

Rapport



Configuration de Active Directory

Encadré par :

- M. Ahmed AMAMOU

Préparé par :

- Fatima BOUYARMANE
- Wissal BOUTAYEB
- Hajar TAIFI BERNOUSSI
- Aya LOTFI

Sommaire

Introduction	3
Notion de base de L'Active Directory.....	4
Introduction	4
Qu'est-ce qu'un Directory Service ?	4
Qu'est-ce qu'un Active Directory ?	4
Quel est le rôle de l'Active Directory ?	5
Comment fonctionne Active Directory ?	5
Pourquoi mettre en place un Active Directory ?	6
Quels sont les services d'Active Directory ?	7
Mise en place d'un annuaire Active Directory.....	8
Partie I : Création d'un Active Directory	8
1- Installation de Windows Server	8
2- Création de Active Directory	14
3- Promouvoir en tant que Contrôleur de domaine	17
4- Créer un utilisateur dans l'Active Directory	20
5- Configuration les profils itinérants	22
6- Joindre un ordinateur a un domaine Active Directory	24
7- Test.....	27
Conclusion	28

Introduction

L'une des principales tâches des administrateurs informatiques consiste à gérer efficacement leurs actifs sur les réseaux d'entreprise. Ils doivent surveiller de près les autorisations des utilisateurs sur le réseau et mettre en place la gestion des permissions.

Cependant, à mesure que les organisations se développent, elles étendent leur réseau, ce qui augmente également leur surface de menace. Les erreurs de configuration ou les défaillances dans la mise en œuvre des politiques d'authentification et d'autorisation entraînent souvent des violations de données et des failles de sécurité. Il devient également difficile de garder la trace des comptes orphelins et de contrer les attaques par escalade de privilèges. Dans ce paysage de menaces complexe et en constante évolution, la gestion efficace de l'**Active Directory (AD)** est de première importance.

Introduction

L'Active Directory (AD) est un annuaire exclusif à Microsoft, intégré dans les systèmes d'exploitation Windows Server depuis 1996. Cet outil de gestion centralise toutes les informations des utilisateurs, des ressources matérielles et des applications au sein d'un réseau d'entreprise. L'AD simplifie l'administration en offrant un accès simplifié à ces informations, contribuant ainsi à une gestion efficace du parc informatique.

Dans ce chapitre, nous explorerons en détail ce qu'est l'Active Directory, son fonctionnement, son rôle crucial dans la gestion des ressources d'un réseau, ainsi que les avantages qu'il offre aux administrateurs et aux utilisateurs. Nous aborderons également les services proposés par l'AD et son utilisation dans les grandes entreprises.

Qu'est-ce qu'un Directory Service ?

Un service d'annuaire, ou "Directory Service", est un conteneur qui organise des objets de façon hiérarchique pour faciliter l'accès et la gestion. Il agit comme un annuaire électronique, permettant de rechercher des informations sans connaître leur emplacement exact. Avant son existence, retrouver des fichiers nécessitait de connaître leur emplacement précis, ce qui devenait compliqué avec les réseaux étendus. Le service d'annuaire simplifie la localisation des ressources, qu'il s'agisse de fichiers, d'ordinateurs ou d'utilisateurs, peu importe où ils se trouvent dans le réseau.

Qu'est-ce qu'un Active Directory ?

L'Active Directory, souvent abrégé "AD", est un service d'annuaire qui centralise les informations sur le réseau d'une entreprise. Il regroupe ces données en trois catégories principales : les utilisateurs, les ressources (comme les ordinateurs, imprimantes, serveurs, dossiers, etc.) et les groupes.

Grâce à l'Active Directory, une entreprise peut mieux contrôler l'utilisation de ses ressources et avoir une vision claire de son système d'information. Elle peut ainsi identifier les composants de son réseau, comprendre comment ils sont utilisés et par qui. De plus, elle peut définir des règles et des autorisations pour chaque élément

répertorié dans l'AD, renforçant ainsi la sécurité de son système d'information et de ses données.

Quel est le rôle de l'Active Directory ?

L'Active Directory vise à centraliser l'authentification et l'accès à un réseau de ressources, permettant aux administrateurs de configurer les autorisations selon les paramètres choisis pour que les utilisateurs puissent accéder aux éléments nécessaires à leur activité. Son objectif est de simplifier la vie des utilisateurs et des administrateurs.

En termes de gestion des accès, l'AD offre une vue globale des ressources et des droits associés, permettant aux administrateurs de contrôler les ordinateurs, d'intervenir à distance, de limiter l'installation d'applications, etc., pour sécuriser le réseau informatique. Ils utilisent des stratégies de groupe pour restreindre les accès aux données.

Les utilisateurs s'identifient une fois pour accéder à toutes les applications et données selon leurs droits, facilitant la recherche d'informations, surtout dans les entreprises avec des filiales dispersées.

La sécurité des données est assurée par l'AD en stockant les données des entreprises et des comptes utilisateurs dans un espace unique, contrôlé par les administrateurs. Ils configurent des paramètres de sécurité et réalisent des sauvegardes pour éviter tout vol d'informations ou intrusion sur les serveurs.

Comment fonctionne Active Directory ?

Active Directory (AD) est un service d'annuaire complexe qui organise les informations sur un réseau d'entreprise. Son fonctionnement est basé sur une architecture hiérarchique comprenant des objets AD, regroupés en trois catégories principales : les utilisateurs, les ressources matérielles et les groupes. Ces objets sont organisés dans des domaines, qui peuvent être comparés à des dossiers, et qui composent des arbres, formant une forêt AD.

Les administrateurs gèrent ces objets et domaines pour définir les autorisations d'accès et les services associés. Ils utilisent des stratégies de groupe pour limiter les accès aux données et applications. L'infrastructure physique de l'AD repose sur des serveurs appelés contrôleurs de domaine (DC), qui communiquent entre eux pour maintenir les données à jour. Un Read Only Domain Controller (RODC) peut également être utilisé pour fournir un accès rapide aux ressources en lecture seule, garantissant la sécurité de l'AD.

Il est important de noter qu'AD ne gère pas les données sur le cloud, mais uniquement sur site. Pour intégrer des données stockées sur un cloud privé, il est nécessaire de compléter AD par une solution de gestion des identités et des accès adaptée à votre environnement de cloud privé.

Pourquoi mettre en place un Active Directory ?

Pour comprendre l'intérêt d'Active Directory, il est important de connaître le contexte d'utilisation.

Utilisation de l'Active Directory au sein de grandes entreprises :

L'intérêt d'utiliser Active Directory dans de grandes entreprises réside dans sa capacité à centraliser la gestion des utilisateurs, des ressources et des droits d'accès. Dans une organisation de plus de 1 000 employés, répartis dans des filiales sur différents sites, la collaboration étroite entre les salariés et les consultants externes est cruciale.

Les employés ont besoin d'accéder à des ressources communes et aux mises à jour des informations de manière efficace. De plus, l'équipe informatique doit gérer un parc informatique étendu, des applications et des autorisations d'accès pour tous les utilisateurs.

Active Directory permet à l'administrateur de configurer ces paramètres à un seul endroit, simplifiant ainsi la gestion et réduisant la charge de travail. Cela garantit une activité optimale au sein de l'entreprise en centralisant un maximum de ressources et en facilitant la gestion par domaine.

Les avantages d'un annuaire comme Active Directory :

Mettre en place un Active Directory au sein de son entreprise compte de nombreux avantages.

- La centralisation des données des utilisateurs et des équipements matériels améliore la sécurité du réseau.
- Les administrateurs gèrent les droits d'accès à des utilisateurs ou des groupes plus facilement.
- Les administrateurs ont accès aux mises à jour des applications et des machines pour limiter les failles de vulnérabilité.
- Les entreprises disposent d'une protection contre la perte de données grâce aux répliquions au sein même de la structure du contrôleur de domaine.
- Active Directory est compatible avec d'autres annuaires de ressources.
- L'administration des ressources est centralisée : les administrateurs gagnent du temps et peuvent se concentrer sur d'autres missions.

Quels sont les services d'Active Directory ?

- **Authentification et autorisation des utilisateurs :** Il offre des outils pour créer, modifier et supprimer des comptes utilisateur ainsi que des groupes, permettant une gestion centralisée des identités et des autorisations.
- **Gestion des utilisateurs et des groupes:** Il offre des outils pour créer, modifier et supprimer des comptes utilisateur ainsi que des groupes, permettant une gestion centralisée des identités et des autorisations.
- **Gestion des ressources :** Active Directory permet de gérer les ressources réseau telles que les ordinateurs, les imprimantes, les serveurs de fichiers, etc., en les organisant dans une structure hiérarchique.
- **Politiques de groupe :** Il permet de définir et d'appliquer des politiques de groupe qui contrôlent le comportement des utilisateurs et des ordinateurs dans un domaine Windows, comme les paramètres de sécurité, les configurations logicielles, etc.
- **Services de domaine :** Active Directory fournit des services de domaine qui permettent aux utilisateurs d'accéder de manière transparente aux ressources réseau, quel que soit l'emplacement physique de ces ressources.
- **Sécurité et audit :** Active Directory offre des fonctionnalités de sécurité avancées telles que la gestion des certificats, l'audit des événements, la surveillance de l'accès aux ressources, etc.

Chapitre II : Mise en place d'un annuaire Active Directory

Pour Arriver à notre objectif nous devons passer par 2 étapes : La 1^{er} est de Créer notre Active Directory et la 2eme consiste à intégrer notre active directory avec vCenter.

Partie I : Création d'un Active Directory

Cette partie explique comment installer et configurer une nouvelle installation Active Directory dans un environnement de laboratoire qui inclut Windows Server 2012 et Active Directory.

Produit concerné : Windows Server 2012

1- Installation de Windows Server

Avant d'installer Windows Server 2012 en tant que machine virtuelle dans VMware Workstation, vous voudrez peut-être vous assurer des éléments suivants :

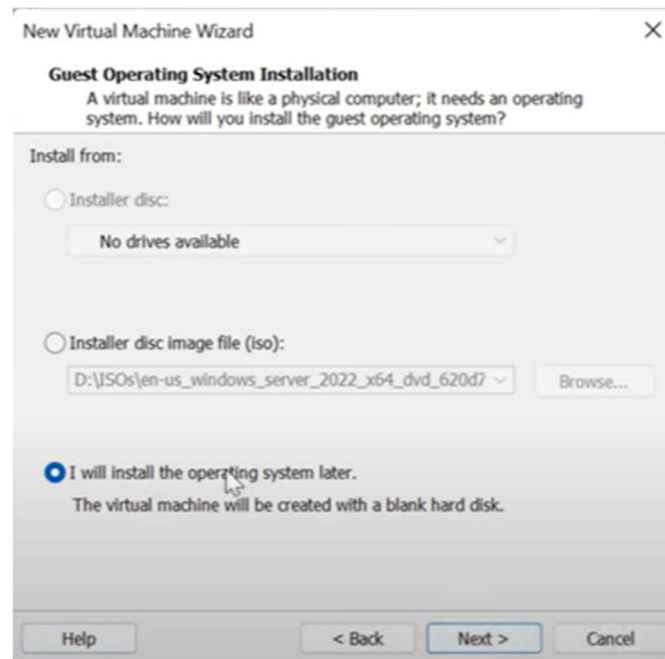
- Au moins 2 Go de mémoire vive ou plus pour l'installation de Hyper-V et de machines virtuelles imbriquées.
- Un processeur prenant en charge et activant la technologie Intel VT.
- Au moins 50 Go d'espace disque dur ou plus pour l'installation de la machine virtuelle Hyper-V.

Cliquez sur "Fichier" dans le menu, puis sélectionnez "Nouvelle machine virtuelle".

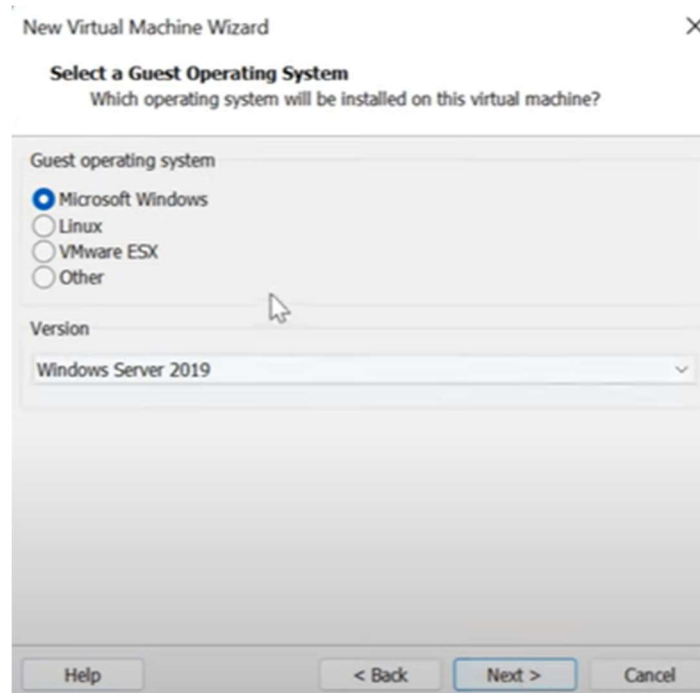


On sélectionne Typical et on clique sur suivant.

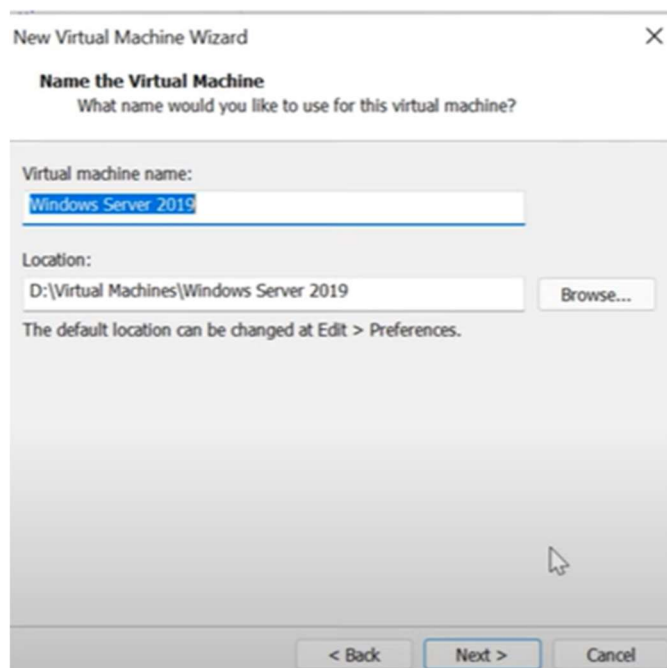
On sélectionne la 3eme option et on clique sur Next.



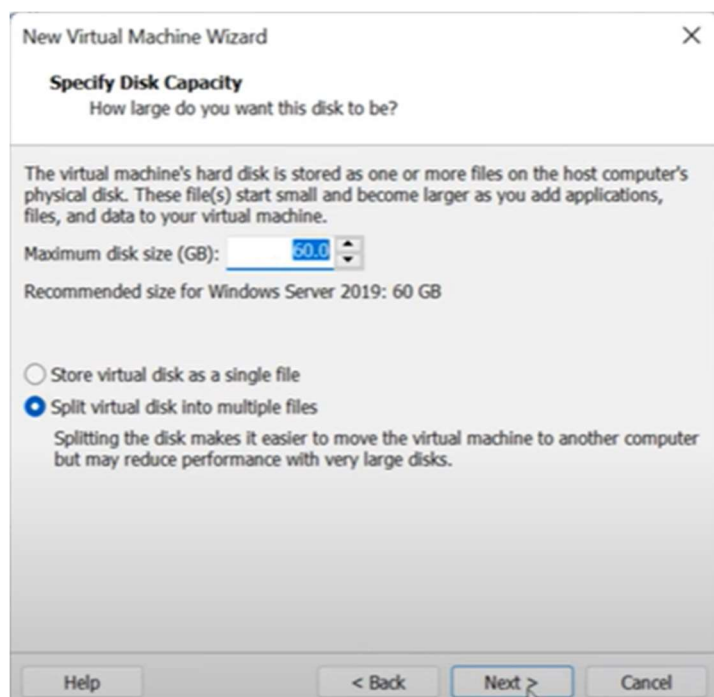
On sélectionne Microsoft Window dans l'operating system choisit et puis on choisit notre version qui sera Windows server 2012



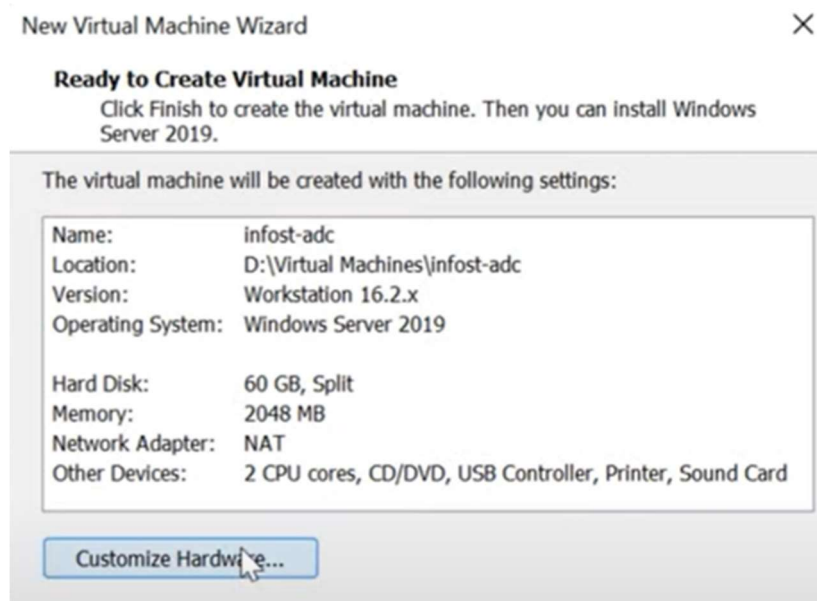
On choisit un nom pour notre serveur et l'emplacement. On a choisit comme nom Windows Server 2019.



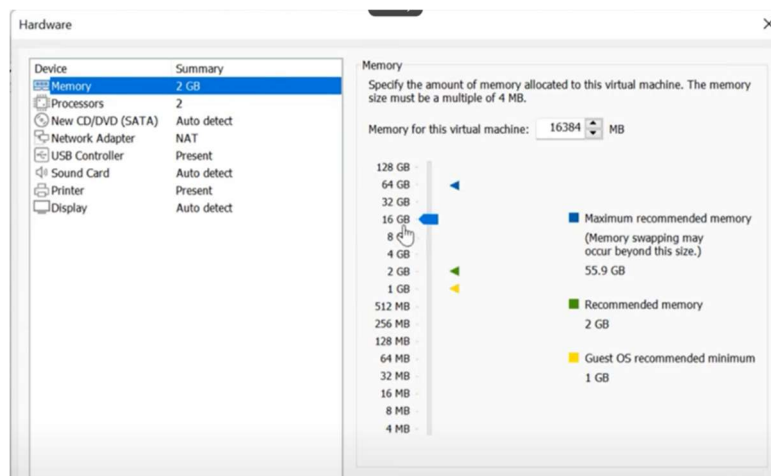
Après on spécifie la capacité du disk dur. Et on choisit la 2eme option "Split virtual disk into multiple files".



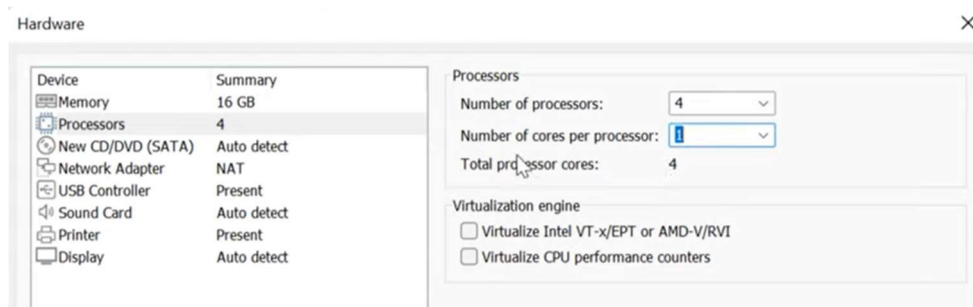
On clique sur Customize hardware



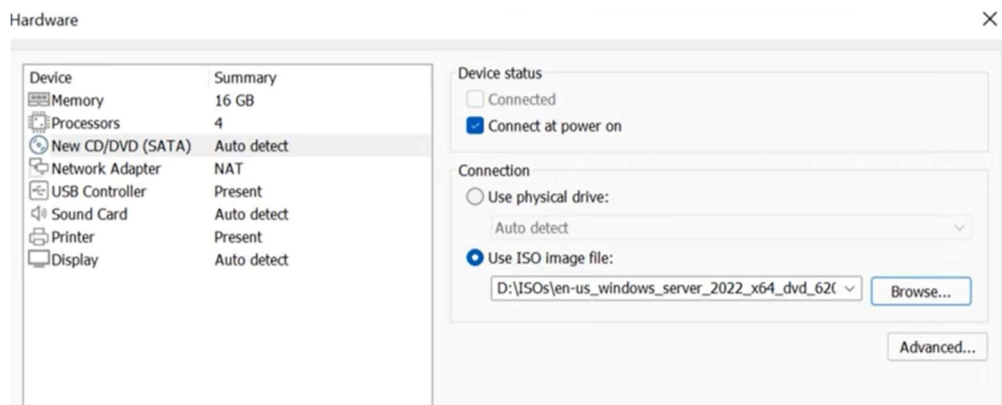
Et on Spécifie la taille de la mémoire RAM nécessaire qui sera dans notre cas 16 bit.



On change aussi le nombre de processeur de 2 a 4 .



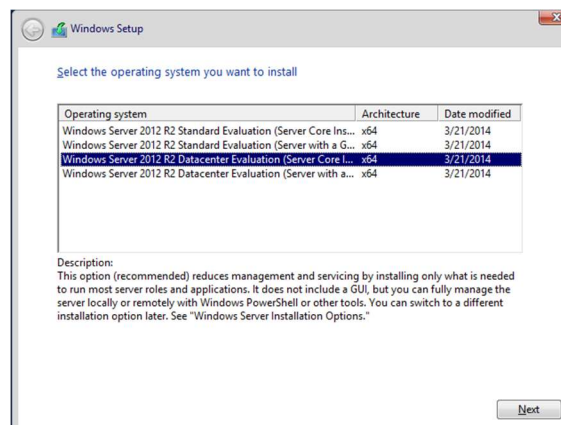
Et maintenant on attache iso file de Windows server



A ce niveau on a terminé la création de la machine virtuelle. Maintenant on allume notre machine.

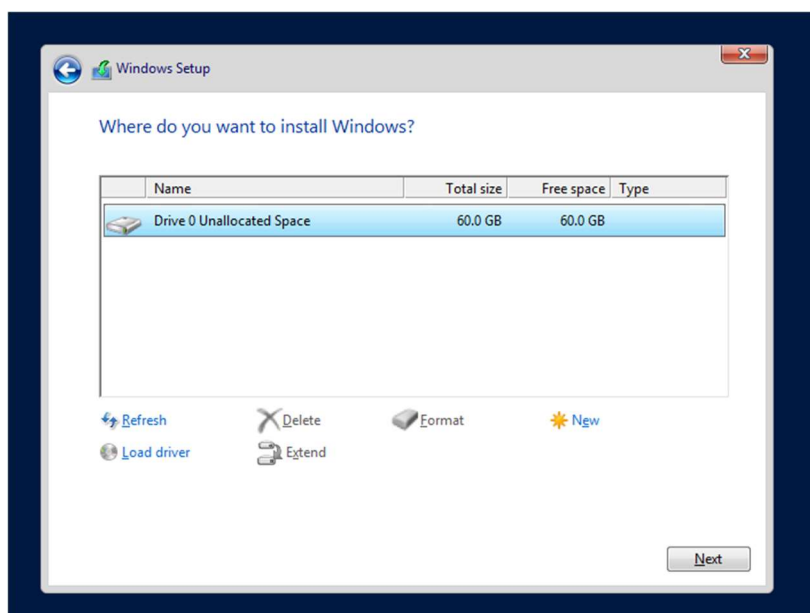


On entre les champs nécessaires et on clique sur Next.

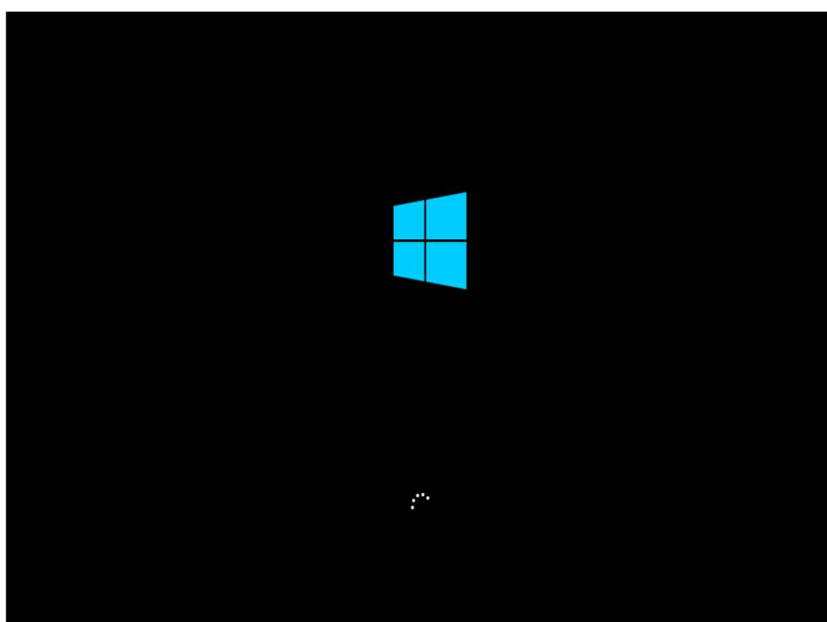


On choisit la 4-ème option et puis sur Next.

On accepte la licence et puis on clique sur Next.



On sélectionne le drive puis sur Next.



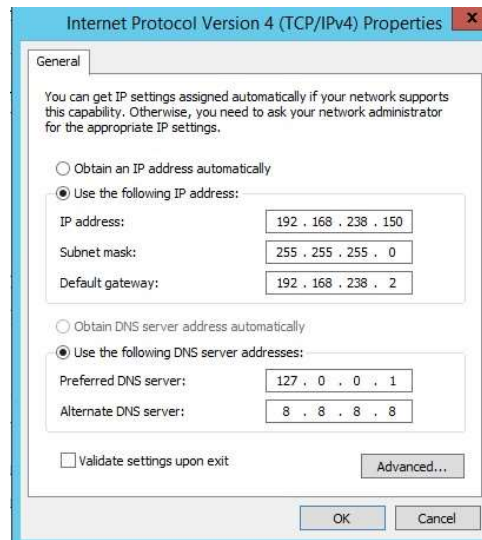
On attend quelques minutes et apres, on entre un username et un mot de passe.

Notre Windows server est installé maintenant. On est maintenant dans le bout de créer notre AD

2- Création de Active Directory

Un serveur doit toujours avoir une adresse IP statique pour ne pas que celle-ci ne change à un moment donné.

Pour cela nous devons définir une adresse IP statique ainsi qu'un serveur DNS préféré.



Avant de promouvoir le serveur en tant que contrôleur de domaine dans un nouveau domaine, il faut installer le rôle « **Service de domaine Active Directory** ».

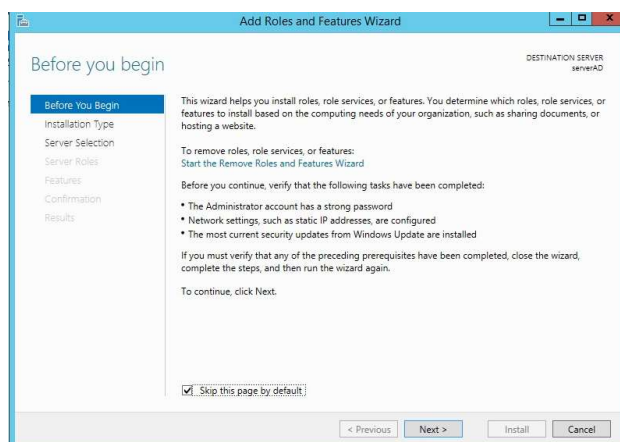
Pour cela, dans la page d'accueil, On Clique sur « **Gestionnaire de serveur** ».



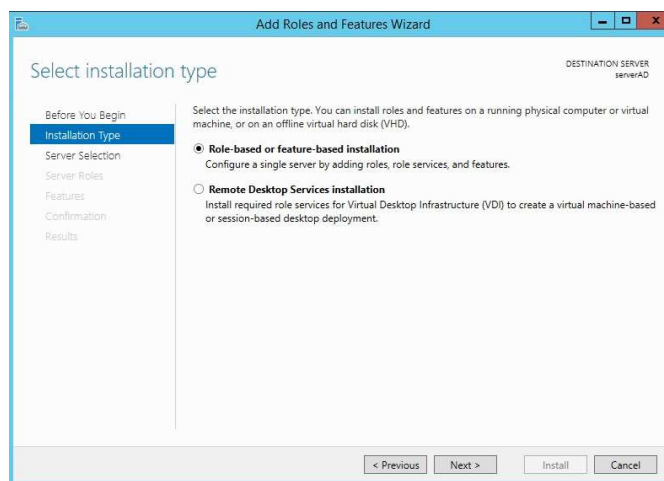
Une fois Sur Server Manager, on clique sur « **Ajouter des rôles et des fonctionnalités** » présent dans la section « **Démarrage rapide** ».



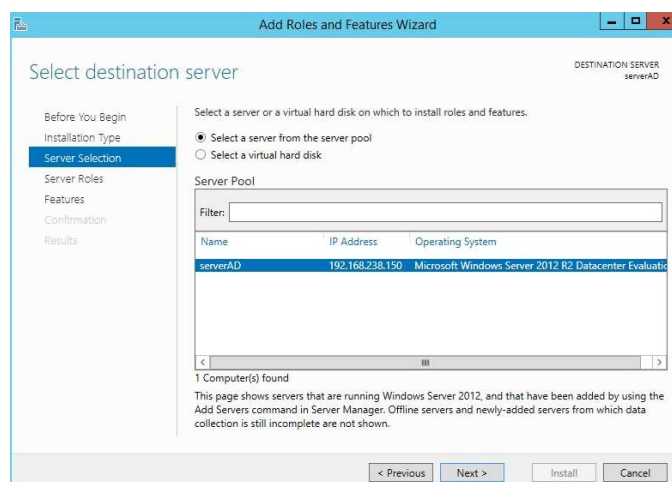
L'assistant s'exécute et vous demande de vous assurer que le compte Administrateur possède un mot de passe fort, que la configuration réseau est en adresse statique et que votre serveur est à jour au niveau des mises à jour de sécurité.
On Clique sur Next.



On laisse le choix par défaut puisque nous souhaitons ajouter un nouveau rôle à notre serveur et non installer des services de Bureau à distance comme le propose le second choix.

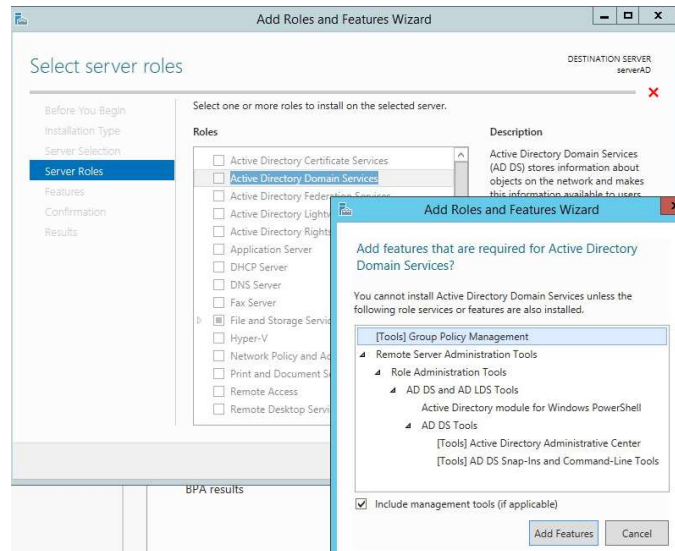


On sélectionne le serveur de destination dans la liste indiquée et on clique sur « **Suivant** ».
Ceci est une nouveauté de Windows Server 2012 qui permet à partir d'un serveur de gérer plusieurs autres serveurs qui sont configurés pour être gérés par un autre serveur. Dans notre cas, il n'y a qu'un seul serveur, le choix est donc restreint.

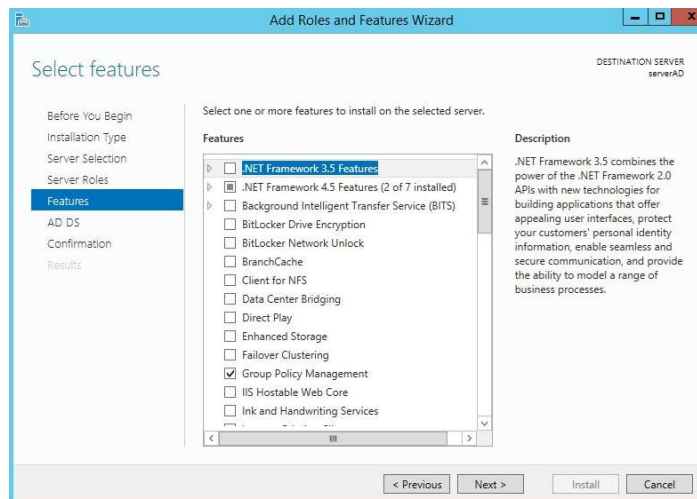


Au niveau des rôles, sélectionnez « **Service AD DS** » qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour vous indiquer que d'autres éléments requis par AD DS doivent être installés, cliquez sur « **Ajouter des fonctionnalités** ». Ensuite, cliquez sur « **Suivant** ».

Au niveau des fonctionnalités, On Vérifie “Group Policy Management” et on clique sur “Next”.

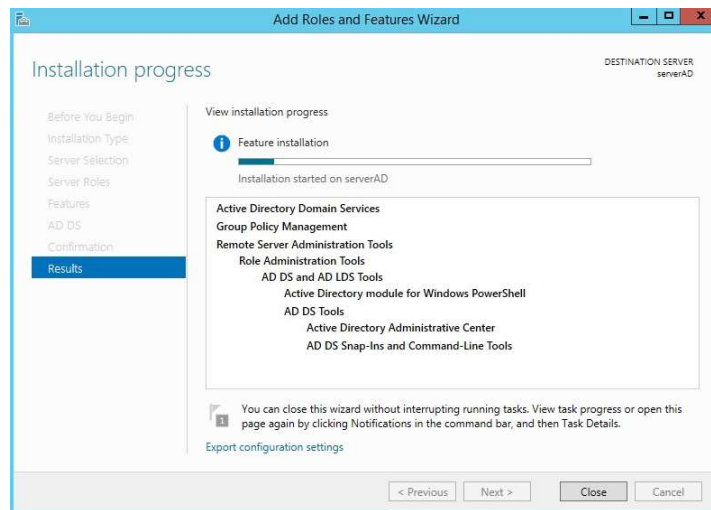


Ensuite, des explications concernant AD DS sont affichées, on clique sur « **Suivant** » à nouveau.



Un récapitulatif des éléments qui vont être installés et affichés, cliquez sur « **Installer** » pour exécuter l'installation des divers éléments.

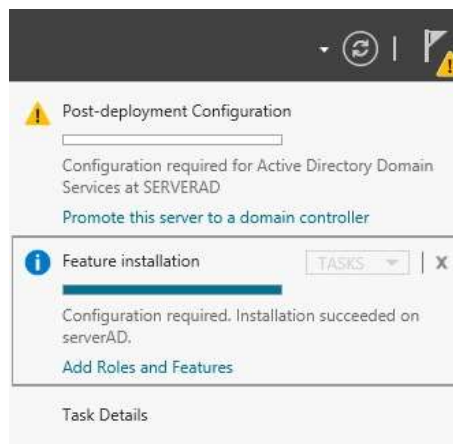
Après on attend quelques secondes jusqu'à ce que l'installation soit terminée.



3- Promouvoir en tant que Contrôleur de domaine

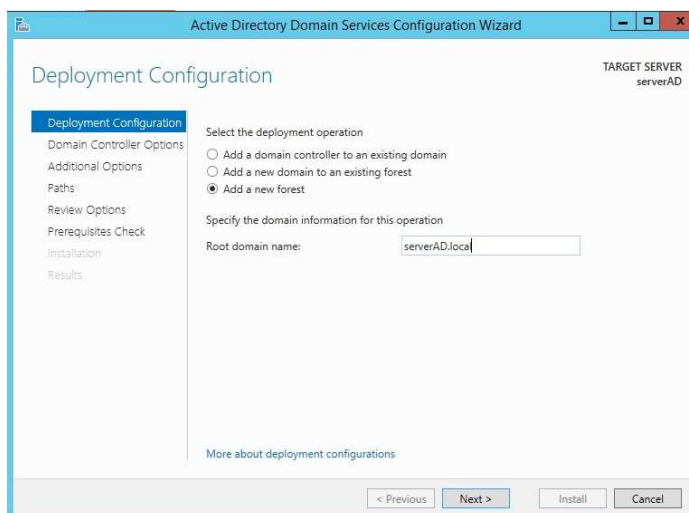
Afin de promouvoir notre serveur en tant que contrôleur de domaine, vous avez l'habitude d'effectuer la commande « **dcpromo** » qui permet d'exécuter l'assistant de promotion de serveur.

Avec Windows Server 2012, dans le Gestionnaire de serveur un symbole d'avertissement apparaît auprès du Centre de maintenance, cliquez dessus et vous verrez apparaître ceci :



Il vous suffit de cliquer sur « **Promouvoir ce serveur en contrôleur de domaine** » pour exécuter l'équivalent d'un DCPROMO sous Windows Server 2012.

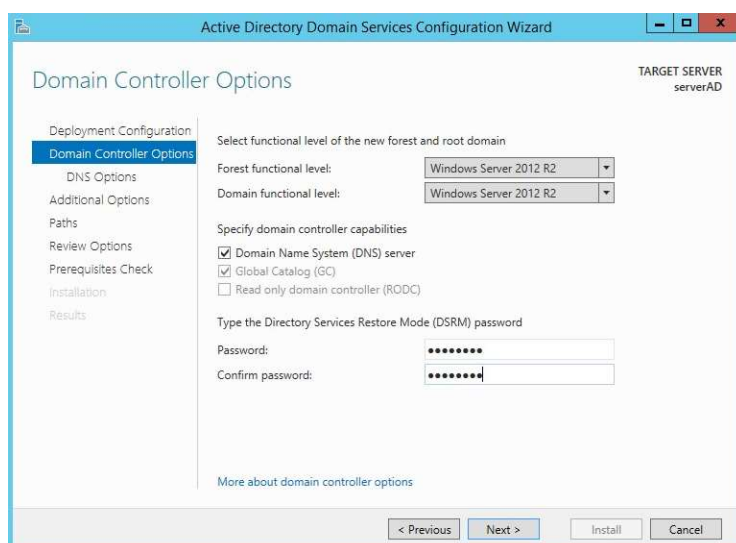
Vu que nous souhaitons créer un nouveau domaine appelé « **serverAD.local** », nous devons déployer une nouvelle forêt (une forêt étant un ensemble de domaines, ce qui permet d'ajouter d'autres domaines dans cette forêt par la suite). Cochez « **Ajouter une nouvelle forêt** » et indiquez « **serverAD.local** ».



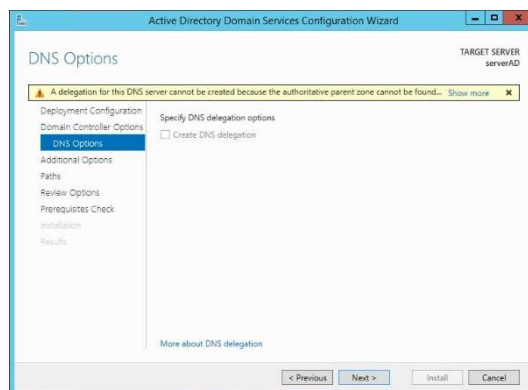
On Choisit le niveau fonctionnel qui nous convient le mieux pour la forêt. Cela dépend de ce que nous prévoyons à l'avenir, dans le cas où nous créons d'autres domaines dans cette forêt nous allons devoir adapter le système d'exploitation embarqué par nos serveurs par rapport au niveau fonctionnel sélectionné.

Pour information, on peut augmenter le niveau fonctionnel, mais en aucun cas le diminuer.

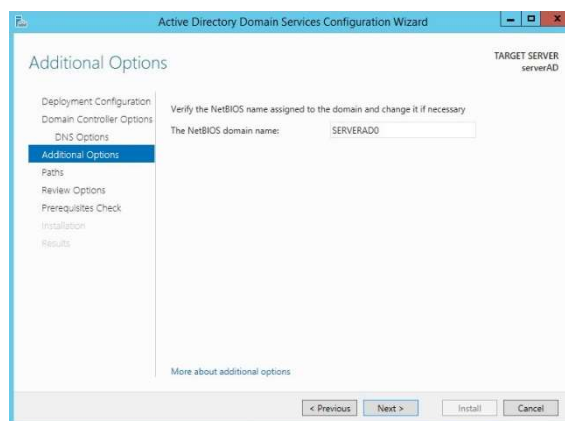
Pour notre part, nous sélectionnons « **Windows Server 2012** » pour les deux niveaux fonctionnels. Laissons cocher « **Serveur DNS** » puisque ce serveur servira également de serveur DNS sur le domaine et indiquons un mot de passe de restauration des services d'annuaires. Une fois que tout est renseigné, on clique sur « **Suivant** ».



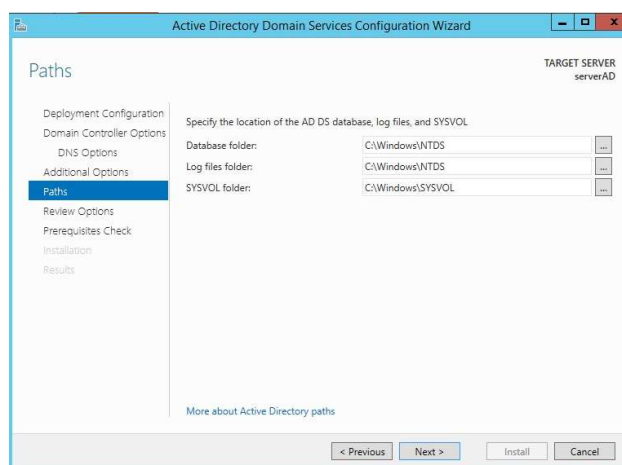
En ce qui concerne les options DNS, on fait suivant puisqu'il n'y a aucune modification à effectuer.



Ensuite, patientons pendant l'affichage du nom NETBIOS de notre domaine et modifions-le si nécessaire, le nom NETBIOS permet notamment d'ouvrir une session et de s'authentifier sur le domaine. Exemple, ouvrir une session « **Hajar** » sur le domaine « **serverAD.local** » ayant pour nom NETBIOS « **serverAD0** » : « **serverAD0\Hajar** ».

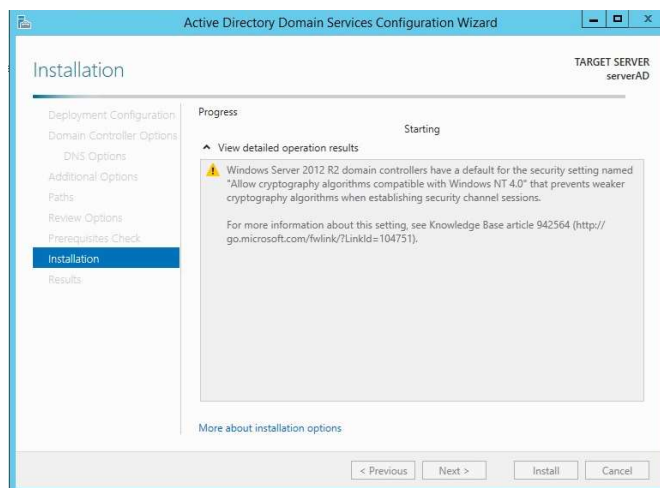


Lorsqu'on vous demande de choisir les différents chemins d'accès pour le dossier SYSVOL, la base de données et les fichiers journaux, C'est mieux de laisser les paramètres par défaut afin de rester standard et d'être sûr de pouvoir les retrouver facilement.



On clique sur « **Suivant** », puis on examine une dernière fois les options que nous avons définies dans la page récapitulative. Une fois que le tour est fait, on clique une seconde fois sur « **Suivant** ».

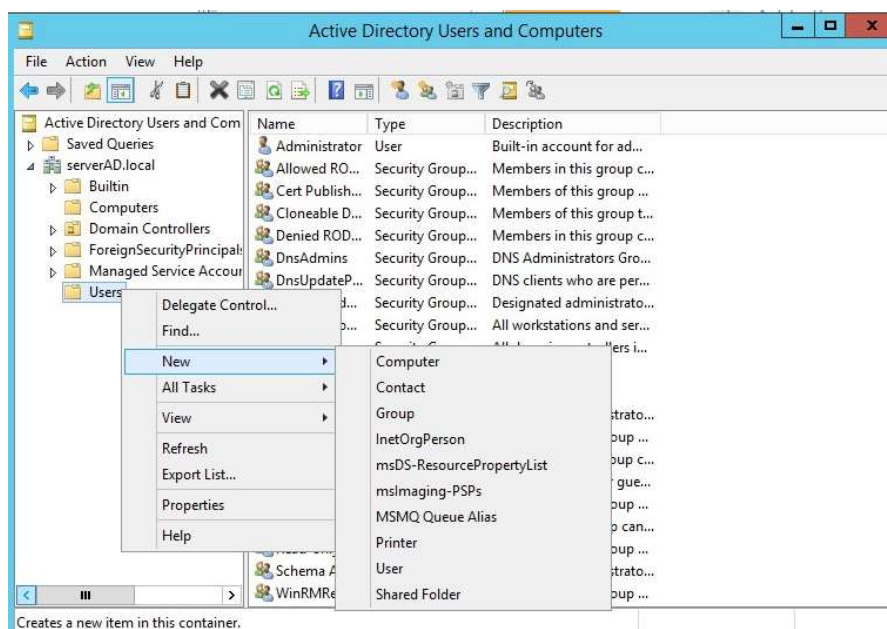
Enfin, vérifions qu'il n'y a pas d'erreur(s) critique(s) et on clique sur « **Installer** ». Le serveur redémarrera automatiquement une fois le déploiement terminé.



Une fois le serveur redémarré, connectez-vous avec le compte Administrateur présent désormais dans l'Active Directory et commencez à administrer votre domaine.

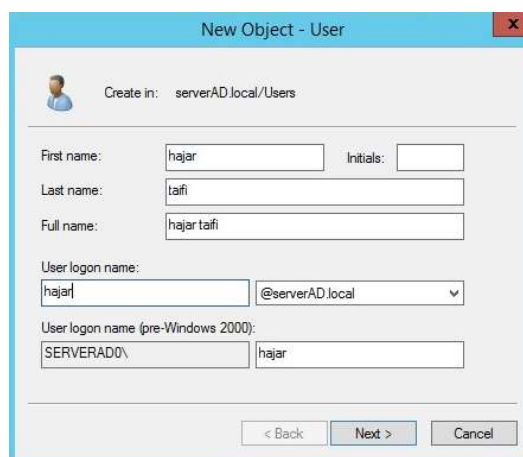
4- Créer un utilisateur dans l'Active Directory

On ouvre la console Utilisateur et ordinateurs Active Directory et se positionner dans l'unité d'organisation (OU) où l'utilisateur doit être créé.

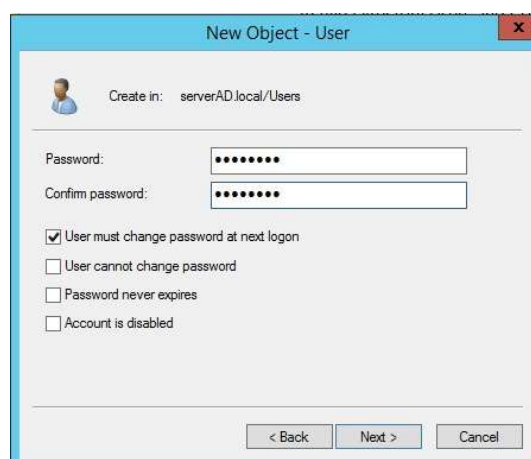


On remplit le formulaire après la clique sur l'icône qui se trouve dans la barre d'action ou en faisant un clic droit puis Nouveau / Utilisateur.

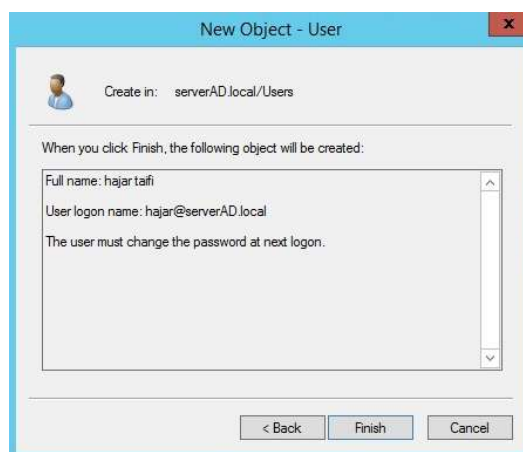
Indiquons le nom, prénom de l'utilisateur et son identifiant Active Directory, qui va lui servir à s'identifier sur les ordinateurs par exemple puis cliquer sur Suivant.



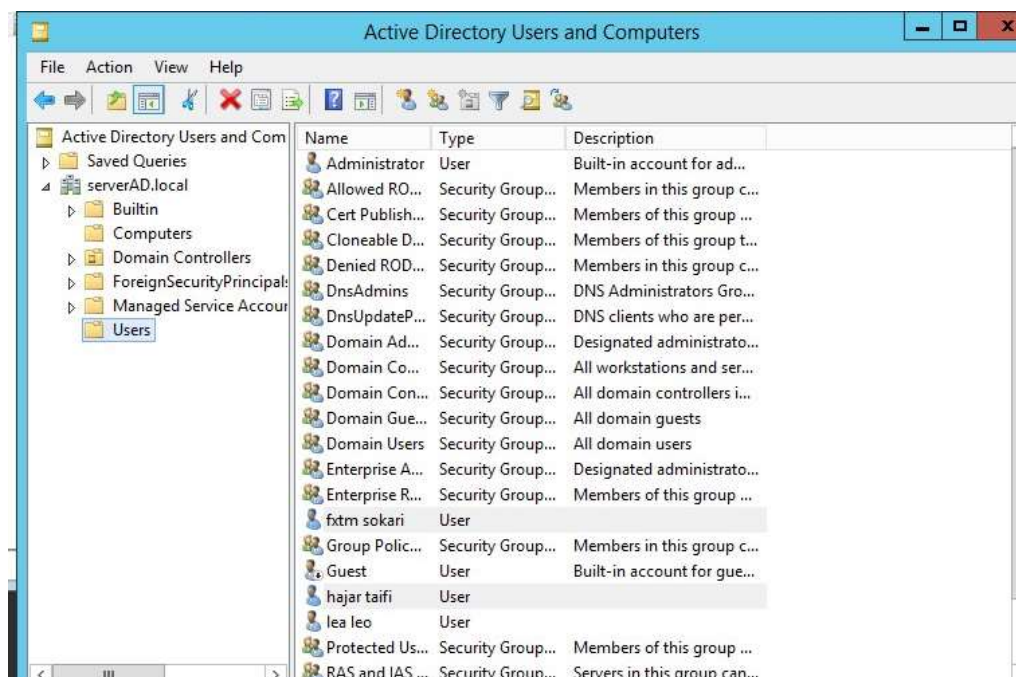
Entrer le mot de passe lié au compte de l'utilisateur et les options de celui-ci comme le changement à la première ouverture de session, si l'utilisateur est autorisé à le changer ou encore si celui-ci n'expire pas. Passer à l'étape d'après en cliquant sur Suivant.



Un résumé du compte s'affiche, confirmer la création du compte de l'utilisateur en cliquant sur Terminer.



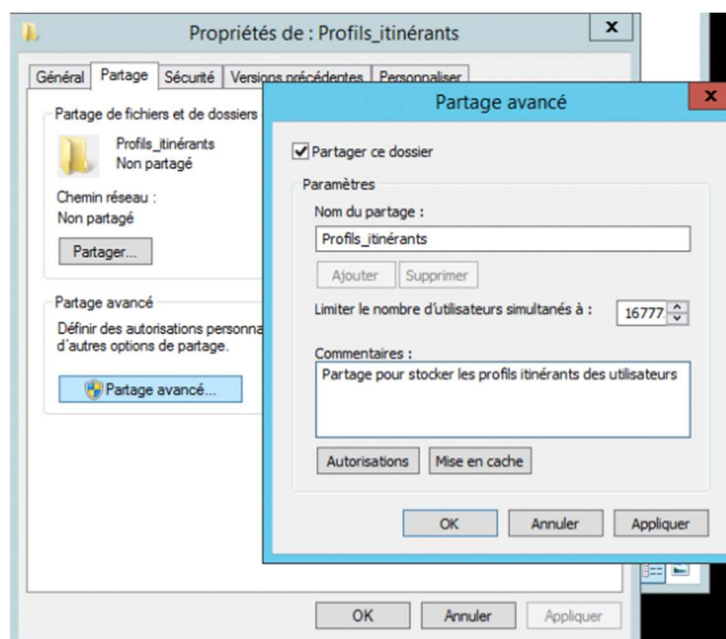
Le compte est maintenant présent dans l'annuaire, il est maintenant possible de l'ajouter à des groupes ou de modifier les propriétés de celui-ci en faisant un clic droit puis en cliquant sur Propriétés.



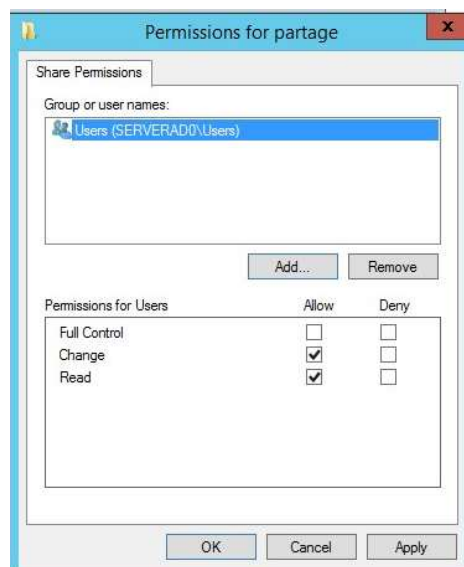
5- Configuration les profils itinérants

La première étape consiste à créer un répertoire que nous allons partager et qui servira à stocker les données des profils. Par exemple, pour ma part je crée répertoire nommé **"Partage"** que je partage sous le même nom.

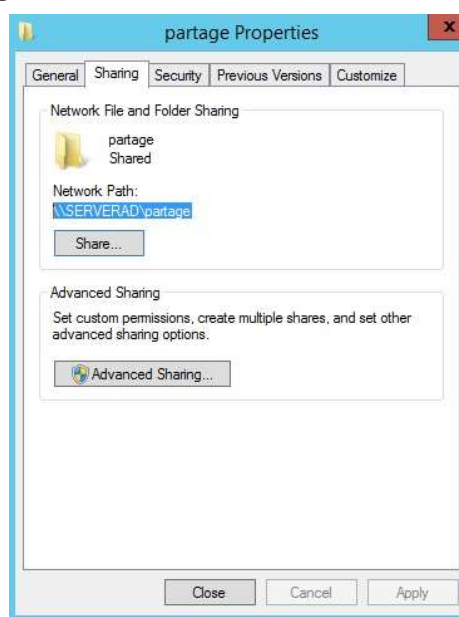
Dans la configuration du partage, cliquez sur **"Autorisations"**



Supprimez "**Tout le monde**" et préférez à la place "**Utilisateurs**", un groupe qui englobe vos utilisateurs de l'Active Directory. Au niveau des droits, la lecture et l'écriture vont suffire, comme ceci :



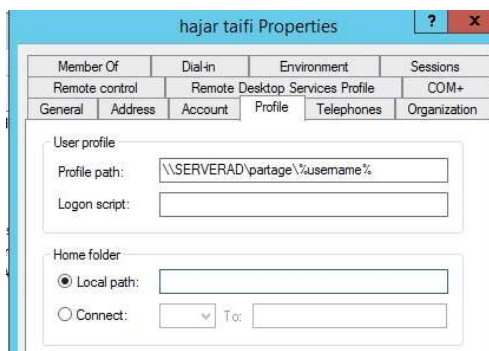
Validez, la création du partage est désormais terminée.



On copie le chemin.

Passons maintenant à la configuration au sein de l'annuaire Active Directory. Il est important de s'assurer également que les "**Utilisateurs authentifiés**" disposent des autorisations NTFS "**Contrôle total**" afin de pouvoir s'approprier des objets au sein de leur dossier de profil. Pour modifier cela, effectuer un clic droit sur le répertoire "**Profils_itinérants**" et éditez l'onglet "**Sécurité**".

Effectuons un clic droit sur un utilisateur qui doit disposer d'un profil itinérant, cliquons sur "**Propriétés**". Accédez à l'onglet "**Profil**" et au niveau du champ "**Chemin du profil**", on indique simplement le chemin UNC vers le serveur, suivi du partage et à la fin **%username%** qui prendra pour valeur le login de l'utilisateur.

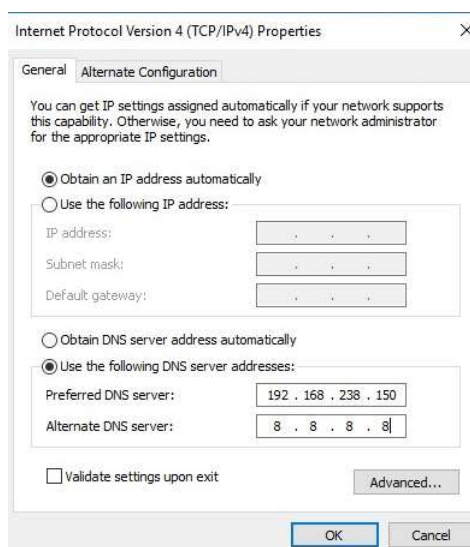


Lorsque le chemin est renseigné, validez.

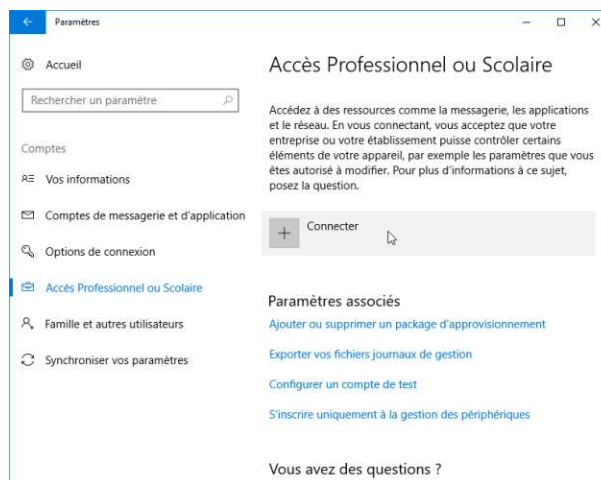
6- Joindre un ordinateur a un domaine Active Directory

Il est indispensable que les postes clients aient l'adresse IP d'au moins un des contrôleurs de domaine comme serveur DNS.

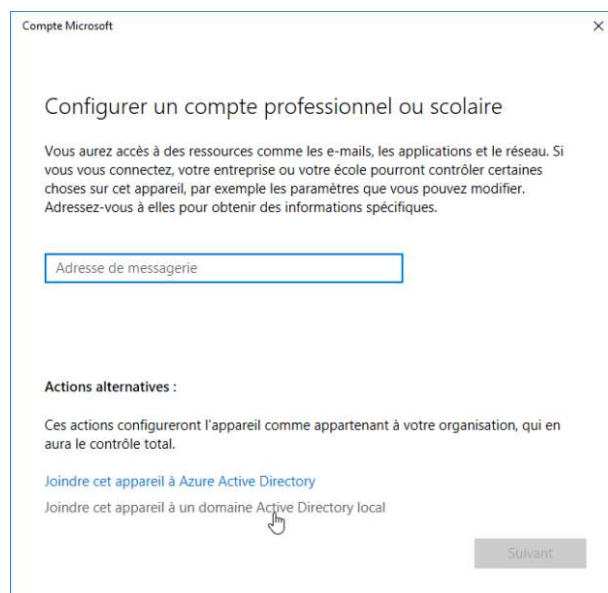
Ceci peut être paramétré soit sur le serveur DHCP dans le cas d'attribution automatique d'adresses IP aux postes clients, soit manuellement dans les paramètres de l'adaptateur réseau :



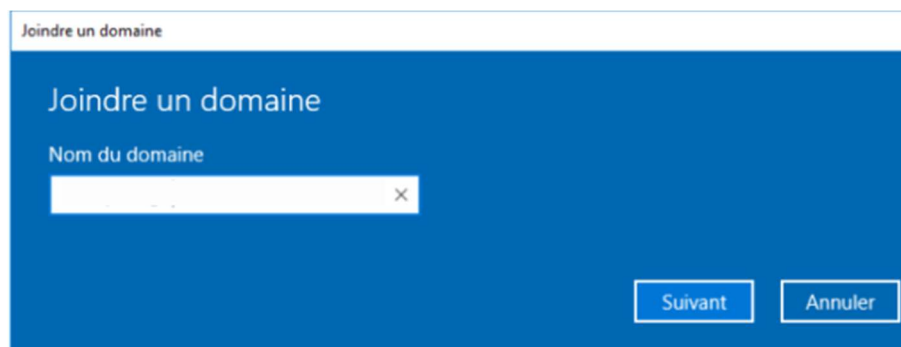
Sur Accès Professionnel ou scolaire on clique sur connecter



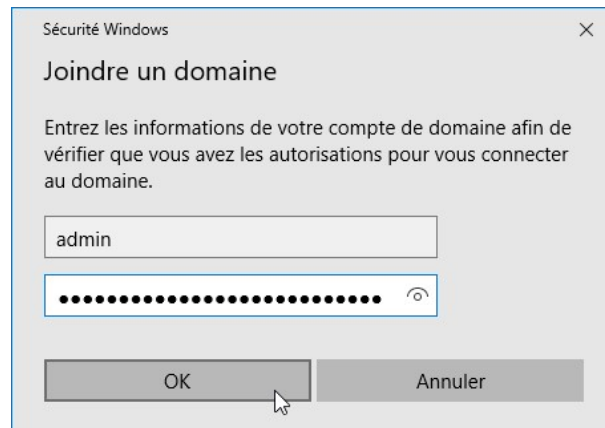
On clique ensuite sur joindre cet appareil a un AD



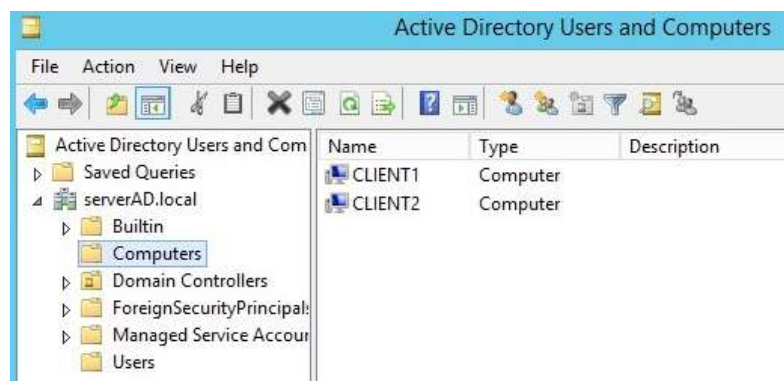
On saisit le nom du domaine et on clique sur suivant



Saisir le nom du compte administrateur du domaine ainsi que la clé secrète ("mot de passe") associée au compte et cliquer sur le bouton Ok



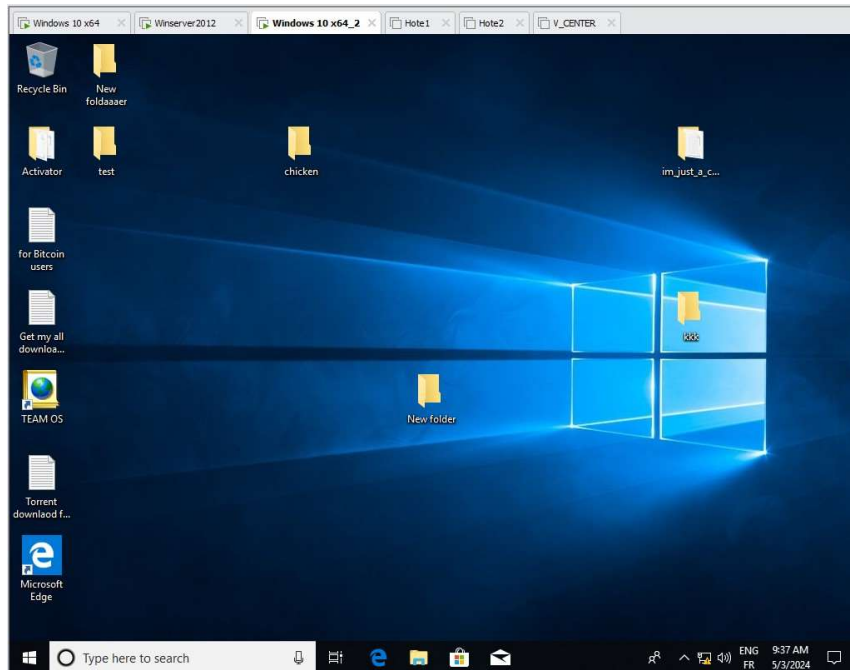
Après le redémarrage le Pc apparaît dans notre AD



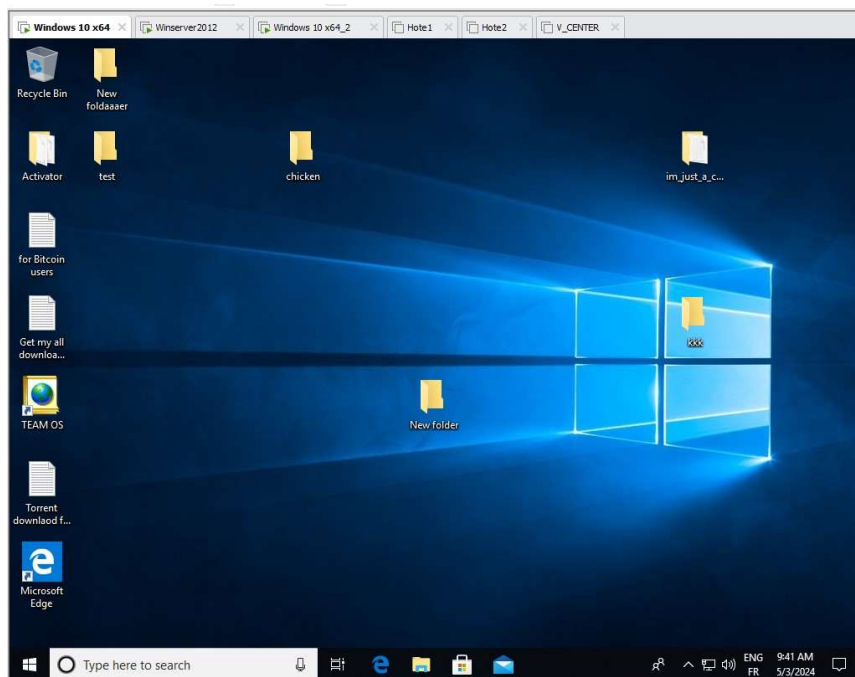
7- Test

A ce niveau On créer des dossier dans une machine dans un compte et essaie apres la fermeture de la session de tester dans une autre machine virtuelle client appartient a AD si les dossier apparait on non.

La 1^{er} VM :



La 2eme VM :



Conclusion

En conclusion, l'Active Directory se révèle être un outil crucial pour la gestion efficace des ressources au sein d'un réseau d'entreprise. En centralisant les informations sur les utilisateurs, les ressources matérielles et les applications, il simplifie l'administration et renforce la sécurité du système d'information. Son rôle essentiel dans la gestion des accès, la mise en place des politiques de groupe et la sécurisation des données en font un élément indispensable pour les administrateurs informatiques.

La mise en place d'un Active Directory, comme détaillé dans ce rapport, nécessite une compréhension approfondie de ses concepts de base, de son architecture et de son fonctionnement. Les étapes de création et de configuration d'un Active Directory, ainsi que l'intégration des postes clients, sont essentielles pour garantir son bon fonctionnement au sein d'un environnement informatique.

En outre, les avantages offerts par l'Active Directory, tels que la centralisation des données, la facilité de gestion des utilisateurs et des groupes, la sécurisation des ressources et la compatibilité avec d'autres annuaires de ressources, en font un choix judicieux pour les entreprises de toutes tailles.

En somme, l'Active Directory demeure un pilier de l'administration système dans les environnements Windows, offrant aux administrateurs les outils nécessaires pour gérer efficacement les ressources et assurer la sécurité des données au sein de leur réseau d'entreprise.