2024-2025

PROJET AUTHENTIFICATION AD

Magne Brigitte

Ben wahab kadi aziz

INTRODUCTION :

Dans le cadre de ce projet, nous allons mettre en place un système d'**authentification dans le réseau GSB**. L'objectif est d'assurer une gestion centralisée des utilisateurs et des machines à travers **Active Directory**.

Ce projet est structuré en plusieurs parties :

- **Installation et configuration du serveur et des machines clientes** : Mise en place du serveur, configuration réseau et déploiement d'Active Directory.
- **Gestion des comptes utilisateurs et intégration des machines au domaine** : Création des comptes et des groupes, ainsi que la gestion des profils et des dossiers personnels.
- **Mise en place des stratégies de groupe (GPO)** : Application de règles de sécurité et de configuration via Active Directory.

Chaque étape repose sur des manipulations techniques précises visant à sécuriser et optimiser l'environnement informatique du réseau GSB. À la fin de ce projet, nous aurons un système d'authentification fonctionnel permettant une gestion efficace des ressources et des utilisateurs.

Sommaire

Projet 2 : Authentification dans le réseau GSB 4
Présentation du projet 4
Présentation des parties à réaliser 4
Consignes pour le compte rendu 4
Partie 1 : Installation et configuration du serveur et de la machine cliente 5
Organisation préalable 5
Présentation des fonctionnalités de bases 5
Installation du serveur et du client 6
Présentation de vos adresses IP et test de ping 8
Nommage des machines 9
Mise en place d'Active directory 12
Installation du Rôle DNS &et ADDS 12
Promouvoir ce serveur en contrôleur de domaine 12
Configuration du Contrôleur de domaine 13
Configuration et optimisation du Service DNS 14
Ajout d'un Pointeur (PTR) sur le Serveur 15
Vérification de la configuration DNS 17
Définir le vieillissement et nettoyage de toutes les zones 18
Paramétrage du navigateur par défaut Internet explorer 21
Vérification du profil réseau du contrôleur de domaine 22
Partie 2 : Gestion des comptes utilisateurs et ajout des machine clientes au domaine 24
Ajout des deux machines clientes dans le domaine LaboGSB 24
Présentation de l'outil « Utilisateurs et ordinateurs Active Directory » 27
Création des unités d'Organisation « OU » 28
Création des groupes d'utilisateurs 28
Création des comptes utilisateurs 30
Création des profils en fonction des utilisateurs 34
Gestion des dossiers personnels 37
Partie 3 : Mise en place stratégies de groupe (GPO) 42
Présentation des stratégies de groupe dans le domaine 42
Mise en place des stratégies de groupe 44

SIO2-SISR - Projet authentification AD 19 Novembre 2024

Projet 2 : Authentification dans le réseau GSB

Présentation du projet

L'administrateur réseau de GSB vous confie la mission de mettre en place une solution de gestion optimisée des utilisateurs du réseau. Vu le nombre important des visiteurs médicaux et du nombre des personnels travaillant dans les différents services de GSB, il est primordial que la solution proposée soit appropriée. En effet, elle devra permettre de gérer de manière cohérente les comptes, comme les mots de passe, la structure d'une entreprise découpée en service, les droits et partages des fichiers de ces mêmes services
La solution Active Directory est la solution qui lui semble intéressant dans l'environnement Windows.

L'installation du service AD

- ⇨ Promeut un serveur en contrôleur de domaine centralisant les échanges, les authentifications, les applications des règles prédéfinies au sein du domaine.

- ⇨ Permet la centralisation de la gestion de l'administration réseau, et ce à travers des objets tels que les comptes utilisateurs, les profils, les GPO (Group Policy Objects) etc..

La mise en place de la solution va consister à :

1. Créer un contrôleur de domaine
2. Joindre les postes clients au domaine
3. Gérer des comptes utilisateurs
4. Gérer des profils itinérants
5. Gérer des unités d'organisation
6. Déployer des stratégies de groupe pour centraliser et optimiser l'administration des objets (comme les postes clients, les comptes utilisateurs) dans un domaine.

Présentation des parties à réaliser

Ce projet, est répartie en 3 parties :

Partie 1 :	Installation et configuration du serveur et de la machine cliente
Partie 2 :	Gestion des comptes utilisateurs et Ajout de la machine cliente au domaine
Partie 3 :	Mise en place des stratégies de groupe dans le domaine

Consignes pour le compte rendu

Rédiger progressivement un compte rendu, penser à y intégrer les captures importantes et /ou demandées.
Il s'agit évidemment d'un document structuré comme vous le savez déjà.

On doit y retrouver entre autres :

- ⇨ Les besoins de GSB vis-à-vis de la mission ;
- ⇨ Les étapes de réalisation (description et captures du travail fait)

Partie 1 : Installation et configuration du serveur et de la machine cliente

Etapes de la réalisation

Contenu :

- ⇨ *Installation des machines*
- ⇨ *Mise en place d'Active Directory*
- ⇨ *Construction du domaine*

Organisation préalable

a) Dans le disque « DATA » :

⇨ Créer un dossier Projet authentification-AD

- Créer 3 dossiers : ISO, VM, CR
- Dans VM créer 3 sous dossiers correspondants aux 3 machines à créer : **Serveur-AD** et **WinClient10-1**, **WinClient10-2**

b) Sur VMware :

⇨ Créer un dossier : E5-Projet-Authentification-AD

⇨ Vous allez y créer les 3 machines indiquées ci-dessous (bien respecter les noms indiqués)

Présentation des fonctionnalités de bases

a) Pour chaque cas cité donner une explication en un paragraphe avec vos propres mots]

Fonctionnalités	Explication
AD DS	
Forêt	
Domaine	
Relations d'approbation	
OU (Organizational Unit)	
Contrôleurs de domaine	
GPO	

Installation du serveur et du client

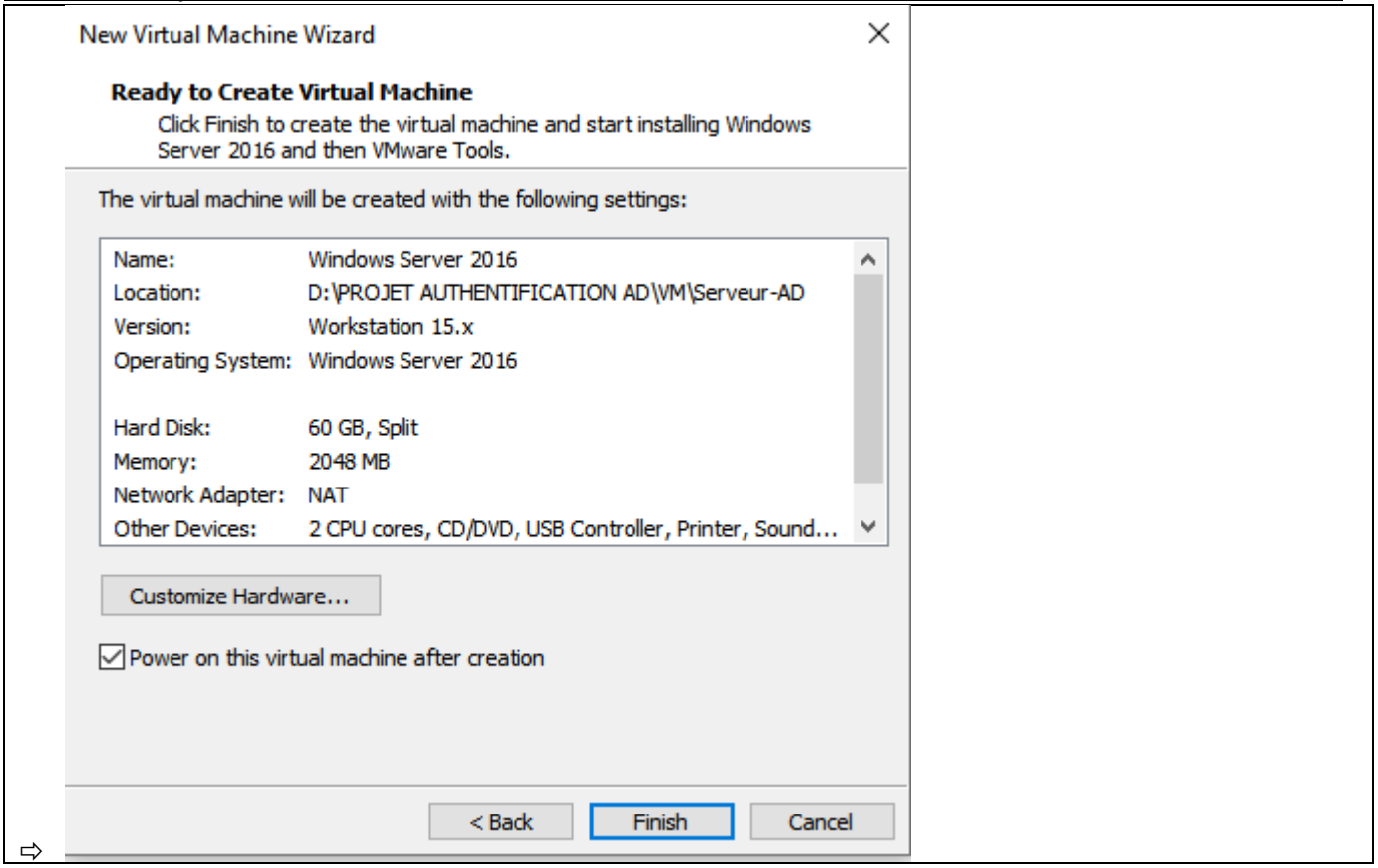
a) Installation des machines

Création du serveur authentification : Serveur-AD

Installation du serveur

Pour l'installation, inutile de mettre beaucoup de captures, 4 suffissent

- ⇨ Installer le serveur
- ⇨ Le nommer **Serveur-AD**
- ⇨ Disque dur 50 Go
- ⇨ RAM 4096 Mo
- ⇨ 1 Carte réseau : carte 1 (LAN1)
- ⇨ Monter dans le lecteur l'iso « Windows2016»
- ⇨ Choisir le bon dossier dans lequel il sera sauvegardé
- ⇨ Configurer la carte réseau LAN
  - Mettre une IP issue de votre plage d'adresses
  - Mettre IP du DNS primaire, c'est l'IP de ce serveur AD
  - Pas de passerelle



Création des 2 machines Clientes : WinClient10-1, WinClient10-2

Cas 1 : Installation de la nouvelle machine :

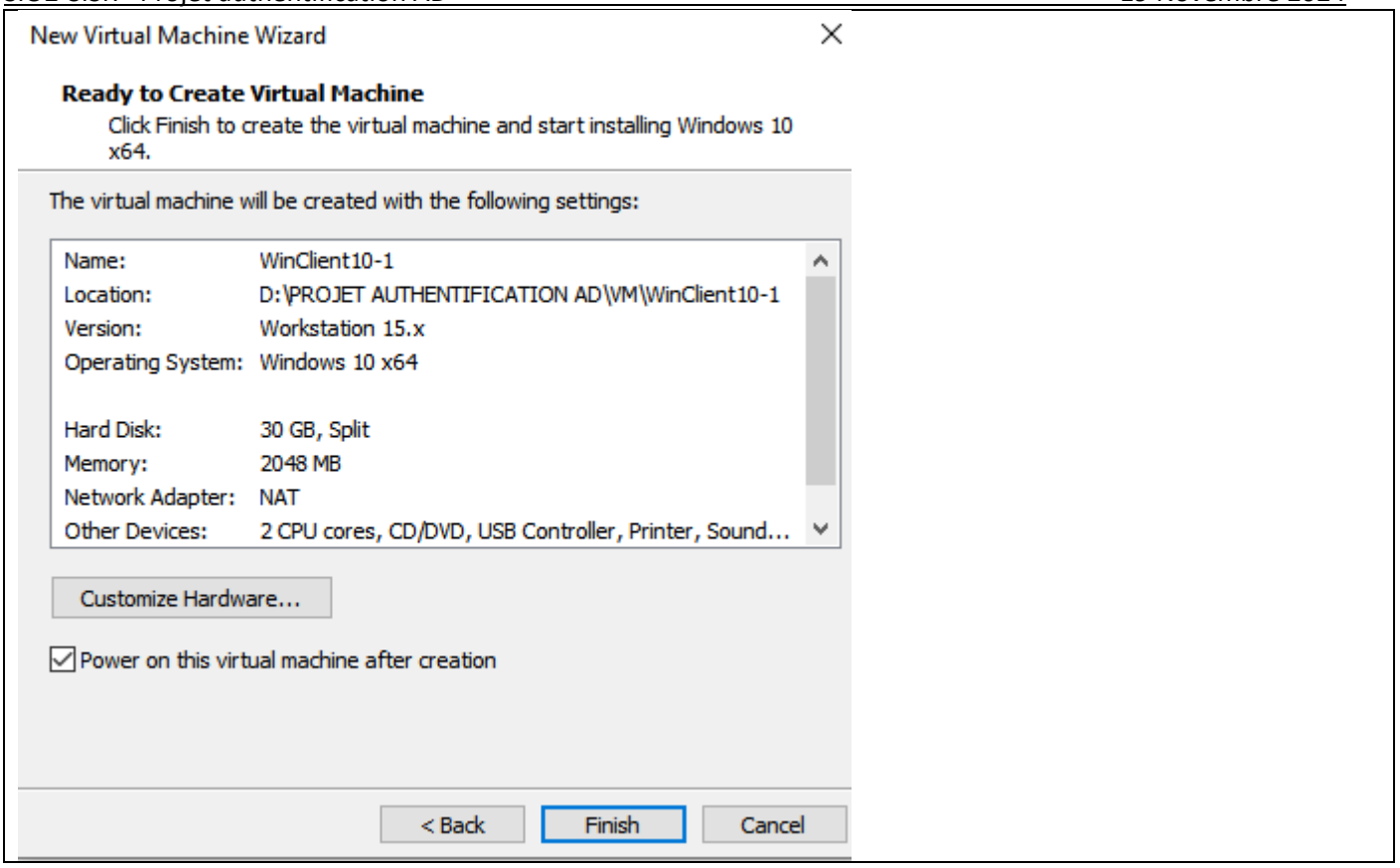
- ⇨ Le nommer **WinClient10-1**
- ⇨ Disque dur 30 Go
- ⇨ RAM 2048 Mo
- ⇨ 1 Carte réseau : carte 1 (LAN1)
- ⇨ Monter dans le lecteur l'iso « Windows10(1903) _64bits »

Faire l'installation qui est assez simple, ***inutile de mettre beaucoup de captures, 2 suffissent.***

- ⇨ Le mot de passe à utiliser : **pas de mot de passe**
- ⇨ Configurer la carte réseau LAN (mettre une IP issue de votre plage d'adresses, mettre le DNS qui correspond au serveur AD)

Cas2 : utilisation du clonage pour WinClient10-2

Après cette installation, créer une nouvelle machine **WinClient10-2** en faisant un clone intégral du client installé



Présentation de vos adresses IP et test de ping

[Compléter ce tableau, ajouter toute la configuration IP de vos 2 machines clientes :

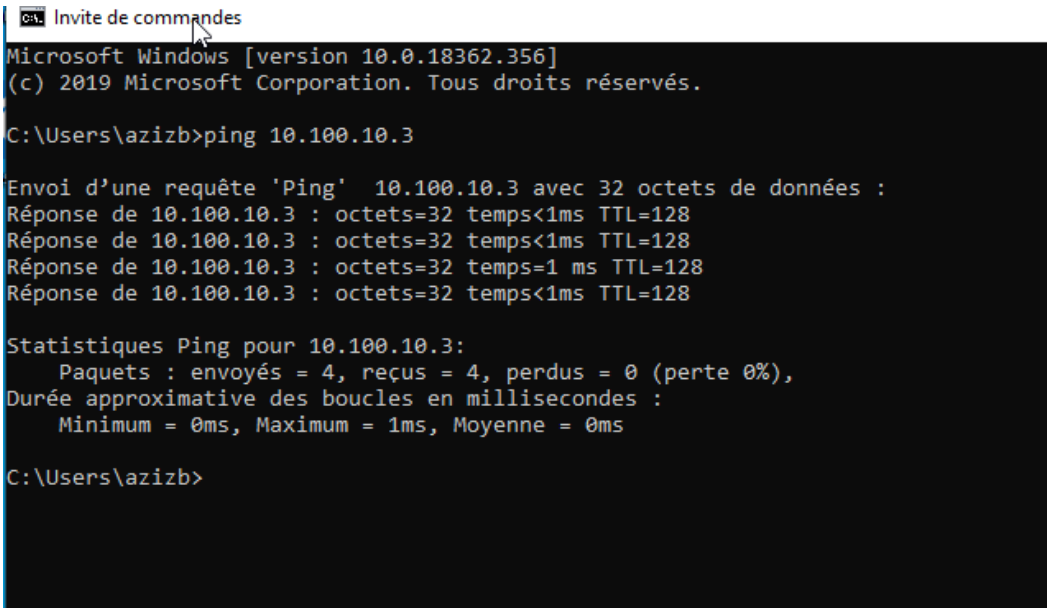
Nom machine	Adresse IP	Masque	DNS
Serveur-AD	10.100.10.1		
WinCleint10	10.100.10.2		
WinCleint10-2	10.100.10.3		

Puis, configurer les adresses IP sur vos machines clientes

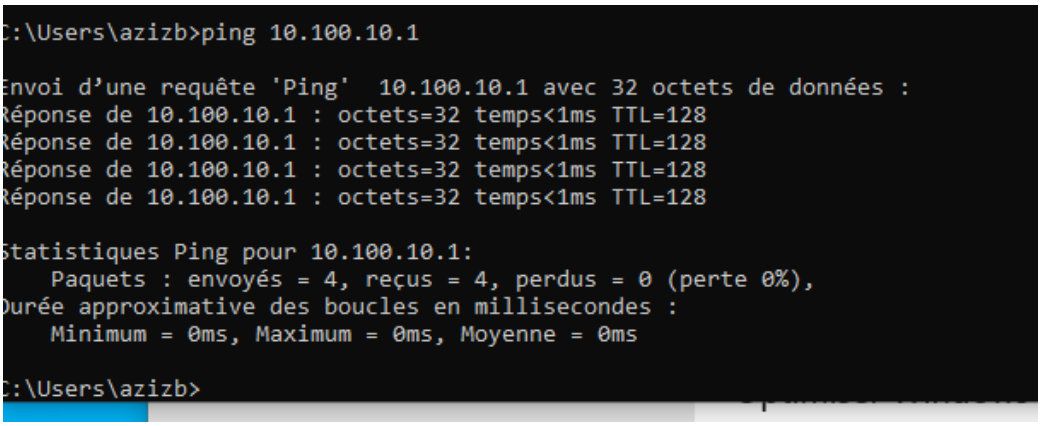
Test de ping : Vérifiez que les pings fonctionnent entre les deux machines.

[Captures montrant les résultats]

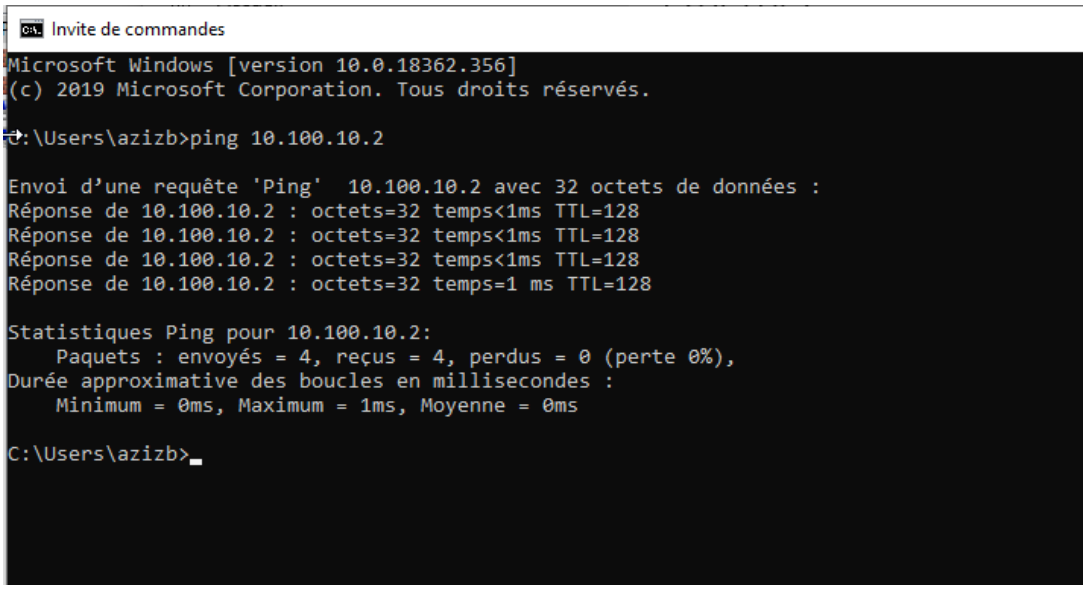
PING PC1-PC2



PING PC1 –SERVEUR



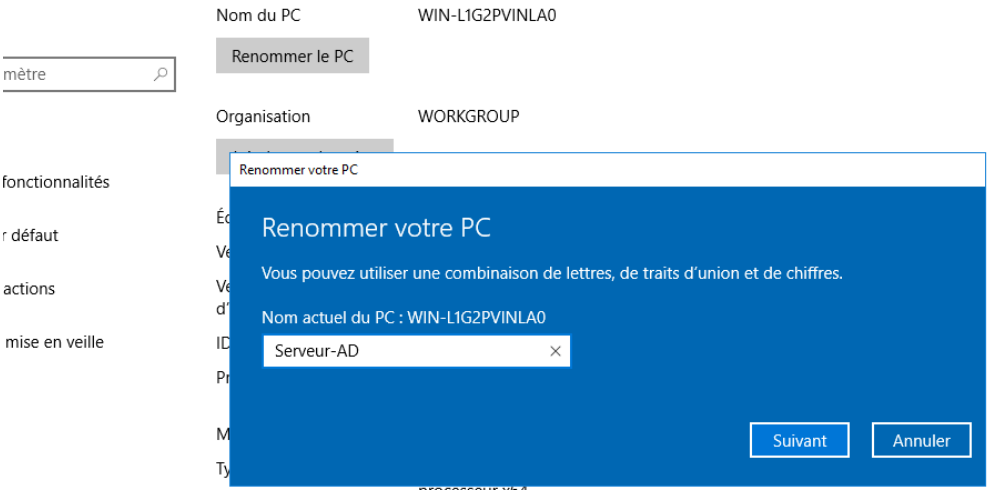
PING PC2-PC1



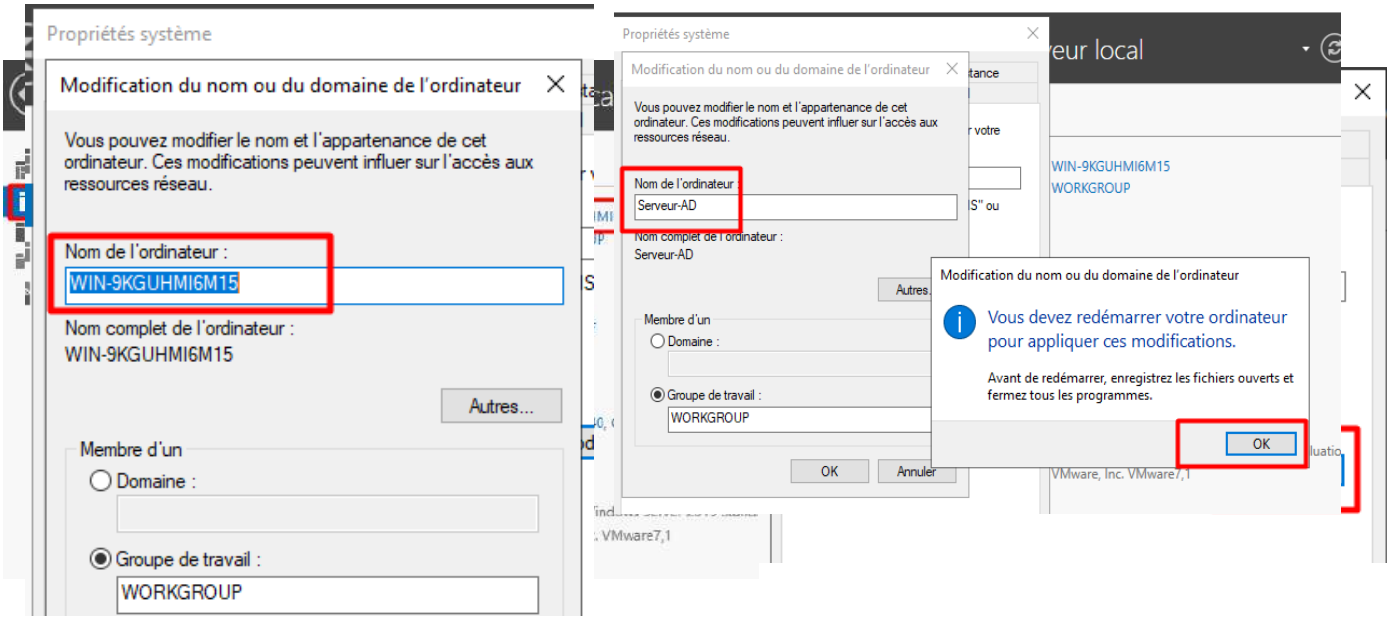
Nommage des machines

Après l'installation des machines, il faut renommer chaque machine, c'est très important.

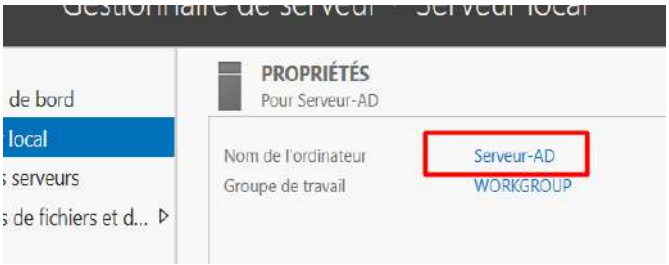
Modification du nom du serveur AD



Voici quelques captures qui montrent le procédé



Après redémarrage du serveur, vous verrez ceci

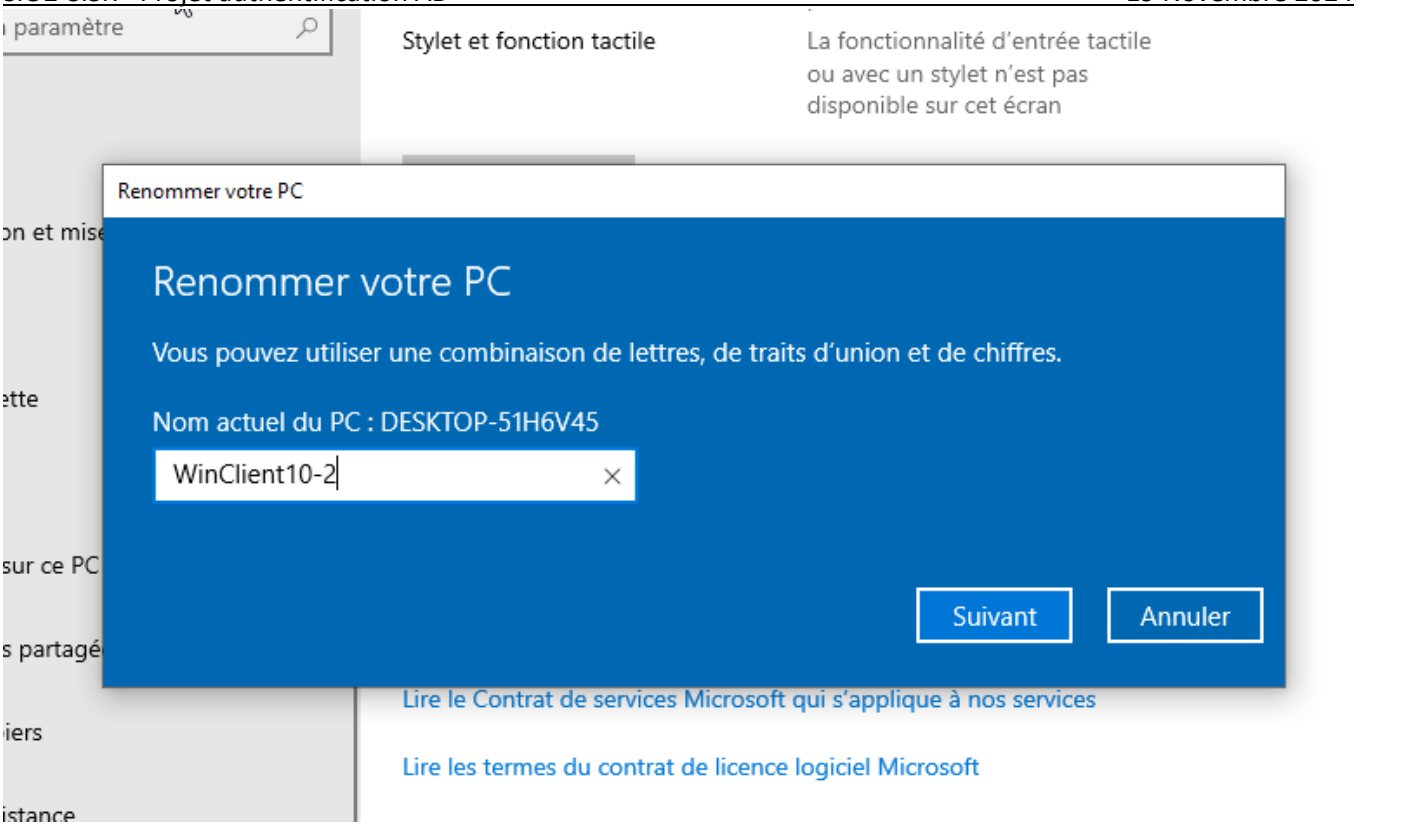


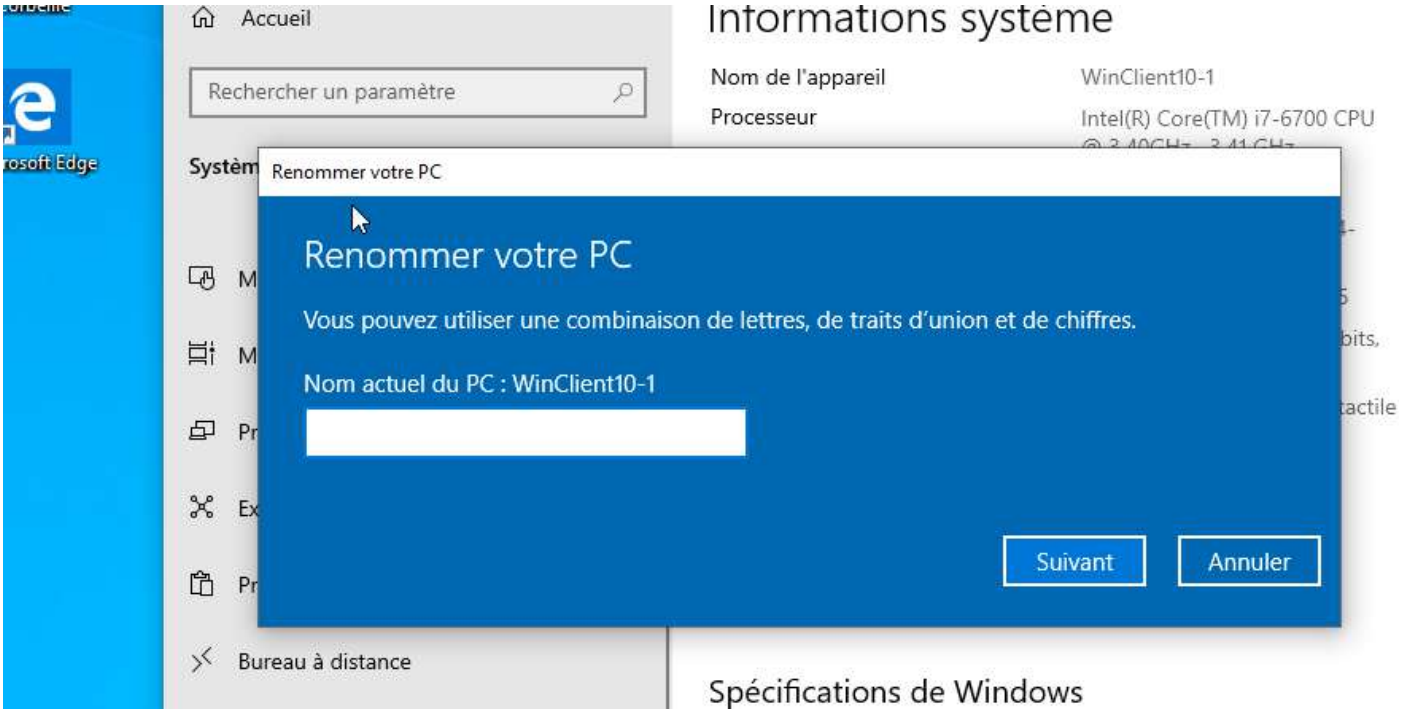
Modification du nom des PC clients

IMPORTANT

A vous de trouver comment le faire, ce n'est pas compliqué.

[2 ou 3 captures seulement]


paramètre
Stylet et fonction tactile
La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran
Renommer votre PC
Renommer votre PC
Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.
Nom actuel du PC : DESKTOP-51H6V45
WinClient10-2
Suivant
Annuler
Lire le Contrat de services Microsoft qui s'applique à nos services
Lire les termes du contrat de licence logiciel Microsoft


Accueil
Rechercher un paramètre
Informations système
Nom de l'appareil
WinClient10-1
Processeur
Intel(R) Core(TM) i7-6700 CPU
Renommer votre PC
Renommer votre PC
Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.
Nom actuel du PC : WinClient10-1
Suivant
Annuler
Bureau à distance
Spécifications de Windows

Mise en place d'Active directory

Installation du Rôle DNS &et ADDS

Pour installer un contrôleur de domaine, deux rôles sont indispensables : **Le rôle DNS et ADDS**.
[Expliquer le rôle de ces services]

Rôle DNS (Domain Name System)

Le DNS est un service essentiel pour toute infrastructure réseau utilisant Active Directory. Son rôle est de convertir les noms de domaine (ex. : serveur.local) en adresses IP (ex. : 192.168.1.1) et vice versa, permettant ainsi aux ordinateurs et aux utilisateurs de localiser facilement les ressources réseau.

Le rôle AD DS permet de transformer un serveur en contrôleur de domaine.

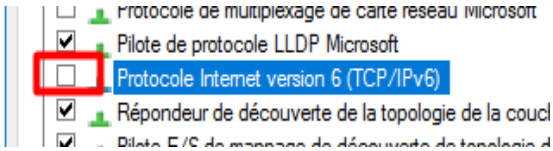
Voici le lien pour voir comment installer les rôles AD DS. Dans le cas où vous ne le savez pas encore.

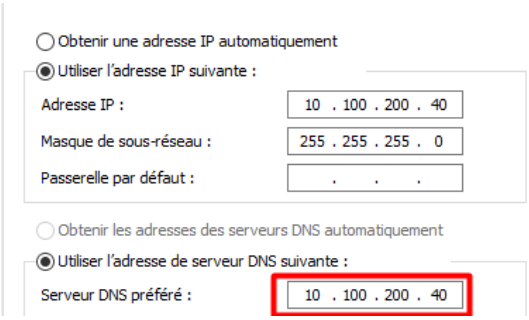
https://www.pc2s.fr/installation-dun-controleur-de-domaine-windows-serveur-2019-2016-2012-r2/

Pendant cette installation et configuration des rôles, vous aurez à tenir compte des précisions évoquées ci-dessous.

Configuration IP importante :

Pour la configuration IP, faire attention à décocher Ipv6 et mettre l'adresse DNS qui est l'IP de votre serveur. Cà ressemblera à ces captures avec votre adresse IP

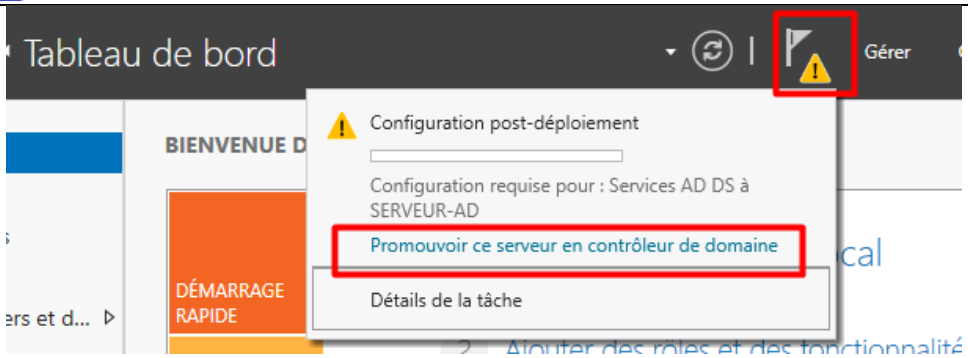




Promouvoir ce serveur en contrôleur de domaine

[Expliquer l'utilité de promouvoir ce serveur en contrôleur de domaine]

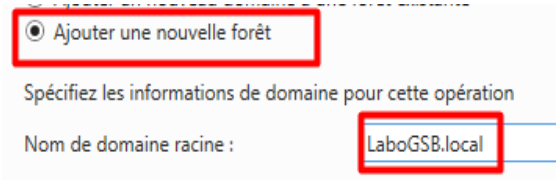
Voici quelques précisions très utiles pour vous aider dans votre installation/configuration



Ajouter une nouvelle forêt

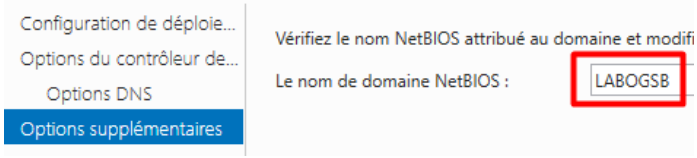
En sélectionnant « Ajouter une nouvelle forêt (aucune foret et domaine n'existe) »

Donner nom au domaine racine : **c**



IMPORTANT Mot de passe restauration annuaire : **utiliser le même mot de passe que celui du projet**

IMPORTANT Le nom de domaine NETBIOS : **LABOGSB « laissez celle proposée »**



Après cette configuration, le serveur redémarre (un peu long car AD et les services s'installent)
Après le redémarrage, vous verrez ceci

[Interpréter cet affichage]

Configuration du Contrôleur de domaine

Après avoir installé Active Directory AD DS, il faut configurer le contrôleur de domaine en y paramétrant certaines fonctionnalités très importantes comme DNS, NTP, ...

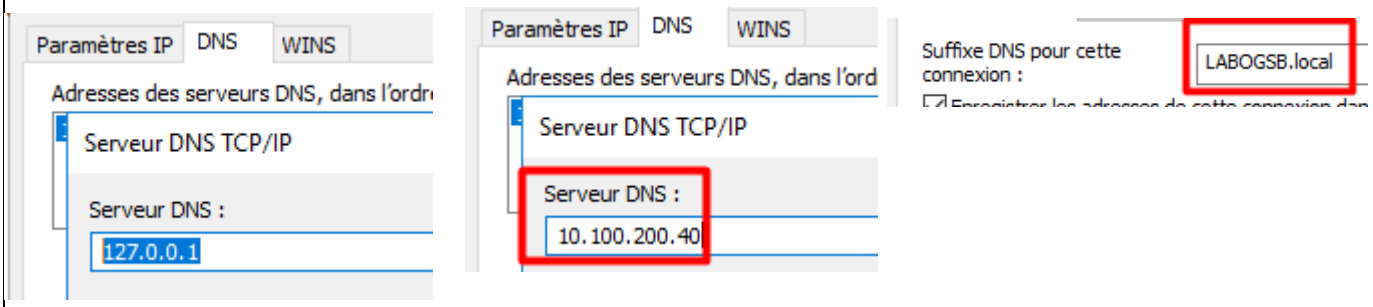
Voici le lien pour configurer AD

https://www.pc2s.fr/configuration-dun-controleur-de-domaine-windows-serveur/

IMPORTANT Voici quelques précisions très utiles pour vous aider dans votre installation/configuration

Pour le DNS
Mettre le nom complet du domaine dans « Suffixe DNS pour cette connexion » : **LABOGSB.local**

Comme ceci avec votre adresse IP



Configuration et optimisation du Service DNS

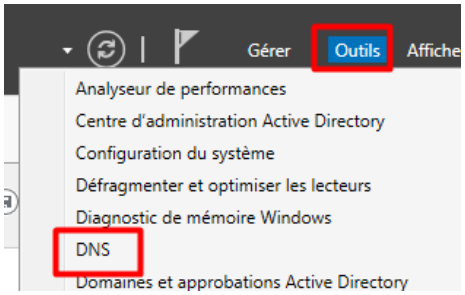
IMPORTANT

Voici quelques précisions très utiles pour vous aider dans votre installation/configuration

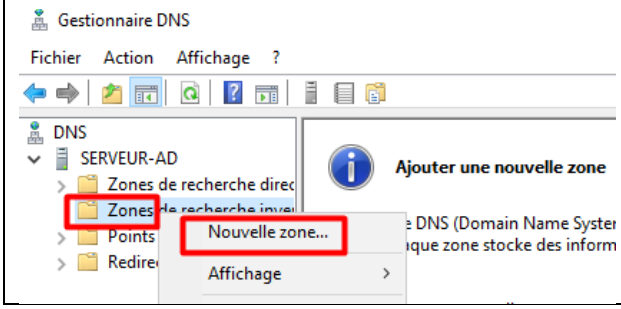
a) Configuration de la zone inversée

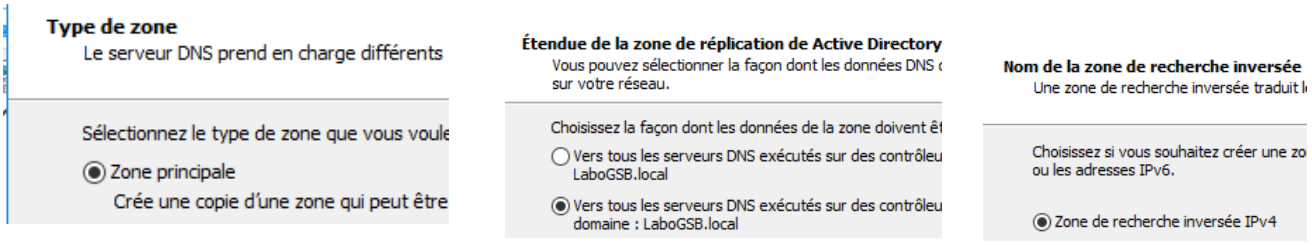
[Expliquer l'utilité de la zone principale et la zone inversée]

Pour cela aller dans le « gestionnaire de serveur » puis dans l'onglet « outils » sélectionner « DNS » comme ceci :



Puis pour la zone de recherche inversée





: ID réseau est l'adresse réseau dans lequel se trouve votre serveur

A la suite de cette création vous aurez un résultat comme ceci

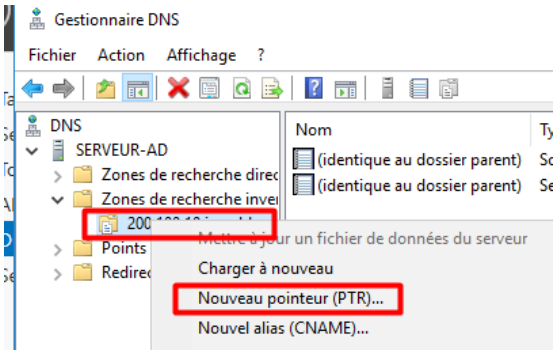
Ajout d'un Pointeur (PTR) sur le Serveur

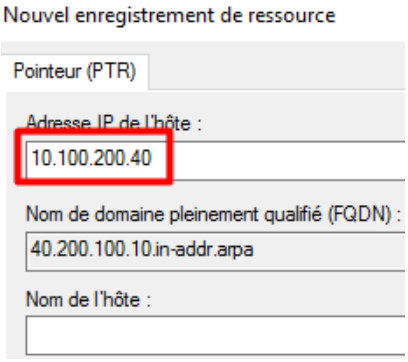
Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration

[Expliquer l'utilité du pointeur (PTR)]

Ces enregistrements sont essentiels pour la résolution inversée de noms, c'est-à-dire la traduction d'une adresse IP en un nom de domaine

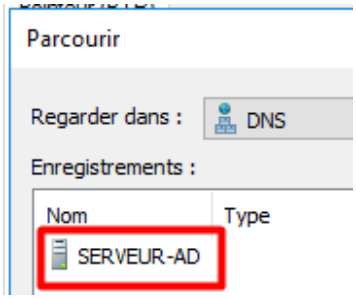
Pour cela, Clic droit sur la nouvelle zone inversée et y créer le pointeur

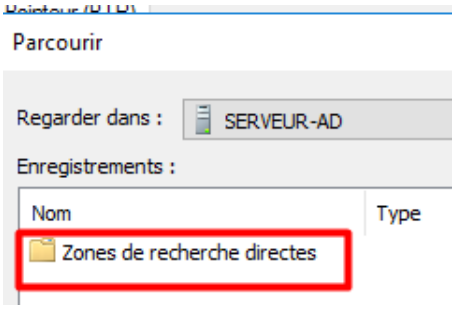


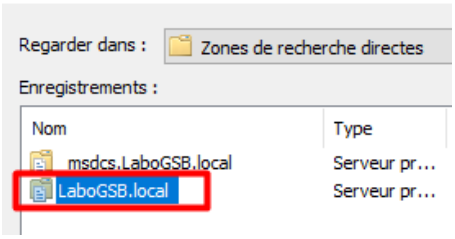


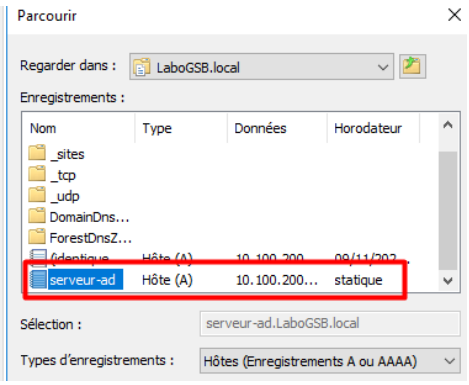
Mettre l'adresse IP de votre serveur et le nom complet

Puis

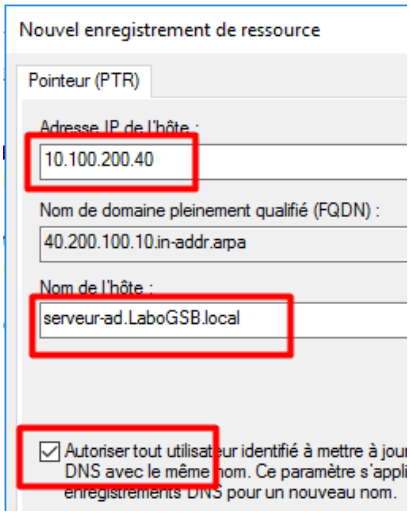








Vous aurez au final ce résultat

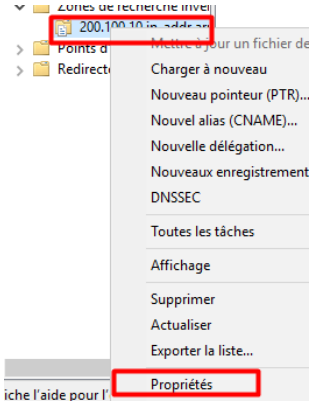


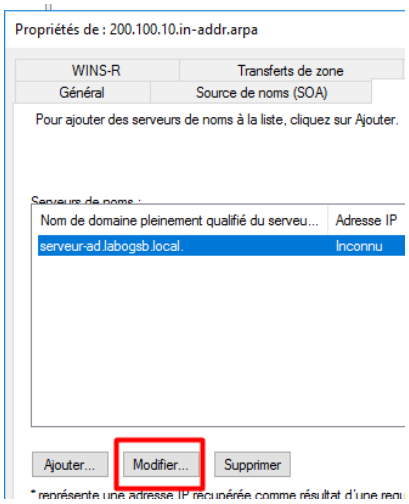
Enregistrement du pointeur dans la zone directe

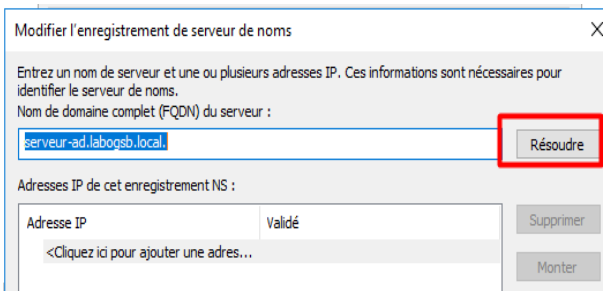
Une fois le pointeur crée, aller dans la « Zones de recherche directes » :

Clic droit sur le serveur-ad puis sur « propriétés » et Cocher **« Mettre à jour l'enregistrement de Pointeur PTR associé »** et **« appliquer »**

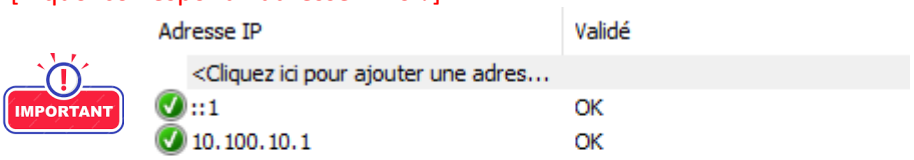
Ajouter l'adresse IP du serveur au niveau de la zone inversée, il faut faire comme ceci :



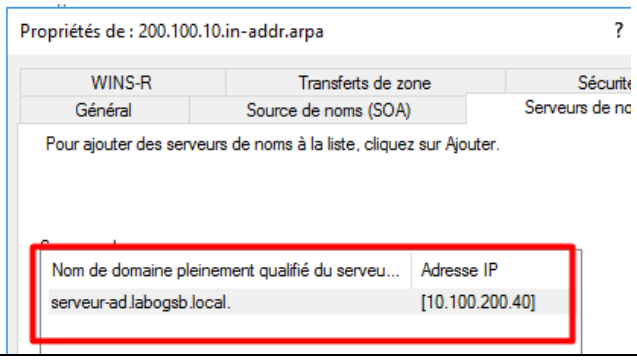




Vous aurez 2 adresses IPV4 et IPV6 qui s'affichent
[A quoi correspond l'adresse IPV6 ?]



Résultat s'affiche, valider cette adresse en clic sur « appliquer » puis « ok »

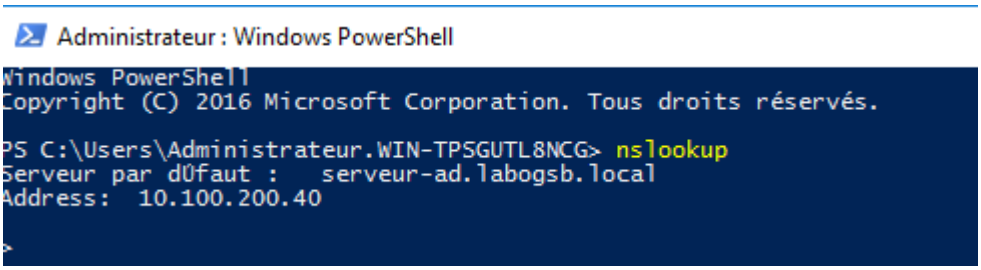


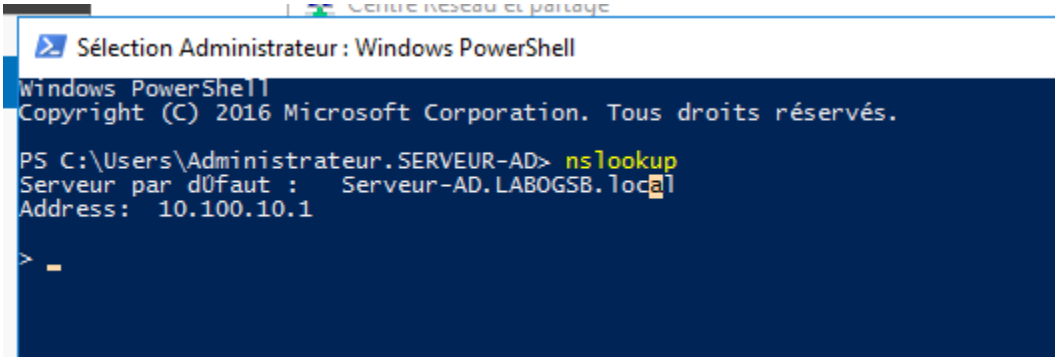
Vérification de la configuration DNS

On va vérifier les zones directes et inversée qu'on vient de créer et configurer

Dans l'invite de commande ou dans PowerShell le avec la commande « **nslookup** »

[Interpréter ce résultat, en un paragraphe]





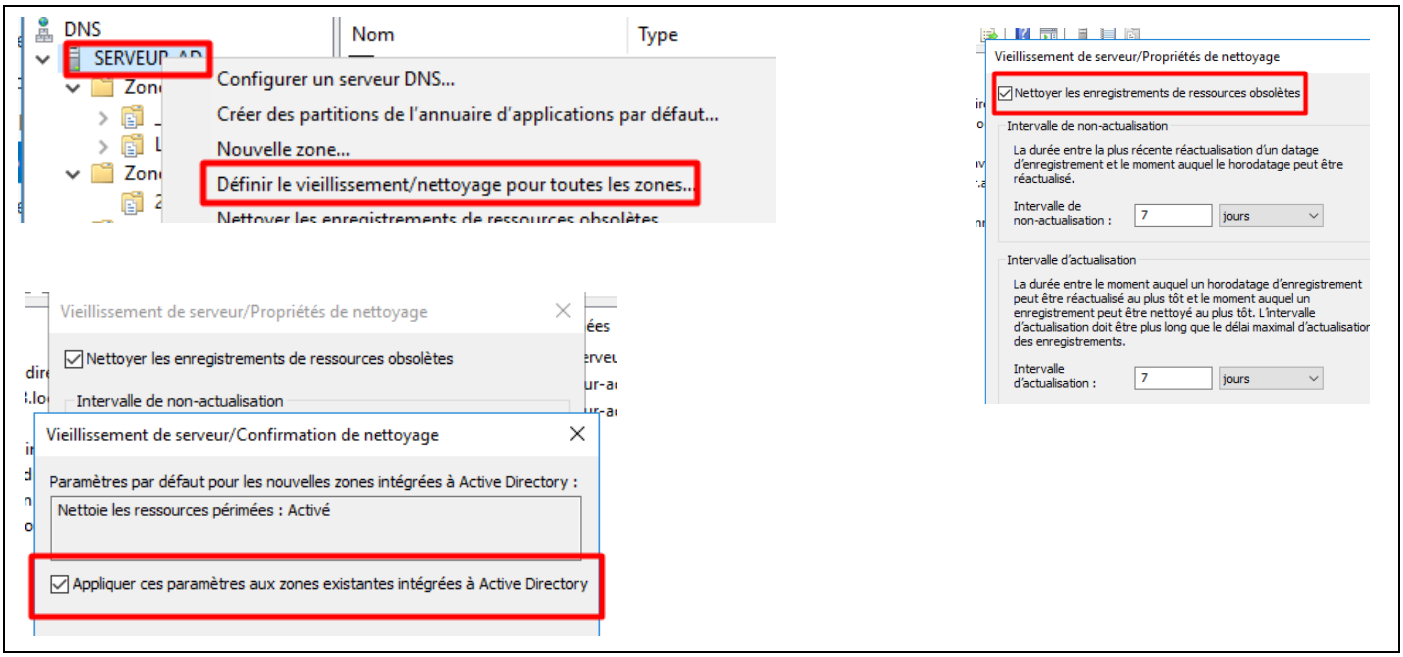
Définir le vieillissement et nettoyage de toutes les zones

[Expliquer l'utilité de cette manipulation, en un paragraphe et avec vos propres mots]

Configuration du vieillissement

Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration

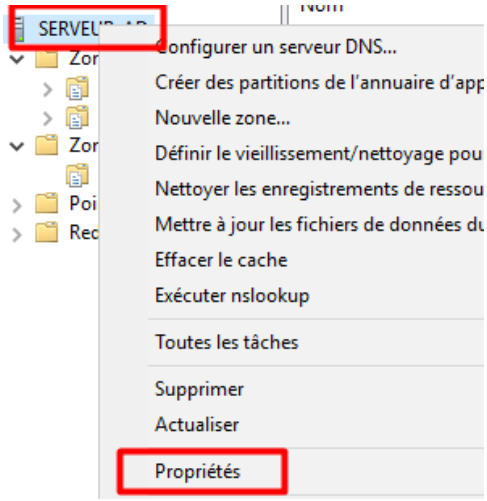
Pour cela, dans le « gestionnaire DNS » clic droit sur le Serveur-AD

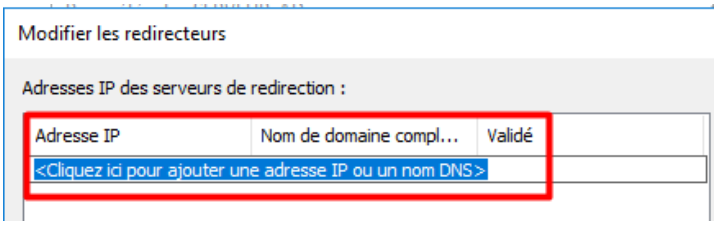


Configuration des redirecteurs

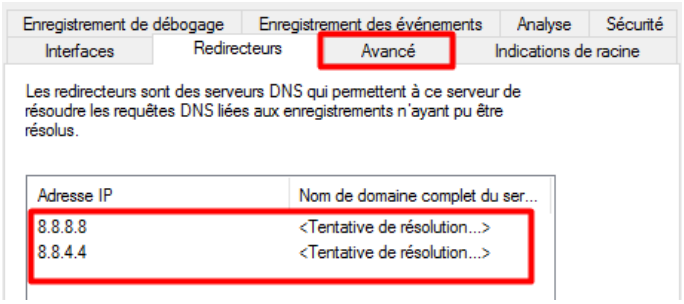
[Expliquer l'utilité de ces redirecteurs, en un paragraphe et avec vos propres mots]

Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration



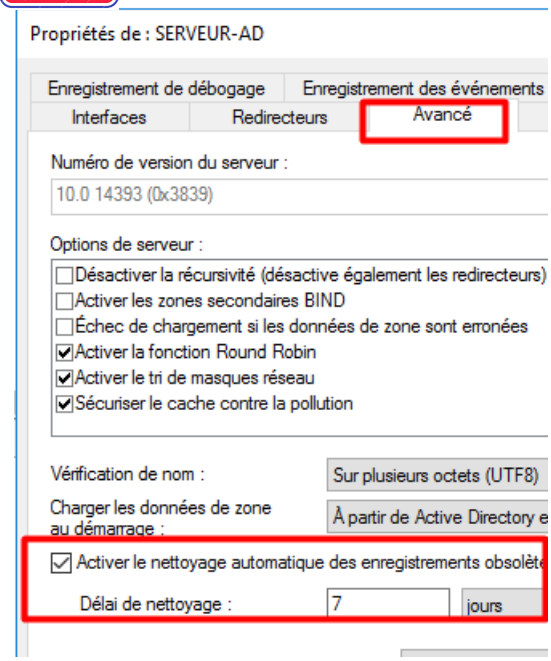


Après ces ajouts, on voit que le résultat suivant :



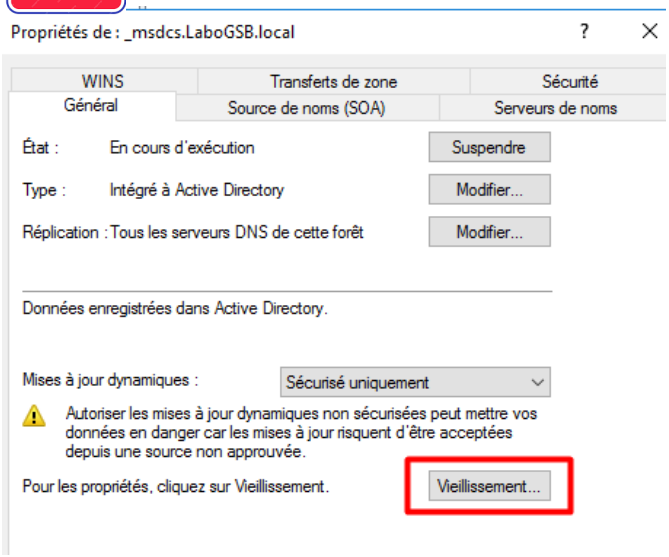
Activation du nettoyage automatique

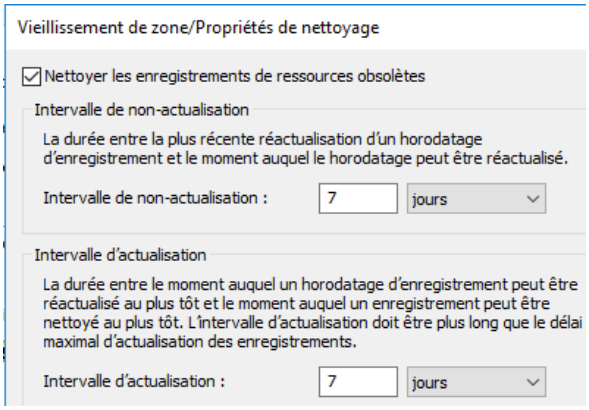
Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration



Vérification que le vieillissement est bien activé

Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration





1- Quelques paramétrages importants

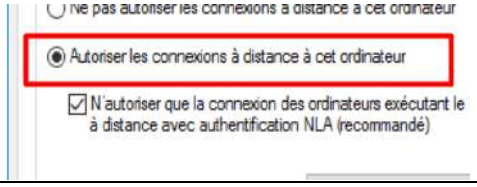
a) Activation du bureau à distance

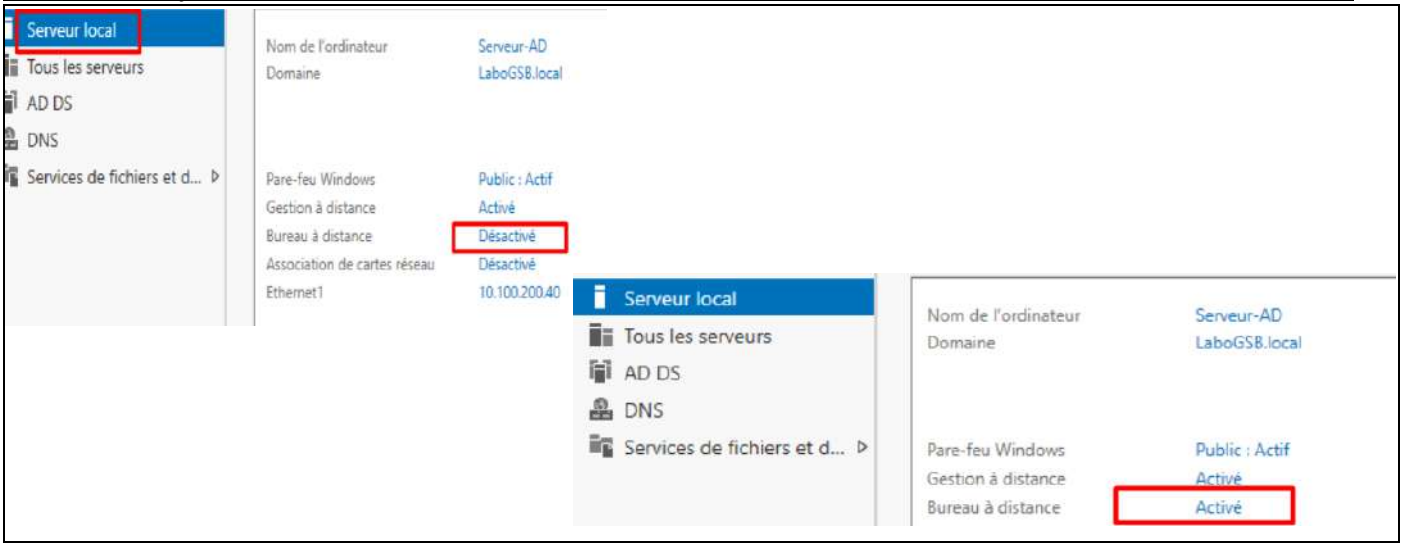
[Expliquer l'utilité de ce changement en un paragraphe et avec vos propres mots]

Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration

Pour cela, retournez dans le gestionnaire de serveur pour

Pour le bureau à distance





Paramétrage du navigateur par défaut Internet explorer

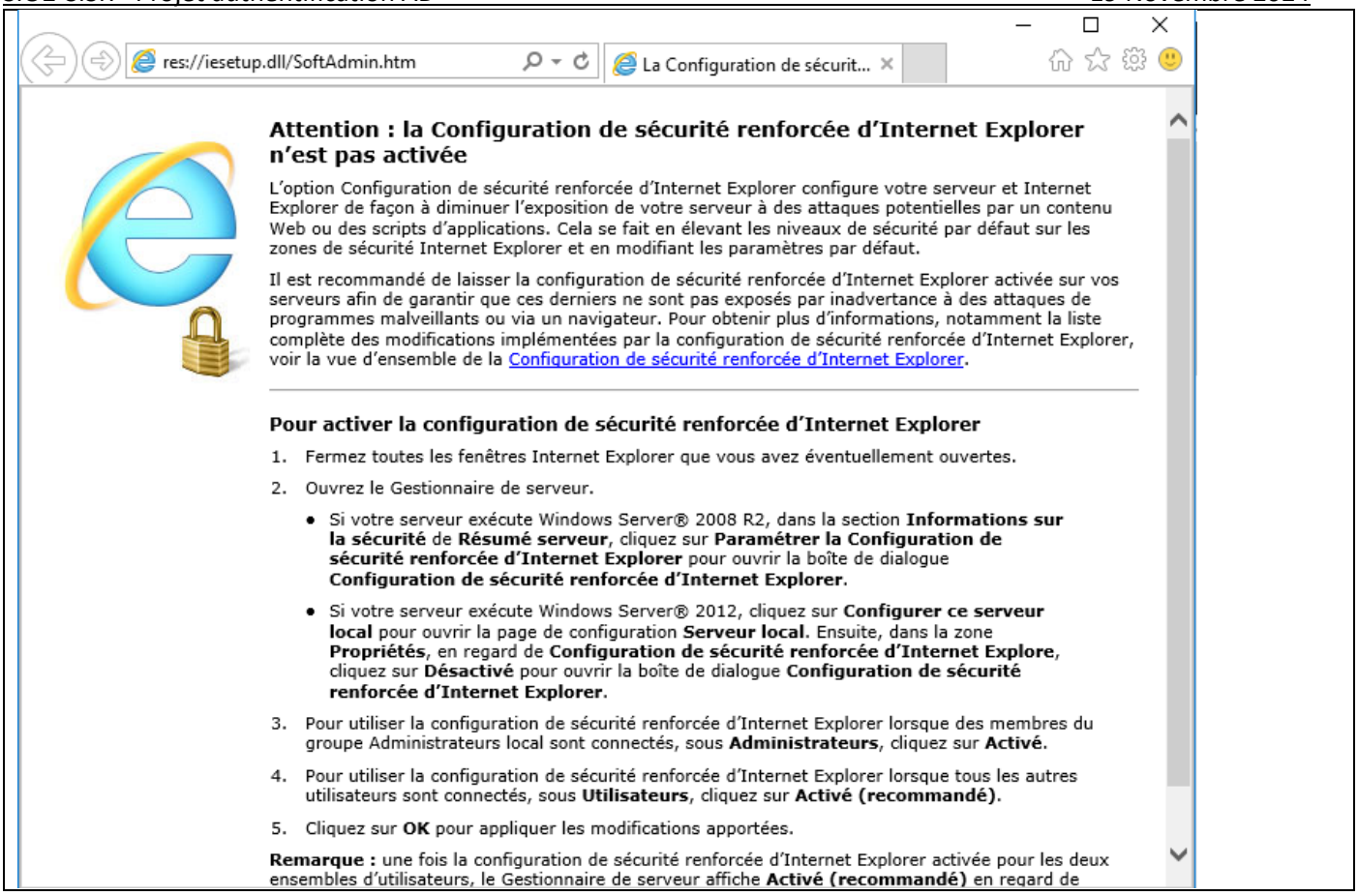
[Expliquer l'utilité de ce changement en un paragraphe et avec vos propres mots]

IMPORTANT

Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration

Clic sur « Actif » pour le paramétrage

Vérifier la désactivation en lançant le navigateur
[Qu'est-ce que vous observez ?]

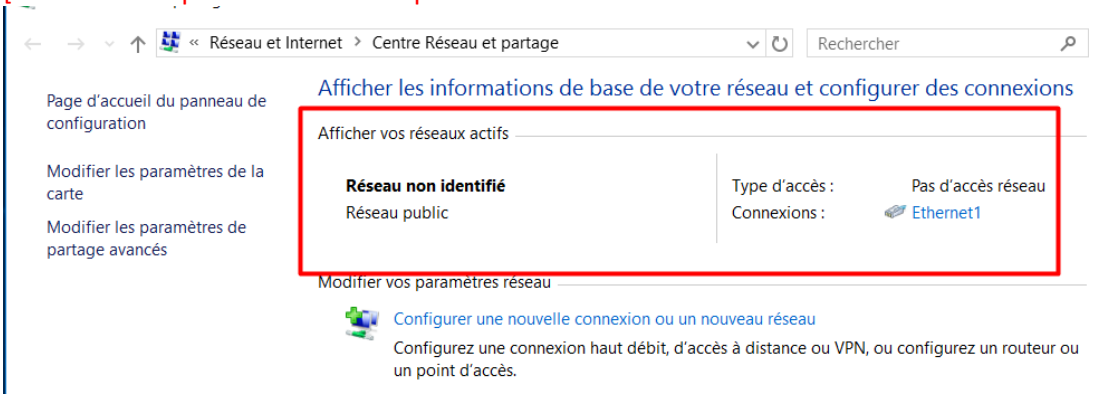


Vérification du profil réseau du contrôleur de domaine

En regardant dans les paramètres de la carte réseau du « Centre Réseau et Partage », il faut voir le nom du domaine configuré précédemment.

IMPORTANT Voici quelques précisions très utiles pour vous aiguiller dans votre installation/configuration

[Mettre une capture montrant les paramètres de la carte réseau du « Centre Réseau et Partage », comme ceci]



IMPORTANT Redémarrer le serveur pour que tous les paramétrages précédents soient pris en comptes

Si après le redémarrage le résultat est le même que ci-dessus et qu'on ne voit toujours pas affiché le domaine LABOGSB.local il faudra modifier la base de registre « regedit »

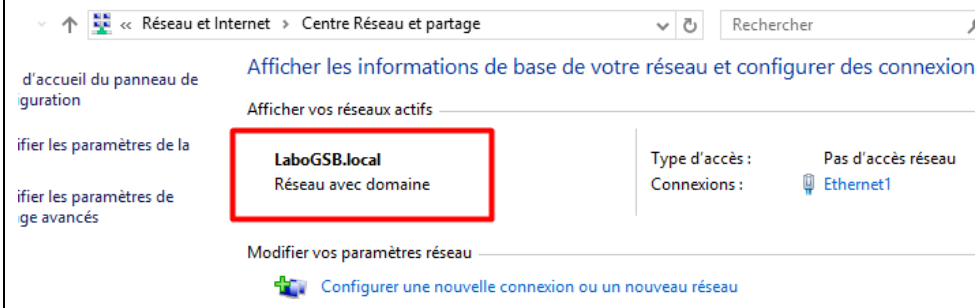
Il faut alors ajouter les Services « DNS » et « NTDS » aux dépendances du Service « NlaSvc » pour qu'ils se lance au démarrage.

Lancer « regedit » et aller à l'emplacement suivant :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc
Sélectionner : **DependOnService**

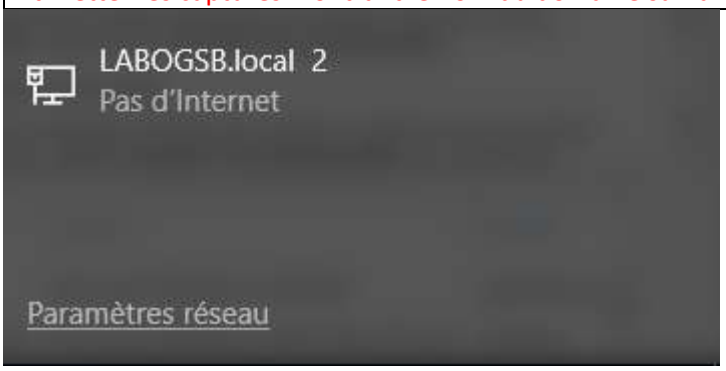
IMPORTANT

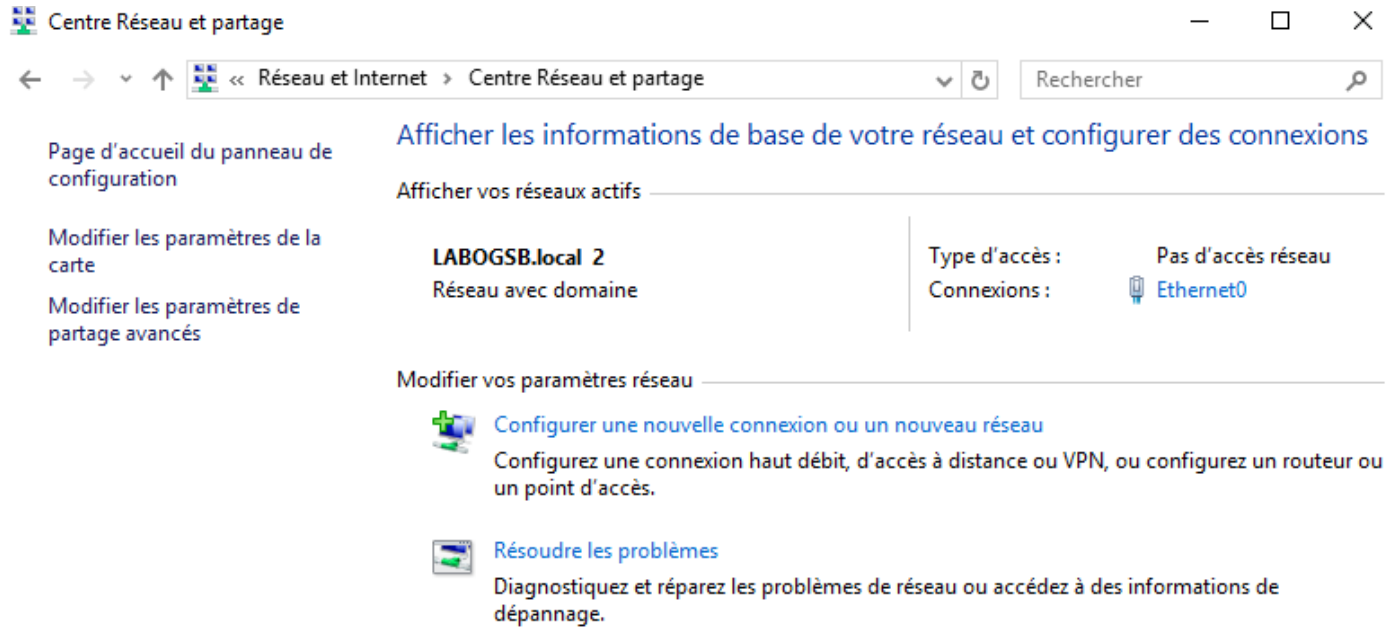
Redémarrer le serveur pour que tous les paramétrages précédents soient pris en comptes

[Mettre une capture montrant que le nom du domaine est bien pris en compte sur « Centre Réseau et Partage »] comme ceci]



Et mettez les captures montrant le nom du domaine sur la fenêtre d'accueil du serveur et sur la barre de tâche.





[Capture montrant les rôles installés sur ce serveur, l'ensemble est visible sur le gestionnaire de serveur]

Fin de la partie 1

Partie 2 : Gestion des comptes utilisateurs et ajout des machine clientes au domaine

Etapes de la réalisation

Cette partie traite de la gestion des objets (utilisateurs, ordinateurs, etc.) dans l'annuaire du domaine AD

Contenu :

- ⇨ *Ajouter une machine au domaine*
- ⇨ *Présentation de l'outil « Utilisateurs et ordinateurs Active Directory »*
- ⇨ *Création des comptes utilisateurs*
- ⇨ *Création des groupes utilisateurs*
- ⇨ *Création des unités d'Organisation « OU »*
- ⇨ *Gérer des profils en fonction des utilisateurs*
- ⇨ *Gestion des dossiers personnels*

Ajout des deux machines clientes dans le domaine LaboGSB

Configurer IP du client :

- Vérifier que vous avez bien ajouté l'adresse DNS sur toutes les machines
- A ce stade tous vos Ping fonctionnent normalement sans problème

Vérifier que le ping fonctionne entre ce client et le serveur

[Capture montrant les Ping entre le serveur vers les 2 clients]

```
C:\Users\azizb>ping 10.100.10.1

Envoi d'une requête 'Ping'  10.100.10.1 avec 32 octets de données :
Réponse de 10.100.10.1 : octets=32 temps<1ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps<1ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps=1 ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 10.100.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Vérifier que ces clients communiquent bien avec votre contrôleur de domaine

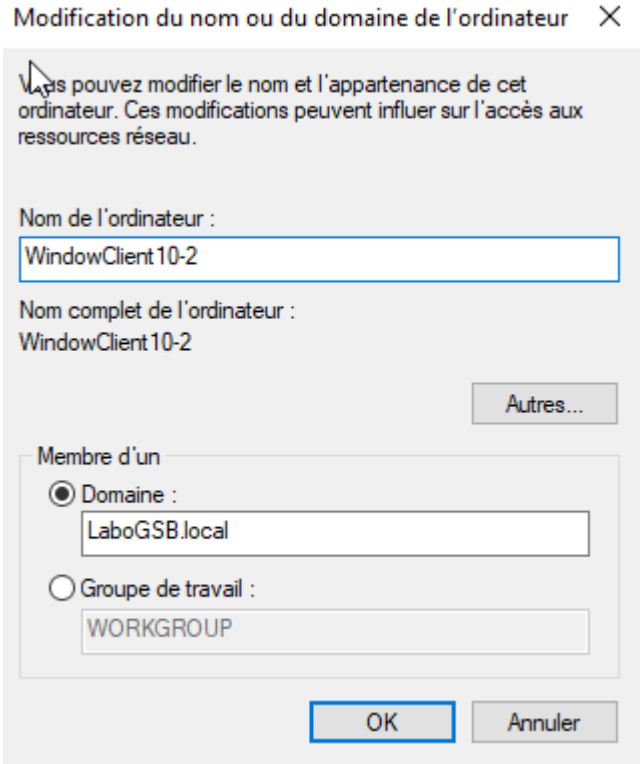
Grâce à la commande : **ping labogsb.local**

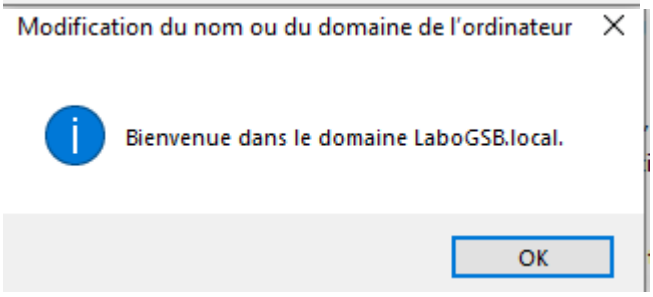
```
C:\Users\azizb>ping labogsb.local

Envoi d'une requête 'ping' sur labogsb.local [10.100.10.1] avec 32 octets de données :
Réponse de 10.100.10.1 : octets=32 temps<1ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps=1 ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps<1ms TTL=128
Réponse de 10.100.10.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.100.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

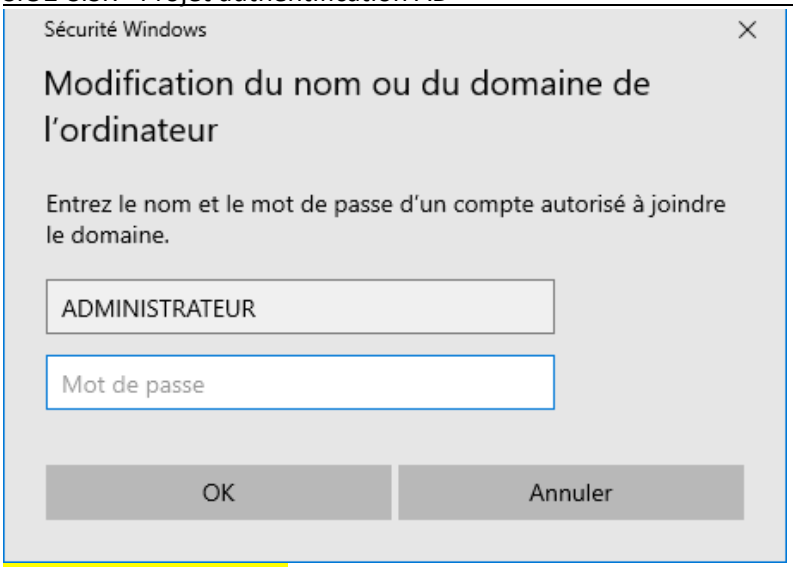
Si vous avez une erreur cela veut dire que vous l'adresse DNS n'est pas correcte sur ces clients.
Et corriger votre erreur ! et mettre la capture qui montre que tout est bon.

Sur AD, vérifier qu'aucun ordinateur n'y est enregistré. Pour cela, allez dans l'OU « computers »
[Capture montrant cette vérification]

Il faut maintenant ajouter les 2 clients sur AD

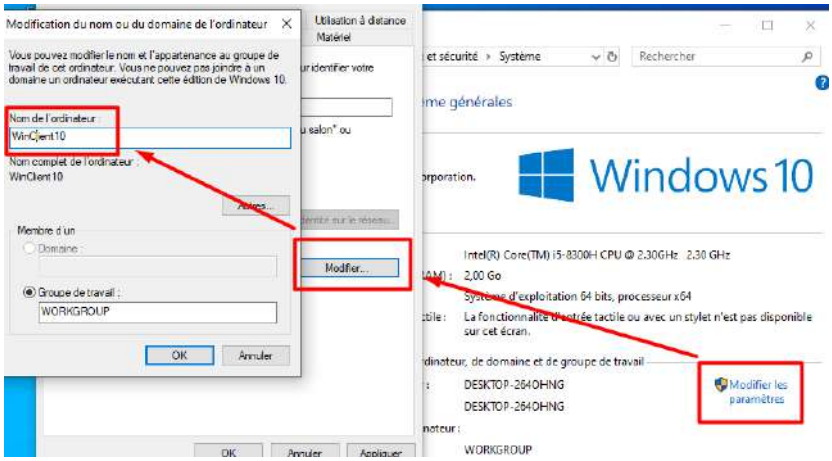






Ajout de WinClient10-2

Pour joindre une machine au domaine, il faut se connecter à la machine cliente en tant qu'**administrateur**



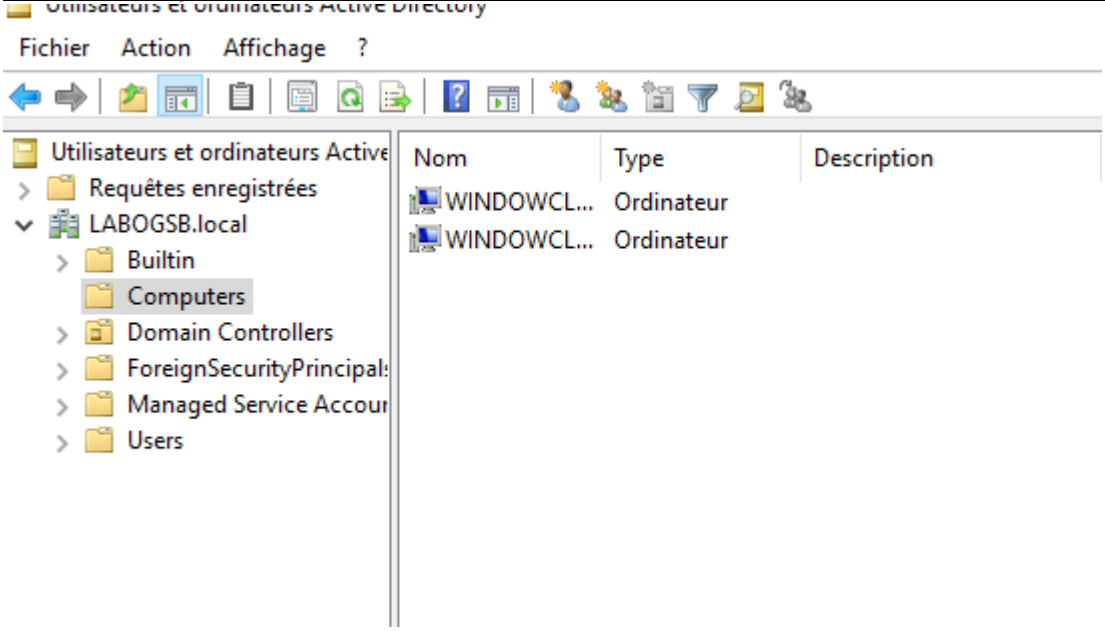
- Se connecter à la machine cliente WinClient10-2
- Aller dans « Système » clic sur « Modifier les paramètres
- Saisir « Deuxième client AD » dans description de l'ordinateur
- Puis clic sur « Modifier » et taper ensuite le nom du domaine **LaboGSB** auquel il doit être ajouté
- Le système vous demande une authentification, mettre le compte administrateur de ce domaine.
- Redémarrer la machine

Suite au redémarrage du client, vous devez pouvoir vous connecter avec le compte « administrateur du domaine, Puis, sur AD, vous allez retrouver cette machine dans votre annuaire au sein de l'UO« **Computers** ».

Ajout de WinClient10-1

Faire les mêmes étapes comme pour le client ci-dessus afin d'ajouter ce PC dans AD.

[Capture montrant bien que les 2 clients sont ajoutés, dans « computers » du serveur AD]



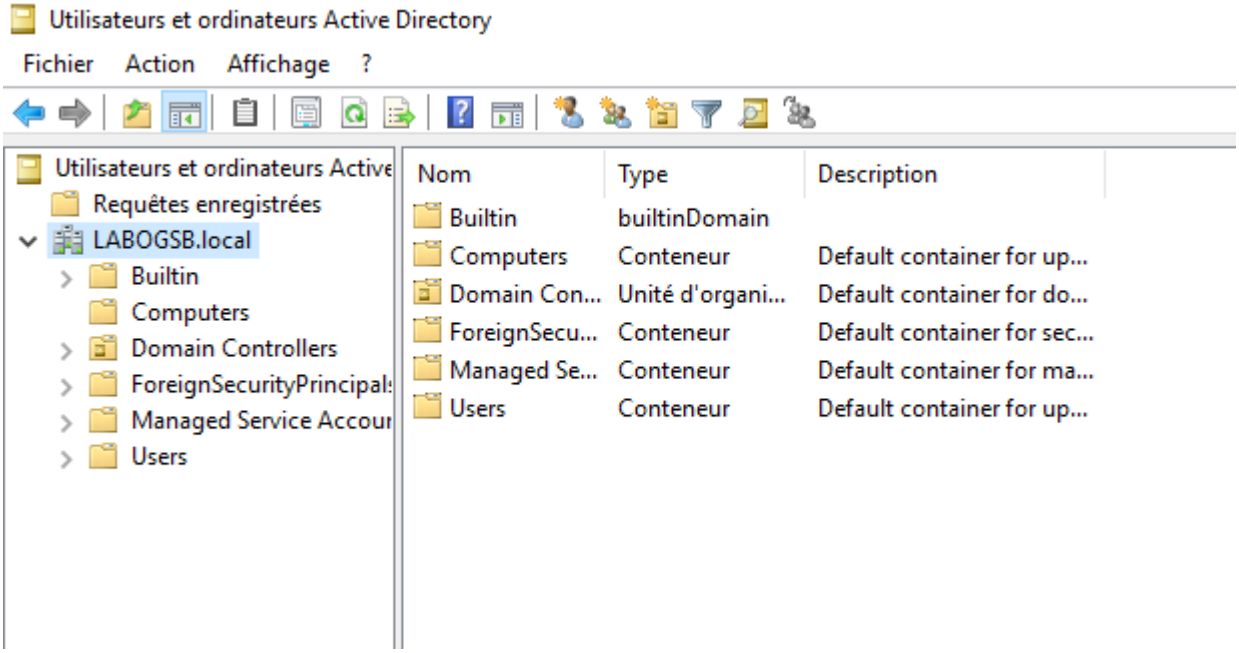
Présentation de l'outil « Utilisateurs et ordinateurs Active Directory »

L'outil « **Utilisateurs et ordinateurs Active Directory** »

[Expliquer l'utilité et le fonctionnement de cet outil, en un seul paragraphe et avec vos propres mots]

L'outil **« Utilisateurs et ordinateurs Active Directory »** est une console d'administration utilisée dans les environnements Windows pour gérer les objets d'un domaine Active Directory

Quand on lance l'outil « **Utilisateurs et ordinateurs Active Directory** »
On y trouve le nom du domaine **LaboGSB.local**. En développant ce dernier, on retrouve tous les objets sous forme d'une arborescence qui contient plusieurs dossiers.
[Ajouter les captures montrant ces dossiers]



[Lister les différents objets visibles et présenter l'utilité de chacun, faire une phrase simple et claire avec vos propres mots]

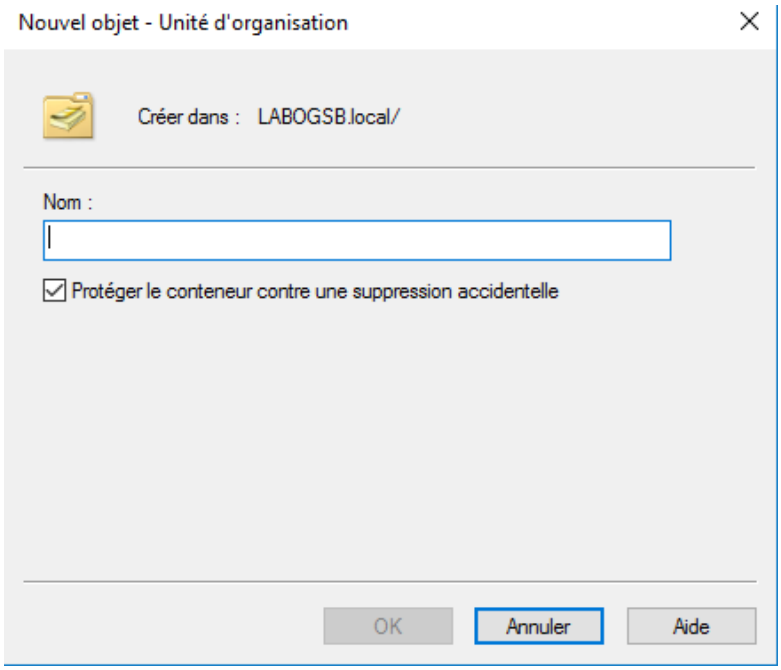
- **Builtin** : C'est un dossier qui contient des groupes prédéfinis pour gérer les droits d'accès (comme les administrateurs).
- Computers : C'est là où sont enregistrés les ordinateurs qui font partie du réseau.

 Domain **Controllers** : C'est le dossier des serveurs qui gèrent la sécurité et les connexions des utilisateurs au réseau.
 ForeignSecurityPrincipals : Il sert à reconnaître des utilisateurs ou groupes venant d'un autre réseau.
 Managed Service Accounts : Ce sont des comptes spéciaux pour les services (programmes) qui changent leurs mots de passe automatiquement.
 Users : C'est le dossier où se trouvent tous les comptes des utilisateurs et groupes du réseau.

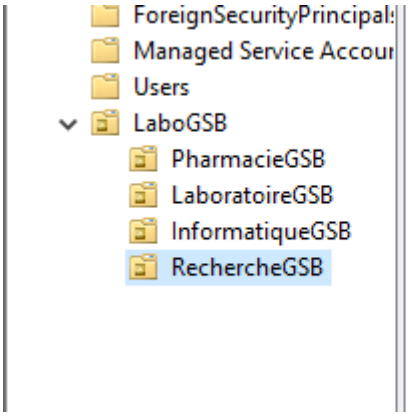
Création des unités d'Organisation « OU »

Les **OU (Unités d'Organisation)** servent à organiser les utilisateurs, groupes, ordinateurs et autres objets dans Active Directory, pour faciliter la gestion et appliquer des stratégies

[Pour la création des OU, mettre quelques captures : une capture montant comment et une autre montrant le résultat de l'ensemble des OU créées suffisent]



-
- Créer l'OU générale : **LaboGSB**
-
- Créer les sous-OU : **PharmacieGSB, LaboratoireGSB, InformatiqueGSB, RechercheGSB** dans LaboGSB



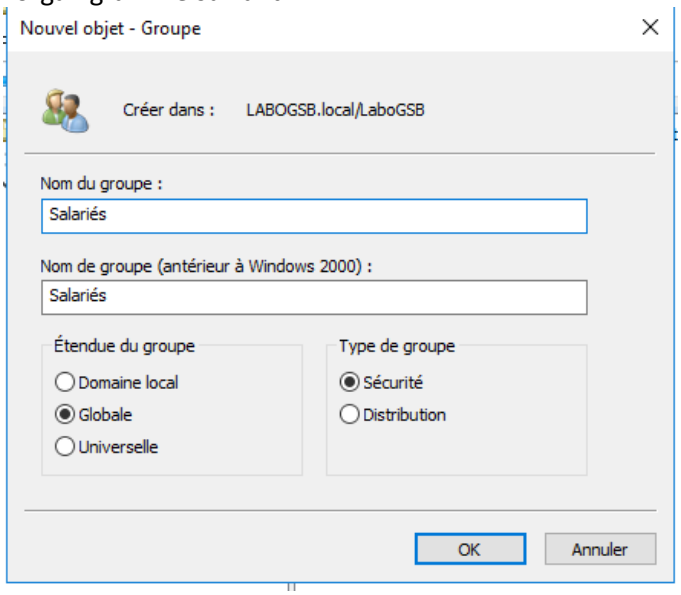
Création des groupes d'utilisateurs

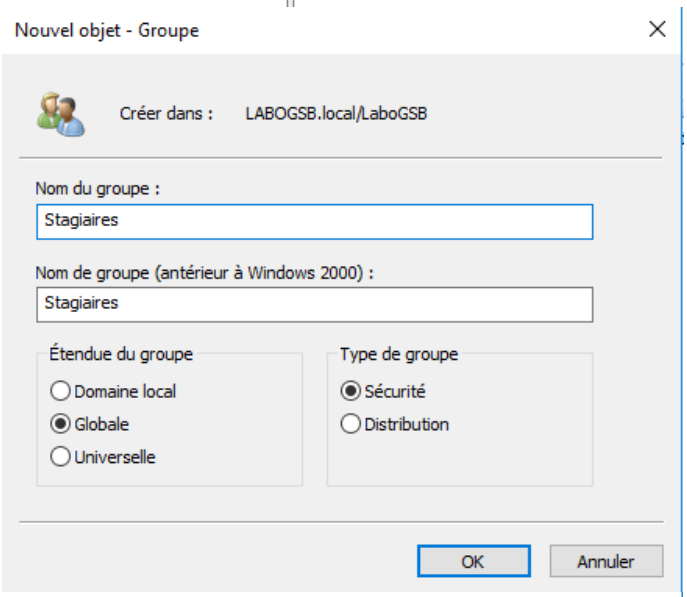
[Expliquer l'utilité des groupes, en une seule phrase et avec vos propres mots]

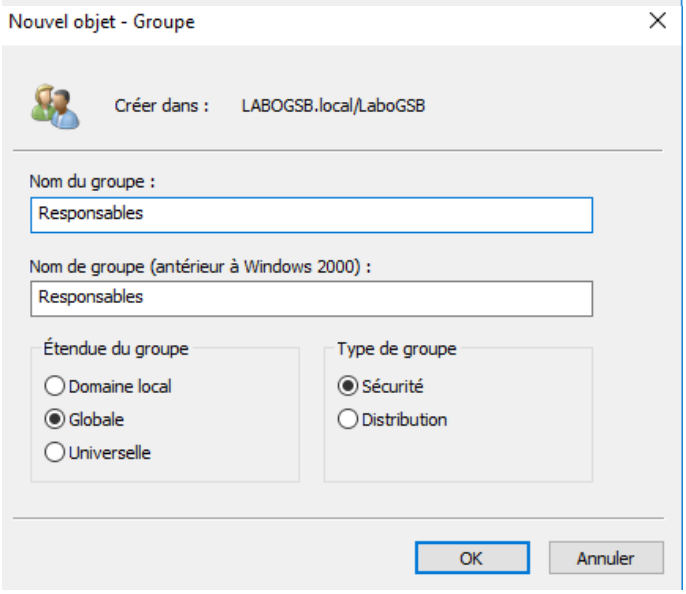
Les groupes d'utilisateurs dans Active Directory (AD) permettent de centraliser et de simplifier la gestion des autorisations

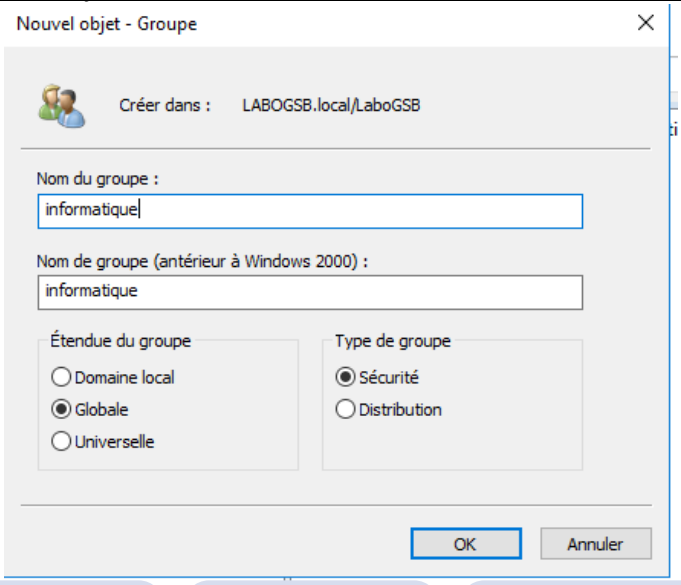
[Mettre 4 Captures montrant l'ajout d'un seul groupe créé, un seul exemple est suffisant]

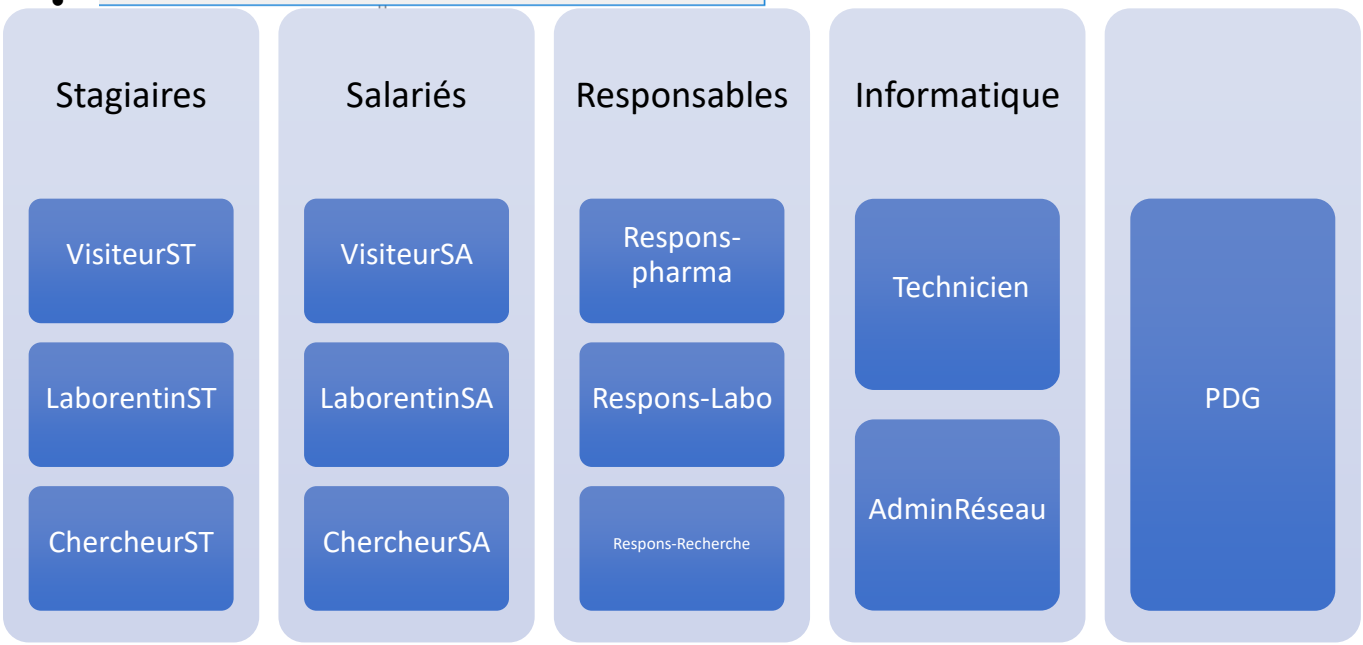
- Créer les groupes suivants : **Salariés, Stagiaires**, **Responsables**, **informatique** comme vous pouvez le voir sur l'organigramme suivant :





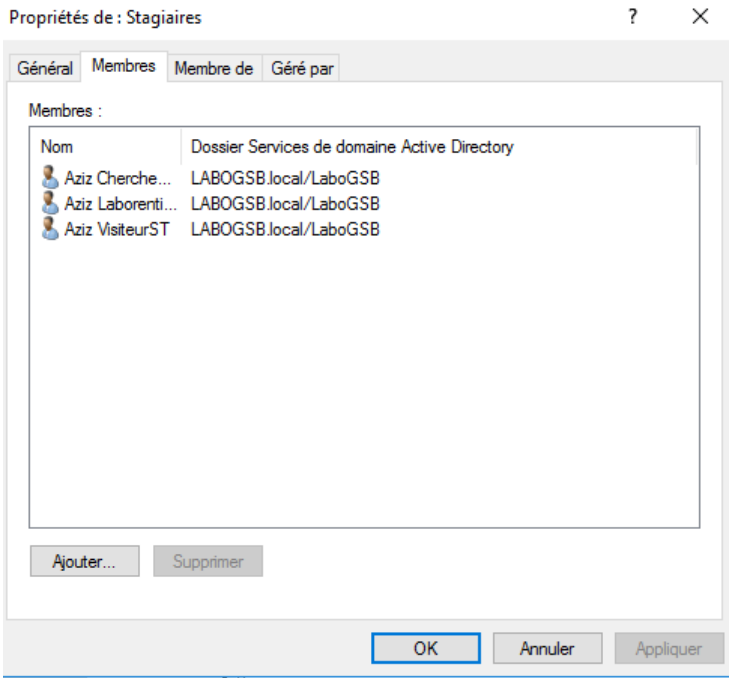


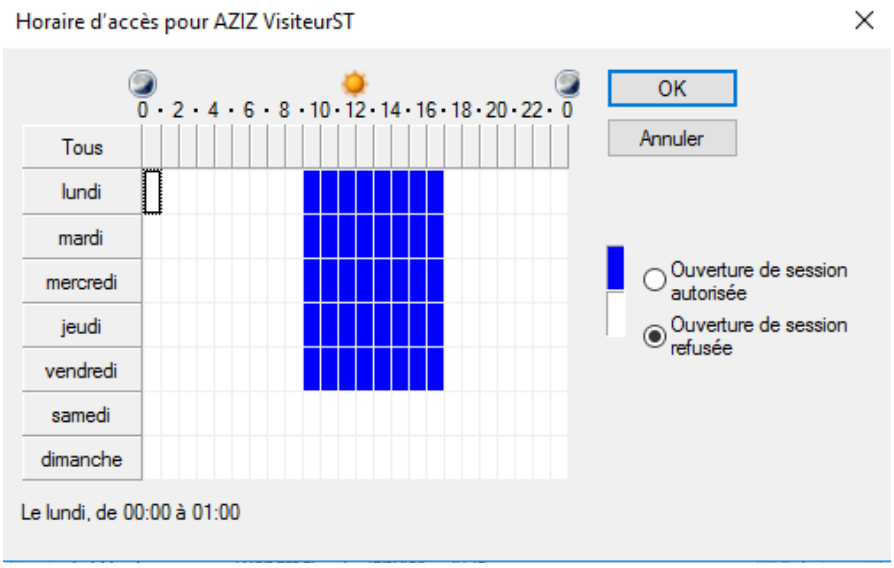




Création des comptes utilisateurs

[Pour la création des comptes, mettre 4 Captures montrant l'ajout d'un compte créé, **il faut un exemple pour chaque catégorie**]





Contraintes liées au compte

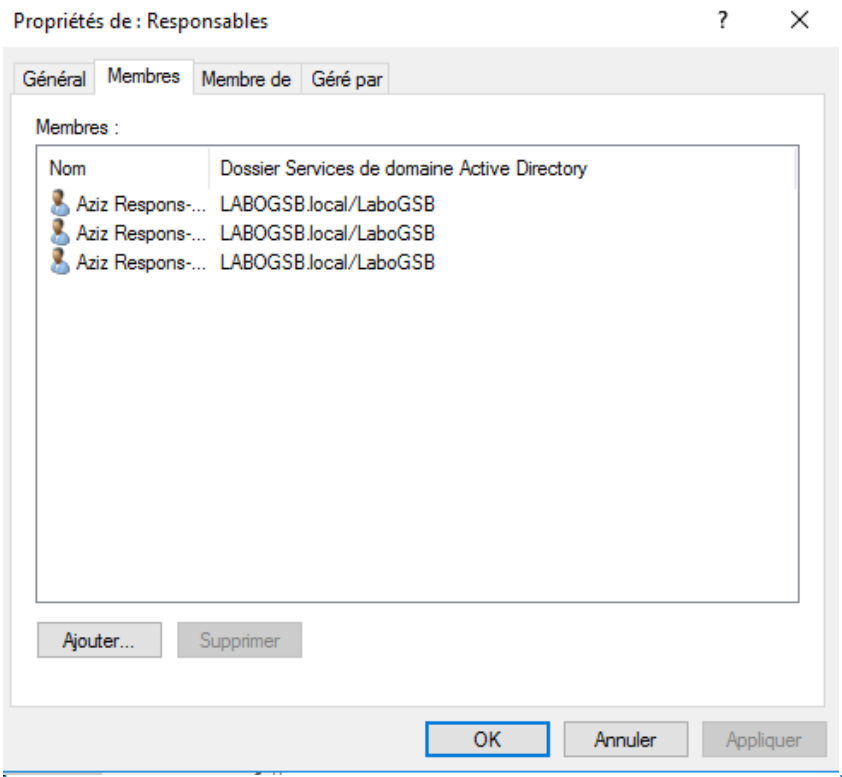
Voici tous les éléments dont vous avez besoin **pour créer les utilisateurs dans « OU global» LaboGSB**
Pour créer les comptes de chaque utilisateur ci-dessus, il faudra respecter les contraintes suivantes :

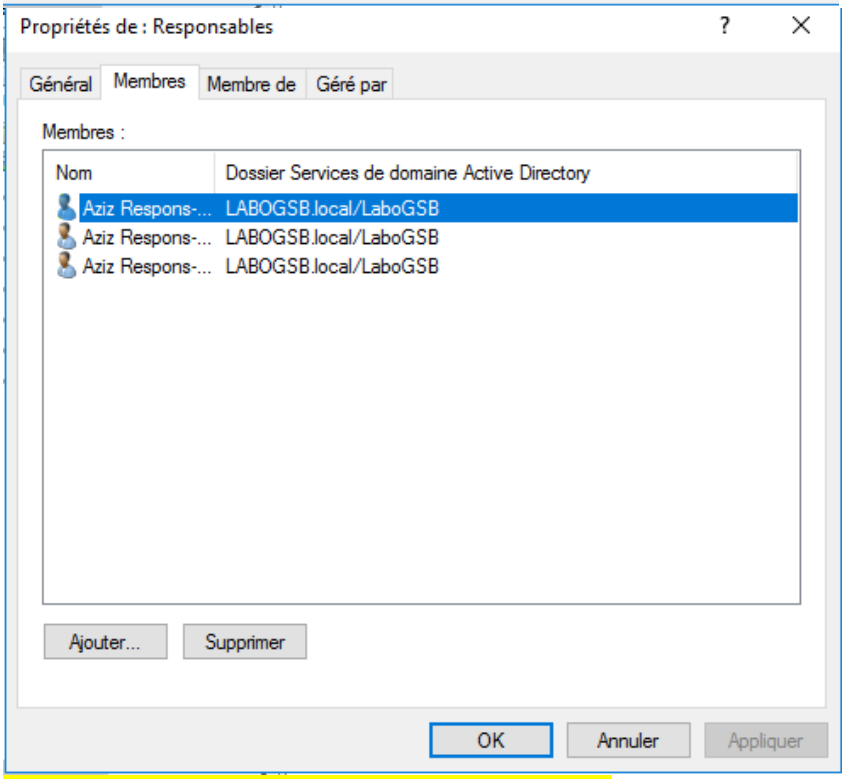
- Le nom des utilisateurs sont ceux que vous voyez sur l'organigramme : VisiteurST, ... et le prénom est le vôtre pour l'ensemble des utilisateurs.
- Chaque utilisateur aura un login suivant : **votre prénom.nomcomplet**
  - **Par exemple :** brigitte.VisiteurST avec pour prénom Brigitte et pour nom VisiteurST
- Mot de passe pour tous ces nouveaux utilisateurs : gsb@2024
- **COCHER** seulement « **L'utilisateur ne doit pas changer son mot de passe »**
- Faire en sorte que les utilisateurs puissent se connecter du Lun à Ven de
  - Pour les stagiaires de 9h – 17h
  - Les salariées de 8h à 19h
  - Tous les responsables de 7h à 20h

Après la création de tous les utilisateurs, il faut maintenant les affecter dans les **groupes et OU**

- Affecter les comptes utilisateurs aux groupes correspondants
- Affecter les groupes aux UO appropriées

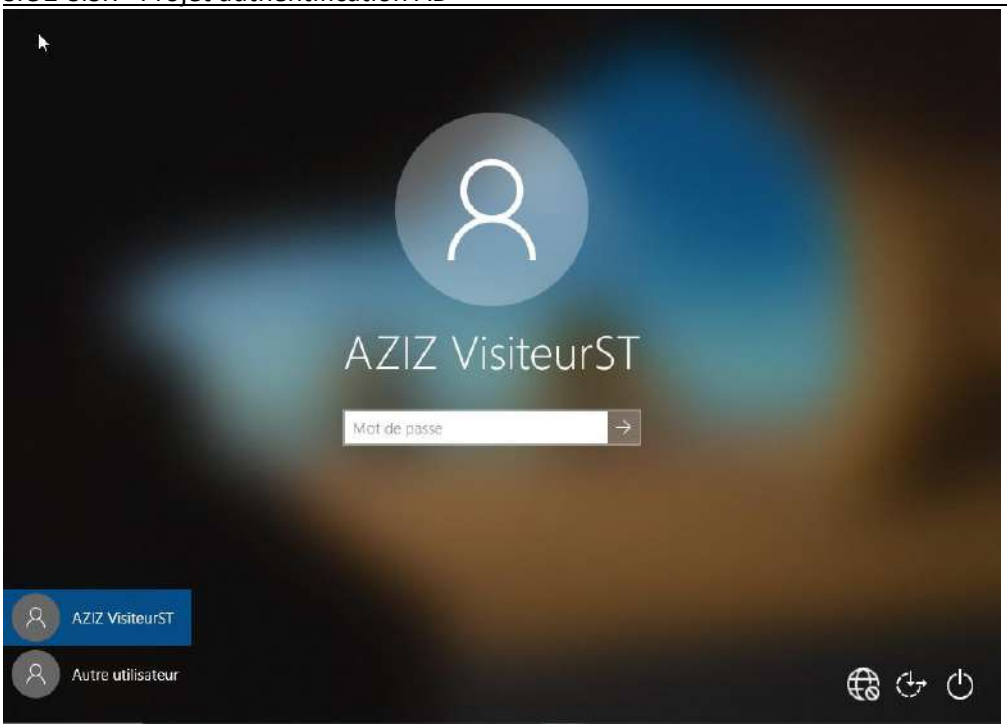
- [Toutes les captures montrant ces affectations, il faut une capture d'affectation pour chaque catégorie et une capture montrant le résultat de l'ensemble des affectations]





Vérification avec la machine cliente WinClient10-2

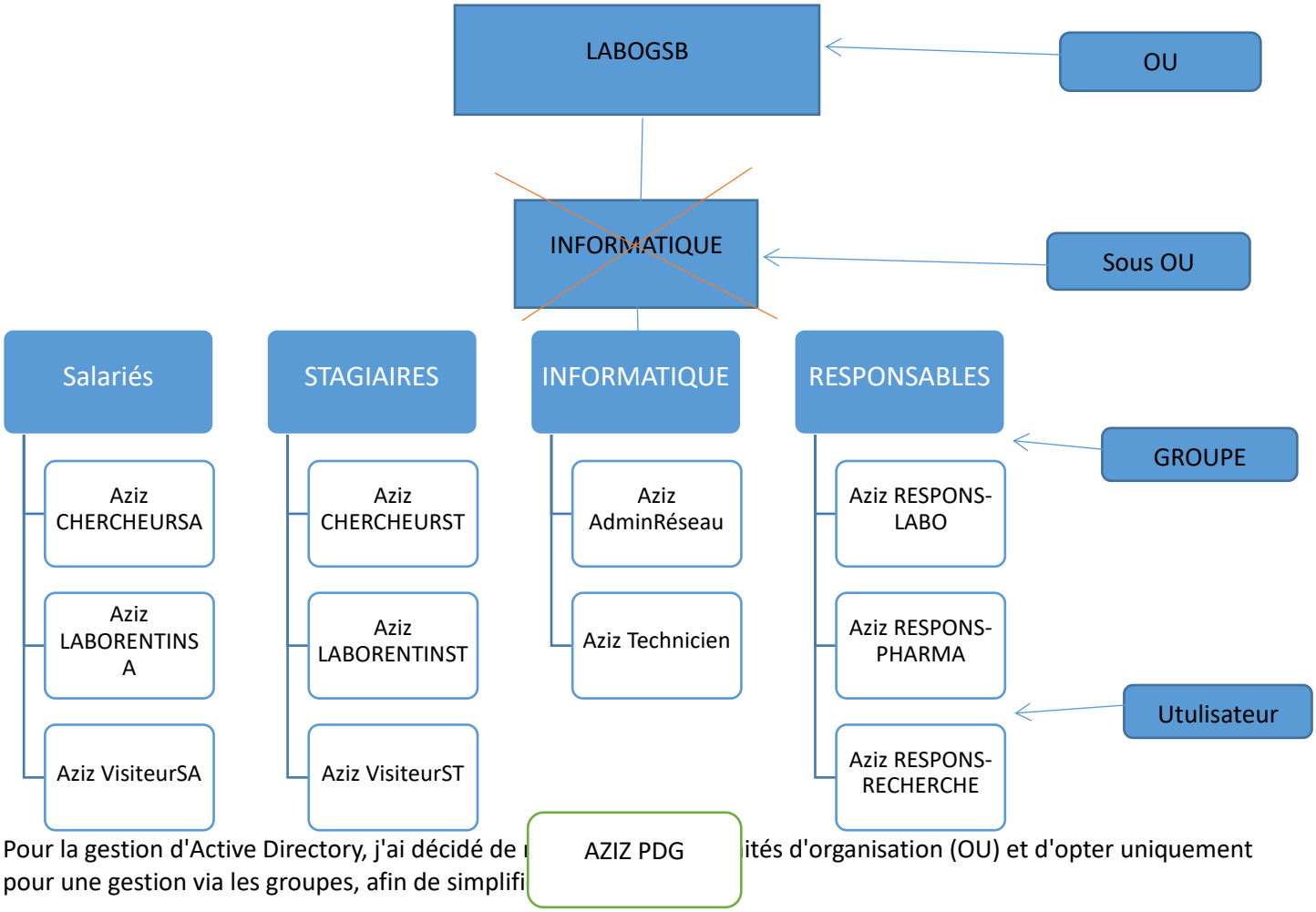
Connectez-vous avec un utilisateur de chaque domaine pour vérifier les sessions créées et tester le fonctionnement de l'autorisation horaire



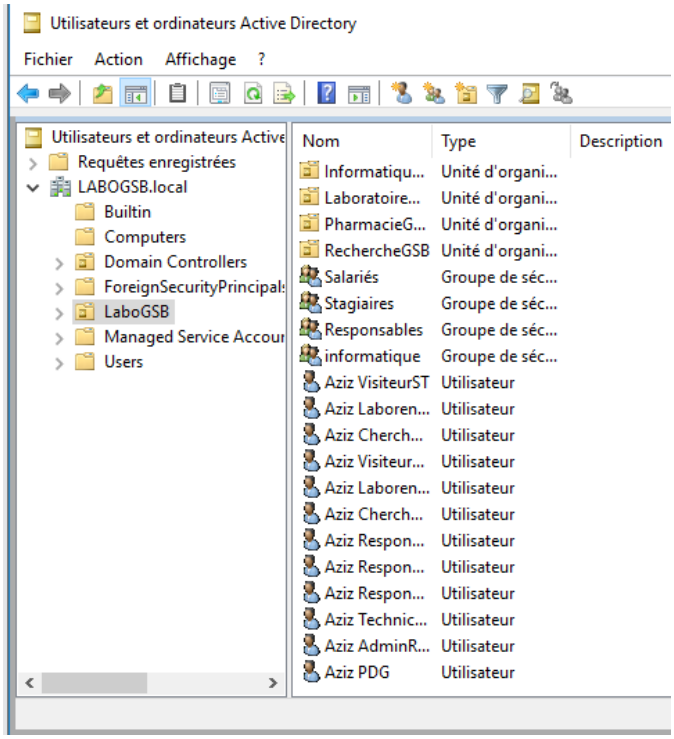
[Comment vérifier que l'autorisation a été bien respectée, expliquer avec vos propres mots les situations que vous allez tester]

IMPORTANT [Montrer 3 cas avec captures montrant ces vérifications]

Vérification de l'organisation mise en place



Pour la gestion d'Active Directory, j'ai décidé de ı ités d'organisation (OU) et d'opter uniquement pour une gestion via les groupes, afin de simplifi



Création des profils en fonction des utilisateurs

[Expliquer l'utilité des profils, en une seule phrase et avec vos propres mots]

les profils permettent de personnaliser l'environnement de travail de chaque utilisateur en conservant leurs préférences, documents et configurations.

[Pourquoi dit-on que le profil est local ?]

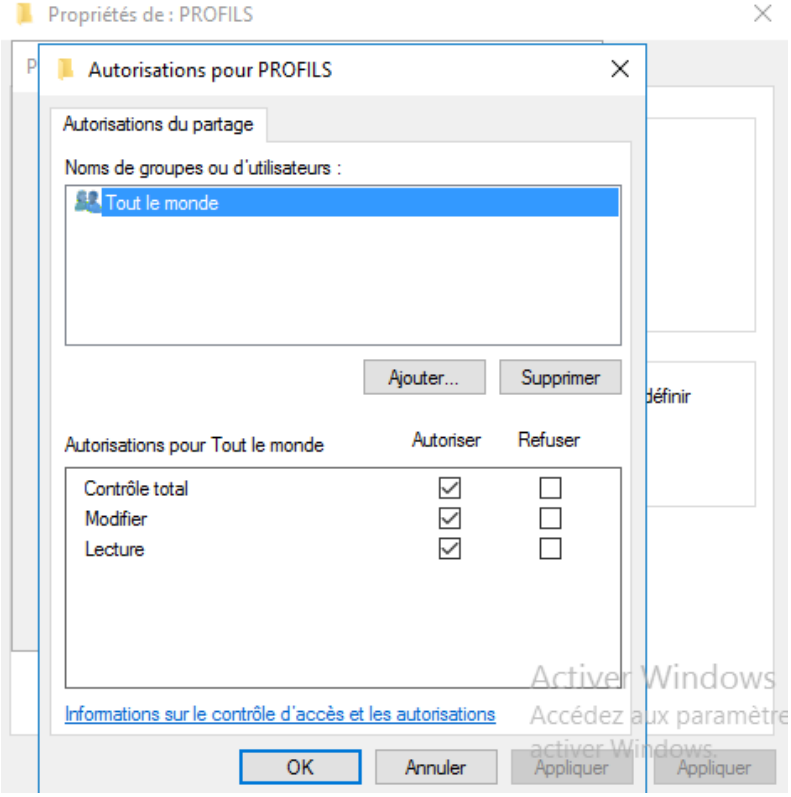
On parle de profil local car les données et paramètres de l'utilisateur sont stockés directement sur l'ordinateur où il se connecte, et ne sont pas accessibles depuis d'autres machines.

[Expliquer comment procéder pour qu'un profil soit accessible sur n'importe quelle machine du réseau]

Pour que le profil utilisateur soit disponible sur toutes les machines du réseau, il faut activer un profil itinérant en configurant Active Directory pour que les données du profil soient enregistrées sur un serveur central. Ainsi, chaque fois que l'utilisateur se connecte à une machine, ses paramètres et fichiers sont chargés depuis le serveur.

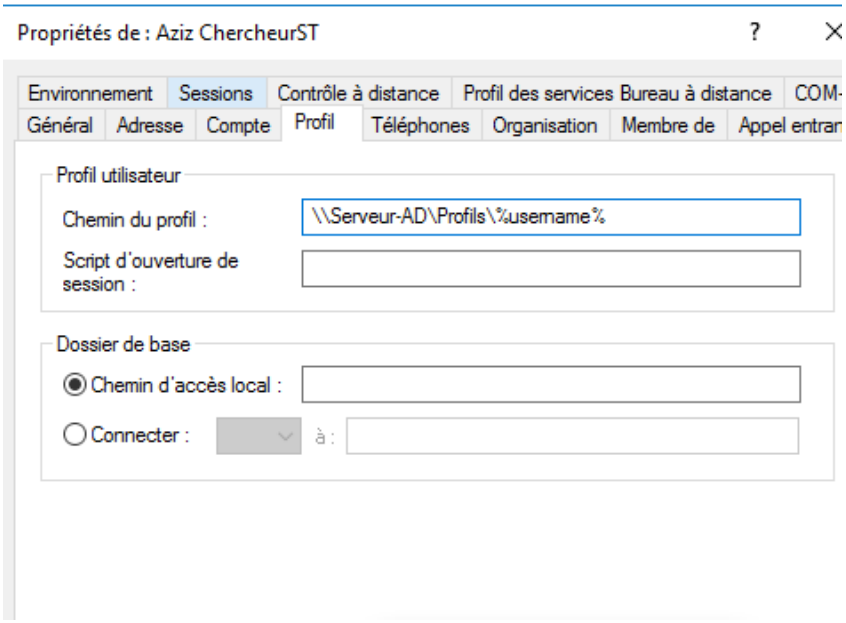
Mise en place d'un profil pour les utilisateurs

[Captures montrant ces ajouts, à vous de choisir les captures qui vous semblent importantes]



Etape 1 : On commence par **créer le dossier partagé pour les profils dans la racine « C : »** sur le Serveur-AD**:**

- Créer un dossier nommé **PROFILS** qui contiendra tous les profils des utilisateurs créés
- Partagez-le en conservant le nom de partage par défaut.
- Modifiez les autorisations de **partage** (onglet « partage et sécurité ») en donnant le contrôle d'accès à tout le monde.



Etape 2 : Dans la console AD, **créer des profils pour tous vos utilisateurs**

- Double clic sur l'utilisateur concerné, Onglet « **Profils** »,
- Saisir le chemin menant au profil de l'utilisateur : ***\\Serveur-AD*\Profils\%username%**

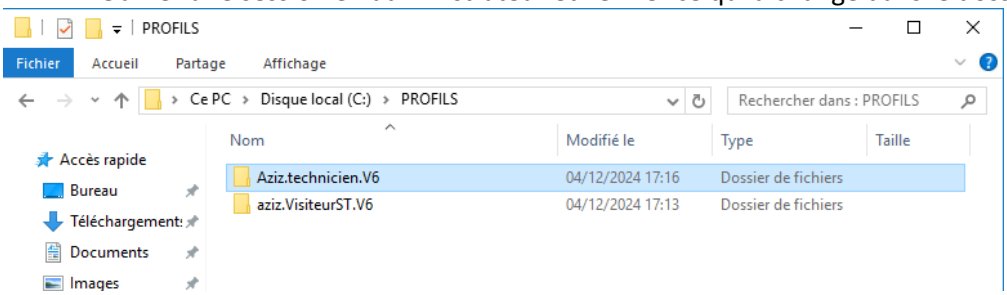
Vérifications à partir de la machine WinClient10-1

[Capture montrant cette modification]

- Ouvrez une session cliente avec un compte utilisateur sur le poste client
- A partir de ce compte, modifier l'arrière-plan du poste, ajoutez une icône sur le bureau puis fermer la session.

[Capture montrant cette vérification]

- Ouvrer une session en administrateur et vérifier ce qui a changé dans le dossier **Profils**



[Qu'est-ce qui a changé ? expliquez ce que vous observez en une phrase avec vos propres mots]

Dans le dossier "Profils" du serveur, un nouveau dossier au nom de l'utilisateur a été créé. Ce dossier contient les données du profil utilisateur

Gestion des dossiers personnels

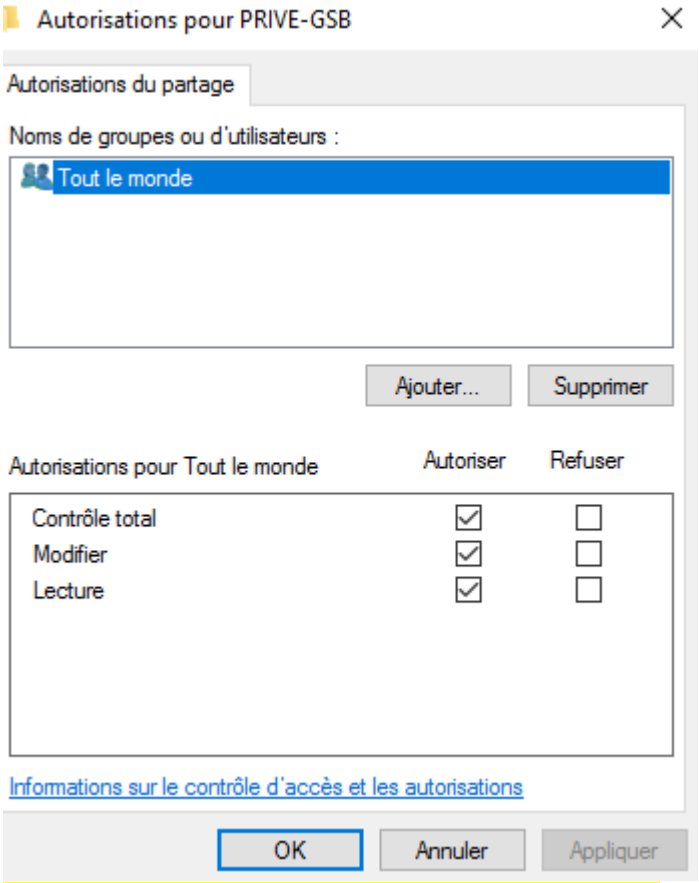
Dossier personnel pour chaque utilisateur

On voudrait que chaque utilisateur dispose d'un dossier personnel sur le Serveur-AD

Etape 1 : On commence par **créer le dossier** nommé **PRIVE-GSB dans la racine « C : » :**

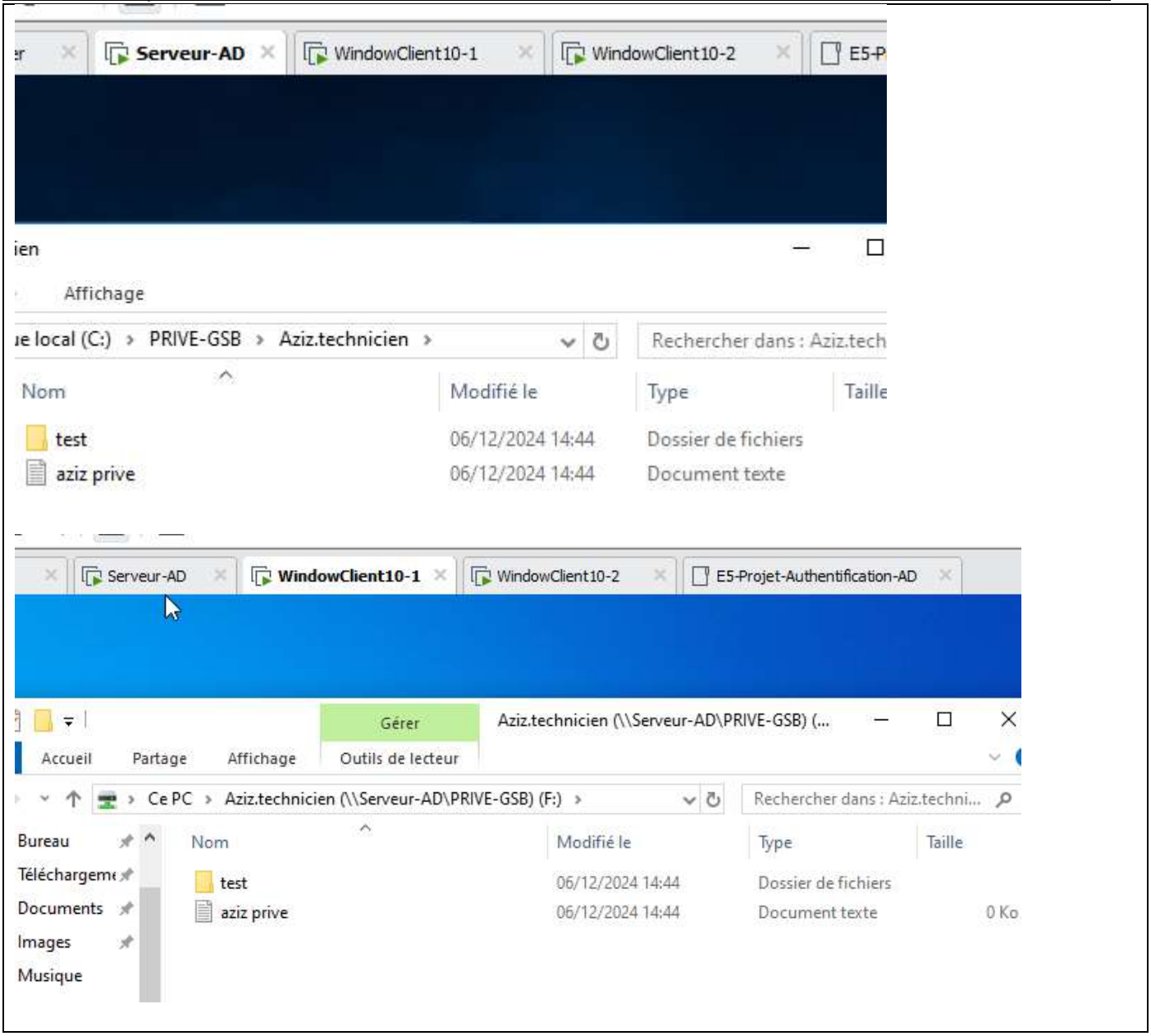
- Qui contiendra tous les dossiers personnels des utilisateurs
- Partagez-le en conservant le nom de partage par défaut.
- Créer le lecteur réseau correspondant sur le serveur AD
    - Aller sur le compte utilisateur et affichez ses propriétés, onglet Profils
    - Dans la partie « Dossier de base », « connecter à », choisir une lettre et indiquer le chemin ***\\Serveur-AD*****PRIVE-GSB\%username%**

ATTENTION POUR FAIRE CELA IL FAUT BIEN COCHER TOUTE LES AUTORISATION POUR TOUT LE MONDE :

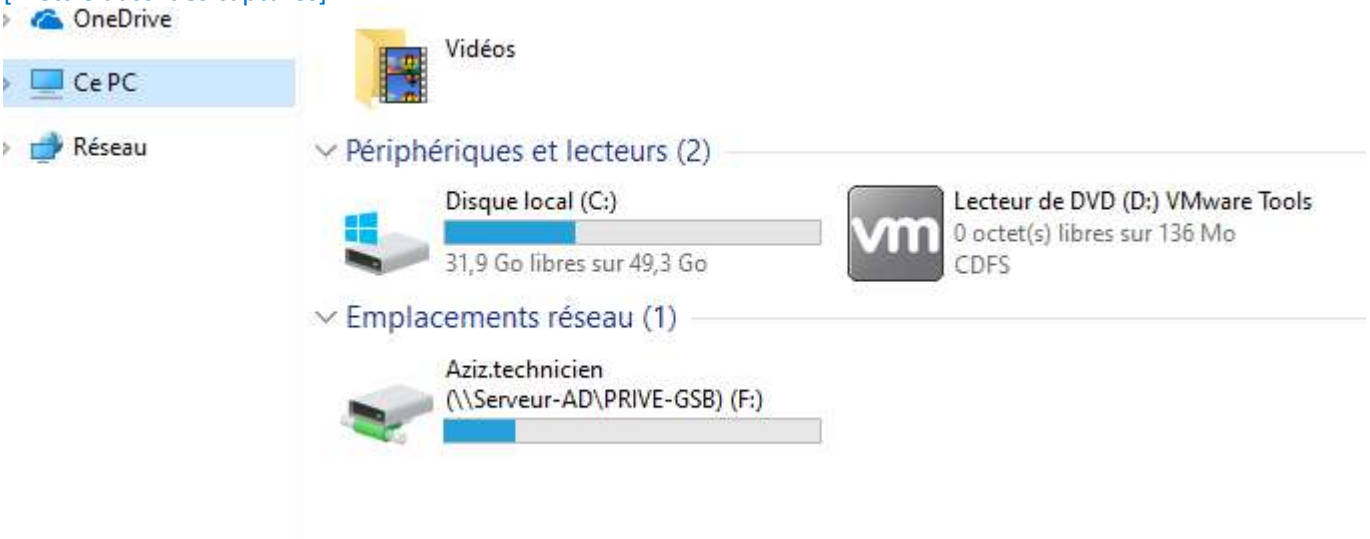


Vérification à partir de la machine cliente WinClient10

[Comment allez-vous faire ? expliquer et montrer comment effectuer cette vérification]

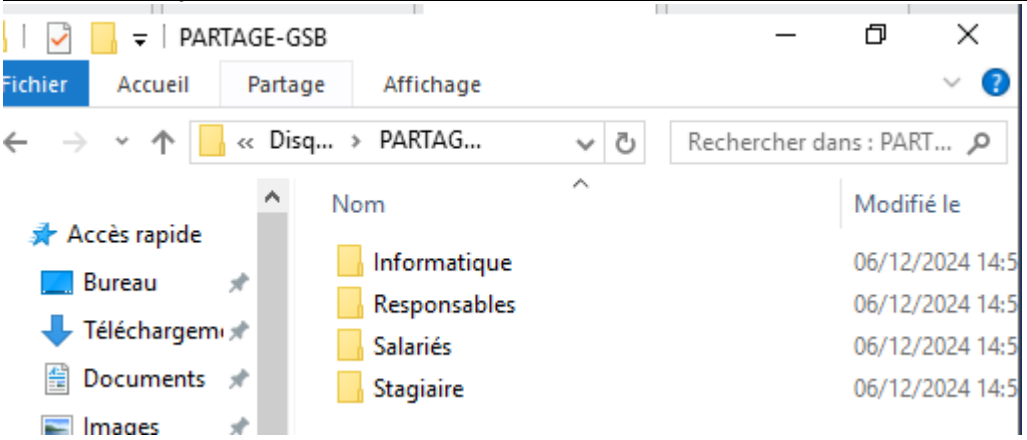


[Mettre aussi des captures]



Dossier partagé commun aux utilisateurs

Cette étape consiste à créer un répertoire que nous allons partager et qui servira à stocker les données des utilisateurs travaillant en commun sur un dossier du même groupe.



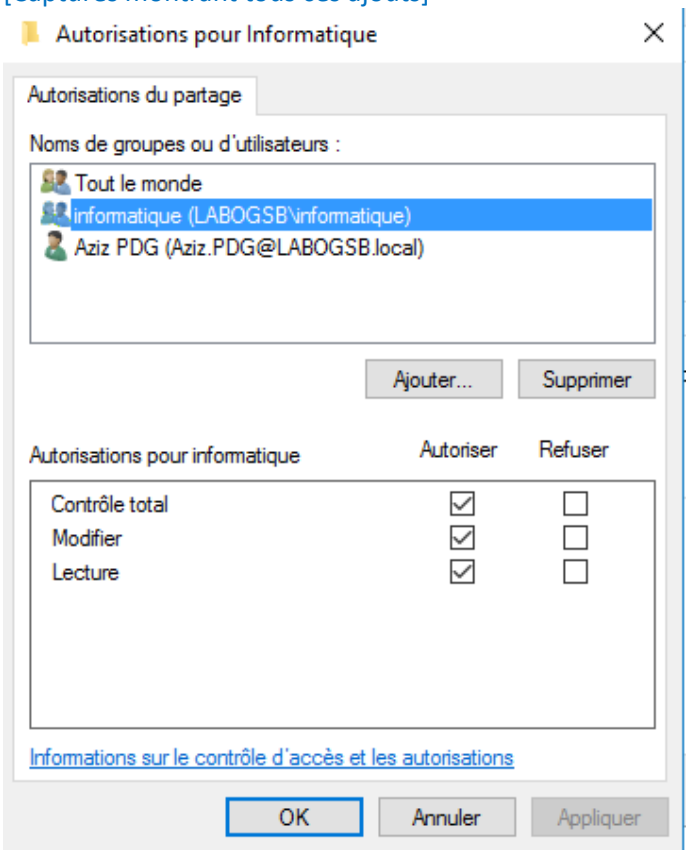
[Captures montrant ces ajouts]

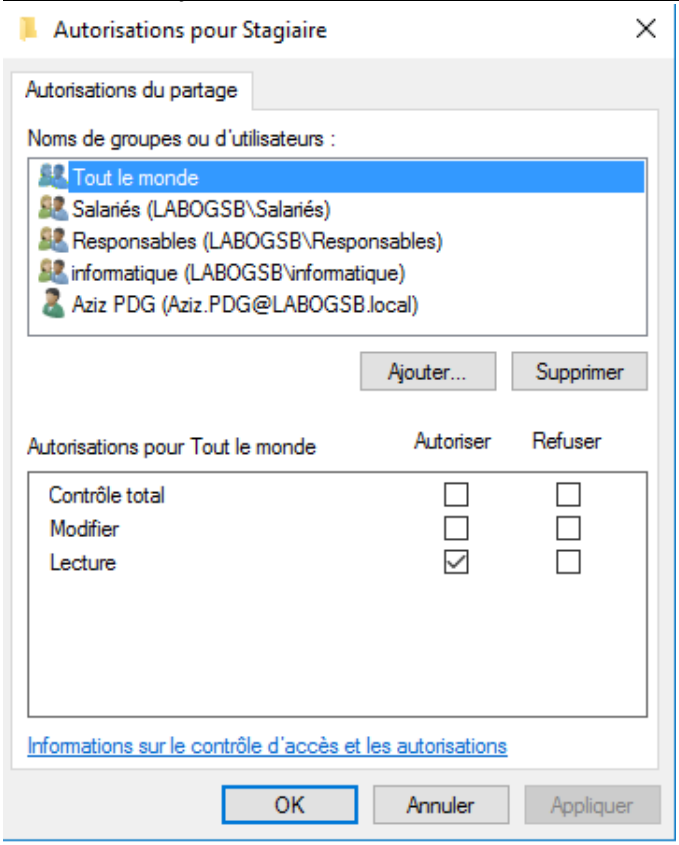
Etape 1 : On commence par **créer le dossier PARTAGE-GSB dans la racine « C : »** sur le Serveur-AD **:**

- Y créer **4 sous dossiers** correspondant aux groupes : **Stagiaire, Salariés, Responsables, Informatique**

Etape 2 : Appliquer les autorisations suivantes en fonction des dossiers :

[Captures montrant tous ces ajouts]

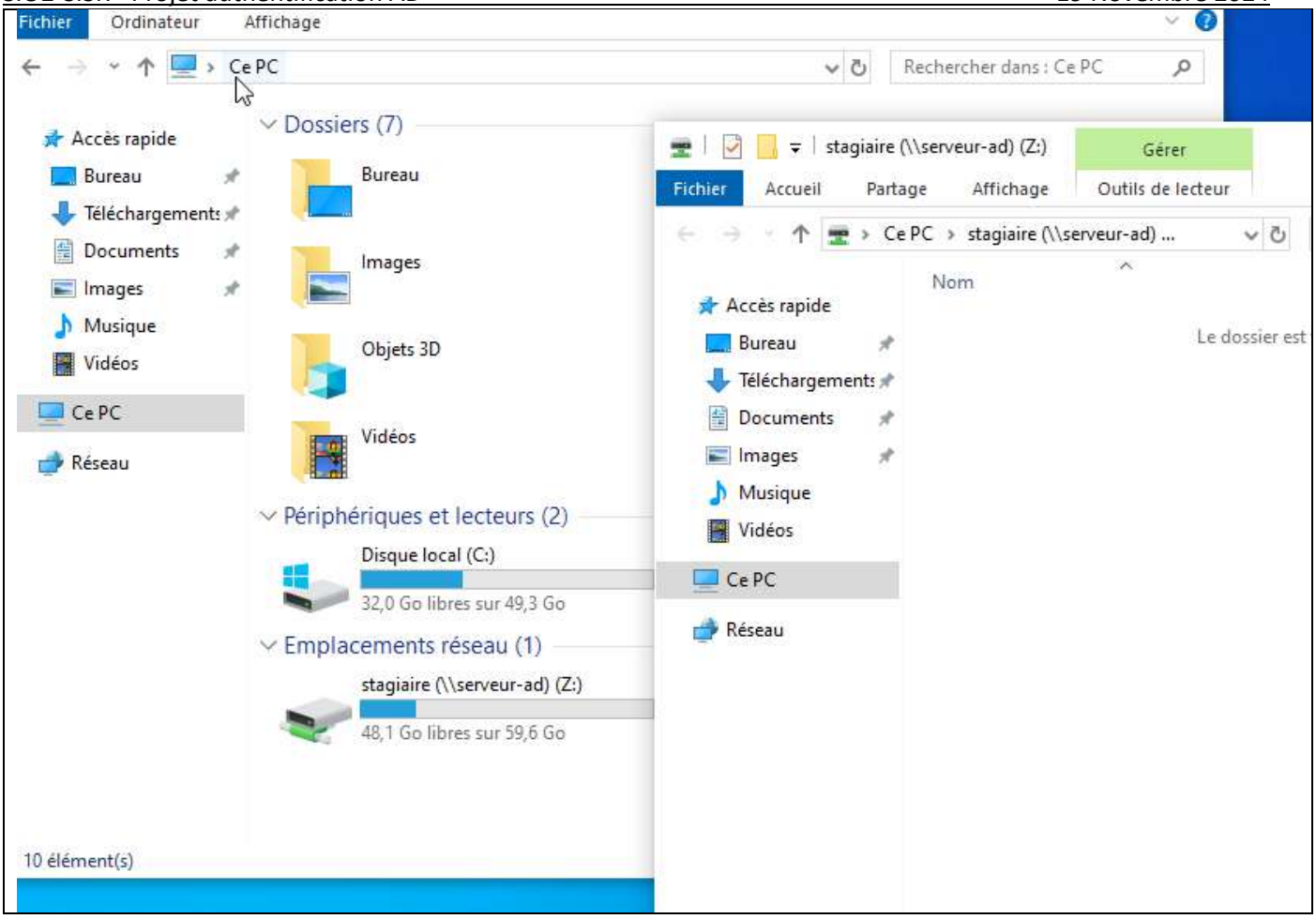




- Les informaticiens auront accès à l'ensemble des dossiers
- Les stagiaires auront seulement accès à leur dossier commun
- Les salariés auront accès à leur dossier commun et au dossier des stagiaires
- Les responsables auront accès à leur dossier commun et aux dossiers des stagiaires et des salariés
- Le PDG aura accès à tout, mais seulement en lecture seule

Vérification de tous les accès à partir de la machine cliente WinClient10-2

[Comment allez-vous faire ? expliquer et montrer comment effectuer cette vérification]



[Mettre aussi des captures]

Fin de la partie 2

Partie 3 : Mise en place stratégies de groupe (GPO)

Etapes de la réalisation

Contenu :

- ⇨ *Mise en place des stratégies de groupe dans le domaine*
- ⇨ *Création des GPO*
- ⇨ *Liaison des stratégies de groupe*
- ⇨ *Application des stratégies de groupe*
- ⇨ *Mise en place des stratégies de groupe*

Présentation des stratégies de groupe dans le domaine

Vous pouvez consultez ce site pour plus d'infos : https://www.it-connect.fr/cours/debuter-avec-les-strategies-de-groupe-sous-windows-server/

Il s'agit de mettre en place les stratégies de groupes Windows ou GPO (Group Policy Object).

Quelle est l'utilité des GPO ?

Les GPO permettent de gérer et de contrôler les paramètres utilisateurs et machines dans un domaine Windows Server. Elles facilitent la gestion centralisée

- Standardisation des environnements utilisateurs.
- Application automatique de règles de sécurité.
- Réduction des erreurs humaines dans la gestion des configurations.

Expliquer ces trois étapes de la création d'une GPO

⇨ Création de la GPO :
Les GPO sont créées dans la console de gestion des stratégies de groupe (GPMC).

⇨ Liaison de la GPO :
Associez les GPO aux objets AD, tels que :

Le domaine.

Une unité organisationnelle (UO).

⇨ Application de la GPO :
Les GPO ne s'appliquent pas instantanément. Vous devez :

Forcer l'application avec `gpupdate /force` via l'invite de commande.

Vérifier le résultat avec `gpresult /h rapport.htm`.

Création des GPO

Lien à utiliser pour savoir comment procéder ou vous basez sur ce que vous avez fait en TP AD.

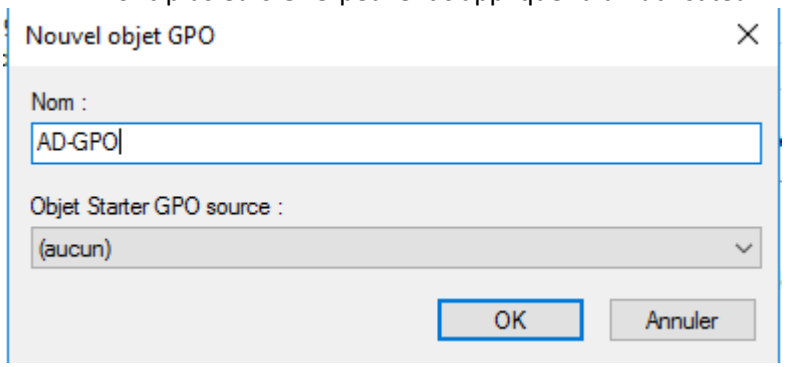
https://www.it-connect.fr/chapitres/comment-creer-sa-premiere-gpo/

Liaison des stratégies de groupe

IMPORTANT

Après avoir créé une stratégie de groupe, elle doit être liée à AD, à un domaine ou à une UO.

- ⇨ Attention, les objets enfants d'AD héritent des objets parents.
- ⇨ Donc plusieurs GPO peuvent s'appliquer à un utilisateur.

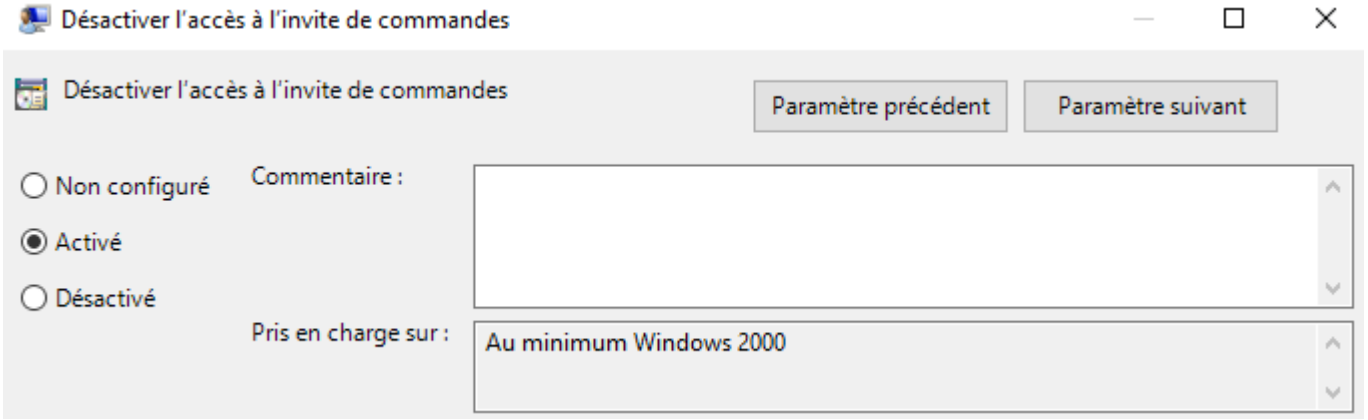


Application des stratégies de groupe

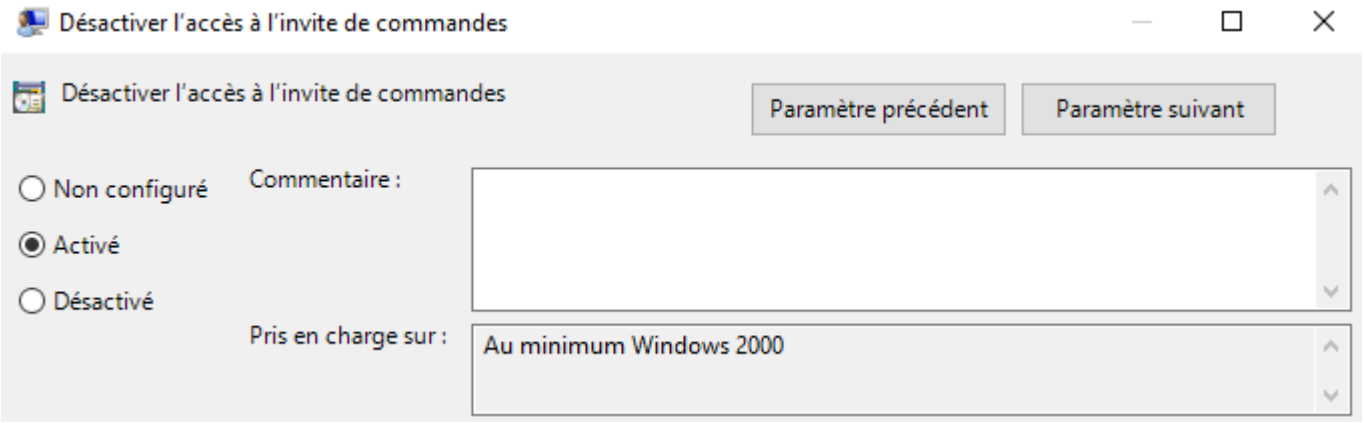
IMPORTANT

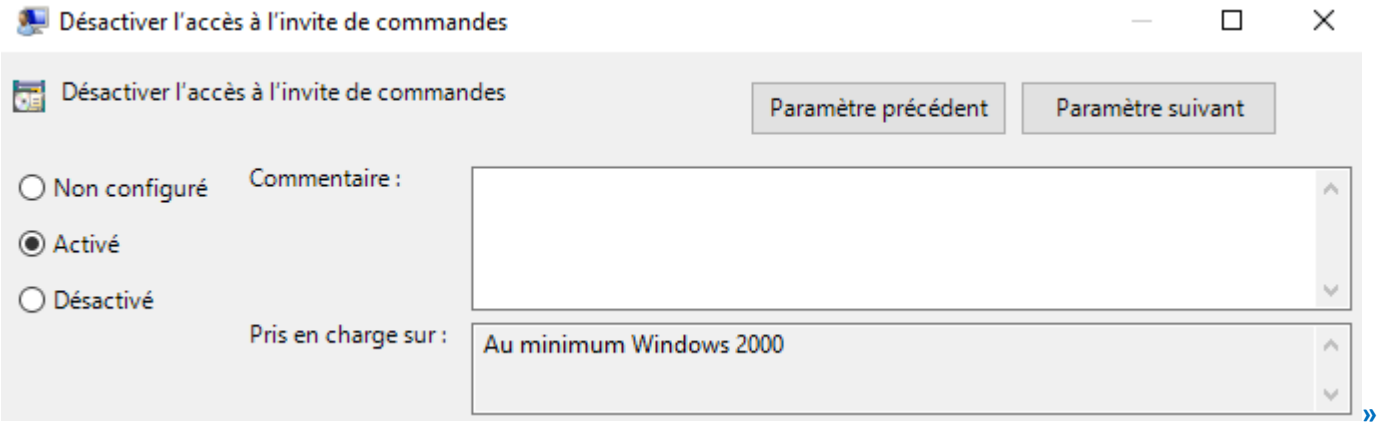
La stratégie de groupe ne s'applique pas tout de suite sur l'utilisateur connecté sur la machine cliente donc il faut forcer la mise à jour des GPO avant de la tester

Pour forcer l'application des GPO, on utilise la commande



«





»

dans le CMD

[Capture le montrant]

Pour vérifier le résultat de l'application des GPO, on utilise la commande « **gpresult /h rapport.htm** »

[Capture le montrant]

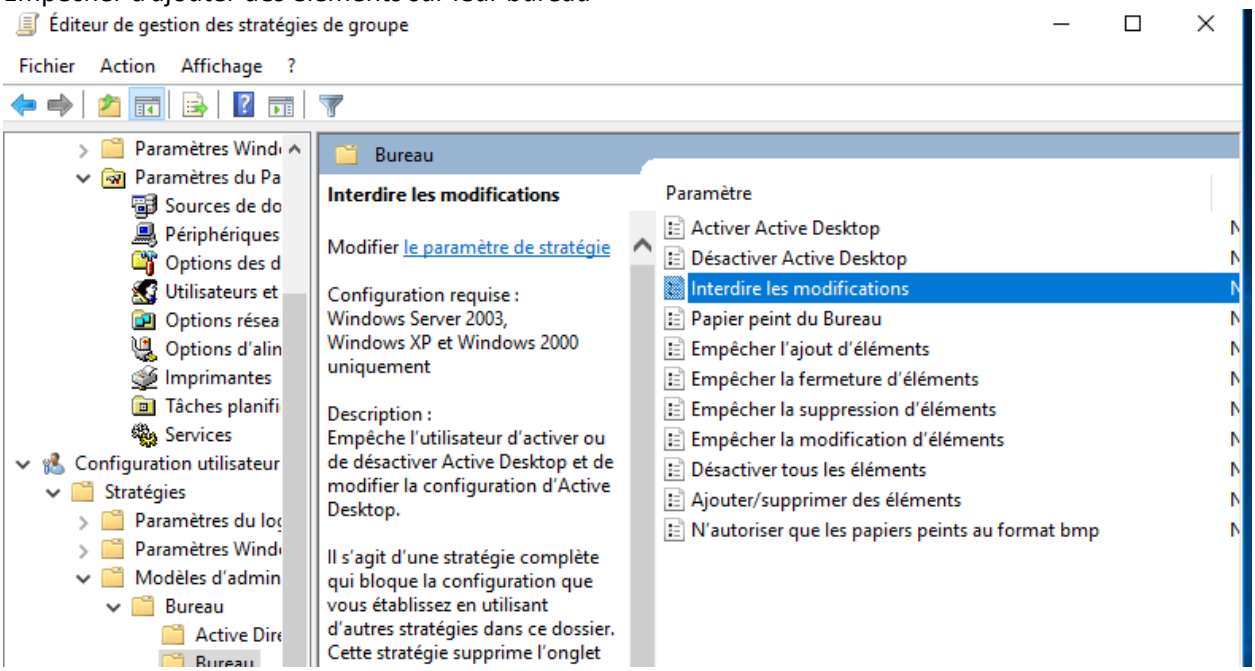
Mise en place des stratégies de groupe

Pour le groupe « stagiaire »

[Expliquer comment et mettre les captures le montrant ce que vous avez fait]

Il faut appliquer aux utilisateurs les règles suivantes :

⇨ Empêcher d'ajouter des éléments sur leur bureau



⇨

Administrateur : Invite de commandes

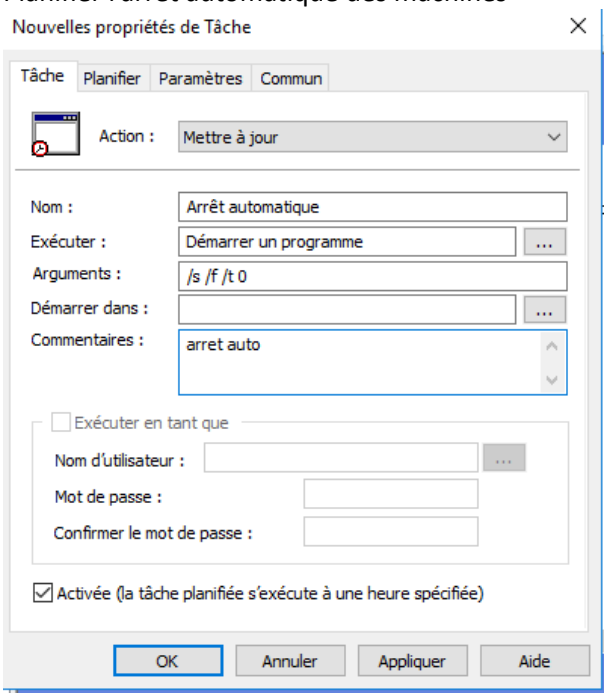
```
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.SERVEUR-AD>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.


C:\Users\Administrateur.SERVEUR-AD>
```

⇨

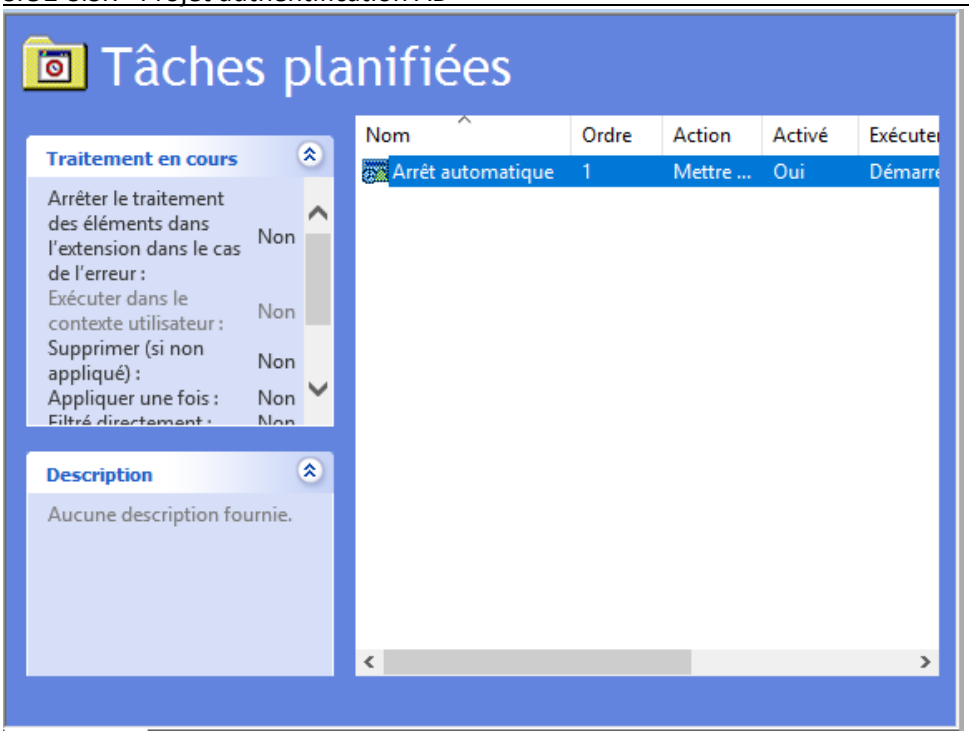
```
GPRESULT [/S système [/U utilisateur [/P mot_de_passe]]]] [/SCOPE étendue]
         [/USER nomutilisateurcible] [/R | /V | /Z] [(/X | /H)
         <nomfichier> [/F]]

Description :
    Cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP)
    Information pour ordinateurs et utilisateurs cibles.

Liste de paramètres :
    /S        système          Spécifie le système distant auquel se connecter.

    /U        [domaine\]utilisateur Spécifie le contexte utilisateur sous lequel
                               la commande doit s'exécuter.
                               Inutilisable avec /X, /H.

    /P        [mot_de_passe]   Spécifie le mot de passe pour le contexte
                               utilisateur donné. Il est demandé s'il est omis.
                               Inutilisable avec /X, /H.

    /SCOPE    étendue          Précise si les paramètres de l'utilisateur ou
```

⇨

⇨ Planifier l'arrêt automatique des machines



⇨

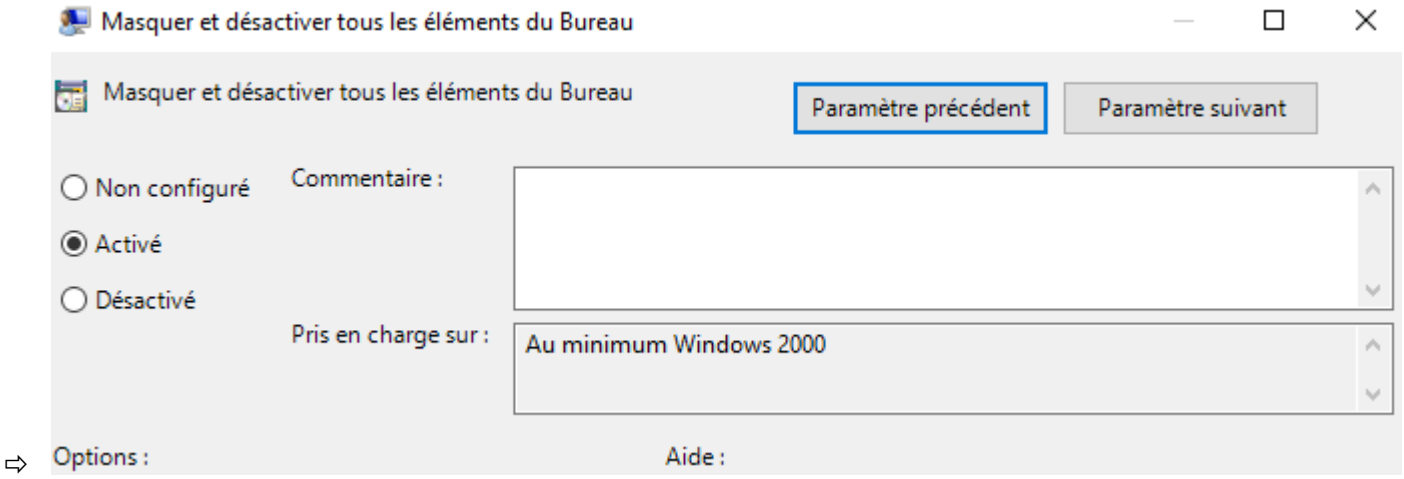


Pour le groupe « visiteurs »

[Expliquer comment et mettre les captures le montrant ce que vous avez fait]

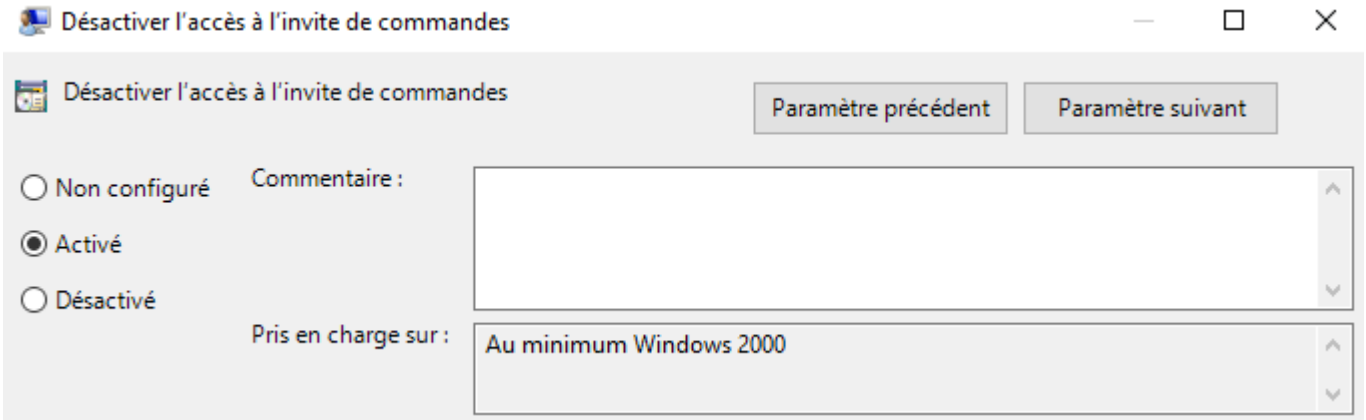
Il faut appliquer aux utilisateurs les règles suivantes :

⇨ Empêcher de masquer et désactiver tous les éléments du bureau



⇨

⇨ Désactiver l'accès à l'invite de commande

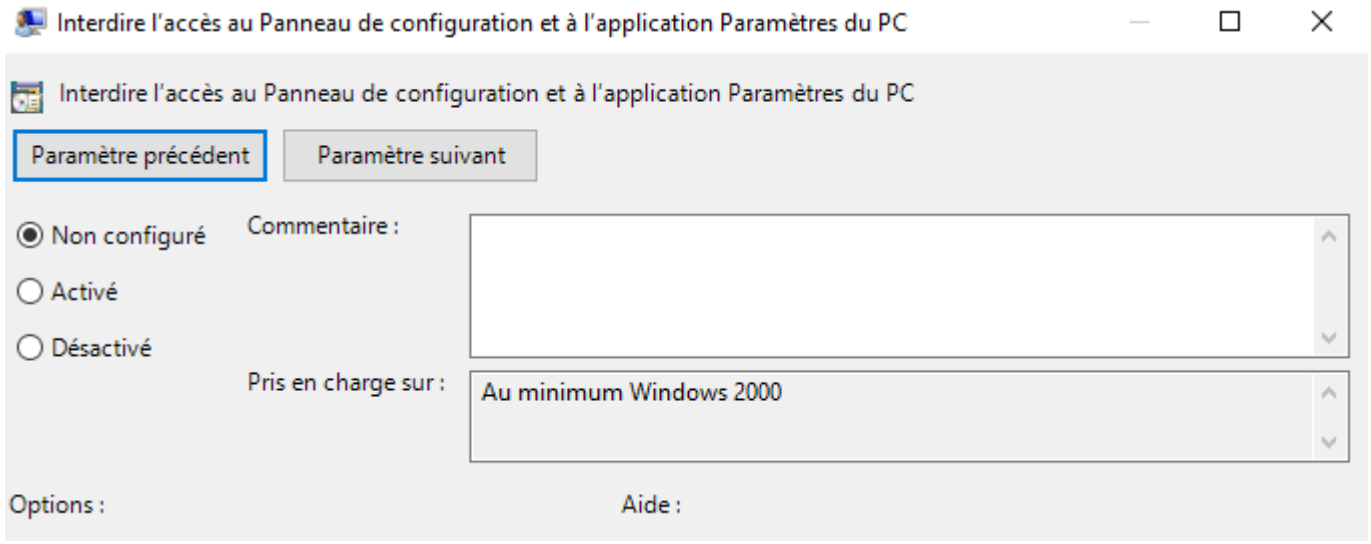


Pour le groupe « Responsables »

[Expliquer comment et mettre les captures le montrant ce que vous avez fait]

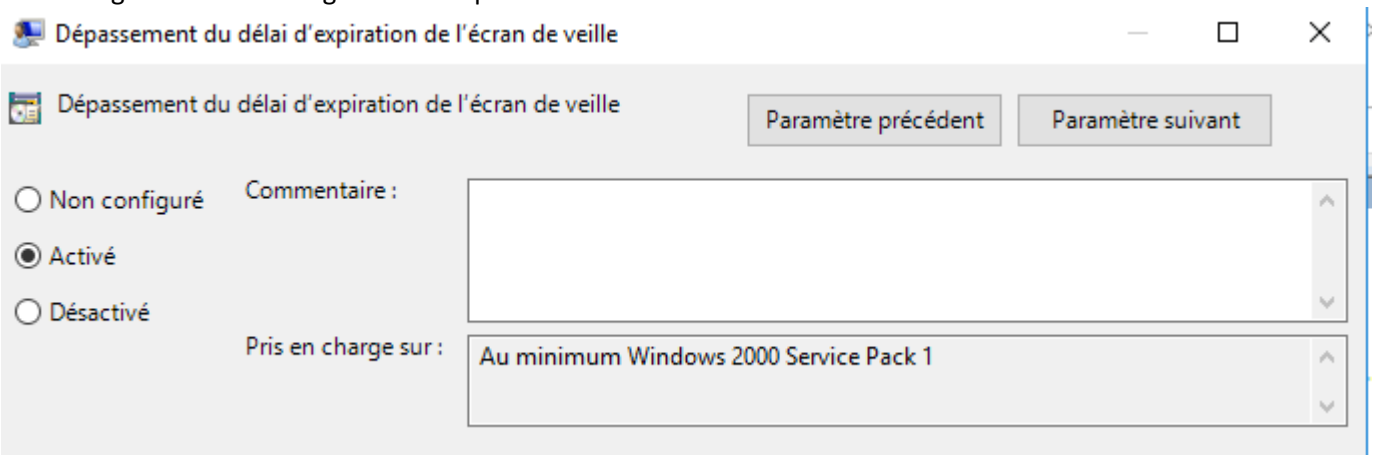
Il faut appliquer aux utilisateurs les règles suivantes :

⇨ Empêcher d'accéder au panneau de configuration



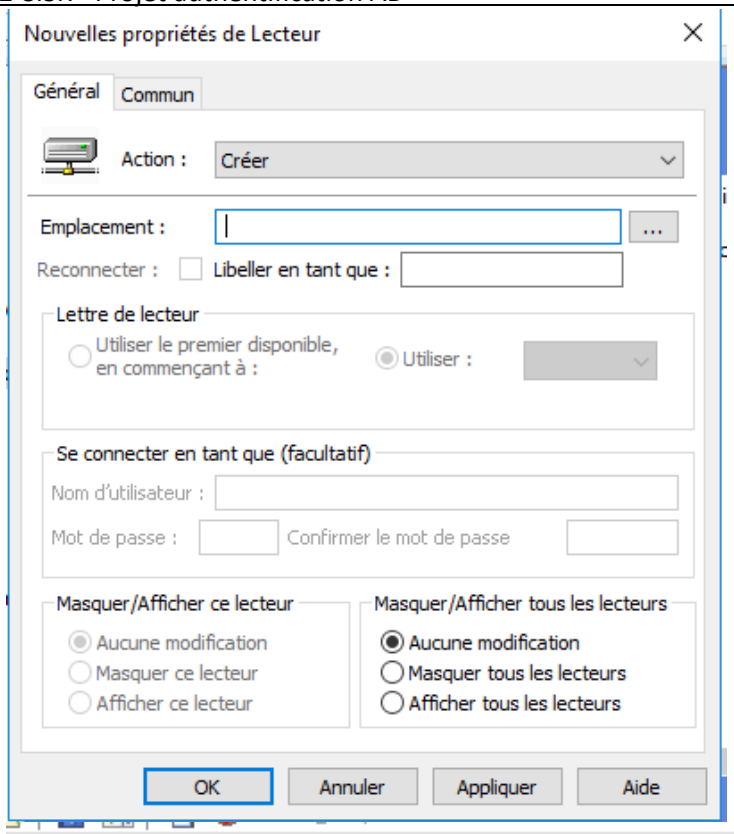
⇨

⇨ Configurer le verrouillage automatique des sessions

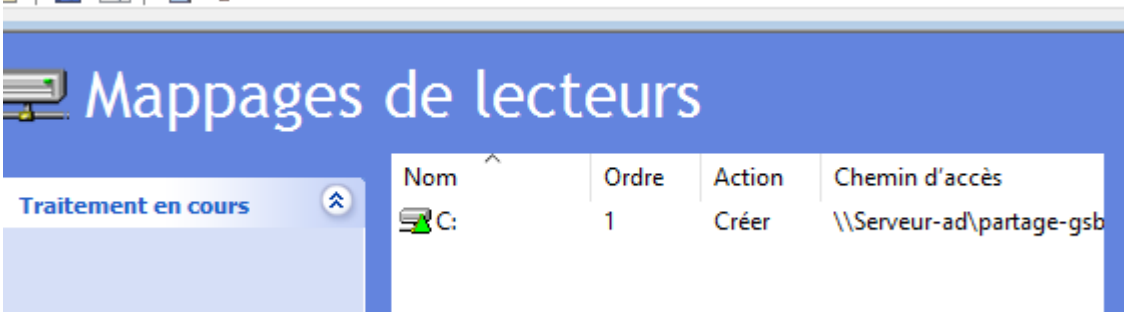


Pour le « PDG »

⇨ Créer son lecteur réseau associé via une stratégie de groupe

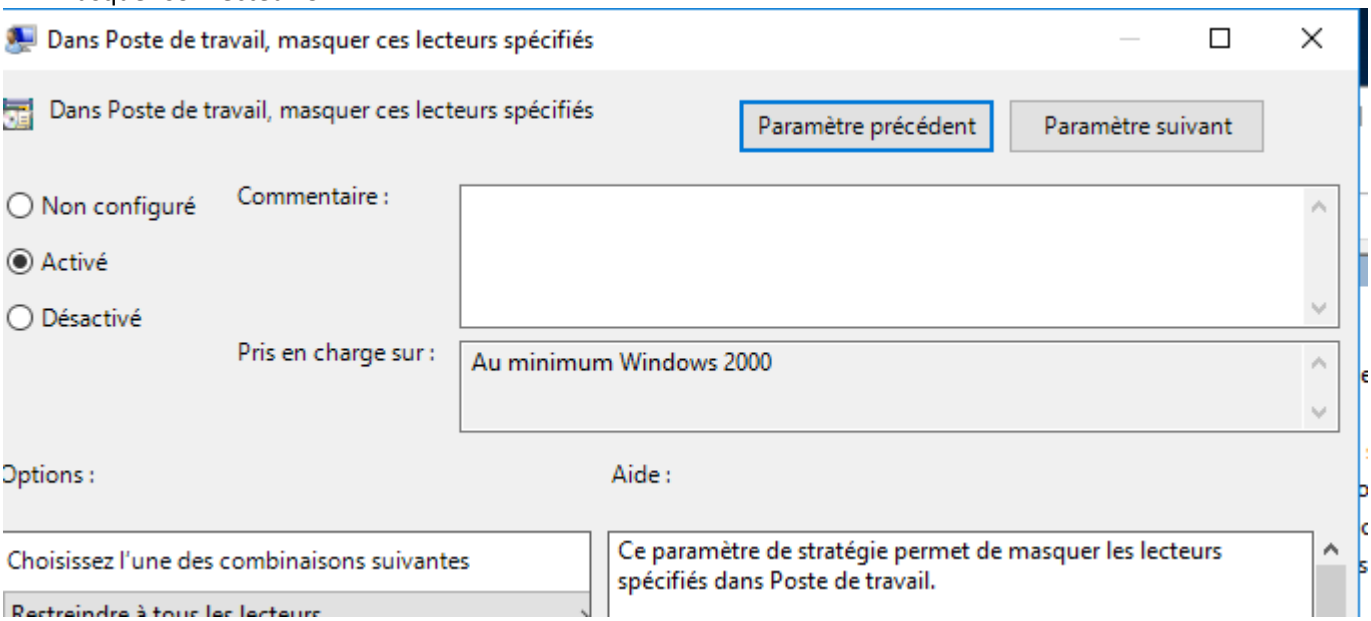


⇨

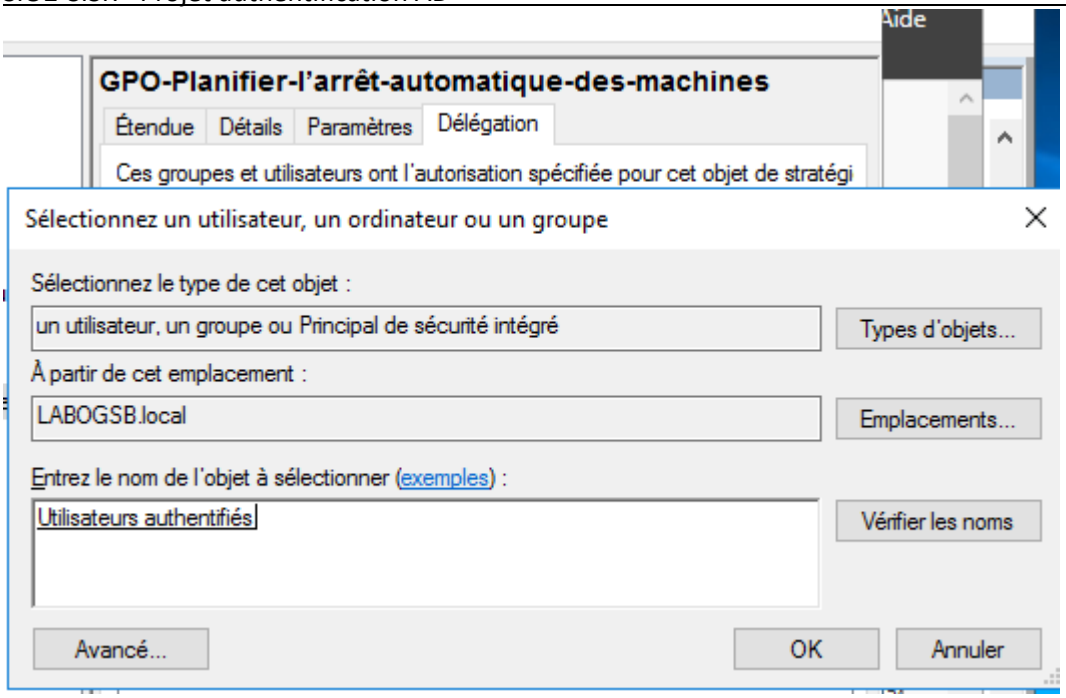


⇨

⇨ Masquer son lecteur C



Vérification des GPO créées :

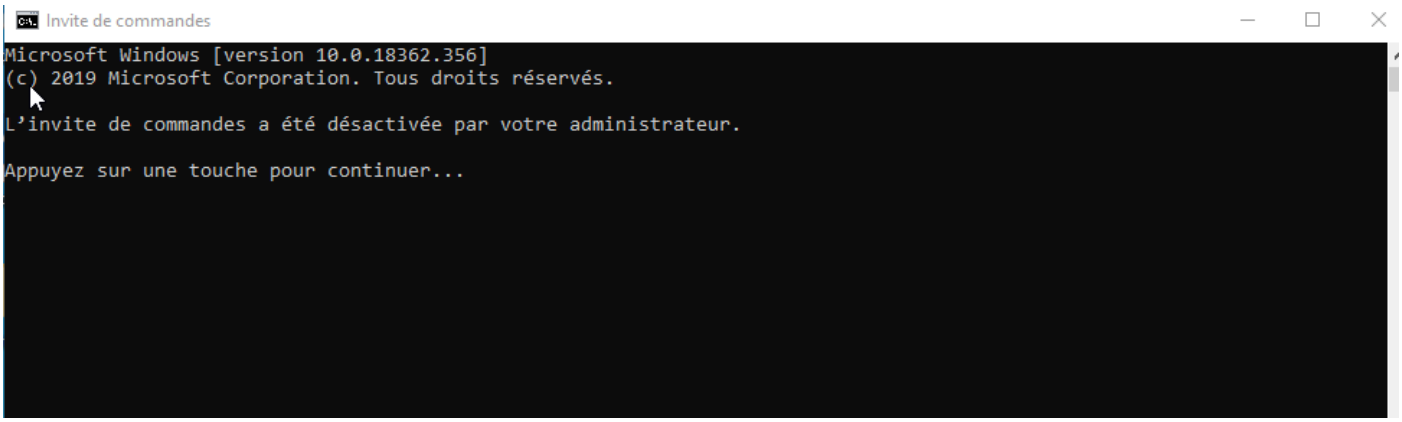


ATTENTION SI VOUS NE METTEZ PAS DANS DELEGATION L'AUTORISATION UTILISATEURS AUTHENTIFIES

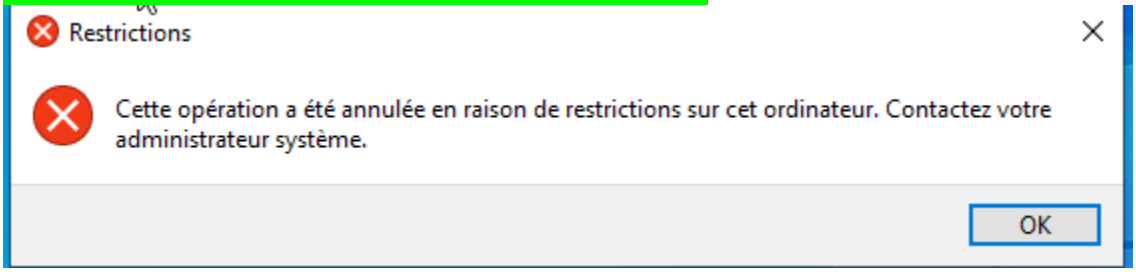
Vérifiez que les stratégies s'appliquent bien aux utilisateurs des différents groupes.

[Mettre les captures montrant tous ces résultats]

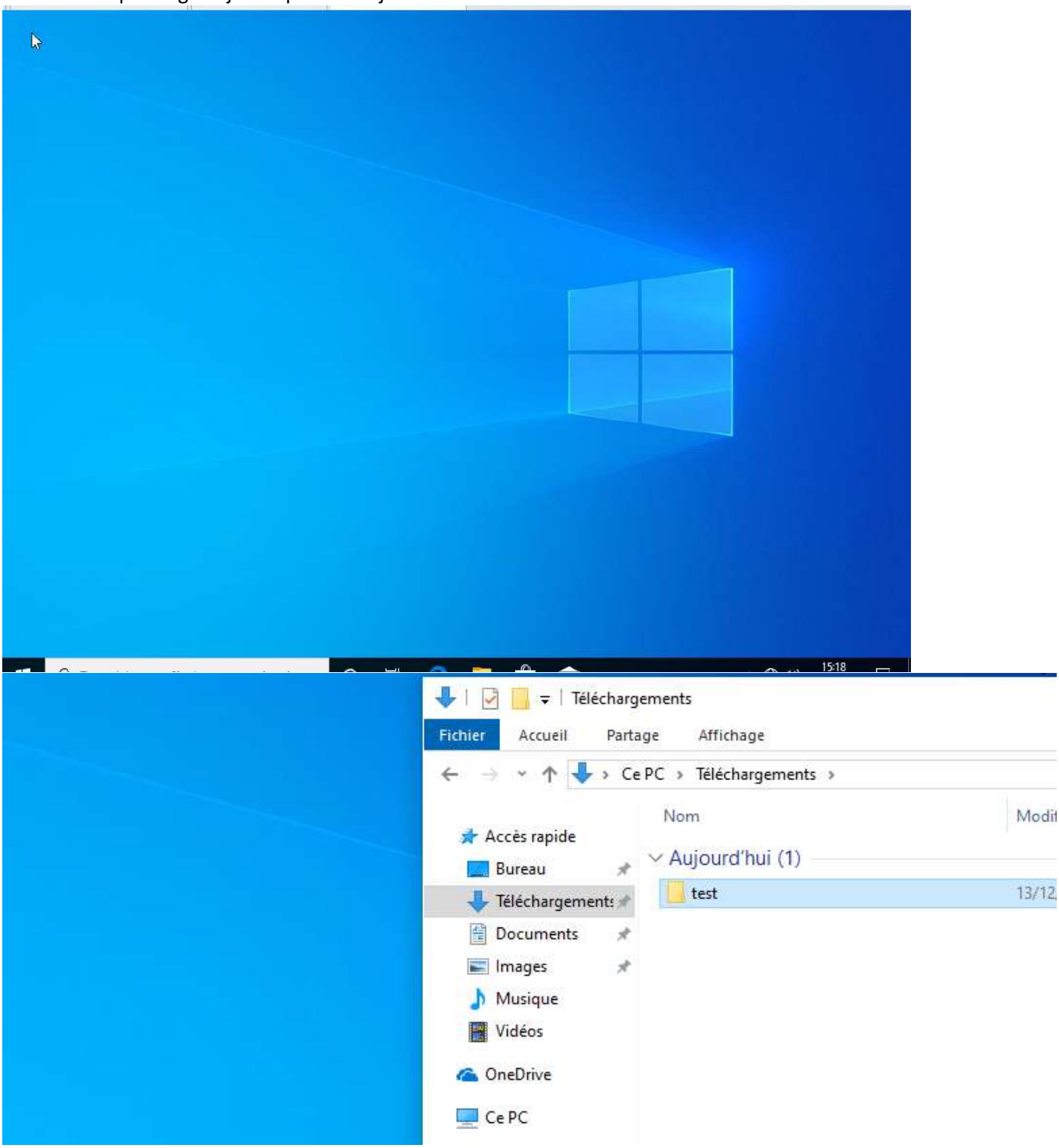
LES VISITEUR NON PAS ACCES AU CMD



LES RESPONSABLE NON PAS ACCES AU PANEAU DE CONFIG



EN Tant que stagaire j'ai Empêcher d'ajouter des éléments sur leur bureau



CONCLUSION :

Ce projet a permis de mettre en place un système d'authentification sécurisé pour le réseau GSB en s'appuyant sur Active Directory. Grâce à l'installation et à la configuration du serveur ainsi que des machines clientes, nous avons pu structurer un environnement réseau cohérent et fonctionnel.

L'intégration des comptes utilisateurs et des machines au domaine a facilité la gestion des accès et des ressources, garantissant un contrôle centralisé et efficace. De plus, la mise en œuvre des stratégies de groupe (GPO) a renforcé la sécurité et l'application des règles adaptées aux besoins du réseau.

À travers ces différentes étapes, ce projet nous a permis d'acquérir des compétences essentielles en administration réseau et en gestion des infrastructures informatiques.