République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A.MIRA-Béjaia

Faculté des sciences Exactes
Département Informatique
Spécialité Administration et Sécurité des Réseaux informatiques

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme

MASTER

Thème

Configuration d'un réseau local en vue de partage des ressources informatiques via l'annuaire Active Directory

Cas pratique : Sonelgaz Bouira(Direction de Distribution)

Présenté par :

Aguerssif Razika

Oukoula Mohand Ameziane

Soutenu Le 02 Juillet 2024

Devant le Jury composé de :

Mme. Ouyahia Samira	**Président**
Mme. Belkhiri Louiza	**Encadrante**
Mme. Zidani Ferroudja	**Examinateur**

Année universitaire : 2023/2024

Remerciements

Je tiens à remercier : tous ceux qui de près ou de loin, ont contribué à l'élaboration de ce modeste travail.

Mes remerciements s'adressent essentiellement au personnel de l'entreprise Pour sa disponibilité et orientations.
Mes remerciements aussi à mon promoteur Mme L.BELKHIRI pour son encadrement.

Je remercie également tout le personnel de l'entreprise SONELGAZ ;Mr Bennani qui nos a soutenu énormément durant la période du stage.

Je suis honoré par la présence de membres du jury d'avoir accepté ce Travail en espérant qu'ils trouveront dans ce projet de quoi être satisfait Et auront la gratitude de l'enrichir avec leurs critiques et corrections.

Table des matières

Table des figures

*

Liste des tableaux

*

Introduction génerale

L'informatique est de plus en plus présente dans notre vie quotidienne. Nous comptons désormais sur les services offerts par les réseaux pour le fonctionnement des outils informatiques, que ce soit en entreprise, lors de transactions bancaires, dans les télécommunications et même dans les facultés. Ces services sont devenus quasi-indispensables. Pour assurer la qualité de ces services, il est nécessaire de surveiller le réseau et d'agir lorsqu'une erreur se produit. En d'autres termes, il faut administrer le réseau informatique.

Dans le souci de répondre efficacement aux besoins des entreprises, Sonelgaz Bouira a mis en place un réseau informatique pour faciliter les traitements et optimiser les temps de réponse. Sonelgaz s'est doté d'un parc informatique composé d'ordinateurs fonctionnant sur des systèmes d'exploitation propriétaires. Cependant, malgré cette infrastructure destinée à automatiser et faciliter les tâches de gestion courantes, des insuffisances persistent dans la gestion des ressources partagées et l'authentification des utilisateurs, ce qui engendre une vulnérabilité du réseau. Afin de relier tous les ordinateurs dans un même réseau et de permettre un accès sécurisé aux ressources partagées, il nous a été demandé de constituer un projet permettant de gérer l'authentification des utilisateurs dans le domaine, ainsi qu'une politique de partage et d'accès aux ressources au sein de ce réseau hétérogène. Le projet est subdivisé essentiellement en trois points : la mise en place d'un serveur de fichiers Active Directory pour gérer le partage des ressources, la mise en place d'un annuaire pour gérer les authentifications et d'un contrôleur de domaine (DC) pour unifier la gestion des droits sur les ressources et mieux définir les accès à celles-ci.

Dans ce mémoire, nous nous intéressons particulièrement à l'installation et à la gestion d'Active Directory, un service de répertoire développé par Microsoft, au sein de l'entreprise Sonelgaz de Bouira. Active Directory est largement utilisé pour la gestion des identités et des accès, ainsi que pour la configuration et l'administration des réseaux dans les environnements d'entreprise.

Ce mémoire est structuré en quatre chapitres principaux :

— Chapitre 1 (Notions générales sur les réseaux informatiques) : Nous commencerons par une présentation des concepts fondamentaux des réseaux informatiques. Ce chapitre abordera les différentes topologies de réseau, les protocoles de communication, ainsi que les matériels et logiciels essentiels pour le fonctionnement des réseaux modernes.

— Chapitre 2 (Étude de l'existant au sein de l'entreprise d'accueil (Sonelgaz de Bouira)) : Dans ce chapitre, nous procéderons à une analyse approfondie de l'infrastructure réseau actuelle de Sonelgaz. Cette étude permettra de comprendre les défis et les besoins spécifiques de l'entreprise en matière de gestion de réseau, et de poser les bases pour l'installation d'Active Directory.

— Chapitre 3 (Installation et déploiement d'Active Directory) : Ce chapitre détaillera les étapes nécessaires à l'installation et au déploiement d'Active Directory au sein de Sonelgaz. Nous décrirons les prérequis matériels et logiciels, les procédures d'installation, ainsi que les configurations initiales nécessaires pour intégrer Active Directory dans l'infrastructure existante.

— Chapitre 4 (Configuration et administration du réseau à l'aide d'Active Directory) : Enfin, nous aborderons la configuration et l'administration du réseau en utilisant Active Directory. Ce chapitre couvrira la gestion des utilisateurs et des groupes, la mise en place des politiques de sécurité, ainsi que les meilleures pratiques pour assurer une administration efficace et sécurisée du réseau.

Chapitre 1

Génariltés sur les réseaux informatique

Instroduction

Dans ce chapitre, nous abordons les caractéristiques fondamentales d'un réseau informatique, indispensables à la maîtrise pour tout administrateur réseau. Les réseaux informatiques représentent le socle de toute infrastructure technologique moderne, facilitant la communication, le partage de données et l'accès aux ressources. Une compréhension approfondie de ces caractéristiques est cruciale pour garantir le bon fonctionnement, la sécurité et l'efficacité d'un réseau. Nous examinerons donc les principaux éléments tels que l'architecture, les protocoles de communication, la sécurité, la gestion des utilisateurs et des ressources, ainsi que les compétences techniques nécessaires pour configurer et dépanner un réseau. En développant ces connaissances, les administrateurs réseau seront mieux équipés pour relever les défis constants de la gestion des réseaux informatiques.

1.1 Réseaux Informatiques

Un réseau informatique est un system de communication reliant plusieurs équipement informatique (matérielles et Logicielles) par des canaux de transmission (câbles, ondes, etc. . .) afin de répondre à un besoin d'échange d'informations.[1]

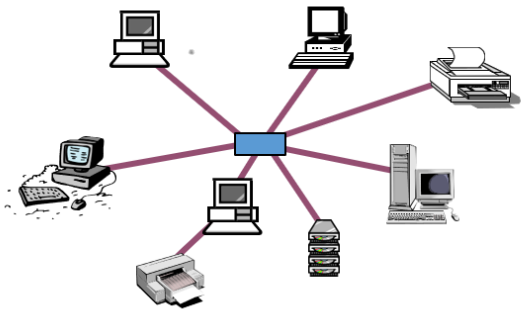


Figure 1.1 – schéma d'un réseau informatique

1.1.1 L'objectif d'utilisations d'un réseau informatique

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications, ou matériels, connexion à internet).
- La communication entre personne distant (courrier électronique, discussion en direct).
- La garantie de l'unicité de l'accès à l'information (bases de données).
- Centralisation de sauvegarde (sécurisation contre les risques comme le vol, la suppression.

1.1.2 Administrateur Réseau

L'Administrateur Réseau, appelé également Administrateur Systèmes et Réseaux, Gestionnaire Réseau ou Network Administrator, a pour rôle de garantir la bonne circulation de l'information au sein de l'entreprise en gérant et vérifiant le bon fonctionnement de son infrastructure informatique.

Les missions principales de l'Administrateur Réseau est d'assure la bonne circulation de l'information dans l'entreprise en veillant à la qualité, la compatibilité et la performance des équipements et du réseau de la structure. Ses fonctions vont de la résolution d'anomalies à la gestion des accès utilisateurs,en passant par le réglage des paramètres et la sécurisation du réseau.

1.2 Classification

1.2.1 Les réseaux PAN : (Personnels Area Network)

La plus petite étendue de réseau est nommée en anglais Personale Area Network(PAN), centrée sur l'utilisateur, elle désigne une interconnexion d'équipements Informatiques dans un espace d'une dizaine de mètres de celui ci. Il est appelé aussi réseau individuel ou réseau domestique.[1]

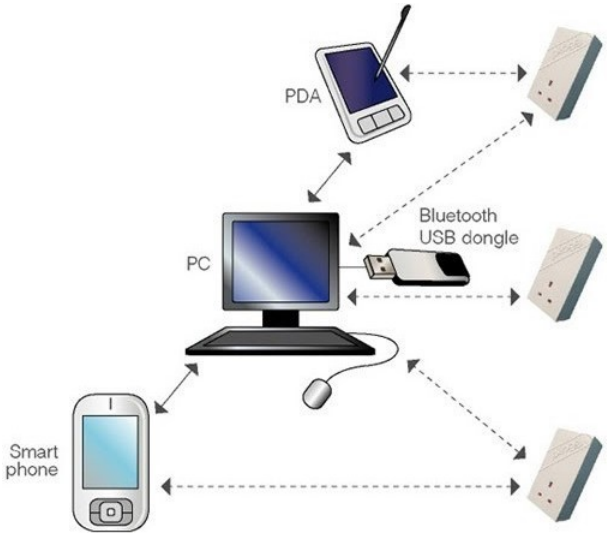


Figure 1.2 – schéma d'un réseau PAN.

1.2.2 Les réseaux locaux LAN : (Local Area Network)

Un réseau qui relais des ordinateurs et des périphériques situé les uns aux autres sur une même pièce au dans un même bâtiment. Il ne comporter pas plus de cent ordinateurs. Ce réseau est limité à une zone géographique réduite au maximum 5 kilomètres.[1]

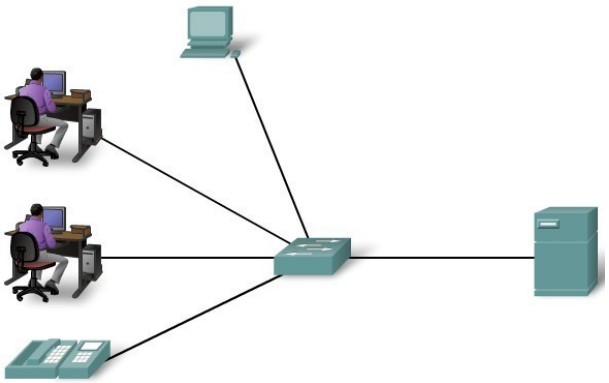


Figure 1.3 – schéma d'un réseau LAN.

1.2.3 Les réseaux métropolitains MAN : (Métropolitains Area Network) :

Constitue d'une série des réseaux locaux permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échèle d'une métropole pour leur donnée la possibilité de dialogué avec l'extérieur. Ce réseau est étendu sur une dizaine de kilomètres.[1]

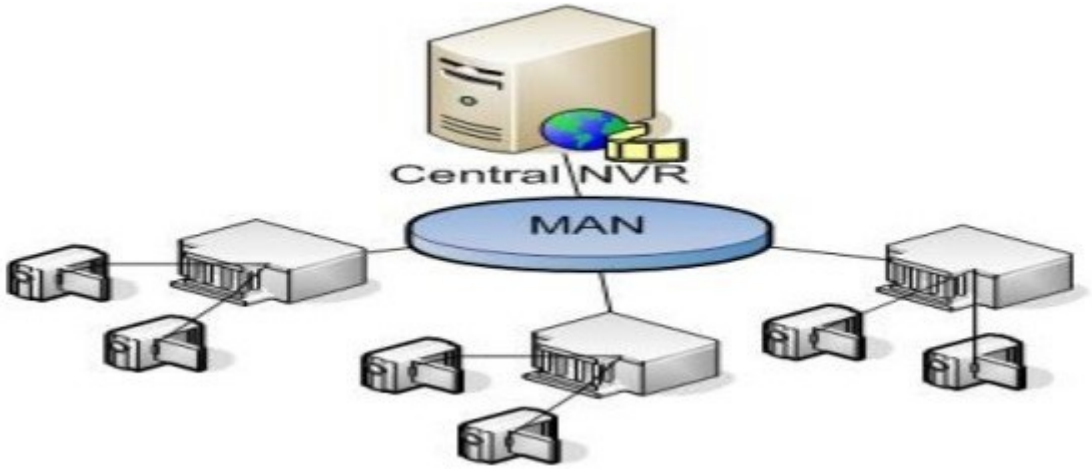


Figure 1.4 – schéma d'un réseau MAN.

1.2.4 Les réseaux distants WAN : (Wide Area Network) :

Destiné a transporté des données numériques sur des distances à l'échèle nationale, voire d'un continent ou plusieurs continents(Internet). Ilssont été terrestres, soientsatellitaires et ils relient des réseaux MAN et LAN.[1]

Figure 1.5 – schéma d'un réseau WAN.

1.3 Les topologies

1.3.1 Topologie en bus :

La topologie en bus est caractérisée par un câble central sur lequel tous les membres du réseau sont connectés, dans cette topologie le câble nécessite des bouchons aux extrémités qui ont pour rôle d'éviter la réflexion du signal électrique qui arrive à l'extrémité du câble.[2]

Figure 1.6 – schéma d'une topologie en bus.

1.3.2 Topologie en étoile :

Dans cette topologie qui est la plus utilisée, les ordinateurs sont reliés par des segments de câbles à un Composant central (HUB ou SWITCH).[2]

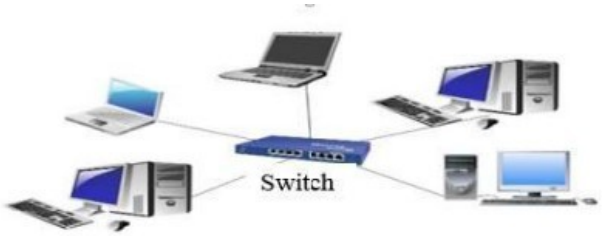


Figure 1.7 – schéma d'une topologie en étoile.

1.3.3 Topologie en anneau :

Dans cette topologie en anneau, les ordinateurs sont disposés de telle sorte que l'ensemble constitue une boucle fermée. (L'information circule dans un même sens surl'anneau).[2]

Figure 1.8 – schéma d'une topologie en anneau.

1.3.4 La topologie maillée :

Le réseau maillé est un réseau dans lequel deux stations de travail peuvent être mises en relation par différents chemins. La connexion est effectuée à l'aide de commutateur.[2]

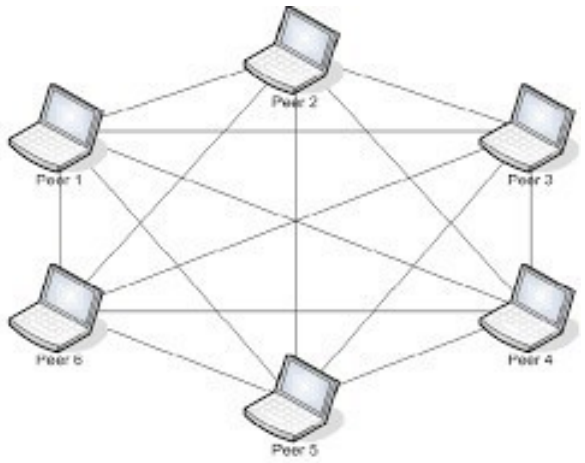


Figure 1.9 – schéma d'une topologie en maillée.

1.4 Les équipements

Dans les réseaux, nous retrouvons différents types d'équipements. Afin de faciliter leurs descriptions respectives, nous allons les présenter selon leur appartenance : les équipements réseaux, les postes de travail et les serveurs ;

1.4.1 Les équipements réseaux

- Répéteur : C'est un équipement électronique simple permettant d'amplifier un signal et d'augmenter la taille d'un réseau.[3]
- Concentrateur (Hub) : Il permet de concentrer le trafic réseau provenant de plusieurs hotes, il agit au niveau de la couche physique du modéle OSI.[3]
- Ponts (bridges) : Il permet de relier des réseaux travaillant avec le méme protocole. Ils travaillent au niveau de la couche 2 du modéle OSI (couche liaison).[3]
- Commutateur (Switch) : C'est un pont multiport c'est-a-dire qu'il s'agit d'un élément actif agissant au niveau de la couche 2 du modéle OSI.[3]
- Passerelle (Gateway) : C'est un systéme matériel et logiciel permettant de faire la liaison entre deux réseaux afin de faire l'interface avec le protocole du réseau différent.[3]
- Routeur : C'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de d´eterminer le chemin qu'un paquet de données va emprunter.[3]
- Layer 3 switch : est un appareil de réseau qui combine les fonctionnalités d'un switch de niveau 2 (Layer 2 switch) et d'un routeur.

Il est capable de commuter (switching) et de router (routing) des paquets de données au sein d'un réseau.[3]

1.4.2 Les postes de travail :

On peut considérer les postes de travail suivants :

- Station Microsoft Windows : Windows est actuellement préinstallé sur plus de 91 pourcent des ordinateurs personnels.
- Station GNU/Linux : C'est un systéme d'exploitation libre s'appuyant sur le noyau Linux et les outils GNU.
- Station Mac OS X et iOS : C'est des systémes préinstallés sur la ma jorité des ordinateurs et appareils mobiles vendus par Apple.

1.4.3 Les serveurs

- Nous distinguons les types de serveurs suivants [4] :
- Serveur DNS : Le serveur DNS joue un rôle crucial dans la gestion et la résolution des noms de domaine, rendant la navigation Internet intuitive et accessible.
- Serveur de fichiers : Il conserve les fichiers partagés par plusieurs ordinateurs dans un emplacement commun. Un utilisateur peut extraire un document depuis son ordinateur, le traiter et l'enregistrer de nouveau sur le serveur.
- Serveur DHCP : Il simplifie la gestion des réseaux en automatisant l'attribution des adresses IP et des configurations réseau, ce qui est particulièrement utile dans les réseaux de grande taille.
- Serveur d'impression : Il permet de partager une ou plusieurs imprimantes.
- Serveur de messagerie : Il gére les messages en distribuant le courrier électronique aux ordinateurs et en les stockant de maniére a permettre un accés a distance.

1.5 les supports de transmission :

La première chose à mettre en œuvre pour constituer le réseau est la transmission des informations d'un équipement à l'autre, on utilisant des supports de transmission. C'est le support qui relie les ordinateurs entre eux.[5]

Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants :

1.5.1 avec fil :

— Le câble coaxial supporte un débit de 10 Méga bits par seconde (10 Mips) ; il est constitué d'un conducteur central en cuivre, d'un isolant puis d'un deuxième conducteur se forme de métal tressé, assurant le blindage et en fin dune gaine isolante assurant la protection mécanique de l'ensemble comme se figure au dessus :

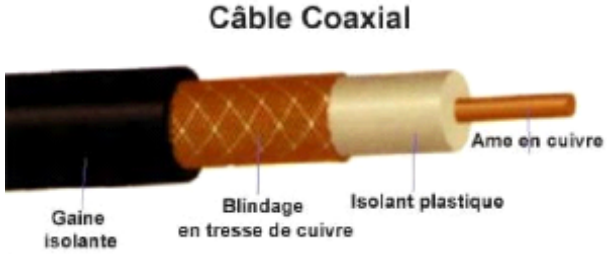


Figure 1.10 – le câble coaxial.

— La paire torsadée ressemble à un câble téléphonique. Suivant sacatégorie elle supporte de 10 à 100 Mbps sur 100 mètres.

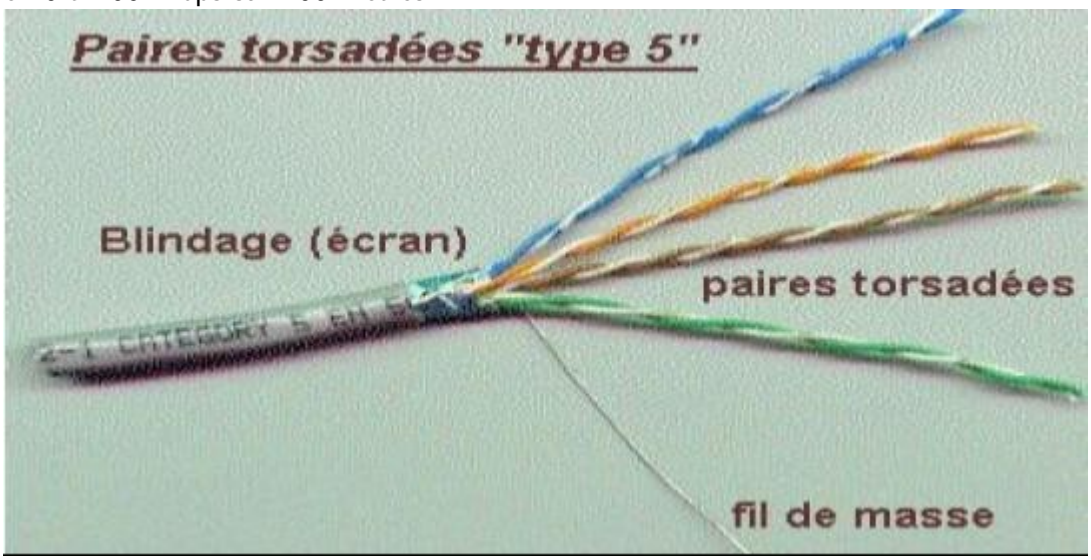


Figure 1.11 – la paire torsadée.

— La fibre optique maintient un débit de 155 Mbps à 10 Gbps Sur plusieurs kms. La fibre transfert les données se forme d'impulsions lumineuse modulée.

Figure 1.12 – la fibre optique.

1.5.2 Sans fil :

— Infra rouge : L 'IrDA, appelé infrarouge, est encore aujourd'hui une technologie de transmission sans fil très répandue (PC portable, PDA, téléphone portable, etc.). Le protocole IrDA est conçu pour le transfert des données, en utilisant la lumière infrarouge. Avec une connectivité rapide, sans installation. Faible coût. sécurisation de transmission.

— Bluetooth : La technologie Bluetooth est une technologie de réseaux sansfils d'une faible portée, de l'ordre de quelques dizaines mètres à un peu moins d'une centaine de mètres, permettant de relier des périphériques (imprimantes, téléphones portables, appareilsdomestiques, oreillettes sans fils, souris, clavier, etc.) et desordinateurset assistants personnels (PDA) entre-deux sans liaison filaire.

  — Il a comme Avantages : Faible consommation d'énergie, Bonne gestion de la communication de la voix. Equipements de taille réduite.Technologie adaptéeà la mobilité et un Faible coût.

  — Inconvénients : Nombre de périphériques limité dans un réseau Faible porté et un Débit limité.

— Wifi : La Wifi, pour Wireless Fidélité, est une technologie standard d'accès sans fil à des réseaux locaux. Le principe est d'établir des liaisons radio rapides entre des équipements et des bornes reliées aux réseaux Haut Débit. Grâce au Wifi, il est possible de créer des réseaux locaux sans fils à haut débit.

Le Wifi possède deux modes de fonctionnement : Le mode infrastructure auquel se connectent toutes les stations (appareils équipés d'un équipement Wifi) à un point d'accès ou un routeur, et le mode ad-hoc où les stations se connectent les unes aux autres sans passer par un point d'accès.

— Wi max : le Wi max est un standard de transmission sans fil à haut débit. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wifi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut débit vers de multiples utilisateurs.

1.6 L'architecture des réseaux :

1.6.1 Le réseau poste à poste (Peer to Peer) :

Chaque poste connecté est à la fois serveur lorsqu'il met ses ressources (imprimantes,dossiers) à disposition des autres postes, et client lorsqu'il bénéficie des ressources des autres postes. Il n'existe pas de gestion centralisée des ressources du réseau. Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et desécurité que les logiciels réseaux pour serveurs dédiés. Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.[9]

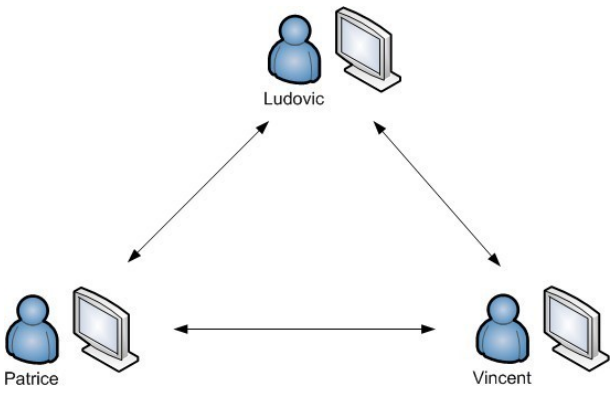


Figure 1.13 – architecture poste à poste.

Avantages

— L'architecture d'égal à égal est simple à mettre en œuvre et son coût est réduite par rapport au coût engendré par la mise en œuvre d'une architecture client/serveur

— La mise hors service d'un poste n'atteint pas gravement le fonctionnement du reste du réseau.

Inconvénients

— Ce système n'est pas centralisé, ce qui le rend très difficile à administrer.

— La sécurité est plus difficile à assurer.

1.6.2 Le réseau client / serveur :

Un ou plusieurs ordinateurs appelés serveur assurent des fonctions centralisées d'administration qui permettent d'authentifier des utilisateurs et de leurs accorder des permissions sur les ressources du réseau.[9]
Lesserveurs peuvent être spécialisés :serveur de fichiers, d'application,d'impression, de communication. Ils offrent des services à des programmes clients (client de messagerie, de base de données anti- virales, etc...)

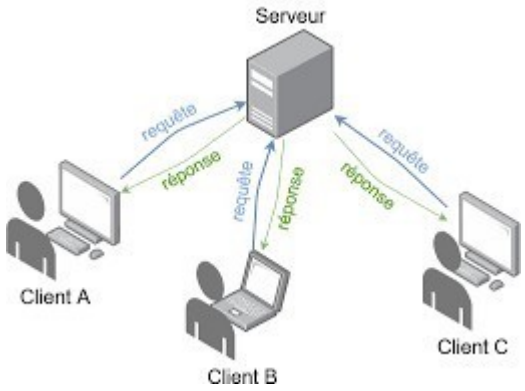


Figure 1.14 – architecture client/serveur.

Avantages

— Des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, commepar exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
— Une meilleure sécurité : car le nombre de points d'entrée permettant l'accès aux données est moins important.
— Une administration au niveau serveur : les clients ayant peu d'importance dans ce modèle,ils ont moins besoin d'être administrés.
— Un réseau évolutif : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

inconvénients

— Un coût élevé dû à la technicité du serveur.
— Un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui.

Ainsi, les réseaux égal à égal sont préférentiellement utilisés pour des applications nenécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

1.7 Les modèles de communication :

1.7.1 Le modèle OSI :

Créé par l'Organisation internationale de normalisation, le modèle conceptuel OSI (Open System Interconnexion) permet à divers systèmes de communication de communiquer à l'aide de protocoles standard. En clair, l'OSI constitue une norme permettant à différents systèmes informatiques de communiquer entre eux.
L'architecture organisée en 7 couches pour faire transiter les données d'une extrémité à une autre d'un réseau.[6]

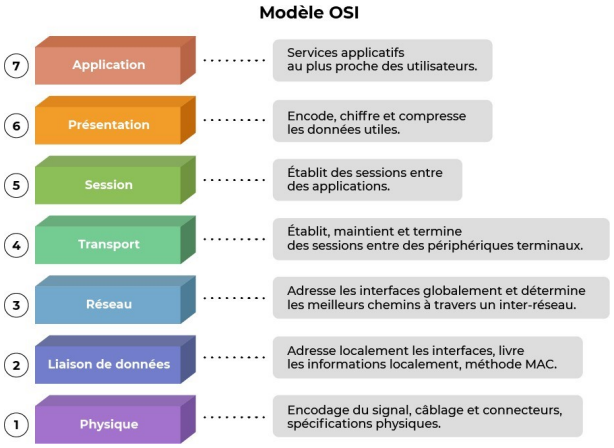


Figure 1.15 – l'architecture de modèle OSI.

1.7.2 modèle TCP/IP

TCP/IP représente l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des données. Le modèle TCP/IP n'est pas vraiment eloingné de modele OSI. Il ne presente cependant que 4 couche, meme si un modele Hybrid, séparent les couches physique et liaison peut faire autorité.[7]

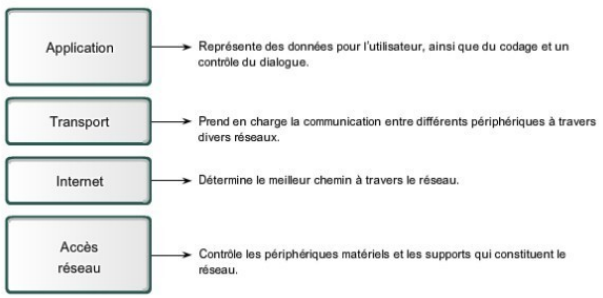


Figure 1.16 – l'architecture de modèle TCP/IP.

1.7.3 Comparaison entre le modèle OSI et TCP/IP

Le modèle OSI est donc plus facile à comprendre, mais le modèle TCP/IP est le plus utilisé en pratique. Il est préférables d'avoir une connaissance du modèle OSI avant d'aborder TCP/IP, carles mêmes principes s'appliquent, mais sont plus simples à comprendre avec le modèle OSI.

1.8 Les protocoles

Un protocole est une méthode standard qui permet la communication entre deux machines. Ensemble de règles et de procédures à respecter pour émettre et recevoir des donnéessur le réseau[8]. Parmi lequel on site :

TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) : Défini la norme de communication, (en fait un ensemble de protocoles) des ordinateurs reliés à Internet. Ce modèle définit les règles que les ordinateurs doivent respecter pour communiquer entre eux sur le réseau Internet

SMB/CIFS

SMB/CIFS (Server Message Block / Common Internet File System) :est un protocole de partage de fichiers réseau qui permet aux applications de lire et d'écrire des fichiers ainsi que de demander des services à des programmes serveur sur un réseau informatique.

Il existe d'autre protocole comme :

- DNS permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (un peu comme un annuaire).
- FTP sert à transporter des fichiers d'un ordinateur à l'autre.
- IRC permet de créer des salons de discussion en direct.
- ICQ permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.
- NTP permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes près.
- P2P permettent de partager des fichiers à grande échelle.
- NNTP permet d'accéder à des forums de discussion sur des milliers de sujets différents.
- SSH permet d'avoir un accès sécurisé à des ordinateurs distants.
- SMTP permet d'envoyer des emails, et le protocole POP3 de les recevoir.
- SMB (Server Message Block) : C'est un protocole de communication réseau principalement utilisé pour fournir un accès partagé aux fichiers, imprimantes et ports série entre les nœuds d'un réseau.
- CIFS (Common Internet File System) : Une version améliorée de SMB, CIFS est souvent utilisé comme synonyme de SMB, bien que techniquement, CIFS soit une version spécifique de SMB (SMB1).

1.9 Adressage réseau :

1.9.1 Adresse physique :

En informatique, une adresse physique fait référence soit à un emplacement mémoire, identifié sous la forme d'un numéro binaire, soit à une adresse MAC (Media Access Control).Une adresse physique est également connue comme une adresse binaire ou une adresse réelle.

Adresse MAC : (Media Access Control)

L'adresse MAC est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire est constituée de douze caractères alphanumériques (hexadécimaux), c'est-à-dire de 0 à 9 et de A à F. Au niveau de son écriture, nous retrouvons des blocs de deux caractères, la plupart du temps sous l'une de ces formes (en fonction des équipements) : Ce qui nous donne par exemple : B4-6D-83-DD-CE-49.

Affichage de l'adresse MAC :

Pour afficher l'adresse MAC de PC, ils fournissent une commande spécifique pour taper sur coquille texte ; cette commande sous Windows ipconfig / all (ifconfig Linux), tandis que la commande arp -a affiche l'ensemble cache Arp d'un réseau local auquel le PC est connecté.

1.9.2 Adresse logique :

L'adresse générée par le processeur pendant l'exécution d'un programme est appelée adresse logique. L'adresse logique est virtuelle car elle n'existe pas physiquement. Par conséquent, il est également appelé en tant qu'adresse virtuelle. Cette adresse est utilisée comme référence pour accéder à l'emplacement de la mémoire physique. L'ensemble de toutes les adresses logiques générées par un programme s'appelle l'espace d'adressage logique.

Adresse IPv4 :

Une adresse IPv4 (Internet Protocol version 4) est une identification unique pour un hôte sur un réseau IP. Une adresse IP est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. La notation est aussi connue sous le nom de "décimale pointée".

Format d'adresse IPv4 :

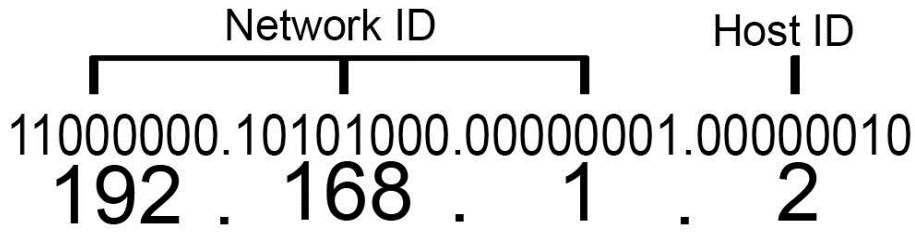


Figure 1.17 – format de l'adresse IPv4.

Types de communication IPv4 :

Un hôte connecté à un réseau peut communiquer avec les autres périphériques de trois façons :

- La monodiffusion : processus consistant à envoyer un paquet d'un hôte à un autre.
- La diffusion : processus consistant à envoyer un paquet d'un hôte à tous les autreshôtes du réseau.
- La multidiffusion : processus consistant à envoyer un paquet d'un hôte à un groupe-d'hôtes spécifique (qui peuvent se trouver sur différents réseaux).

Type d'dresse IPv4

- Adresse réseau : adresse IP dont la partie hôte est composée de zéros.Exemple : 192.168.1.0
- Hôte : ordinateur ou autre périphérique sur un réseau TCP/IP.Exemple : 192.168.1.14
- Adresse de diffusion : adresse IP dont la partie hôte est composée de "1".

Les classes d'adresses IPv4 :

Classe A :

Les adresses de la classe (A) ont deux parties, une partie réseau sur 8bits, et une partie hôte sur 24 bits. Son masque de sous réseau est 255.0.0.0

Classe B :

Les adresses de la classe (B) ont une partie réseau sur 16 bits, et unepartie hôte de la même taille. Son masque de sous réseau est 255.255.0.0

Classe C :

Les adresses de classe (C) ont une partie réseau sur 24 bits, et une partiehôte sur 8 bits. Son masque sous réseau est 255.255.255.0

Classe D :

Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits depoids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes(host groups)

Classe E :

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

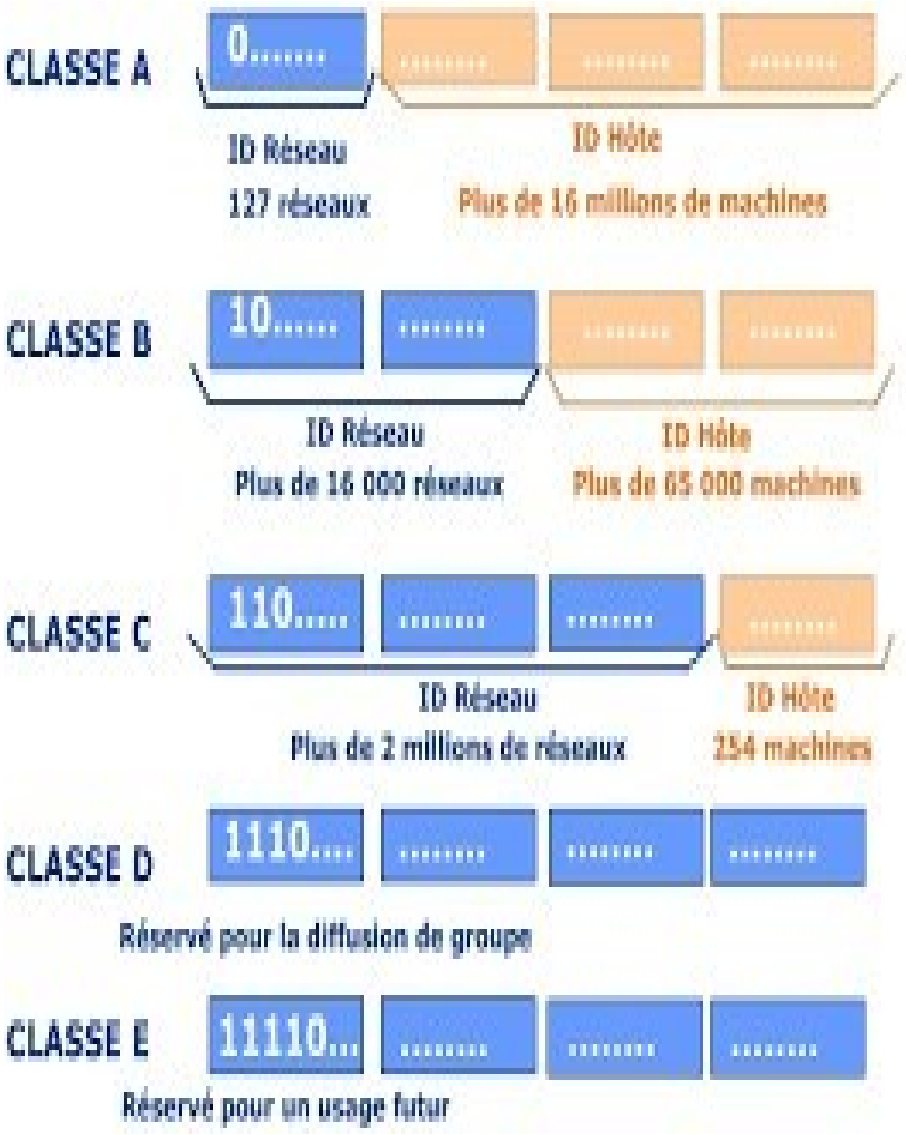


Figure 1.18 – Les classes d'adressage IPv4.

Les adresses réservées :

L'espace d'adressage réservé est le groupe d'adresses IP (Internet Protocol) réservées et catégorisées uniquement pour une utilisation avec des réseaux internes ou des intranets, voici quelques exemples :

Les adresses publiques :

Les adresses publiques sont des adresses routables, c'est-à-dire qu'elles permettentd'être identifié sur le réseau internet et donc d'échanger des informations via Internet.

Les adresses privées :

Les adresses privées sont destinées à un usage privé ; c'est-à-dire qu'un routeur n'achemine pas cette adresse sur Internet. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

- Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
- Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
- Classe C : plage de 192.168.0.0 à 192.168.255.55 ;

1.10 Attaques et moyens de sécurité réseau :

Le réseau local constitue l'épine dorsale de la plupart des opérations informatiques de nos organisations. En conséquence, il est impératif de garantir sa sécurité. Cette importance cruciale justifie pleinement la nécessité de consacrer une attention particulière à la sécurisation des réseaux locaux.

Par ailleurs, il est généralement estimé que la majorité des malveillancesinformatiques ont une origine complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significatives des pertes par rapport aux deux autres accidents et erreurs) .devant cette spécificité il donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local dés sa conception.

Il est donc nécessaire d'établir des configurations de systèmes d'exploitation comprenant leurs réseaux et multiples branches, sécurisés avec les techniques les plussophistiquées en matière de firewalls et de contrôles d'accès.

1.10.1 Les attaques réseau courantes :

Dans les attaques réseau courantes, nous trouvons plusieurs, nous citerons :

Attaques de reconnaissance

Des pirates externes peuvent utiliser des outils Internet, comme les utilitaires nslookup et whois, pour découvrir facilement les adresses IP attribuées à une entreprise ou à une entité donnée. Une fois ces adresses IP connues, l'assaillant peut lancer des requêtes ping vers les adresses publiquement accessibles pour déterminer celles qui sont actives.[11]

Attaques d'accès

Ces attaques exploitent les vulnérabilités connues des services d'authentification, services FTP (File Transfer Protocol) et services Web pour accéder à des comptes Web, des bases de données confidentielles et d'autres informations sensibles. Une attaque par accès permet à une personne d'obtenir un accès non autorisé à des informations qu'elle n'a pas le droit de consulter.[12]

Attaques d'ingénierie sociale

Une attaque par ingénierie sociale manipule la cible pour accéder à des informations confidentielles. Le criminel emploie des tactiques de manipulation (l'exploitation émotionnelle, par exemple) pour que la cible lui confie des informations confidentielles telles que ses codes d'accès ou mots de passe.[13]

Attaques par déni de service (DOS)

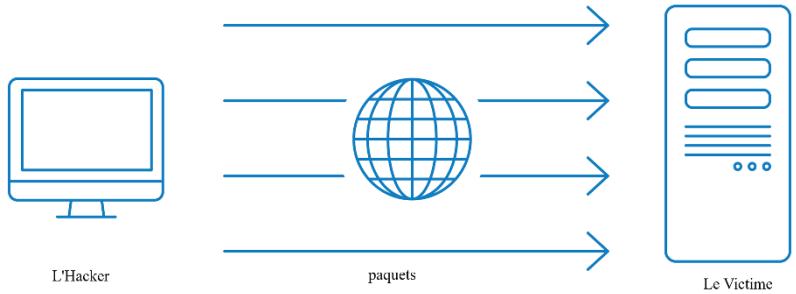


Figure 1.19 – Attaque par DoS

Une attaque DOS (Denial of services) consiste à saturer les ressources d'un système de façon à empêcher son bon fonctionnement, en lui envoyant des milliers de paquets IP depuis la machine de l'hacker. L'hacker ne s'infiltre généralement pas dans des réseaux informatiques et n'a donc pas besoin de mots de passe ou d'autres moyens d'accès similaires, ce qui rend cette technique possible et simple à réaliser.[14]

1.10.2 La politique de Sécurité réseau :

La politique de sécurité est une démarche de toute entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité pour son activité. La politique de sécurité réseau fait éventuellement partie de la démarche sécuritaire de l'entreprise.
Tout d'abord, elle doit déterminer les éléments critiques qui est une tache très délicate en passant par une analyse de risque qui consiste à identifier les ressources ou les biens vitaux de l'entreprise .Ces derniers peuvent être de plusieurs ordres : matériels,données ,logiciels et personnes.

1.10.3 Principe d'une politique de sécurité réseau :

La politique de sécurité réseau vise à satisfaire les critères suivants :

- Authentification : information permettant de valider l'identité pour vérifier que la personne est celle qui prétend l'être .
- Identification : information permettant d'indiquer la personne inscrite.
- Autorisation : information permettant d'indiquer les ressources de l'entreprise auxquelles un utilisateur identifié aura accès ainsi que les actions autorisées sur ses ressources.
- intégrité : regroupe les mécanismes garantissant qu'une information n'à pas été modifiée ou altérée.
- Disponibilité : regroupe les mécanismes garantissant que les ressources de l'entreprise sont accessibles.
- non-répudiation : mécanisme permettant de prouver qu'un message a bien été envoyé par un émetteur et reçu par un récepteur.

La politique de sécurité réseau couvre les éléments suivants :

- sécurité d'accès : détermine la sécurité d'accès aux ressources de l'entreprise que soit localement ou via un accès distant, ainsi que la gestiondes utilisateurs et leurs droit d'accès aux systèmes d'information de l'entreprise.
- écurité de l'infrastructure : couvre la sécurité des équipements et des connexions réseaux.
- sécurité de l'intranet face à internet : couvre la sécurité logique des accès aux ressources de l'entreprise et l'accès aux ressources extérieures (internet).

1.10.4 Solutions de sécurité réseau

Une bonne stratégie de sécurité vise à mettre en ouvre des mécanismes de sécurité ; des procédures de surveillance des équipements de sécurité, des contrôles et audits desécurité.

Système de détection d'intrusion (IDS) :

Les IDS (Intrusion Detection System) et les IPS (Intrusion Prevention System) font tous deux partie de l'infrastructure réseau. Les IDS/IPS comparent les paquets de réseau à une base de données de cybermenaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures. La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle . L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu. Les solutions IDS (Intrusion Détection System) pour un réseau garantit unesurveillance permanente du réseau.[15]

Utilisation de sessions :

L'exigence d'avoir au moins deux sessions pour chaque poste dans un réseau local de l'entreprise , une pour l'utilisateur avec privilège restreint de préférence pour ne pas modifier la configuration initiale et la deuxième pour l'administrateur qui est le seul à pouvoir modifier les paramètres de base. Une authentification par Login et Mot de passe est obligatoire.[16]

VPN :

Le VPN (Virtual Privat Network) représenter un réseau privé virtuel crypté, permettant à une société dont les locaux sont géographiquement dispersés, de communiquer et partager des documents de façon sécurisée, comme s'il n'y avait qu'un réseau interne. L'objectif d'un VPN est créer un lien virtuel (tunnel) entre deux points connecté pour permet la sécurisation et le chiffrement des données de bout en bout. Le chiffrement est effectué en temps réel.[17]

Solution Firewall :

La solution de filtrage consiste à déployer trois niveaux de filtrage surles ressources du réseau[18], comme écrit ci-dessous :

— Firewall à filtrage de paquets : La majorité des équipements de routage actuels disposent d'une fonctionnalité de firewalling basé sur le filtrage de paquets. Cette technique permet de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC.

- Firewall State full Inspection : Cette solution sera implémentée par un équipement firewall matériel qui agit en tant que passerelle, afin de garantir la sécurité entre le trafic du réseau interne, public et démilitarisé Au niveau architecture du réseau, le firewall propose trois domaines de sécurité :
  - Zone interne : Représente le réseau local de l'organisme. Cette zone contientle plus haut niveau de sécurité
  - Zone externe : représente la zone publique par laquelle passe tout le trafic dedestination internet.
  - Zone démilitarisée : représente la zone contenant les serveurs visibles del'extérieur dont l'accès est public.
- Firewall Applicatif : Un Firewall applicatif sera installé sur tous les postes client et les serveurs afin de protéger en premier lieu des tentatives d'intrusion interne. L'utilisation d'un firewall applicatif permet de contrôler les connexions depuis et versces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants.

Les antivirus :

Un antivirus est logiciel informatique destiné à identifier et à effacer des logiciels malveillants,également appelés virus, Chevaux de Trois ou vers selon les formes.[19]

l'Annuaire :

Un annuaire permet de stocker des données légèrement typées, organiséesselon des classes particulières et présentées dans un arbre. On peut trouver des solutions d'annuaire comme LDAP, c'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leur valeur : la racine O 'organisation' , le sous ensemble d'une organisation ou 'organisation Unit', le nom de domaine DC 'Domain Component ' et la personne Person schéma standard pour une personne .[20]
Exemple : Le service d'annuaire Active Directory

déploiement complet d'Active Directory :

Active directory fournit des services centralisés de Gestion des ressources etde la sécurité, il permet également l'attribution et l'application de stratégies.
Le contrôle d'accès peut être défini non seulement sur chaque objet de l'annuaire, mais aussi sur chaque propriété de chacun des objets. Active Directory fournit à la fois le magasin et l'étendue de l'application pour les stratégies de sécurité.[21]

Une stratégie de sécurité peut inclure des informations de compte, telles que des restrictions de mot de passe applicables sur l'ensemble du domaine ou des droitspour des ressources de domaine spécifiques. Les stratégies de sécurité sont mises en place par le biais des paramètres de stratégiede groupe. Ainsi les avantages d'Active directory est :

- Amélioration de la tolérance de pannes pour réduire les périodesd'indisponibilité.
- Amélioration de la sécurité.
- Amélioration de la productivité des utilisateurs.
- Réduction des tâches d'administration informatique.

Conclusion :

Ce chapitre à montré des notions sur les réseaux informatiques tel que les différents types de réseau, les modèles OSI et TCP/IP. Ainsi qu'une vue brève sur les solutions de sécurité d'un réseau au sein de l'entreprise.

Chapitre 2

Etude de l'organisme d'acceuille

Introduction

Au cours de ce chapitre, nous allons nous consacrer à l'étude de l'existant pour comprendre le fonctionnement de l'organisme d'accueil, et mettre en évidence les différents documents manipulés et aussi les acteurs intervenant dans ce système, et leurs besoins.

2.1 Présentation de l'organisme d'accueil :

2.1.1 Historique de Sonelgaz

La SONELGAZ (société nationale de l'électricité et du gaz) est une compagnie chargée de la production, transport et distribution de l'électricité et du gaz en Algérie. Elle a été créée par ordonnance N°69.59 de 28 juillet 1969 autres fois dénomme E.G.A (Électricité et gaz d'Algérie) parue au journal N°69 lui-même crée en 1948 lors de la normalisation de l'électricité et du gaz inscrits au registre de commerce d'Alger sous le N°84B411 du 20/11/1984 dont le siège est à Alger.

Cette entreprise est l'une des plus importantes sociétés du pays, elle détient le monopole de la production, le transport et la distribution de l'électricité et du gaz, elle fournit toutes les capacités (humaines et matérielles) pour l'amélioration de sa productivité afin de répondre aux besoins de tous les secteurs du pays.

La Société Algérienne de Distribution de l'Électricité et du Gaz, dénommée " SADEG. Spa ", société par actions et dont le siège social est situé au niveau de l'immeuble 500 bureau- Route nationale n°38- Gué de Constantine- Alger, gère à travers ses soixante-cinq (65) Directions de Distribution, 58 concessions électricité et gaz s'étendant sur le territoire national. De par ses missions et attributions, la SADEG met au service de ses clients pas moins de 187 Districts Électricité et 186 Districts Gaz ainsi que 405 agences commerciales.[D]

2.1.2 Présentation de Sonelgaz de Bouira (Direction de Distribution)

Il s'agit d'une direction chargée dans les limites de ses compétences de la distribution de l'énergie, de l'électricité et du gaz et répondant aux besoins du client en termes de coût, de qualité des services et de sécurité. Il dispose de 10 agences commerciales qui existent comme suit (Bouira,Lakhdaria, Sour El-Ghozlane, Ain Bessem, M'Chedallah, Bechloul, El-Hachimia, Bordj-Okhris, Larbi Ben-M'hidi) et 05 districts d'électricité et gaz qui existent comme suit (Bouira, Lakhdaria, Ain Bessem, Sour El-Ghozlane, M'Chedallah).

La Direction de la Distribution est située rue du 19 mars 1962 au centre de Bouira, comme le montre la figure ci-dessous :

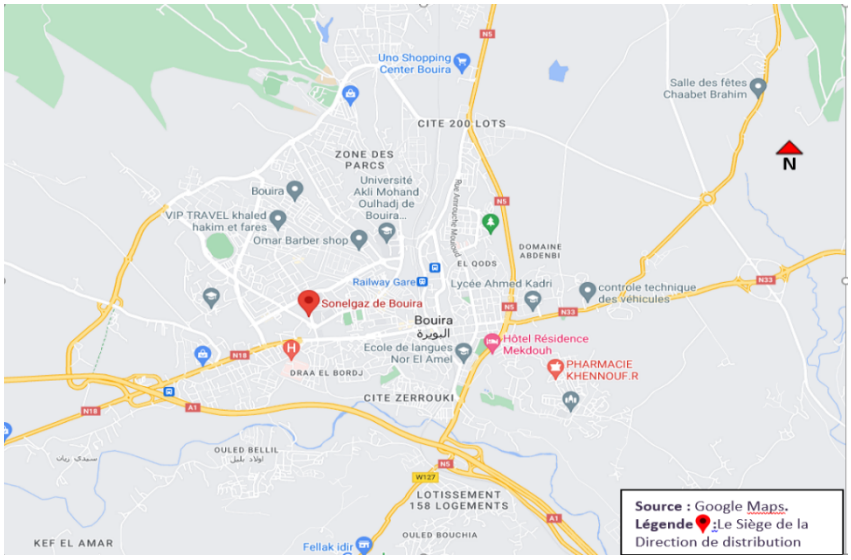
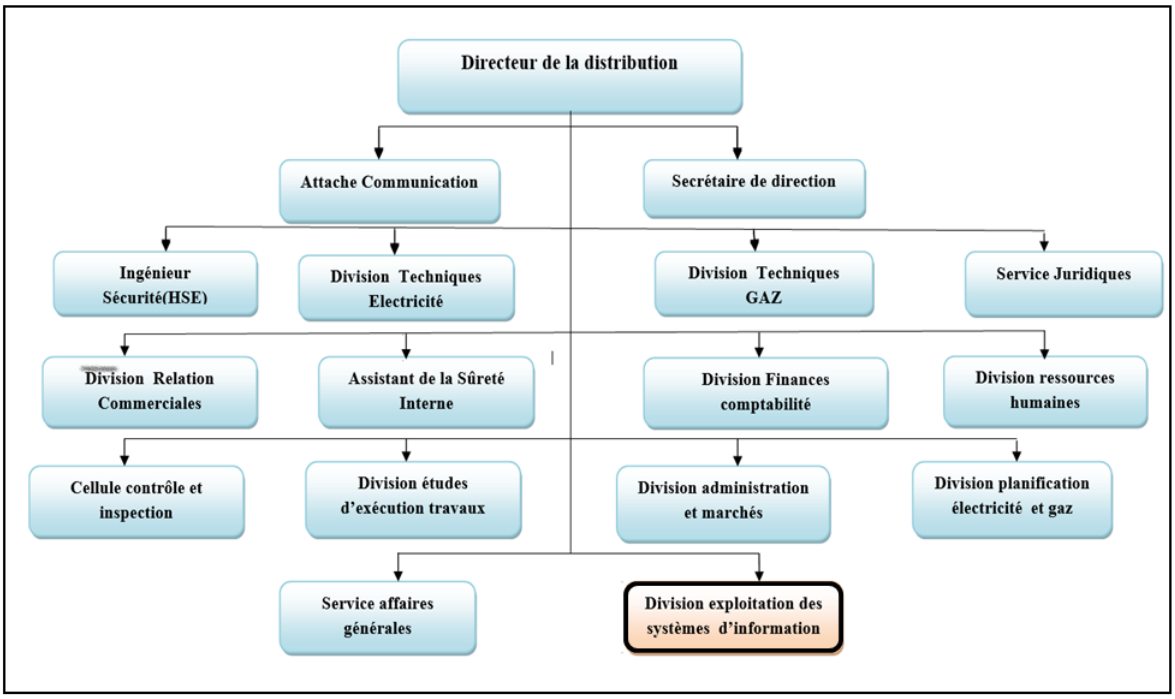


Figure 2.1 – Localisation de la direction de la distribution.

Organigramme

L'organigramme hiérarchique de la direction de distribution est le suivant :



Source : Direction de distribution Bouira.
Légende : champ d'étude

Figure 2.2 – Organigramme de la direction de distribution.

2.1.3 Division exploitation des systèmes d'informations (DESI)

Nous effectuons notre stage au sein de la DESI (Direction des Systèmes d'Information). Nous nous intéressons donc particulièrement à cette division pour comprendre les différentes tâches et responsabilités qu'elle assume. La DESI est chargée de :

- Gérer l'ensemble du matériel informatique et périphérique affecté à la direction de distribution ;
- Installer des systèmes d'exploitation ;
- Gestion des différentes bases de données ;
- Administrer et configurer les comptes TENSIK (open, ex-change) Messagerie professionnelle pour une communication efficace rapide et sécurisée, et toutes les fonctionnalités nécessaires pour gérer efficacement le travail collaboratif ;

— Installer, configurer, mettre à jour et réparer les systèmes d'exploitation ;
— Participer aux projets de développement internes en collaboration avec la direction générale ;
— Administrateur réseau local (LAN) et Télécoms ;
— Gérer les comptes utilisateurs et droits d'accès aux ressources logicielles et matérielles présentes sur le serveur et le réseau ;
— Mettre en œuvre et déployer une stratégie de sécurité informatique ;
— Installer un anti-virus client-serveur et déploiement ;
— La téléphonie IP : c'est la voix sur réseau IP, technique qui permet de communiquer par voix à distance via le réseau internet ;
— Gestion du réseau : Direction de Bouira dispose d'un réseau d'internet compose 5 Vlan, il est constitué de plusieurs équipements 10 Switch L3 un Firewall et salle de serveur ;
— Diagnostiquer et réparer Installer et mettre à jour les systèmes d'exploitation et utilitaires ;
— Conseiller et assister les utilisateurs ;
— La gestion et administration de la téléphonie IP (c'est la voix sur réseau IP).

2.2 Etude du réseau existant

L'organisme d'accueil à sa disposition différents moyens physiques et logiques et l'achitecture de son réseau local est :

2.2.1 Architecteur de réseau local existant

La figure ci-dessous, illustre l'architecture de réseau de l'entreprise : l'architecture de réseau local (LAN) d'entreprise est segmentée en plusieurs VLANs (Virtual Local Area Networks) pour améliorer la gestion et la sécurité du réseau. Voici une explication du segment VLAN 0 (10.64.0.0/24) :

— Ce VLAN contient le serveur principal et les ressources de stockage de l'entreprise.
— Il y a également des ordinateurs et des téléphones connectés.
— Le serveur est un point central, utilisé pour les services comme Active Directory, les bases de données, et les fichiers partagés.

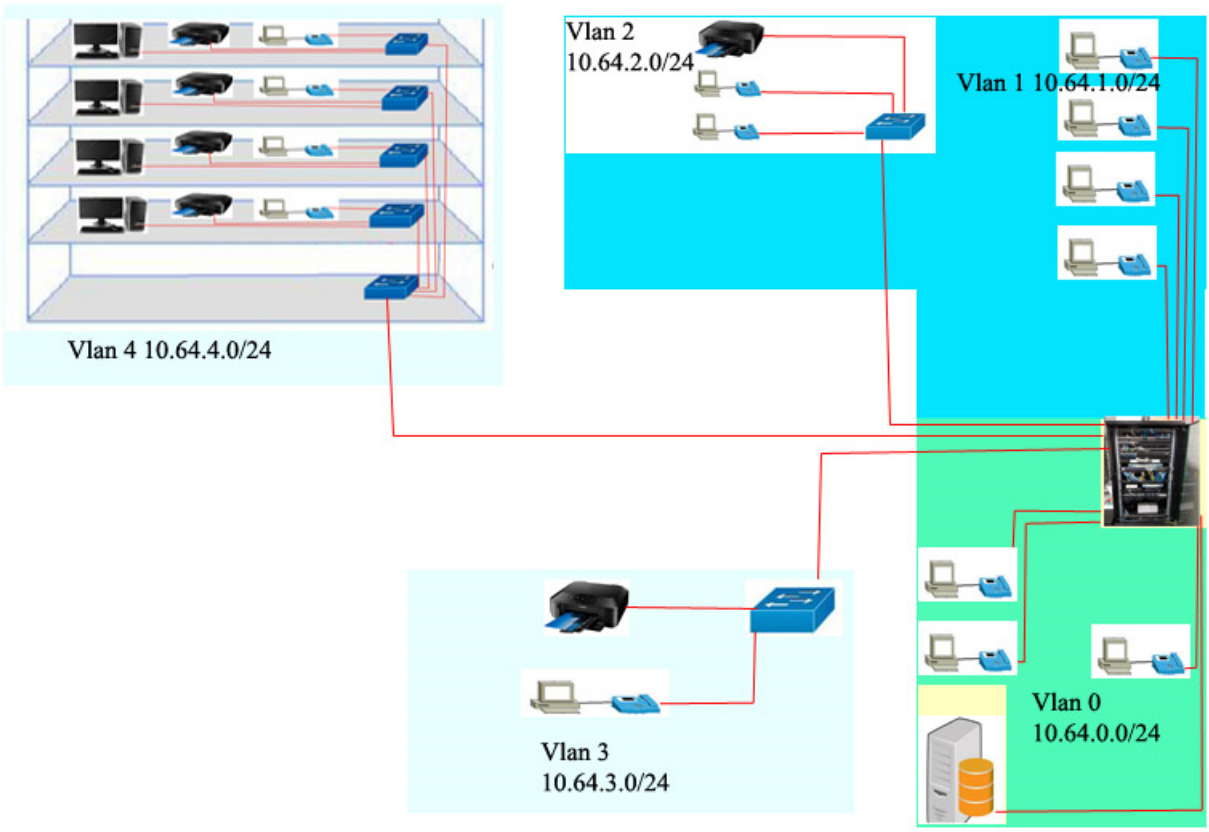


Figure 2.3 – Architecteur du réseau local

2.2.2 Parametres du serveur :

NOM DU DOMAINE	DIST-BOUIRA- SONELGAZ.LOCAL
NOM DU SERVEUR	SERV-BOUIRA
ADRESSE IP SERVEUR	10.64.0.10
MASQUE	255.255.252.0
PASERELLE	10.64.0.1
DNS	10.64.0.10
POOL D'ADRESSE IP	DHCP DEBUT 10.64.1.1 FIN 10.64.1.255
ISA SERVEUR	10.64.0.0 NON INSTALLE
MASQUE	10.64.255.255

Table 2.1 – Parametres du serveur

2.2.3 Equipements informatiques

Dans cette partie, nous allons présenter les différents équipements d'interconnexion, les serveurs, les ordinateurs et les applications utilisées.

Equipements d'interconnexion

Types de terminaux	Modèles	Nombres
Switches niveau 3	Huawei	10
Firewall	Fortinet	1
modem	ADSL	1
modem	Fortinet	1

Table 2.2 – Les équipements d'interconnexion

2.2.4 Serveurs

Rôle de serveur	Type de serveur	Système d'exploitation	Nombres
Serveur FTP	Serveur Fujitsu	Windows Server 2008 R2	1
Serveur Télé Relève	Serveur Dell	Windows Server 2016	1
Serveur TSP	Serveur Dell	Windows Server 2016	1
Serveur Base de donnée	Serveur Dell	Linux	1
Serveur Base de donnée SGC	Serveur IBM	AIX	1

Table 2.3 – Les Serveurs.

2.2.5 Applications réseau

Parmi les applications installées sur les serveurs, nous trouvons :

Type d'application	Editeur
Gestion de compteurs "ADDAD"	Sonelgaz Service Ex-ELIT
Messagerie "Tensik"	Sonelgaz Service Ex-ELIT
Système de Gestion de la relation client "CRMS"	Sonelgaz Service Ex-ELIT
Antivirus	Symantec

Table 2.4 – Applications Réseau

La répartition des autres équipements d'informatique par structure comme suite :

Structure	Existant				
	PC de bureau	Imprimante Laser	Imprimante matriciel	Imprimante multifonction	Onduleurs
Direction	7	3	0	1	0
DGSI	6	2	0	0	2
DEET	12	5	2	0	0
DRC	23	33	31	6	28
DFC	12	8	0	1	2
DTE	25	7	3	0	4
DPEG	6	2	0	0	1
DTG	13	6	4	0	0
DRH	8	3	4	0	1
DAM	13	6	4	1	1
SAG	7	3	0	0	2
Total	**132**	**78**	**48**	**9**	**41**
Observation	Les systèmes d'exploitation utilisés sont Windows 8 et Windows10				

Figure 2.4 – La répartition des équipements d'informatique

2.2.6 Gestion des utilisateurs et autorisations d'accès au réseau

Chaque employé possède un compte sur son ordinateur (dont les identifiants vous sont donnés à votre arrivée dans l'entreprise par le service informatique), sécurisé par un mot de passe. Lorsque l'ordinateur s'allume le nom d'utilisateur et le mot de passe sont demandés par leserveur. C'est lui qui s'occupe d'authentifier l'utilisateur et lui autoriser l'accès à son poste de travail.

Le serveur va également mettre à disposition des employés des dossiers partagés, accessibles à certains et pas à d'autre, selon le poste de l'employé.
Par exemple le service Comptabilité pourra mettre en commun les résultats financiers, tableaux de calculs et documents sur lesquelles plusieurs personnes travaillent en collaboration. Ce dossier sera accessible seulement par le service comptabilité et la direction par exemple, mais pas par les autres.
Chaque service pourra avoir son propre dossier partagé. Le secrétariat pour avoir un dossier partagé avec tous les employés pour mettre à leur disposition des documents types, notes de frais...

2.3 Critiques de l'existant et les améliorations proposées

2.3.1 Problématique :

Dans une architecture de réseau local segmentée par VLAN, comme celle illustrée, l'absence d'un système de gestion centralisée comme Active Directory (AD) peut entraîner plusieurs défis. Ces défis incluent la gestion des utilisateurs, l'application des politiques de sécurité, le déploiement de logiciels, et la maintenance générale du réseau. La nécessité d'une gestion manuelle et décentralisée augmente les risques d'erreurs et d'incohérences, tout en rendant le réseau plus vulnérable aux attaques.

"Comment optimiser la gestion des utilisateurs et des ressources réseau dans une architecture VLAN segmentée sans compromettre la sécurité et l'efficacité opérationnelle ?"

2.3.2 Objectif du projet :

Le déploiement d'un serveur d'annuaire apparaît comme une solution efficace pour réduire les coûts administratifs, améliorer la sécurité, et offrir un environnement de travail plus productif aux utilisateurs.

Notre projet vise à centraliser la gestion des utilisateurs c'est-a-dire mettre en place un système permettant de créer, modifier et supprimer des comptes utilisateurs de manière centralisée., le partage de fichiers et d'imprimantes, ainsi que la gestion des autorisations d'accès aux différentes ressources.

2.3.3 Solution proposé :

Active directory est un service d'annuaire LDAP très répondu depuis son lancement , grâce à son caractère évolutif ,fiable ,souple et sécurisé ,mon choix est porté sur Active Directory comme annuaire . de plus tout les services critiques du réseau fonctionnent sous Windows.

2.4 Active Directory :

Active Directory nos permet de gérer nous ressources réseau de manière simple et centralisée. Cette gestion s'appuie sur la structure physique et logique de l'annuaire Microsoft. La structure physique concerne notre placement des contrôleurs de domaine, le contrôleur de domaine eux-mêmes, les sites Active Directory, et bien d'autres choses encore. La structure logique, quant à elle, correspond à toute la partie logicielle et de structuration. On pourra notamment y intégrer les objets, les unités d'organisation (UO / OU), les domaines, les arborescences de domaine ou encore les forêts Active Directory. Pour créer ces objets logiques, Active Directory va se baser sur le schéma Active Directory. En effet, lorsque vous allez créer un objet, celui-ci va être validé ou non selon les informations que vous lui affectez avant d'être écrit dans la base Active Directory.

2.4.1 Rôle du service d'annuaire dans l'entreprise

Le service d'annuaire est l'un des composants les plus importants d'un système d'information, et ce, quelle que soit sa taille. Il offre des services centraux capables de fédérer les multiples éléments qui composent le système d'information lui-même. Par exemple, un utilisateur recherche un élément du réseau sans pour autant en connaître le nom ou l'endroit. L'utilisateur pourra résoudre lui-même ce problème en initiant une recherche vers le système d'annuaire sur la base d'un ou de plusieurs attributs qu'il connaît. De cette manière, il est par exemple possible à notre utilisateur de localiser une imprimante couleurs supportant l'impression recto verso et ce, à un emplacement géographique particulier.
L'annuaire Active Directory doit offrir les moyens de stocker toutes les informations qui caractérisent l'ensemble des objets pouvant exister dans le réseau de l'entreprise ainsi que disposer des services capables de rendre ces informations globalement utilisables par les utilisateurs, et ce, en fonction de leurs droits et privilèges.

Figure 2.5 – Partitions de l'Active Directory

2.4.2 Structure de l'Active directory

Domaines

Un domaine regroupe des ordinateurs, des périphériques, des utilisateurs. C'est une sorte de zone sécurisée, sur laquelle on ne peut pénétrer que quand on a été authentifié par le Contrôleur de Domaine.

Arbres de domaines

Un arbre est un regroupement hiérarchique de plusieurs domaines.

Forêts

En effet, une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt. Les domaines d'une forêt fonctionnent de

façon indépendante, mais la forêt facilite les communications entre les domaines, c'est-à-dire dans toute l'architecture.

Conclusion

L'étude de l'existant nous à permet de ce familiariser avec le réseau actuel de SONELGZ et de l'étudier , c'est ce qui nous à permet de voir ses faiblesses, et conduit à proposé la solution pour palier à ces derniers. Le chapitre suivant va être concrétisé à la description de la réalisation des différentes étapes, à savoir l'installation ,déploiement de l'annuaire Active Directory et la configuration des différents services.

Chapitre 3

Deploiment et configuration de l'Active Directory

Introduction

Ce chapitre est consacré à la mise en œuvre et au déploiement d'Active Directory. Nous y aborderons les différents outils utilisés, notamment Windows Server 2012 R2. Nous détaillerons ensuite les étapes d'installation et de configuration des services essentiels tels que DNS et DHCP.

Pour réaliser notre projet, nous avons préparé l'environnement nécessaire, comprenant un ordinateur et les programmes requis, tels que VMware Workstation. Nous avons ensuite créé plusieurs machines virtuelles sur cet ordinateur pour simuler les appareils physiques.

3.1 VMware Workstation

VMware Workstation est une application de virtualisation permettant aux utilisateurs de créer et de gérer des machines virtuelles sur leur ordinateur. Développé par VMware, il offre la possibilité d'exécuter différents systèmes d'exploitation simultanément sur un seul matériel, facilitant ainsi le test de logiciels, le développement d'applications et la création d'environnements de test.

Nous avons créé les machines virtuelles suivantes :

- Une machine exécutée sous Windows serveur 2012 R2
- Une machine exécutée sous Windows 7 Professionnel(post de travail) ;
- Une machine exécutée sous Windows 7Enterprise(post de travail) ;

3.1.1 Mise en place de la machine virtuelle

Après avoir installé VMware sur la machine physique, nous allons maintenant crée les machines virtuelles : Windows 7Professionel , Windows 7Enterprise, Windows server 2012 R2.

3.1.2 Création les machines virtuelles

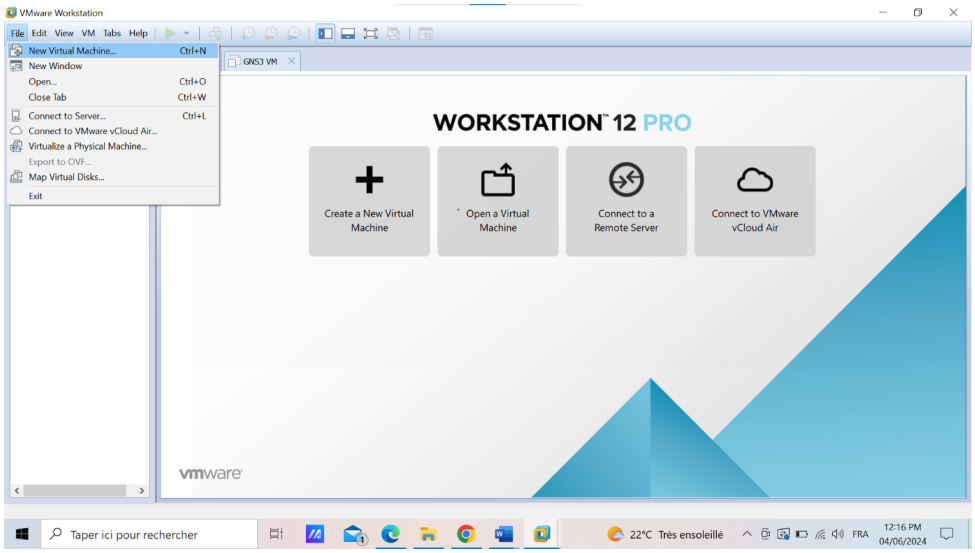


Figure 3.1 – Création les machines virtuelle.

Nous choisissons la méthode de connexion "Custom","Host-only ", on spécifiant la carte réseau VMnet3

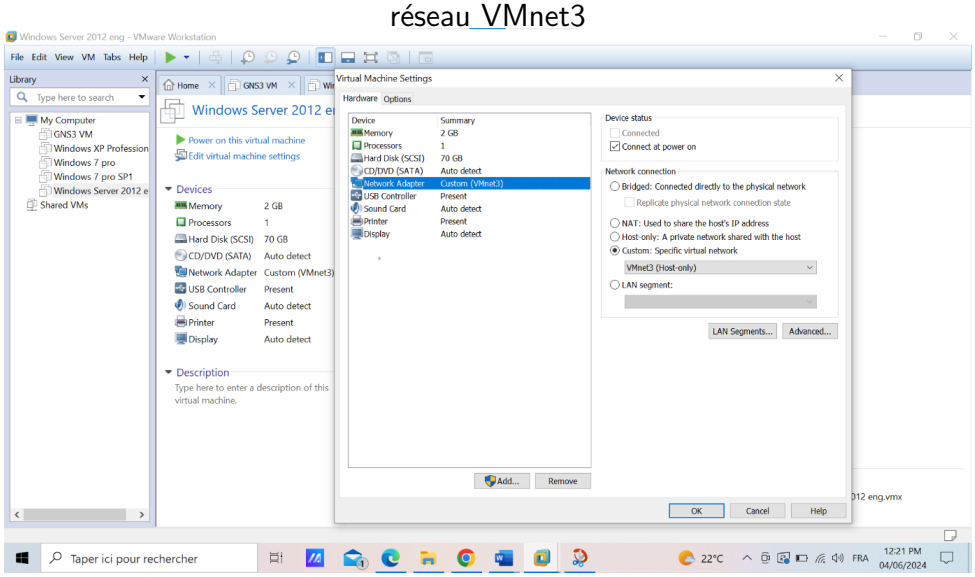


Figure 3.2 – Connexion des machines virtuelle sur passerelle Custom (VMnet3).

Notant que l'adresse IP sur un serveur doit être ajouter de manière statique.

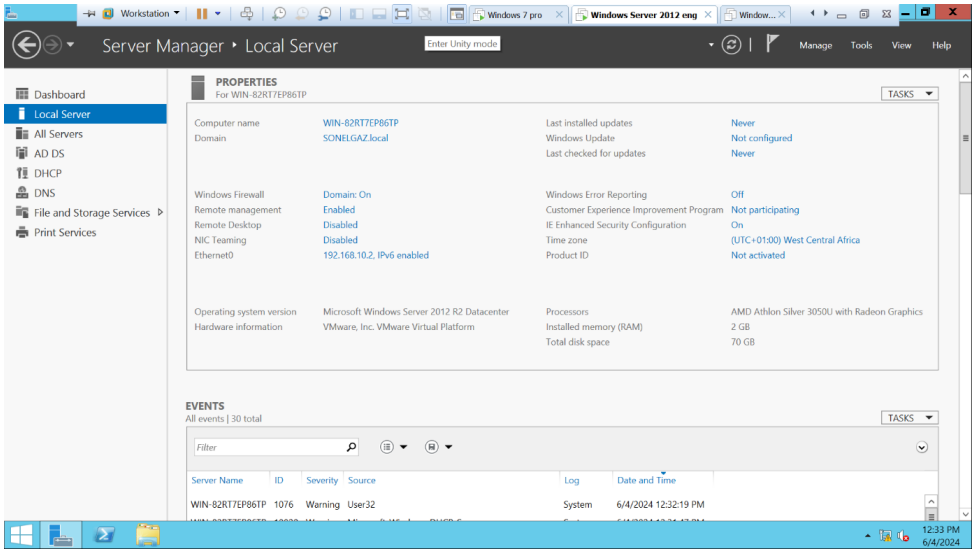


Figure 3.3 – adresse IP server

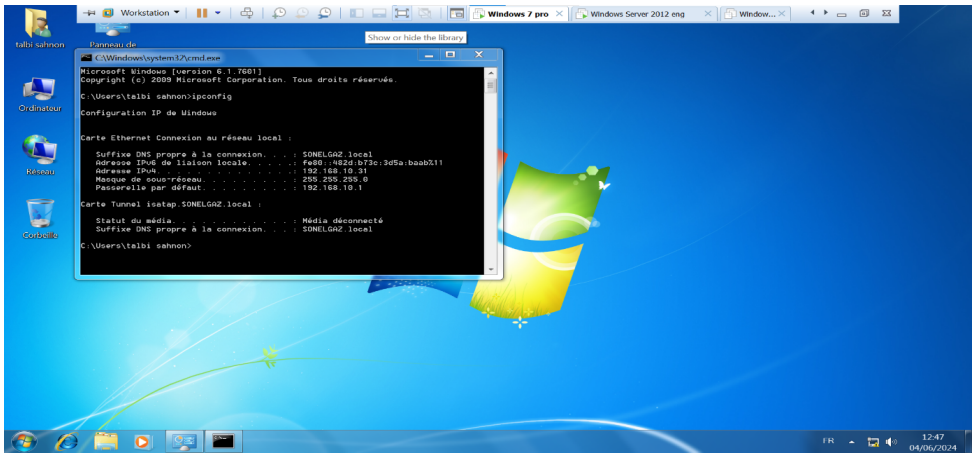


Figure 3.4 – Adresse IP de la machine virtuel Windows 7 Professionnel

3.2 Windows server 2012

3.2.1 Présentation Windows server 2012

Le système d'exploitation Windows Server 2012 est la cinquième version majeure de Windows Server proposé par Microsoft et est sortie le 4 septembre 2012. Elle caractérise par l'arrivée de la virtualisation Hyper-V ainsi que l'apparition d'outils pour cloud. De plus, elle inclut l'interface controversé Metro, soit un menu démarrer se retrouvant modifié de la même manière que Windows 8. Enfin, il inclut un gestionnaire d'espace d'adressage virtuel IPAM offrant les mêmes fonctionnalités d'infrastructure d'adresses IP virtuelle que les fonctionnalités ASM pour l'espace d'adressage IP physique.[22]

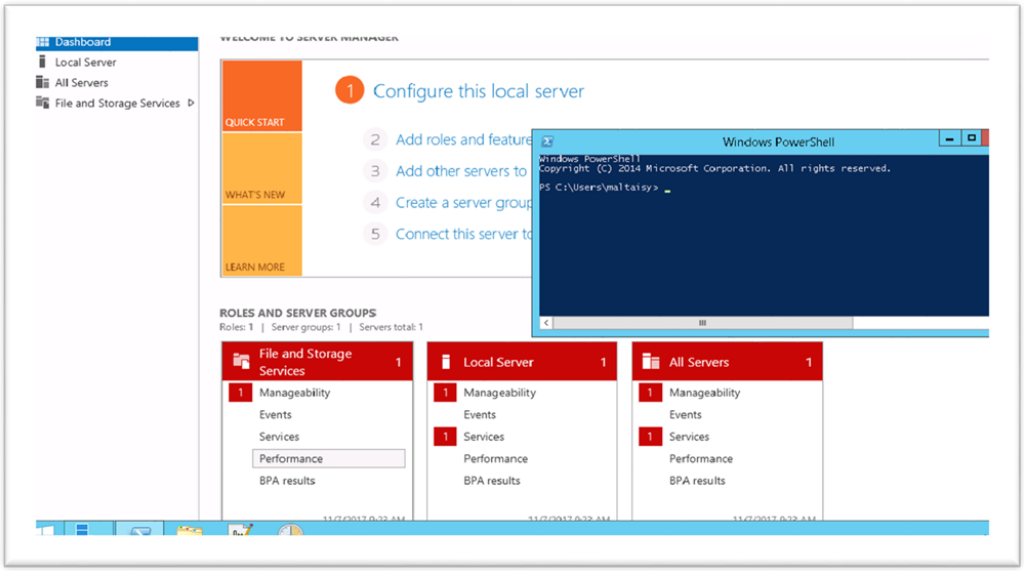


Figure 3.5 – Dashboard Windows

3.2.2 Les versions de Windows serveur 2012

On distingue principalement 4 versions de Windows Serveur 2012 :

— Windows Server 2012 R2 Foundation
— Windows Server 2012 R2 Essentials
— Windows Server 2012 R2 Standard
— Windows Server 2012 R2 Datacenter

Si l'on souhaite comparer correctement ces versions, il est préférable de faire 2 groupes : Foundation-Essentials d'un coté et Standard-datacenter de l'autre.

En effet, beaucoup plus de limitations sont présentes pour les versions Foundation-Essentials comme le nombre d'utilisateurs (respectivement 15 et 25),la virtualisation non supportée ou encore le mode core inexistant. Alors que pour les versions Standard-Datacenter, toutes les limitations précités disparaissent. [22]

3.2.3 Rôles et fonctionnalités

Sur un Windows Server , on distingue 2 types de "service" :

— Rôles

— Fonctionnalités

Les rôles vont représenter le ou les services principaux que va fournir le serveur aux clients. Les fonctionnalités de Windows Serveur peuvent être comparées a des logiciels/outils qui vont être utilisé par les rôles du serveur. Par exemple ,certains rôles peuvent avoir besoin du Framework .NET 3.5 pour fonctionner correctement.

Une fonctionnalité n'est pas forcément obligatoire pour un rôle mais peut lui apporter une plus-value qui va permettre a un rôle de devenir hautement disponible.[22]

3.2.4 Nouveautés de Windows Serveur 2012 R2

La console server Manager permet :

— De paramétrer le serveur (adresse IP, par feu ,bureau a distance ,Windows Update).

— D'ajouter les composants Windows répartis entre rôles et fonctionnalités.

— D'activer ou de désactiver la configuration renforcée de la sécurité d'internet Explorer (IE ESC).

— De configure les paramètres de mises a jour.

— De se connecter a un autre serveur a distant.

— D'accéder depuis un point unique aux principales consoles pour gérer chaque rôle / fonctionnalité.

3.3 Installation d'Active Directory(AD)

Pour installer et déployer le serveur Active directory, quelques notions deprérequis sont essentielles [L2] :

— Un serveur fonctionnel sous Windows 2012 R2 ;

— Le serveur doit avoir une configuration IP statique ;

— Le compte "Administrateur" du serveur doit avoir un mot de passe fort, sinon l'installation ne pourra pas se faire (l'AD utilisant ce compte lors de l'initialisation du domaine).

Sur le tableau de bord du serveur, on clique sur " Ajouter des rôles et desfonctionnalités " :

Figure 3.6 – ajout du role Active Directory

Dans la nouvelle fenêtre qui s'ouvre, on clique sur " Suivant " :

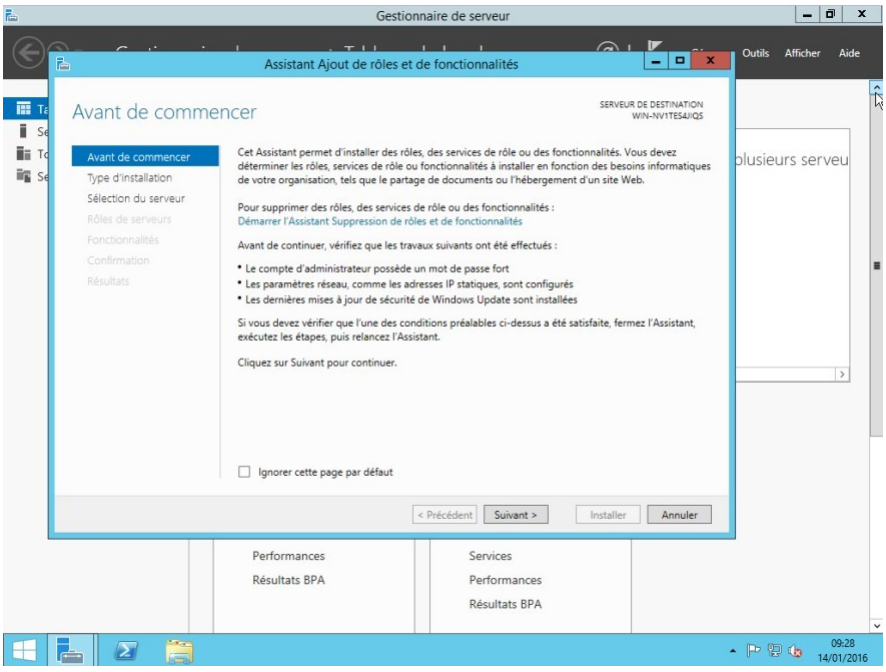


Figure 3.7 – assistant ajout deroles et de fonctionnalité

On sélectionner l'Installation basée sur un rôle ou une fonctionnalité. On Clique ensuite sur Suivant :

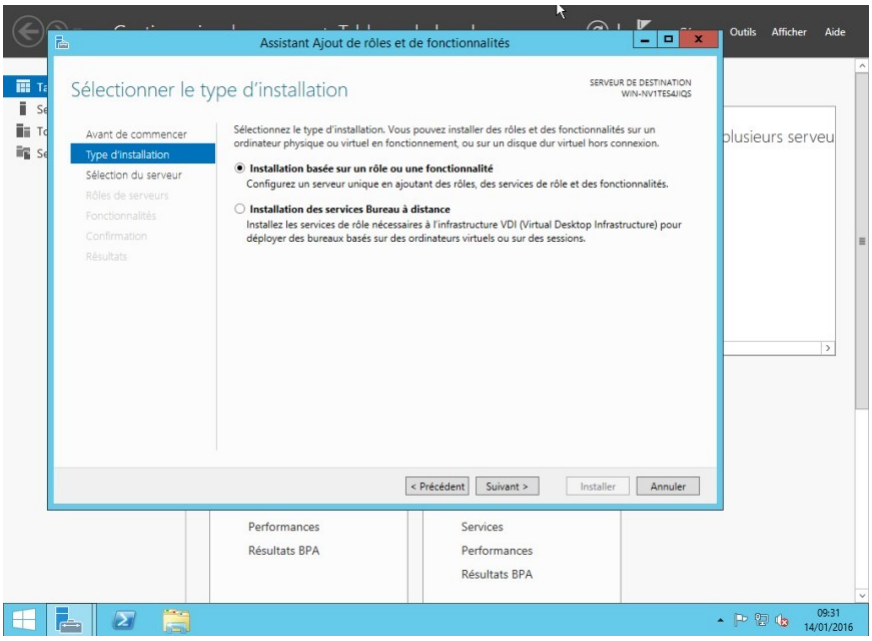


Figure 3.8 – Sélectionner le type d'installation

On coche Sélectionner un serveur du pool de serveurs ,On clique sur le serveur choisi et ensuite Suivant.

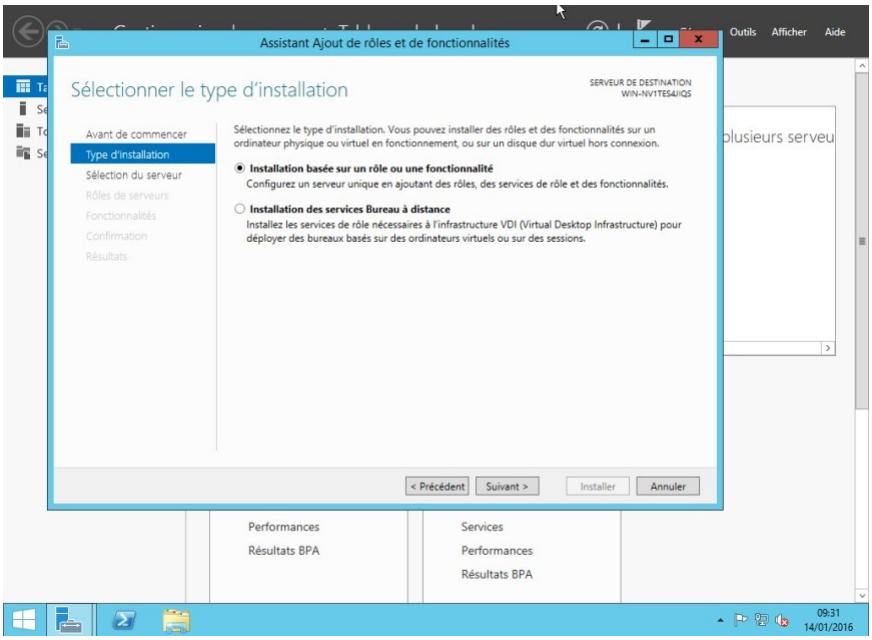


Figure 3.9 – Sélectionner des roles de serveurs

On coche le rôle Service AD/DS.

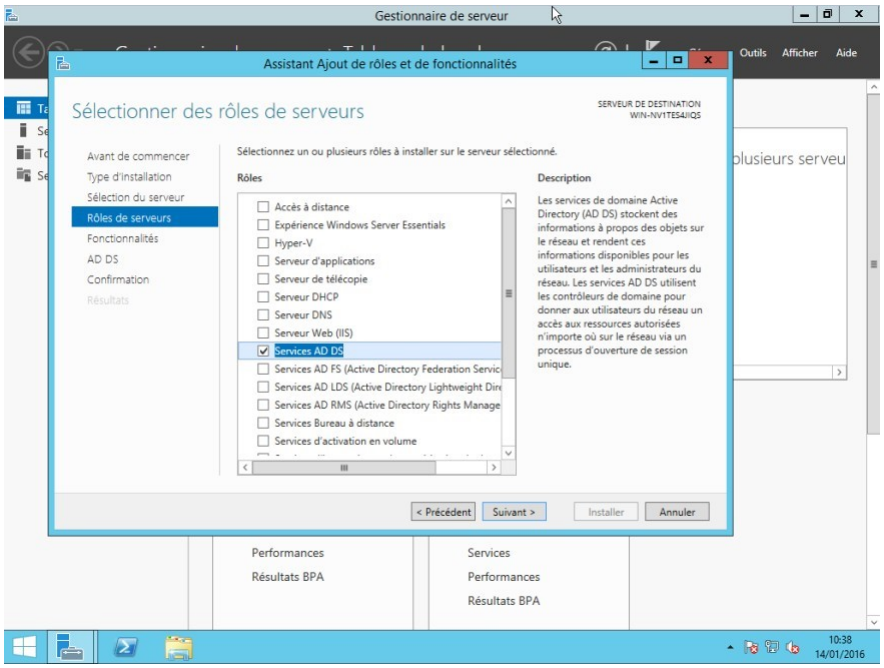


Figure 3.10 – Ajout des fonctionnalité

Les fonctionnalités requises pour le Service AD DS sont énumérées, on clique sur Ajouter des fonctionnalités.

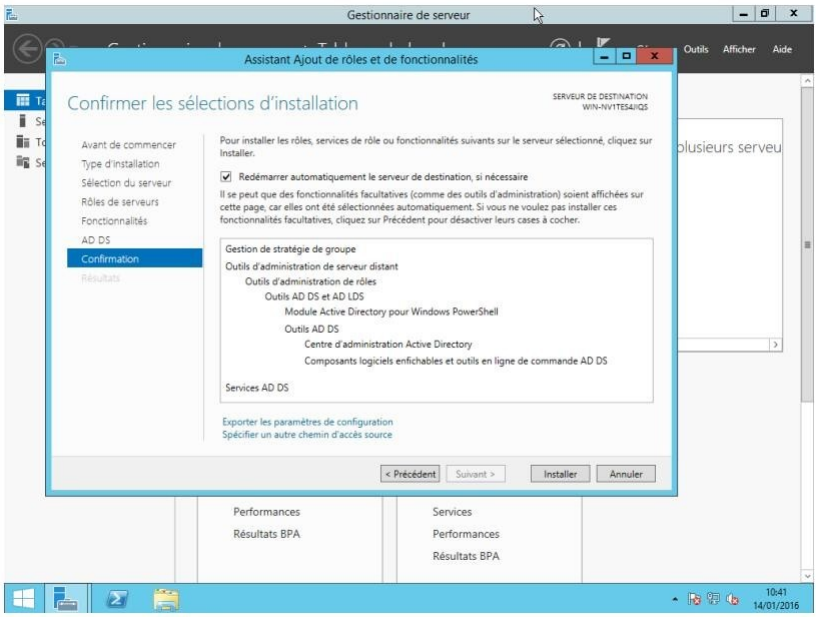


Figure 3.11 – Interface de Confirmation

La page "Confirmer les sélections d'installation" apparait, on coche Redémarrer automatiquement le serveur de destination, si nécessaire puis on clique sur Suivant.

L'installation se lance ensuite ;

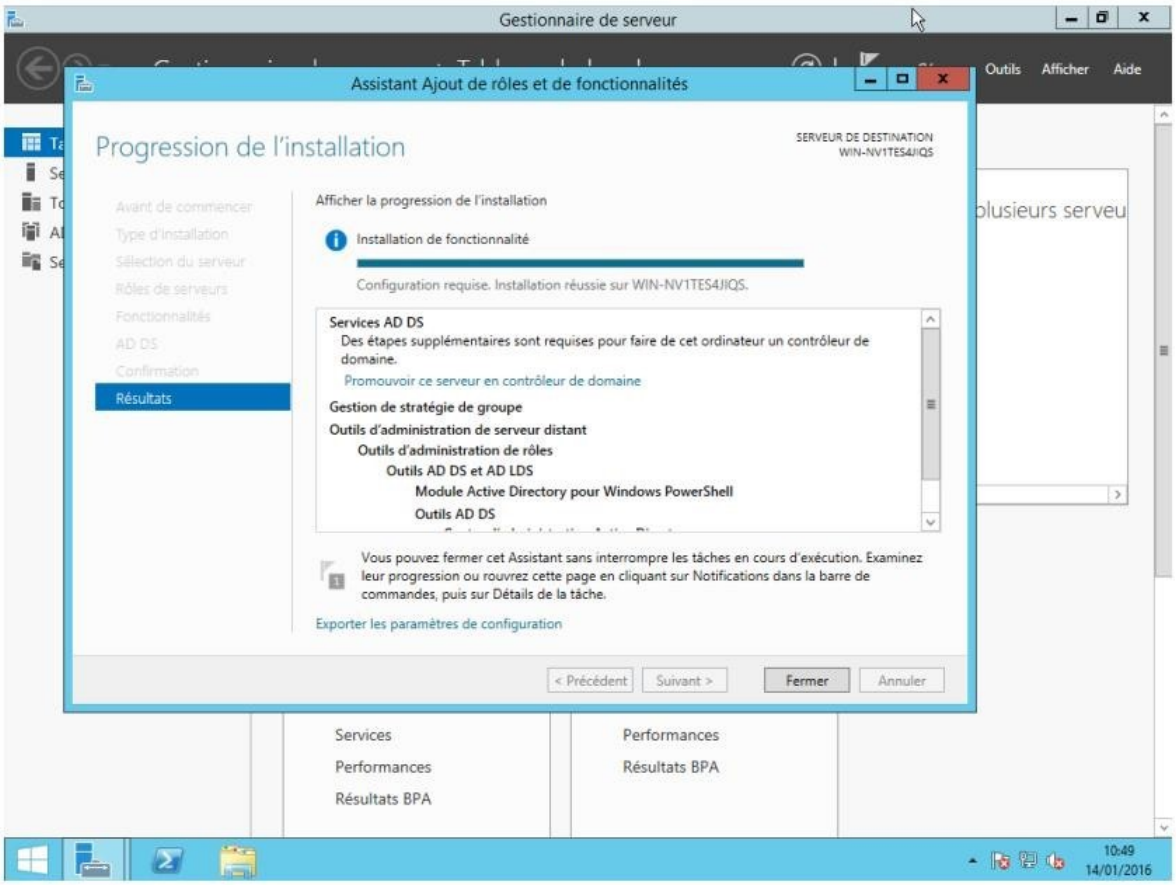


Figure 3.12 – Progression de l'installation

Voilà l'installation terminée, on clique sur Promouvoir ce serveur en contrôleur de domaine. Choisir l'opération de déploiement Ajouter une nouvelle forêt et entrer le nom de domaine ;

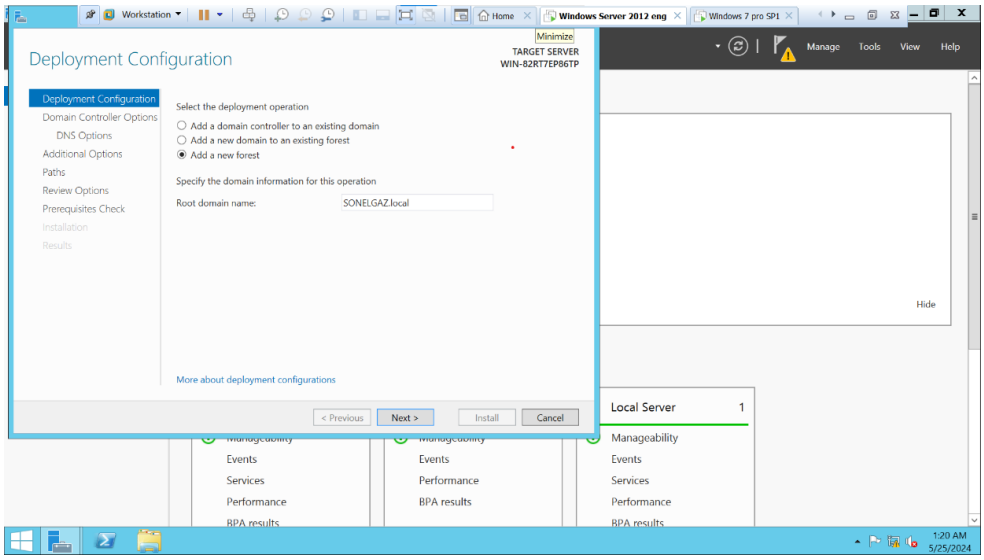


Figure 3.13 – configuration et déploiment

L'installation se lance ensuite ;

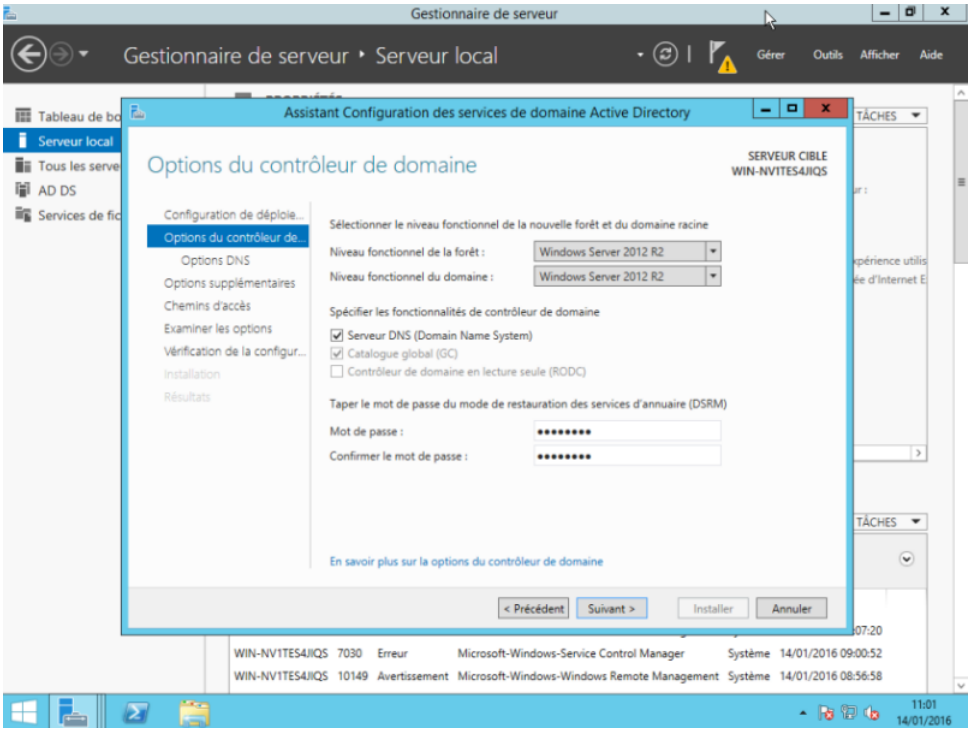


Figure 3.14 – Option du controler de domaine

Dans ce nouvel onglet, cocher serveur DNS et entrer un mot de passe, ici c'est Password.

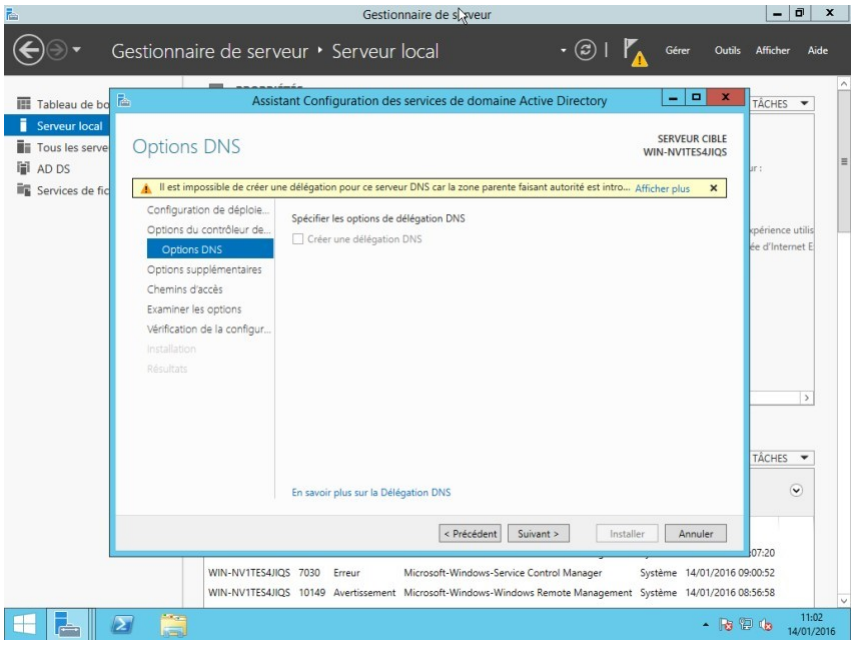


Figure 3.15 – Option DNS

Ici, On clique sur suivant

Entrer un nom de domaine pour notre cas c'est SONELGAZ

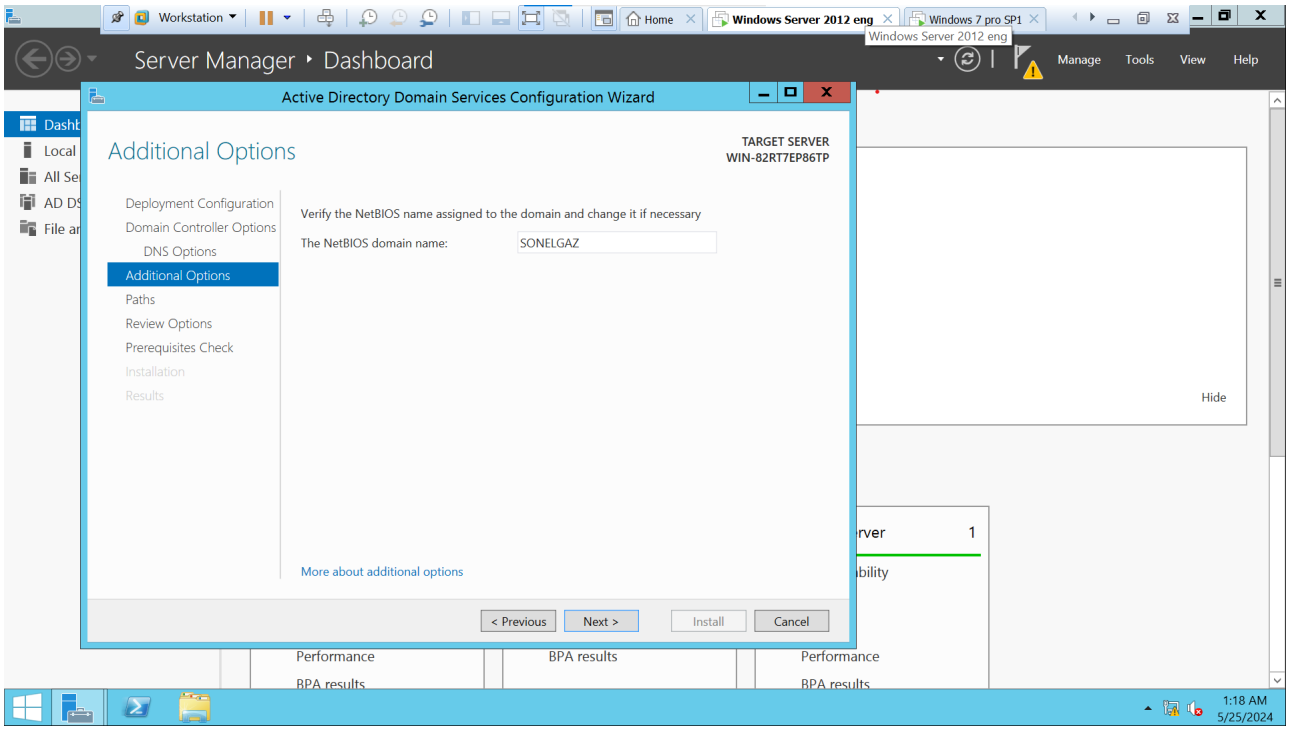


Figure 3.16 – Option Additionel

Vérification des chemins d'accès et on clique sur suivant.

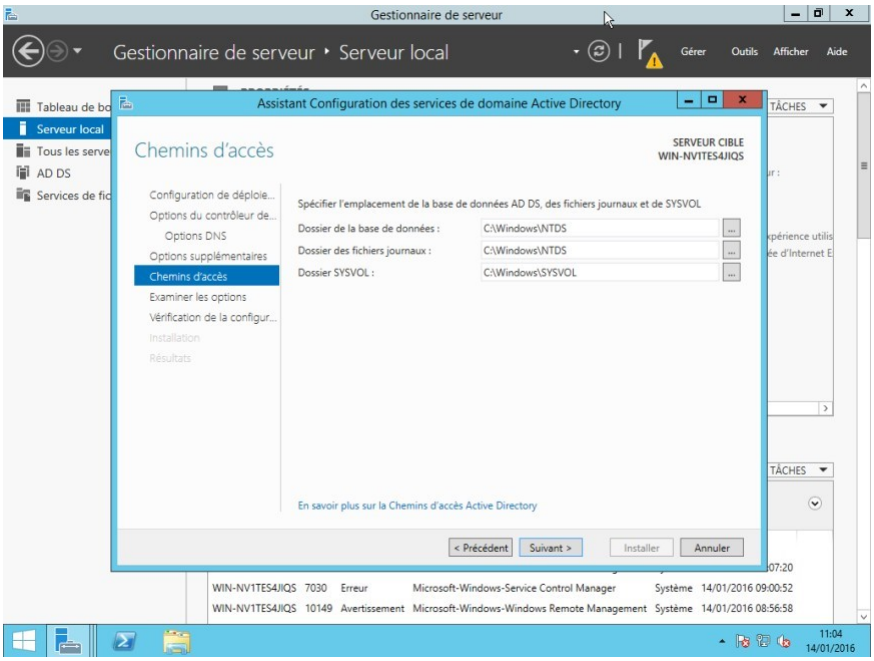


Figure 3.17 – Chemins d'accées

On terminer par cliquer sur Installer.

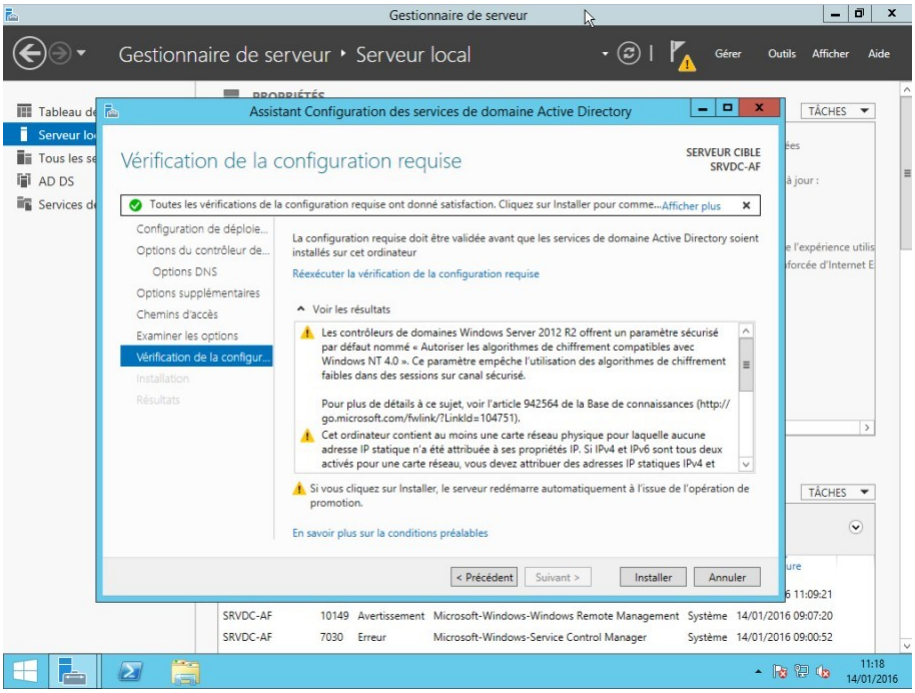


Figure 3.18 – Interface d'installation

3.4 Installation du serveur DNS

Le DNS (Domain Name System) est un service permettant de traduire un nom de domaine à une adresse IP associé. Pour accéder à un site internet nous devons taper son adresse IP, Par exemple 172.217.16.78 pour accéder à Google, par contre pour les utilisateurs, il est difficile de retenir les adresses numériques du genre 172.217.16.78,mais avec un nom alphabétique il est plus facile de retenir les adresse des sites internet, par exemple "www.google.com". Ceci est applicable pour tous les adresses IP.[L2]

On sélectionne ensuite "Serveur DNS", puis une nouvelle fois ON clique sur "Ajouter des fonctionnalités" puis "Suivant" :

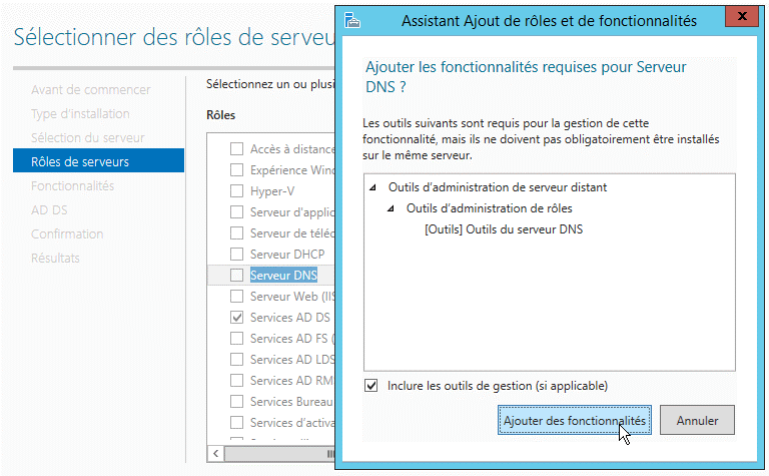


Figure 3.19 – Roles de serveurs

On Laisse les fonctionnalités proposées par défaut, puis On clique sur " Suivant " :

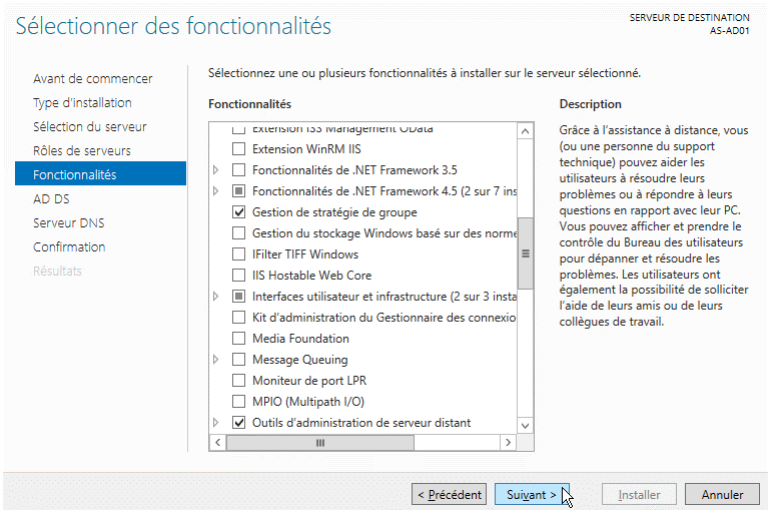


Figure 3.20 – fonctionnalités

On clique sur " Suivant " :

Figure 3.21 – Service de domaine Active Directory

On clique sur " Suivant " :

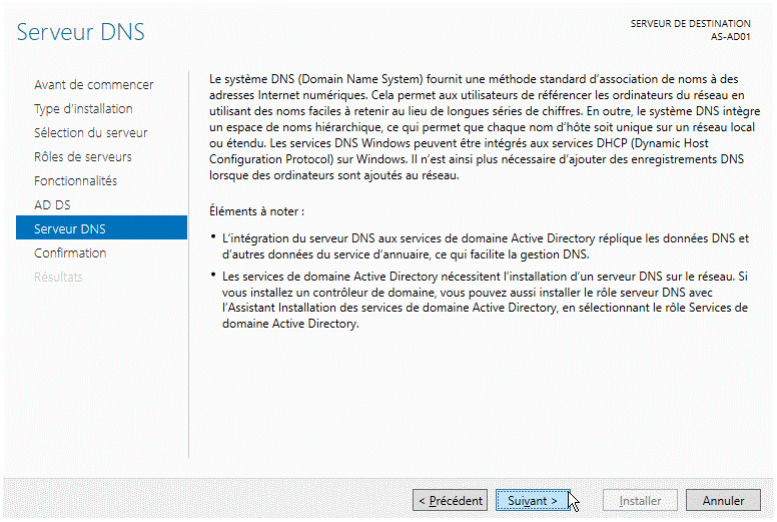


Figure 3.22 – Serveur DNS

On clique sur " Suivant " :

On coche " Redémarrer automatiquement le serveur de destination, si nécessaire ",on confirme avec " Oui " puis on clique sur " Installer " :

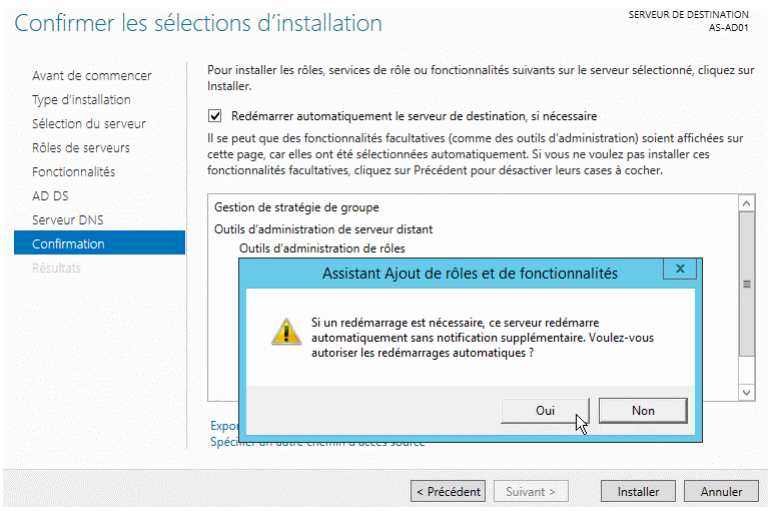


Figure 3.23 – Confirmation

On clique sur " Suivant " :

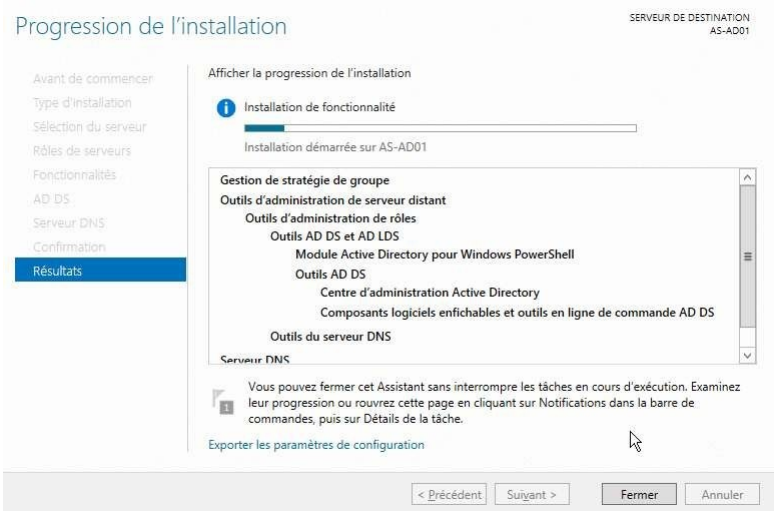


Figure 3.24 – Résultats

Une fois l'installation terminée, on clique sur " Fermer " :

3.5 Installation du serveur DHCP

Le DHCP (Dynamic Host Configuration Protocol) : Un serveur DHCP délivre des adresses IP de façon automatique aux ordinateurs se connectant au réseau. En plus d'une adresse IP le serveur DHCP vous informe de la configuration réseau tel que la passerelle par défaut et le masque de sous-réseau. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies[L2] :

Étendue

Une étendue est la plage consécutive complète des adresses IP probables d'un réseau. Les étendues désignent généralement un sous-réseau physique unique de votre réseau auquel sont offerts les services DHCP. Les étendues constituent également pour le serveur le principal moyen de gérer la distribution et l'attribution d'adresses IP et de tout autre paramètre de configuration associé aux clients du réseau.

Étendue globale

Une étendue globale est un regroupement administratif des étendues pouvant être utilisé pour prendre en charge plusieurs sous-réseaux logiques IP sur le même sous-réseau physique. Les étendues globales contiennent uniquement une liste d'étendues membres ou d'étendues enfants qui peuvent être activées ensemble. Les étendues globales ne sont pas utilisées pour configurer d'autres détails concernant l'utilisation des étendues. Pour configurer la plupart des propriétés utilisées dans une étendue globale, vous devez configurer individuellement les propriétés des étendues membres.

Plage d'exclusion

Une plage d'exclusion est une séquence limitée d'adresses IP dans une étendue, exclue des offres de service DHCP. Les plages d'exclusion permettent de s'assurer que toutes les adresses de ces plages ne sont pas offertes par le serveur aux clients DHCP de votre réseau.

Pool d'adresses

Une fois que vous avez défini une étendue DHCP et appliqué des plages d'exclusion, les adresses restantes forment le pool d'adresses disponible dans l'étendue. Les adresses de pool peuvent faire l'objet d'une affectation dynamique par le serveur aux clients DHCP de votre réseau.

Bail

Un bail est un intervalle de temps, spécifié par un serveur DHCP, pendant lequel un ordinateur client peut utiliser une adresse IP affectée. Lorsqu'un bail est accordé à un client, le bail est

actif. Avant l'expiration du bail, le client doit renouveler le bail de l'adresse auprès du serveur. Un bail devient inactif lorsqu'il arrive à expiration ou lorsqu'il est supprimé du serveur. La durée d'un bail détermine sa date d'expiration et la fréquence avec laquelle le client doit le renouveler auprès du serveur.

Réservation

Utilisez une réservation pour créer une affectation de bail d'adresse permanente par le serveur DHCP. Les réservations permettent de s'assurer qu'un périphérique matériel précis du sous-réseau peut toujours utiliser la même adresse IP.

Types d'options

Les types d'options sont d'autres paramètres de configuration client qu'un serveur DHCP peut affecter lors du service de baux aux clientsDHCP. Par exemple, certaines options régulièrement utilisées comprennent des adresses IP pour les passerelles par défaut (routeurs), les serveurs WINS et les serveurs DNS. Généralement, ces types d'options sont activés et configurés pour chaque étendue. La console DHCP vous permet également de configurer les types d'options par défaut utilisés par toutes les étendues ajoutées et configurées sur le serveur. La plupart des options sont prédéfinies via la RFC 2132, mais vouspouvez utiliser la console DHCP pour définir et ajouter des types d'options personnalisés si nécessaire.

Classes d'options

Une classe d'options est un moyen pour le serveur de continuer à gérer les types d'options proposés aux clients. Lorsqu'une classed'options est ajoutée au serveur, les clients de cette classe peuvent être fournis en types d'options spécifiques à la classe pour leur configuration. Pour Microsoft Windows 2000 et Windows XP, les ordinateurs clients peuvent également spécifier un ID de classe lorsqu'il communique avec le serveur. Pour des clients DHCP plus récents qui ne prennent pas en charge le processus d'ID de classe, le serveur peut être configuré avec les classes par défaut à utiliser lors du placement des clients dans une classe. Les classes d'options peuvent être de deux types : les classes de fournisseurs et les classes d'utilisateurs.

Avant de commencer, Il est nécessaire de configurer son serveur en IP fixe et de l'avoir renommé. Nommer votre serveur en fonction de la convention de nommage de votre entreprise. Ici, nous installerons le rôle DHCP sur notre contrôleur de domaine, Et depuis le Gestionnaire de serveur, on clique sur l'étape Gérer puis Ajouter des rôles et fonctionnalités :

Figure 3.25 – Ajout du role DHCP

On sélectionne le type d'installation " Installation basée sur un rôle ou une fonctionnalité ".

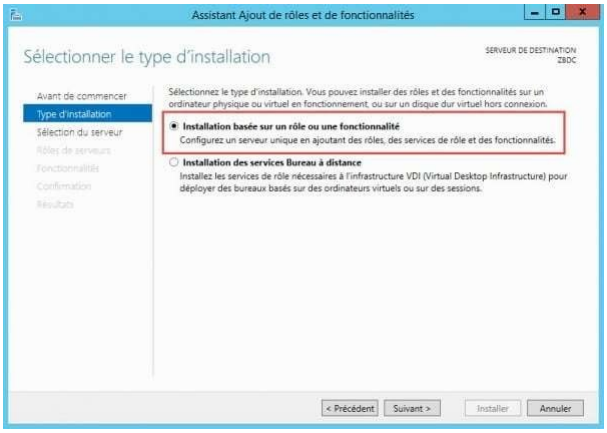


Figure 3.26 – Type d'installation

Pour le moment, on a qu'un seul serveur dans le pool, j'ai donc juste à le sélectionner et puis sur Suivant :

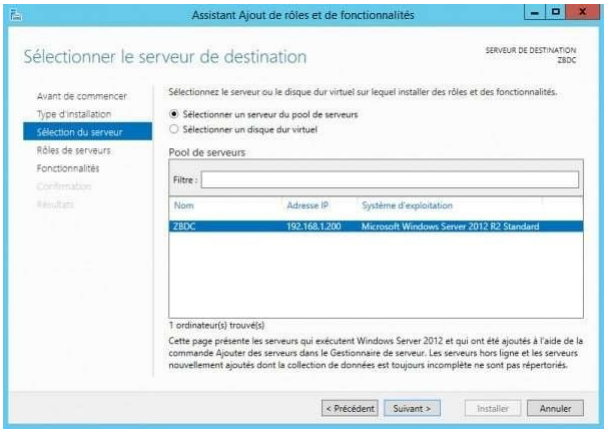


Figure 3.27 – Sélection du serveur

Vous êtes maintenant sur la fenêtre de sélection des rôles. Nous allons donc installer le rôle DHCP. Pour cela,on coche simplement DHCP dans la fenêtre de sélection des rôles.Enfin, On clique sur Suivant :

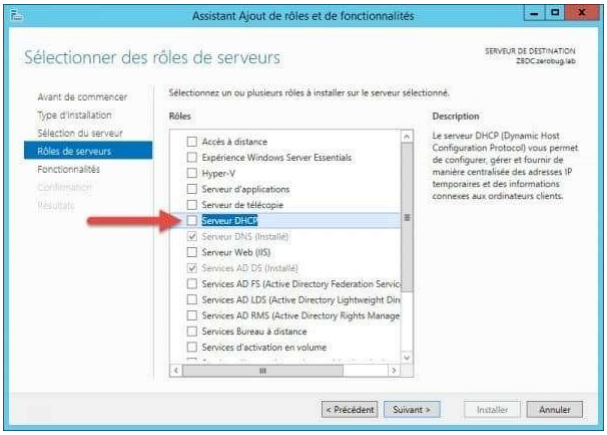


Figure 3.28 – Roles de serveurs

On ajoute Des fonctionnalités supplémentaires automatiquement sélectionnées,

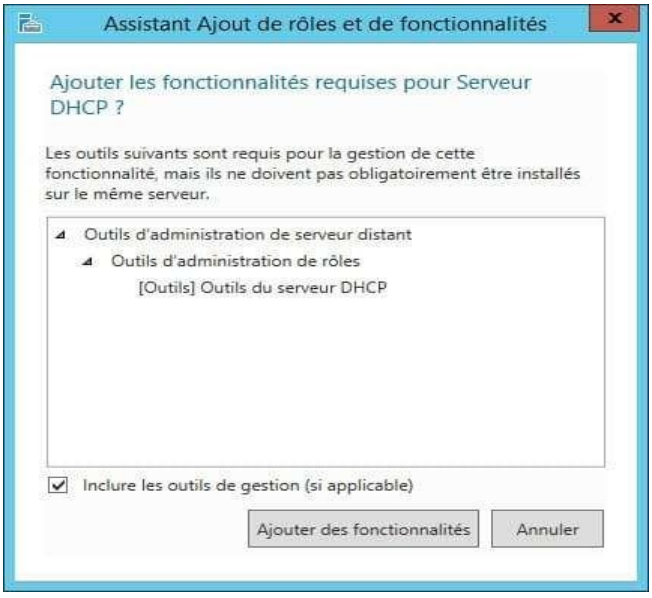


Figure 3.29 – Ajout des fonctionnalité requise pour le role DHCP

Après avoir ajouté des rôles, on peut ajouter des fonctionnalités supplémentaires.

En général, toutes les fonctionnalités nécessaires pour prendre en charge le rôle ciblé sont déjà sélectionnées, ce qui permet de simplement cliquer sur le bouton "Suivant" pour continuer.

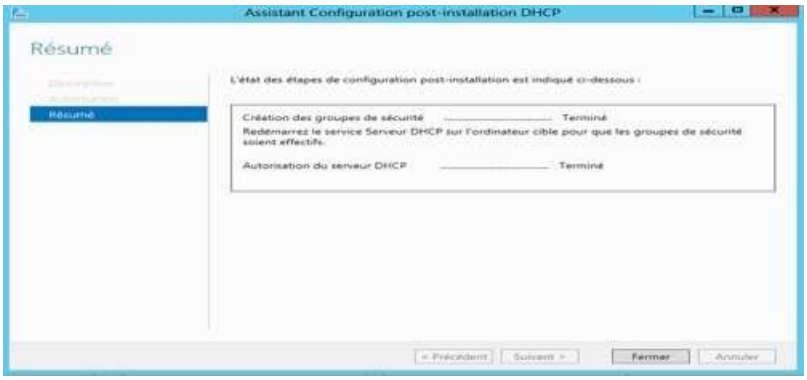


Figure 3.30 – Installation términé

Nous devons maintenant créer nos étendues DHCP à l'aide de la console d'administration DHCP, que nous pouvons lancer depuis le menu Outils du gestionnaire de serveur. Pour créer une étendue IPv4, cliquez avec le bouton droit sur IPv4, puis choisissez Nouvelle étendue.

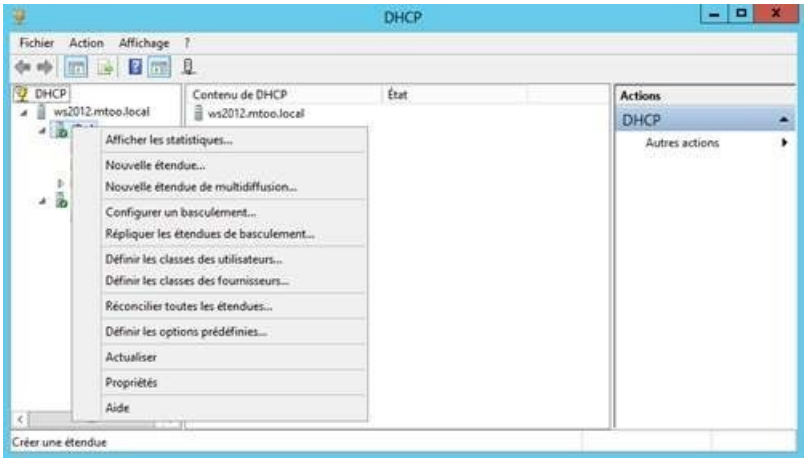


Figure 3.31 – Etendue

L'assistant de création de nouvelle étendue nous permettra ensuite de donner un nom et une description à notre étendue.

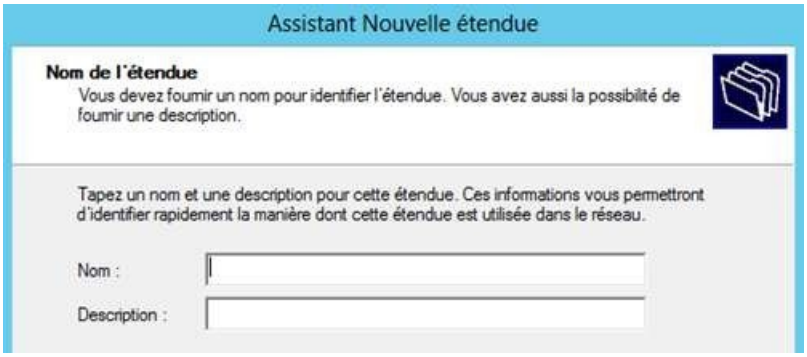


Figure 3.32 – Nom de l'etendue

Définir la plage d'adresse à distribuer et le masque de sous réseau :

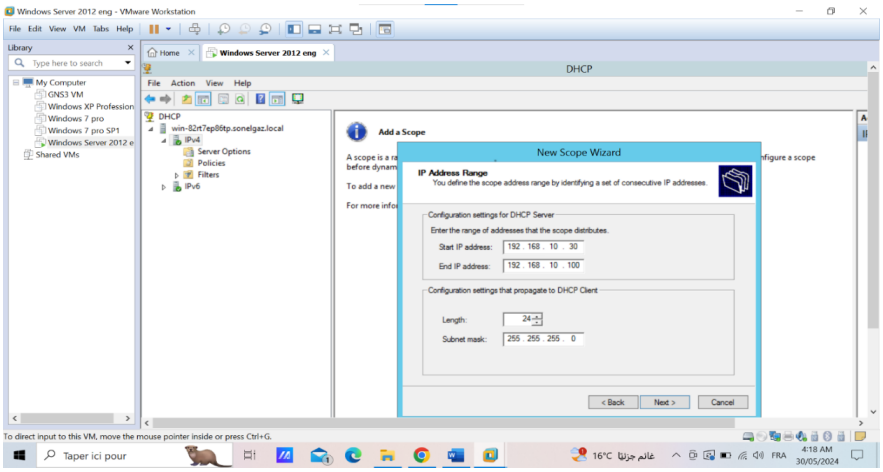


Figure 3.33 – Plage d'adresse

Ajouter d'éventuelles exclusions afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP, PCen adresse fixe, serveur,...) :

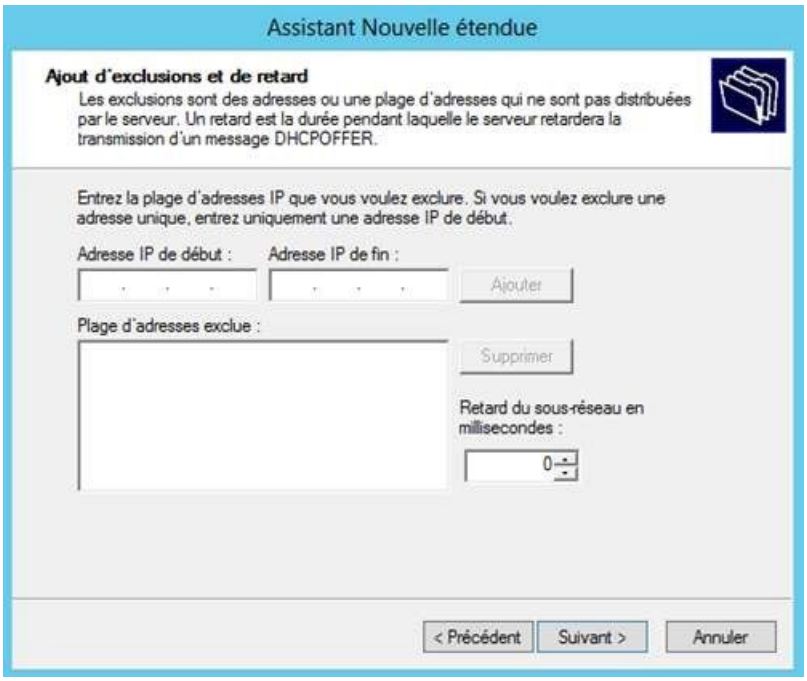


Figure 3.34 – Ajout d'exclusions et de retard

Puis la durée du bail, c'est à dire le temps pendant lequel le PC est autorisé à utiliser cette adresse sans la renouveler :

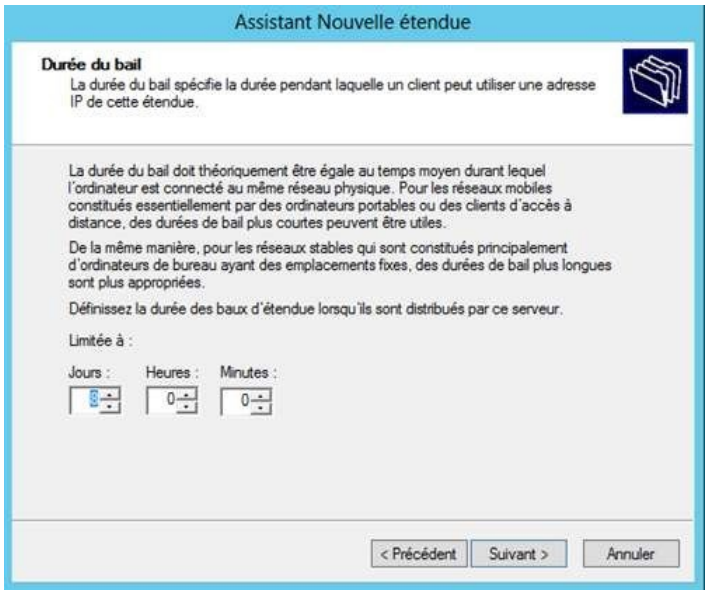


Figure 3.35 – Durée du bail

Nous pouvons ensuite configurer des option qui sont des paramètres supplémentaires que nous pouvons configurer, comme l'adresse de la passerelle et ensuite activer l'étendue.

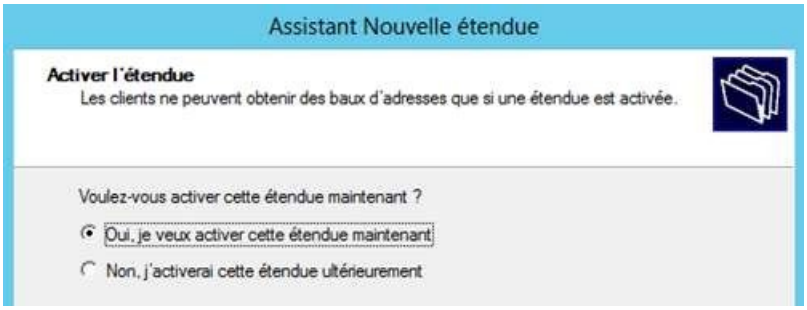


Figure 3.36 – Activer l'étendue

Nous pouvons vérifier les options d'étendue dans la console. Voici un exemple avec les paramètres usuels :

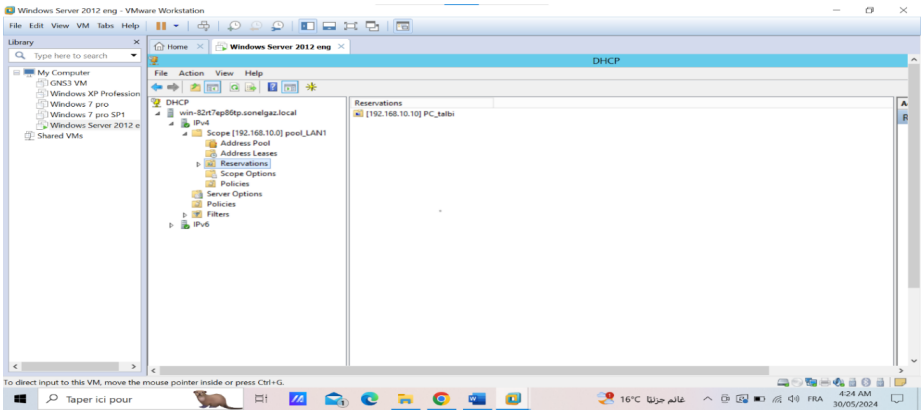


Figure 3.37 – Parametres usuels

3.6 Installation du rôle Serveur d'impression

Le serveur peut être utilisé comme un serveur d'impression qui fournisse et gère l'accée aux imprimantes réseau et à leur pilote ;

En effectuant les étapes et les tâches suivantes :

- Ajouté une ou plusieurs imprimantes.
- Partagé des imprimantes pour permettre aux clients d'envoyer des travaux d'impression aux imprimantes.
- Ajouté, si nécessaire, des pilotes d'imprimante clients.
- Gérer de façon centralisée les imprimantes
- Faciliter l'installation des imprimantes sur les PC
- Gérer les autorisations d'accès aux imprimantes grâce a des groupes de sécurité
- Préconfigurer les imprimantes(configuration par défaut a l'installation sur les PC)
- Gérer les files d'attente d'impression de façon centralisé

Le serveur d'impression est un rôle qu'on peut ajouter après l'installation d'Active Directory, Dans la console "Gestionnaire de serveur", il faut aller dans la partie "Tableau de bord" et cliquer sur"Ajouter des rôles et des fonctionnalités".

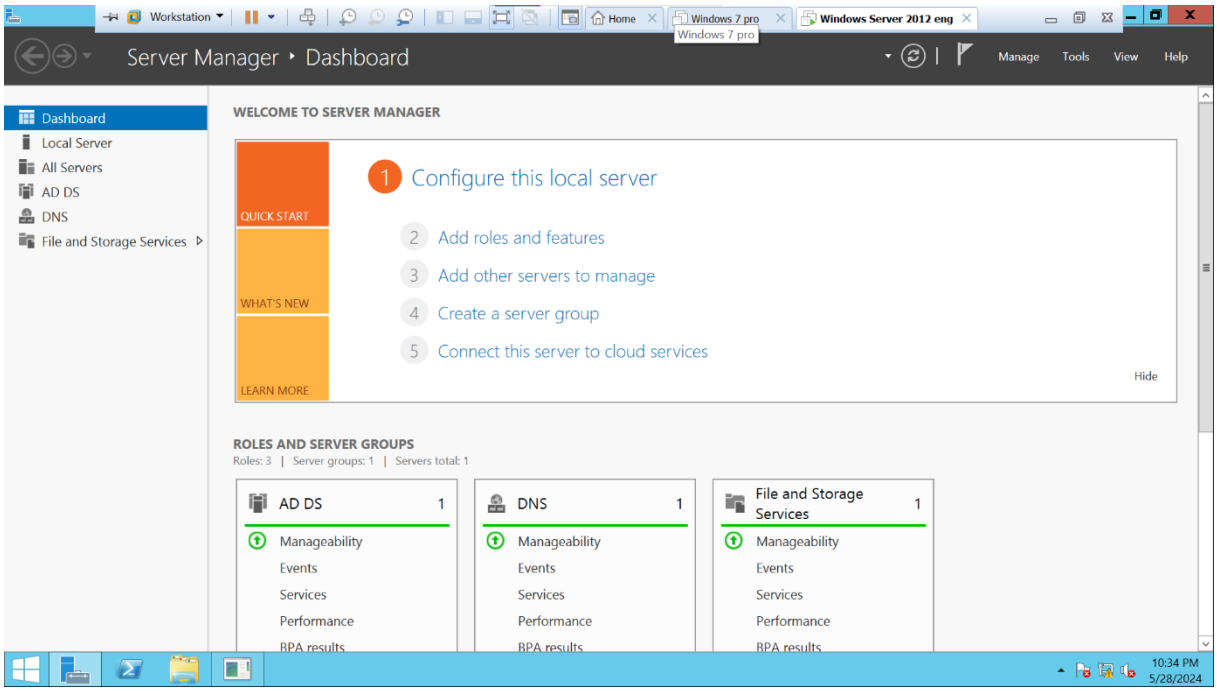


Figure 3.38 – Ajout du role serveur d'impression

suivant les étapes d'installations on sélectionne "Services d'impression et de numérisation de documents"

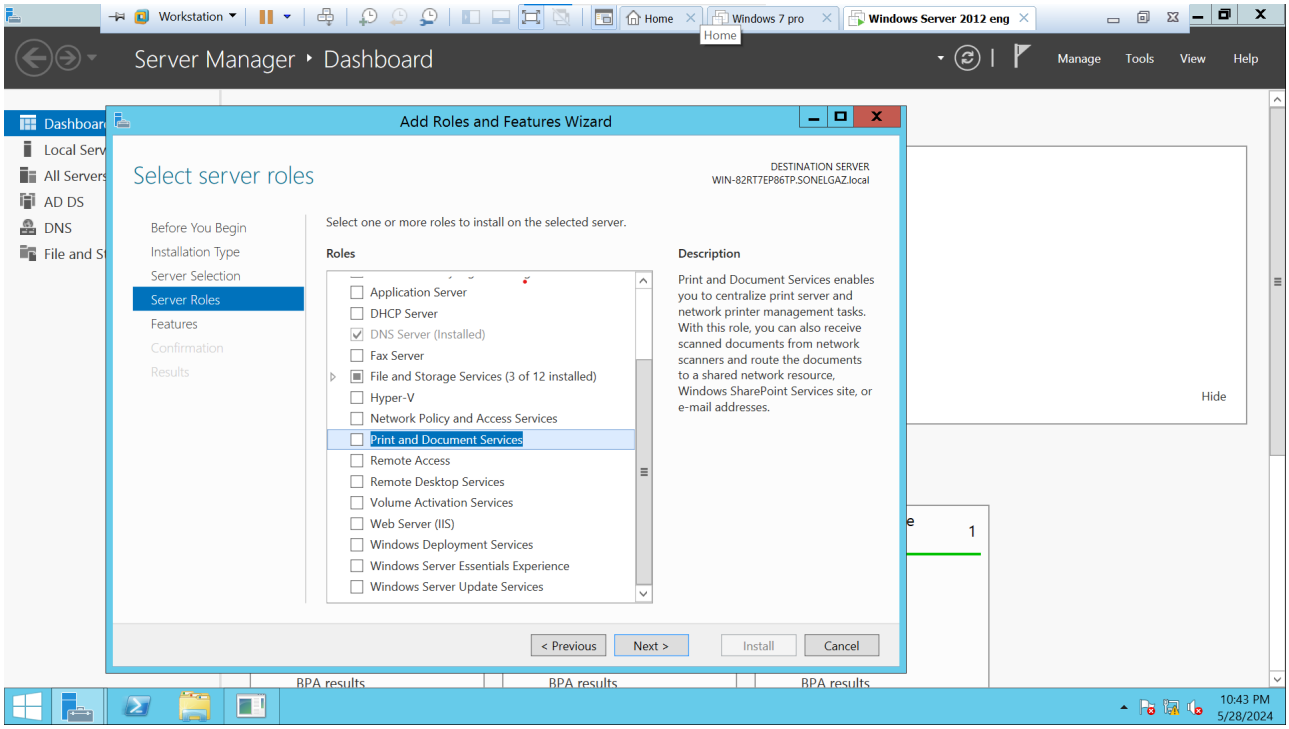


Figure 3.39 – Roles de serveurs

Et voici le résumé des composants qui seront installés et enfin on clique sur "Installer"

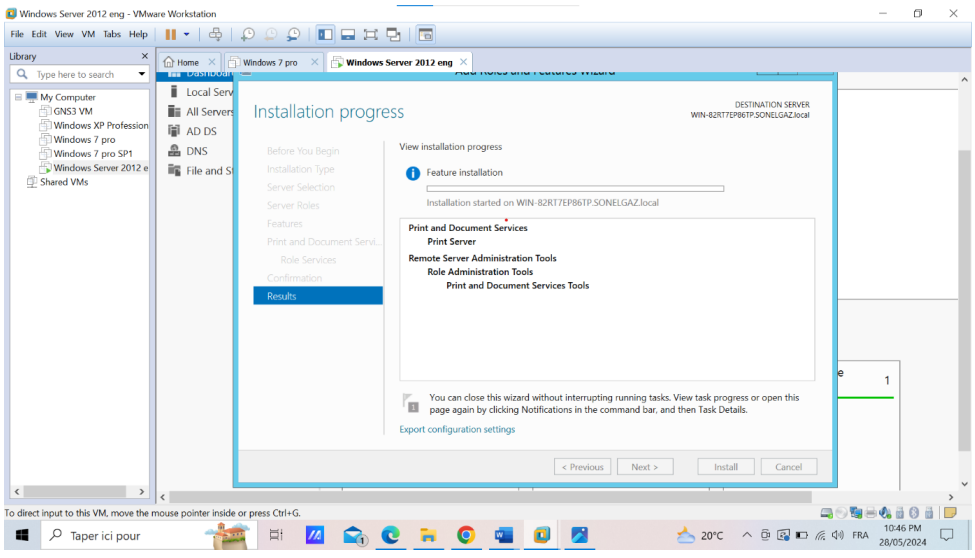


Figure 3.40 – Resultats

Une fois l'installation est terminé on peut voir dans le menu démarrer que le serveur d'impression est bien installer , comme figure ci-dessus ;

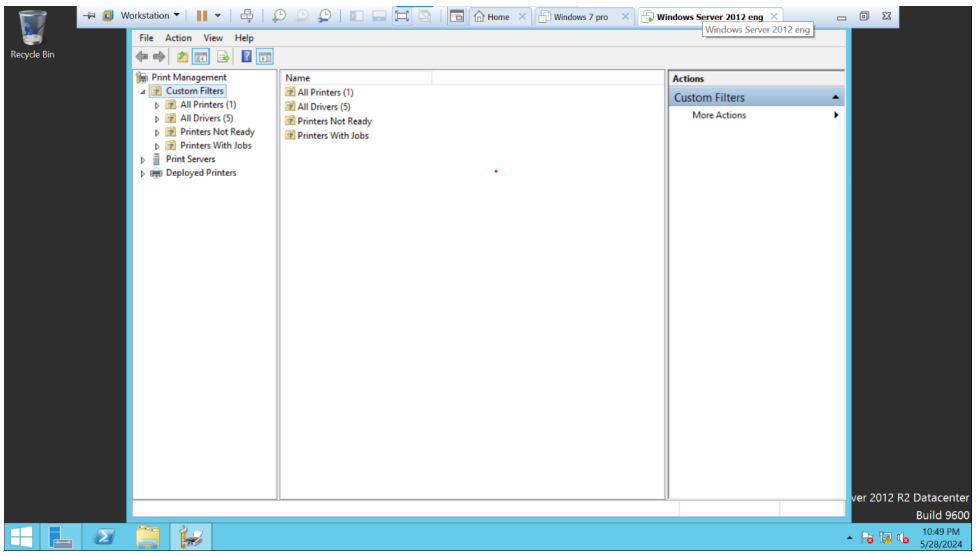


Figure 3.41 – Parametres usuels serveur d'impression

3.7 Installation d'un serveur de fichiers

Le serveur de fichier est un rôle qu'on peut ajouter après l'installation d'Active Directory ,la première étape est d'installer les rôles de serveur de fichiers pour cela on procède comme suite : Gérer > ajouter des rôles et fonctionnalités

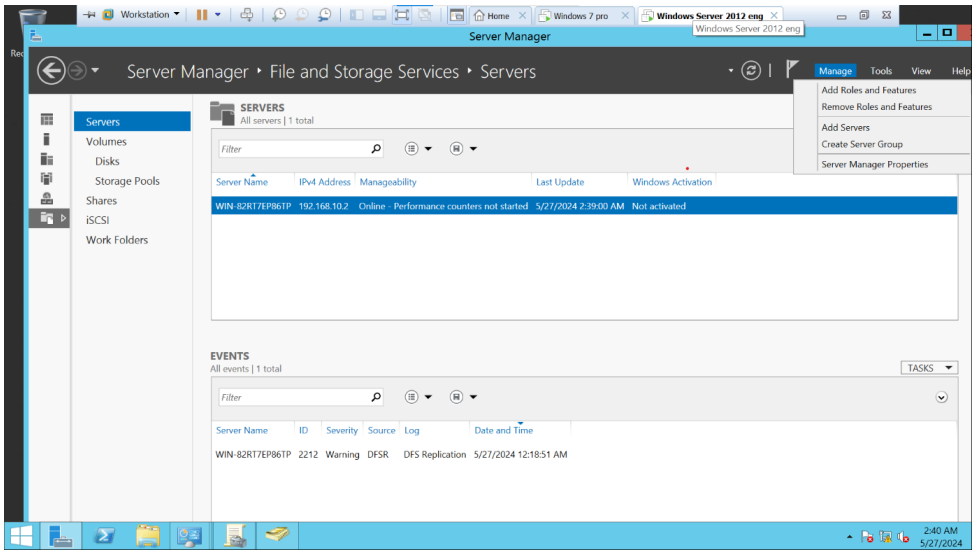


Figure 3.42 – Ajouter des rôles et fonctionnalités

On couche le gestionnaire de ressources du serveur de fichiers , avec ca on vas pouvoir gérer proprement les partages et les différents options de partage de données ;

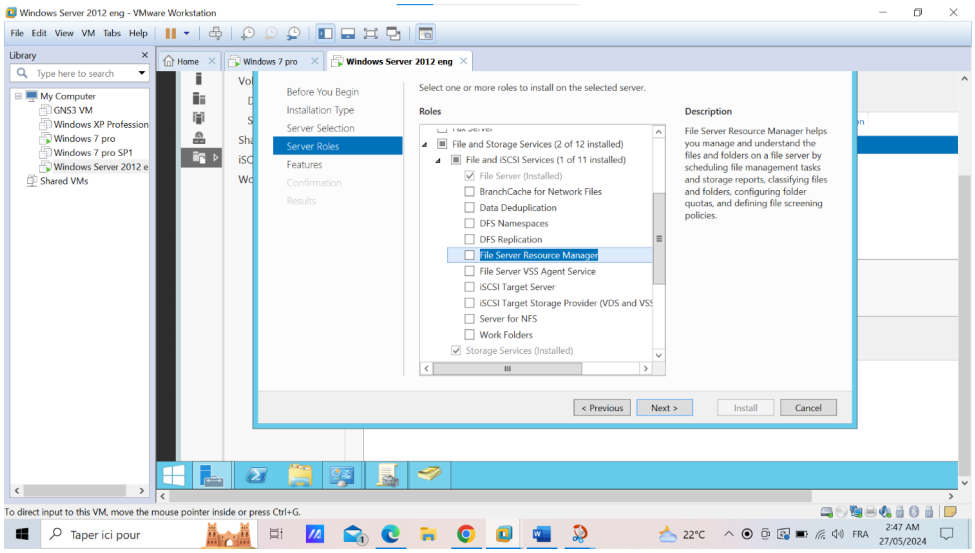


Figure 3.43 – Ajout du rôle serveur de fichier

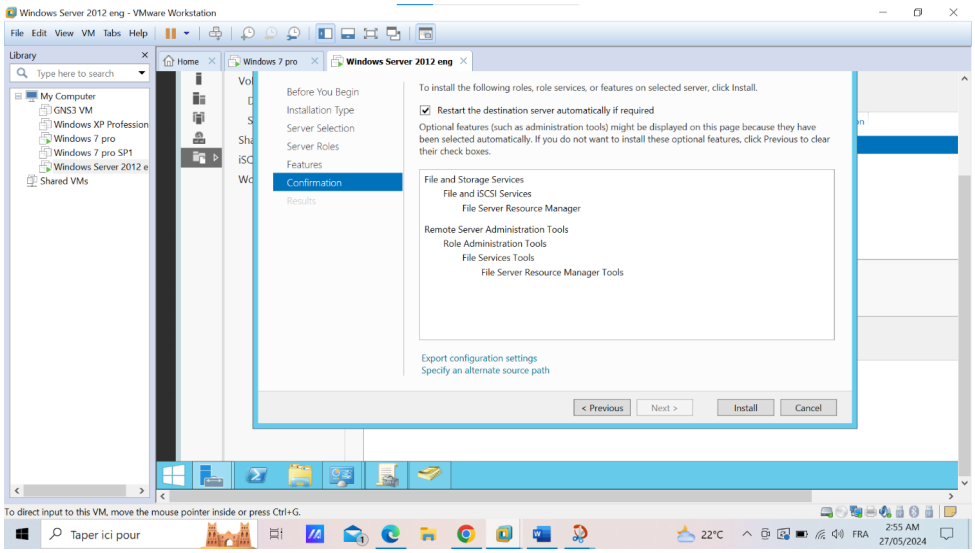


Figure 3.44 – Confirmation

On termine par installé ;

Conclusion

Ce chapitre nous a permit de découvrir l'environnement de Windows Server 2012 R2 et de se familiariser avec ces différentes composants et services ,ceci nous a permit de voir la puissance de cette environnement en terme de fonctionnalités à savoir l'organisation des ressources de l'entreprise. Dans le prochain chapitre, nous passerons à la réalisation de notre travail.

Chapitre 4

Réalisation

Introduction

Dans ce chapitre, nous verrons en détail comment créer des unités organisationnelles, gérer les utilisateurs, créer des groupes, et attribuer des droits d'accès. Nous aborderons également la configuration de divers services tels que les domaines, les approbations, les sites et les services. Nous terminerons par la mise en place de partages de fichiers et d'imprimantes sur le réseau, ainsi que la configuration des serveurs DNS et DHCP.

La gestion efficace de ces éléments est essentielle pour assurer une administration fluide et sécurisée des ressources informatiques de l'entreprise.

4.1 Résumé du projet

Dans ce projet, nous avons d'abord installé VMware sur notre machine physique. Ensuite, nous avons créé trois machines virtuelles : la première était un serveur Windows Server 2012 R2, tandis que les deuxième et troisième machines virtuelles étaient respectivement des postes de travail sous Windows 7 Professionnel et Windows 7 Enterprise.

Nous avons ensuite connecté les machines virtuelles ensemble en tant que réseau local et testé la connexion entre elles pour nous assurer que le réseau fonctionnait correctement. Enfin, nous avons procédé aux configurations des différents services essentiels de l'annuaire Active Directory.

4.2 Gérer les utilisateurs et ordinateurs Active Directory

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénoms, login, adresse e-mail, téléphone, département, etc.). Ces attributs peuvent permettre de trouver des utilisateurs dans notre domaine. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets de notre Active Directory. Lorsque vous commencerez à avoir plusieurs utilisateurs, vous pourrez les gérer par groupe.

Parmi les objets que l'on trouve dans l'Active Directory existe :

— Ordinateurs : Les ordinateurs clients intégrés au domaine, mais aussi les serveurs et les contrôleurs de domaine.
— Utilisateurs : Comptes utilisateurs qui permettent de s'authentifier sur le domaine, et accéder aux ressources et ordinateurs.
— Imprimantes : Ressource de type "imprimante".
— Unités d'organisations : Dossier pour créer une arborescence et organiser les objets.
— Groupes : Regrouper des objets au sein d'un groupe, notamment pour simplifier l'administration.
— Contacts : Enregistrer des contacts, sans autorisation d'authentification.

La gestion des utilisateurs d'un domaine ne peutse faire que si le rôle Active Directory est installé.
Pour vérifier si c'est bien le cas on peut utiliser le " Gestionnaire de serveur " qui, en principe, s'ouvre au démarrage du serveur.

Ici on peut voir que le rôle Active Directory, nommé " AD DS ", est bien installée

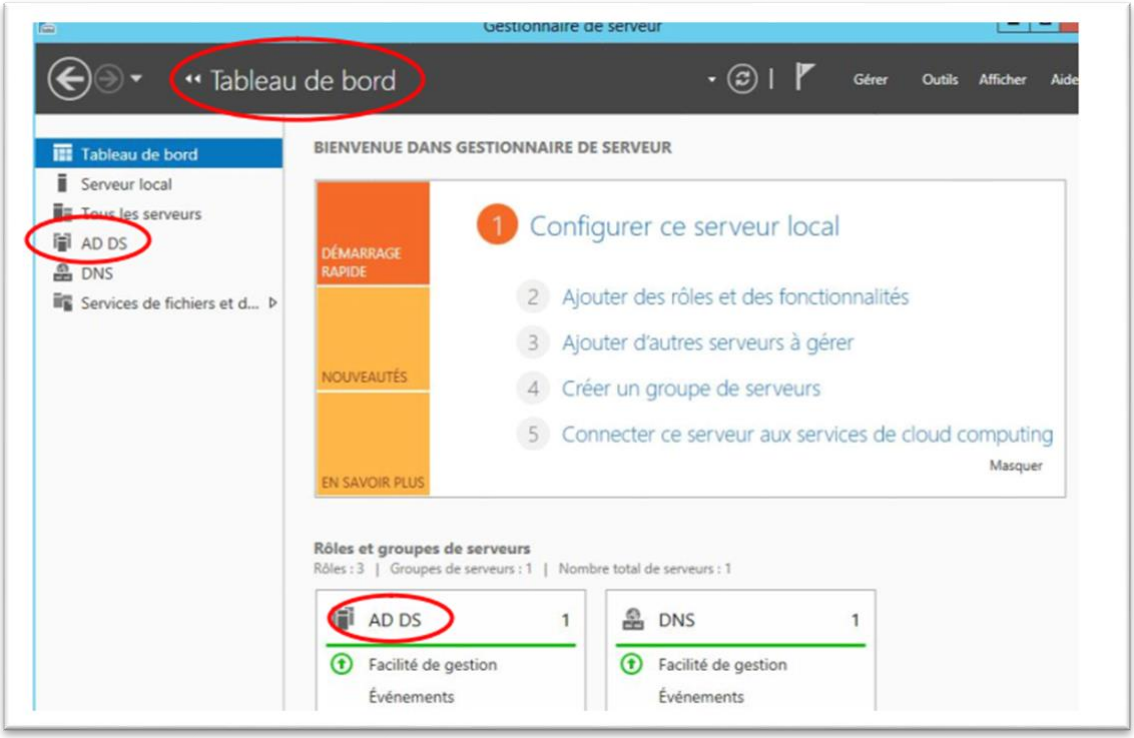


Figure 4.1 – Rôle Active Directory

Le gestionnaire des utilisateurs est accessible via le menu " Outils " du " Gestionnaire de serveur".On sélectionne ensuite "Utilisateurs et ordinateurs Active Directory ".

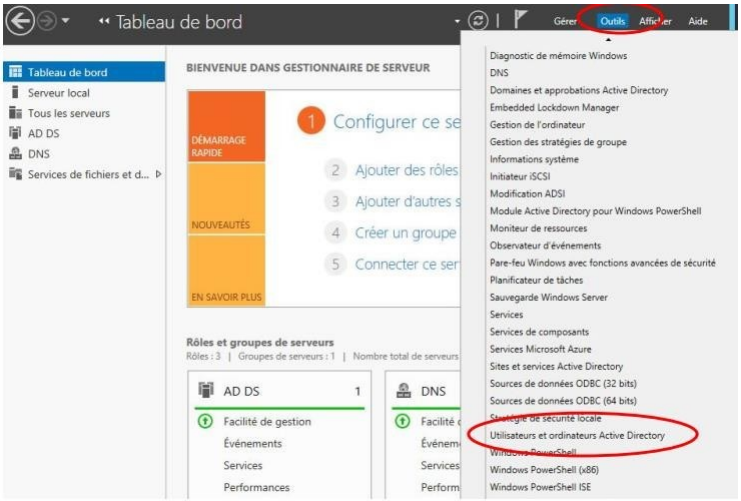


Figure 4.2 – Tableau de bord

La fenêtre du gestionnaire " Utilisateurs et ordinateurs Active Directory " est la suivante :

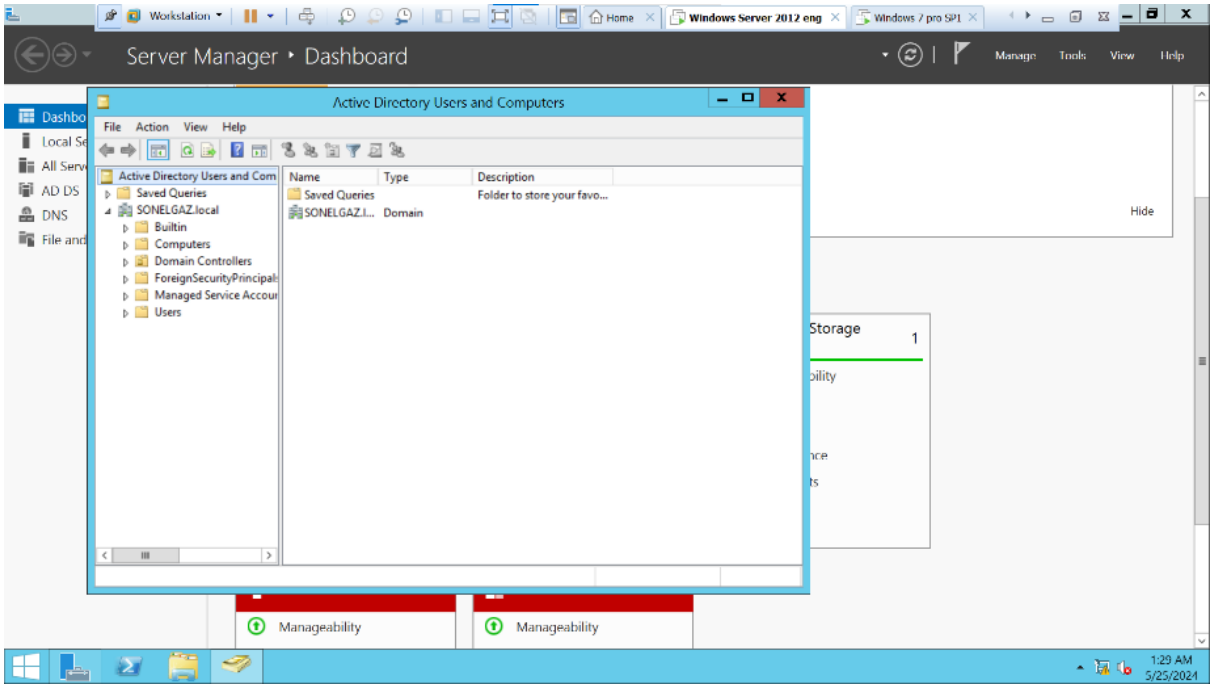


Figure 4.3 – Utilisateurs et ordinateurs Active Directory

Ensuite dans le dossier "Users" pour afficher la liste des utilisateurs existants.
On peut constater que par défaut il y a déjà quelques utilisateurs et beaucoup plus de groupes.

4.2.1 Création des unités organisationnelles :

Pour créer une unité organisationnelle il suffit faire un clique droit sur notre domaine ->nouveau -> unité d'organisation comme illustré ci-dessus :

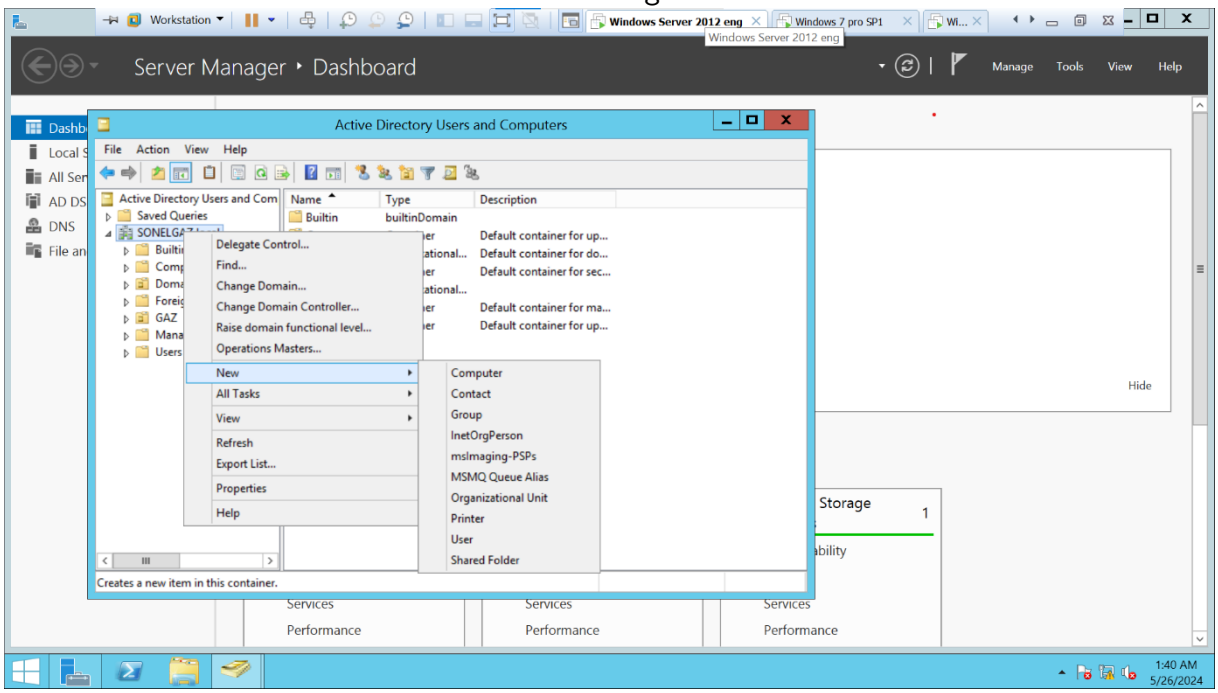


Figure 4.4 – Ajout et création des unités d'organisation

Cette procédure nous permet de regrouper des ordinateurs ou des utilisateurs dans une seule unité afin de pouvoir leurs appliquer des procédures et des stratégies de groupes.
Dans notre cas on a nommé l'Unité Organisation racine :" GAZ ";
Ensuite, on a crée deux autre unités ou chaque unité représente un département on a choisi DEPT INFO (informatique)et DEPT COM(communication) . Et puis crée et déplacé les utilisateurs et les ordinateurs sur lesquels on veut appliquer des stratégies de groupes, comme le montre l'image suivantes :

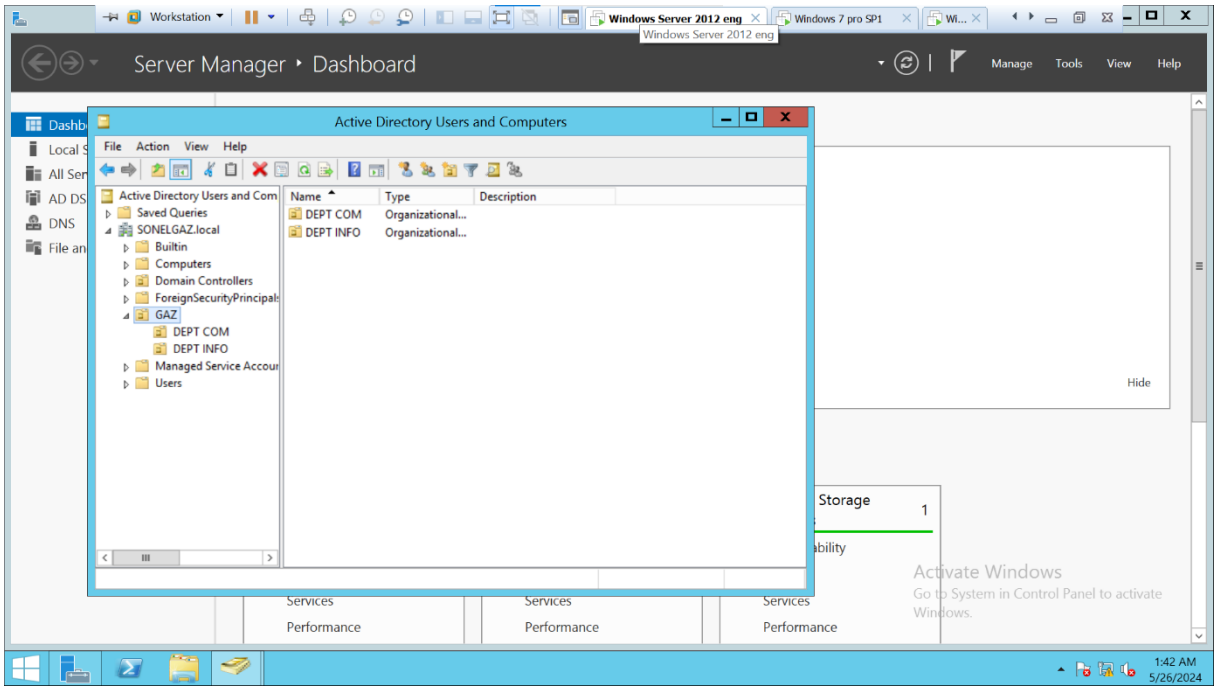


Figure 4.5 – Les unités et sous-unités d'organisation crées

Une fois que l'utilisateur appartient à un département dans le contrôleur de domaine, on doit l'ajouter à l'unité d'organisation pour lui attribuer des droits d'accès, ainsi que le partage de fichiers et d'autres ressources, à condition qu'il soit ajouté au domaine.

4.2.2 Création des utilisateurs :

Pour ajouter des utilisateurs à gérer dans Active Directory, on doit suivre les étapes suivantes : Gérer des utilisateurs et des ordinateurs -> Utilisateurs -> Nouvel utilisateur, puis on remplit les champs nécessaires comme le montre la figure suivante :

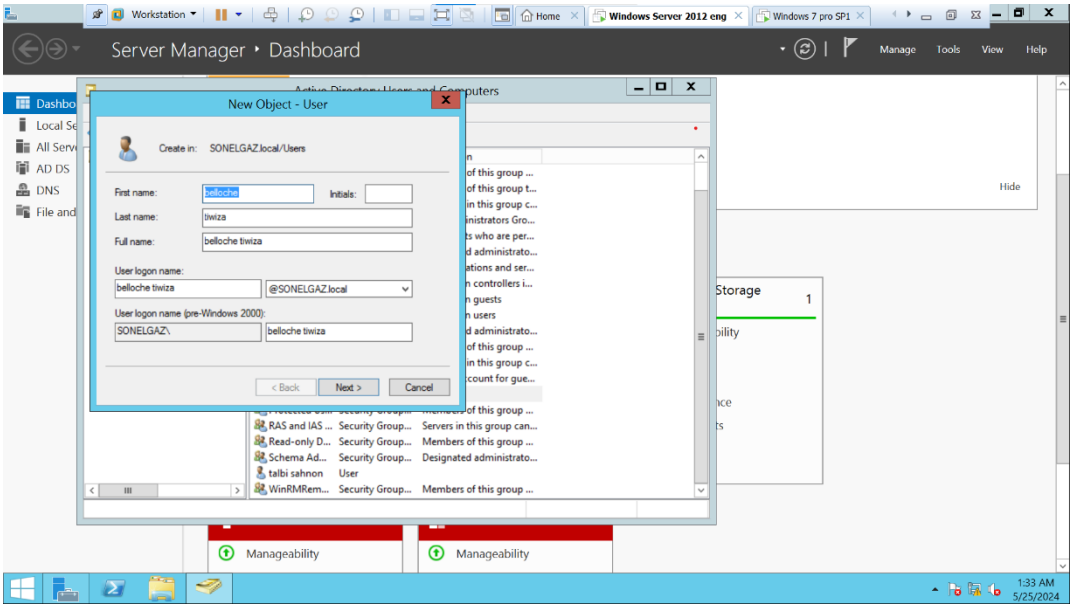


Figure 4.6 – Création d'un utilisateur

Ensuite, une fenêtre apparaît, demandant de spécifier un mot de passe pour cet utilisateur, puis on valide en cliquant sur "OK".

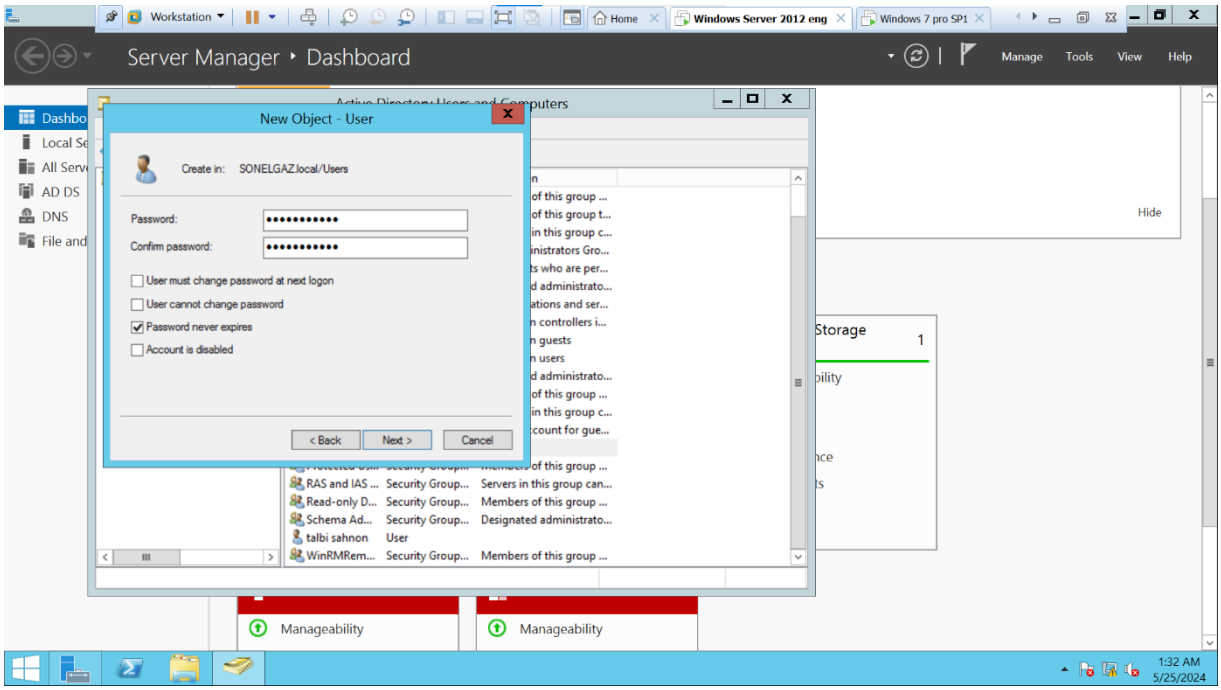


Figure 4.7 – Création d'un mot de passe utilisateur

Un message nous indique si la création s'est bien déroulée ou non(en cas d'erreur).

Pour chaque département, nous avons créé des utilisateurs et attribué des mots de passe afin de leur spécifier des comptes utilisateurs , comme illustré dans les tableaux suivants :

UTILISATEURS	MOT DE PASSE
talbi sahnon	Univ*info123
Stagiere informatique	Univ*info321

–Mot de passe des Utilisateurs créer pour département informatiques –

UTILISATEURS	MOT DE PASSE
Belloche twisa	Univ*info123
Stagiere com	Univ*info321

- Mot de passe des Utilisateurs créer pour département commercial –

Figure 4.8 – Mots de passe des utilisateurs crées

Voici la liste des utilisateurs et ordinateurs crée à chaqu'un des deux départements :

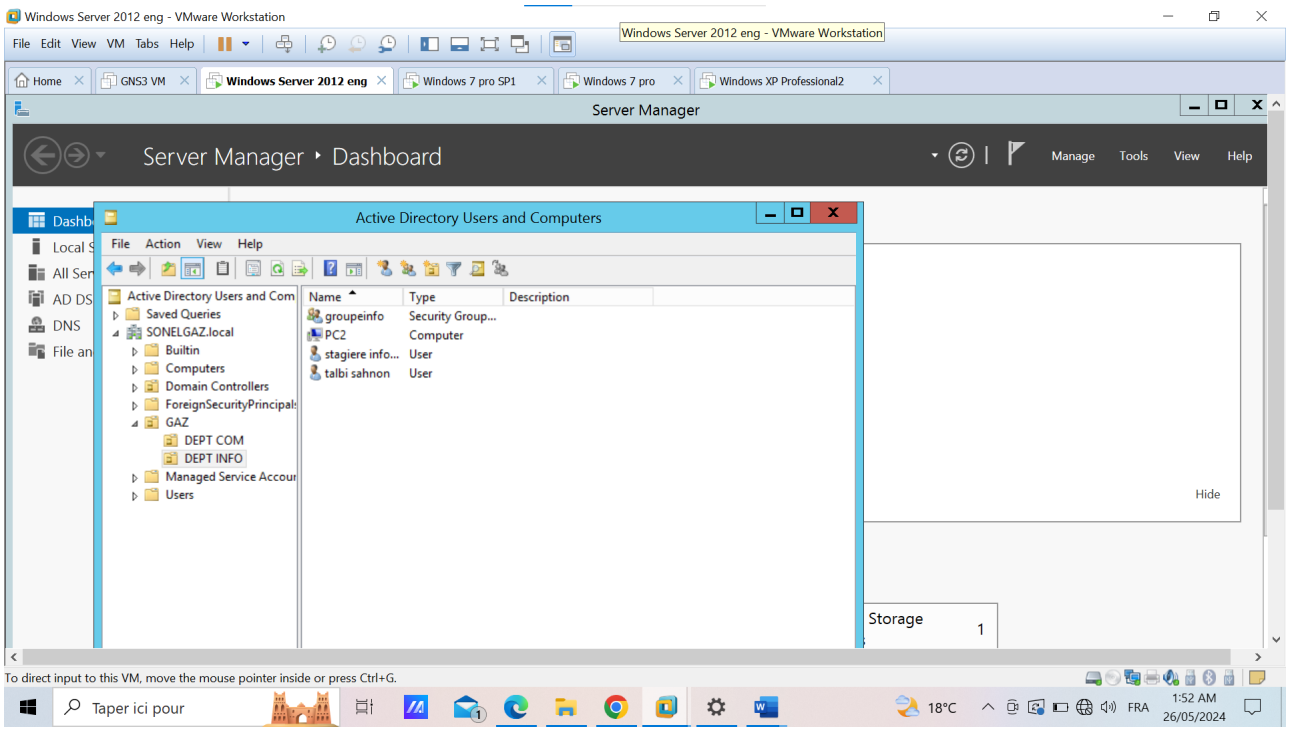


Figure 4.9 – Utilisateurs et ordinateurs DEPT INFO

Les mêmes étapes sont suivies pour la création des utilisateurs dans le deuxième département, qui est le département commercial, comme expliqué dans la figure suivante :

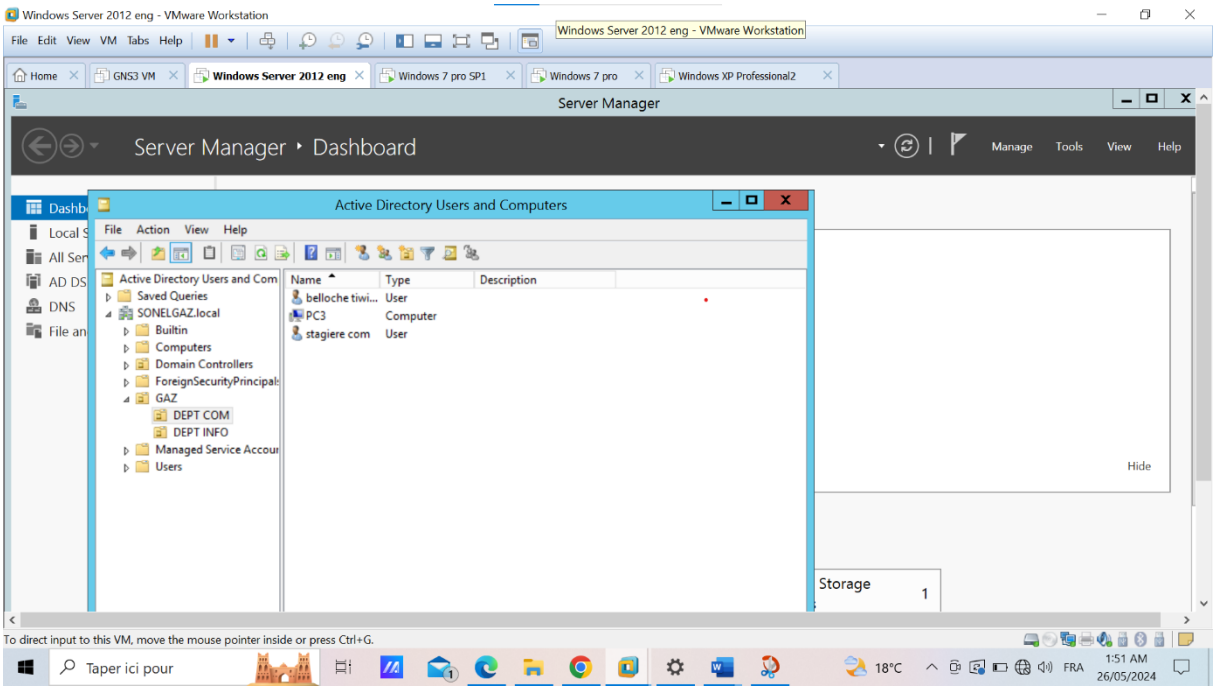


Figure 4.10 – Utilisateurs et ordinateurs DEPT COM

4.2.3 Création des Groupes :

Les groupes peuvent contenir des utilisateurs, des ordinateurs et d'autres objets, simplifiant ainsi la gestion d'un grand nombre d'entités. Nous avons créé deux groupes comme suit :

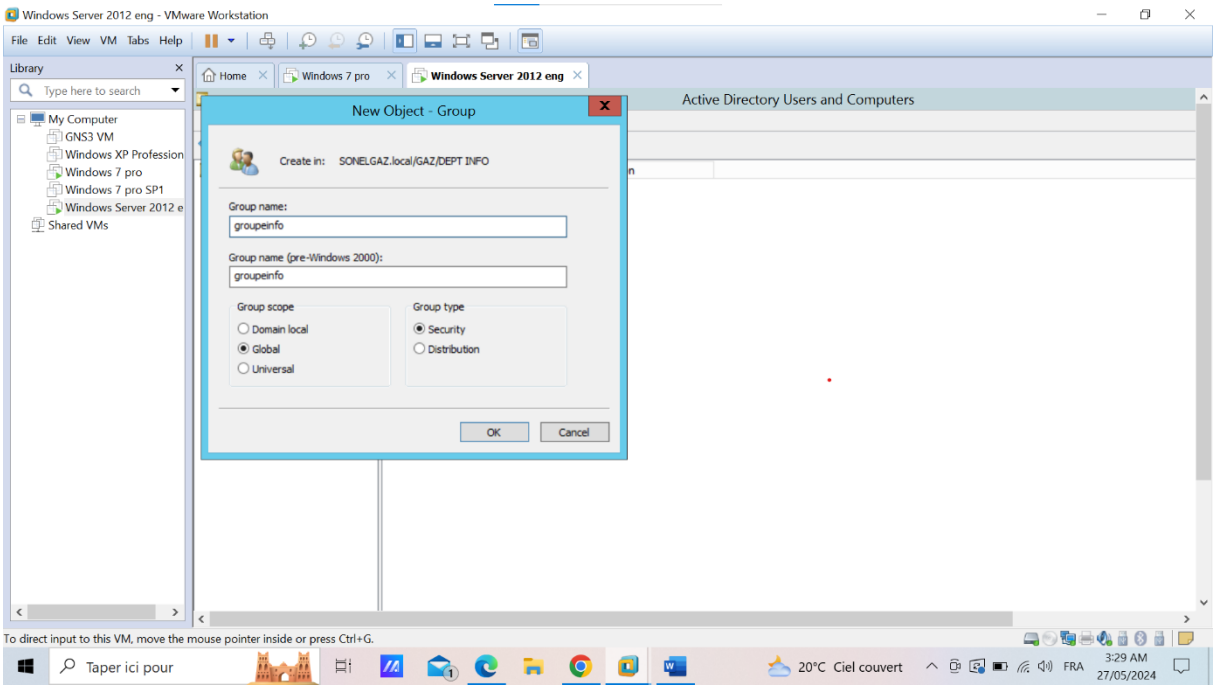


Figure 4.11 – Création du Groupe "groupeinfo"

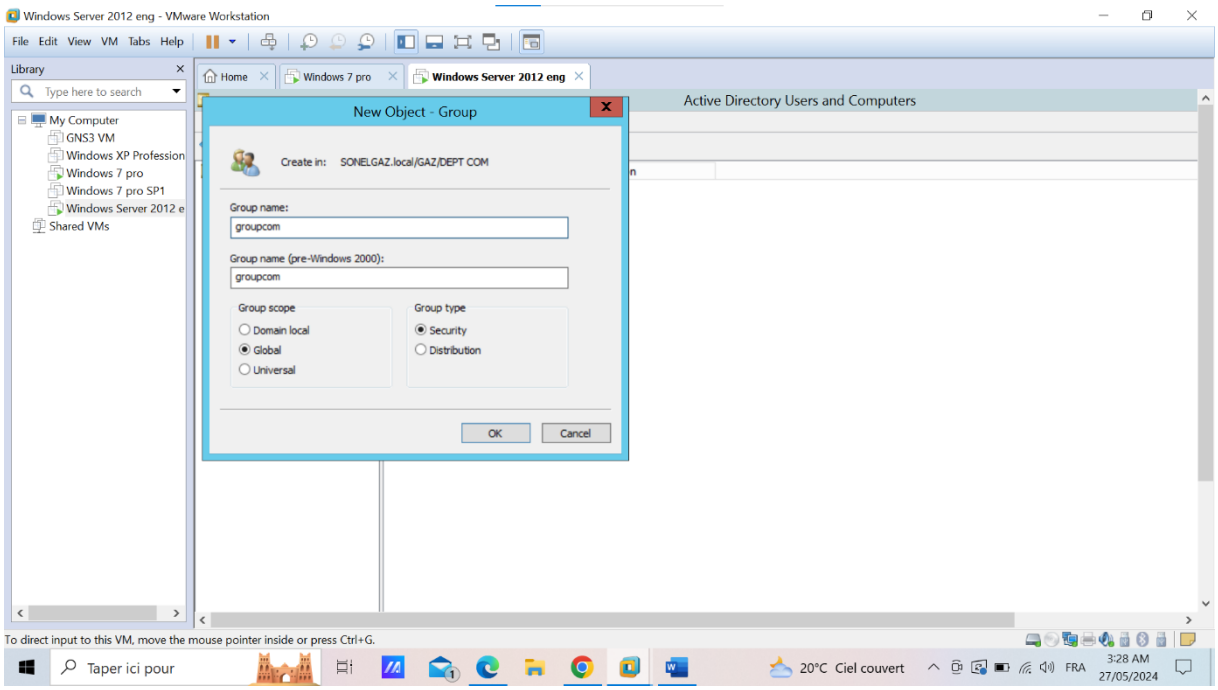


Figure 4.12 – Création du Groupe "groupecom"

Ensuite, l'ajout des utilisateurs aux groupes respectifs se déroule comme suit : Les membres du "groupeinfo" sont "Talbi Sahnon" et "Stagiere Informatique".

clique droit sur un utilisateur >ajouter a un groupe

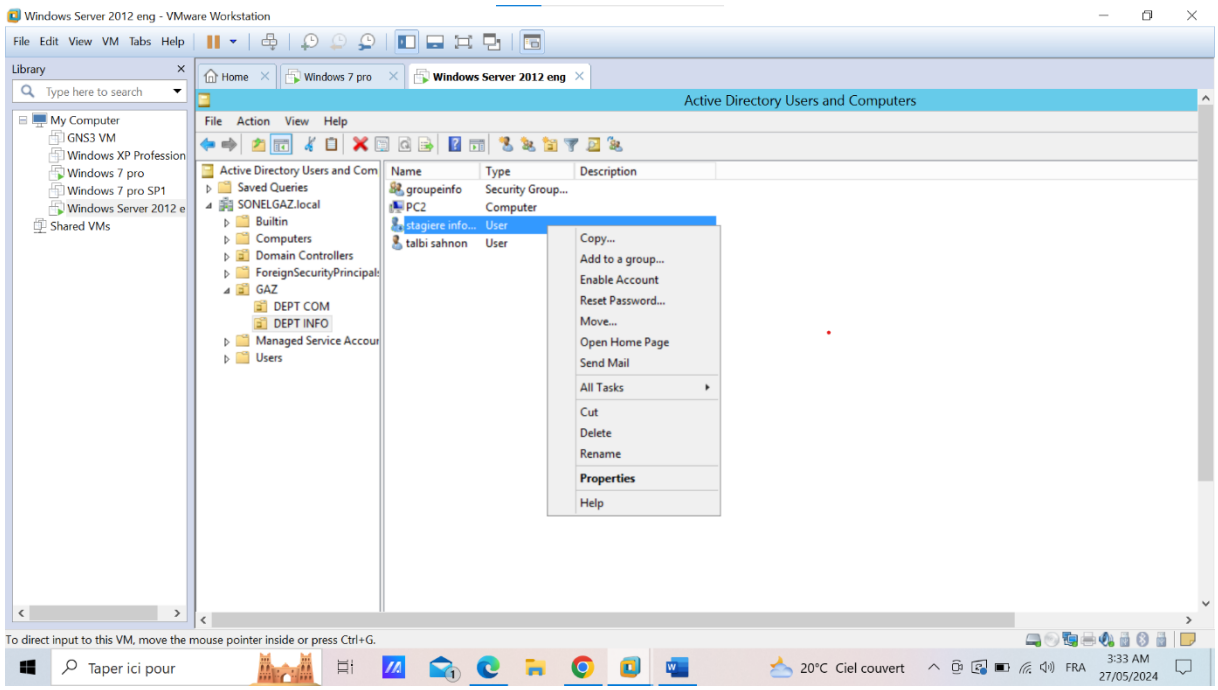


Figure 4.13 – Interface d'ajout d'un utilisateur à un groupe

Entrer le nom du groupe souhaité puis valider ;

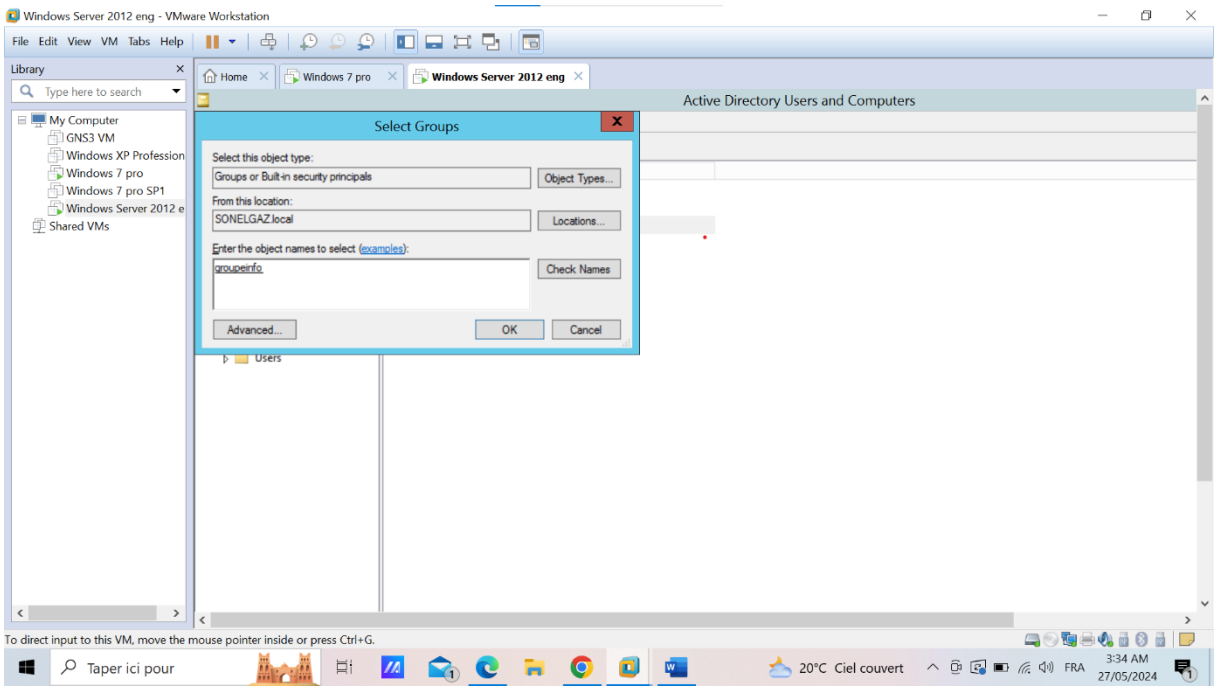


Figure 4.14 – saisie le nom du groupe

L'utilisateur a bien étais ajouté ;

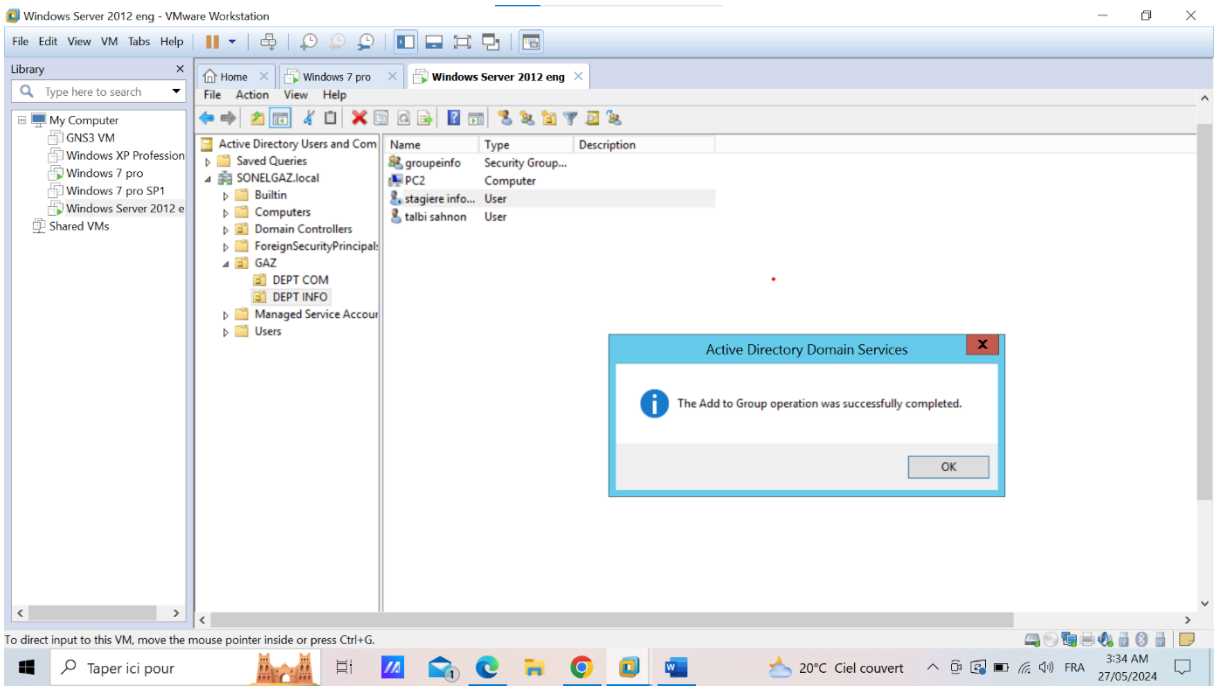


Figure 4.15 – Interface de confirmation que l'utilisateur a bien été ajouter

La même chose pour les membres du "groupecom" : "Belloche Tiwisa" et "Stagierecom".

4.2.4 Spécification d'Horaires d'accès au compte utilisateurs :

Bien que cet outil soit intégré dans l'annuaire Active directory, l'administration du serveur sera effectuée d'une manière souple et performante ; pour chaque compte utilisateurs en peut le programmé des horaires d'ouverture de session journée et heure d'accès :
Pour belloche tiwiza par exemple en peut lui programmé l'ouverture de session autorisée est pour mardi , de 9 :00 à 12 :00 ;

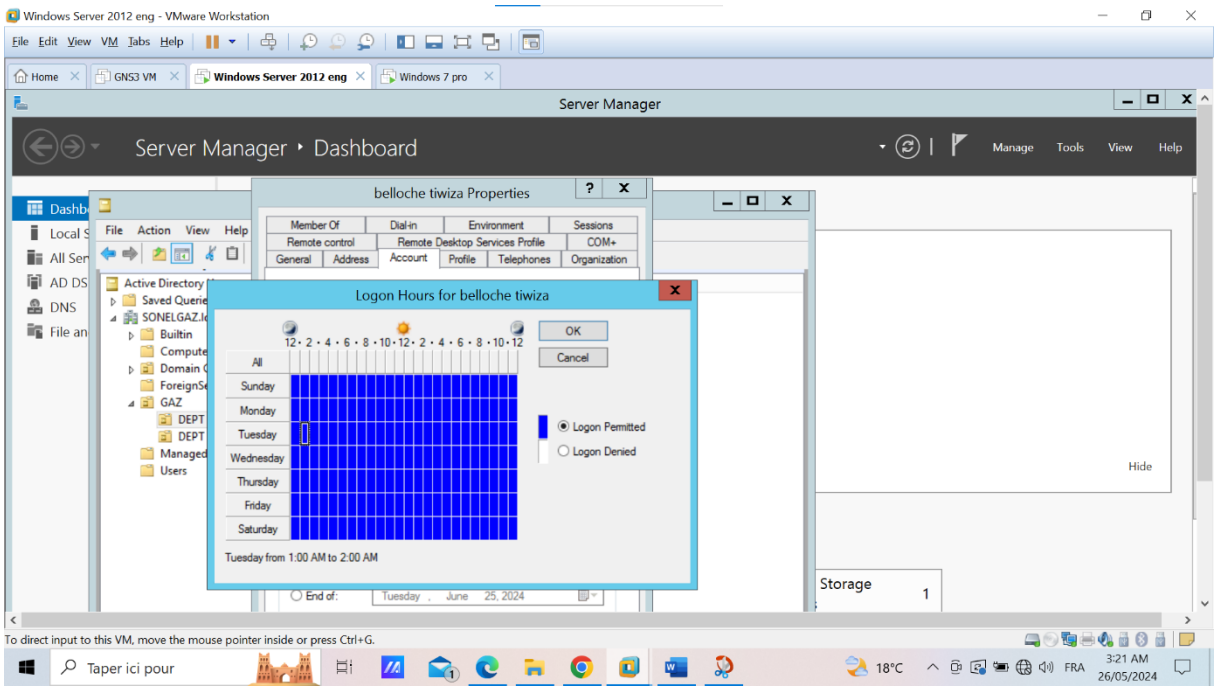


Figure 4.16 – Horaire d'ouverture de session autorisé pour l'utilisateur Belloche

De même pour l'utilisateur Talbi on accède de la façon suivante : Gestion de serveur - > utilisateurs -> propriétés -> compte -> horaire d'accès

La fenêtre ci-dessous va figurer :

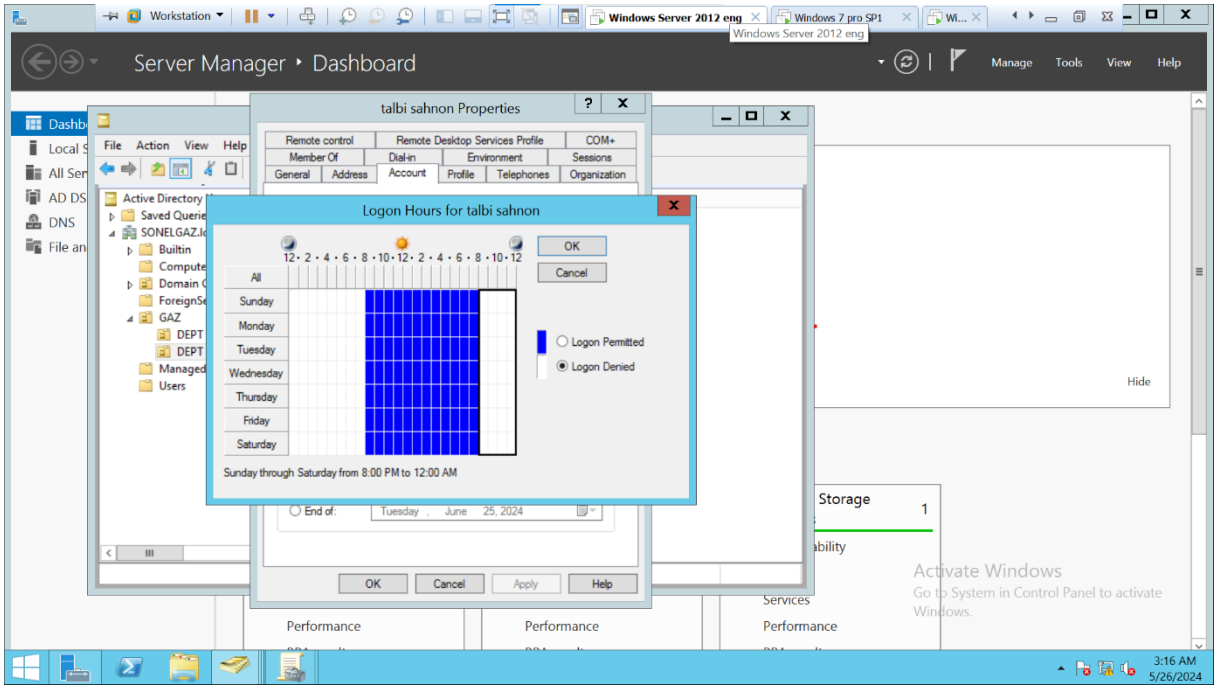


Figure 4.17 – Horaire d'ouverture de session autorisé pour l'utilisateur Talbi

4.2.5 Rendre un utilisateur administrateur du domaine :

Clique droit sur le nom de l'utilisateur puis on selectionne propriétés

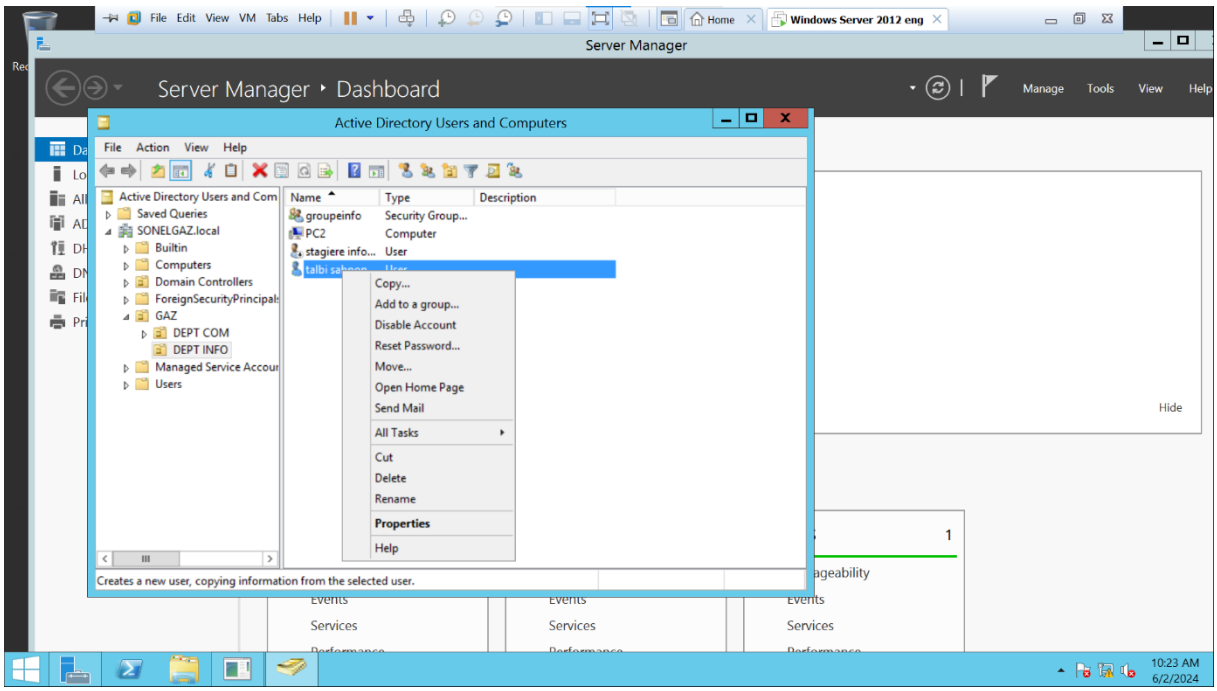


Figure 4.18 – choix de l'utilisateur

La fenêtre suivante va apparaître ; elle donne une description des propriétés de l'utilisateur choisi, comme illustré ci-dessous :

on clique sur le bouton membre de -> ajouter ->avancé

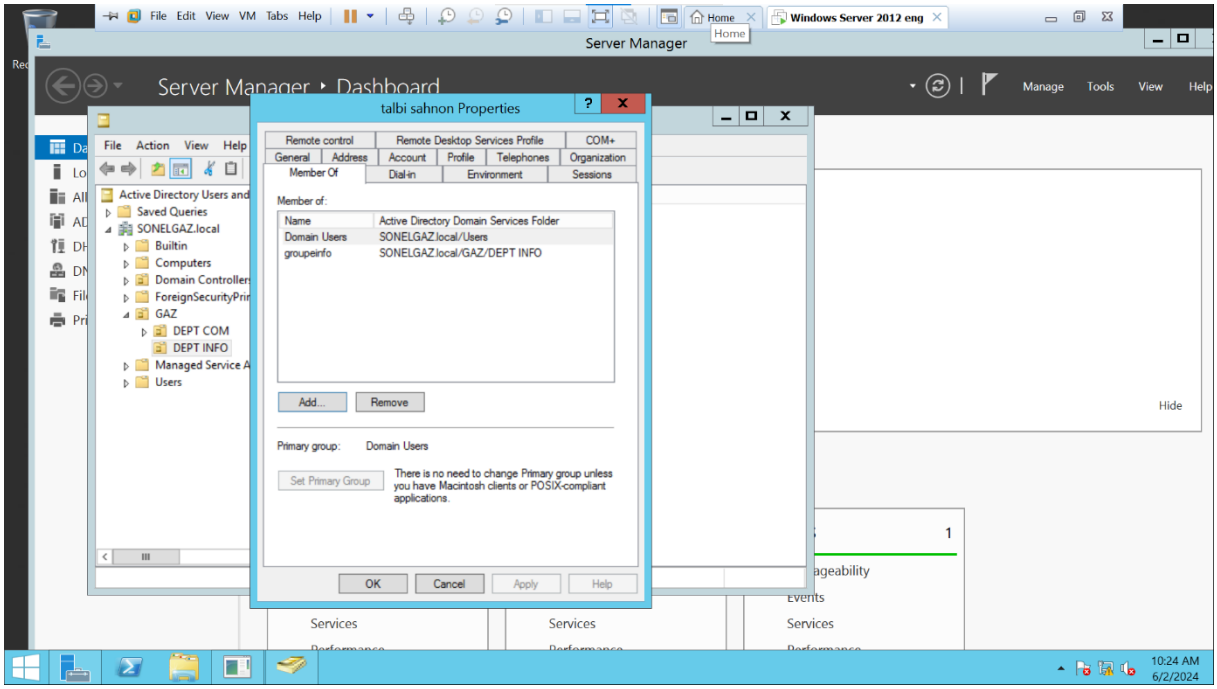


Figure 4.19 – les propriétés de l'utilisateur

On choisit "Administrateur du domaine" puis on valide.

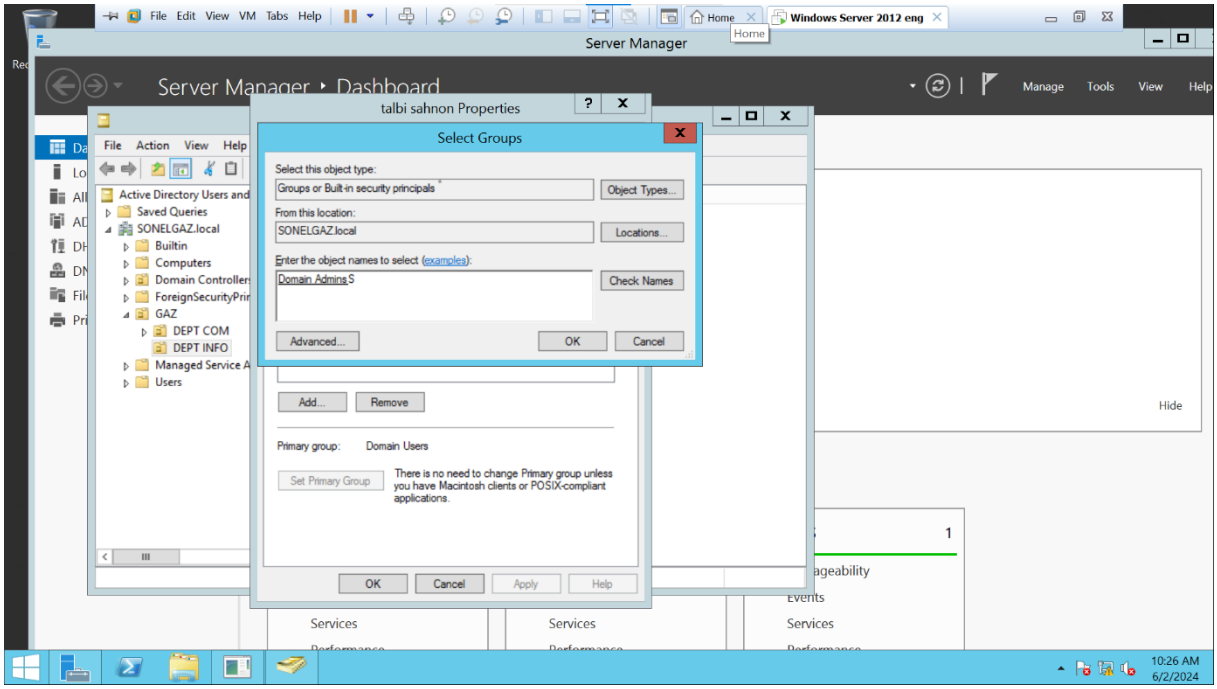


Figure 4.20 – Administrateur du domaine

Les autres utilisateurs seront uniquement des membres du domaine avec des droits limités par rapport à l'administrateur du domaine. Ils pourront seulement consulter les données partagées, mais pas les modifier.

4.3 Gérer les domaines et les approbations

Ce service réalise l'administration des utilisateurs, des groupes d'utilisateurs et des ordinateurs d'un domaine (il leur a attribué un compte) : Création, destruction et propriétés ;

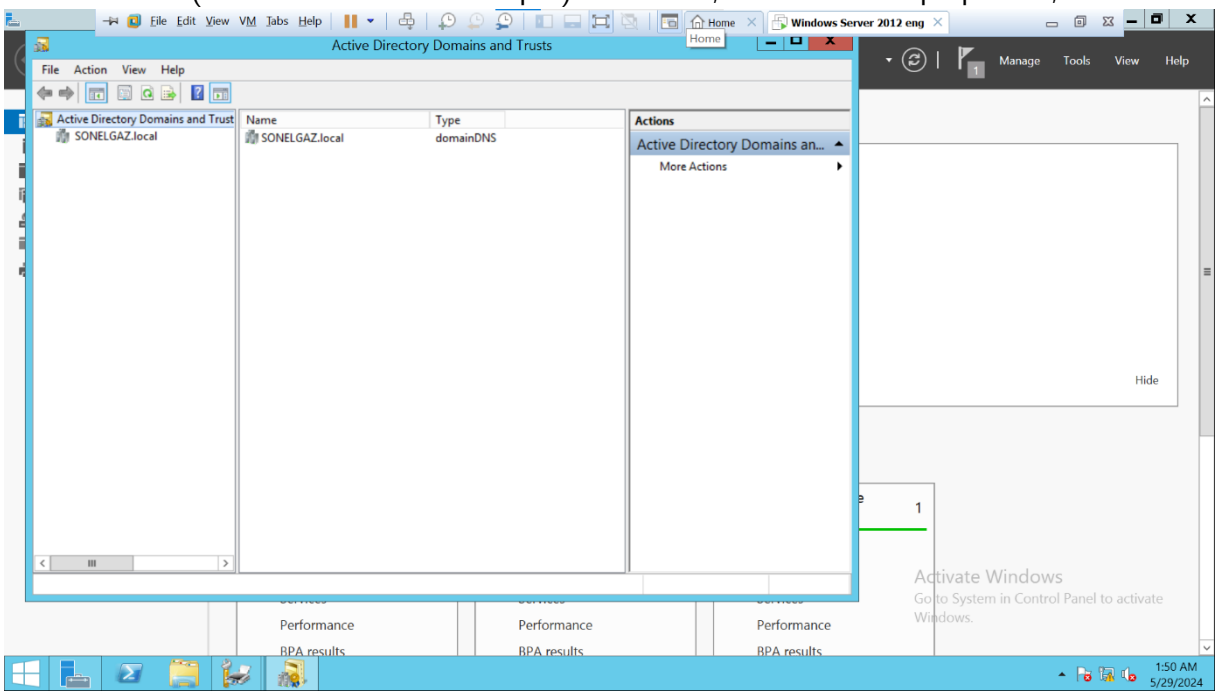


Figure 4.21 – les domaines et les approbations

4.4 Gérer les sites et les services

Grâce à cet outil, un administrateur peut gérer chaque domaine de la forêt, gérer des relations d'approbations entre domaines, configurer le mode d'opération pour chaque domaine (mode natif ou mixte) et configurer les autres suffixes UPN (User Principal Name) pour la forêt.
Lors de la création du premier contrôleur de domaine, on coche la case catalogue global une fois, mais si on veut répliquer les données alors on crée un deuxième contrôleur de domaine et on coche la case " catalogue global "
Dans notre cas pratique on a crée une forêt nommée : SONELGAZ et un domaine SONELGAZ.local qui contient un site du même nom.
Et le site approprié contient le serveur d'hébergement SERVEUR, comme illustré ci dessous :

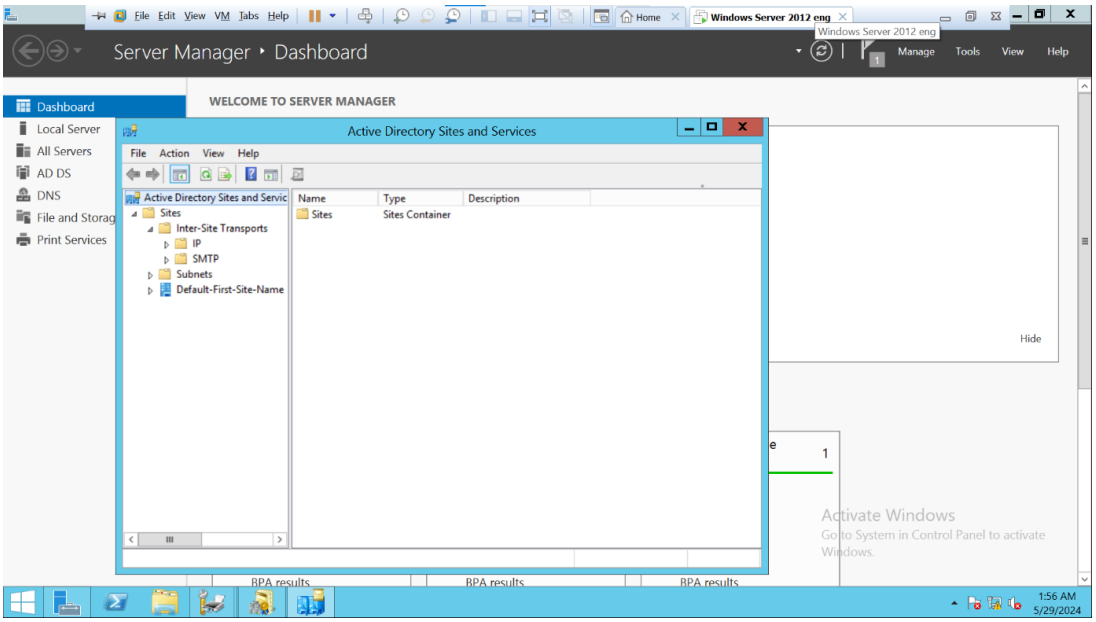


Figure 4.22 – Les sites et les services

On peut déplacer notre serveur d'un site à l'autre, autrement dit on peut héberger plusieurs sites dans un même serveur.

4.5 Configurer les clichés instantané

C'est une fonctionnalité de Windows serveur qui permet d'avoir un retour en arrière possible sur l'ensembles des données via la technologie de cliché instantané, On vas d'abord l'activé comme suite ;

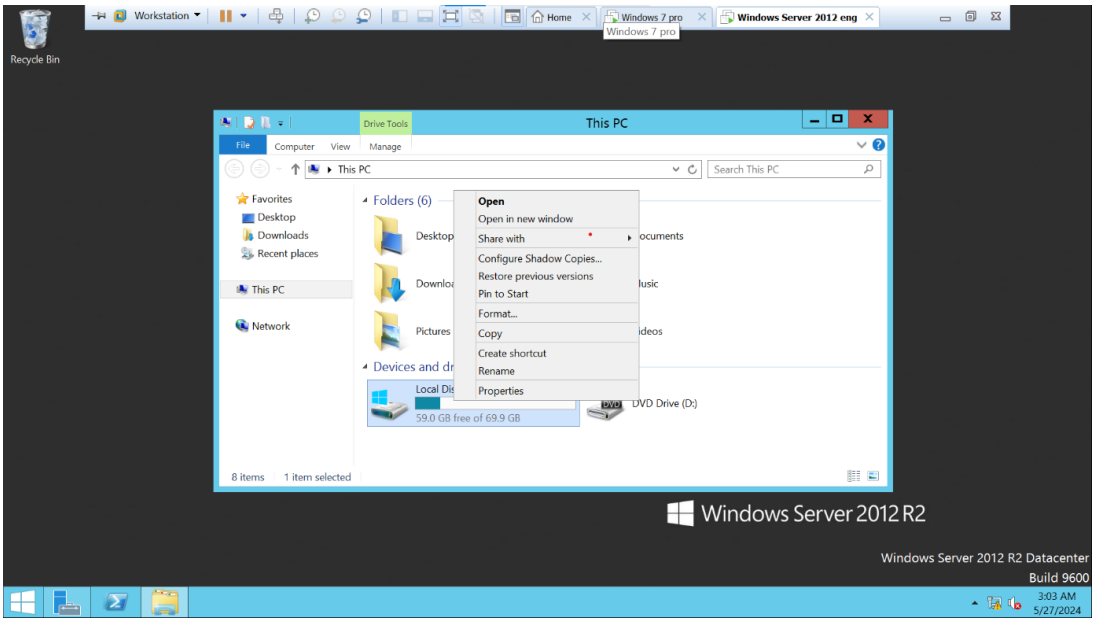


Figure 4.23 – configurer les clichés instantané

On vas sur PC clique droit et configurer les clichés instantané ;

Puis confirmation de l'activation des clichés instantané en appuyant sur oui ;

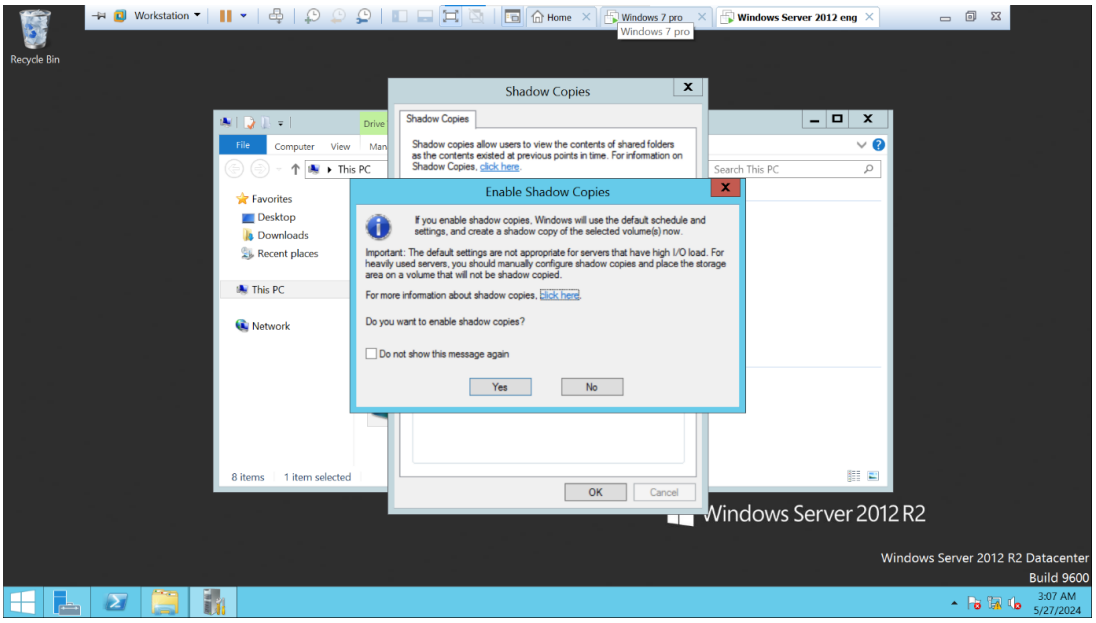


Figure 4.24 – l'activation des clichés instantané

cella vas permettre de consulter les version précédente de n'importe quel dossier ,c'est tres pratique pour revenir en arrière sur un dossier ou sur un fichier.

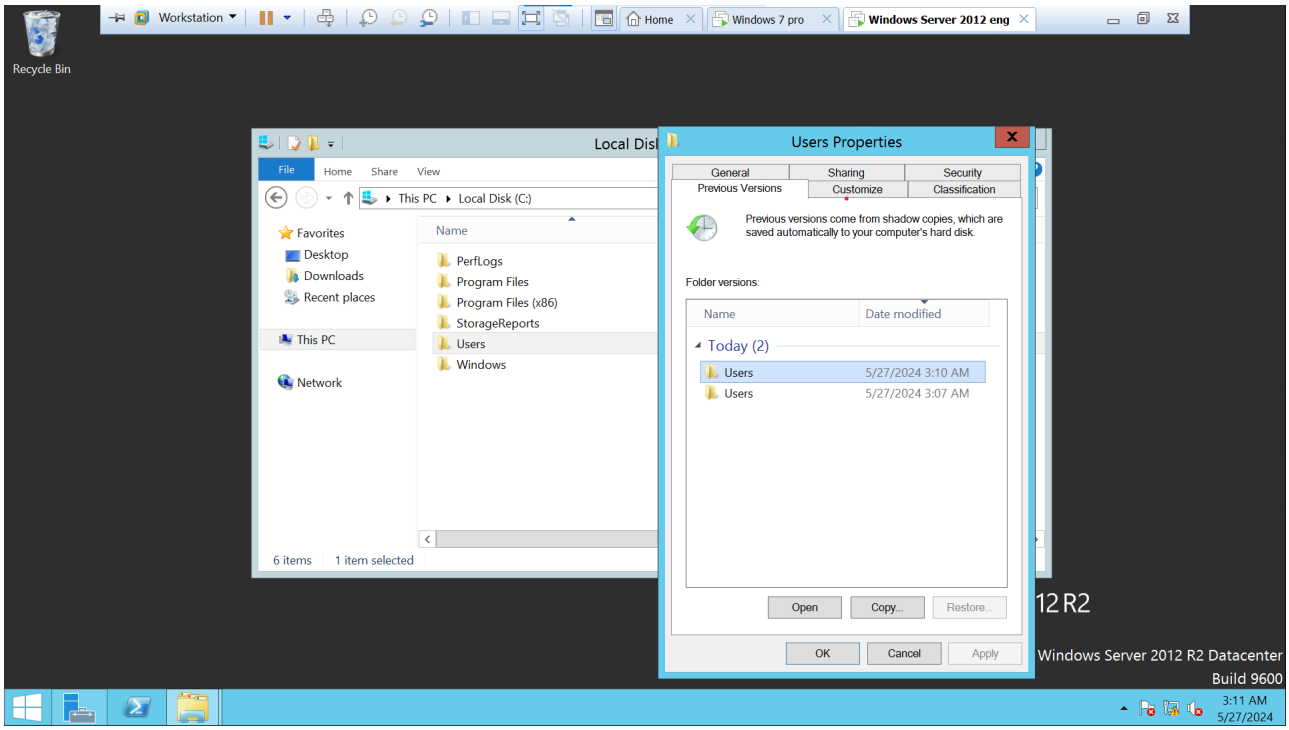


Figure 4.25 – Clichés instantané configuré

4.6 Partage de fichiers

Pour un premier partage, nous avons opté pour l'utilisation de l'explorateur de fichiers. Nous avons créé le partage de données à la racine du lecteur dédié. Cette approche vise à éviter les chemins d'accès excessivement longs. En effet, plus un chemin d'accès est prolongé, plus le risque d'atteindre la limite de caractères imposée par Windows augmente, ce qui peut poser des problèmes lors du renommage ou de la copie de fichiers.

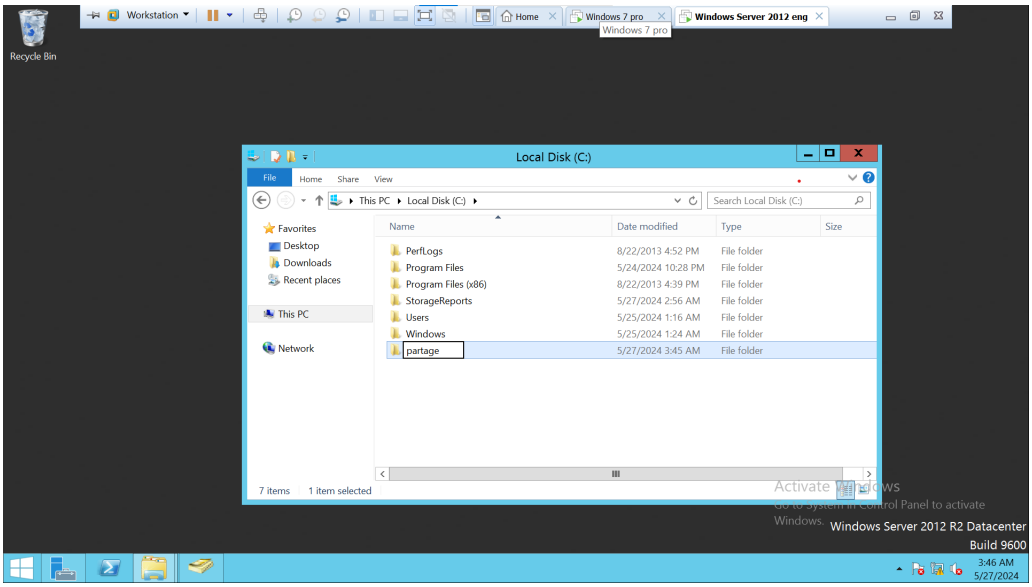


Figure 4.26 – Création du fichier Partage

Ensuite, on passe à la création des sous-dossiers a savoir DEPT INFO et DEPT COM ;

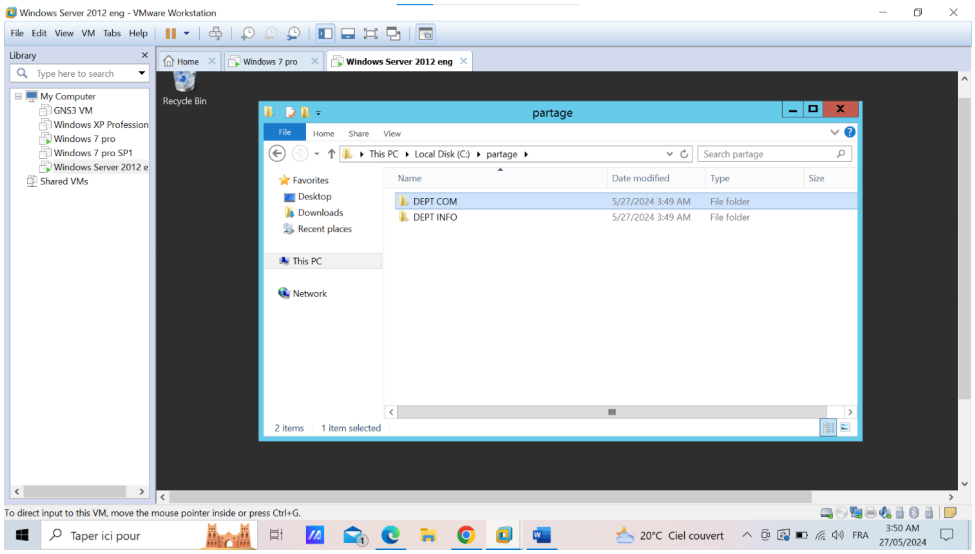


Figure 4.27 – Création des sous-dossiers DEPT INFO et DEPT COM

Par default, le dossier partage n'est pas accessible au réseau, donc on selectionne le dossier à partager et on affiche ses propriété, puis on clique sur partage.

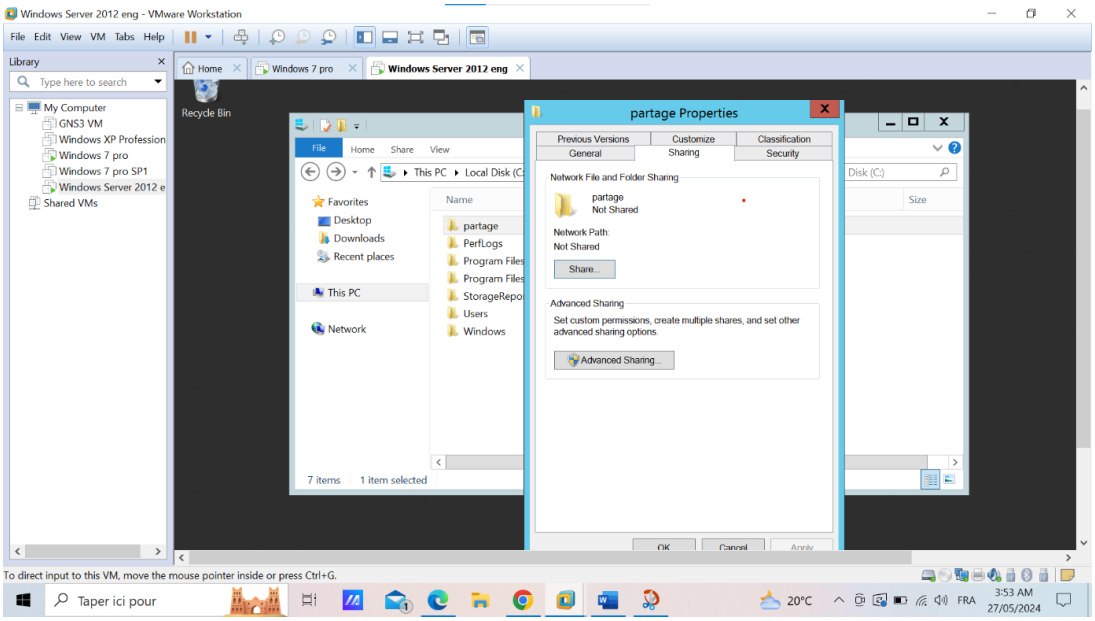


Figure 4.28 – Partage proprieté

Ensuite, on clique sur "Partage avancé" et on coche la case "Partager ce dossier" pour rendre le dossier accessible via le réseau. On peut également limiter le nombre total d'utilisateurs autorisés.

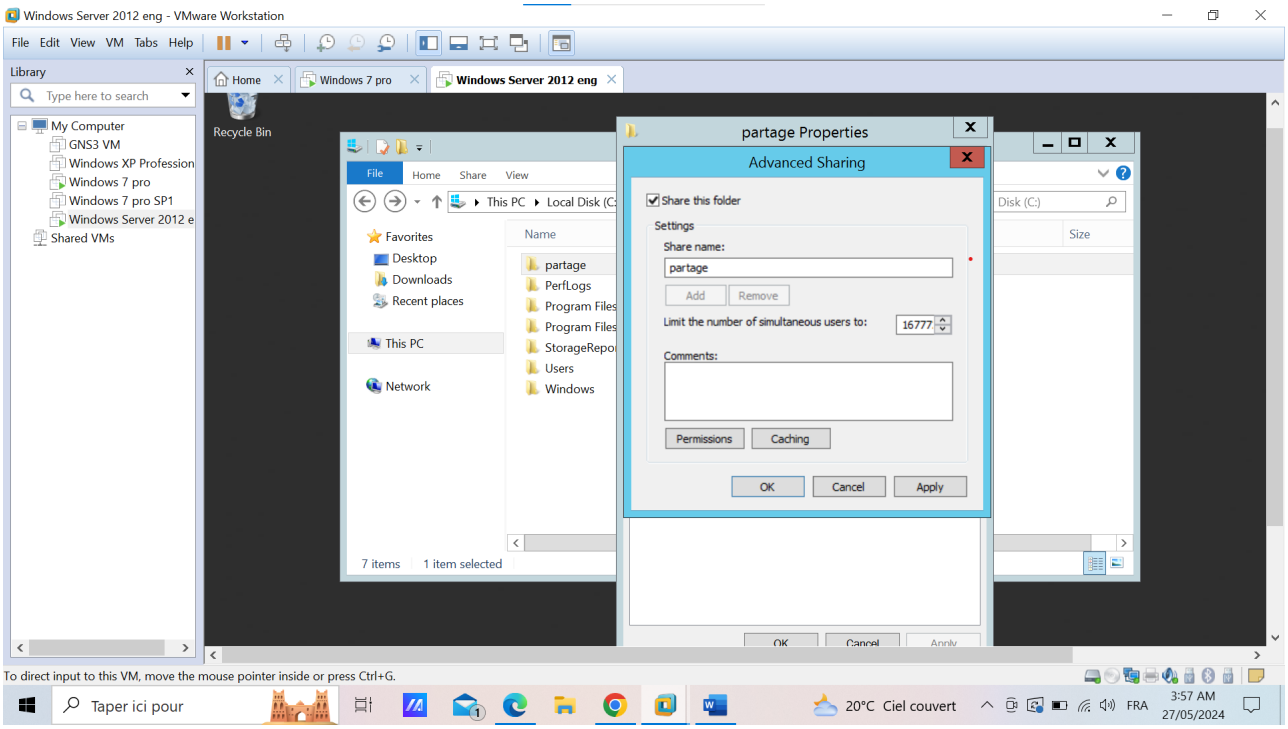


Figure 4.29 – Gestion du nombre d'utilisateurs total ;

On clique sur "Autorisation" pour gérer les accès au partage. On supprime "Tout le monde" et on ajoute "Utilisateur de domaine", en cochant les cases "Lecture" et "Modifier".

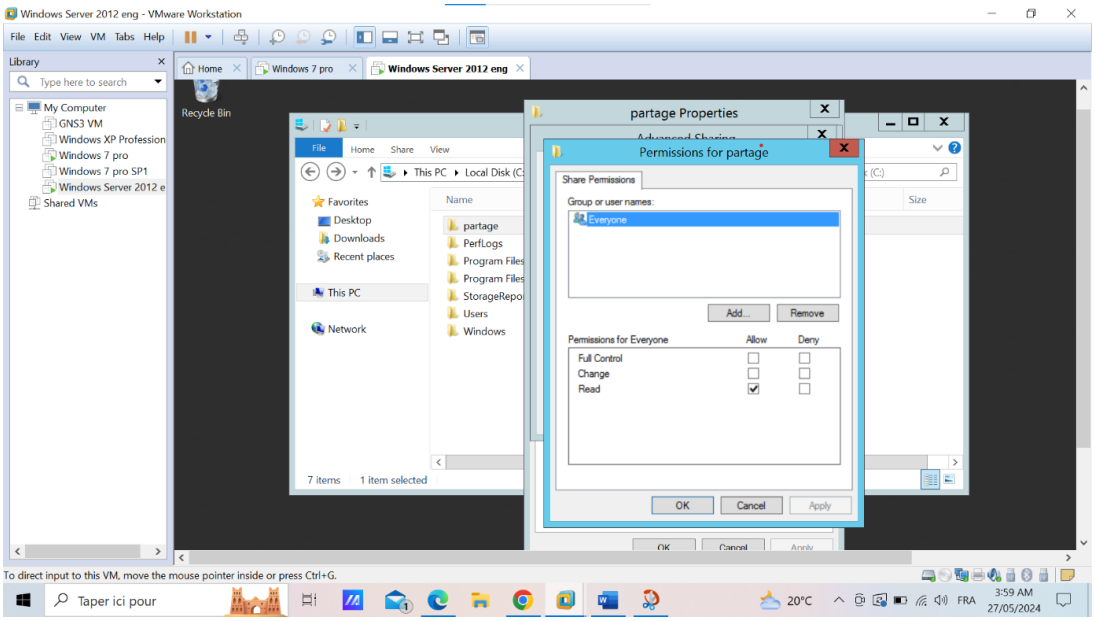


Figure 4.30 – drois d'accées sur le fichier partagé

On voit que le dossier est partagé donc il est accessible sur le réseau ;

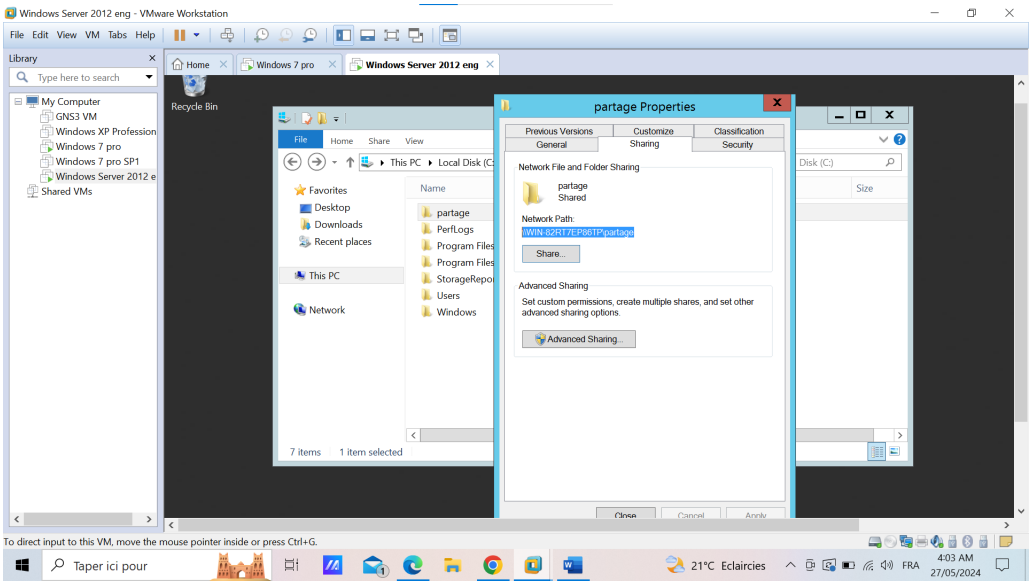


Figure 4.31 – Partage du dossier

4.7 Gestion des droits d'accès NTFS

Les droits d'accès NTFS sur un serveur de fichiers déterminent les autorisations pour accéder, modifier ou supprimer des fichiers et des dossiers, permettant un contrôle précis sur les données. Les permissions incluent la lecture, l'écriture, l'exécution, la modification des attributs et le contrôle total. NTFS permet une gestion fine des permissions, renforçant la sécurité et protégeant l'intégrité des données.

Pour gérer les droits d'accès NTFS, on va sur le dossier Partage > DEPT INFO > clic droit > Propriétés > Sécurité.

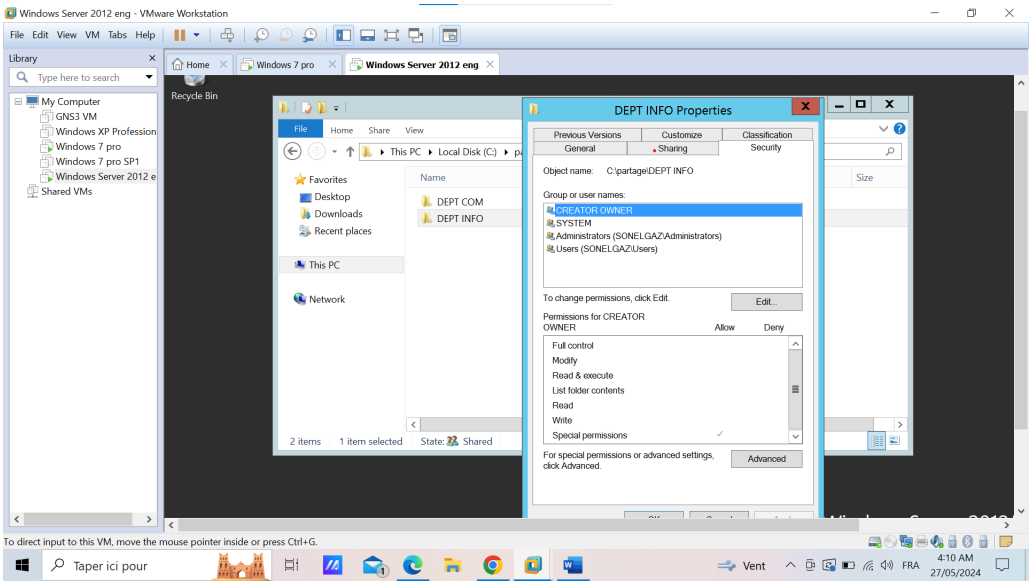


Figure 4.32 – Propriété DEPT INFO

On va supprimer "Utilisateurs" car nous voulons que le dossier "DEPT INFO" soit accessible uniquement au groupe "groupeinfo". Avant cela, il faut prendre en compte le lien d'héritage du dossier parent.

Pour ce faire, on clique sur "Avancé", on désactive l'héritage, puis on supprime "Utilisateurs".

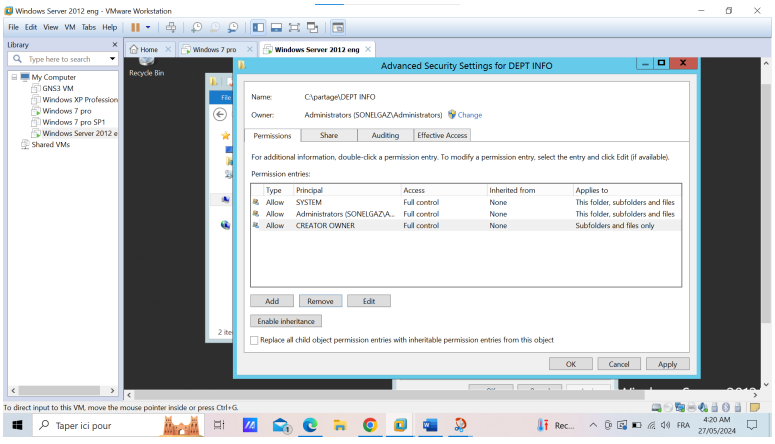


Figure 4.33 – Interface de désactivation de l'héritage et suppression des utilisateurs

On ajoute ensuite le groupeinfo en cliquant sur ajouter et puis choisir le groupe comme suit :

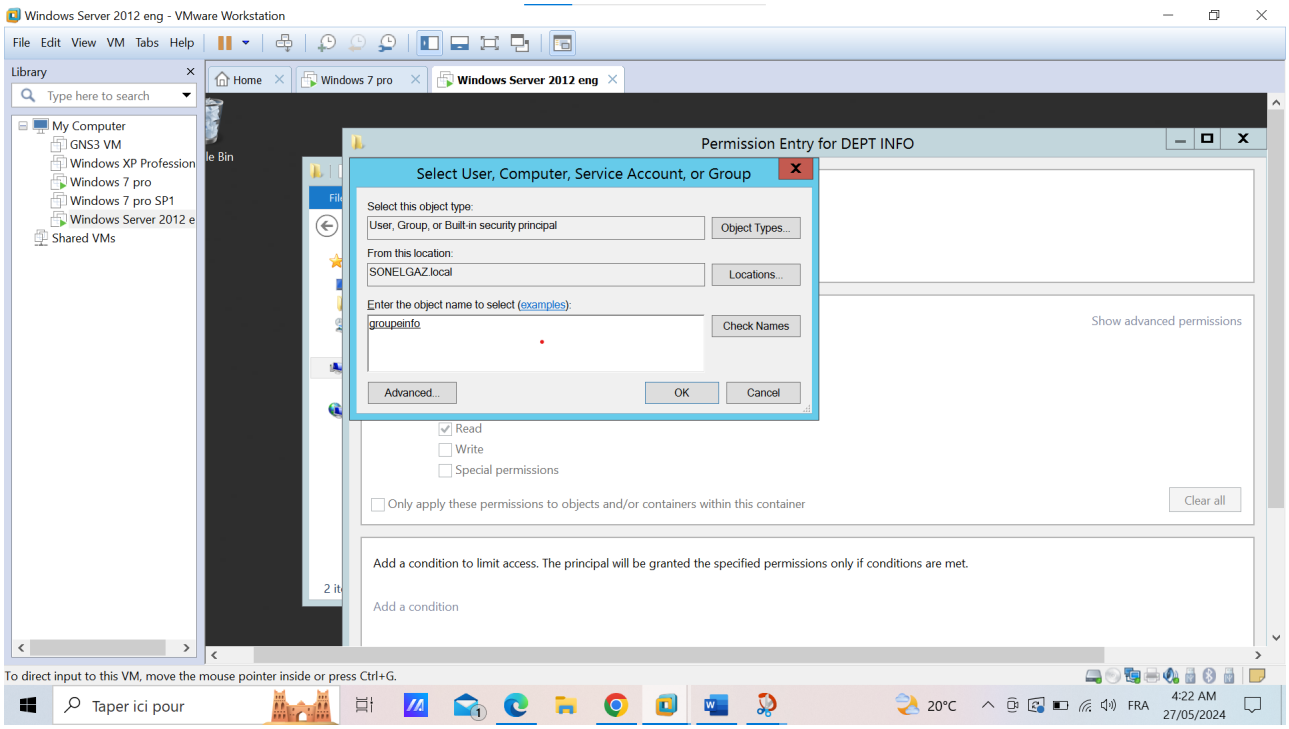


Figure 4.34 – Ajout du groupeinfo

Ensuite on passe à l'attribution des permissions comme ci-indiqué :

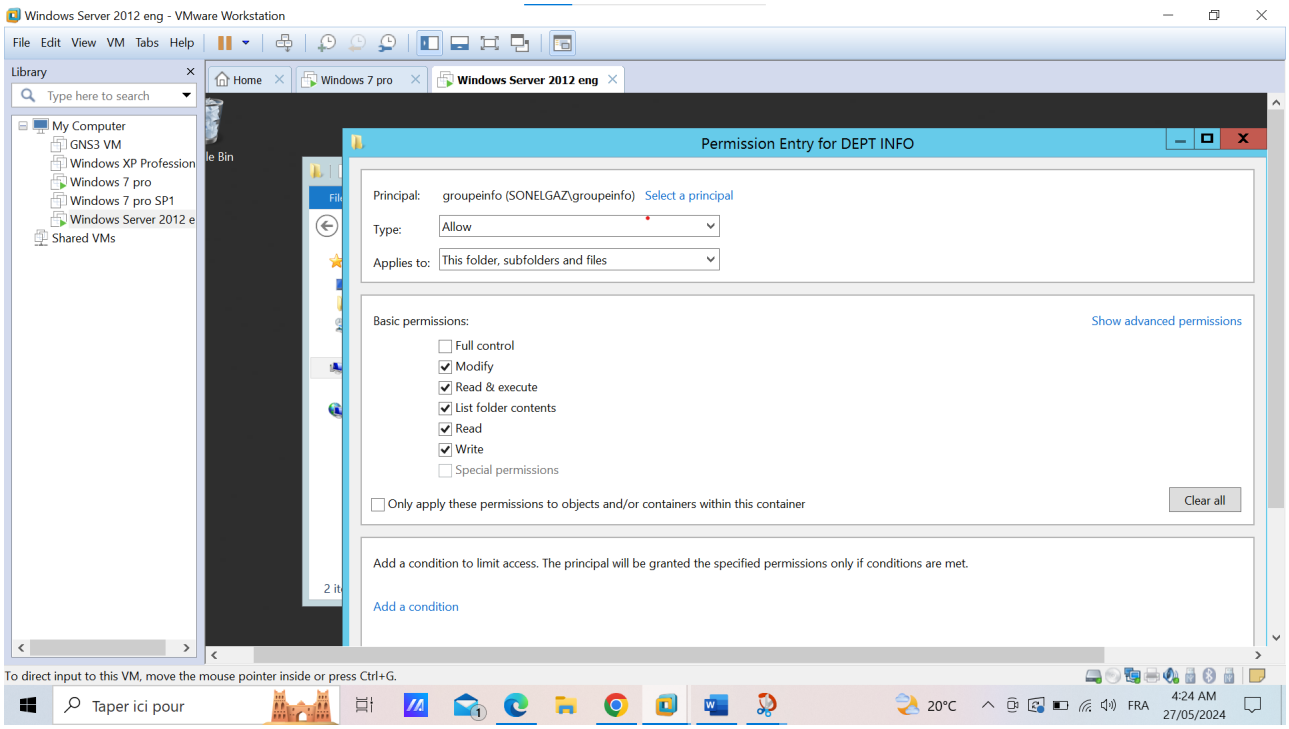


Figure 4.35 – Interface d'attribution des permissions du groupeinfo

On répéte le même processus pour le département "DEPTCOM";

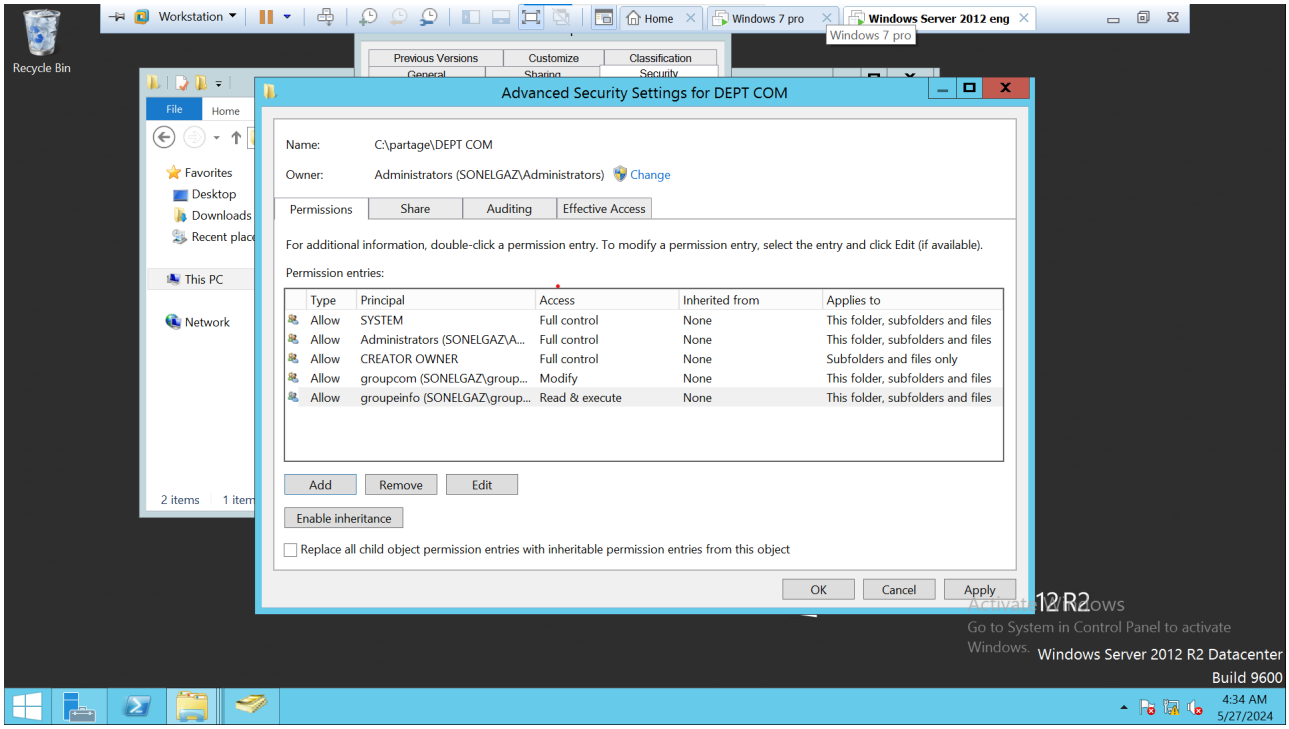


Figure 4.36 – Permission du groupcom

Nous avons choisi de limiter l'accès du groupe "groupeinfo" au dossier "DEPT COM" en lecture seule. Pour ce faire, nous avons répété le même processus, en veillant à ne pas cocher les cases "modifier" et "écriture".

Verification de la configuration ;

Se connecter a un compte du groupeinfo ;

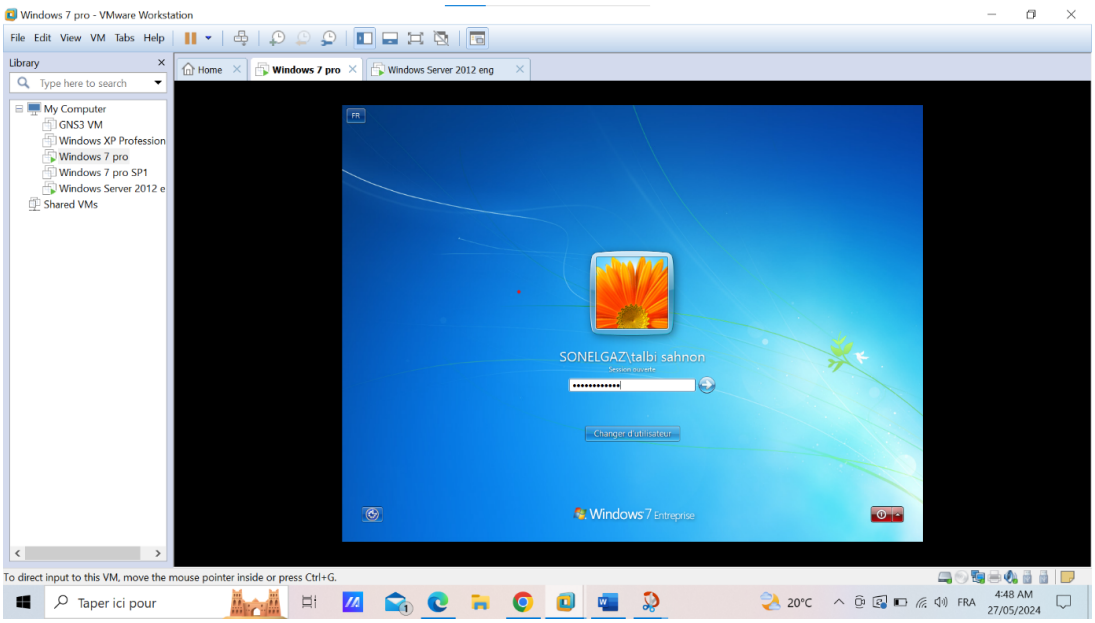


Figure 4.37 – Utilisateur du groupeinfo

On vois que le dossier est bien partagé et visible pour l'utilisateur Talbi Sahnon ;

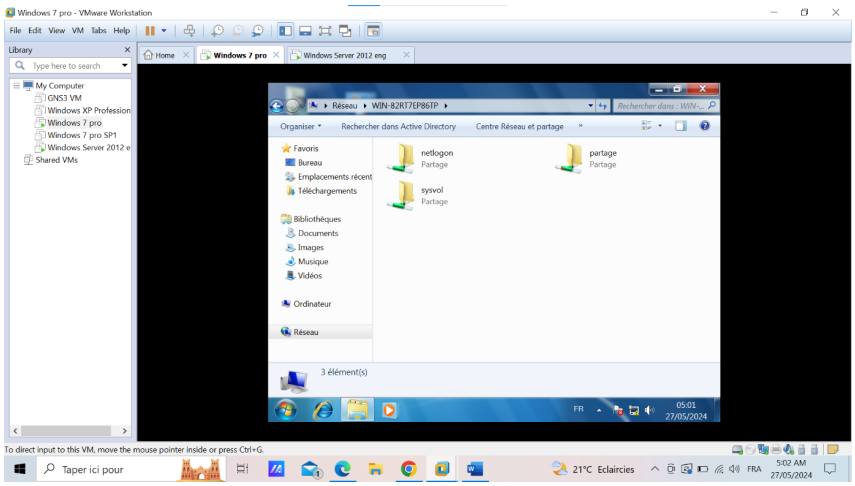


Figure 4.38 – Dossier partager

Ainsi les deux sous-dossier ;

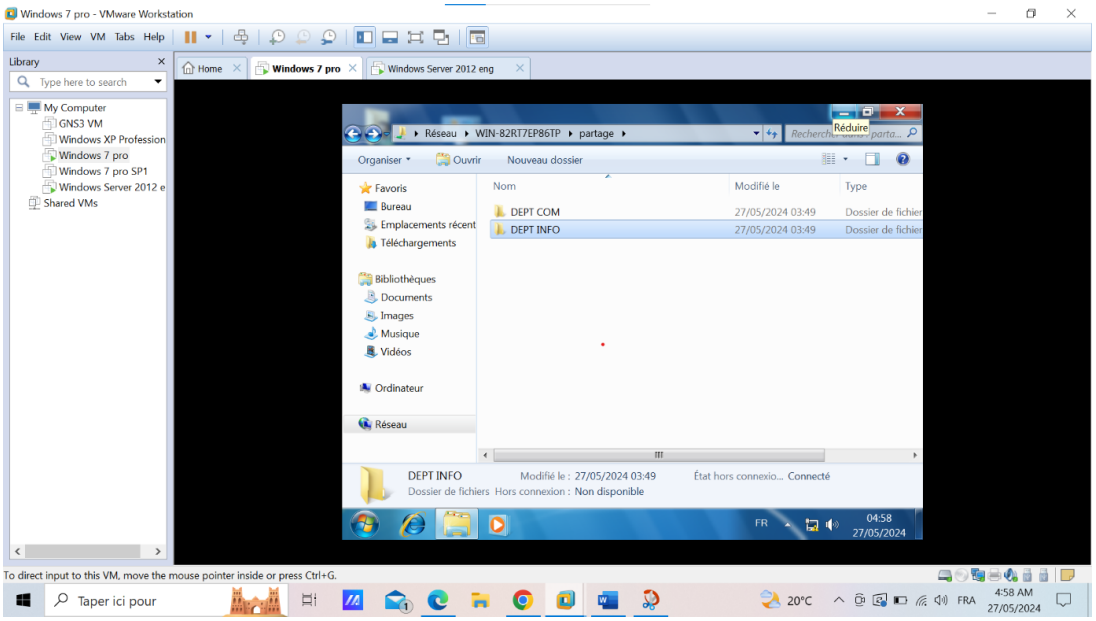


Figure 4.39 – Sous-dossier partager

Pour l'utilisateur talbi sahnon qui est du groupeinfo on voit bien que les droit d'écriture ,création et modifier sont valable ainsi pour la lecture du DEPT COM ;

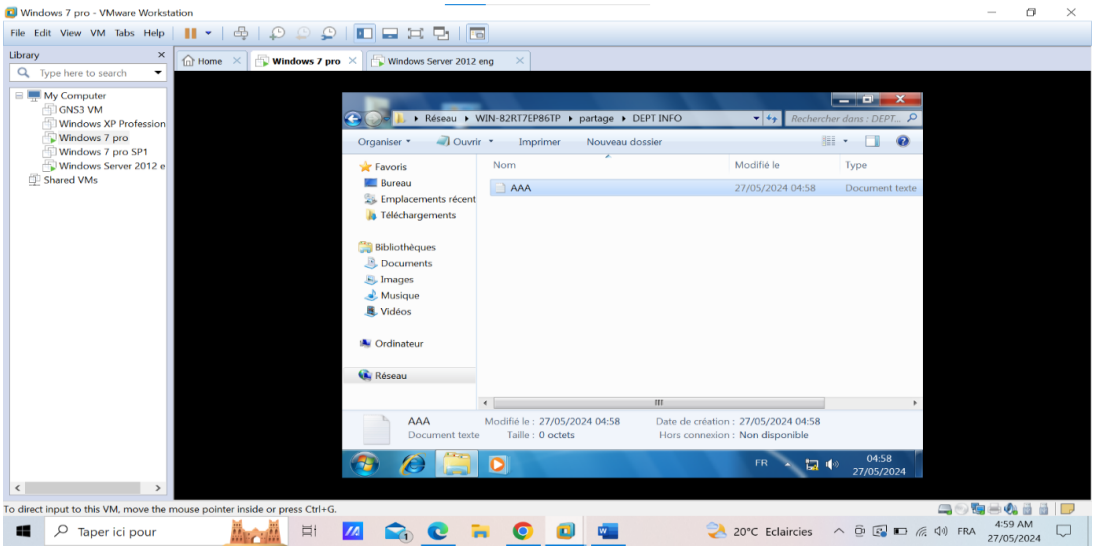


Figure 4.40 – validité des droits attribuer pour DEPT INFO

Par contre sur le dossier DEPT COM il a le droit que pour la lecture en essayent de créer un fichier un message d'erreur s'affiche comme suit :

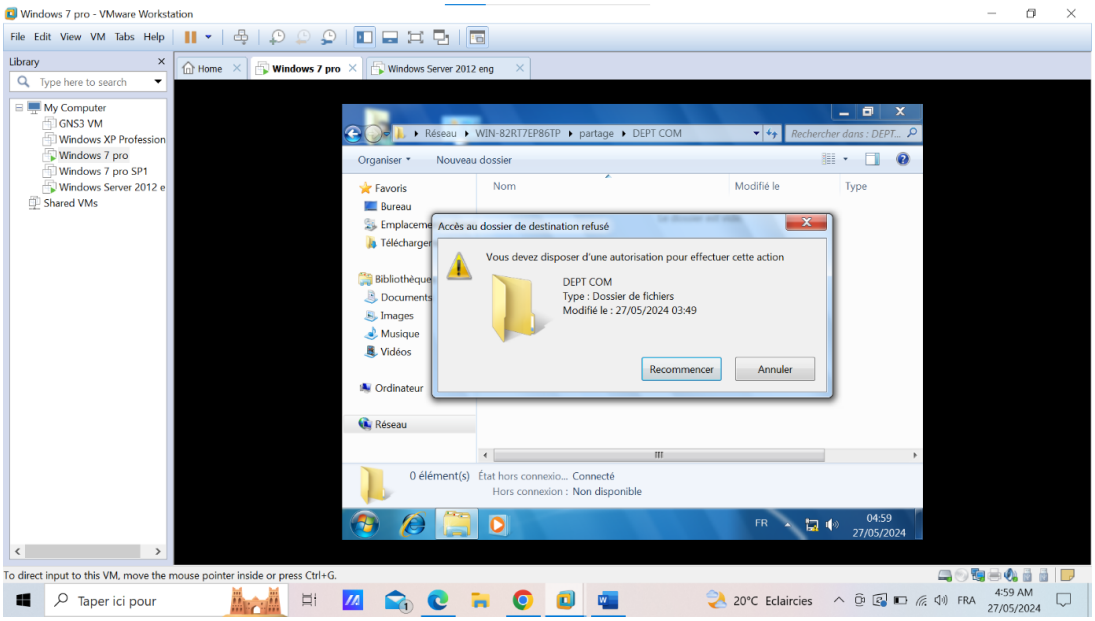


Figure 4.41 – validité des droits attribués pour DEPT COM

4.8 Préconfiguration de l'imprimante

On peut personnaliser davantage la configuration de l'imprimante afin qu'elle soit configurée de manière personnalisée au niveau des postes clients.

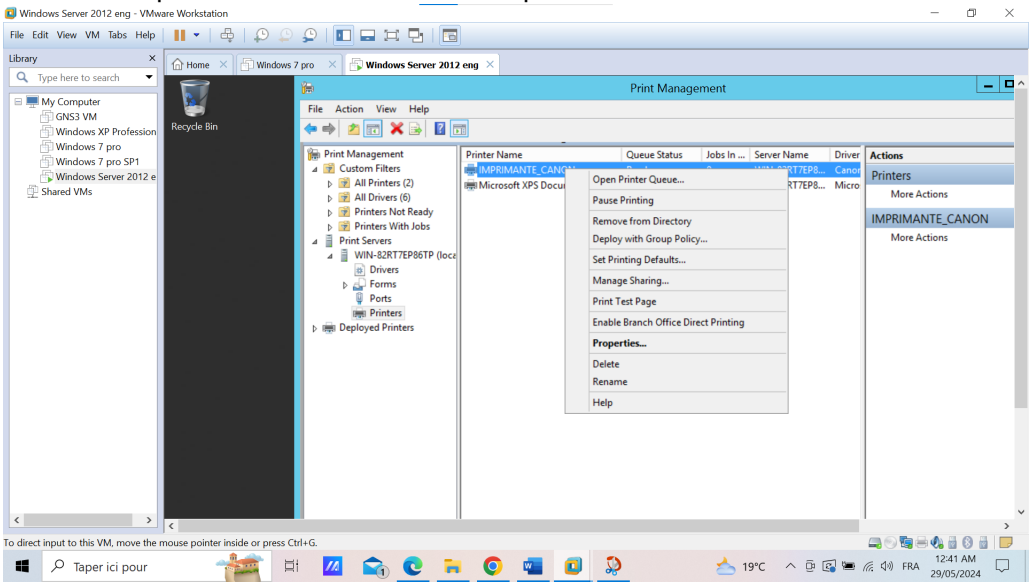


Figure 4.42 – Définir les valeur d'impression par default

Clique droit sur l'imprimante>Définir les valeur d'impression par default ;

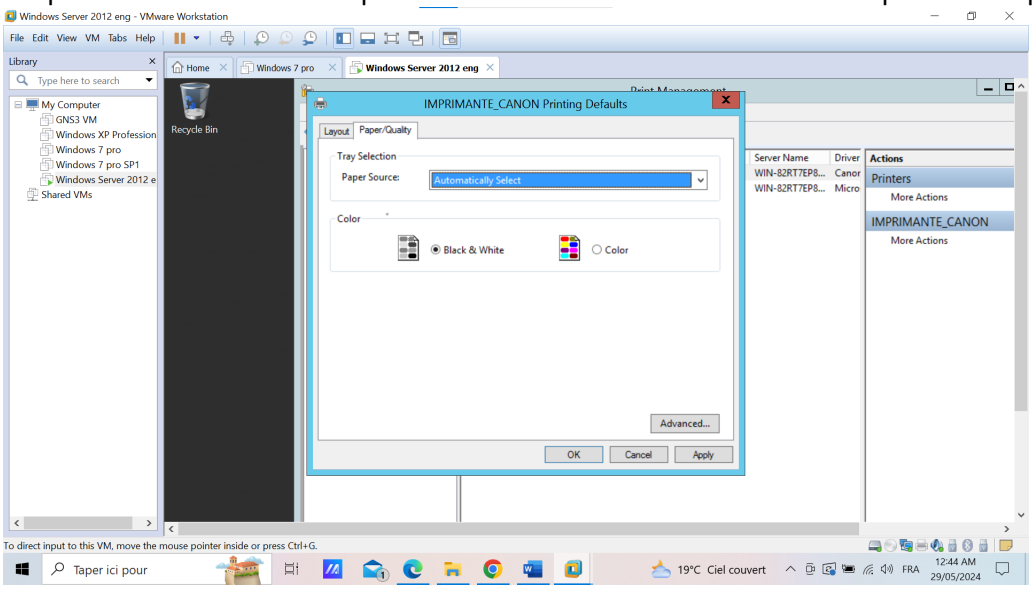


Figure 4.43 – Préconfiguration de l'imprimante

Dans notre cas, nous avons opté pour que l'impression sur cette imprimante soit uniquement en noir et blanc.

Note : En entreprise, les impressions couleur sont beaucoup plus coûteuses que les impressions en noir et blanc, d'où l'utilité de la préconfiguration de l'imprimante.

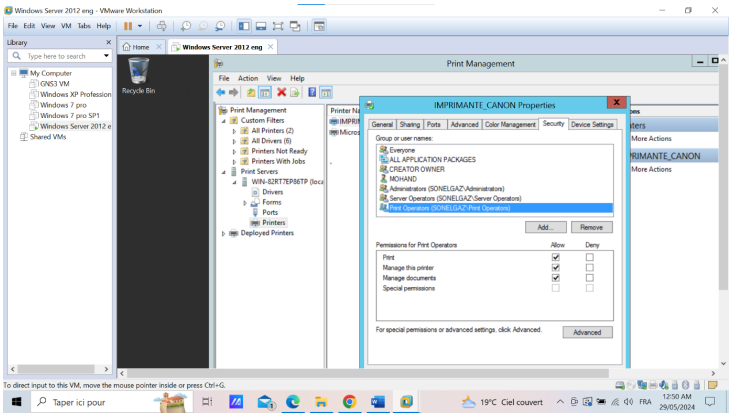


Figure 4.44 – Accessibilité et gestion de l'imprimante

On souhaite que l'imprimante soit accessible uniquement pour le groupinfo, pour se faire on suit les étapes suivantes :

On effectue un clic droit sur l'imprimante, puis propriété, puis sécurité

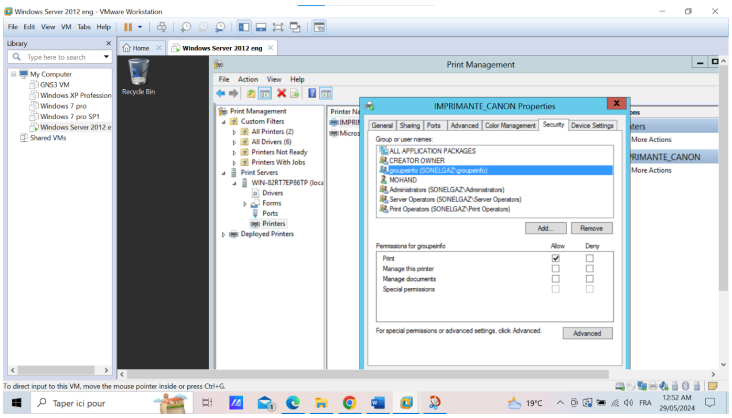


Figure 4.45 – Imprimante accessible uniquement au groupeinfo

On supprime " tout le monde " et on ajoute le groupinfo avec l'autorisation d'imprimer uniquement ;

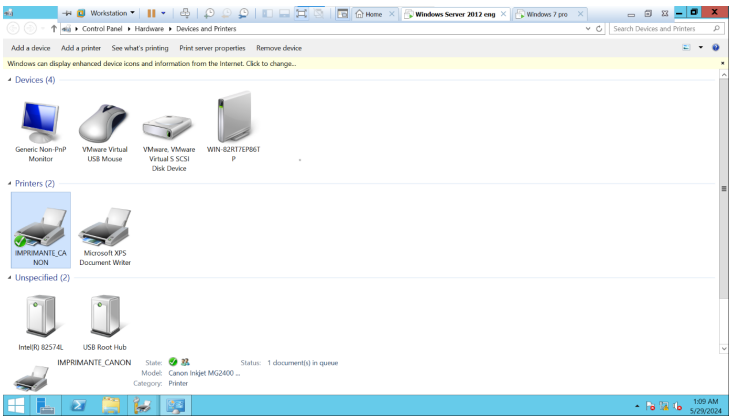


Figure 4.46 – Imprimante Partagée

L'imprimante est désormais disponible sur le serveur d'impression. Il suffira aux clients de saisir l'adresse ou le nom du serveur d'impression pour l'installer rapidement et efficacement.

Installer manuellement l'imprimante partagée

On accède avec l'utilisateur talbi sahnon qui fait partie du groupe ayant accès a l'imprimante, Sur le menue on tape imprimante et périphériques puis ajouter une imprimante ;

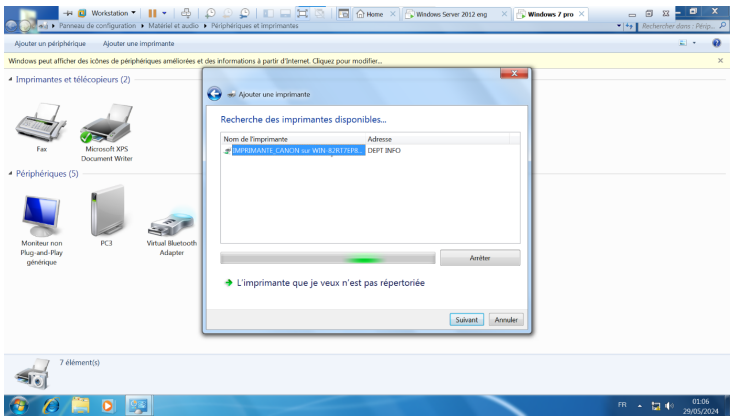


Figure 4.47 – Installation de l'imprimante sur un post-client

On clique sur suivant pour ajouter l'imprimante ;

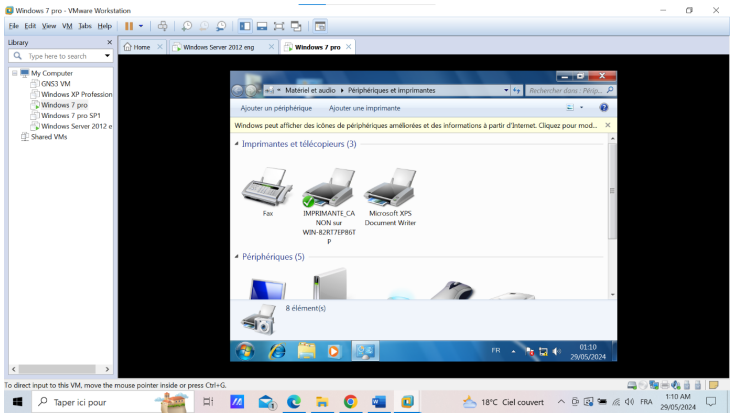


Figure 4.48 – Interface d'ajout d'une imprimante

Notre imprimante est bien ajoutée ;

- NB : L'imprimante ne peut s'ajoute sur un utilisateur hors du groupe "groupeinfo" sans l'intervention de l'administrateur du domaine.

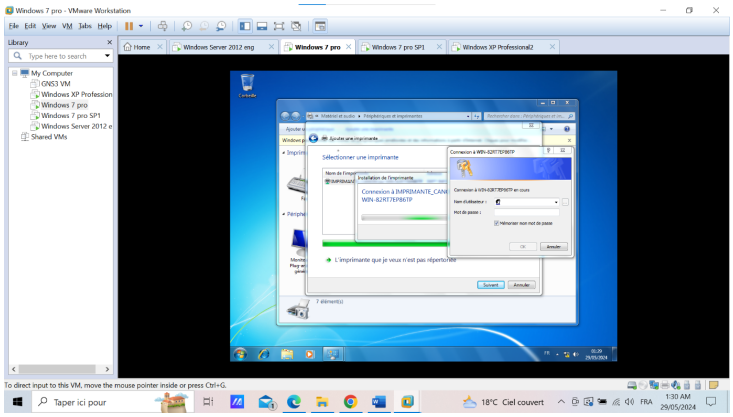


Figure 4.49 – Accès non autorisé pour le groupcom

4.9 Serveur DNS

On distingue deux zones de recherche qui sont :

— Zone de recherche directe : se base sur la résolution nom vers adresse IP

— Zone de recherche inversée : se base sur la résolution d'adresse IP vers nom.

Le DNS est configuré d'une manière locale, mais le serveur joue aussi le rôle d'un serveur redirecteur afin de permettre l'accès à l'internet, ce serveur traduit toutes adresses DNS interne en une adresse DNS externe et vis-versa.

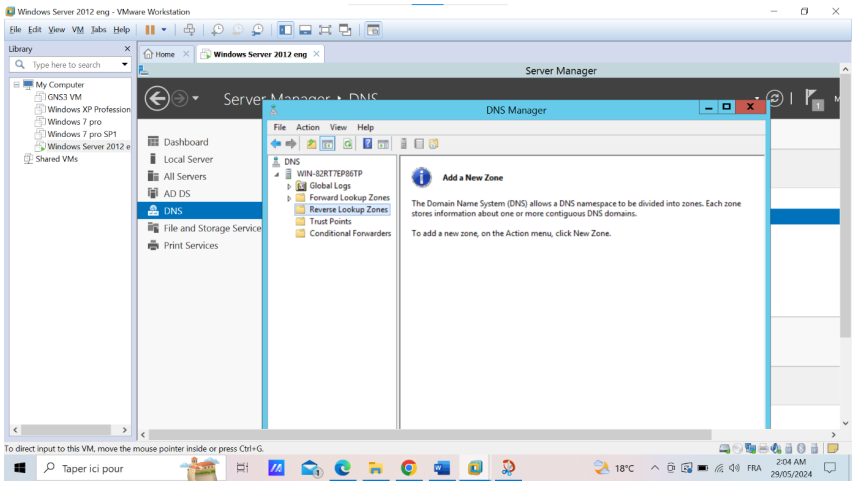


Figure 4.50 – Les zones de recherche DNS

Pour la configuration de la Zone de recherche inversée on procède comme suit :
On clique sur ajouter une nouvelle Zone ;

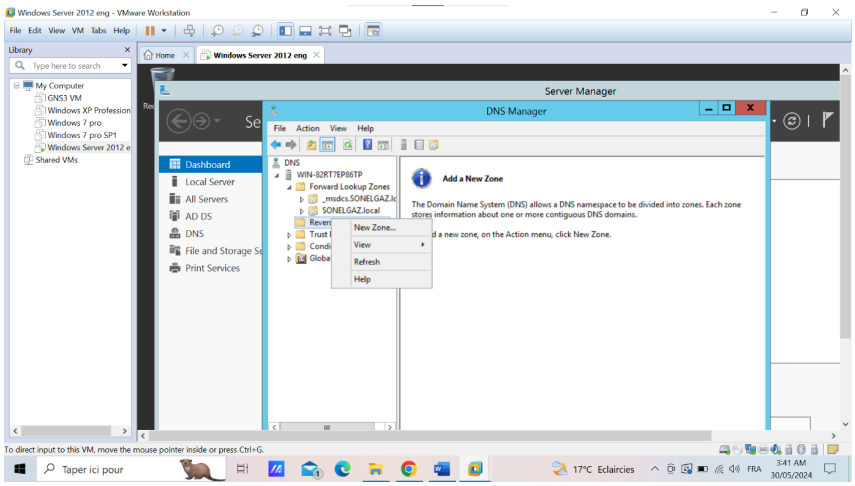


Figure 4.51 – Ajout de la zones de recherche inversée

Puis on spécifie l'adresse de notre réseau qui est 192.168.10.X

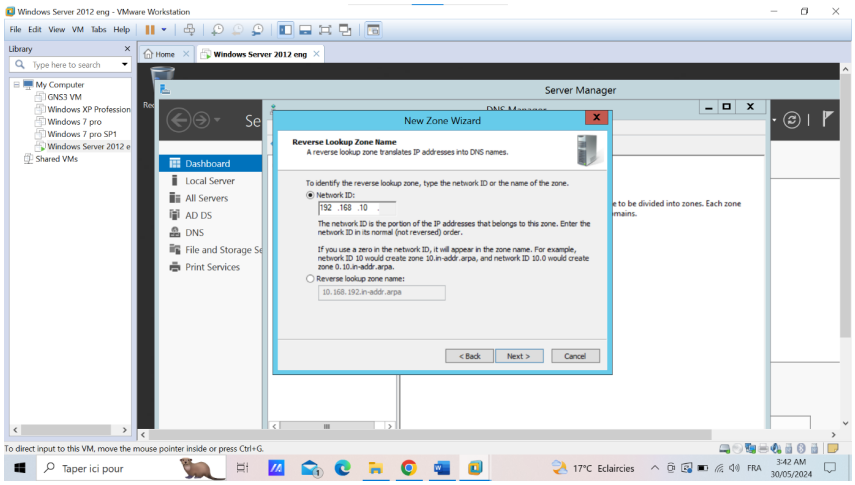


Figure 4.52 – Specification de l'adresse réseau

Ensuite, on ajoute un pointeur pour finaliser la zone de recherche inversée ;

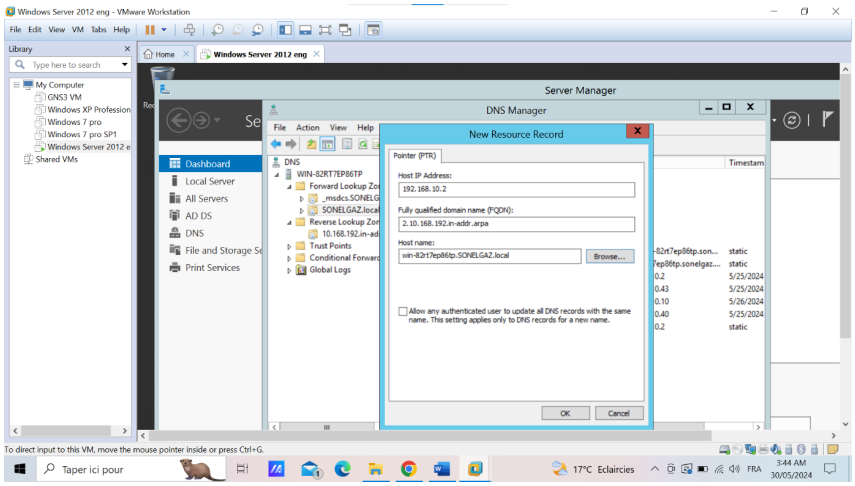


Figure 4.53 – Ajout d'un pointeur

En tapant la commande " nslookup 192.168.10.2 ", on voit que l'adresse ip et le nom du serveur s'affiche d'où l'utilité de la zone de recherche inversé ;

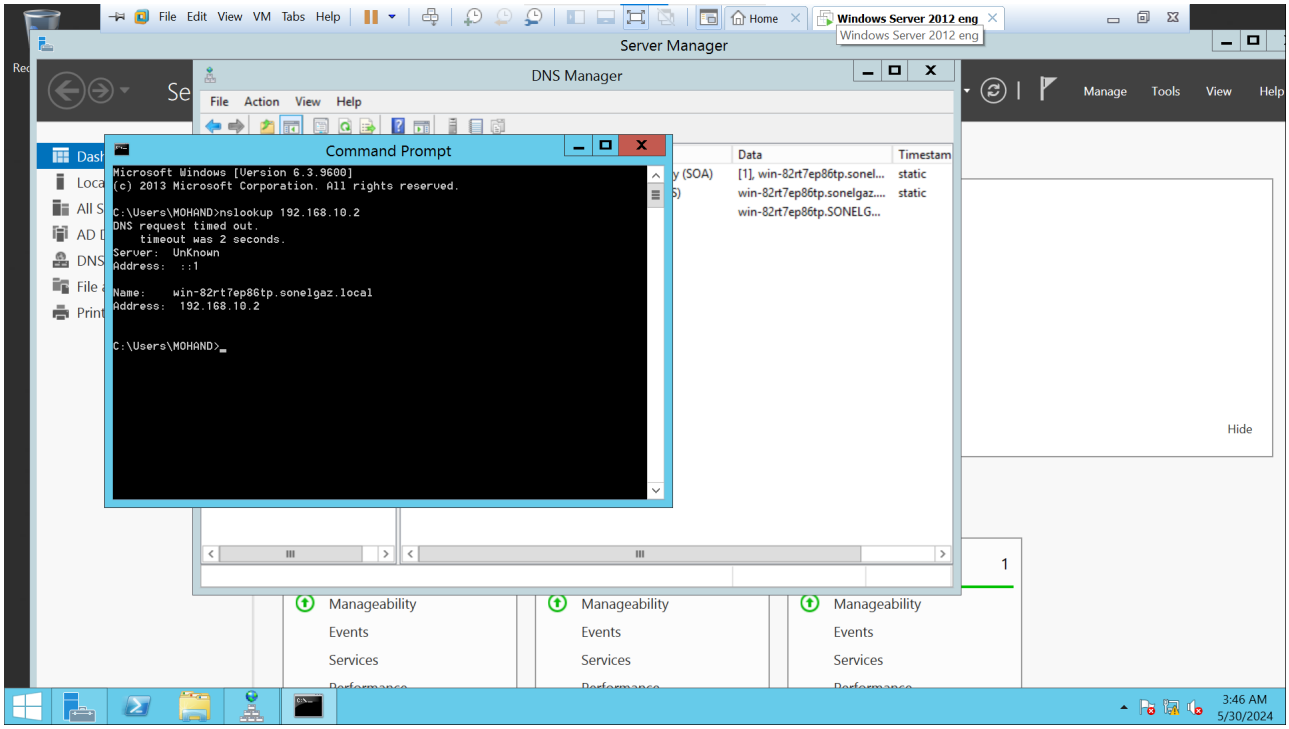


Figure 4.54 – Vérification

4.10 Serveur DHCP

Le DHCP (Dynamic Host Configuration Protocol) : Un serveur DHCP délivre des adresses IP de façon automatique aux ordinateurs se connectant au réseau. En plus d'une adresse IP le serveur DHCP vous informe de la configuration réseau tel que la passerelle par défaut et le masque de sous-réseau.

L'administrateur crée d'abord une étendue pour chaque sous-réseau physique, puis utilise l'étendue pour définir les paramètres utilisés par les clients. Une étendue possède les propriétés suivantes :

- Une plage d'adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP ;

- Un masque de sous-réseau, qui détermine le sous-réseau correspondant à une adresse IP donnée ;

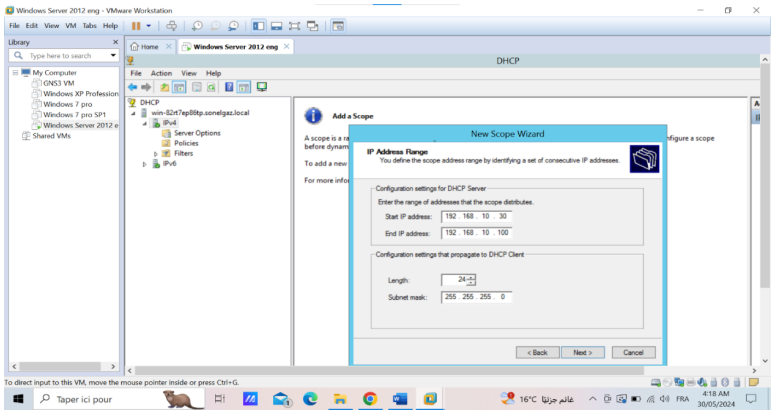


Figure 4.55 – Plage d'adresse

- Un nom affecté à l'étendue lors de sa création ;

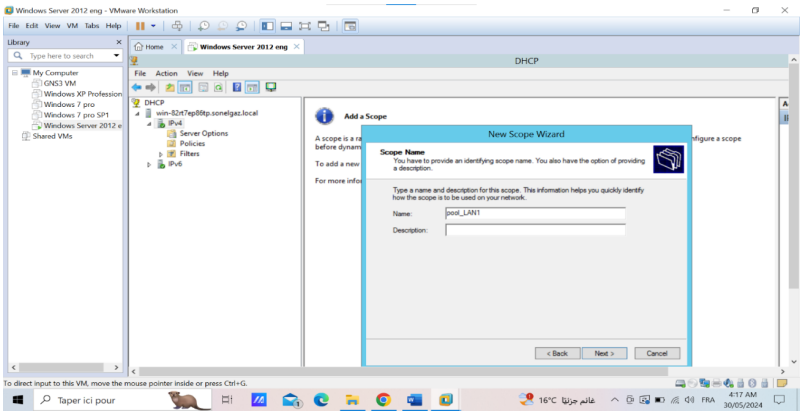


Figure 4.56 – Nom de l'etendue

- Des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP de manière dynamique ;

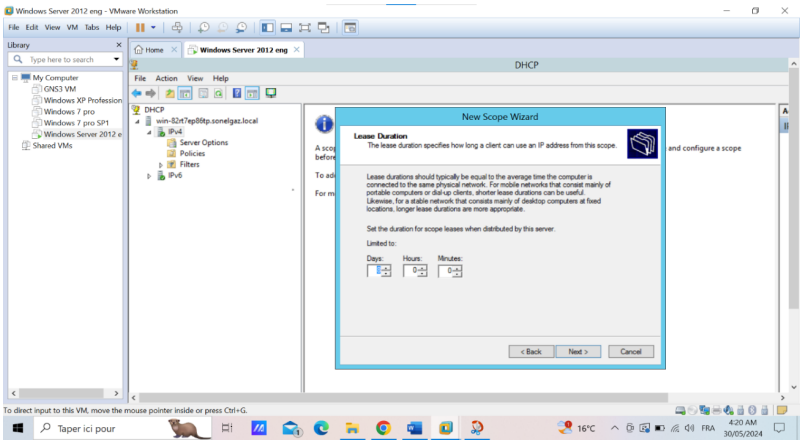


Figure 4.57 – Durée de bail

- Des options d'étendue DHCP configurées pour être affectées aux clients DHCP, telles qu'un serveur DNS, l'adresse IP d'un routeur ;

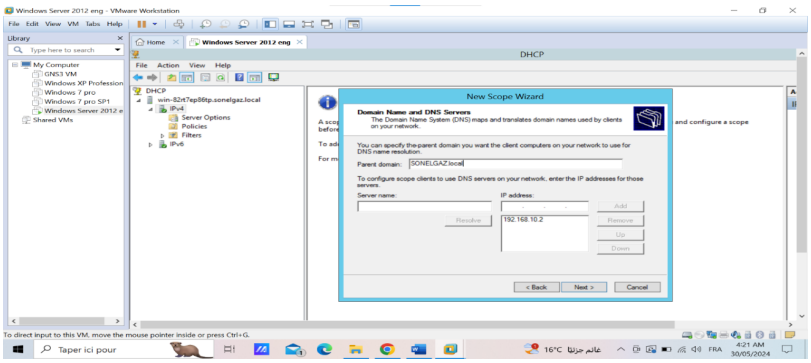


Figure 4.58 – Option de l'etendue DHCP

- Des réservations, utilisées de manière optionnelle pour s'assurer qu'un client DHCP reçoit toujours la même adresse IP, comme le montre la figure suivante :

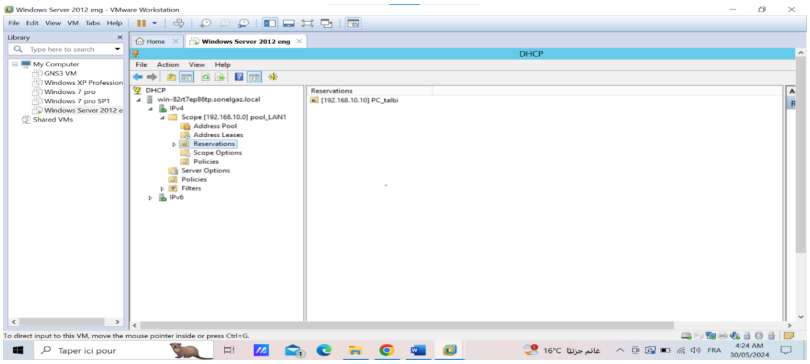


Figure 4.59 – Réservation d'adresse

Pour effectuer une réservation d'adresse on procède comme suite ;
Menu Réservation-> sélectionner nouvelle réservation, puis il ya une boite de dialogue qui s'affiche, on doit introduire les informations nécessaires telle que l'adresse IP et l'adresse physique (mac) de la machine comme le montre la figure suivante :

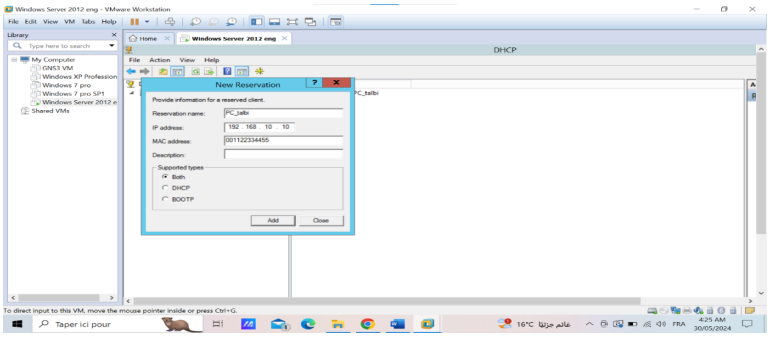


Figure 4.60 – Réservation d'adresse pour un post-client

N.B :le format de l'adresse MAC est (sans séparateurs) 001122334455 .

Conclusion

Ce chapitre a détaillé les étapes essentielles pour la gestion des infrastructures informatiques via Active Directory.
Nous avons exploré la création et la gestion des unités organisationnelles, des utilisateurs, et des groupes, ainsi que l'attribution des droits d'accès pour assurer une administration sécurisée et efficace des ressources informatiques.Nous avons également couvert la configuration des partages de fichiers et des imprimantes, et la mise en place des serveurs DNS et DHCP, éléments clés pour assurer la connectivité et la gestion réseau au sein de l'entreprise.

Conclusion génerale

Dans ce monde actuel où tout devient automatisé, l'administration, la connaissance du fonctionnement, la création et la configuration des réseaux informatiques paraissent indispensables pour un administrateur réseau.

Notre travail avait pour principal objectif la mise en œuvre d'un réseau local d'entreprise ainsi que le partage de ressources via Active Directory. Ce projet nous a permis de mettre en pratique les connaissances acquises durant notre stage pratique chez Sonelgaz Bouira, de nous familiariser avec un environnement dynamique et de mieux comprendre l'importance du réseau dans une entreprise.

Le stage pratique que nous avons effectué au sein de l'entreprise Sonelgaz Bouira nous a permis d'acquérir de nombreuses connaissances sur l'administration réseau, notamment sur Active Directory et ses différents composants tels que DHCP, DNS et Windows Server 2012. Nous avons également pu réaliser un réseau local d'entreprise efficace et extensible.

Ce projet visait à assurer le fonctionnement optimal des ressources réseau de l'entreprise et à offrir à ses membres un accès rapide à l'information ainsi qu'un partage facile des données. Grâce à l'utilisation de l'annuaire Active Directory lors de ce stage, nous avons découvert ses nombreux avantages : il offre aux utilisateurs finaux un environnement de travail très fiable, permet aux administrateurs de bénéficier d'une sécurité et d'une facilité de gestion accrues, et aide les utilisateurs à effectuer leurs tâches de manière optimale.

La réalisation de ce projet a été bénéfique pour nous car elle nous a permis d'approfondir et d'acquérir de nouvelles connaissances qui nous seront utiles à l'avenir.

Bibliographie

Documents

[D] Document de l'entreprise

Webographie

[1] https ://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/

[2] https ://sti2d.ecolelamache.org/ii-rseaux-informatiques-7-topologie-des-rseaux.html

[3] https ://www.freelance-informatique.fr/actualites/reseau-informatique-equipements

[4] https ://www.weodeo.com/blog-materiel/quels-sont-les-types-de-serveurs

[5]https ://www.furet.com/media/pdf/feuilletage/9/7/8/2/7/4/4/0/9782744076640.pdf

[6] https ://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7236472-prenez-du-recul-sur-votre-pratique-grace-au-modele-osi

[7] https ://www.frameip.com/tcpip/

[8] https ://datascientest.com/protocoles-reseau-tout-savoir

[9] http ://hautrive.free.fr/reseaux/architectures/organisation-des-reseaux.html

[10] https ://www.formip.com/pages/blog/adressage-ip

[11] https ://aidesecurite.blogspot.com/2013/03/types-dattaques-dun-reseau.html

[12]https ://cisco.ofppt.info/ccna1/course/module11/11.2.2.3/11.2.2.3.html

[13] https ://www.ibm.com/fr-fr/topics/social-engineering

[14] https ://www.cloudflare.com/fr-fr/learning/ddos/glossary/denial-of-service/

[15] https ://www.fortinet.com/fr/resources/cyberglossary/intrusion-detection-system

[16] https ://www.vaadata.com/blog/fr/comment-securiser-les-systemes-dauthentification-de-gestion-de-sessions-et-de-controle-dacces-de-vos-applications-web/

[17] https ://www.kaspersky.fr/resource-center/definitions/what-is-a-vpn

[18] https ://www.forcepoint.com/fr/cyber-edu/firewall

[19] https ://fr.norton.com/blog/malware/what-is-antivirus-and-do-i-need-it

[20] https ://www.piloter.org/techno/support/annuaire-ldap.htm

[21] https ://www.semperis.com/fr/blog/active-directory-security/what-is-active-directory-security/

[22] https ://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2012-r2

Mémoires

[M1] Administration d'un réseau local sous Windows serveur-Président du jury Mr. GRESSIER CNAM Paris – Département informatique

Livres

[L1] Patrice KADIONIK, Maître de Conférence à l'ENSEIRB "L'ADMINISTRATION DE RESEAU"

[L2] Raphael Yende. COURS D'ADMINISTRATION DES RÉSEAUX INFORMATIQUES. Licence.BENI (RDC), Congo-Kinshasa. 2019, pp.108. ffcel-01995184f

Résumé

Ce projet vise à résoudre les problèmes de partage des ressources informatiques au sein d'une entreprise. Plus précisément, il propose une solution permettant de centraliser les équipements et les ressources utilisées par les utilisateurs grâce au déploiement d'un annuaire nommé Active Directory.Le déploiement d'un service d'annuaire comme Active Directory présente de nombreux avantages. Il permet de créer un environnement de travail extrêmement fiable pour les utilisateurs finaux. De plus, il offre aux administrateurs une sécurité accrue et une gestion simplifiée des ressources. Cela permet aux utilisateurs d'accomplir leurs tâches de manière plus efficace.

Mots clés : gestion des utilisateurs,partage de fichiers, domaine, LDAP, Active Directory.

This project aims to address the issues of sharing IT resources within a company. Specifically, it proposes a solution to centralize the equipment and resources used by users through the deployment of a directory service called Active Directory. The deployment of a directory service like Active Directory offers numerous advantages. It creates a highly reliable working environment for end users. Additionally, it provides administrators with enhanced security and simplified resource management. This allows users to perform their tasks more efficiently.

Keywords : file sharing, user management, domain, LDAP, Active Directory.