



Diplôme Universitaire de technologie

Filière : Informatique

Rapport Stage de fin d'études

Effectué à : l'Agence urbaine de Taza-Taounate

Sujet de stage :

Administration d'une infrastructure Windows server

Soutenu le 24 juin 2024 devant le jury composé de :

- Pr. Mohamed BENSLIMANE
- Pr. EL-MEKKAOUI Jaouad

Réalisé par :

Hiba BENDAKHKHOU

Encadré par :

Mr. Ismail BOUYOUSSEF (Enterprise)

Pr. Mohamed BENSLIMANE (EST)

Année universitaire 2023 – 2024

Ecole Supérieure de Technologie de Fès – (ESTF) - B.P. 2427 – Route d'Immouzer – 30000 Fès

Site web: <http://www.est.usmba.ac.ma>

Remerciement

À l'issue de ce stage, je souhaite exprimer ma profonde gratitude à toutes les personnes qui m'ont soutenu et accompagné tout au long de ces quatre semaines. Leur aide précieuse, leurs conseils avisés et leur disponibilité constante ont été essentiels à l'accomplissement de ce projet. Sans leur soutien, je n'aurais pas pu mener à bien ce travail qui, bien que modeste, représente une étape importante dans mon parcours professionnel.

Je tiens tout particulièrement à remercier mes encadrants, collègues, et tous ceux qui ont partagé leur expertise et leur expérience, me permettant ainsi de tirer le meilleur de cette expérience enrichissante. Je tiens également à exprimer ma reconnaissance envers Ismail BOUYOUSSEF pour son support et son encadrement attentif. C'était une expérience enrichissante qui m'a permis d'acquérir de nouvelles compétences et une meilleure compréhension du domaine.

Enfin, je souhaite remercier Mohammed BENSLIMANE, mon encadrant à l'École Supérieure de Technologie (EST), pour son soutien continu et ses précieux conseils. Son encadrement a été déterminant pour le succès de ce stage et pour mon développement professionnel.

Sommaire

Remerciement.....	2
Sommaire	3
Introduction.....	4
Présentation de lieu de stage	5
I. Projet : Outils et technologie utilisé.....	6
1. VirtualBox	6
2. Windows Server 2019.....	6
3. Windows 7	6
II. Présentation de projet	7
1. Généralisation sur le projet	7
2. C'est quoi l'active directory domaine services	7
3. Domaine, Sous Domaine, Forêt et Arbre	7
4. Les objets Active Directory	8
5. Profile itinérant	8
6. WDS	8
7. GPO,file Sharing & FSRM,Storage pool et Nic teaming	9
III. Partie Pratique A (Avec L'interface graphique).....	10
1. Installation de Windows server & Windows7 sous Virtual Box.....	11
2. Création de domaine	13
3. Création des Unité Organisationnelles, les utilisateurs et les groupes	16
4. Profile itinérants.....	23
5. Configuration WDS	26
6. Configuration des GPO.....	35
7. Configuration Storage Pool.....	43
8. Configuration de File Sharing & FSRM	45
9. Configuration de Nic Teaming	48
VI. Partie Pratique B (PowerShell)	49
1. Création de Domaine	49
2. Création des Unités Organisationnelles, Utilisateurs et Groupes.....	53
3. Configuration profile itinérant	57
4. Configuration WDS	58
5. Configuration des GPO.....	59
6. Configuration File Sharing et FSRM	64
7. Configuration Storage Pool.....	66
8. Configuration de Nic Teaming	67
Conclusion	69

Introduction

Dans un environnement informatique moderne, la gestion centralisée des ressources et des utilisateurs est devenue essentielle pour assurer la sécurité, la cohérence et l'efficacité des opérations. Active Directory Domain Services (AD DS) de Microsoft est l'une des solutions les plus couramment utilisées pour répondre à ce besoin, offrant une infrastructure robuste pour la gestion des identités et des accès au sein d'une entreprise.

Dans le cadre de ce projet, nous avons entrepris de déployer un environnement AD DS utilisant VirtualBox, une plateforme de virtualisation polyvalente et gratuite. L'objectif principal de ce déploiement est de simuler un environnement d'entreprise standard afin de comprendre le processus d'installation, de configuration et de gestion d'AD DS, tout en minimisant les coûts et les contraintes matérielles grâce à l'utilisation de machines virtuelles.

Dans ce rapport, nous détaillerons les étapes suivies pour mettre en place notre infrastructure AD DS dans VirtualBox, les défis rencontrés et les solutions apportées, ainsi que les résultats obtenus à l'issue de nos tests et validations. Nous concluons en tirant des enseignements de cette expérience et en proposant des pistes pour des développements futurs.

Présentation de lieu de stage

J'ai effectué mon stage au sein de l'Agence Urbaine de Taza-Taounate, une institution qui joue un rôle essentiel dans la gestion et la planification urbaine au Maroc. Ces agences sont des établissements publics bénéficiant de la personnalité morale et de l'autonomie financière. Placées sous la tutelle du ministère chargé de l'Urbanisme, elles sont également soumises au contrôle financier de l'État. Le Maroc compte un total de 30 agences urbaines, chacune ayant une portée territoriale spécifique, couvrant ainsi l'ensemble du pays. Ces agences sont responsables de la coordination des politiques d'urbanisme, de l'aménagement du territoire et de la gestion des espaces urbains.

L'Agence Urbaine de Taza-Taounate est investie de deux missions principales :

1. Une mission d'études et de planification urbaines.
2. Une mission de gestion urbaine et de contrôle.

Conformément à l'article 3 du Dahir portant loi n° 1-93-51 du 22 Rabi'a I 1414 (10 septembre 1993), l'Agence Urbaine de Taza-Taounate est chargée de :

- Réaliser les études nécessaires à l'établissement des schémas directeurs d'aménagement urbain et suivre les orientations qui y sont définies.
- Programmer les projets d'aménagement inhérents à la réalisation des objectifs des schémas directeurs.
- Préparer les projets de documents d'urbanisme réglementaires, notamment les plans de zonage, les plans d'aménagement et les plans de développement.
- Donner un avis conforme dans un délai maximum d'un mois sur les projets de lotissements, groupes d'habitations, morcellements et constructions, qui doivent lui être transmis, à cet effet, par les autorités compétentes.
- Contrôler la conformité des lotissements, morcellements, groupes d'habitations et constructions en cours de réalisation avec les dispositions législatives et réglementaires en vigueur et avec les autorisations de lotir, de morceler, de créer des groupes d'habitations ou de construire accordées.

Ce stage m'a offert une expérience pratique précieuse au sein d'un environnement professionnel dynamique et en lien direct avec les enjeux de développement urbain de la région.

I. Projet : Outils et technologie utilisé

1. VirtualBox

VirtualBox est un puissant logiciel de virtualisation à source ouverte. Elle permet aux utilisateurs de créer et d'exécuter des machines virtuelles sur leurs ordinateurs, ce qui leur permet d'installer et d'exécuter plusieurs systèmes d'exploitation à la fois.

C'est un outil puissant et polyvalent pour la virtualisation qui offre une solution abordable et flexible pour les besoins de développement, de test et d'apprentissage des utilisateurs.

Cela est particulièrement utile pour tester des logiciels, expérimenter différentes configurations et isoler des environnements pour une sécurité accrue.

VirtualBox offre une solution flexible et pratique pour l'utilisation de différents systèmes d'exploitation sans avoir à utiliser de machines physiques séparées, ce qui la rend idéale pour les développeurs, les administrateurs de système et les testeurs de logiciels.

2. Windows Server 2019

Windows Server 2019 est la douzième version du système d'exploitation Windows Server de Microsoft, faisant partie de la famille des systèmes d'exploitation Windows NT. Il s'agit de la deuxième version du système d'exploitation serveur basée sur la plateforme Windows 10, après Windows Server 2016.

Conçu pour répondre aux besoins des entreprises et des organisations, Windows Server 2019 offre une plateforme robuste et fiable pour exécuter une large gamme de services et d'applications, allant des services web et des bases de données aux services de fichiers, d'impression, de messagerie, et bien plus encore.

La gamme de fonctionnalités offertes par Windows Server est vaste et inclut des services tels qu'Active Directory pour la gestion des identités et des accès, Hyper-V pour la virtualisation, Remote Desktop Services pour l'accès distant aux applications et aux bureaux, Windows Server Update Services (WSUS) pour la gestion des mises à jour logicielles, et bien plus encore.

En tant que système d'exploitation serveur, Windows Server est conçu pour offrir des performances élevées, une fiabilité accrue, une sécurité renforcée et une gestion simplifiée, ce qui en fait un choix populaire pour les entreprises de toutes tailles et de tous secteurs d'activité.

3. Windows 7

Windows 7 est un système d'exploitation développé par Microsoft, qui a été lancé le 22 octobre 2009 en tant que successeur de Windows Vista et est devenu l'un des systèmes d'exploitation les plus populaires de Microsoft.

Il introduit de nombreuses fonctionnalités et améliorations par rapport à son prédécesseur, notamment une interface utilisateur plus conviviale.

II. Présentation de projet

1. Généralisation sur le projet

Le projet consiste à utiliser Windows Server 2019 en tant que contrôleur de domaine, c'est-à-dire un serveur qui contrôle l'Active Directory ou, pour être plus précis, tous les hôtes des différents départements de l'entreprise. Dans mon cas, il s'agit de l'Agence Urbaine de Taza. L'objectif de ce projet est de créer un réseau local pour cette entreprise et de gérer les utilisateurs et les ordinateurs de tous les départements afin d'obtenir un réseau bien configuré et bien structuré pour l'agence.

2. C'est quoi l'active directory domaine services

L'Active Directory Domain Services (AD DS) est un outil utilisé pour appliquer les politiques de sécurité sur tous les ordinateurs et pour tous les utilisateurs de notre réseau. Contrairement au Workgroup qui est une configuration où chaque ordinateur gère ses propres paramètres de sécurité et d'authentification de manière indépendante, l'AD DS permet à un administrateur de centraliser le travail en appliquant toute la configuration sur notre contrôleur de domaine (DC). Ainsi, pour chaque hôte inclus dans notre domaine, nous aurons donc une gestion centralisée des comptes utilisateurs, des stratégies de groupe et des autres paramètres de sécurité définis par l'administrateur.

Parmi les principales fonctionnalités fournies par notre AD DS deux fonctionnalités principales qui sont l'authentification et l'autorisation puisqu'il fournit des mécanismes d'authentification sécurisés pour permettre aux utilisateurs d'accéder aux ressources du réseau, tout en contrôlant les autorisations pour garantir que seuls les utilisateurs autorisés peuvent y accéder. Les stratégies de groupe qui permettent aux administrateurs de définir et d'appliquer des configurations spécifiques à des groupes d'utilisateurs ou d'ordinateurs, ce qui facilite la gestion des paramètres de sécurité, des configurations système et des logiciels.

3. Domaine, Sous Domaine, Forêt et Arbre

Forêt (Forest) : C'est une collection de domaines interconnectés dans Active Directory. Une forêt partage une base de données d'annuaire commune et est définie par un schéma de réplication d'annuaire commun.

Arbre (Tree) : Une structure hiérarchique de domaines qui partagent une relation parent-enfant. Chaque domaine dans une arborescence est lié à un domaine parent, à l'exception du domaine racine de l'arborescence. Les domaines partagent des informations d'annuaire et des politiques de sécurité communes, mais ils peuvent aussi avoir des configurations spécifiques à leur domaine.

Domaine : La notion domaine dans Active Directory Domain Services est une unité d'organisation logique qui regroupe un ensemble d'ordinateurs, d'utilisateurs et de ressources partageant une base

de données d'annuaire commune. Il est identifié par un nom de domaine unique dans laquelle tous ces ordinateurs et utilisateurs partagent les informations d'identification et les politiques de sécurité communes.

SubDomaine : Une subdivision logique d'un domaine principal dans une infrastructure Active Directory. Il permet d'organiser et de hiérarchiser les ressources en fonction de leur fonction, de leur localisation géographique ou de toute autre logique organisationnelle.

4. Les objets Active Directory

Les Utilisateurs : Dans le service de domaine Active Directory, les utilisateurs représentent les employés de l'entreprise. Les comptes utilisateur sont des objets qui contiennent un ensemble d'informations pour chaque employé de l'agence. Chaque compte utilisateur contient un schéma qui est le type de données utilisé pour identifier ce compte utilisateur, et il peut être modifié en fonction des besoins.

Les groupes : Les groupes sont également des objets qui regroupent un ensemble d'utilisateurs. Dans un groupe, on ne trouve pas uniquement les utilisateurs, mais on peut aussi voir d'autres groupes inclus dans un groupe.

Les unités organisationnelles : OU est l'abréviation d'Unité Organisationnelle, correspond à *Organizational Unit* en anglais. C'est une unité utilisée pour organiser les objets tels que les utilisateurs, les groupes et les ordinateurs en fonction de la structure organisationnelle de l'entreprise. Leur avantage est qu'ils facilitent l'organisation des objets au sein du domaine sans la nécessité de créer un autre domaine supplémentaire, et d'appliquer les politiques de sécurité, qui sont l'élément principal de la gestion dans l'active directory.

5. Profile itinérant

Même si l'on a créé des utilisateurs uniques dans notre domaine, on ne peut pas avoir un utilisateur unique dans le réseau, mais plutôt pour une machine locale. La solution pour avoir un compte utilisateur unique dans le réseau est l'utilisation de Profils itinérants (Roaming Profiles). Cette fonctionnalité permet aux utilisateurs dans le réseau de conserver leurs paramètres et leurs données sur n'importe quel ordinateur du réseau, et cela se passe avec la démarche suivante:

Les données des utilisateurs sont stockées dans notre DC (contrôleur de domaine) ou un autre serveur de fichiers. À chaque déconnexion de cet utilisateur, ses données stockées sur le serveur seront synchronisées et sauvegardées.

6. WDS

La méthode traditionnelle pour installer un système d'exploitation sur une machine consiste à utiliser une clé USB bootable et à suivre les étapes manuellement, cela peut prendre beaucoup de temps,

surtout lorsqu'il s'agit de déployer des systèmes sur un réseau au sein d'une agence ou d'une entreprise. Ici l'utilité de WDS (Windows Deployment Services).

WDS est une solution de déploiement réseau développée par Microsoft, conçue spécifiquement pour faciliter le déploiement automatisé de systèmes d'exploitation Windows sur plusieurs machines en même temps. Il permet de créer une image maître de l'OS ainsi que des configurations prédéfinies, puis de distribuer cette image sur les ordinateurs du réseau de manière centralisée.

Grâce à WDS, les administrateurs système peuvent automatiser et simplifier le processus d'installation des systèmes d'exploitation, ce qui permet d'économiser du temps et des ressources lors du déploiement de nouveaux ordinateurs ou de la mise à jour des systèmes existants au sein d'une agence ou d'une entreprise.

7. GPO,file Sharing & FSRM,Storage pool et Nic teaming

GPO : Les "Group Policies" (GPO) dans Active Directory (AD) sont une fonctionnalité de gestion qui permet aux administrateurs réseau de définir et d'appliquer des paramètres spécifiques, des configurations et des politiques de sécurité pour les utilisateurs et les machines au sein d'un réseau basé sur Windows. C'est un composant essentiel de Windows Server et joue un rôle central dans la simplification de la sécurité, de la gestion et de la maintenance d'un environnement réseau.

File Sharing : C'est une technique qui nous permet de partager un fichier avec un groupe afin qu'il soit accessible uniquement par les membres de ce groupe. L'avantage de cette technique est que le fichier est accessible pour chaque utilisateur de ce groupe comme s'il était sur sa propre machine locale, et cela facilite la collaboration et le partage de fichiers au sein d'une équipe. De plus, cette méthode permet de mieux contrôler l'accès aux fichiers en limitant la visibilité aux seuls membres autorisés du groupe, ce qui renforce la sécurité et la confidentialité des données.

FSRM : C'est l'abréviation de file service resource Management), c'est un outil qui nous permet de spécifier les types des fichiers ajoutés dans un dossier partagé.

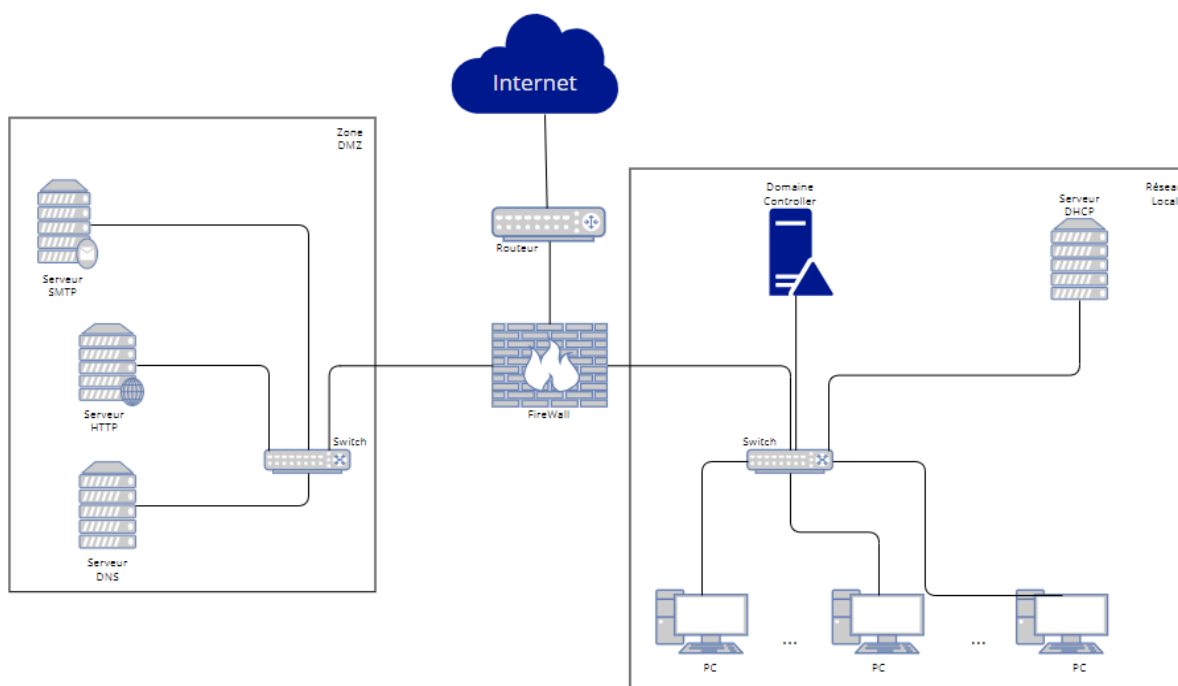
Storage pool : Le "Storage Pool" est une technique qui nous permet de combiner plusieurs disques durs physiques pour fonctionner comme une seule unité logique. Cela permet d'augmenter la capacité de stockage disponible et offre une tolérance aux erreurs, car les données sont répliquées ou distribuées de manière redondante sur plusieurs disques physiques. Ainsi, en cas de défaillance d'un disque dur, les données peuvent être récupérées à partir des autres disques, assurant la disponibilité continue des données et la récupération du système de stockage en cas de panne d'un des disques durs.

Nic teaming : Afin d'obtenir une performance élevée des cartes réseau pour les machines qui ont plus d'une seule carte réseau, le "Nic teaming" est une technique qui nous permet de combiner ces composants physiques en un seul composant logique avec une combinaison de performances. Cette technique n'a pas uniquement un avantage en termes de performances, mais elle offre également une tolérance aux pannes grâce à la redondance.

III. Partie Pratique A (Avec L'interface graphique)

- L'Infrastructure réseau

Voici la maquette générale de notre réseau :



Pour une organisation efficace de l'infrastructure réseau au sein d'une entreprise, il est recommandé d'adopter une structure bien organisée, notamment :

Zone DMZ (Demilitarized Zone) :

Les serveurs interagissant avec des réseaux externes sont regroupés dans une seule zone distincte appelée la zone DMZ. Cette zone est conçue pour héberger des services accessibles depuis l'extérieur tout en limitant les risques de compromission du réseau interne.

Réseau Local (LAN) :

Le réseau local de l'entreprise comprend les équipements utilisés au sein de l'entreprise. Dans cette zone, un serveur DHCP est nécessaire pour attribuer des adresses IP aux autres machines sans nécessiter de configuration manuelle sur chacune d'elles. De plus, un contrôleur de domaine (Domain Controller) est indispensable. C'est l'élément essentiel dans la gestion des utilisateurs et des ordinateurs au sein de l'entreprise.

Le Domain Controller est également utilisé comme serveur pour la gestion des utilisateurs et des ordinateurs au sein de l'entreprise. Cette gestion peut être réalisée avec différents outils, mais dans notre projet, nous utilisons Windows Server 2019 avec Active Directory Domain Services (AD DS) pour cette fonction.

1. Installation de Windows server & Windows7 sous Virtual Box

L'installation de Virtual box se fait avec le téléchargement de package.exe et suivie les étapes de l'installation.

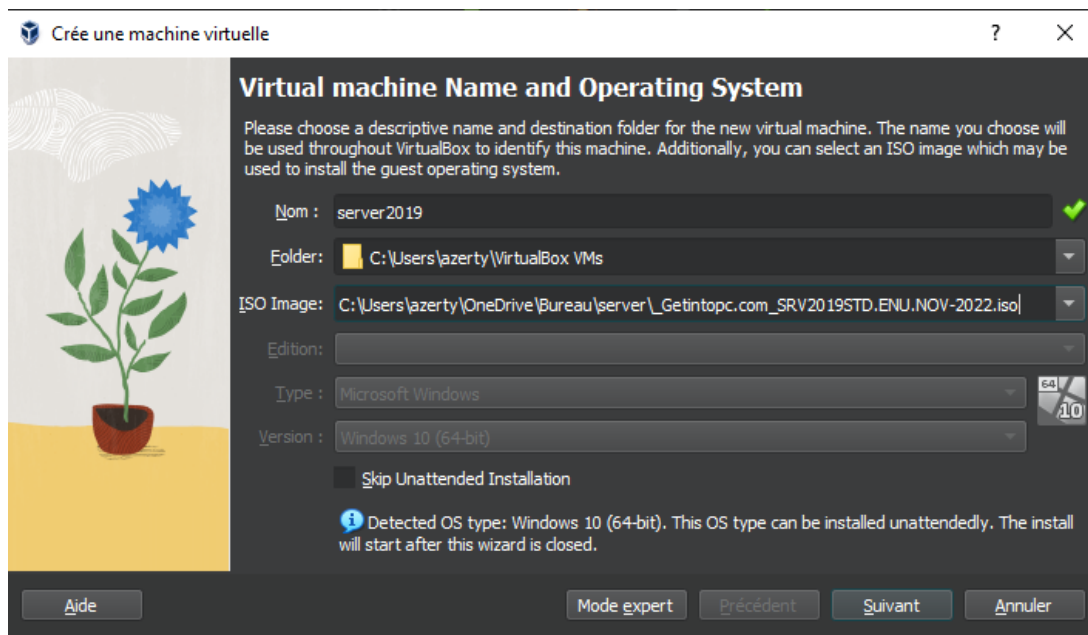
Après l'installation de VirtualBox on passe vers la création des machines virtuelles (machine serveur et machine Client) .il est important d'avoir une image iso pour les deux (serveur et client), après on accède vers Virtual Box et on commence la création des machines virtuelles

Pour le serveur :

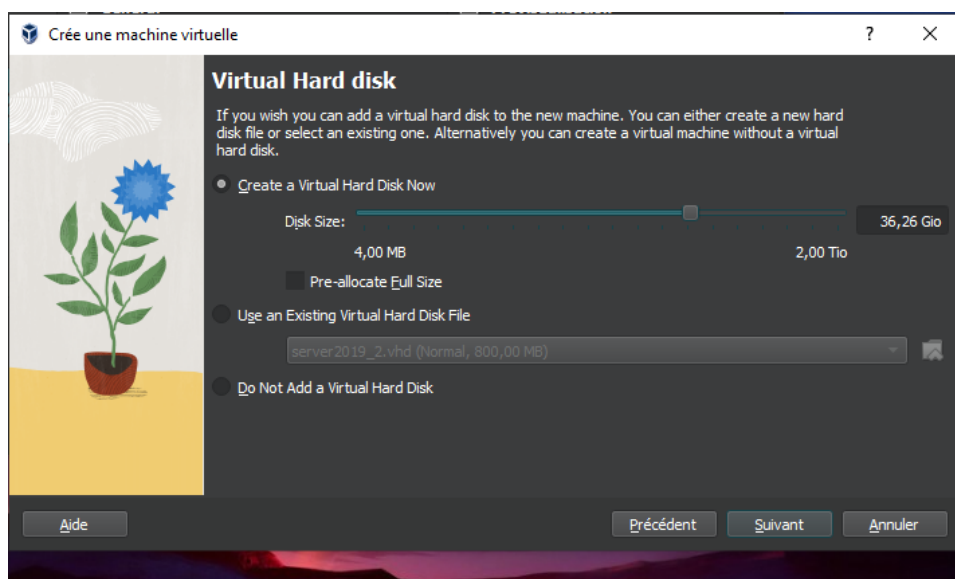
On attribue le nom et l'emplacement des fichiers de la machine ainsi que l'emplacement de

- Windows Server 2019 :

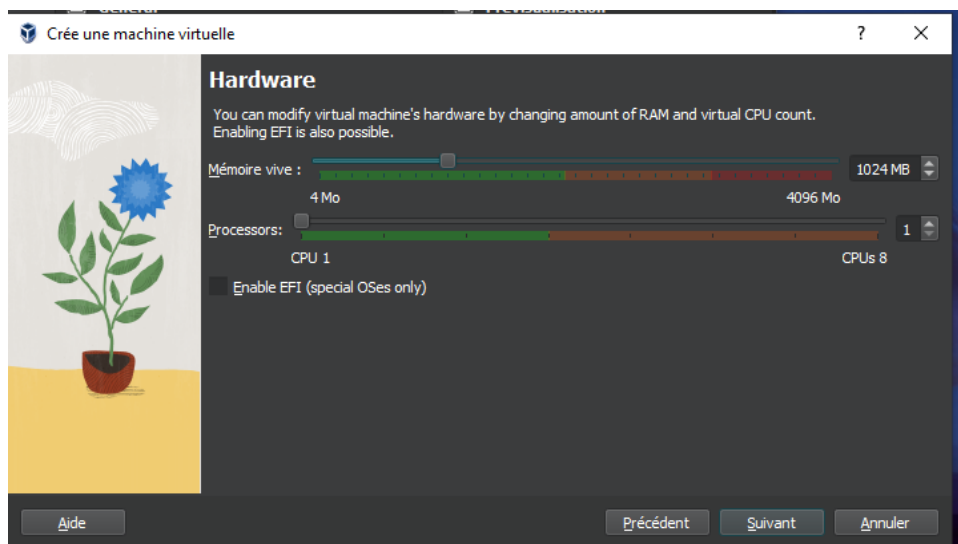
L'image iso :



On donne l'espace disque nécessaire (pour Windows server2019 32G au minimum) :



Ainsi que les paramètres de CPU et RAM :

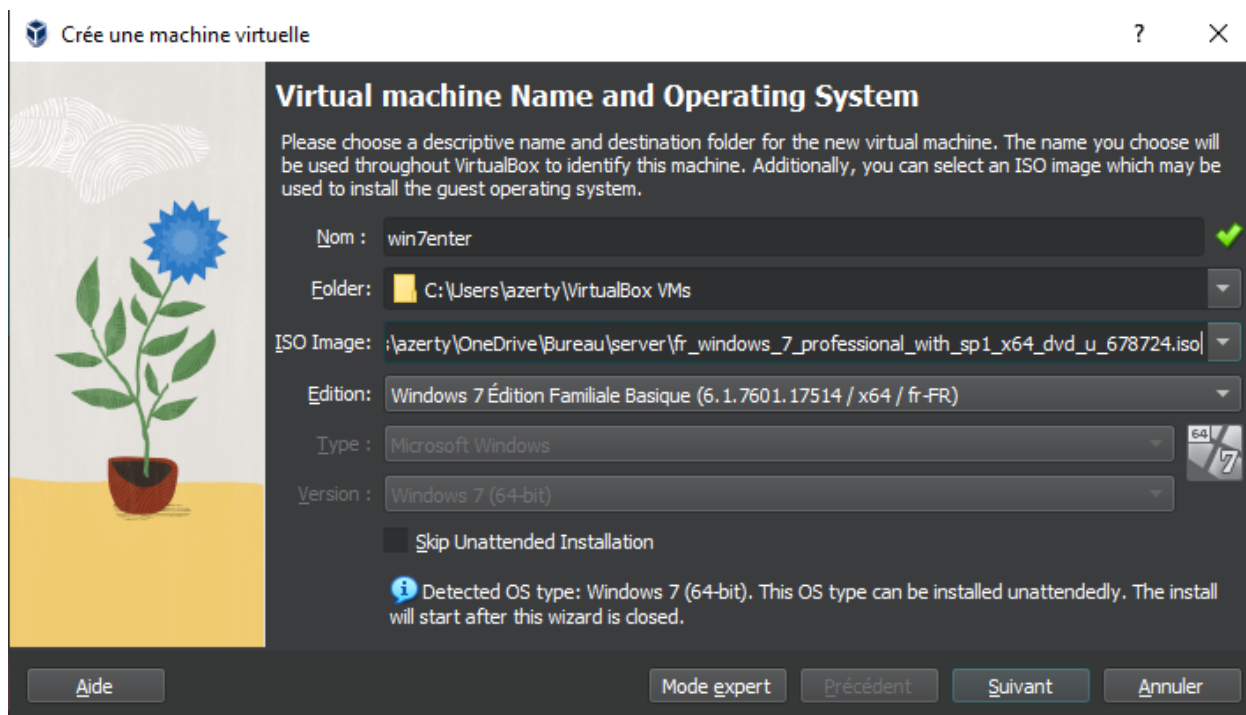


La même chose pour la machine client (Windows7) :

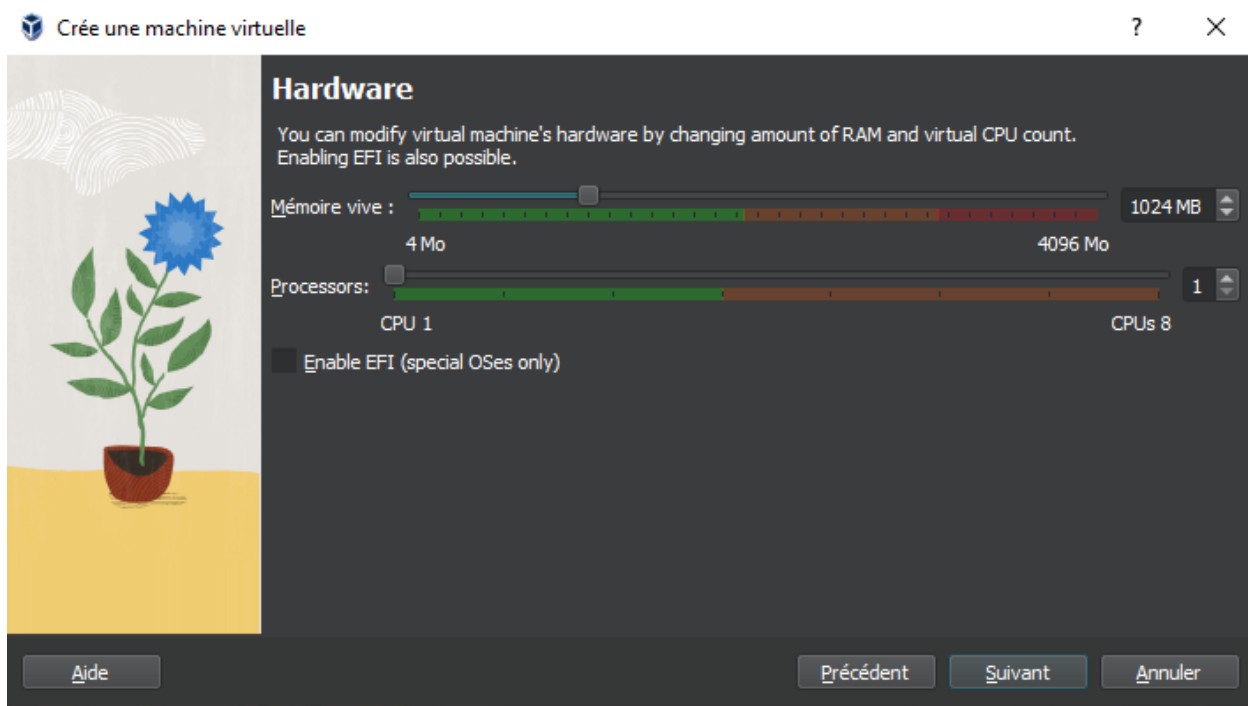
NB : Afin qu'on peut inclure notre machine Client dans notre Domaine et faire les traitements nécessaires il faut avoir une machine entreprise ou professionnelle ou ultimement, une machine famille ne peut pas être utilisée avec l'Active Directory.

- Windows 7 :

Le nom, l'emplacement et l'image ISO :



Le CPU et la RAM :

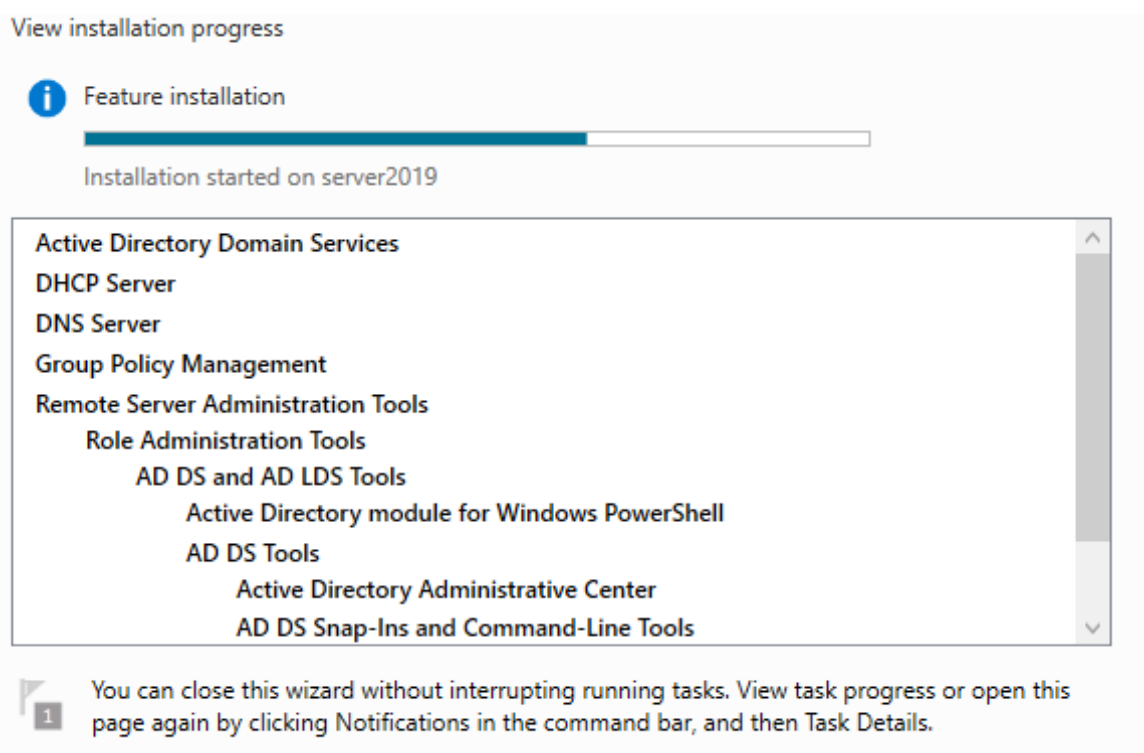


→Après qu'on termine le setup de notre environnement virtuel, on est maintenant près à commencer notre travail.

2. Création de domaine

Dans le Gestionnaire des services (Services Manager) on ajoute le service AD DS la rubrique de rôles, et suivie les étapes de l'installation :

Dans mon cas, j'ai décidé de télécharger DHCP et DNS en parallèle, puisqu'ils seront aussi utilisés.



Après la fin de processus de l'installation, en commence par la création d'une nouvelle Forêt(Forest), en créé une nouvelle Forêt pour ne pas avoir une autre en place, cette Forest sera contenir notre domaine de l'entreprise (dans mon cas c'est L'agence urbaine de Taza) AUT.

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name: auTaza1.ma

Le Nom de Notre Domaine est " auTaza1.ma. ,, .

On a coché la case de DNS afin que notre AD faire la configuration automatique de DNS, aussi la case Global Catalog (GC) qui représente un ensemble des index pour tout la base de données stocké dans notre Domaine Controller, il est utilisé pour faciliter la tâche de recherche et navigation dans les données de DC.

Et on a aussi donné le mot de passe de DRSM, c'est l'abréviation de Directory services Restore Mode, il est utilisé pour accéder au mode de restauration des services d'annuaires en cas de corruption de la base de données de notre contrôleur de domaine (DC).

Domain Controller Options

TARGET SERVER
server2019

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

La base de données de l'Active Directory Domain Services (AD DS) est composé de deux bases de données principales : NTDS et SYSVOL. Voici la différence entre ces deux :

The screenshot shows the 'Paths' step of the Active Directory Domain Services Configuration Wizard. The window title is 'Active Directory Domain Services Configuration Wizard'. In the top right corner, it says 'TARGET SERVER server2019'. On the left, there is a navigation pane with the following options: 'Deployment Configuration', 'Domain Controller Options', 'DNS Options', 'Additional Options', 'Paths' (which is highlighted in blue), 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area of the wizard is titled 'Specify the location of the AD DS database, log files, and SYSVOL'. It contains three input fields, each with a text box and a browse button (three dots): 'Database folder:' with the value 'C:\Windows\NTDS', 'Log files folder:' with the value 'C:\Windows\NTDS', and 'SYSVOL folder:' with the value 'C:\Windows\SYSVOL'.

Specify the location of the AD DS database, log files, and SYSVOL	
Database folder:	C:\Windows\NTDS
Log files folder:	C:\Windows\NTDS
SYSVOL folder:	C:\Windows\SYSVOL

Base de données NTDS (NT Directory Services) :

La base de données NTDS représente la base de données du DC (Domain Controller). C'est essentiellement la base de données qui stocke toutes les informations relatives aux objets de domaine, tels que les utilisateurs, les groupes, les ordinateurs, etc. Elle contient également des informations sur la structure du domaine, les stratégies de groupe, les relations de confiance, etc.

Elle est essentielle pour le fonctionnement global d'Active Directory car elle maintient l'état actuel du domaine et assure la cohérence des données entre tous les contrôleurs de domaine d'un même domaine.

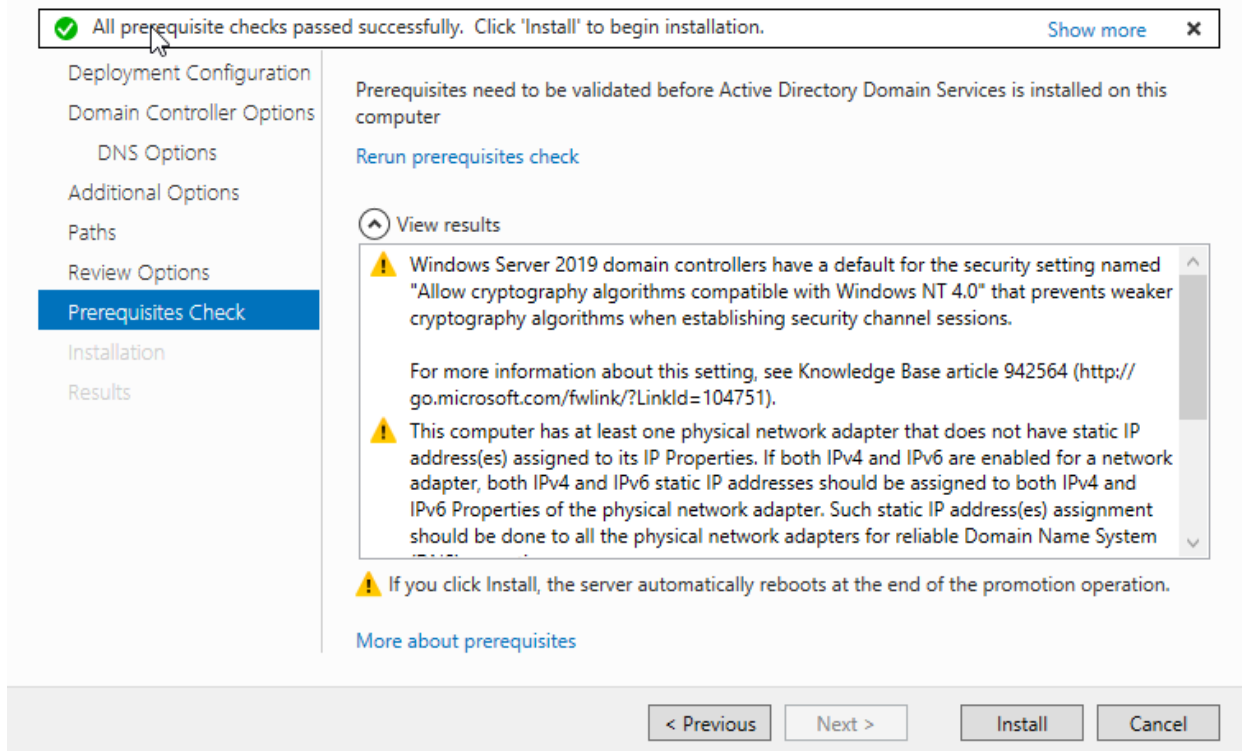
Base de données SYSVOL :

La base de données SYSVOL représente un dossier partagé créé par le système avec la permission lecture seul (Read-Only). Ce dossier contient Les données de GPO (Group Policy Objects) ainsi que Les scripts de connexion et de déconnexion qui s'exécutés lorsqu'un utilisateur se connecte ou se déconnecte d'un ordinateur du domaine.

SYSVOL assure la réplication de ces informations entre tous les contrôleurs de domaine d'un même domaine afin de garantir la cohérence des stratégies de groupe et des scripts dans tout l'environnement Active Directory.

Prerequisites Check

TARGET SERVER
server2019

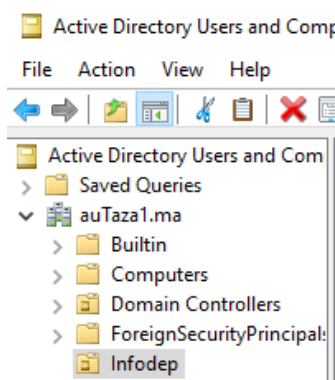


Après la vérification de toutes les informations, en fait l'installation des éléments configurés, puis en redémarre le serveur.

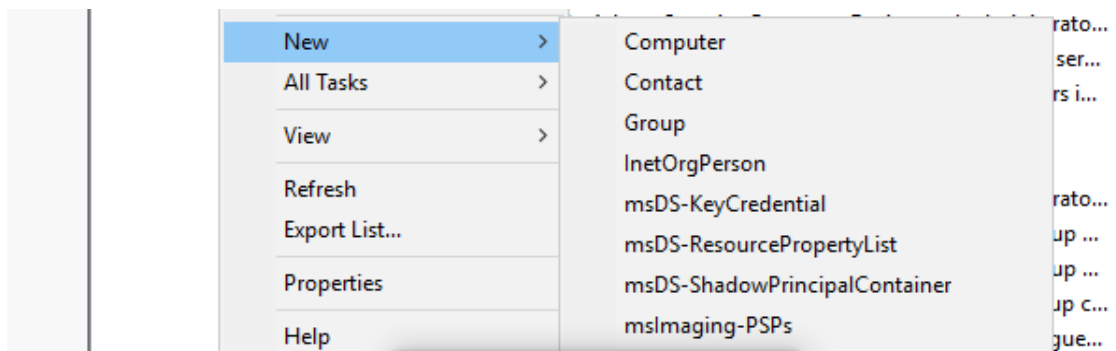
Après le redémarrage de serveur, on remarque que le nom de notre domaine est ajouté dans le login, cela signifie que nous ouvrons une session avec un compte active Directory.

3. Création des Unité Organisationnelles, les utilisateurs et les groupes

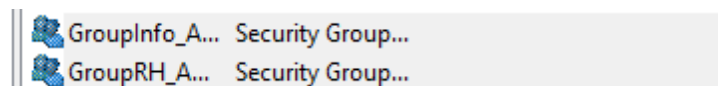
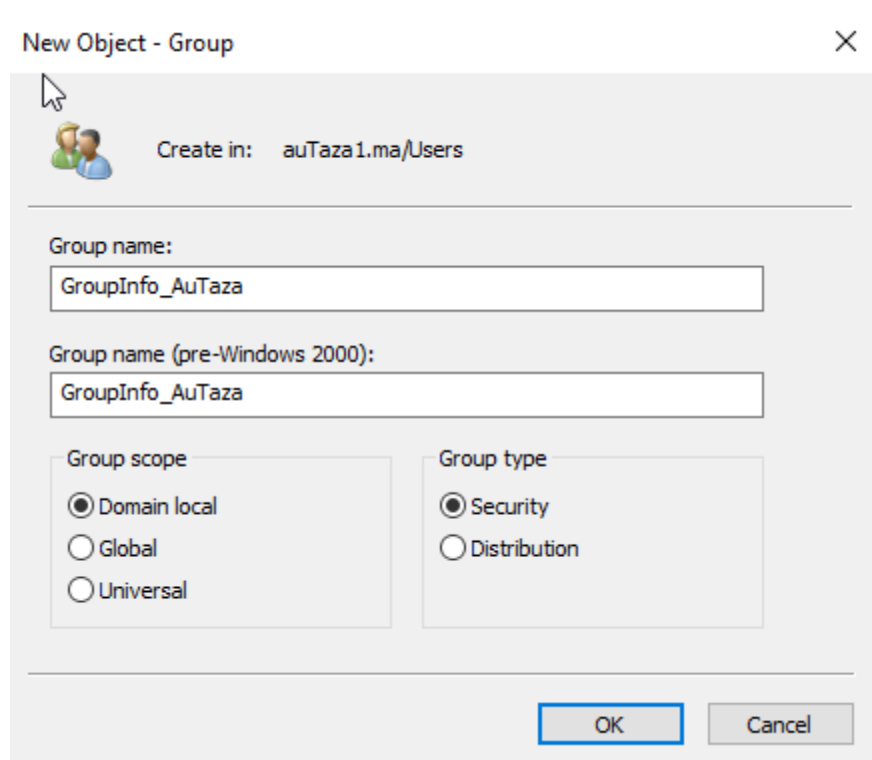
Pour créer l'unité organisationnelle en se dirige vers active Directory users and Computers, puis on choisit notre domaine et on choisit new Organizational Unit, on donne un nom a cette dernière, dans cet exemple j'ai créé une Unité Organisationnelle avec le nom InfoDep :



Après la création de OU, en passe vers la création des groupes, l'étape de création et assez simple, on fait un clic droit sur notre OU et en choisie new Group,




en attribue le nom a ce group ,et en coch domaine Local ,se group sera onc ajouté dans notre OU InfoDep



Après la création de group en passe vers la création des utilisateurs , et les ajouté dans notre group, dans les captures , j'ai créé deux group ,un pour le département informatique et l'autre pour le département des ressources Humain ,bien sûr j'ai suivie pendant la création des Unité Organisationnelle et Groups et utilisateurs j'ai suivie l'infrastructure de l'agence Urbain de Taza ,j'ai uniquement fournie des exemples .

Aussi pour la création des utilisateurs, on accède vers l'OU où on veut les créé, click droit et choisie new User, et en remplie les informations nécessaires :



Create in: auTaza1.ma/Users

First name: Initials:

Last name:


Full name:

User logon name:

User logon name (pre-Windows 2000):

L'ors d'ajoute de mot de passe en choisie si on veut que ce dernier soit modifier après la première authentication ou le gardé, cela avec les options fournie.

New Object - User ×



Create in: auTaza1.ma/Users

Password:

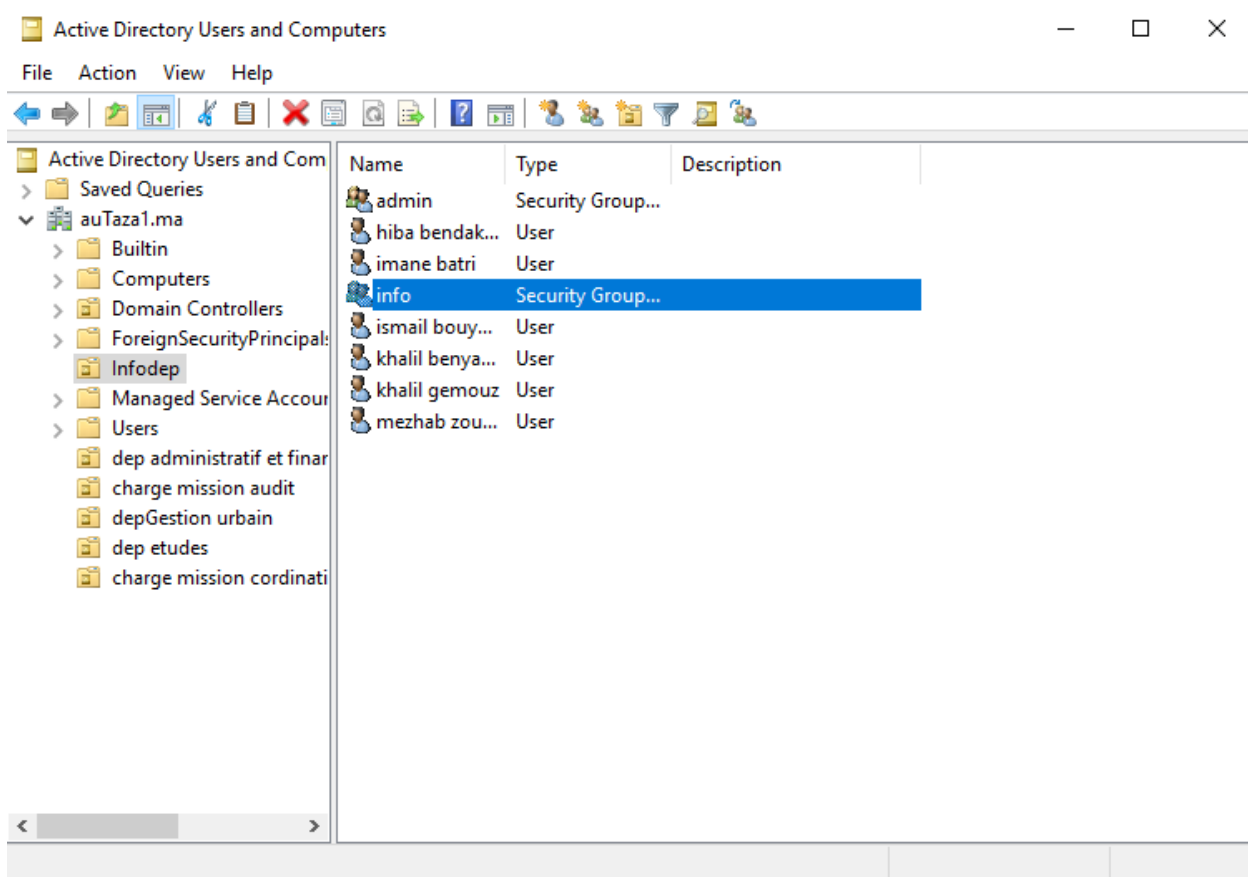
Confirm password:

☒ User must change password at next logon

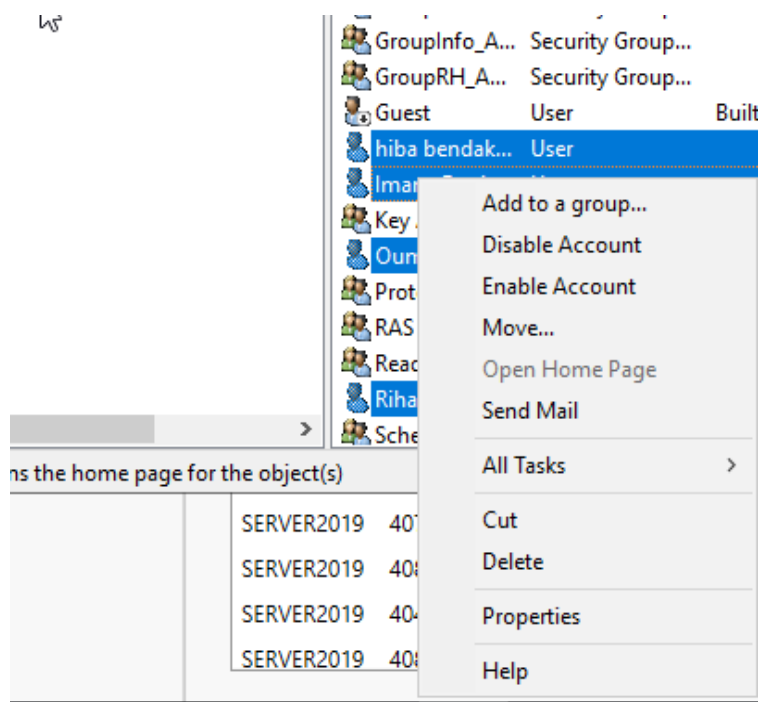
☐ User cannot change password

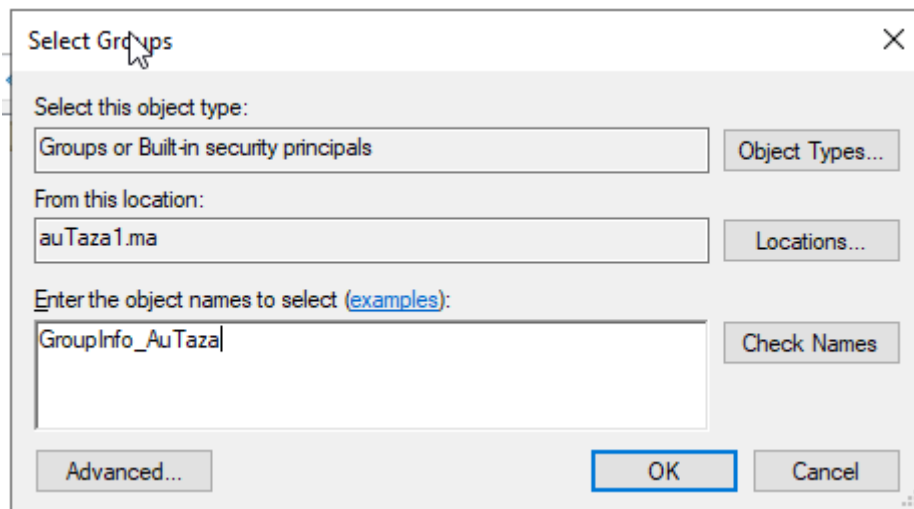
☐ Password never expires

☐ Account is disabled

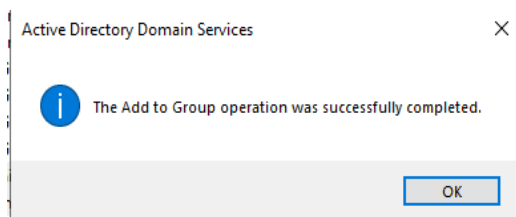


Et pour les ajouté dans notre group en sélection tous les utilisateurs qu'on veut ajouter dans un group et on fait un click droit et add to group





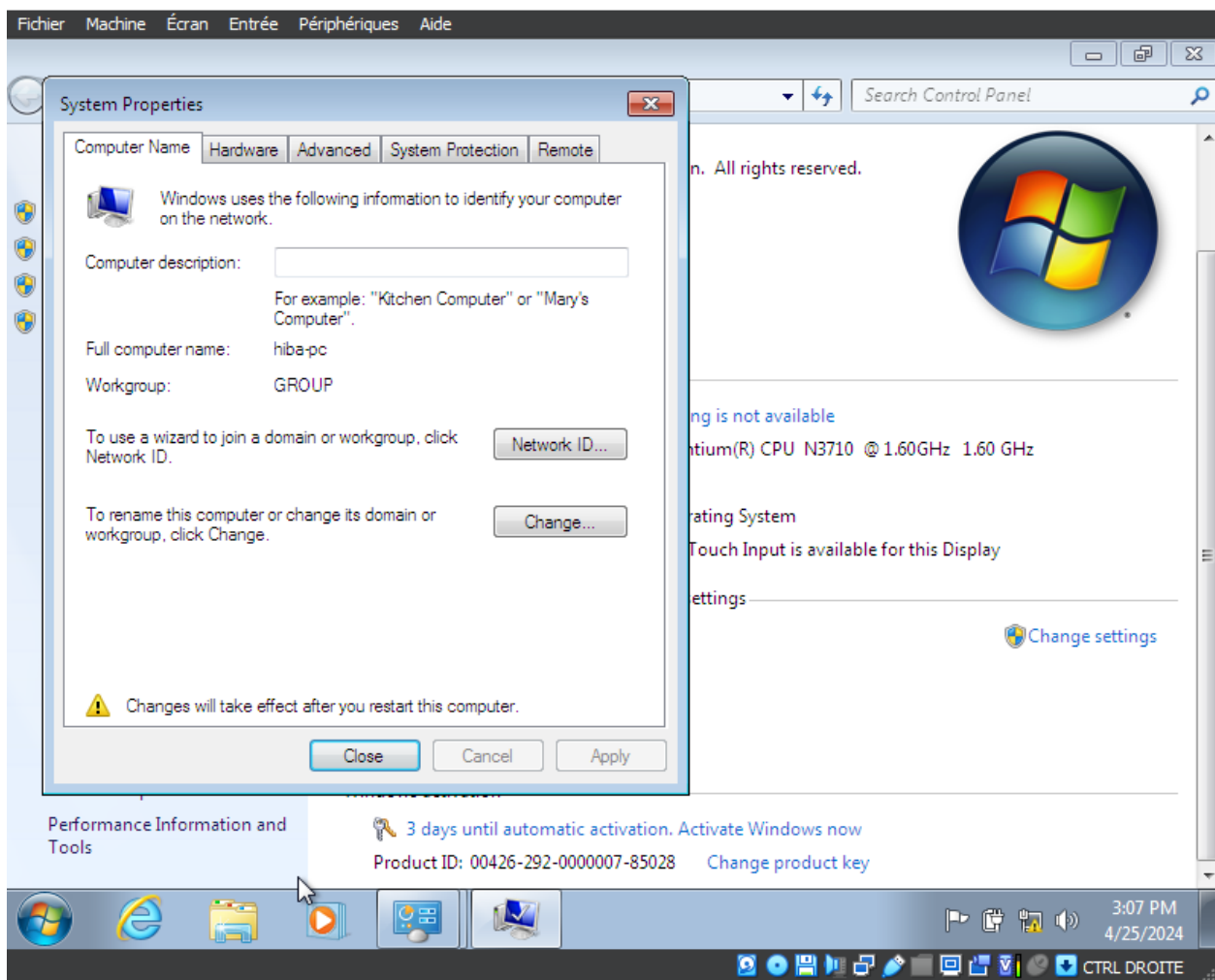
Message de succès :



➔ après qu'on aouté notre utilisateurs dans le groupe InfoDep ,en passe vers le coté client ,càd ajouté une Machine client dans notre domaine, dans notre cas ,j'ai utilisé comme client une machine windows7 ,voici les étapes pour l'ajouté au domaine :

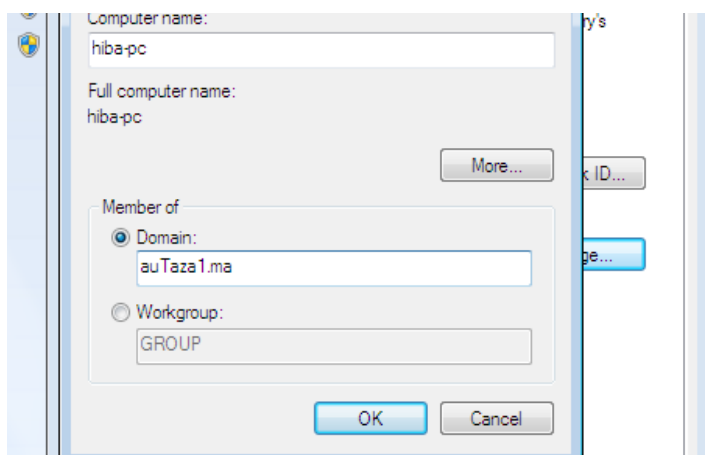
La premier étape et d'avoir les eux machine (client et serveur)au même réseau, dans mon cas j'ai déjà configuré DHCP et choisie réseau intern ,et la machine a donc obtenu une adresse IP de mon plage dans la configuration DHCP, j'ai tester la connectivité avec des ping entre les deux machine

En accède vers l'ongle panneau de configuration->sécurité et system->sécurité :

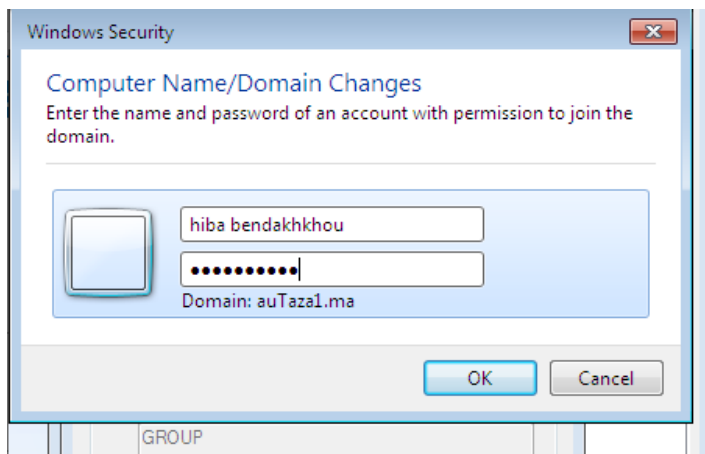


La machine est en mode workGroup, en cliquant sur Change pour la mettre dans notre domaine :

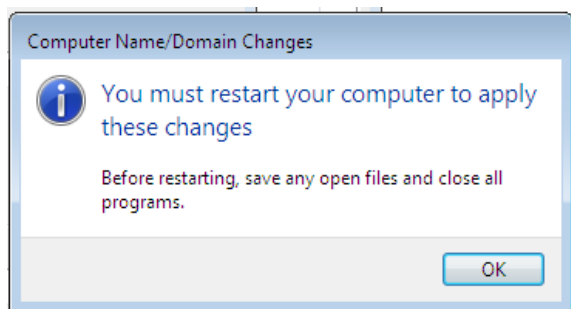
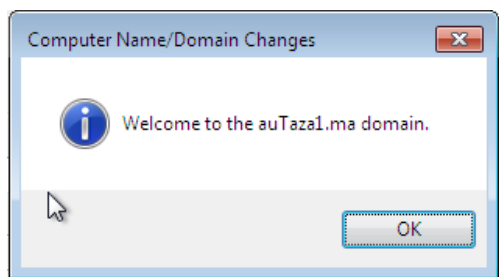
En donnant le nom de notre domaine, il est important d'avoir une version professionnelle / entreprise / ultime de Windows 7 ou quel que soit notre machine client mais pas une version home ou basic, car ces deux versions ne peuvent pas être incluses dans un domaine.



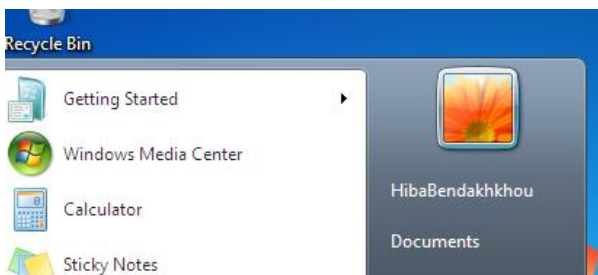
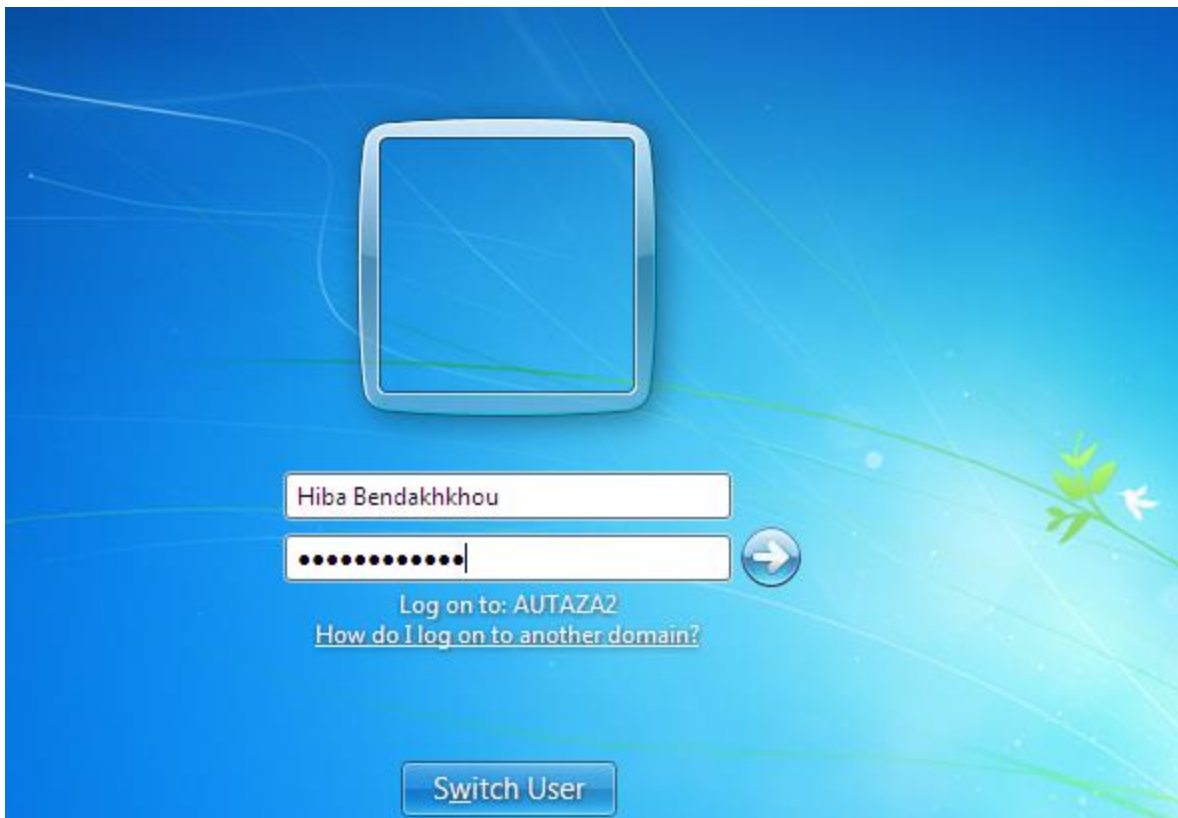
On donne le Nom de l'utilisateur et le mot de passe de notre compte utilisateur dont on veut se connecter :



Un redémarrage et demander après cette étape :



Après le redémarrage on peut s'identifier par le compte qu'on veut, il suffit de le choisir et d'insérer le mot de passe et on a accès à ce compte :



4. Profile itinérants

afin de configuré le Roaming Profils en doit premièrement créé un répertoire partagé avec le nom Profils ,j'ai choisie SmbShare ,j'ai créé un répertoire dans C avec le Nom Profils ,puis je donne le nom de share ,j'ai ajouté \$ pour qu'il soit caché, puis j'ai modifier les permission ,d'après la documentation Windows Server, puis dans le Gestionnaire des users et groups j'ajoute le path de profils ,en peut ajouter le path de chacun avec le userName ,mais ans mon cas j'ai sélectionné la liste des users et ajouter le path avec %username% pour une configuration automatique de chacun des users sélectionné :

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Server:

Server Name	Status	Cluster Role	Owner Node
SScript	Online	Not Clustered	

Share location:

☐ Select by volume:

Volume	Free Space	Capacity	File System
C:	11.9 GB	32.8 GB	NTFS
E:	7.45 GB	7.98 GB	NTFS
F:	46.4 GB	50.0 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

☒ Type a custom path:

Specify share name

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Share name:

Share description:

Local path to share:

Remote path to share:

Name: C:\profiles

Owner: Administrators (AUTAZA2\Administrators) [Change](#)

Permissions

For additional info

Permission entries

Type	Principal
Allow	SYS
Allow	Adm
Allow	Use
Allow	Use
Allow	CRE

Block Inheritance

What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

Les permissions :

Permission Entry for profiles

Principal: RH1 (AUTAZA2\RH1) [Select a principal](#)

Type: Allow

Applies to: This folder only

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Write attributes
<input type="checkbox"/> Traverse folder / execute file	<input checked="" type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

☐ Only apply these permissions to objects and/or containers within this container

[Clear all](#)

Name: C:\profiles

Owner: Administrators (AUTAZA2\Administrators) [Change](#)

Permissions Share Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (AUTAZA2\A...	Full control	None	This folder, subfolders and files
Allow	Users (AUTAZA2\Users)	Read & execute	None	This folder, subfolders and files
Allow	Users (AUTAZA2\Users)	Special	None	This folder and subfolders
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	RH1 (AUTAZA2\RH1)	Special	None	This folder only

New Share Wizard

Confirm selections

- Select Profile
- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation**
- Results

Confirm that the following are the correct settings, and then click Create.

SHARE LOCATION

Server: SScript

Cluster role: Not Clustered

Local path: C:\profiles

SHARE PROPERTIES

Share name: profiles\$

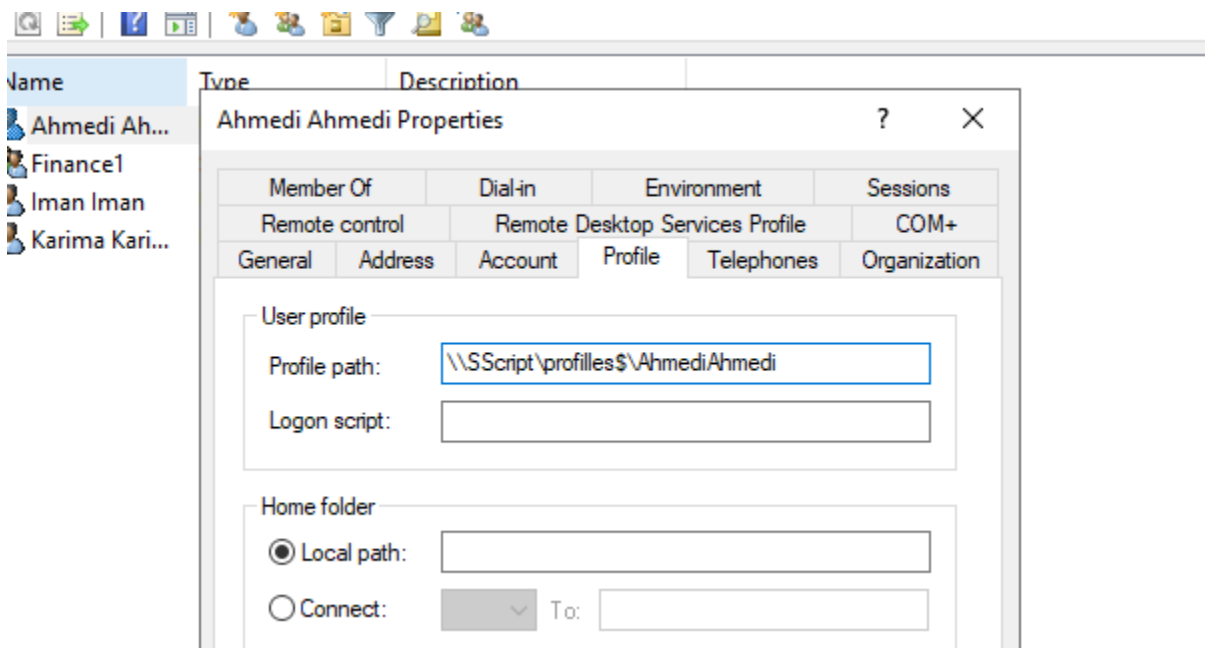
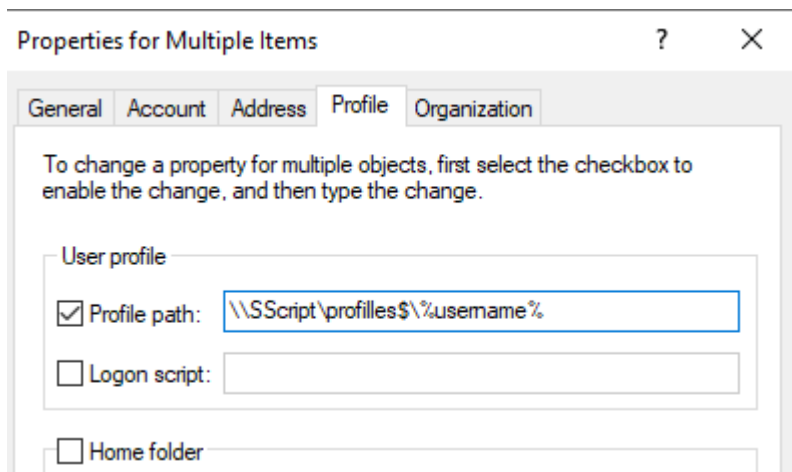
Protocol: SMB

Access-based enumeration: Enabled

Caching: Enabled

BranchCache: Disabled

Encrypt data: Disabled

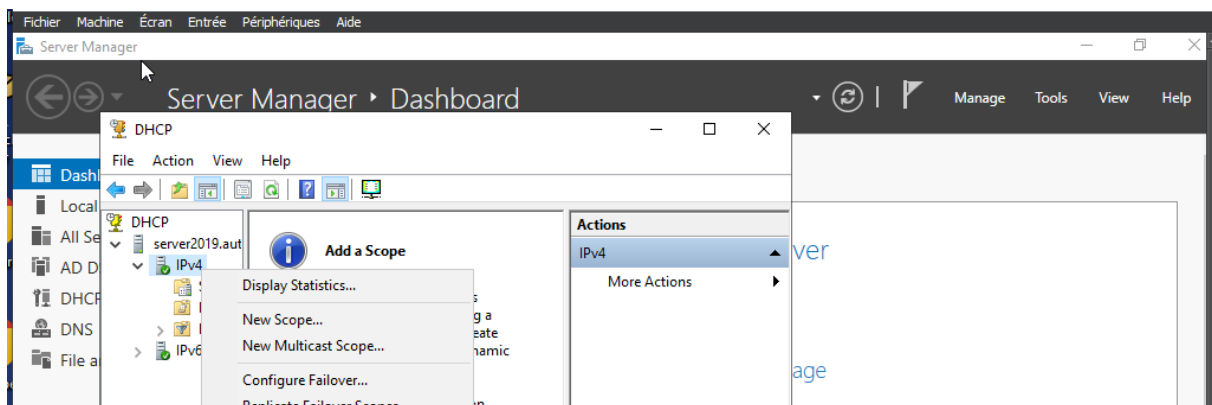


Et comme ça nous serons avoir pour chaque utilisateur un profile unique ,et pas un profile local.

5. Configuration WDS

▪ Configuration DHCP

Après l'installation de DHCP que j'ai déjà fait au début l'ors de l'installation de AD DS, en accède à l'interface de configuration de ce dernier et en créé une nouvelle Scope :



L'adresse du serveur DNS :

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text" value="SERVER2019"/>	<input type="text" value="10 . 0 . 0 . 1"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="10.0.0.1"/>	<input type="button" value="Remove"/>

Plage des adresses et le masque :

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

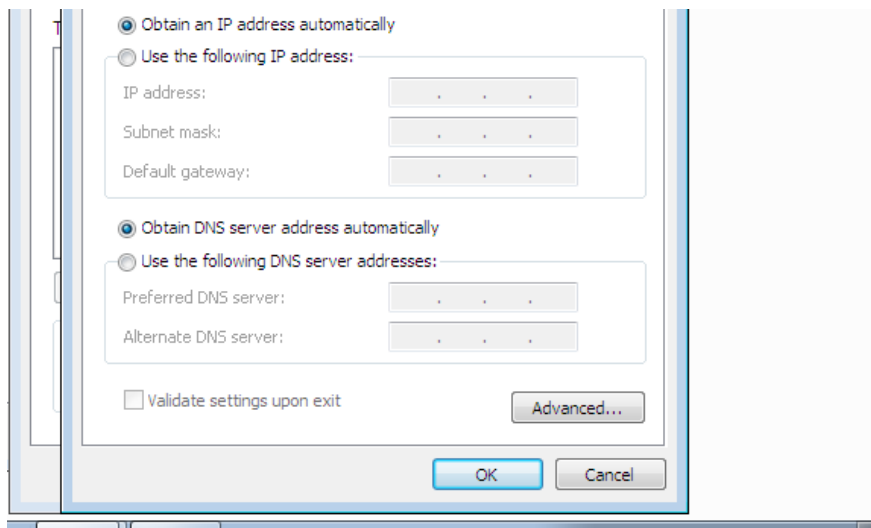
Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

J'ai testé par la machine client :



Il a obtenue une adresse dans le plage de mon scope :

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\imane batri>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : auTaza1.ma
    Link-local IPv6 Address . . . . . : fe80::41ca:83a4:8412:f84x11
    IPv4 Address. . . . . : 10.0.0.100
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . :

Tunnel adapter isatap.auTaza1.ma:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : auTaza1.ma

C:\Users\imane batri>_

```

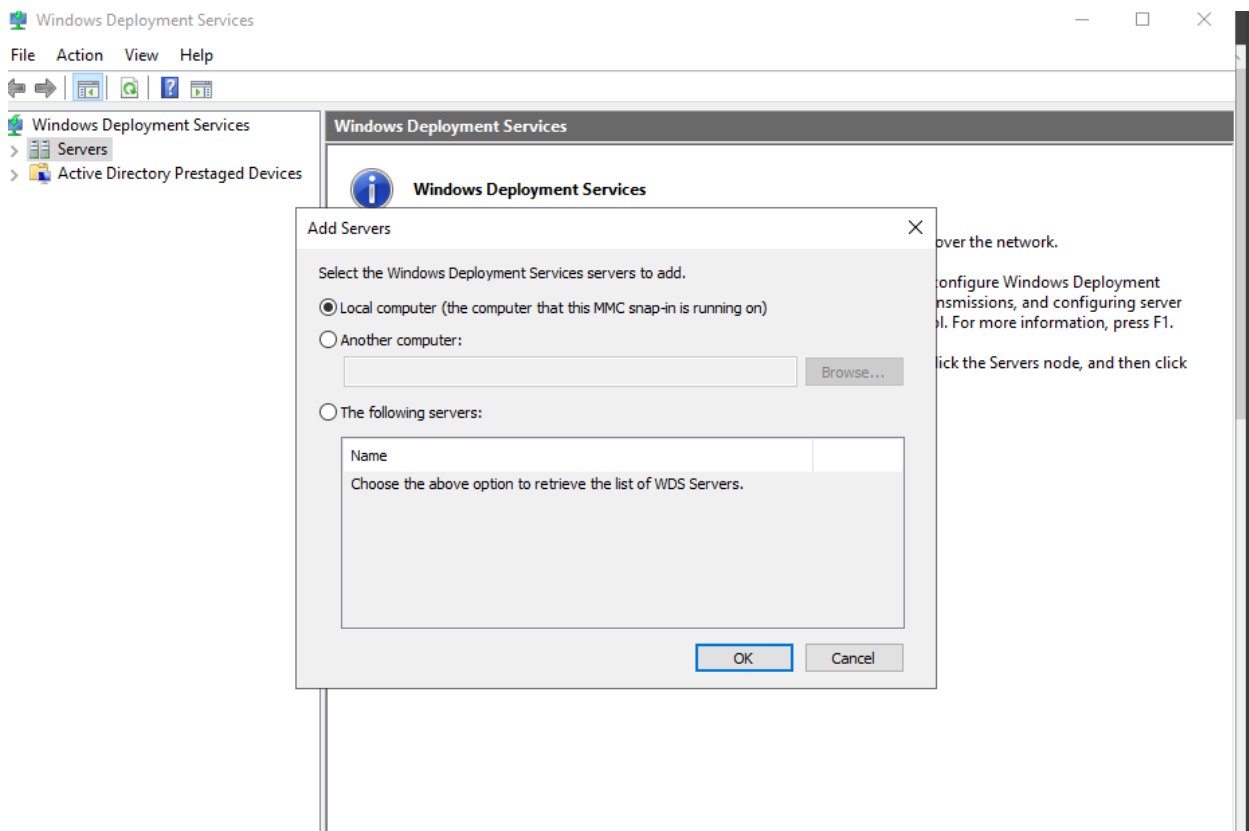
▪ Configuration WDS :

Dans la partie théorique, nous avons souligné l'importance de WDS dans un réseau, où le déploiement et la mise à jour des systèmes d'exploitation peuvent devenir des défis majeurs en raison du nombre élevé de machines. Pour configurer WDS, plusieurs étapes sont nécessaires. Tout d'abord, il est crucial d'avoir une image ISO du système d'exploitation sur le serveur. Ensuite, la configuration du serveur DHCP est essentielle, car elle permet aux machines d'obtenir une adresse IP dans le réseau et de communiquer avec le serveur pour récupérer l'image ISO.

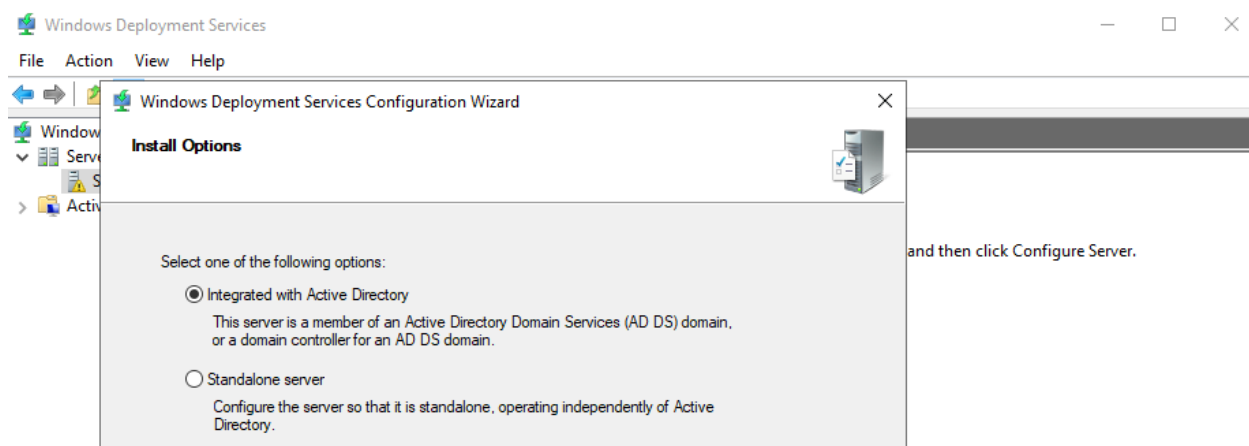
Le processus de démarrage PXE est une composante clé de cette configuration. Lorsque le client démarre, il informe le serveur DHCP de l'utilisation du serveur PXE. Le DHCP envoie alors l'adresse IP du serveur PXE (Option 66)(c-à-d le serveur où i y a l'image iso) ainsi que le nom du fichier de démarrage (Option 67) (les fichiers boot.wim et install.wim) au client. Le client contacte ensuite le serveur PXE pour demander ces fichiers de démarrage. Ces fichiers sont envoyés au client par le serveur PXE, et le processus de l'installation de l'OS commence.

Pour la configuration de WDS dans notre Windows server, il faut installer le module premièrement Bien-sûr en inclue Management Tools.

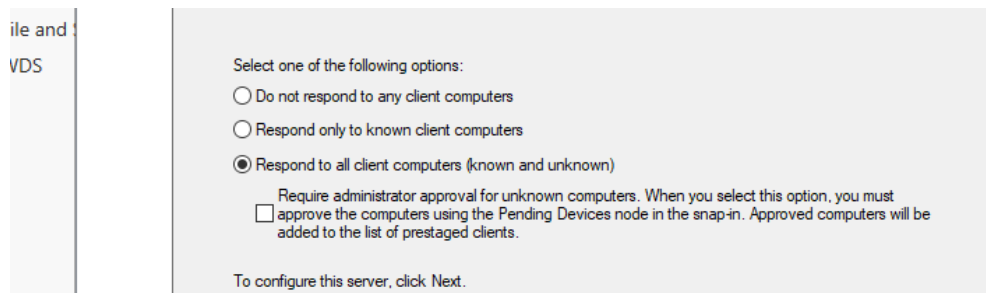
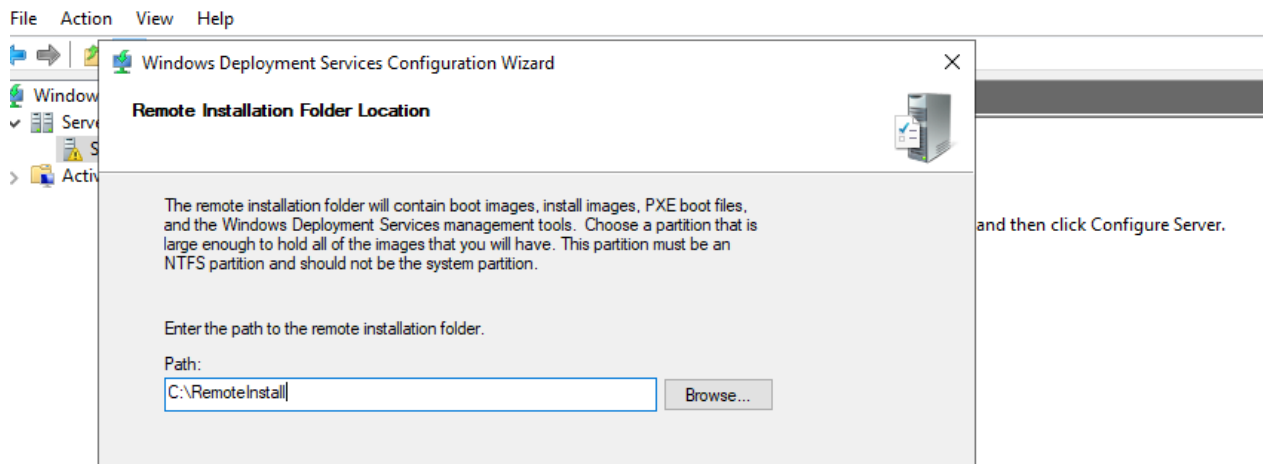
L'étape suivant et d'accéder vers l'onglet de configuration, dans laquelle en donne l'emplacement (le serveur) où en veut ajouter notre service WDS,



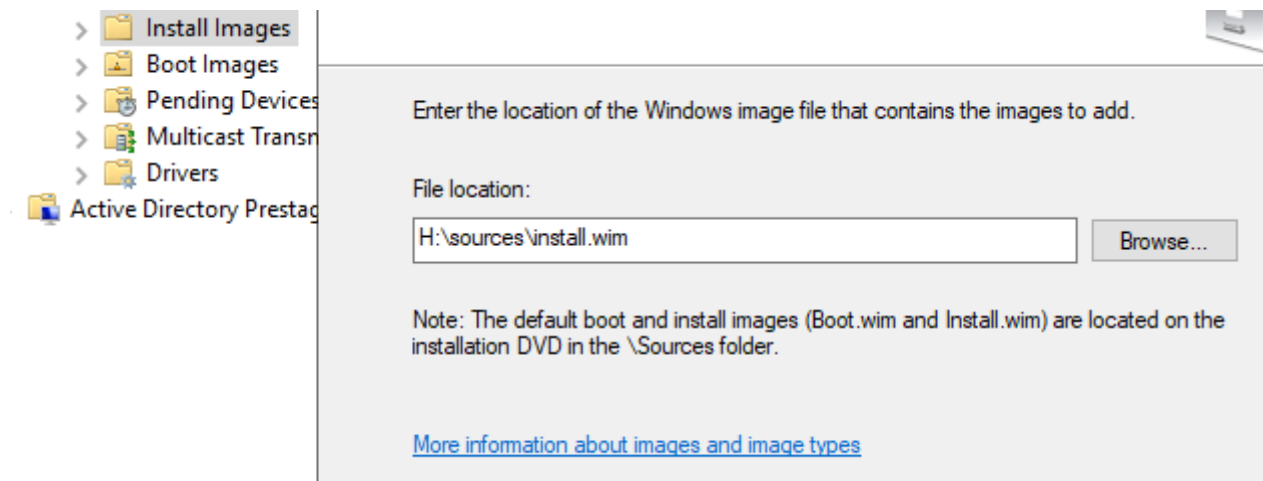
dans mon cas j'ai choisi le serveur local que j'ai configuré comme serveur DNS,DHCP et DC au même temps ,(pour la configuration DHCP il sera donné par la suite de cette partie) ,puis en choisie si on veut que notre serveur sera incluse avec le AD DS ou séparé de ce dernier(dans mon cas c'est incluse),



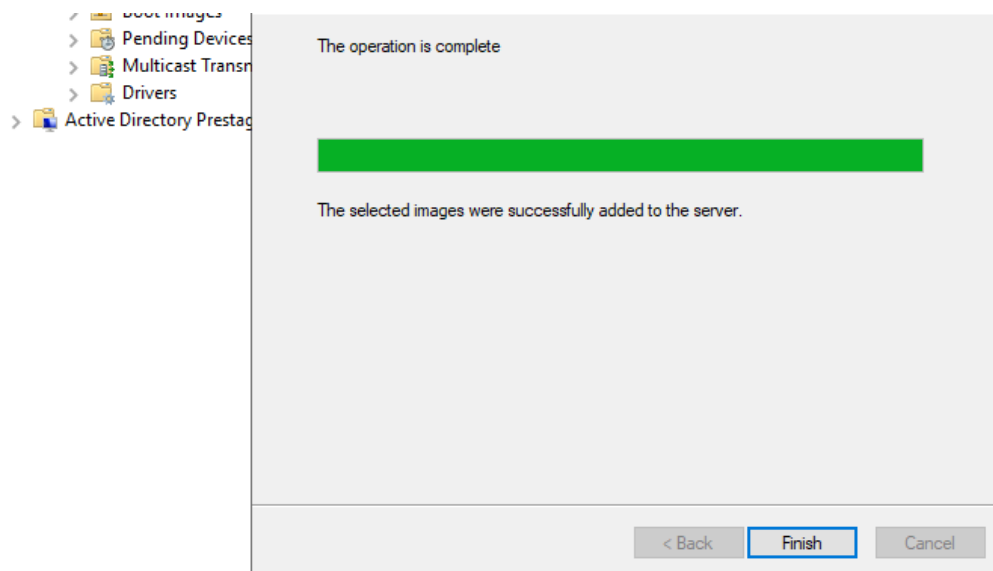
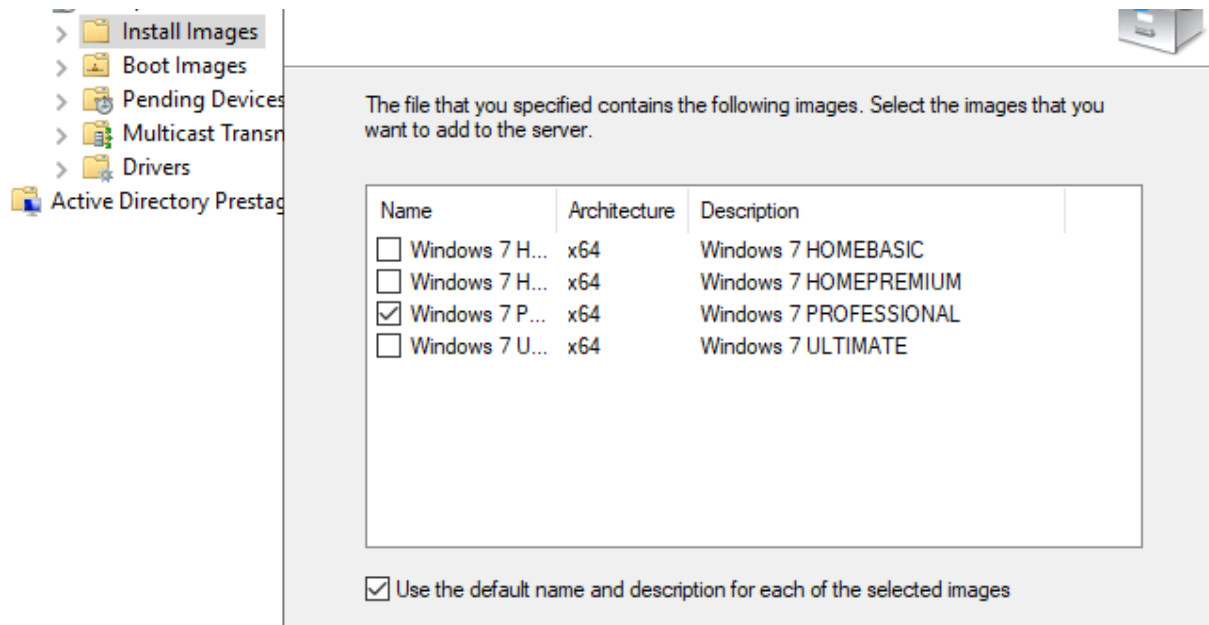
puis je donne l'emplacement de dossier qui sera contenir tout mes fichier de l'installation (Images iso et fichier boot PXE),et je choisie que WDS répondre a toutes les machines :



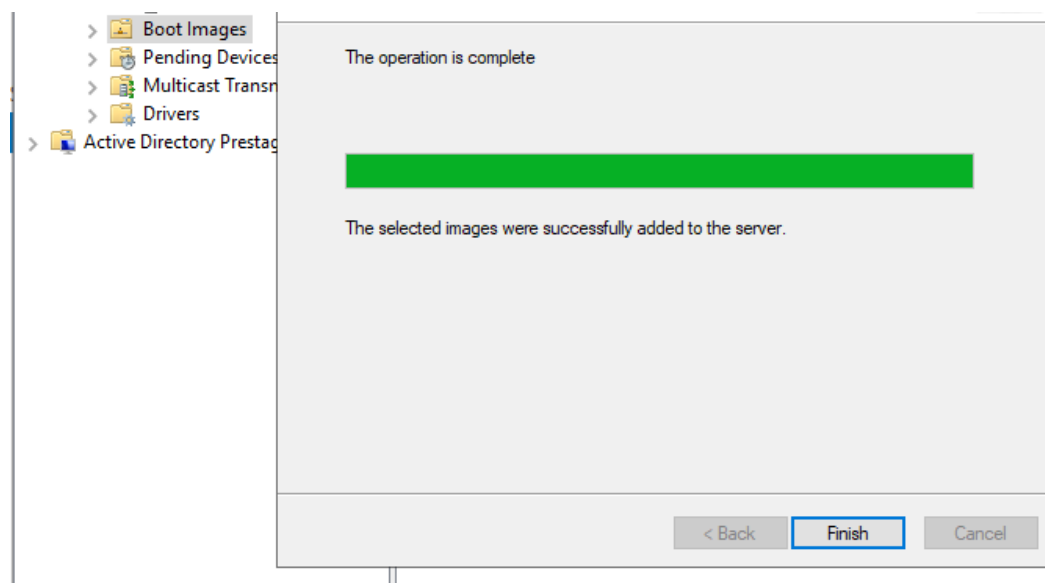
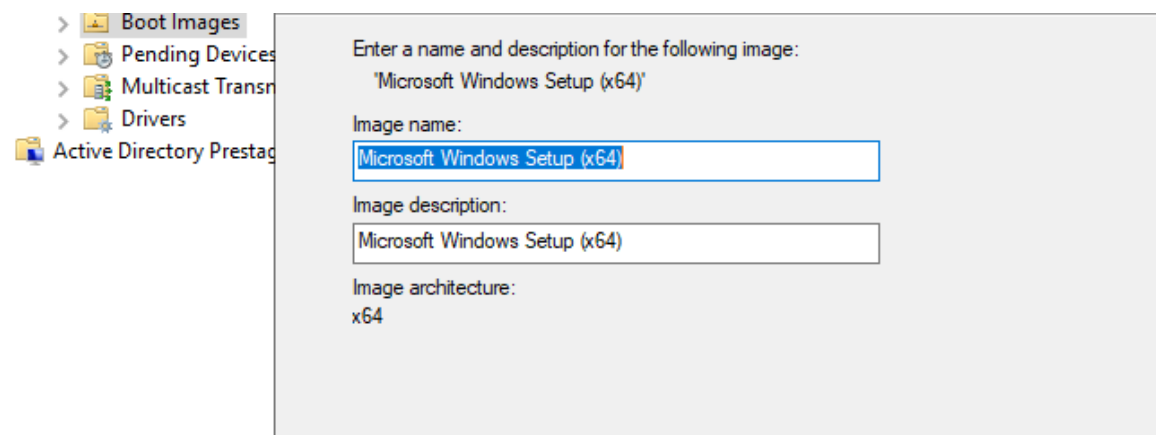
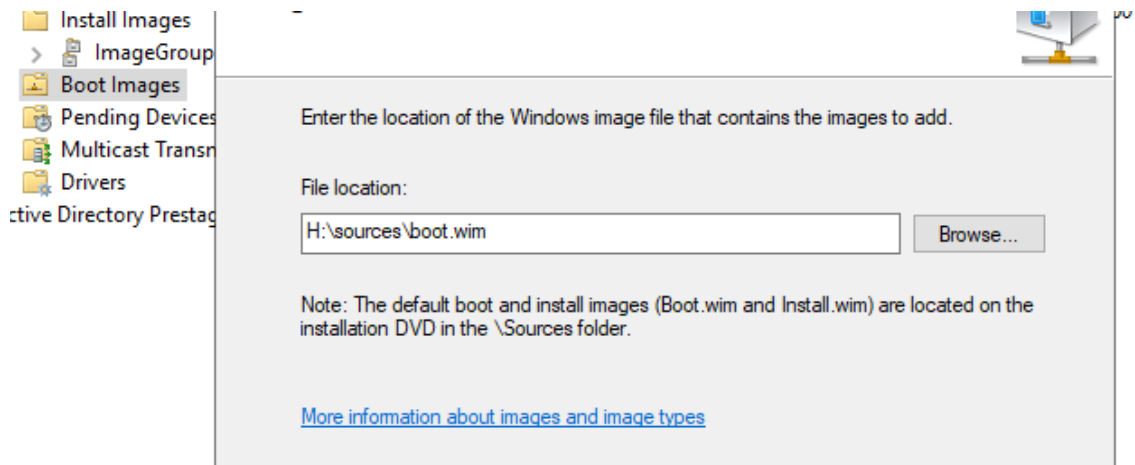
En spécifier l'emplacement :



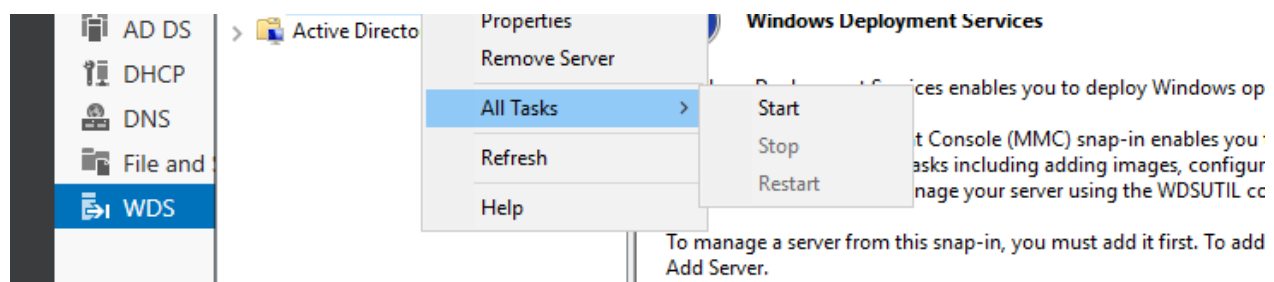
En choisie l'image qu'on veut (dans mon cas Windows 7 Professional) :



Même chose pour boot image :



en démarre le serveur :



Puisque j'utilise virtualBox je dois télécharger une extension qui me permet de faire le PXE boot.

Le test :

Pour tester on doit créer une machine virtuelle sans avoir déposé une image iso , et activé l'option *boot from Network*, ainsi que mettre la carte réseau en réseau interne ,et notre machine serveur doit être aussi démarré .

Ici On donne le nom de l'utilisateur e notre domaine et son mot de passe :

Entrez votre nom d'utilisateur au format domaine\utilisateur ou utilisateur@domaine.com.

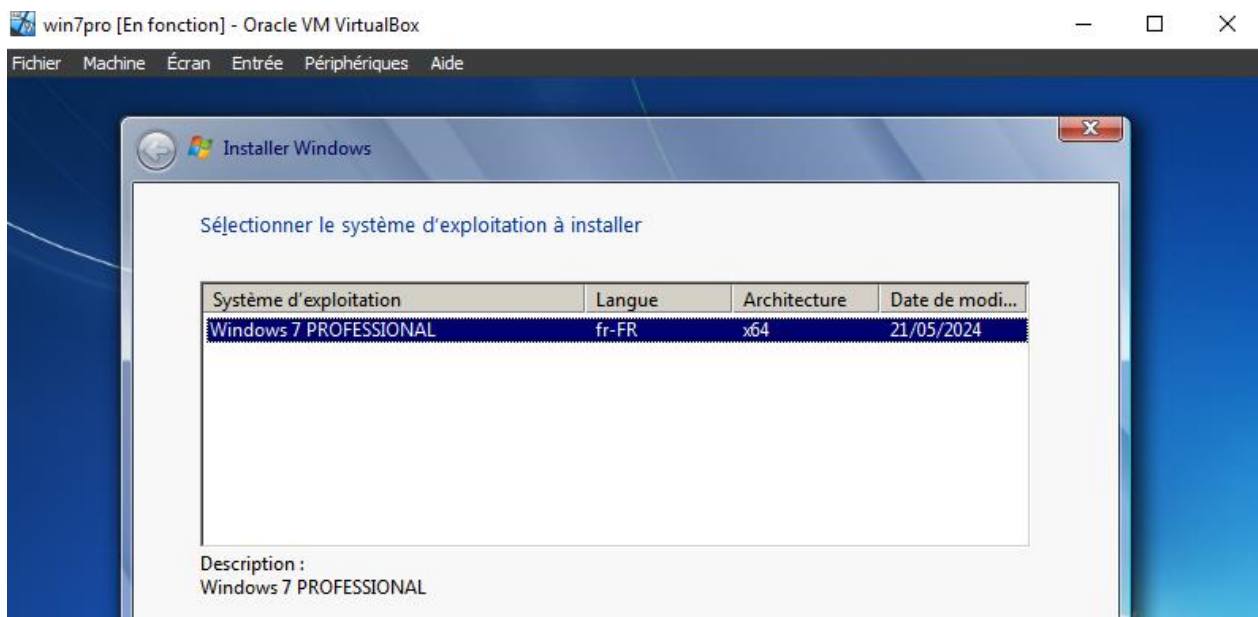
Nom d'utilisateur :

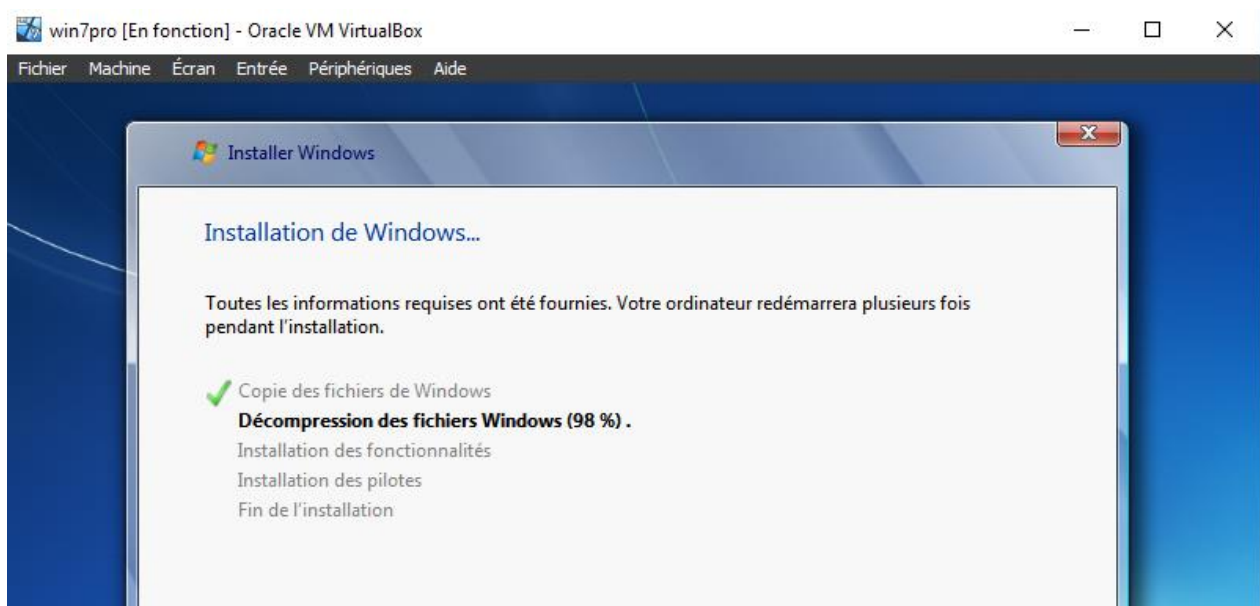
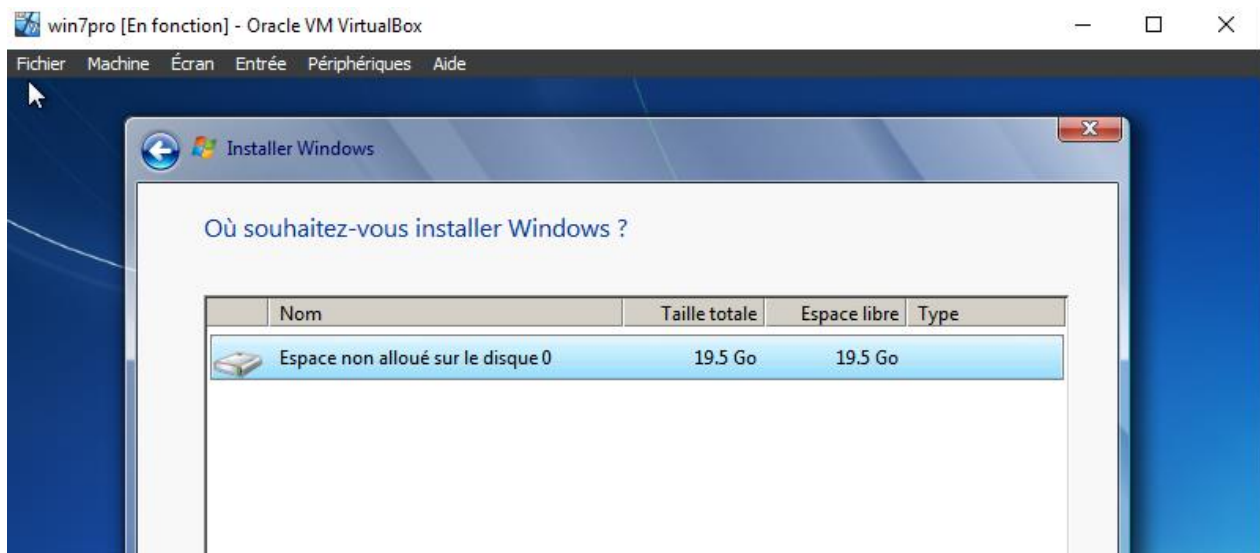
Mot de passe :

OK Annuler

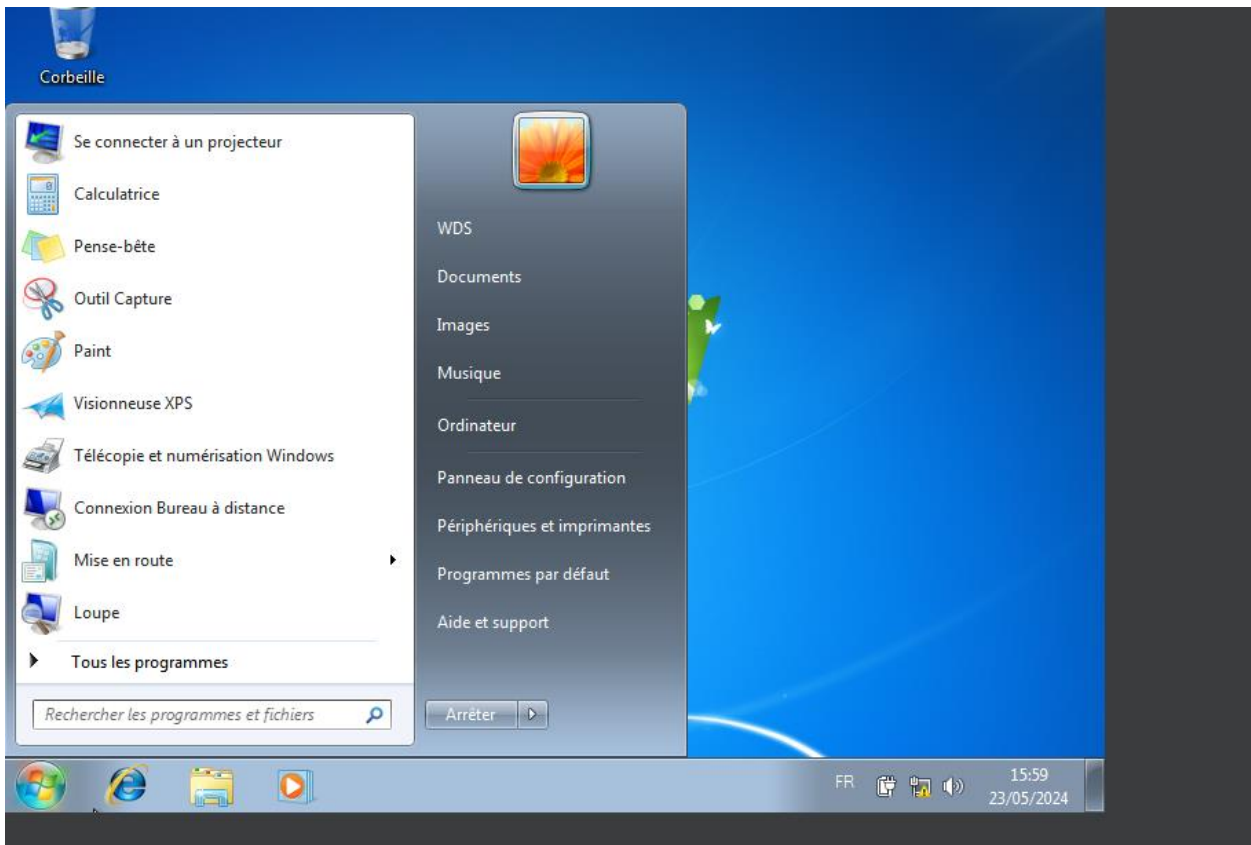
Paramètres régionaux: Français (France)

Clavier ou méthode d'entrée: Français





Et comme ça, notre System d'exploitation est installé avec WDS.



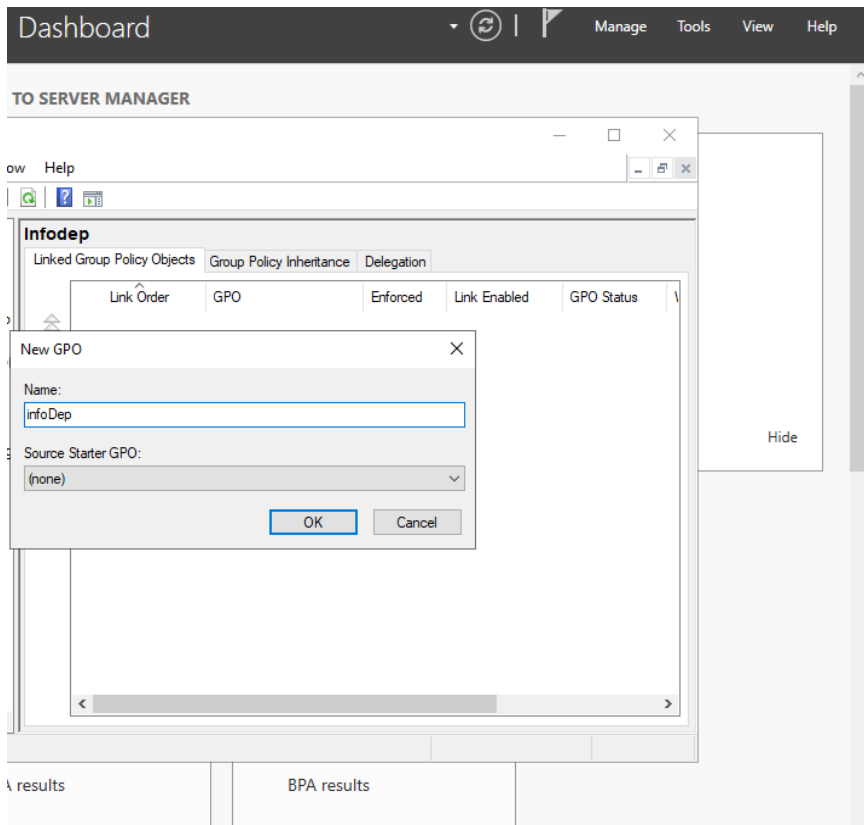
6. Configuration des GPO

Les GPO mentionnées précédemment représentent des mesures de sécurité et de contrôle d'accès mises en place pour protéger le système informatique de l'entreprise. Les GPO appliquées sont les suivantes :

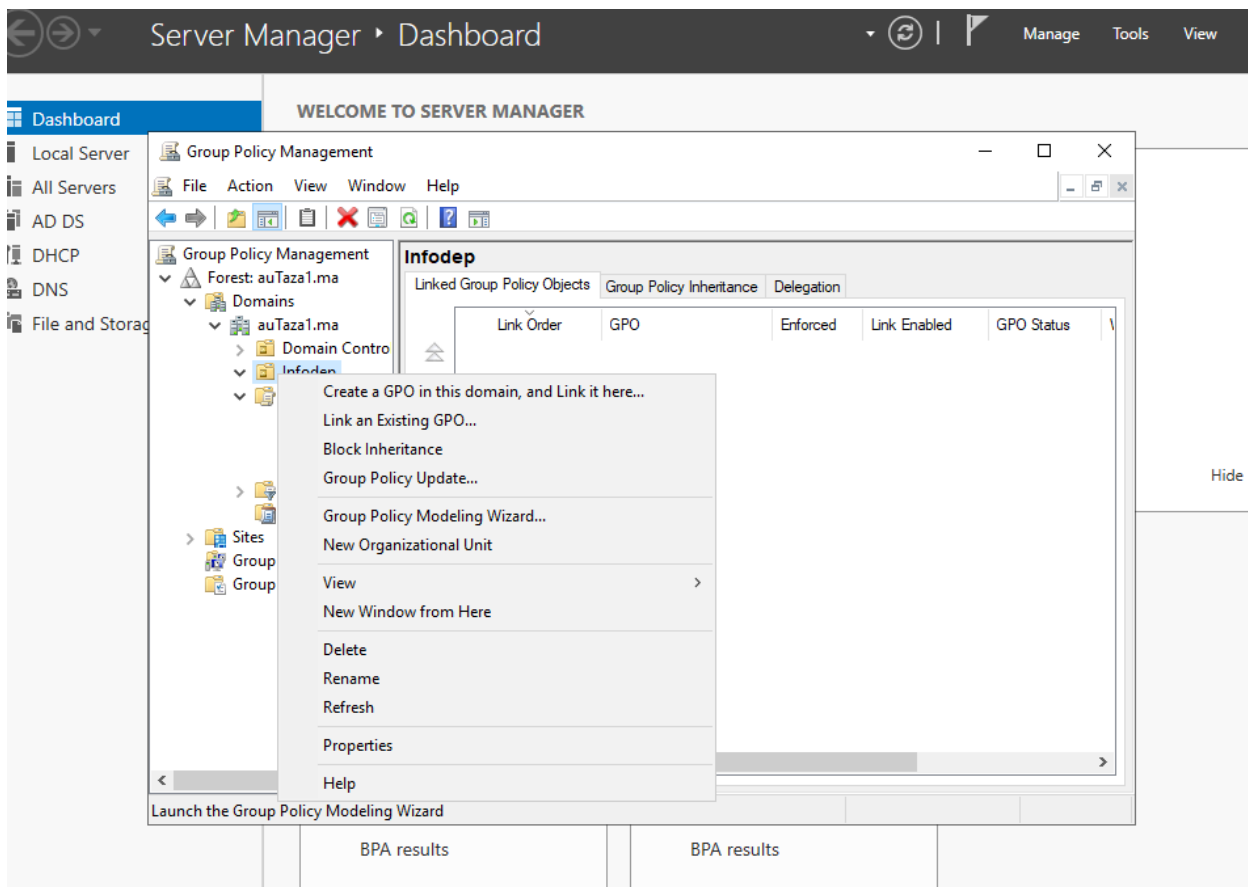
- Interdiction de changer le fond d'écran du menu Démarrer.
- Interdiction d'accéder au Panneau de configuration.
- Interdiction d'accéder à l'invite de commandes (cmd).
- Interdiction de lire les clés USB insérées.

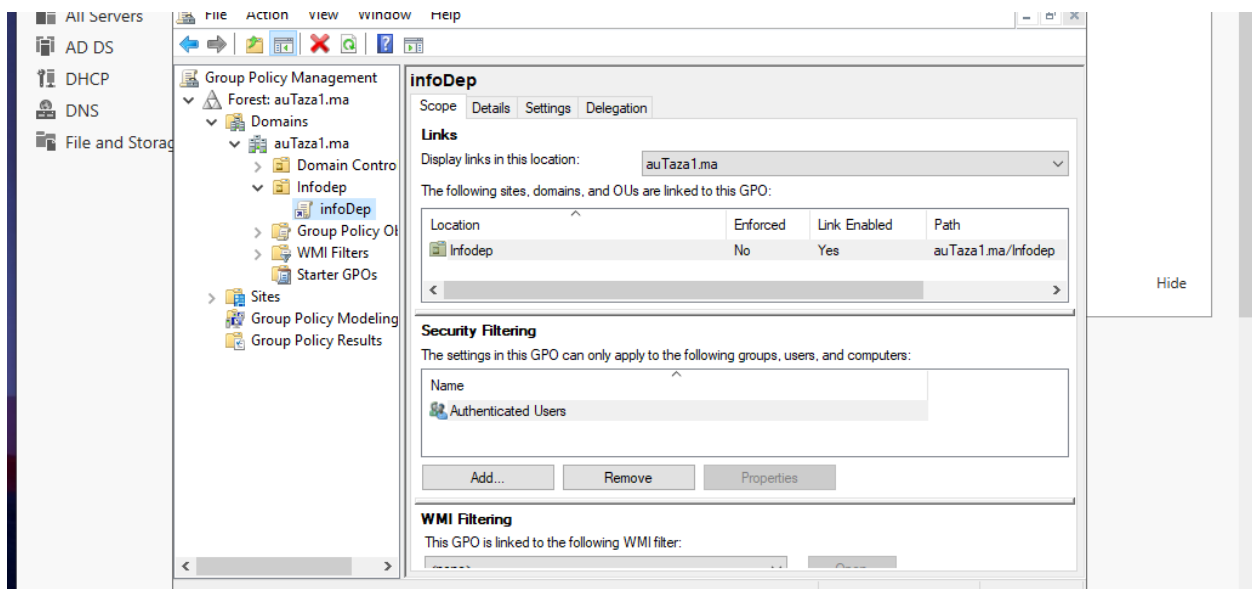
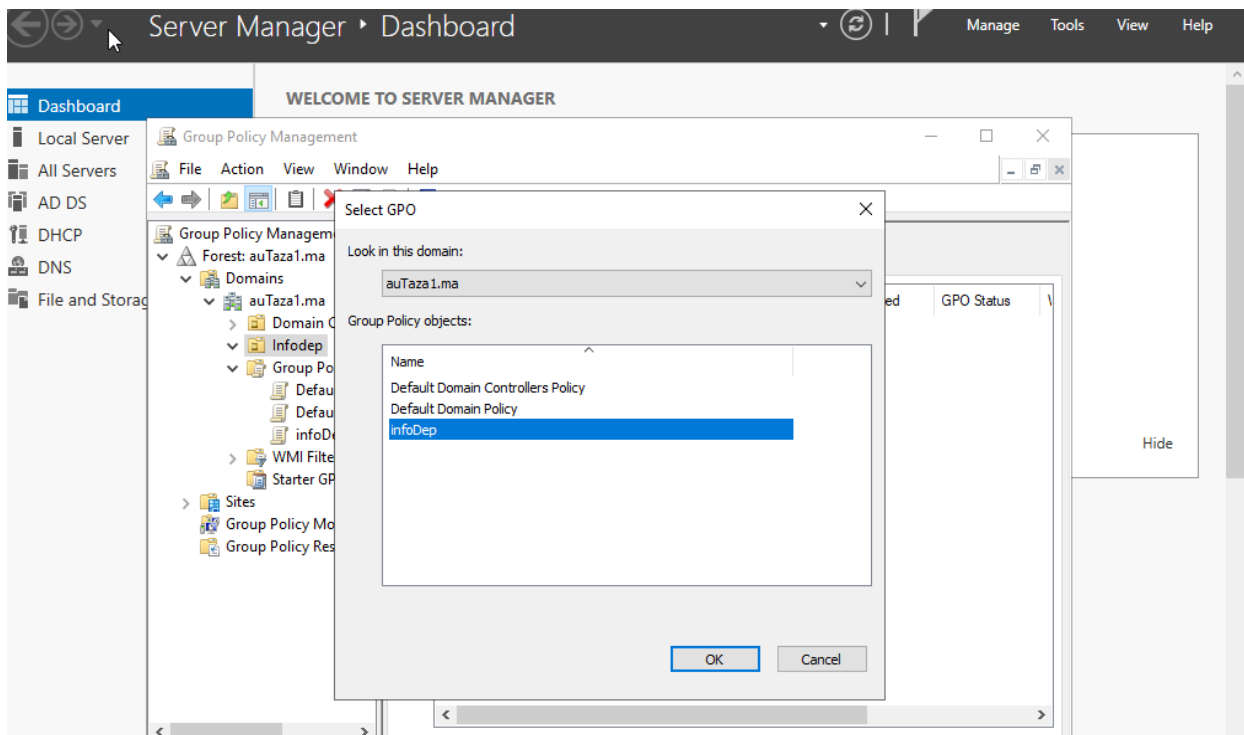
Bien sûr, les GPO dans ce projet ont été appliquées à chaque unité organisationnelle (OU) en fonction des besoins spécifiques de chaque département et des logiciels nécessaires à chaque utilisateur. Les captures de données ne sont fournies qu'à titre explicatif.

Premièrement pour appliquer les GPO on accède au Group Policies Management, clic droit sur GPO et en choisir new GPO, on donne le nom :



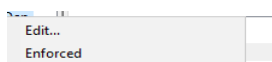
Après cette étape on doit lier notre GPO avec notre GPO dans ce cas on fait un clic droit sur la GPO et on sélectionne le OU sur lequel on veut appliquer notre GPO.



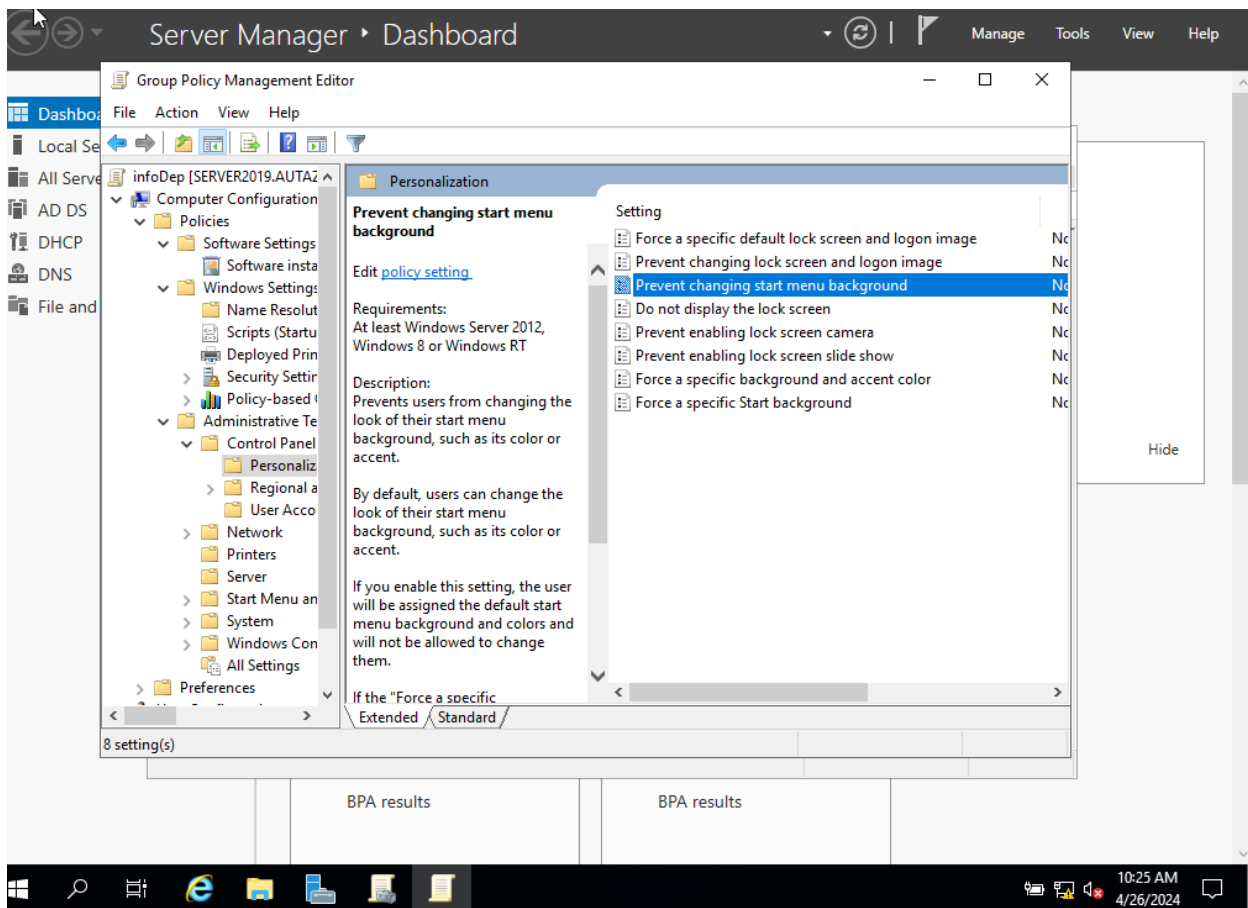


(link enabled Path auTaza1.ma/Infodep)

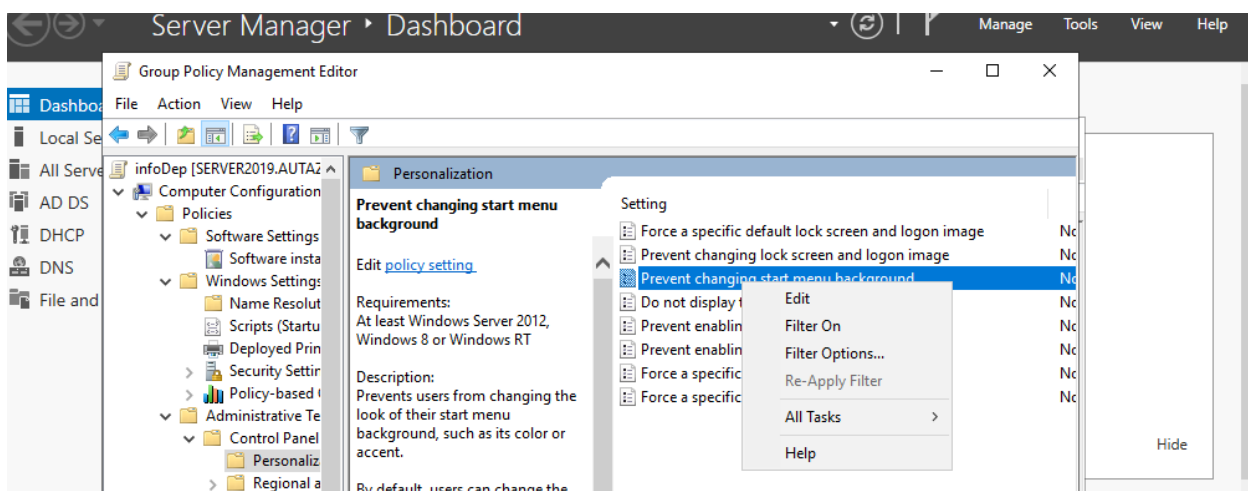
Après cette étape en passe vers l'application des GPO que j'ai mentionné précédemment :

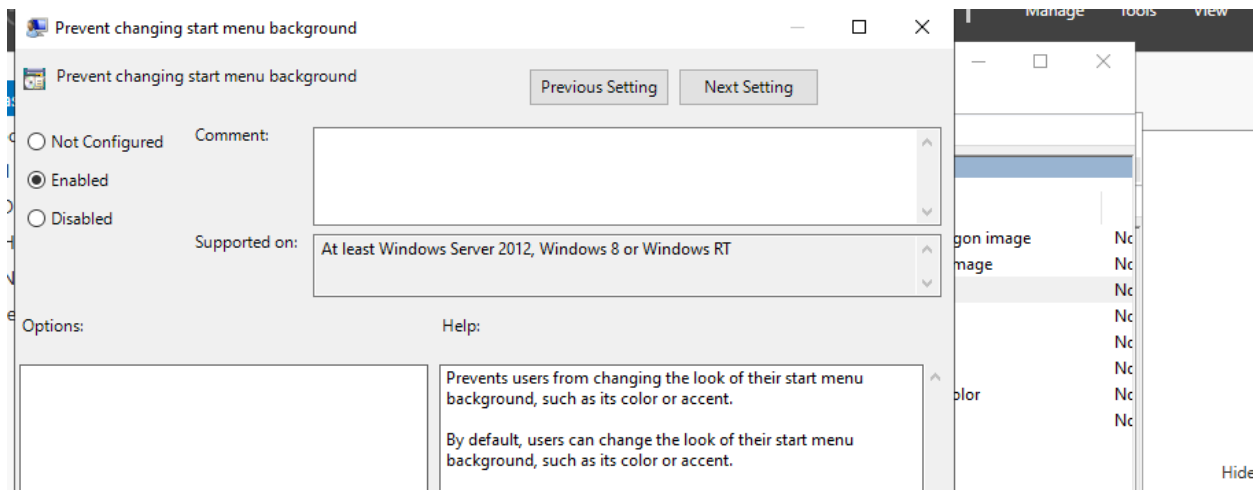


On accède au groupe policies management editor ,l'outil que nous serons utilisé pour configuré les GPO qu'on veut appliquer .

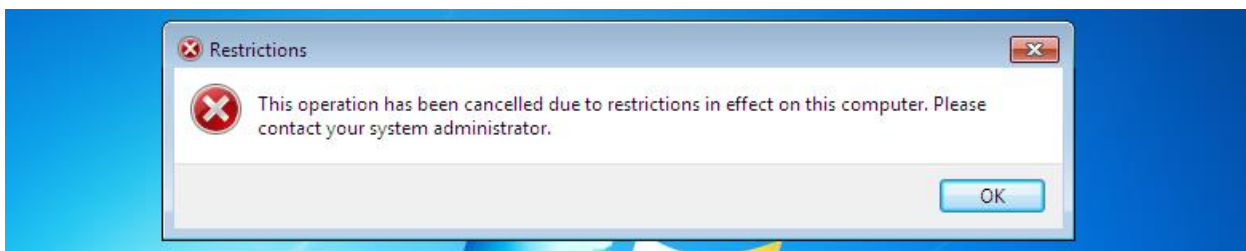
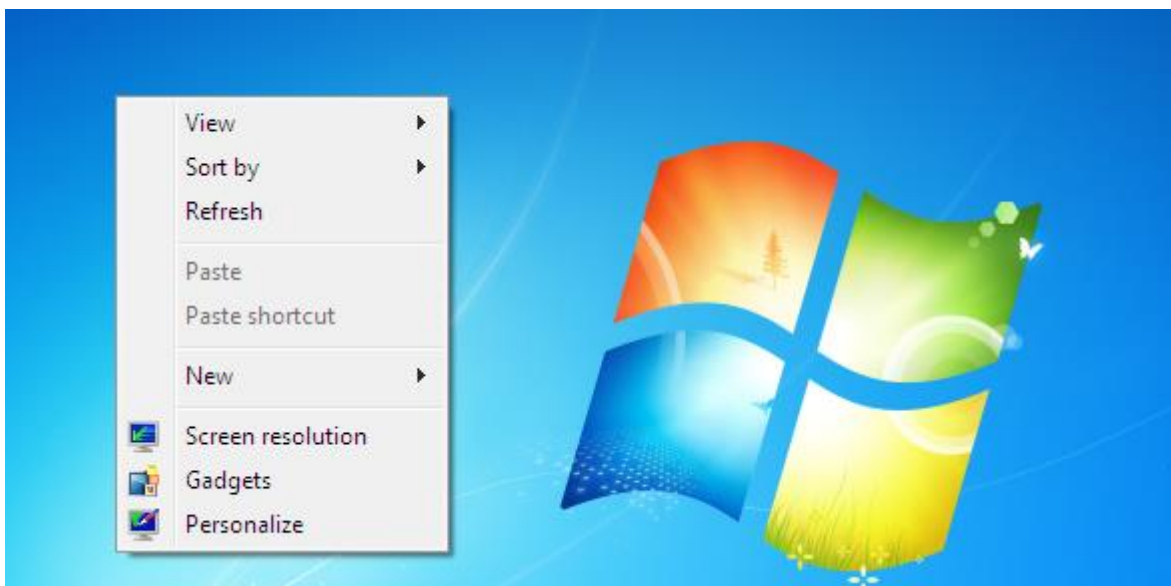


Interdiction de changer le fond d'écran du menu Démarrer.

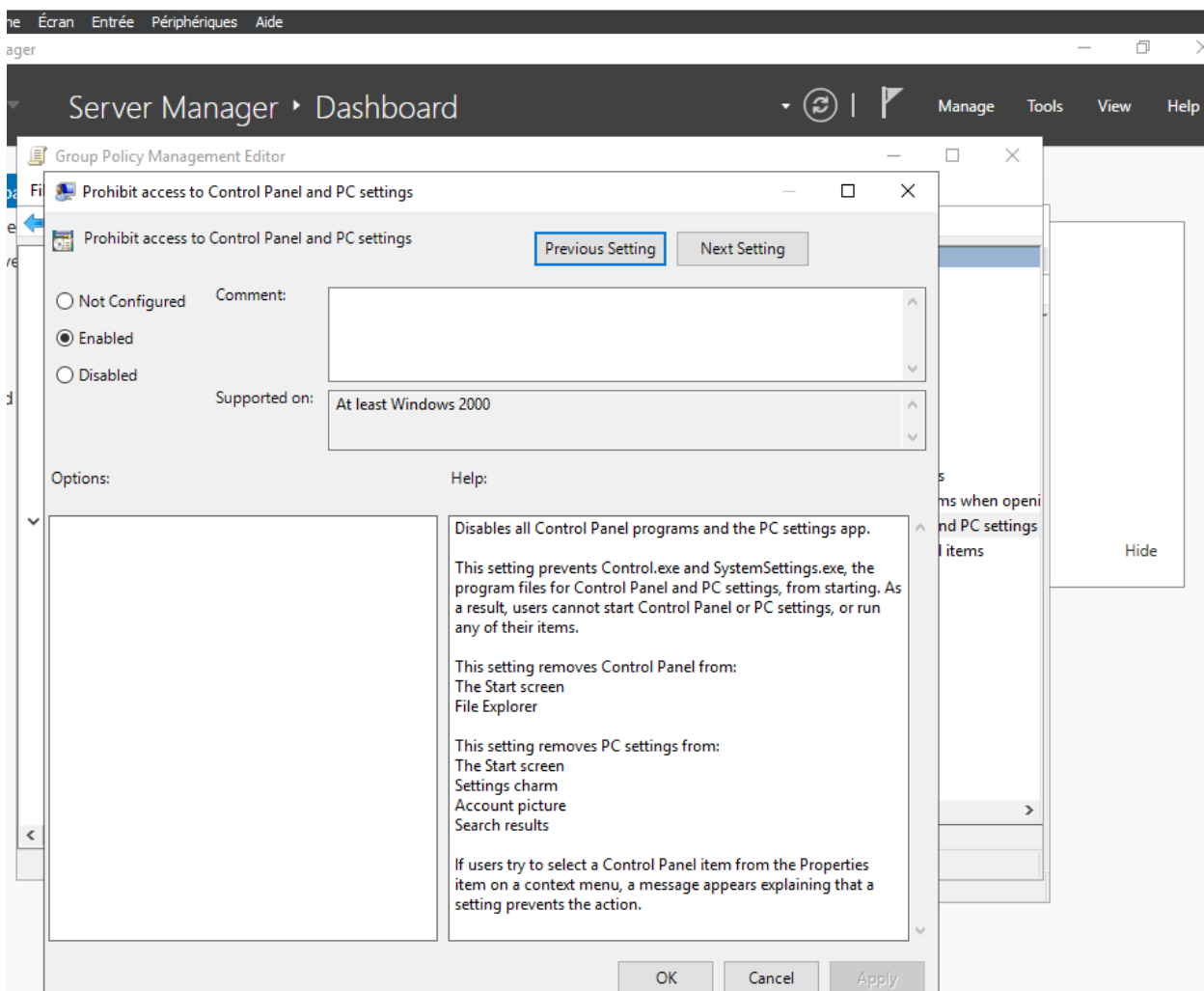
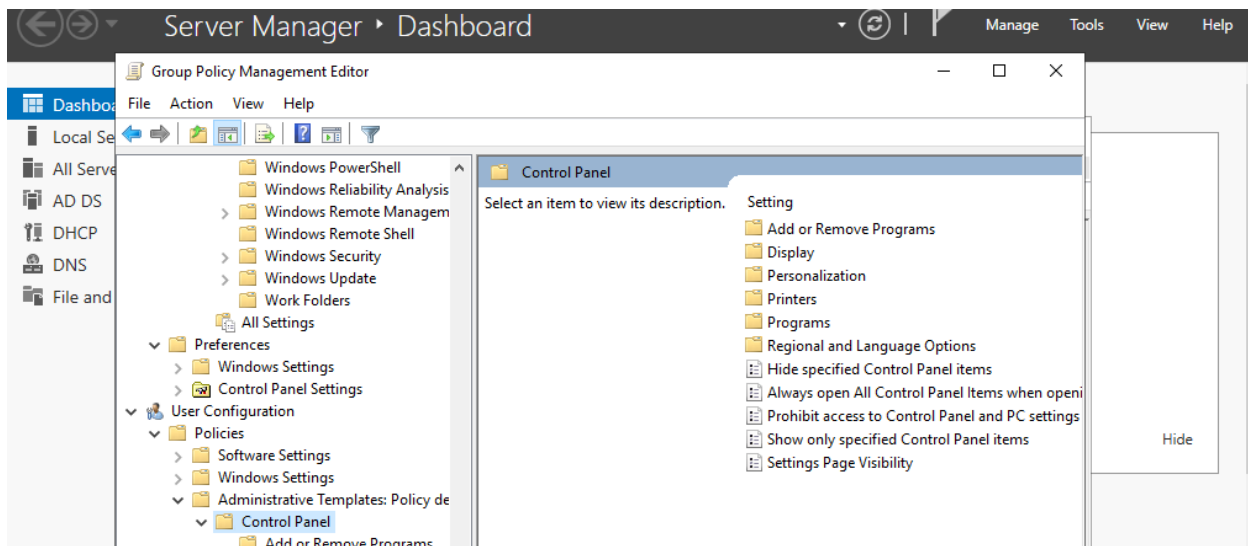




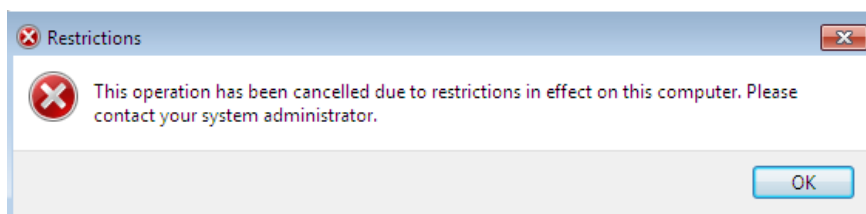
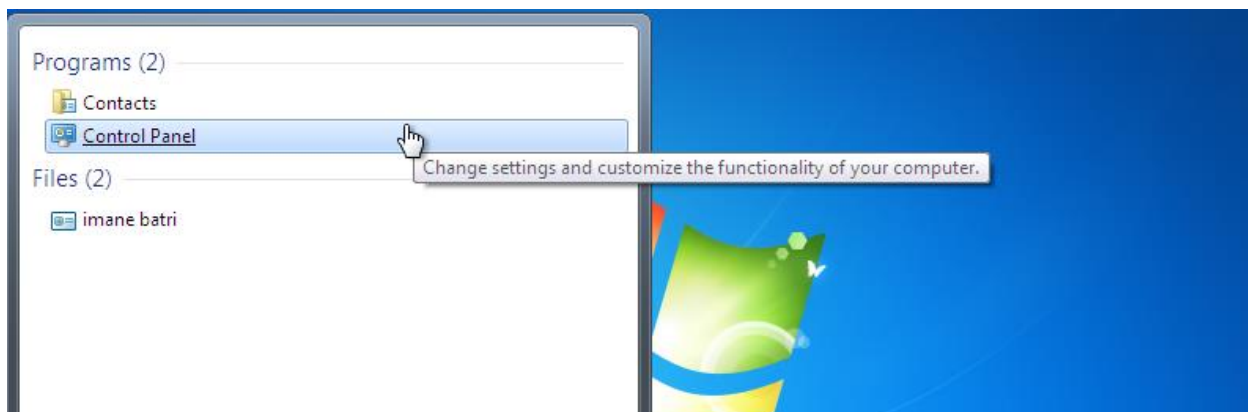
Test :



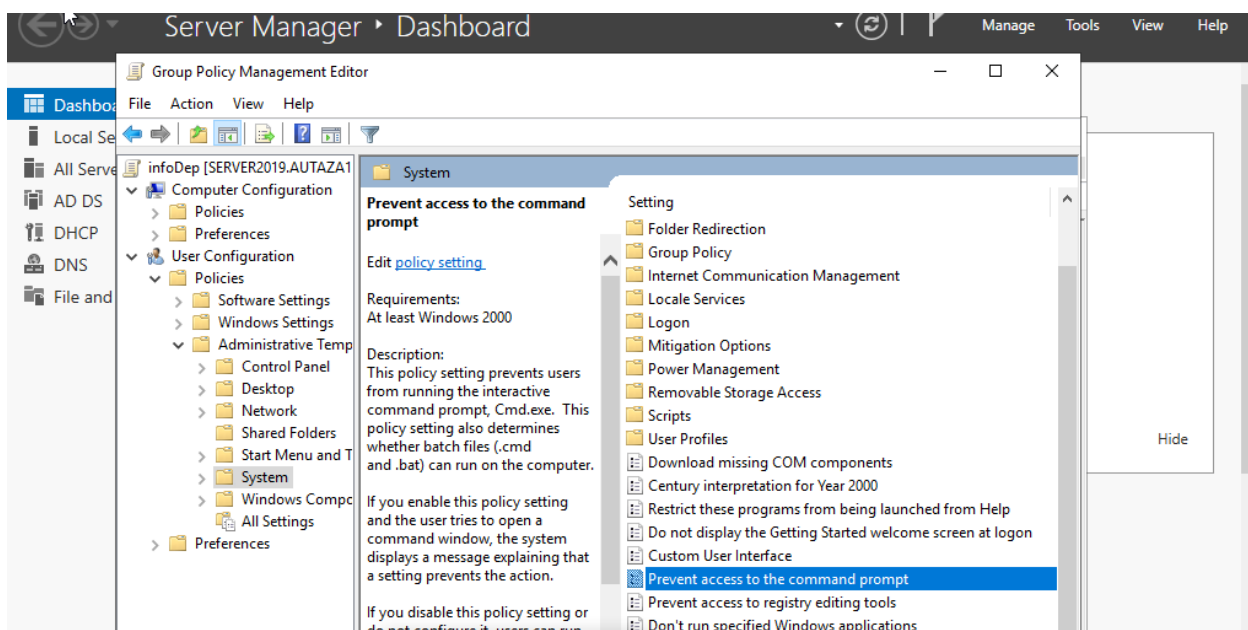
Interdiction d'accéder au Panneau de configuration.

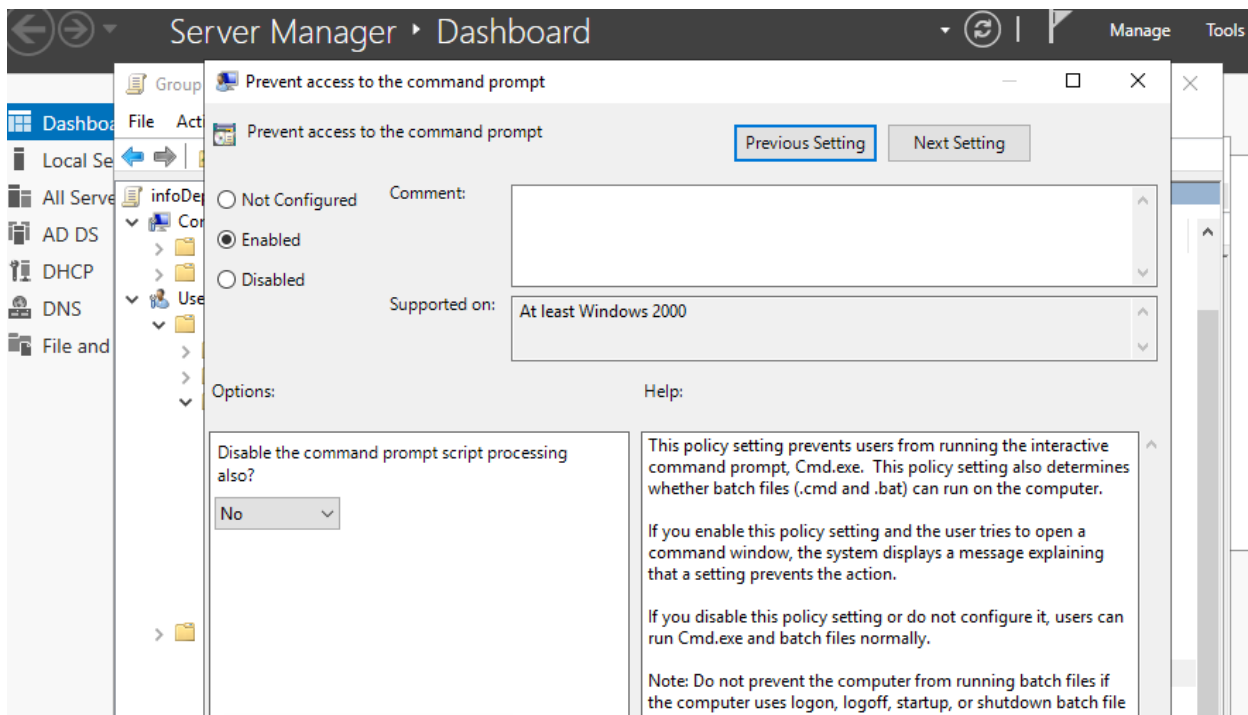


Test :

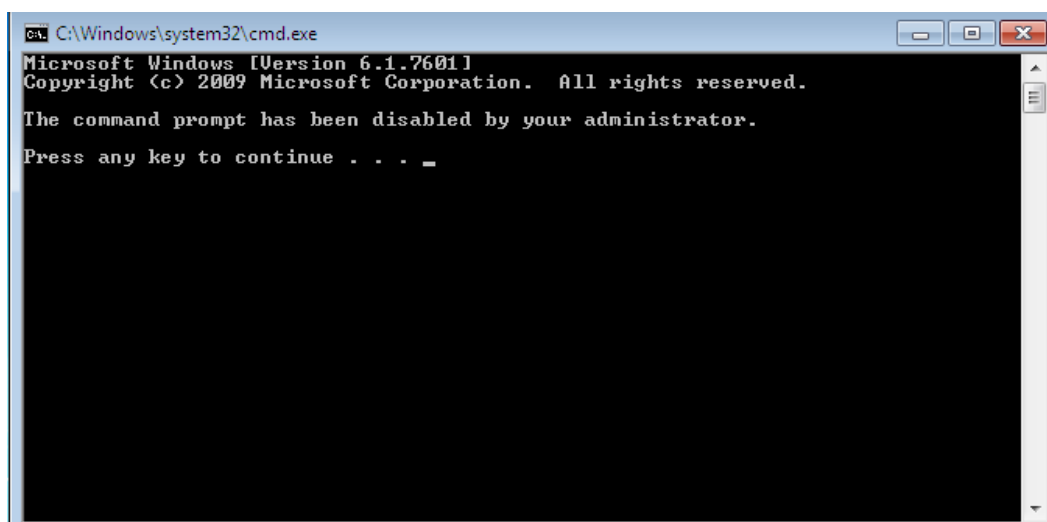
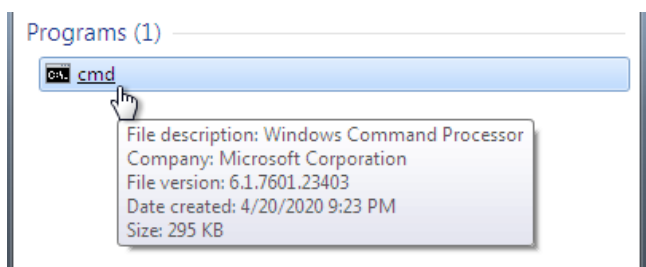


Interdiction d'accéder à l'invite de commandes (cmd).

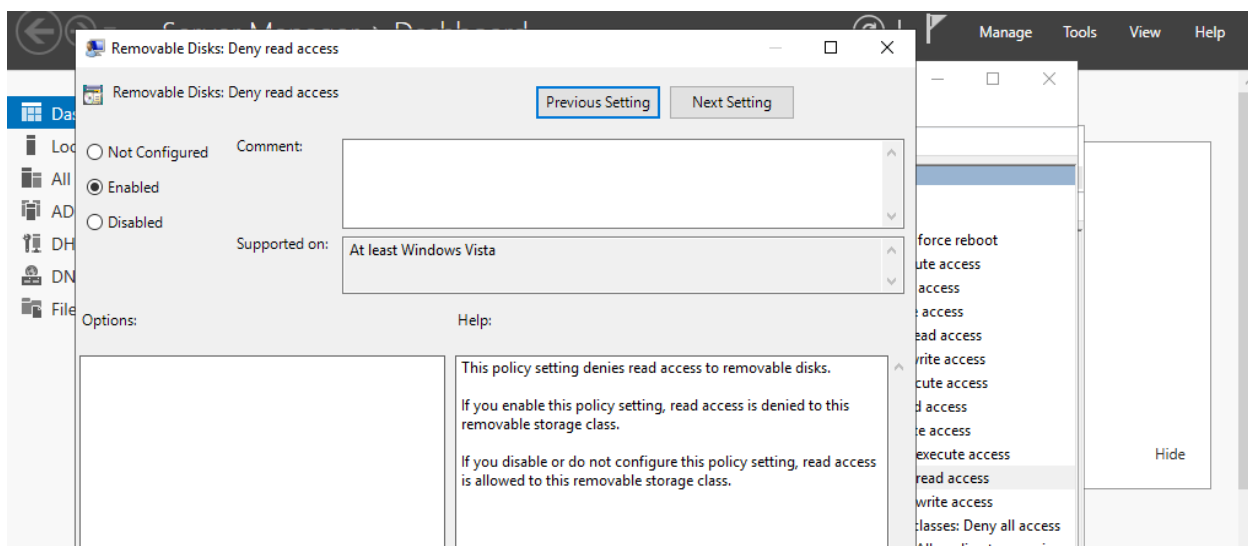
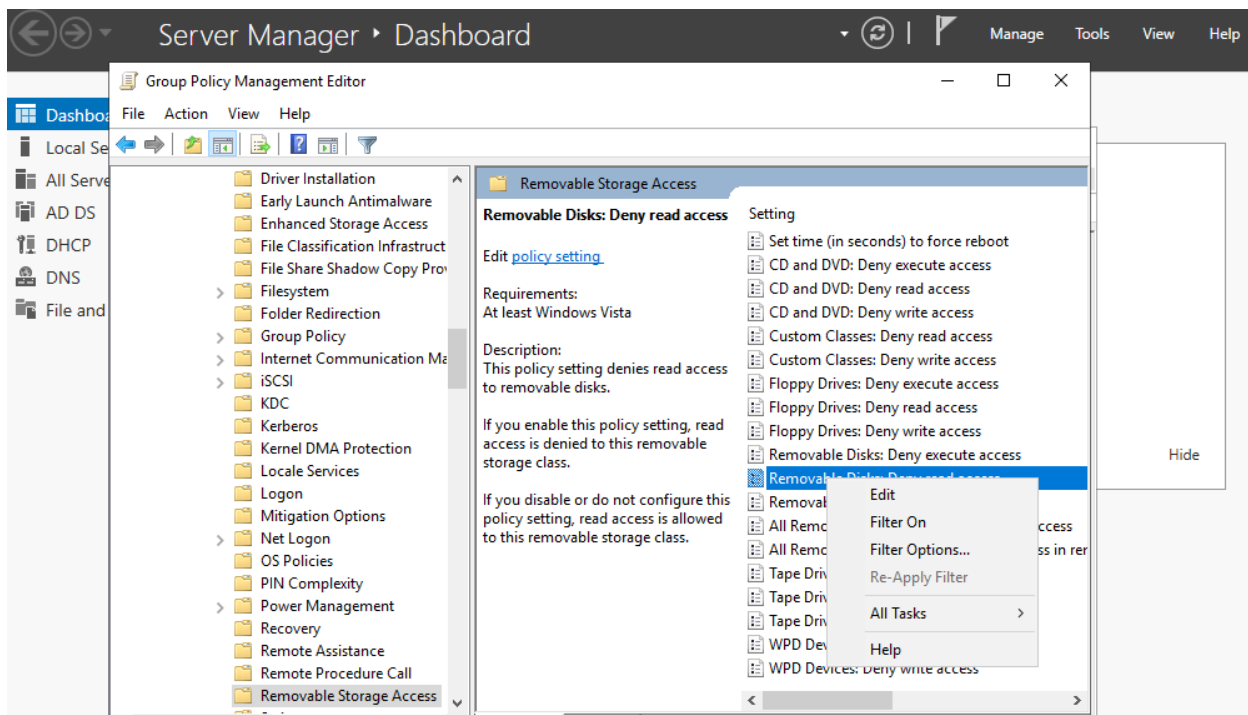




Test :



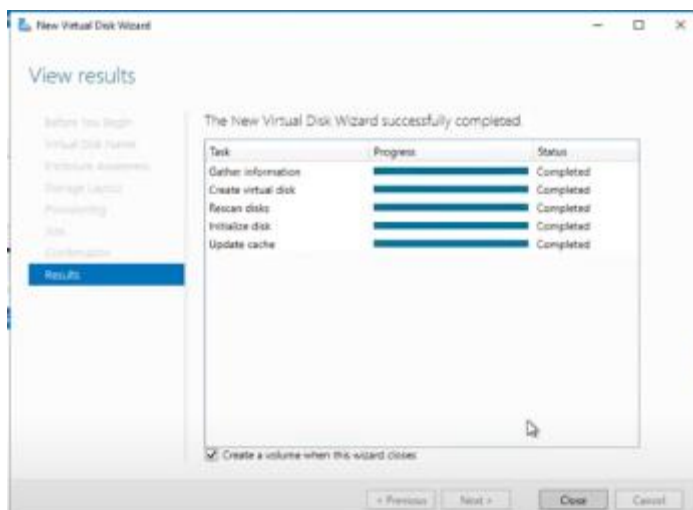
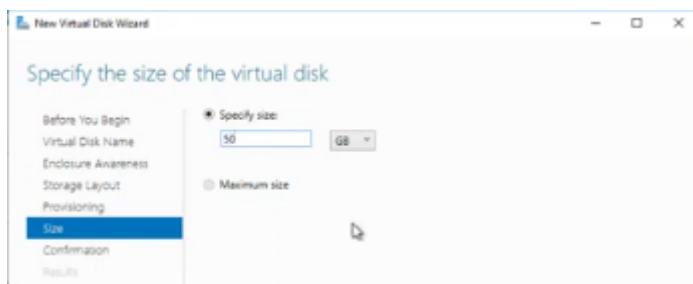
Interdiction de lire les clés USB insérées :



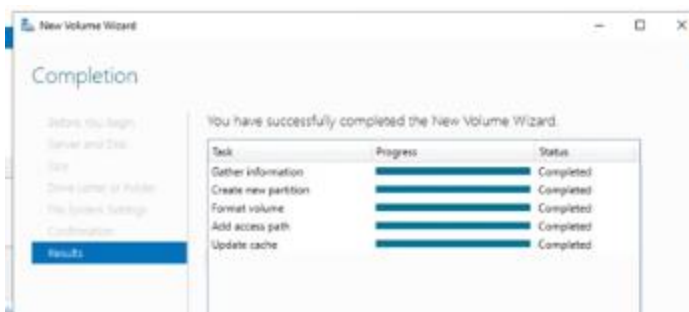
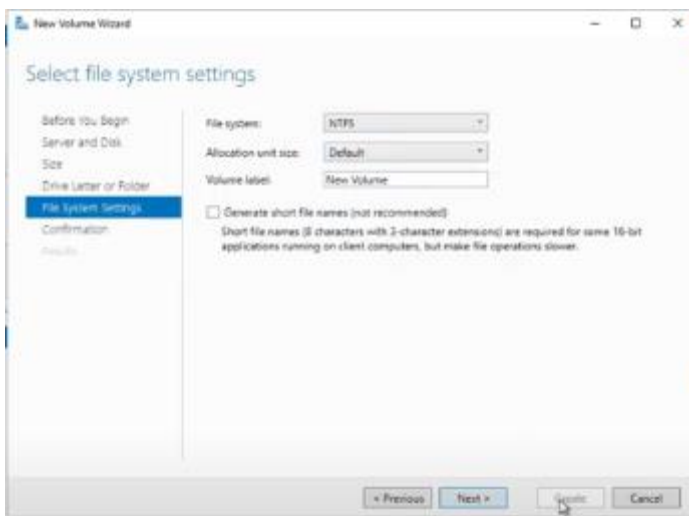
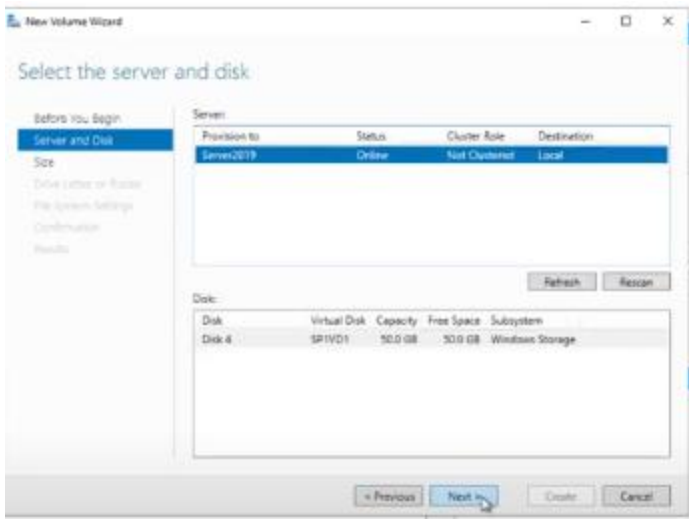
7. Configuration Storage Pool

Afin de configurer le Storage pool dans notre machine en doit premièrement ajouter des disques virtuels dans cette dernière :

Après l'ajoute des disques virtuelle, en accède au l'onglet servers, puis storagePool, en click sur task et en choisie new StoragePool, et en choisie par la suite le nom de notre nouveau disque virtuelle, ainsi que la technique de stockage, dans mon cas j'ai donné le nom StoragePool et le type de Stockage Mirror :



Après la fin de cette étape une nouvelle fenêtre sera afficher pour créer un nouveau volume, en spécifier le nom de notre nouveau volume et le system de fichier qui est dans mon cas NTFS et c'est fini :



8. Configuration de File Sharing & FSRM

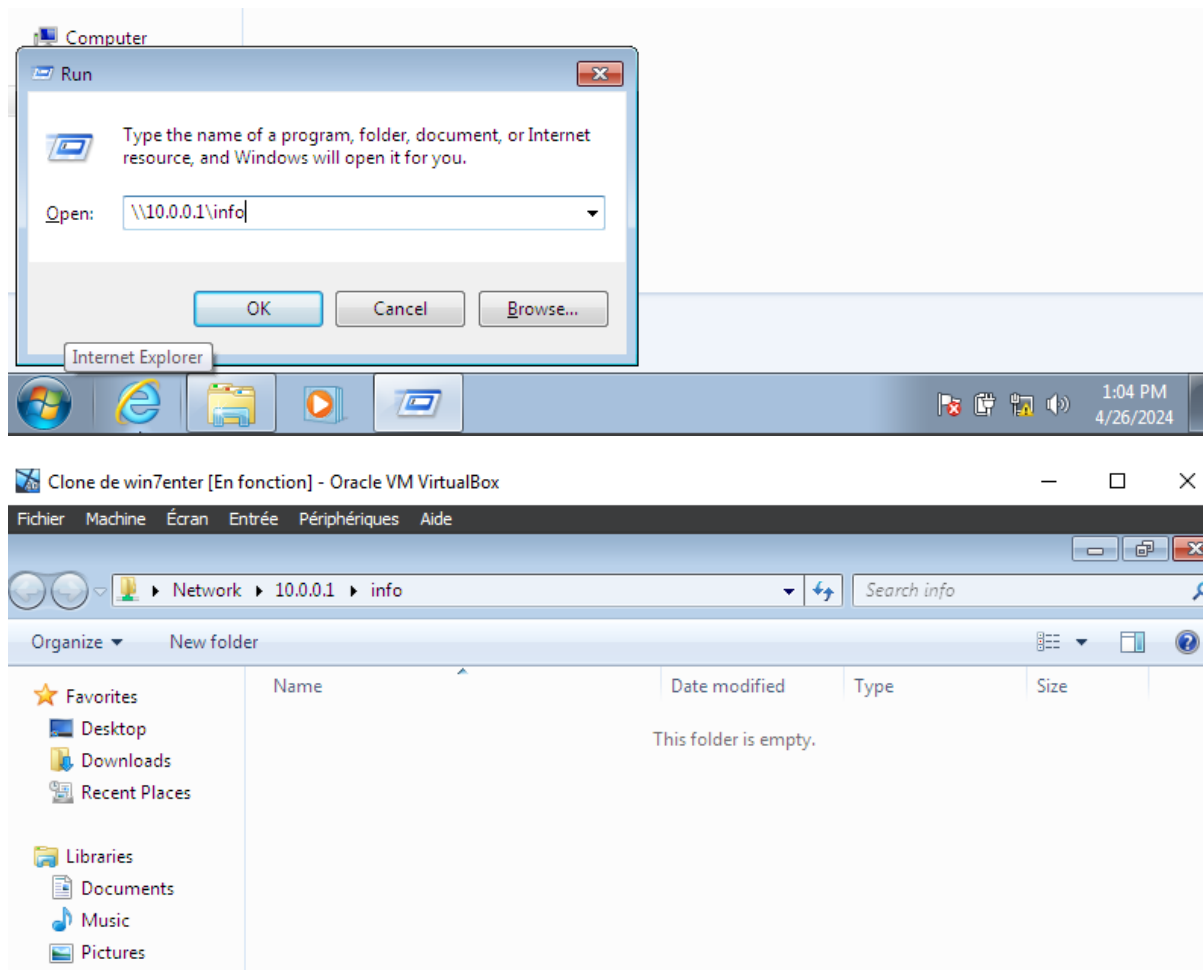
▪ File Sharing :

Pour la configuration de file sharing, en commence premièrement par la création de notre fichier ou répertoire qu'on veut partager, en pas vers l'Anglet All Servers, Share, en click sur task et new sharedFile, après en spécifier le nom que ce répertoire sera prend dans notre réseau, et en spécifier

le chemin de ce dernier et en clic sur commit, après en fait un clic droit sur le fichier et Propriétés ,puis dans la partie des droits d'accès de NTFS en ajoute notre group et le type d'accès autorisé à ce dernier .

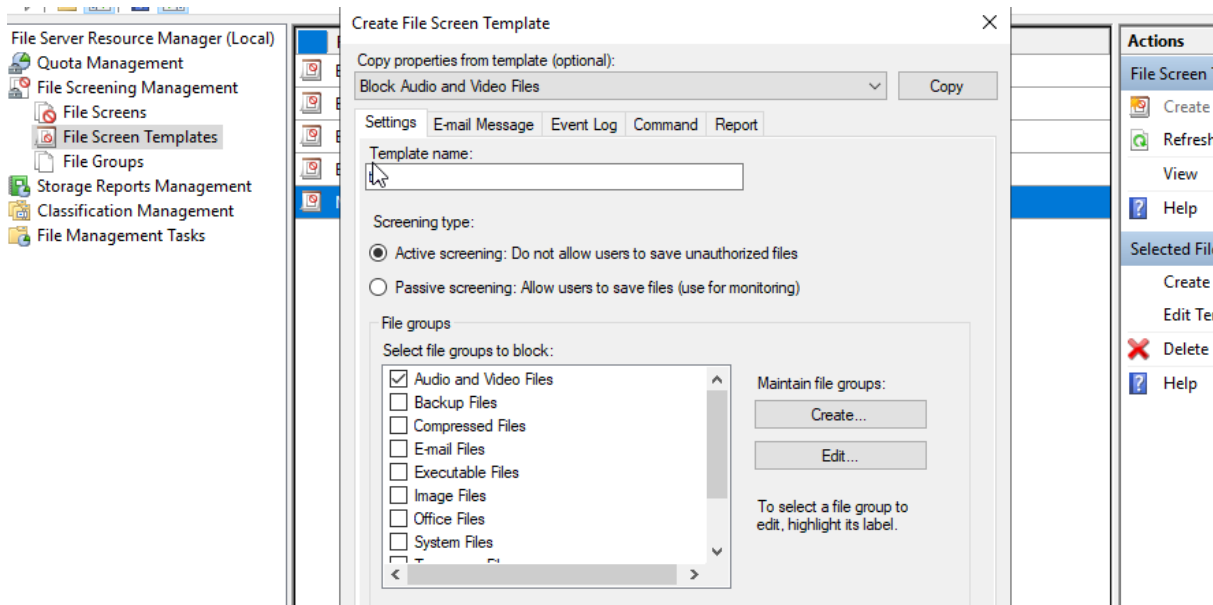
NB : Dans le cas des droit d'accès d'un fichier dans un réseau en trouve qu'il y a deux types des droit d'accès le premier et les droit de Share et le deuxième et le NTFS, si on donne a un group le droit de full Control pout le Share mais uniquement la lecture dans le cas des droit NTFS, ce dernier ne sera obtenir que le droit de lecture (NTFS).

Voici le test pour un client dans le groupe :

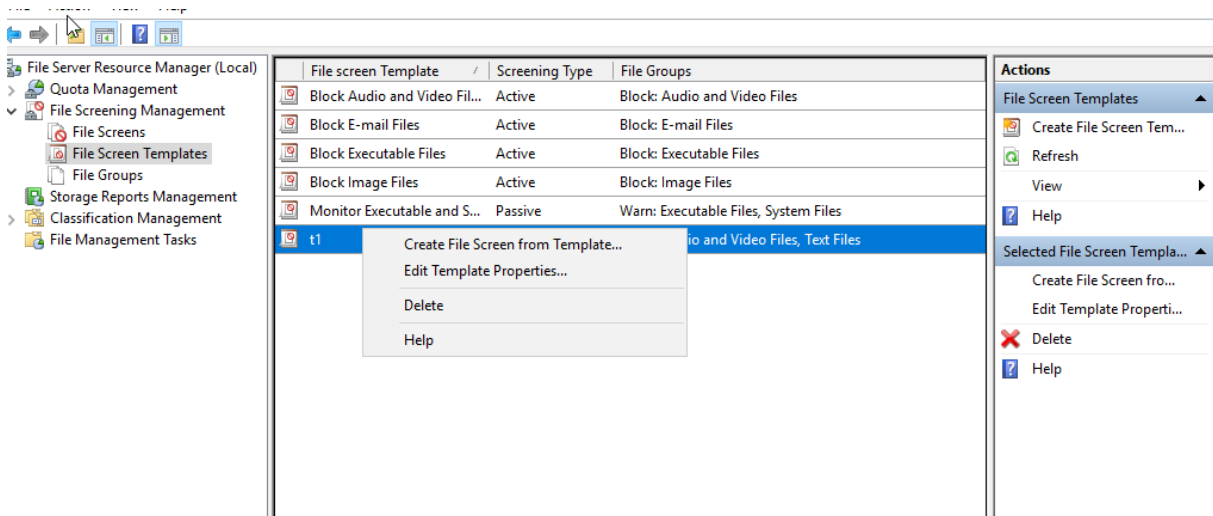
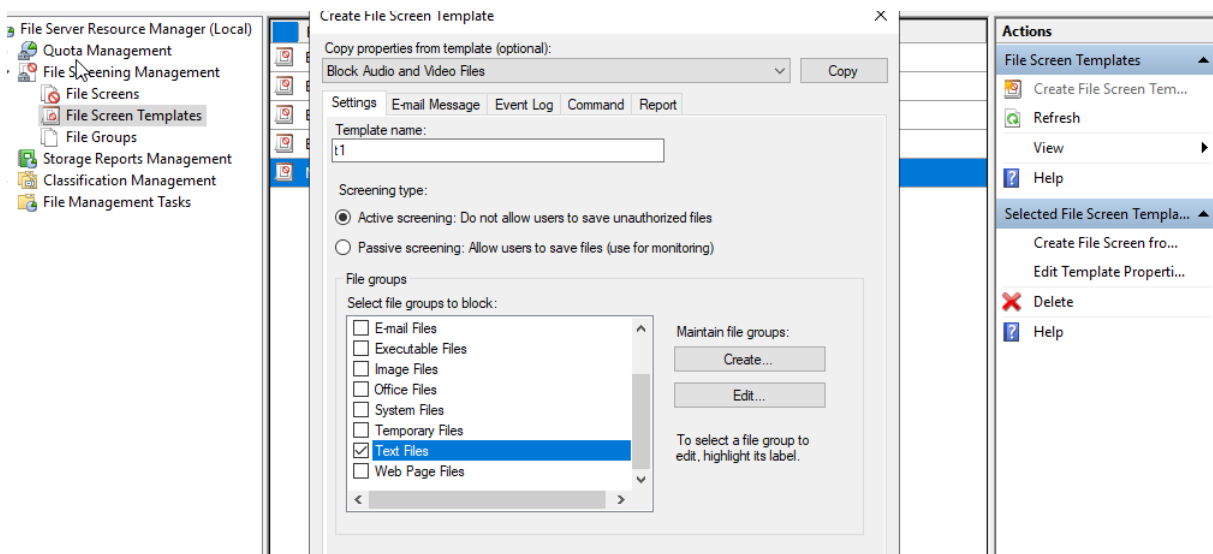


▪ FSRM :

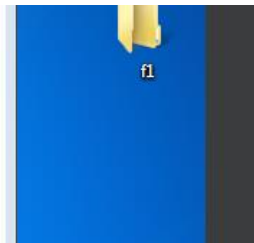
Maintenant en veut empêcher l'ajout d'un fichier .MP3 dans notre dossier partager, pour cela en installe FSRM (File Server resource manager) avec les management Tools et après l'installation en clic sur task ans la partie quota, et en choisie configure quota, puis en crée une nouvelle file screen Template, en donne à cet dernier un nom et en choisie les type des fichiers qu'on veut bloquer dans notre ca audio et vidéo files pour les .MP3 et .MP4



Par la suite en commence par la création d'une nouvelle screen d'après cette Template, dans cette screen en spécifier l'emplacement du répertoire partagé sue lequel en veut appliquer cette notion et OK.



Voici le test :

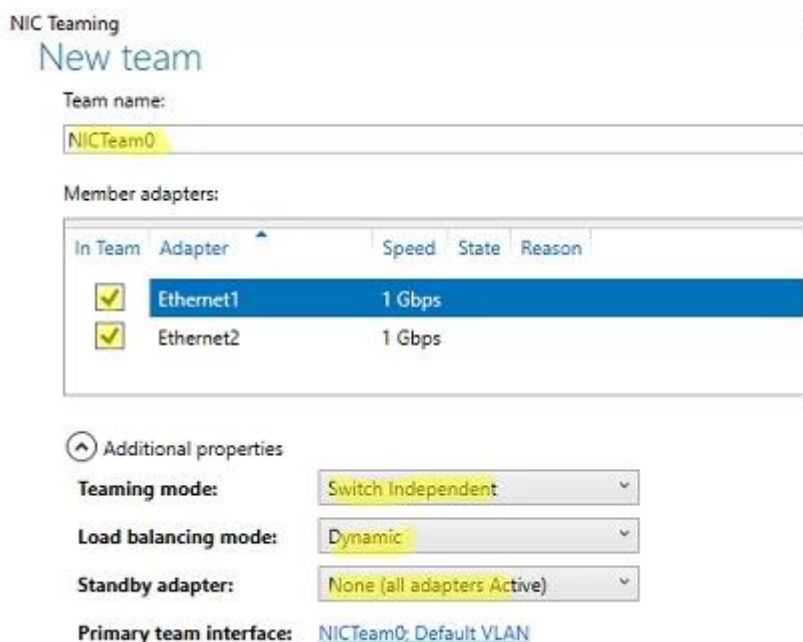


9. Configuration de Nic Teaming

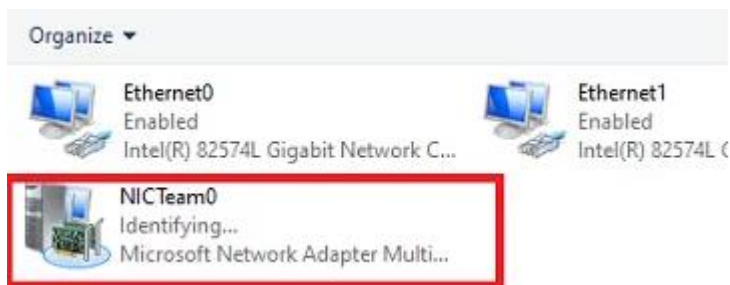
Comme déjà mentionné dans la partie théorique, le Nic-teaming est fait de regrouper les cartes réseau d'une machine, afin qu'elles fonctionnent comme une seule carte avec la capacité des autres. Ainsi, il nous donne une accélération par rapport au débit ainsi qu'une tolérance en cas de panne d'un des équipements.

Afin d'appliquer le Nic teaming, on doit premièrement ajouter des cartes réseau dans notre machine et les mettre en réseau interne:

Après cette étape, on démarre notre machine, on spécifie les cartes Ethernet à ajouter dans notre team ainsi que les autres paramètres supplémentaires.



Maintenant nous serons donnés l'adresse IP de notre team qui est 10.0.0.1/24 ainsi que l'adresse de serveur DNS.



VI. Partie Pratique B (PowerShell)

Dans cette partie, nous utiliserons uniquement le Shell Scripting pour réaliser toute la configuration que nous avons faite avec l'interface graphique, pour un serveur Windows. Il y a toujours deux distributions : une avec une interface graphique et une autre en ligne de commande (CLI). L'avantage de l'utilisation de la CLI est que c'est plus sécurisé puisqu'il n'y a pas de programmes par défaut qui sont en train de s'exécuter.

Dans mon cas, puisque je ne possède pas d'une image ISO d'un serveur Windows CLI, je vais utiliser uniquement une autre machine virtuelle Windows Server 2019 avec une interface graphique (GUI). Cependant, pour la configuration, je vais me reposer uniquement sur l'outil PowerShell.

PowerShell est un framework de gestion de configuration et d'automatisation des tâches développé par Microsoft. Il se compose d'une interface en ligne de commande (CLI) et d'un langage de script intégré, conçu principalement pour l'administration système et la gestion de réseaux. PowerShell permet aux administrateurs de gérer à la fois les systèmes Windows et d'autres plateformes, grâce à des cmdlets (command-lets) qui exécutent des fonctions spécifiques. Il offre également des fonctionnalités avancées de scripting, de manipulation d'objets, et de gestion de fichiers, rendant les tâches administratives plus efficaces et automatisées.

1. Création de Domaine

Pour créer le model en import le Module Server Manager, puis en télécharge AD DS avec Management Tools :

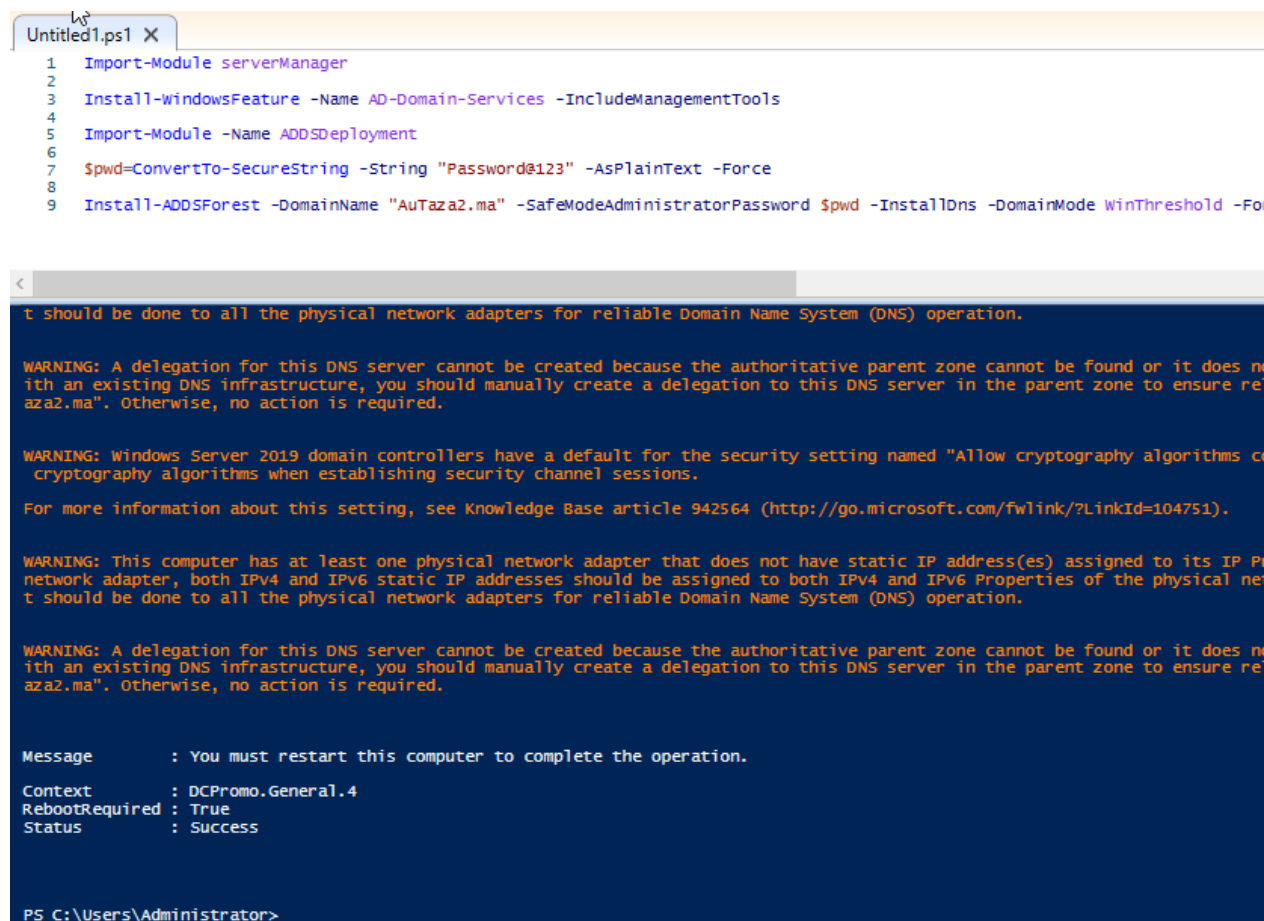
```
1 Import-Module serverManager
2
3 Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```



```
PS C:\Users\Administrator> C:\Users\Administrator\Desktop\Untitled1.ps1
PS C:\Users\Administrator> C:\Users\Administrator\Desktop\Untitled1.ps1
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Group P...

L'étape suivante consiste à créer une nouvelle forêt. Pour cela, nous importons le module ADDSDeployment, définissons un mot de passe et utilisons la commande Install-ADDSForest. Pour les options, nous donnons le nom de notre domaine, le mot de passe de récupération ainsi que la configuration automatique de DNS, et déterminons la version acceptée en cas d'ajout d'un autre contrôleur de domaine (DC) dans le même domaine. La création de la forêt nécessite un redémarrage de la machine. J'ai désactivé le redémarrage automatique pour que je puisse le faire manuellement.



The image shows a PowerShell script in a text editor and its execution output in a terminal window.

Script (Untitled1.ps1):

```
1 Import-Module serverManager
2
3 Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
4
5 Import-Module -Name ADDSDeployment
6
7 $pwd=ConvertTo-SecureString -String "Password@123" -AsPlainText -Force
8
9 Install-ADDSForest -DomainName "AuTaza2.ma" -SafeModeAdministratorPassword $pwd -InstallDns -DomainMode WinThreshold -Fo
```

Output:

```
t should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not exist with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable operation for "AuTaza2.ma". Otherwise, no action is required.

WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms to be used when establishing security channel sessions."

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

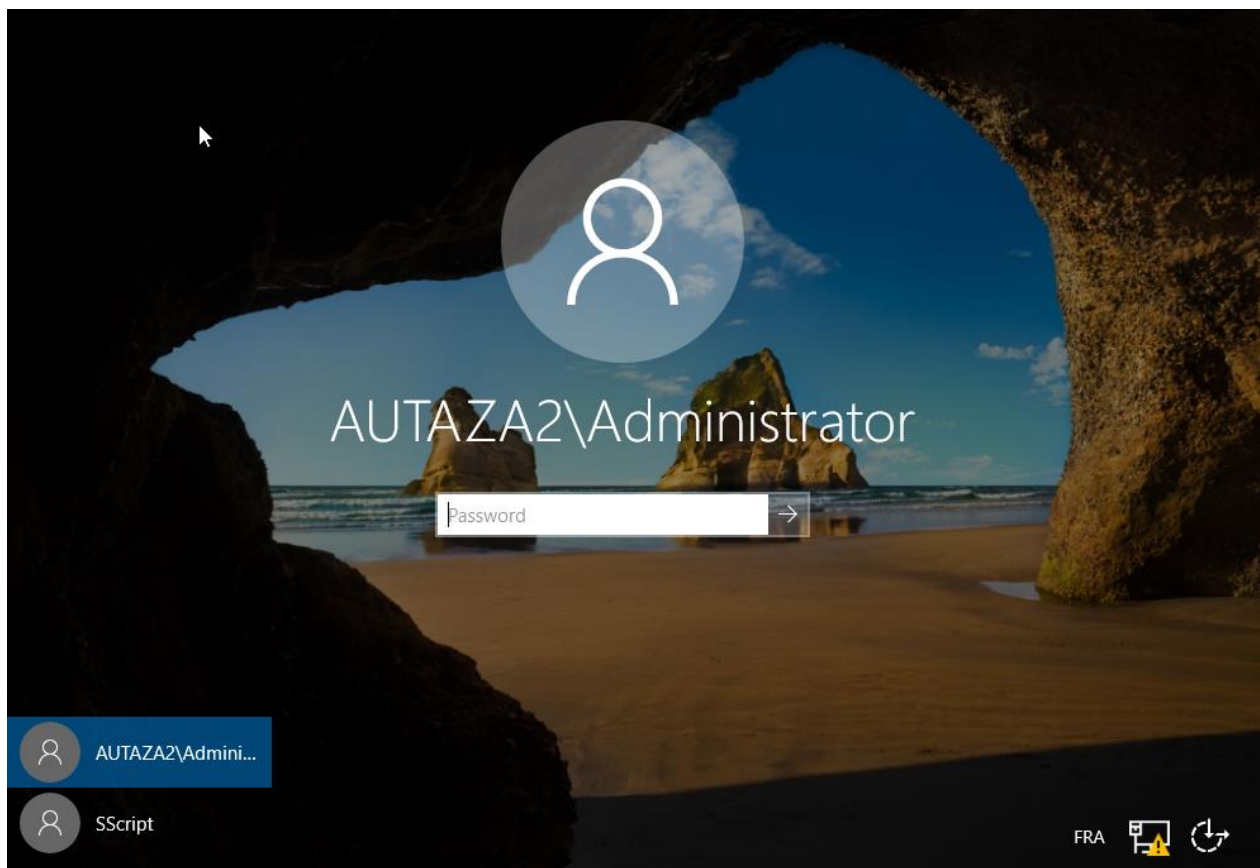
WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. For reliable DNS operation, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. For reliable DNS operation, it should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not exist with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable operation for "AuTaza2.ma". Otherwise, no action is required.

Message      : You must restart this computer to complete the operation.
Context      : DCPromo.General.4
RebootRequired : True
Status       : Success

PS C:\Users\Administrator>
```

Après le redémarrage, on remarque que la création de notre domaine est faite par succès, puisqu'on a le nom de notre domaine suivi par le nom d'utilisateur (Dans ce cas Administrateur) :



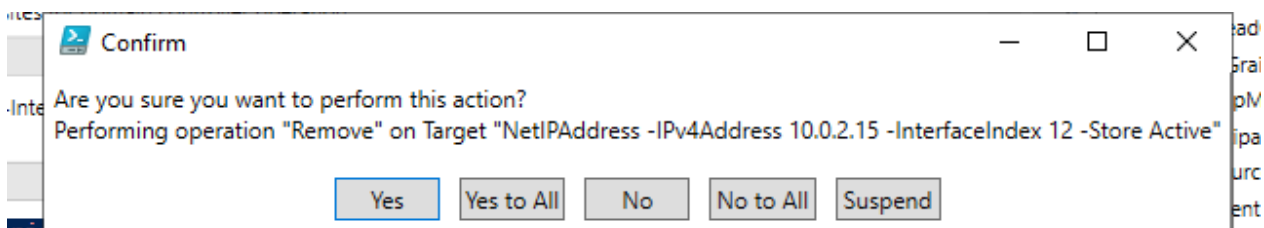
L'étape suivante est de donner notre serveur une adresse IP d'une manière statique, pour cela on demande des infos par rapport à l'interface qu'on a dans ce serveur :

```
Untitled1.ps1 X
10
11 Get-NetIPAddress

RequestedState : 12
TimeOfLastStateChange :
TransitioningToState : 12
CreationClassName :
SystemCreationClassName :
SystemName :
NameFormat :
OtherTypeDescription :
ProtocolIFType : 4096
ProtocolType :
Address :
AddressOrigin : 0
AddressType :
IPv4Address : 10.0.2.15
IPv6Address :
IPVersionSupport :
PrefixLength : 24
SubnetMask :
AddressFamily : IPv4
AddressState : Preferred
InterfaceAlias : Ethernet
InterfaceIndex : 12
IPAddress : 10.0.2.15
PreferredLifetime : 23:42:45
PrefixOrigin : Dhcp
SkipAsSource : False
Store : ActiveStore
SuffixOrigin : Dhcp
Type : Unicast
ValidLifetime : 23:42:45
PSComputerName :
ifIndex : 12
```

Pour faire cela en doit supprimé l'ancien adresse et donner une autre nouvelle (mon réseau est 10.0.0.0/24) :

Le nom (l'alias) de l'interface est Ethernet, alors pour la suppression de l'ancienne adresse en utilise Remove-IPAddress et en montions l'alias de l'interface ainsi que l'ancien adresse IP a supprimé (une boîte de message sera afficher pour valider l'action de suppression)



```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "10.0.0.1" -PrefixLength 24
```

```

PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore
|
IPAddress         : 10.0.0.1
InterfaceIndex    : 12
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore

```

et en attribue à l'interface la nouvelle adresse (10.0.0.1) en mentionne aussi le masque qui est /24 avec l'option –PrefixLength.

2. Création des Unités Organisationnelles, Utilisateurs et Groupes

La tâche de création des utilisateurs et group avec le Scripting et devenue plus facile puisqu'on peut utiliser des boucle sur des tableau qui contiennent les noms des utilisateurs ainsi que les group et les unités organisationnelles ,dans mon cas j'ai utilisé un tableau dans lequel j'ai les utilisateur en trois départements principales qui sont successivement Finance, RH et Urbanisme , j'ai utilisé une boucle imbriquée afin de créer à la fois les OUs et à l'intérieur de chacune des OU ,les Users et les groupes ,et au même temps ajouter chaque user à son group spécifier.

```

49 $pwdUsers=ConvertTo-SecureString -String "P@$w0rd" -AsPlainText -Force
50
51 $AllUsers=@(("AhmediAhmedi", "Ahmedi", "Ahmedi", "AhmediAhmedi@AuTaza2.ma", "Ahmedi Ahmedi"),
52             @("ImanIman", "Iman", "Iman", "ImanIman@AuTaza2.ma", "Iman Iman"),
53             @("KarimaKarima", "Karima", "Karima", "KarimaKarima@AuTaza2.ma", "Karima Karima")),
54
55 @(("AhmedoAhmedo", "Ahmedo", "Ahmedo", "AhmedoAhmedo@AuTaza2.ma", "Ahmedo Ahmedo"),
56   @("SaidSaid", "Said", "Said", "SaidSaid@AuTaza2.ma", "Said Said"),
57   @("KarimKarimi", "Karim", "Karimi", "KarimKarimi@AuTaza2.ma", "Karimi Karimi")),
58
59 @(("AhmedAhmedo", "Ahmed", "Ahmedo", "AhmedAhmedo@AuTaza2.ma", "Ahmed Ahmedo"),
60   @("SaidaSaid", "Saida", "Said", "SaidaSaid@AuTaza2.ma", "Saida Said"),
61   @("KarimaKarimi", "Karima", "Karimi", "KarimaKarimi@AuTaza2.ma", "Karima Karimi"))
62 )
63
64
65 $Ous=@("Finance", "Urbanisme", "RH")
66 $Groups=@("Finance1", "Urbanisme1", "RH1")
67
68
69 $i=0
70 Foreach ($OU in $Ous){
71     New-ADOrganizationalUnit -Name $OU
72     New-ADGroup -Name $Groups[$i] -GroupScope DomainLocal -GroupCategory Security -Path "OU=$OU,DC=AuTaza2,DC=ma"
73     Foreach ($Usr in $AllUsers[$i]){
74         {
75             New-ADUser -Name $Usr[4] -GivenName $Usr[1] -Surname $Usr[2] -SamAccountName $Usr[0] -UserPrincipalName $Usr[3] | -Accou
76             ADD-ADGroupMember -Identity $Groups[$i] -Members $Usr[0]
77         }
78     }
79     $i++
80 }

```

J'ai ajouté une autre boucle qui sert à désactiver la protection de Accident Delete pour ne pas rencontrer un erreur en cas de suppression d'un Object AD DS.

```
$Sou= Get-ADOrganizationalUnit -Filter *
foreach ($p in $Sou){
$sp | Set-ADObject -ProtectedFromAccidentalDeletion $false
}
```

Pour visualisé le résultat ,en utilise Get-ADObject -Filter * -SearchBase "OU=NomDeOU,DC=NomDeDomaine,DC=NomDeDomaine" ,pour afficher tous les Ous ainsi que tous les AD objets créé à l'intérieur de cette dernière ,en peut bien-sûr utilisé une boucle sur les noms des OUs qu'on a obtenues avec 'Get-ADOrganisationalUnit'-Filter * :

```
232
233 Get-ADOrganizationalUnit -Filter *
234
235
236
237
```

```
Country :
DistinguishedName : OU=Finance,DC=AuTaza2,DC=ma
LinkedGroupPolicyObjects : {cn={1EE0BC4E-7F26-4F41-A1AF-1BF726670162},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={E1542645-3DFD-45C2-8F21-57FD47EC5873},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={1A6BA6AD-E486-4AEF-94BC-EF17275C5245},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={86104C87-F983-4CE1-9B5C-430E2D06AE55},cn=policies,cn=system,DC=AuTaza2,DC=ma}
ManagedBy :
Name : Finance
ObjectClass : organizationalUnit
ObjectGUID : 9409baba-8e7a-4ea5-a615-0c93f67f10ff
PostalCode :
State :
StreetAddress :

City :
Country :
DistinguishedName : OU=Urbanisme,DC=AuTaza2,DC=ma
LinkedGroupPolicyObjects : {cn={1EE0BC4E-7F26-4F41-A1AF-1BF726670162},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={E1542645-3DFD-45C2-8F21-57FD47EC5873},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={1A6BA6AD-E486-4AEF-94BC-EF17275C5245},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={86104C87-F983-4CE1-9B5C-430E2D06AE55},cn=policies,cn=system,DC=AuTaza2,DC=ma}
ManagedBy :
Name : Urbanisme
ObjectClass : organizationalUnit
ObjectGUID : e1e2b6cd-54e6-49ac-a783-3f2a00ecb887
PostalCode :
State :
StreetAddress :

City :
Country :
DistinguishedName : OU=RH,DC=AuTaza2,DC=ma
```

```
City :
Country :
DistinguishedName : OU=RH,DC=AuTaza2,DC=ma
LinkedGroupPolicyObjects : {cn={1EE0BC4E-7F26-4F41-A1AF-1BF726670162},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={E1542645-3DFD-45C2-8F21-57FD47EC5873},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={1A6BA6AD-E486-4AEF-94BC-EF17275C5245},cn=policies,cn=system,DC=AuTaza2,DC=ma, cn={86104C87-F983-4CE1-9B5C-430E2D06AE55},cn=policies,cn=system,DC=AuTaza2,DC=ma}
ManagedBy :
Name : RH
ObjectClass : organizationalUnit
ObjectGUID : f1cbb915-e68e-4127-960e-80dbce040a1d
PostalCode :
State :
StreetAddress :
```

Et pour afficher la liste des users a l'intérieur des group en utilise une boucle :

```
$Grps=@("Finance1","Urbanisme1","RH1")
foreach ($Grp in $Grps)
```



```
{
Get-ADGroupMember -Identity $Grp
}
```

```
158
159 $Grps=@("Finance1","Urbanisme1","RH1")
160 foreach ($Grp in $Grps)
161 {
162     Get-ADGroupMember -Identity $Grp
163 }
164
165 New-Item -Type Directory -Path "C:\Users\Administrator\Desktop" -Name $Grp
```

```
PS C:\Users\Administrator> $Grps=@("Finance1","Urbanisme1","RH1")
foreach ($Grp in $Grps)
{
Get-ADGroupMember -Identity $Grp
}
```

```
distinguishedName : CN=Karima Karima,OU=Finance,DC=AuTaza2,DC=ma
name              : Karima Karima
objectClass       : user
objectGUID        : 7db861c9-f867-45cc-af10-ac44f1a51757
SamAccountName    : KarimaKarima
SID               : S-1-5-21-3987355723-1345502917-1439793352-1148

distinguishedName : CN=Iman Iman,OU=Finance,DC=AuTaza2,DC=ma
name              : Iman Iman
objectClass       : user
objectGUID        : c4dfbccd-00e7-4bb0-979a-c321d6fc289a
SamAccountName    : ImanIman
SID               : S-1-5-21-3987355723-1345502917-1439793352-1147

distinguishedName : CN=Ahmedi Ahmedi,OU=Finance,DC=AuTaza2,DC=ma
name              : Ahmedi Ahmedi
objectClass       : user
objectGUID        : 027bd9dc-eb5f-42d0-bc64-74906a1441fa
SamAccountName    : AhmediAhmedi
SID               : S-1-5-21-3987355723-1345502917-1439793352-1146
```

```
distinguishedName : CN=Ahmedo Ahmedo,OU=Urbanisme,DC=AuTaza2,DC=ma
name              : Ahmedo Ahmedo
objectClass       : user
objectGUID        : d0f6e36b-ab1c-4ec3-bd04-e1d68883e3a5
SamAccountName    : AhmedoAhmedo
SID               : S-1-5-21-3987355723-1345502917-1439793352-1150

distinguishedName : CN=Karima Karimi,OU=RH,DC=AuTaza2,DC=ma
name              : Karima Karimi
objectClass       : user
objectGUID        : 85a4af32-b0fa-4c57-8ac3-58bd444ed99d
SamAccountName    : KarimaKarimi
SID               : S-1-5-21-3987355723-1345502917-1439793352-1156

distinguishedName : CN=Saida Said,OU=RH,DC=AuTaza2,DC=ma
name              : Saida Said
objectClass       : user
objectGUID        : 07fd37b0-d06f-4809-ae5d-4c11ece8874c
SamAccountName    : SaidaSaid
SID               : S-1-5-21-3987355723-1345502917-1439793352-1155

distinguishedName : CN=Ahmed Ahmedo,OU=RH,DC=AuTaza2,DC=ma
name              : Ahmed Ahmedo
objectClass       : user
objectGUID        : 2de71ccf-84ce-46f2-bb33-3a5503b8a5c4
SamAccountName    : AhmedAhmedo
SID               : S-1-5-21-3987355723-1345502917-1439793352-1154
```

Maintenant en doit créer une nouvelle machine client et la mettre dans notre domaine, la machine que j'ai créé et Windows7 Professional et j'ai mettre l'interface en réseau interne.

Je dois attribuer à cette machine une nouvelle adresse IP dans le même réseau que mon DC, puisque je n'ai pas encore configuré un Serveur DHCP.

Les scripts de la distribution Windows 7 sont différent que l'un de serveur Windows Server 10, c'est pour cela pour avoir la même syntaxe il faut utiliser des versions de Windows 8 au plus mais dans mon cas j'ai utilisé uniquement Windows 7.

Premièrement et affiche es info des interfaces des machines :

```
PS C:\Users\Administrator> netsh interface ipv4 show interfaces
```

Idx	Met	MTU	State	Name
1	50	4294967295	connected	Loopback Pseudo-Interface 1
11	10	1500	connected	Local Area Connection

Le nom de l'interface est Local area Connection, maintenant en change l'adresse IP de ce dernier avec cmdlet netsh

Puis

```
netsh interface ipv4 set address name="Local Area Connection" static "10.0.0.5" "255.255.255.0"  
netsh interface ipv4 show interfaces
```

Maintenant en affiche les infos de l'interface pour vérifier :

```
DHCPEnabled : False  
IPAddress :  
DefaultIPGateway :  
DNSDomain :  
ServiceName : NdisWan  
Description : WAN Miniport (Network Monitor)  
Index : 6  
  
DHCPEnabled : False  
IPAddress : {10.0.0.5, fe80::927:e135:2fa9:f4e9}  
DefaultIPGateway :  
DNSDomain :  
ServiceName : E1G60
```

Aussi en doit configuré l'adresse de serveur DNS préféré qui est la même que l'une de notre DC :

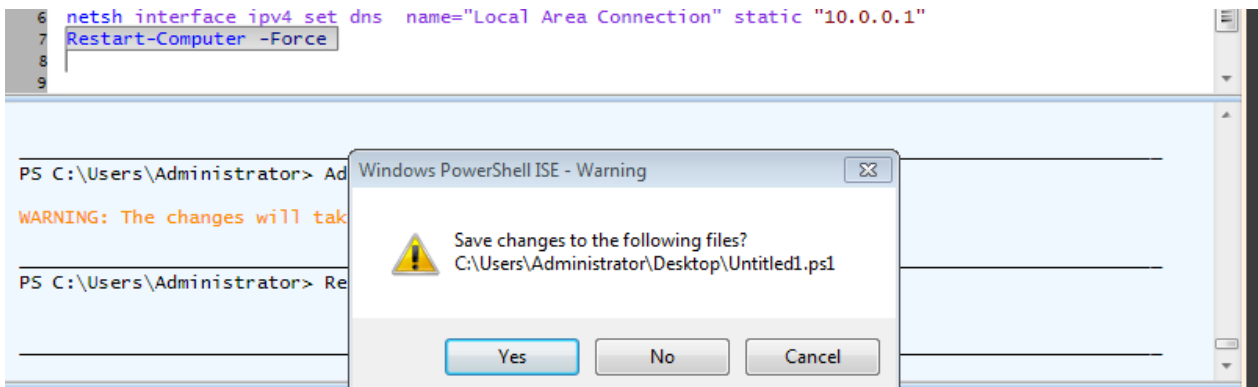
```
6 netsh interface ipv4 set dns name="Local Area Connection" static "10.0.0.1"
```

L'étape suivant et d'ajouter la machine dans notre domaine AuTaza2.ma :

```
5 Add-Computer -DomainName "AuTaza2.ma"
```

```
PS C:\Users\Administrator> Add-Computer -DomainName "AuTaza2.ma"  
  
WARNING: The changes will take effect after you restart the computer CLINT.
```

Un message Warning nous informe que les changements seront effectuer après le redémarrage de la machine, alors en faire le redémarrage :



Après le redémarrage notre machine et incluse dans le domaine, j'ai fait l'authentification pour quelques users :



3. Configuration profile itinérant

Pour la configuration de Roaming profiles, j'ai commencé par la création d'un répertoire Profiles dans lequel chaque user sera son dossier personnel, ce dossier sera partagé avec SmbShare et le droit d'accès est donné à tous les users, puis j'ai créé une boucle qui parcourt chaque utilisateur récupéré précédemment et utilise la commande Set-ADUser pour définir le chemin du profil de chaque utilisateur sur le chemin spécifié "C:\Profiles\%username%".

J'ai fait le Roaming profiles uniquement pour les users de département RH dans cet exemple.

```
New-Item -Name "Profiles" -ItemType Directory -Path "C:\"
New-SmbShare -Path C:\Profiles -Name Profiles
Grant-SmbShareAccess -Name Profiles -AccountName Everyone -AccessRight Full

$RhUsers = Get-ADUser -Filter * -SearchBase "OU=RH,DC=AuTaza2,DC=ma"
Foreach ($user in $RhUsers){
    Set-ADUser -Identity $user.SamAccountName -ProfilePath "C:\Profiles\%username%"
}
```

Voici le résultat :

```
PS C:\Users\Administrator> Get-ADUser -Filter * -SearchBase "OU=RH,DC=AuTaza2,DC=ma" -Properties ProfilePath | Select-Object SamAccountName, ProfilePath

SamAccountName ProfilePath
-----
C:\Profiles\CN=Ahmed Ahmedo,OU=RH,DC=AuTaza2,DC=ma
C:\Profiles\CN=Saïda Saïd,OU=RH,DC=AuTaza2,DC=ma
C:\Profiles\CN=Karima Karimi,OU=RH,DC=AuTaza2,DC=ma
```

4. Configuration WDS

Pour la configuration WDS, j'ai commencé premièrement par la configuration DHCP dans laquelle téléchargé DHCP avec ManagementTools et puis j'ai créé une nouvelle Scope e 10.0.0.10/24 à 10.0.0.100/24,et par la suite j'ai ajouté l'adresse de Serveur DNS et le scoop ID que dans mon cas j'ai choisi la première adresse IP dans ma Scope 10.0.0.10/24

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
Import-Module DhcpServer
Add-DhcpServerv4Scope -Name "AuTaza2Scope" -StartRange "10.0.0.10" -EndRange "10.0.0.100" -SubnetMask "255.255.255.0" -State Active
Set-DhcpServerv4OptionValue -ScopeId "10.0.0.10" -DnsServer "10.0.0.1"
```

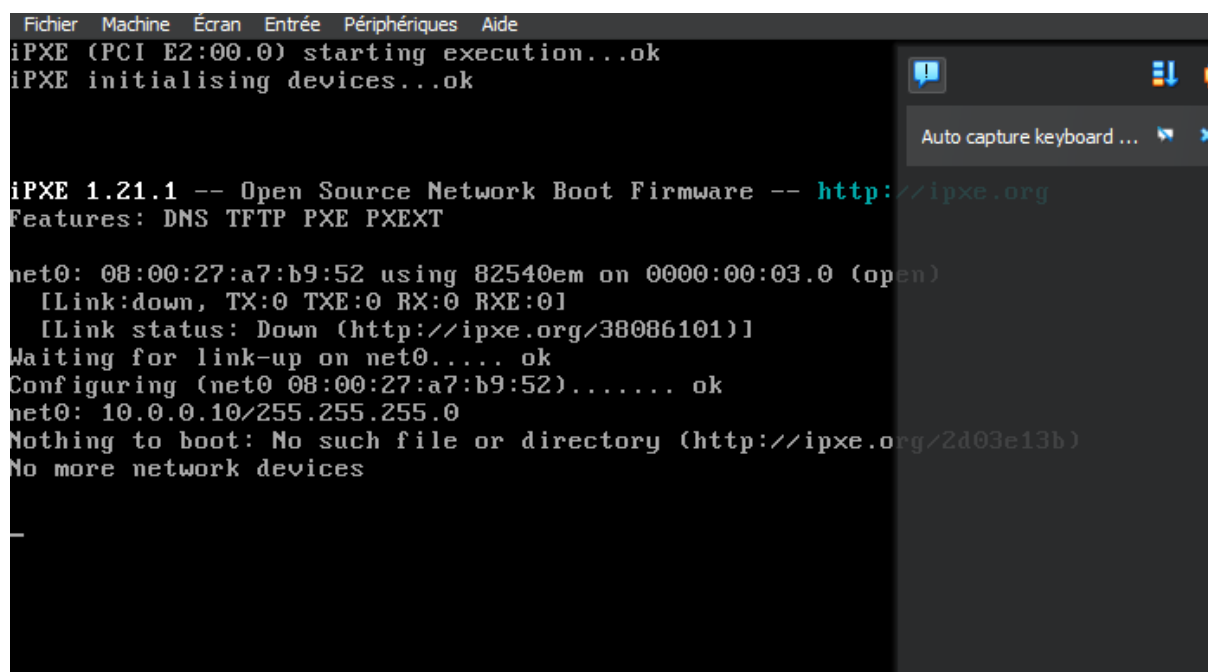
Maintenant pour la configuration WDS, j'ai commencé par l'installation de Module WDS, puis j'ai l'initialisé et créé le répertoire qui sera contenue les images des OS que je veux ajouter et le démarré avec Start-Servie -Name WDS, après ça j'ai ajouté les deux images Boot.wim et install.wim.

```
Install-WindowsFeature -Name WDS -IncludeManagementTools
Import-Module Wds
#Initialize-WdsServer -ServerName "." -RemInstPath "C:\RemoteInstall"
$res = wdsutil /initialize-server /reminst:"C:\RemoteInstall"
$res | select -Last 1
Start-Service -Name WDS

Import-WdsBootImage -Path "H:\sources\boot.wim"
Import-WdsInstallImage -Path "H:\sources\install.wim"
```

J'ai testé dans une autre machine virtuelle que j'ai créée sans déposer l'image iso et j'ai activé le BootFromNetwork :

elle a obtenue une adresse ip du plage que j'ai fournie



```
Fichier  Machine  Écran  Entrée  Périphériques  Aide
iPXE (PCI E2:00.0) starting execution...ok
iPXE initialising devices...ok

iPXE 1.21.1 -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS TFTP PXE PXEXT

net0: 08:00:27:a7:b9:52 using 82540em on 0000:00:03.0 (open)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086101)]
Waiting for link-up on net0..... ok
Configuring (net0 08:00:27:a7:b9:52)..... ok
net0: 10.0.0.10/255.255.255.0
Nothing to boot: No such file or directory (http://ipxe.org/2d03e13b)
No more network devices
```

Par la suite elle a commencée l'importation des fichiers de boot et d'installation d'après mon serveur :

```
Loading files...
```

```
IP: 10.0.0.1, File: \Boot\x64\Images\boot-(1).wim
```

5. Configuration des GPO

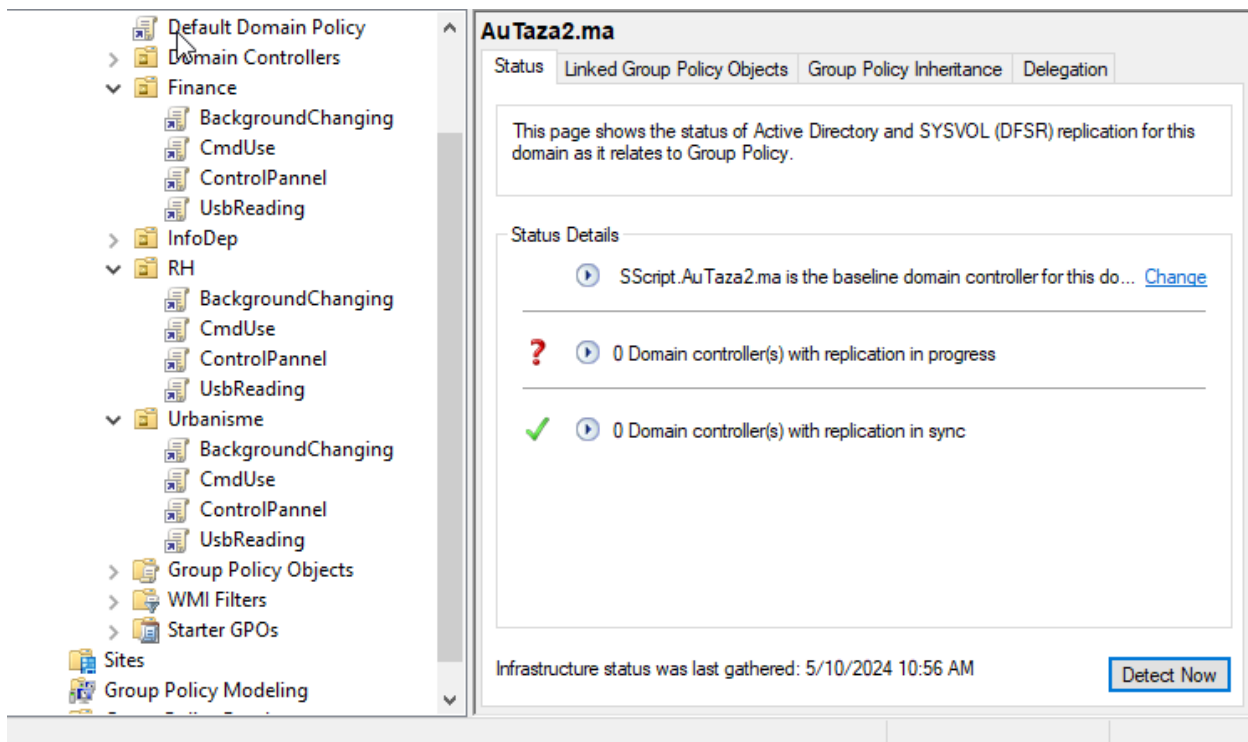
La configuration de GPO avec le script est fait avec la création des fichier DWORD dans des emplacement spécifique ,nom et Valeurs spécifique dépend de ce qu'on veut appliquer, dans mon cas ,j'ai créé trois GPO l'un pour l'accès vers control panel ,un autre pour cmd ,un pour le changement de Background et le dernier pour la lecture de USB inséré , J'ai lié donc ces GPOs au même temps avec les Trois OUs des trois départements .

```
90
91 $GPOs = ("ControlPannel", "UsbReading", "BackgroundChanging", "CmdUse")
92 $Ous=@("Finance", "Urbanisme", "RH")
93
94 Foreach($OU in $OUs){
95     Foreach ($GPO in $GPOs){
96         New-GPLink -Name $GPO -Target "OU=$OU,DC=AuTaza2,DC=ma"
97     }
98 }
99
100
101
```

```
Enforced : False
Target    : OU=RH,DC=AuTaza2,DC=ma
Order     : 3

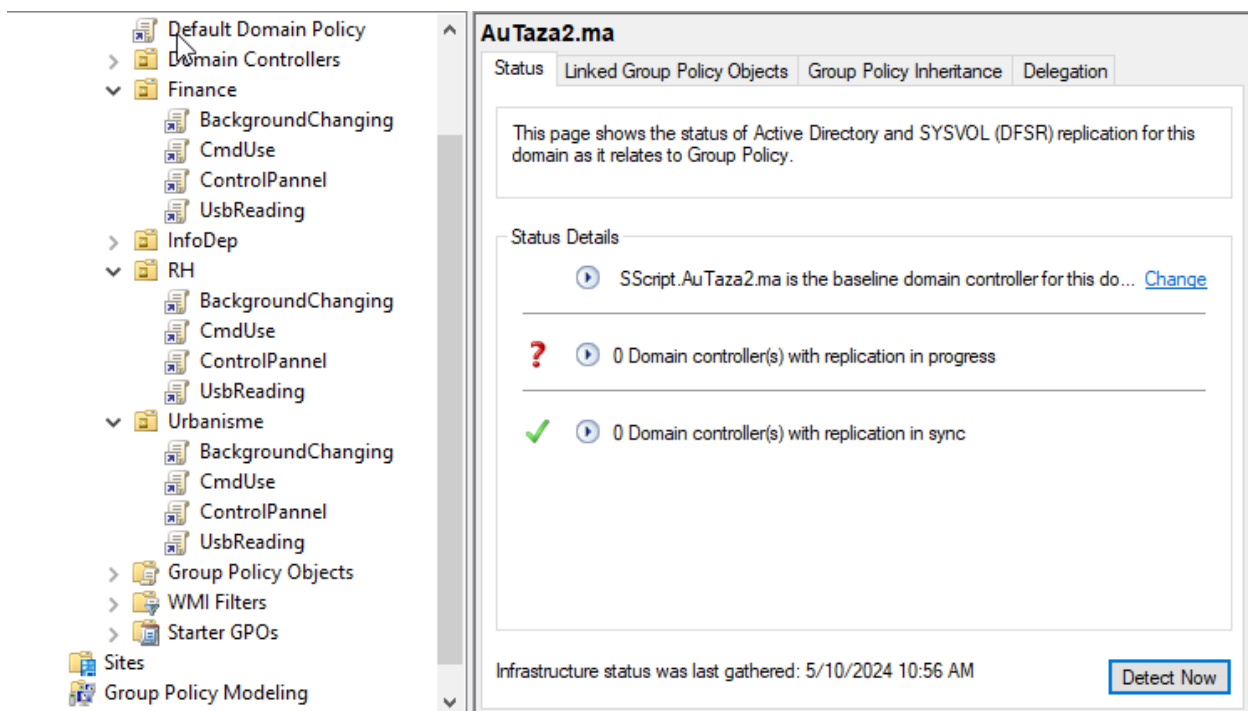
GpoId     : 1ee0bc4e-7f26-4f41-a1af-1bf726670162
DisplayName : CmdUse
Enabled    : True
Enforced   : False
Target     : OU=RH,DC=AuTaza2,DC=ma
Order     : 4
```

Voici le résultat sur l'interface graphique :



Maintenant il faut éditer les GPO pour que chacune faire son fonctionnement principales .

Pour la restriction de l'utilisation de Control Panel :



```

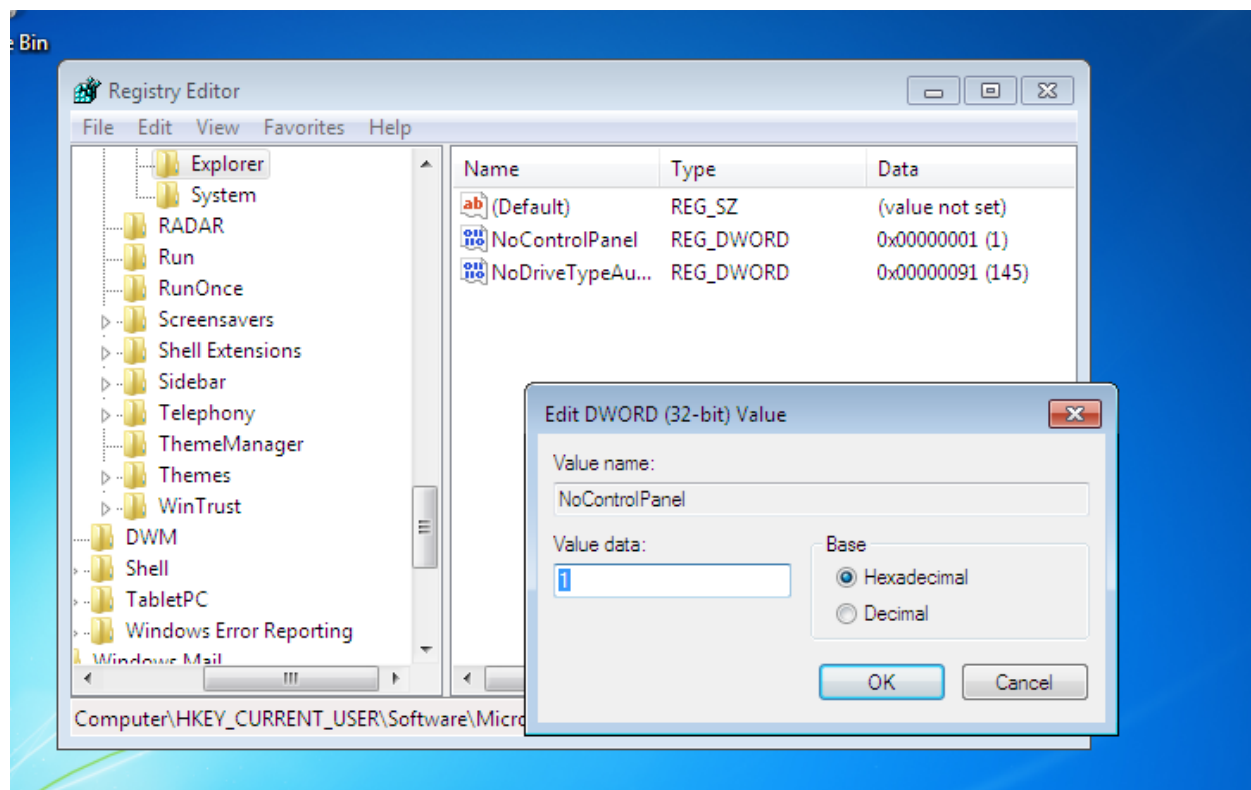
90
91 $GPOs = ("ControlPanel","UsbReading","BackgroundChanging","CmdUse")
103
104 #GPO_ControlPanel
105
106
107 Set-GPRegistryValue -Name $GPOs[0] -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName "NoControlP
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

Voici une explication de cette script :

-Key représente l'emplacement (le Path) dans LocalRegistry dans lequel nous serons créé notre fichier DWord , -ValueName représente le nom de la valeurs de ce fichier dans ce cas c'est 'NoControlPanel', il faut bien vérifier l'écriture et les Maj et Min puisqu'une fausse sera empêcher notre configuration, aussi -Value et la valeur de NoControlPanel, dans mon cas c'est 1 c.-à-d disable accès to ControlPanel.

Maintenant dans la machine client en accède à ce path pour vérifier :



Le fichier est créé avec le nom et la valeur qu'on a donné.

Pour la restriction de l'usage de CMD :

Ce sont les mêmes étapes que la restriction de control panel, la seule chose à changer est le Key ,ValueName et Value ,par les valeurs qui empêchent l'accès vers CMD.

```

109 #GPO_CmdUse
110
111 Set-GPRegistryValue -Name $GPOs[3] -Key "HKCU\Software\Policies\Microsoft\Windows\System" -ValueName "DisableCMD" -Type Dword -Value 1
112
113

```

```

DomainName : AuTaza2.ma
Owner      : AUTAZA2\Domain Admins
Id         : 1ee0bc4e-7f26-4f41-a1af-1bf726670162
GpoStatus  : AllSettingsEnabled
Description :
CreationTime : 5/8/2024 1:26:27 PM
ModificationTime : 5/10/2024 11:29:10 AM
UserVersion : AD Version: 5, SysVol Version: 5
ComputerVersion : AD Version: 0, SysVol Version: 0
WmiFilter  :

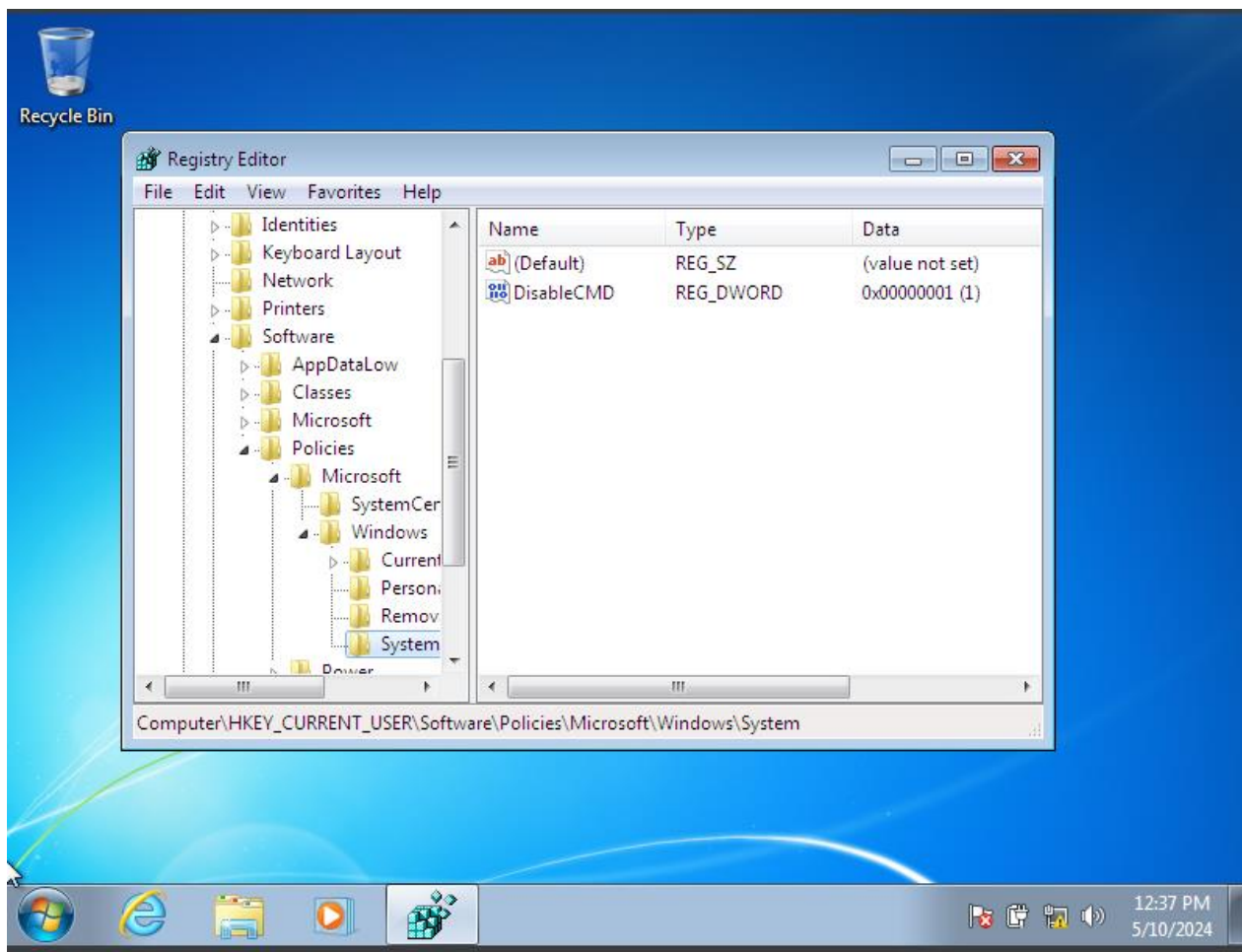
```

```

olicies\Microsoft\Windows\System" -ValueName "DisableCMD" -Type Dword -Value 1

```

Vérification :



La restriction de la lecture d'un USB :

```

115 #GPO_UsbReading
116
117 Set-GPRegistryValue -Name $GPOs[1] -Key "HKCU\Software\Policies\Microsoft\Windows\RemovableStorageDevices" -ValueName "Deny_Read"
118
119

```

```

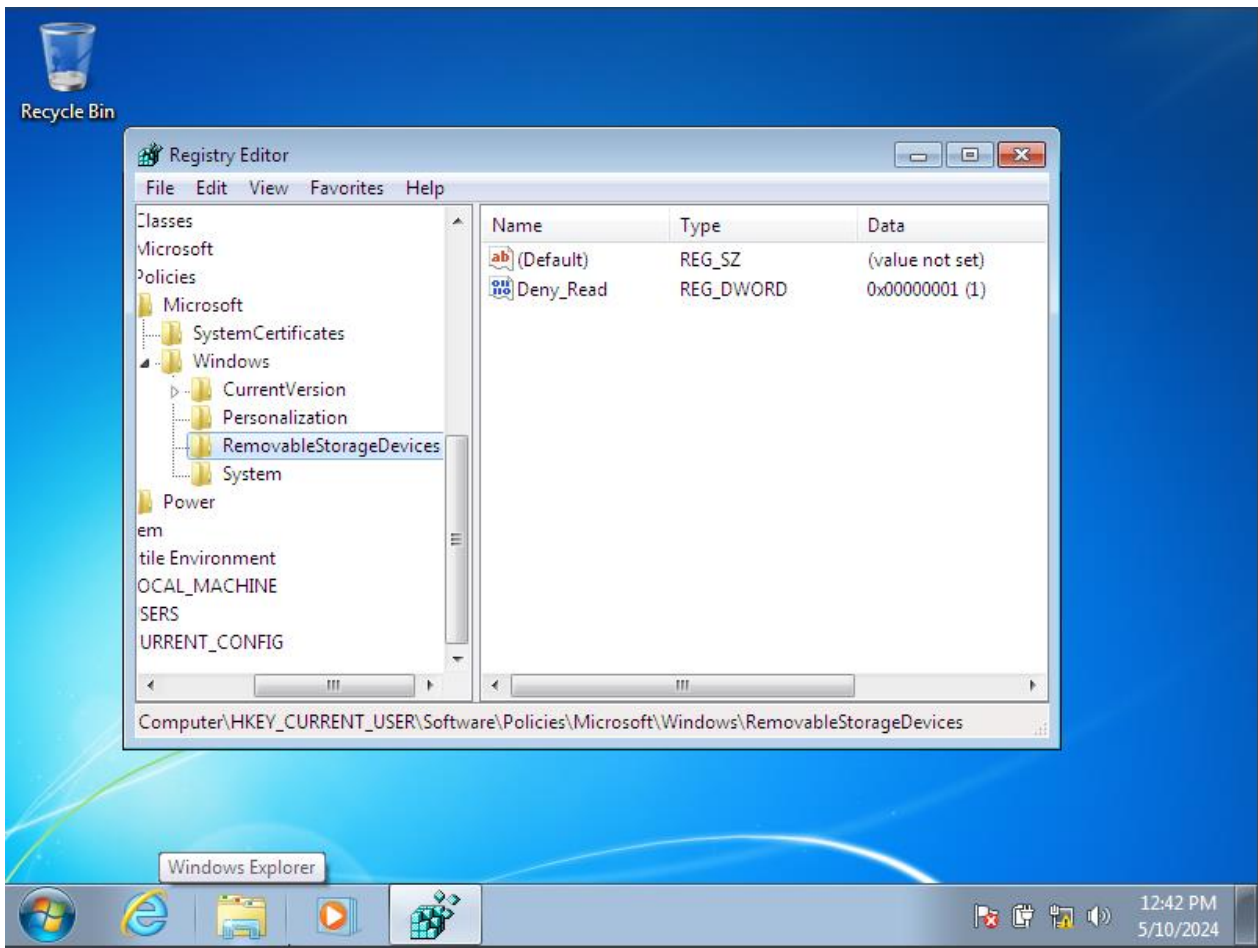
DisplayName       : UsbReading
DomainName        : AuTaza2.ma
Owner             : AUTAZA2\Domain Admins
Id                : 1a6ba6ad-e486-4aef-94bc-ef17275c5245
GpoStatus         : AllSettingsEnabled
Description       :
CreationTime      : 5/8/2024 1:26:25 PM
ModificationTime  : 5/10/2024 11:33:10 AM
UserVersion       : AD Version: 1, SysVol Version: 1
ComputerVersion   : AD Version: 0, SysVol Version: 0
WmiFilter         :

```

```

115
116
117 HKCU\Software\Policies\Microsoft\Windows\RemovableStorageDevices" -ValueName "Deny_Read" -Type Dword -Value 1
118
119

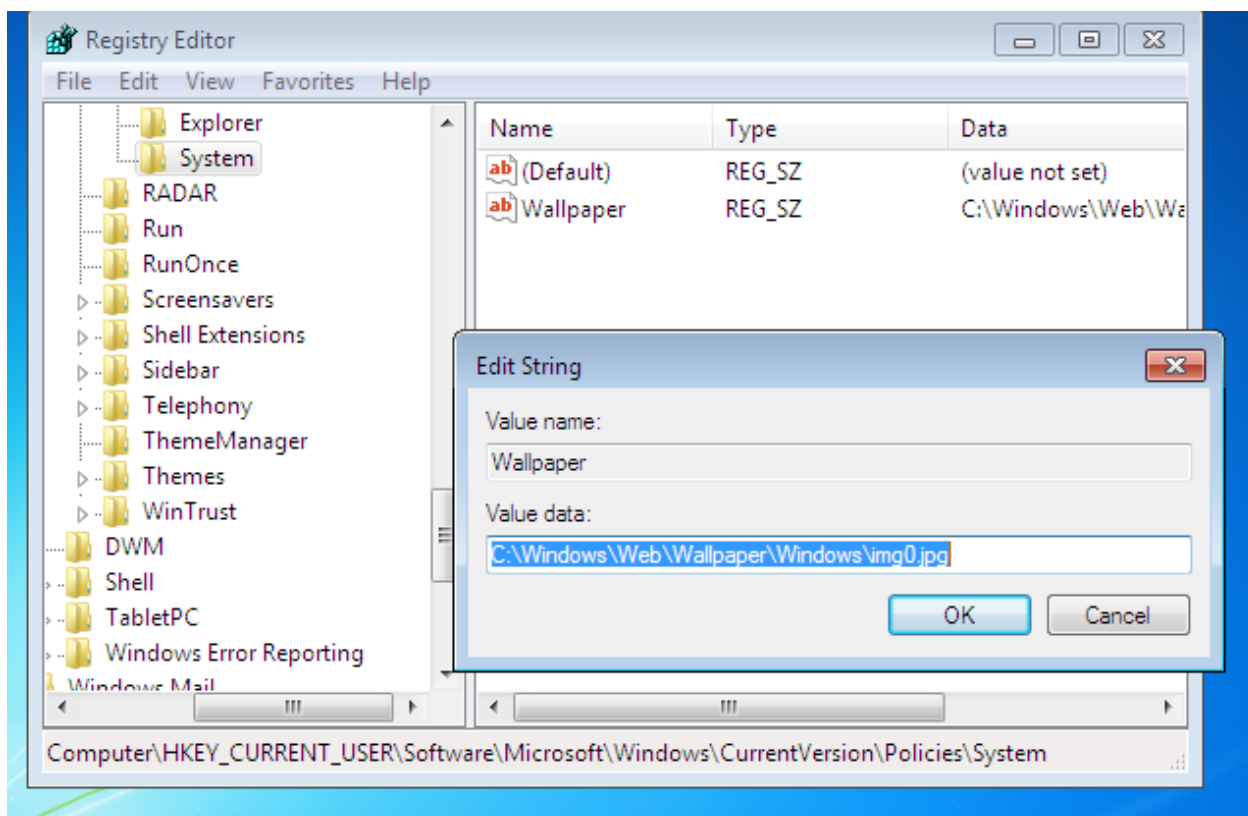
```



Restriction de changement de background :

```
Set-GPRegistryValue -Name $GPOs[2] -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName "Wallpaper" -Type String -Value "C:\Windows\Web\Wallpaper\Windows\img0.jpg"
```

La différence par rapport à la restriction de changement de wallpaper est dans le type qui est string ainsi qu'on doit uniquement spécifier le path de l'image qu'on veut considérer comme background par défaut.



6. Configuration File Sharing et FSRM

Pour la file sharing, j'ai créé premièrement trois répertoires Finance, RH et Urbanisme pour chacun des départements :

```

1 $Groups=@("Finance","Urbanisme","RH")
2 foreach ($folder in $Groups)
3 {
4     New-Item -ItemType Directory -Path "C:\Users\Administrator\Desktop" -Name $folder
5 }
6
7

```

J'ai les créé dans le desktop et voici la liste :

```

PS C:\Users\Administrator> Get-ChildItem -Path "C:\Users\Administrator\Desktop" -Directory

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----          5/14/2024 10:35 AM             Finance
d-----          5/14/2024 10:35 AM              RH
d-----          5/14/2024 10:35 AM          Urbanisme

```

Après ça j'ai utilisé une boucle sur la liste des départements, puisque les noms des dossiers est les même que les noms des Groups, et pour chaque dossier créé j'ai également créé un Share SMB avec le même nom et j'ai donné au group comme droit de Share full Control,

Cela n'est pas suffisant puisque je dois donner à chaque group également le droit NTFS full Control cela fait avec **icacls** qui est utilisé pour modifier les ACL des répertoires sur Windows, j'ai affiché par la suite la liste des Shares créé avec Get-SmbShare


```

161 #FileSharing
162
163 $Deps=@("Finance","Urbanisme","RH")
164 foreach ($Dep in $Deps)
165 {
166     New-Item -ItemType Directory -Path "C:\Users\Administrator\Desktop" -Name $Dep
167     $GName = $Dep + "1"
168     New-SmbShare -Name $Dep -Path "C:\Users\Administrator\Desktop\$Dep" -fullAccess "AuTaza2\$GName"
169     $Grant = $GName + ":(OI)(CI)F"
170     icacls "C:\Users\Administrator\Desktop\$Dep" /grant $Grant /T
171 }
172 Get-ChildItem -Path "C:\Users\Administrator\Desktop" -Directory |Select *
173 Get-SmbShare
174
175

```

```

PS C:\Users\Administrator> Get-SmbShare

Name      ScopeName Path                                     Description
-----
ADMIN$     *      C:\Windows                             Remote Admin
C$         *      C:\                                     Default share
E$         *      E:\                                     Default share
Finance    *      C:\Users\Administrator\Desktop\Finance
IPC$       *      C:\Windows\SYSVOL\srvol\AuTaza2.ma\SCRIPTS Remote IPC
NETLOGON   *      C:\Windows\SYSVOL\srvol\AuTaza2.ma\SCRIPTS Logon server share
RH         *      C:\Users\Administrator\Desktop\RH
SYSVOL     *      C:\Windows\SYSVOL\srvol               Logon server share
Urbanisme  *      C:\Users\Administrator\Desktop\Urbanisme

```

Maintenant je veux interdire l'ajoute des fichiers exécutables pour le département Finance, pour cela, j'ai créé un nouveau FsrmsFileGroup dans lequel j'ai inclus les fichiers avec l'extension .exe, c-à-d les fichiers exécutables, puis j'ai créé une FileScreenTemplate basé sur ce FsrmsFileGroup et j'ai l'activé, et enfin j'ai créé un nouveau FsrmsScreen d'après cette Template et j'ai l'activé également.

```

191 New-FsrmsFileGroup -Name "Exe" -IncludePattern "*.exe"
192
193 New-FsrmsFileScreenTemplate -Name "NoExe" -IncludeGroup @('Exe') -Active
194
195 New-FsrmsFileScreen -Path "C:\Users\Administrator\Desktop\Finance" -Template "NoExe" -Active
196

```

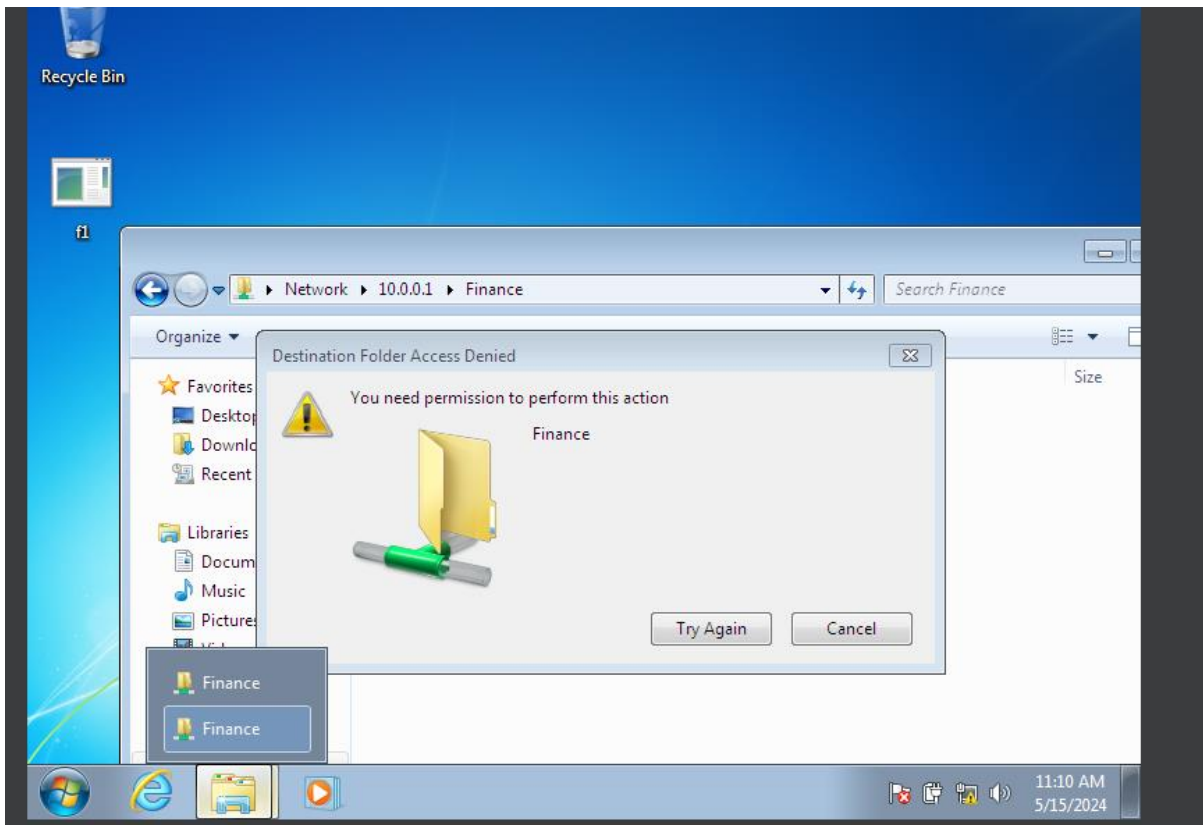
```

Active      : True
Description :
IncludeGroup : {Exe}
Name        : NoExe
Notification :
UpdateDerived : False
UpdateDerivedMatching : False
PSComputerName :

Active      : True
Description :
IncludeGroup : {Exe}
MatchesTemplate : True
Notification :
Path        : C:\Users\Administrator\Desktop\Finance
Template    : NoExe
PSComputerName :

```

Voici le test dans la machine client, j'ai authentifié avec les infos d'un membre de département Finance, j'ai créé un fichier exécutable (f1), et lorsqu'il essaie de l'ajouter dans mon dossier partagé je rencontre ce pop-up de refus:



7. Configuration Storage Pool

Après l'ajoute des disques, on commence la configuration, la première étape est de retourner la liste des disques insérés dans la machine, puis on crée notre Storage pool avec New-Storage pool et on donne le nom et les disques qu'on veut ajouter ainsi que le type de stockage, que j'ai choisie Mirror, puis j'ai créé un volume avec New-Virtualdisk et le style de la partition que j'ai choisie GPT et j'ai terminé par le formatage dans lequel j'ai choisie NTFS comme système de fichier.

```
#StoragePool
$disks = Get-PhysicalDisk
$disks
Get-StorageSubSystem
New-StoragePool -FriendlyName "mnVStoragePool" -PhysicalDisks $disks[1] , $disks[2] -StorageSubsystemFriendlyName "Windows Storage"
Get-StoragePool -FriendlyName "mnVStoragePool"
#CreateNewVolumeForStoragePool
New-VirtualDisk -StoragePoolFriendlyName "mnVStoragePool" -FriendlyName "NMVolum" -ResiliencySettingName Mirror -UseMaximumSize
Get-VirtualDisk -FriendlyName "NMVolum"
#CreatingNewPartition&Volume
Get-Disk | Select *
Initialize-Disk -Number 3 -PartitionStyle GPT
New-Partition -DiskNumber 3 -UseMaximumSize -AssignDriveLetter
Format-Volume -DriveLetter E -FileSystem NTFS -NewFileSystemLabel "MNVolum_"

sicalDisks $disks[1] , $disks[2] -StorageSubsystemFriendlyName "Windows Storage on SScript" -ResiliencySettingName Mirror

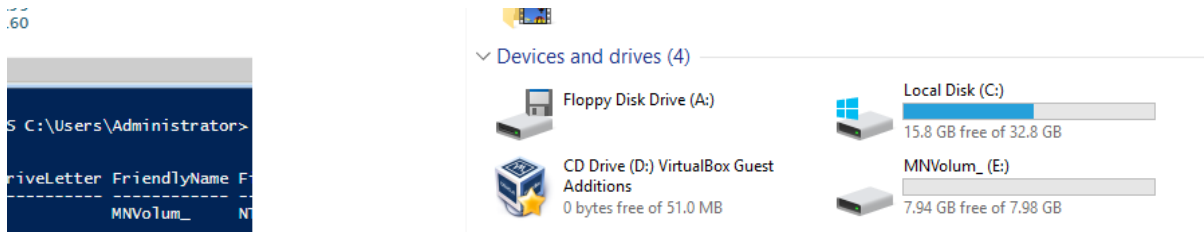
ePool" -FriendlyName "NMVolum" -ResiliencySettingName Mirror -UseMaximumSize

DriveLetter
FileSystemLabel "MNVolum_"
```

```
PS C:\Users\Administrator> New-VirtualDisk -StoragePoolFriendlyName "mnVStoragePool" -FriendlyName "NMVolum" -ResiliencySettingName Mirror
```

FriendlyName	ResiliencySettingName	FaultDomainRedundancy	OperationalStatus	HealthStatus	Size	FootprintOnPool
NMVolum	Mirror	1	OK	Healthy	8 GB	18 GB

Voici le résultat :



8. Configuration de Nic Teaming

Pour la configuration Nic Teaming en dois commencer par la suppression des adresses IP pour les interfaces que nous serons utilisés pour faire le Nic Teaming :

Cela fait avec :

```
Remove-NetIPAddress -InterfaceAlias "Ethernet*" -IPAddress *
```

Puisque tous les noms des interfaces commence par Ethernet et suivie d'un nombre j'ai utilisé «Ethernet*»

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Default Gateway . . . . . : 

C:\Users\Administrator>
```

L'étape suivante est de créer le team qui combine tous ces interfaces, j'ai obtenu la liste des interface avec Get-NetAdapter , et j'ai ajouté les nom des interfaces obtenues en tant que membres de team, j'ai vérifié cette création avec Get-NetLPfoTeam ,et j'ai terminé par l'affectation de l'adresse de mon serveur a ce team créé.

```

Remove-NetIPAddress -InterfaceAlias "Ethernet*"
$interfaces = Get-NetAdapter
New-NetLbfoTeam -Name "EthernetsTeam" -TeamMembers $interfaces[0].Name , $interfaces[1].Name , $interfaces[2].Name
Get-NetLbfoTeam
New-NetIPAddress -InterfaceAlias "EthernetsTeam" -IPAddress "10.0.0.1" -PrefixLength 24
Get-NetAdapter | Select Name ,Speed

```

Maintenant la vérification avec Get-NetAdapter, en filtrant le résultat pour avoir uniquement le nom et la vitesse :

```

PS C:\Users\Administrator> Get-NetAdapter | Select Name ,Speed

```

Name	Speed
-----	-----
Ethernet	1000000000
Ethernet 2	1000000000
EthernetsTeam	3000000000
Ethernet 3	1000000000

Conclusion

Ce projet a brillamment illustré l'importance de maîtriser l'administration d'une infrastructure Windows Server, en mettant l'accent sur les aspects fondamentaux tels que l'installation, la configuration et la gestion des services essentiels. En outre, je n'ai pas seulement renforcé ma compréhension théorique, mais j'ai également mis en œuvre une infrastructure informatique robuste et sécurisée.

L'administration de divers services a révélé des défis et des problèmes inattendus qui ont occupé une grande partie de mon temps pendant la préparation du projet. Cependant, ces défis ont également offert des opportunités d'apprentissage précieuses. Le projet peut être amélioré en explorant des aspects tels que la haute disponibilité, la sauvegarde et la reprise après sinistre, ainsi que l'amélioration de la sécurité.

En conclusion, je suis fier du travail accompli et déterminé à poursuivre mon développement dans le domaine des réseaux informatiques et de l'administration de serveurs. Cette expérience m'a permis d'acquérir des compétences pratiques essentielles et d'affiner ma capacité à résoudre des problèmes complexes, me préparant ainsi à relever de futurs défis professionnels avec confiance et compétence.