racine du disque local pour éviter les chemins d'accès trop longs et éviter d'atteindre la limite de caractères imposée par Windows qui peut nous causer des soucis lors de renommage ou de copie de fichiers.

- Nous avons deux commandes intéressantes sur les stratégies de groupe :

gpresult /r : nous donne le résultat des GPOs appliquées à notre utilisateur et de voir les groupes/OU auxquels il appartient. Très utile si la GPO ne s'applique pas, nous pouvons vérifier plusieurs paramètres différents.

gpupdate /force qui force l'ordinateur et l'utilisateur à interroger le serveur pour voir si une mise à jour de la GPO a eu lieu (Attention, ça ne l'appliquera pas, pour qu'une stratégie de groupe s'applique il faut :

- Redémarrer le poste quand c'est une GPO ordinateurs.
- Déconnecter et reconnecter la session quand c'est une GPO utilisateurs.

Conseils de sécurité

- Le premier conseil est de bien laisser coché l'option pour que les nouveaux utilisateurs qu'on crée puisse choisir eux même leurs mots de passes lors de la première connexion.

- Il faut bien évidemment et comme toujours créer un serveur dédié pour chaque rôle que l'on souhaite installer, donc un serveur Active Directory, et un serveur de partage de fichier dans notre cas

- Sur un serveur de fichier, il est impératif d'activer les clichés instantanés qui nous permettent d'avoir une antériorité sur nos fichiers à un moment donné et une solution de récupération ou de restauration en cas de souci

- L'option « partager ce dossier » ne sert qu'à définir qui peut voir le partage via le réseau et non qui peut faire quoi sur ce dernier. Pour gérer les droits d'accès, il faut gérer les droits NTFS dans l'onglet sécurité. Les permissions NTFS déterminent qui peut accéder, modifier ou supprimer des fichiers.

- Il est ESSENTIEL de supprimer le groupe « Tout le monde » dans les options de partage avancées qui veut bien dire que tout le monde pourra voir le dossier sur le réseau,

et ajouter à la place « utilisateurs authentifié » ou « utilisateurs du domaine » qui est bien plus sécurisé.

- De même, pour les droits NTFS, il faut bien supprimer les utilisateurs et créer des groupes dédiés pour gérer les droits sur ces dossiers, selon qui peut y avoir accès ou non (Ne pas oublier de désactiver l'héritage comme mentionné dans le procédé pas à pas).

- Les droits en contrôle total sur des dossiers sont uniquement à laisser pour les administrateurs et le système (pour les MAJ ou autres), et ne jamais laisser de droits en contrôle totale à d'autres personnes qui leur permettrait de modifier les droits d'accès, ce qu'on ne veut surtout pas.

- L'option ABE est très intéressante en matière de sécurité car elle permet de ne laisser afficher les dossiers que des utilisateurs qui ont des droits en lecture au minimum sur ces derniers. Si un utilisateur n'a pas de droit, il ne verra pas le dossier lors de sa connexion au partage.

- Il faut définir un mot de passe fort pour la restauration en cas de panne d'Active Directory (lors de l'installation du rôle), seul ce mot de passe pourra être utilisé. (Il permet d'accéder en admin au serveur)