Université de Nouakchott
Faculté des sciences et techniques

Département Mathématiques et Informatique

PROJET DE FIN D'ETUDES

Pour l'obtention du

DIPLÔME DE LICENCE EN MIAGE

Thème :

ACTIVE DIRECTORY

Réalisé par :
Khaye sidi Coulibaly C20904

Encadré par :
Dr El Veth Sidi

Membres du jury

Président du jury	**Ahmed Mohamed**
Membre 1	**Amal Noula**
Membre 2	**Med Elmoudtapha El Arby**

Année universitaire 2024-2025

Remerciements

Avant toute chose, je tiens à vous exprimer ma profonde gratitude à toutes les personnes qui ont contribué de près ou de loin à la réussite de ce projet de fin d'études. Leur soutien, leur accompagnement et leurs encouragements m'ont permis de mener à bien ce projet dans les meilleures conditions.

Je remercie tout particulièrement Dr El VETH SIDI, mon encadrant universitaire, pour son suivi, ses conseils précieux et sa disponibilité tout au long de ce projet. Ses remarques pertinentes et son expérience ont grandement contribué à l'amélioration du contenu de ce rapport.

Mes remerciement vont également à Mr Ibrahim Diallo qui m'a accueilli au sein Direction de l'Administration Système et de la sécurité, pour son accompagnement et pour m'avoir permis de découvrir le fonctionnement d'un réseau administratif dans un réel.

Je n'oublie pas mes enseignants, camarades de promotion et de ma famille pour leur soutien constant tout au long de la formation.

Table des matières

INTODUCTION GENERALE

Dans un environnement professionnel où les systèmes d'information jouent un rôle stratégique dans la gestion et le bon fonctionnement des organisations, la centralisation et la sécurisation des ressources informatiques constituent aujourd'hui des priorités incontournables. La maîtrise des accès, la protection des données et l'automatisation des tâches administratives sont essentielles pour garantir la continuité des services et la performance des infrastructures réseau.

C'est dans ce contexte que s'inscrit ce projet de fin d'études, qui a permis de concevoir et de déployer une infrastructure réseau virtuelle sous Windows Server 2012, intégrant les services Active Directory, DNS, DHCP et GPO, à l'aide de VMware Workstation. L'objectif principal de ce travail était de simuler un environnement d'entreprise structuré et sécurisé, permettant de gérer efficacement les utilisateurs, les ressources réseau et les politiques de sécurité à partir d'un point central.

Au cours de ce projet, plusieurs étapes ont été réalisées avec succès :

L'installation et la configuration d'un serveur Windows Server 2012 dans un environnement virtualisé.

La mise en place du rôle Active Directory Domain Services et la promotion du serveur en contrôleur de domaine.

La structuration de l'annuaire Active Directory à travers la création de domaines, unités d'organisation (OU) et groupes.

La configuration des services DNS et DHCP pour assurer la résolution de noms et l'attribution dynamique des adresses IP.

La définition et l'application de stratégies de sécurité via des GPO pour uniformiser les configurations et sécuriser les postes clients.

La mise en place de partages de fichiers sécurisés et de scripts automatisés.

Enfin, la réalisation de tests de fonctionnement et de validation a permis de confirmer la cohérence, la fiabilité et la sécurité de l'infrastructure déployée.

Ce projet m'a permis d'acquérir des compétences techniques solides en administration système et en gestion d'environnement Active Directory sous Windows Server, ainsi qu'en virtualisation avec VMware. Il m'a également sensibilisé à l'importance de la sécurité et de la gestion centralisée dans les systèmes d'information modernes.

PRESENTATION DE L'ENTREPRISE

Le ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration (MTNIMA) a pour objectif principal de conduire la transition numérique en Mauritanie. Il œuvre à moderniser les services publics en promouvant l'innovation et l'e-administration, tout en renforçant les infrastructures numériques nationales. Pour cela, le MTNIMA s'appuie sur un agenda national (2022-2025) axé sur :

L'amélioration des infrastructures numériques : déploiement de réseaux de fibre optique et connectivité améliorée.

La modernisation de l'administration : mise en place d'intranets gouvernementaux et de solutions cloud pour faciliter les échanges de données.

La transformation sectorielle : intégration du numérique dans les domaines de la santé, de l'éducation, de l'agriculture, et de la pêche.

Le développement de l'économie numérique : soutien aux startups, déploiement de paiements et de solutions d'e-commerce.

Le ministère pilote également plusieurs projets clés, tels que WARDEEP pour améliorer la couverture haut-débit, un centre de données national pour sécuriser les informations, et le déploiement d'un système d'identité numérique mobile. Il est soutenu par des partenariats avec des entités nationales et internationales (notamment le Conseil supérieur

PROBLEMATIQUE ET OBJECTIFS DU STAGE

- **PROBLEMATIQUE**

Dans un environnement professionnel où l'informatique est au cœur des activités quotidiennes, la gestion manuelle et dispersée des utilisateurs, des ressources et des services réseau devient rapidement inefficace, source d'erreurs et difficilement maîtrisable. Cette méthode complique la gestion des accès aux ressources, fragilise la sécurité du système d'information et alourdit la charge de travail des administrateurs réseau.

Face à ces contraintes, une question se pose :

Comment concevoir et mettre en place une infrastructure réseau centralisée et sécurisée, capable de gérer efficacement les comptes utilisateurs, les ressources partagées et les stratégies de sécurité, tout en offrant une administration simplifiée et cohérente de l'environnement réseau ?

- **L'OBJECTIF**

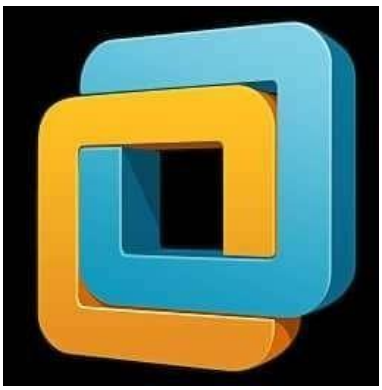
L’objectif principal de ce stage est de concevoir et de déployer une infrastructure réseau virtuelle sous Windows Server 2012, permettant de centraliser et de sécuriser la gestion des utilisateurs, des ressources et des services réseau d’une entreprise, tout en assurant une administration simplifiée et efficace grâce à l’utilisation d’Active Directory et de ses services associés.

Pour atteindre cet objectif général, plusieurs objectifs spécifiques ont été définis :

- Installer et configurer Windows Server 2012 dans un environnement virtualisé avec VMware Workstation.
- Mettre en place le rôle Active Directory Domain Services (AD DS) et promouvoir le serveur en contrôleur de domaine.
- Organiser l’annuaire Active Directory à travers la création de domaines, unités d’organisation (OU) et groupes d’utilisateurs.
- Configurer les services DNS et DHCP, indispensables au bon fonctionnement de l’infrastructure réseau.
- Définir et appliquer des stratégies de sécurité via des GPO pour gérer les paramètres des utilisateurs et des ordinateurs du domaine.
- Créer des dossiers partagés sécurisés avec des droits d’accès personnalisés selon les besoins des utilisateurs.
- Réaliser des tests de bon fonctionnement et de sécurité pour valider la stabilité et l’efficacité de l’infrastructure déployée

Chapitre 1 : Étude théorique et technologique

1-1 Qu’est-ce que VMware



VMware est une entreprise américaine fondée en 1998, spécialisée dans les solutions de virtualisation et de cloud computing. Elle propose des logiciels qui permettent d'exécuter plusieurs systèmes d'exploitation sur un seul ordinateur physique, en créant des machines virtuelles (VM).

✞ Principaux produits de VMware

VMware Workstation

Destiné aux postes de travail (Windows et Linux).

Permet de créer et gérer des machines virtuelles localement.

Utilisé par les développeurs et les étudiants pour tester des systèmes.

VMware vSphere

Suite pour les environnements serveur.

Inclut ESXi (hyperviseur de type 1) et vCenter (gestion centralisée).

Utilisé dans les data centers pour consolider les serveurs.

VMware Fusion

Version pour MacOs.

Permet d'exécuter des systèmes Windows ou Linux sur un Mac.

VMware vs AN (Virtual SAN)

Solution de stockage définie par logiciel.

Intègre les disques des serveurs pour créer un pool de stockage partagé.

VMware Horizon

Solution de virtualisation de postes de travail (VDI).

Permet aux utilisateurs d'accéder à leur bureau depuis n'importe où.

VMware utilise un hyperviseur, qui est un logiciel permettant de créer et gérer plusieurs machines virtuelles sur un seul hôte physique.

Types d'hyperviseurs :

Type 1 (bare metal) : installé directement sur le matériel (ex. : VMware ESXi).

Type 2 (hosted) : installé sur un système d'exploitation (ex. : VMware Workstation).

Chaque machine virtuelle possède :

Son propre système d'exploitation.

Son propre espace mémoire.

Son propre disque virtuel.

✞ Avantages de la virtualisation avec VMware

Réduction des coûts matériels.

Meilleure utilisation des ressources.

Sauvegarde et restauration simplifiées.

Facilité de test et de développement.

Isolation entre les systèmes.

Haute disponibilité et tolérance aux pannes (avec vSphere).

- **Cas d’usage de VMware**

Entreprises : centralisation des serveurs, haute disponibilité.

Laboratoires : test de logiciels et systèmes.

Enseignement : formation aux systèmes d'exploitation et aux réseaux.

Cloud hybride : intégration avec AWS, Azure, etc.

- **Alternatives à VMware**

VirtualBox (gratuit)

Hyper-V (Microsoft)

Proxmox

KVM (Linux)

1-2 Présentation de Windows Server 2012

Windows Server 2012 est un système d’exploitation serveur développé par Microsoft et destiné à gérer les réseaux d’entreprise. Il succède à Windows Server 2008 et propose de nombreuses améliorations en matière de virtualisation, de gestion des ressources, de sécurité et de services réseau.

Parmi ses principales fonctionnalités, on retrouve :

La gestion centralisée des utilisateurs et des ressources via Active Directory.

La virtualisation des serveurs avec Hyper-V.

La gestion simplifiée des services réseau tels que DNS, DHCP et les services de fichiers.

L’application de stratégies de sécurité et de configuration automatisées via les stratégies de groupe (GPO).

Windows Server 2012 permet ainsi de bâtir une infrastructure réseau sécurisée, fiable et évolutive, adaptée aux besoins des entreprises de toutes tailles.

Windows serveur 2012 est disponible en quatre Edition :

Edition	Description
Datacenter	Pour les environnements virtualisés massifs (nombre illimité de machines virtuelles)
Standard	Pour les environnements physiques ou légèrement virtualisés (2 machines virtuelles maximum)
Essentials	Pour les petites entreprises (maximum 25 utilisateurs, 50 appareils)
Fondation	Édition de base (limité à 15 utilisateurs, pas de virtualisation).

✞ Nouveautés clés par rapport à Windows Server 2008 R2

Interface Modern UI (Metro) : nouvelle interface utilisateur similaire à Windows 8.

Gestion centralisée avec Server Manager : gestion multiserveur améliorée.

PowerShell 3.0 : pour l'automatisation avancée des tâches d'administration.

Hyper-V 3.0 : amélioration de la virtualisation (réplication, meilleure gestion de la mémoire, etc.)

ReFS (Résilient File System) : un nouveau système de fichiers plus fiable que NTFS.

Storage Spaces : permet de créer des volumes de stockage virtuels.

IP Adresse Management (IPAM) : gestion centralisée des adresses IP.

Dynamic Access Control : pour un contrôle d'accès basé sur les métadonnées.

Direct Access amélioré : accès distant plus simple et plus sécurisé.

✞ Rôles et fonctionnalités

Les rôles permettent d'attribuer des fonctions spécifiques à un serveur.

Rôles principaux de Windows Server 2012 :

Active Directory Domain Services (AD DS) : gestion des utilisateurs, ordinateurs et politiques de sécurité.

DHCP (Dynamic Host Configuration Protocol) : attribution automatique des adresses IP.

DNS (Domain Name System) : résolution de noms en adresses IP.

Hyper-V : création et gestion de machines virtuelles.

File and Storage Services : gestion du stockage et des partages réseau.

Web Server (IIS) : hébergement de sites web et applications.

Remote Desktop Services (RDS) : accès à distance aux bureaux et applications.

Print and Document Services : gestion des imprimantes.

Windows Deployment Services (WDS) : déploiement automatisé de systèmes d'exploitation.

✞ Sécurité

BitLocker : chiffrement de disques.

Windows Defender : protection contre les malwares.

AppLocker : restrictions sur les applications.

Pare-feu Windows avec fonctions avancées.

Contrôle d'accès dynamique (DAC) : gestion des droits basée sur l'identité et le contenu.

✞ Outils d'administration

Server Manager : tableau de bord pour la gestion de plusieurs serveurs.

PowerShell : Scripting avancé pour automatiser les tâches.

Group Policy Management : gestion des stratégies de groupe.

Event Viewer : suivi des journaux système.

Task Scheduler : planification des tâches.

✞ Avantages pour les entreprises

Haute performance et fiabilité.

Optimisation pour les environnements virtualisés.

Administration centralisée facilitée.

Sécurité renforcée.

Réduction des coûts avec la virtualisation**.**

1-3 Notions importantes

Pour mener à bien ce projet, il est essentiel de comprendre les concepts fondamentaux liés aux services proposés par Windows Server 2012. Voici les principaux services étudiés et mis en œuvre.

1-3-1 Active Directory

Active Directory Domain Services (AD DS) est un service d'annuaire intégré à Windows Server qui permet de centraliser la gestion des utilisateurs, des groupes, des ordinateurs et des ressources réseau. Il fournit une structure hiérarchique organisée en domaines, forêts et unités d'organisation (OU).

Grâce à Active Directory, l'administrateur peut :

Authentifier et gérer les comptes utilisateurs et ordinateurs.

Structurer l'entreprise selon des OU logiques et fonctionnelles.

Définir et appliquer des stratégies de sécurité via les GPO.

Gérer les ressources partagées et leurs permissions.

Fonctionnalités principales d'Active Directory

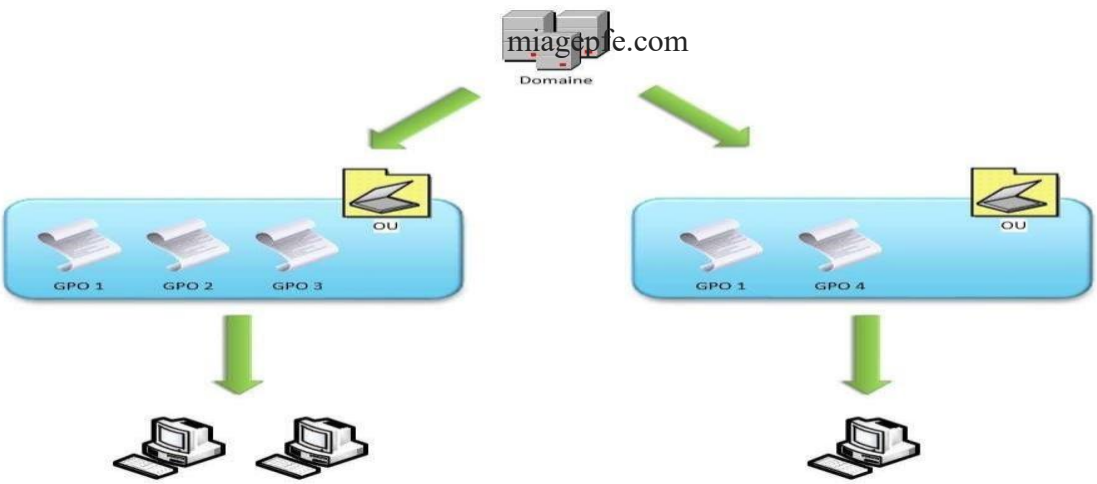
Active Directory offre plusieurs fonctionnalités essentielles à la gestion des réseaux d'entreprise :

Gestion centralisée des utilisateurs et ressources : création, modification et suppression des comptes utilisateurs, groupes et ordinateurs à partir d'un point unique.
Authentification et autorisation : contrôle des accès utilisateurs aux ressources du réseau via des processus d'identification et de droits d'accès.
Application de stratégies de groupe (GPO) : déploiement et application de règles de sécurité et de configuration sur les postes et utilisateurs du réseau.

Répartition logique et hiérarchique : organisation des ressources en domaines, unités d'organisation et forêts.
Gestion des services réseau : intégration et gestion de services comme DNS, DHCP, et autres services de sécurité.

1-3-2 Domaine, Arbre, Forêt et Unité d'Organisation (OU)

✞ Domaine :



Un regroupement logique d'objets AD (utilisateurs, ordinateurs, groupes) partageant une base de données commune et des règles de sécurité. Exemple : miagepfe.com

Contrôleur de Domaine (Domain Controller)

Le contrôleur de domaine est un serveur Windows qui exécute Active Directory et gère toutes les demandes d'authentification et d'accès au réseau. Il maintient la base de données AD et assure la réplication avec d'autres contrôleurs du domaine pour garantir la disponibilité et la redondance des données

Arbre : est un ensemble de domaines qui sont organisés de manière hiérarchique et qui partagent un espace de nom continu

Forêt : Ensemble de plusieurs domaines qui partagent un même schéma AD mais disposent chacun de leur propre base de données. Elle représente la limite de sécurité maximale dans Active Directory.

Unité d'Organisation (OU) : Structure hiérarchique dans un domaine permettant de regrouper des objets pour faciliter leur administration et appliquer des GPO spécifiques.

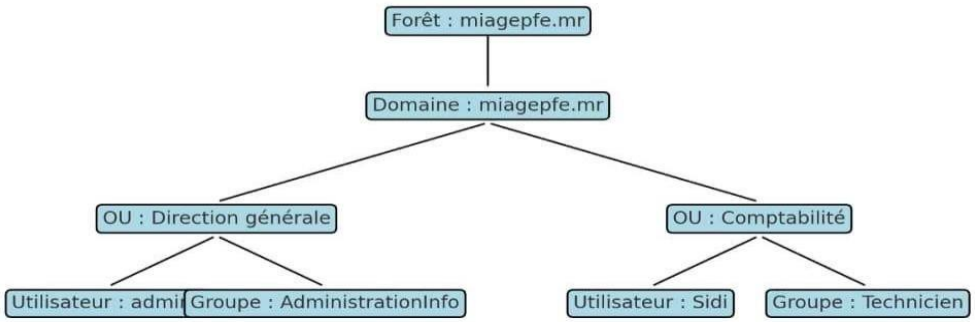
1-3-3 Objets et Attributs

Objet : Élément représenté dans Active Directory, tel qu'un utilisateur, un ordinateur, un groupe ou une imprimante.

Attribut : Information associée à un objet. Par exemple, pour un utilisateur : nom, prénom, adresse e-mail, téléphone

1-3-4 Schéma Active Directory

Le schéma d'Active Directory est la définition formelle de tous les objets et attributs qu'Active Directory peut contenir. Il s'agit d'une collection de définitions stockées dans la base AD, permettant de structurer et normaliser les données des objets.



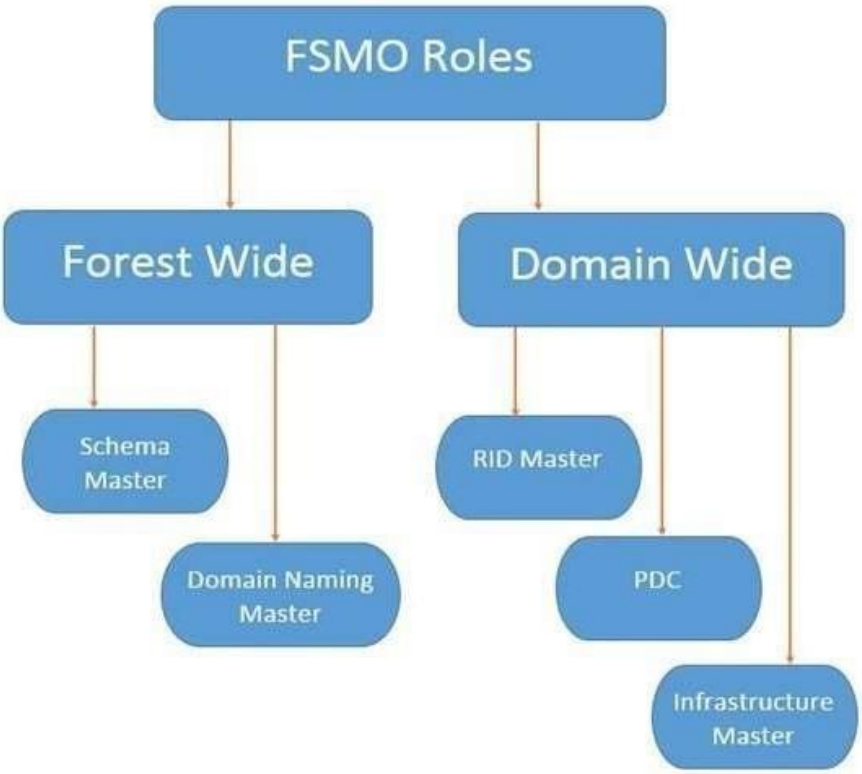
1-3-5 FSMO (Flexible Single Master Operations)

Dans un environnement Active Directory, certains rôles spécifiques appelés FSMO sont attribués à un ou plusieurs contrôleurs de domaine pour assurer certaines opérations sensibles et éviter des conflits.

Il existe cinq rôles FSMO :

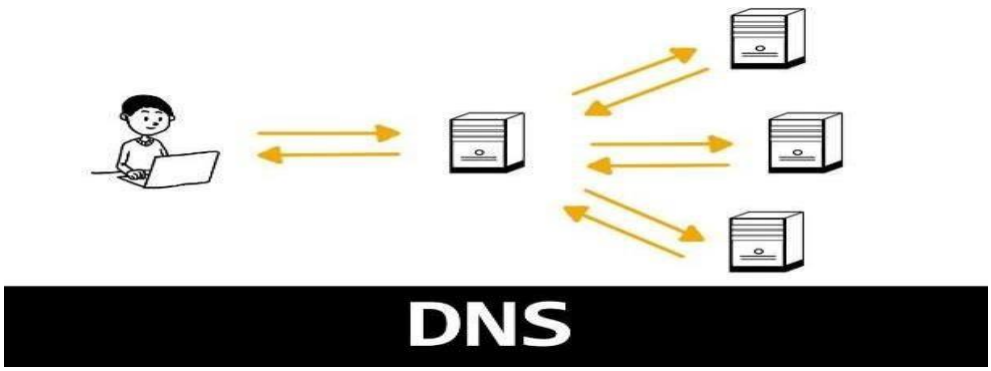
- Schéma Master : gère les modifications du schéma AD.
- Domain Naming Master : contrôle l'ajout et la suppression des domaines dans la forêt.
- RID Master : attribue des identifiants uniques aux objets du domaine.
- PDC Emulator : gère les synchronisations horaires et les mots de passe.
- Infrastructure Master : gère les références inter-domaines.

Schéma FSMO ci-dessous


FSMO Roles
Forest Wide
Domain Wide
Schema Master
Domain Naming Master
RID Master
PDC
Infrastructure Master

1-3-
6 DNS et DHCP :

Le service DNS (Domain Name System) :



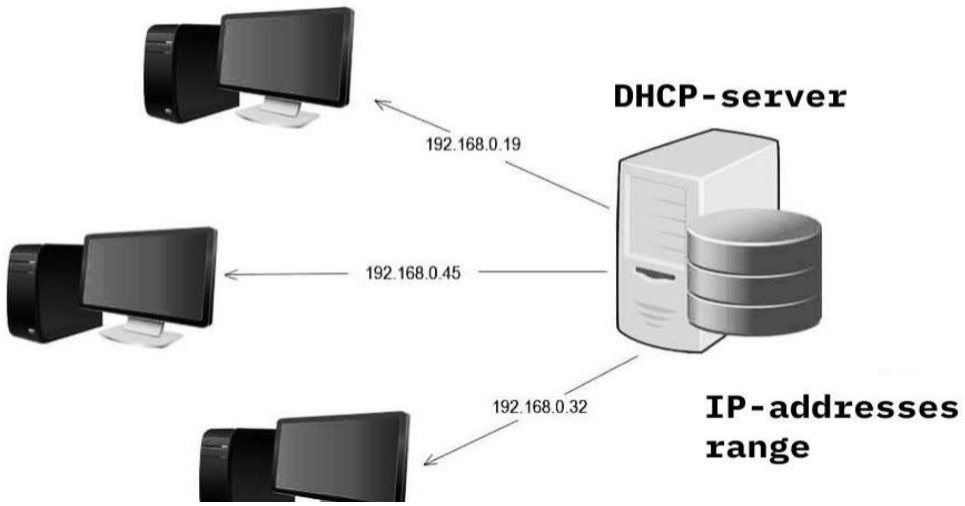
Est étroitement intégré à Active Directory. Il assure la résolution des noms d'hôtes en adresses IP et est indispensable pour le bon fonctionnement des services AD. Lors de l'installation d'AD, des enregistrements DNS spécifiques sont créés pour permettre aux clients de localiser les services du domaine.

DHCP (Dynamic Host Configuration Protocol) :

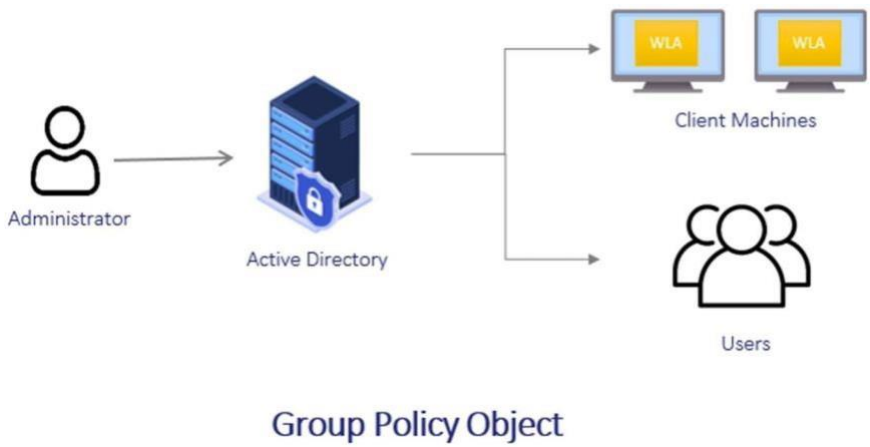
Le service DHCP permet d'attribuer automatiquement des adresses IP et d'autres paramètres réseau (masque, passerelle, DNS…) aux postes clients du réseau. Il simplifie ainsi la gestion des adresses IP et évite les conflits d'adressage postes clients du réseau. Il simplifie ainsi la gestion des adresses IP et évite les conflits d'adressage.

Ces deux services sont indispensables au bon fonctionnement d'une infrastructure Active Directory, car ils facilitent la communication et la gestion dynamique des ressources réseau.

1-3-



7 GPO (Group Policy Object)



Les GPO (Group Policy Object) sont des outils de gestion centralisée des configurations et des politiques de sécurité dans un environnement Active Directory. Elles permettent d'appliquer des règles spécifiques aux utilisateurs et ordinateurs d'un domaine ou d'une unité d'organisation.

Par exemple, grâce aux GPO, l'administrateur peut :

Imposer une politique de mot de passe (longueur minimale, expiration…).

Restreindre l'accès à certaines fonctionnalités ou applications.

Déployer des logiciels automatiquement.

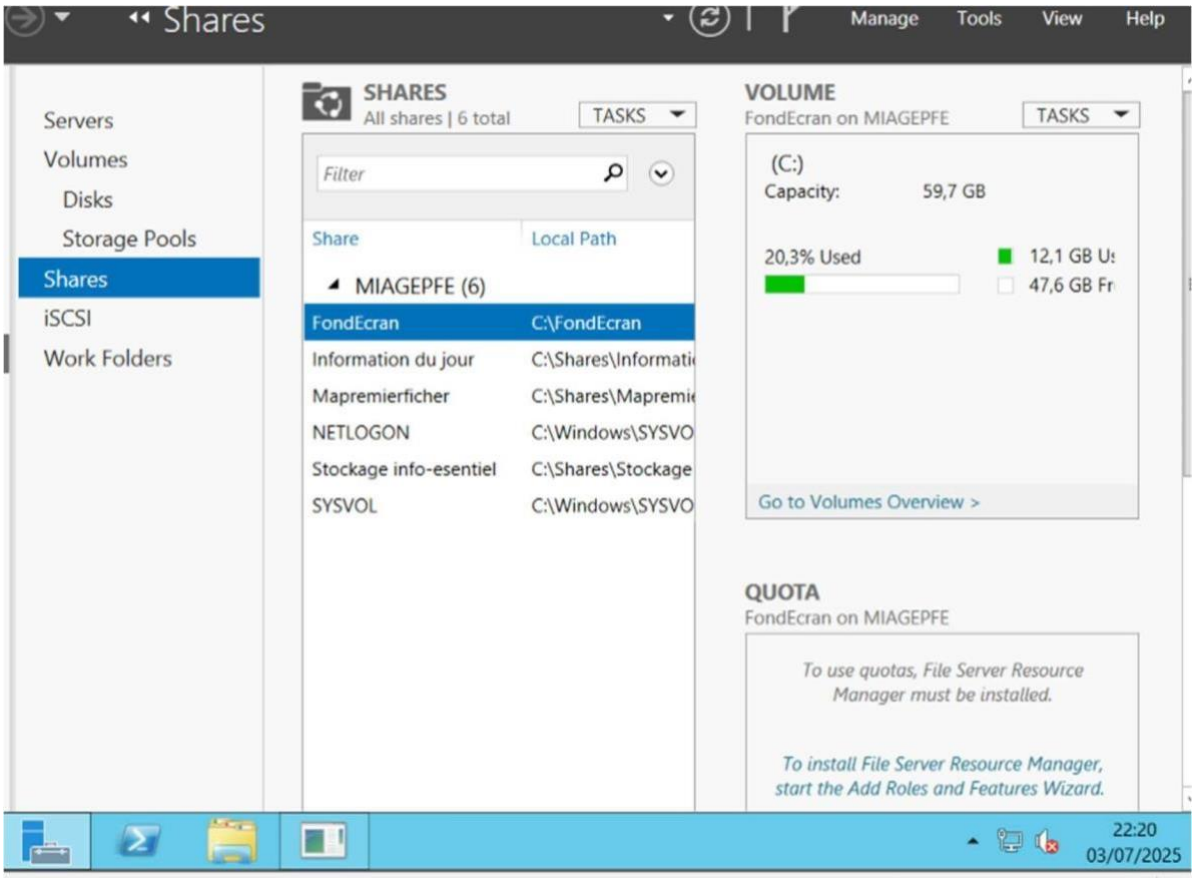
1-3-

Configurer des scripts au démarrage ou à la fermeture des sessions.

Les GPO assurent ainsi une homogénéité de la configuration et renforcent la sécurité du système d'information.

Les GPO sont essentielles pour uniformiser les politiques de sécurité et la configuration sur tout le réseau.

8 Services de fichiers et de rôles



Windows Server 2012 propose également des services de fichiers et de rôles qui permettent de partager des dossiers et des ressources sur le réseau, avec un contrôle précis des droits d'accès.

L'administrateur peut :

Créer des dossiers partagés accessibles à certains utilisateurs ou groupes.

Définir des autorisations NTFS et des autorisations de partage.

Mettre en place des quotas de stockage pour limiter l'espace disque attribué à chaque utilisateur.

1-3-

Installer d’autres rôles serveur comme le serveur d’impression, le serveur web (IIS) ou Hyper-V pour la virtualisation. Ces services assurent la gestion et la sécurisation des ressources partagées au sein de l’entreprise.

Chapitre 2 : Réalisation

Dans ce chapitre, nous allons décrire les étapes pratiques de la mise en œuvre d'une infrastructure Active Directory sous Windows Server 2012, associée aux services réseau et à la gestion des stratégies de groupe dans un environnement virtualisé via VMware Workstation.

2-1 Présentation de l'environnement

2-1-1 Matériel utilisé

Pour la réalisation de ce projet, les ressources suivantes ont été utilisées :

Ordinateur physique (hôte) :

Processeur : Intel Core i3 / 7th Gen (ou supérieur)

Mémoire RAM : 4 Go minimum

Disque dur : 100 Go disponible

Système d'exploitation : Windows 7

Environnement virtualisé VMware Workstation :

1 VM Windows Server 2012 et1 à 2 VM Windows 10 pour les postes clients

Logiciels nécessaires :

VMware Workstation Pro

ISO Windows Server 2012 Datacenter, ISO Windows 10 Professionnel et Outils RSAT pour la gestion distante.

2-1-2 Installation du système

La première étape a consisté à créer une machine virtuelle sous VMware Workstation et à installer Windows Server 2012 :

Paramétrage de la VM :

2 processeurs virtuels

2 Go de RAM et 60 Go de disque

Carte réseau en mode Host-Only ou Bridge

Installation de Windows Server 2012 depuis l'image ISO

Définition d'un mot de passe administrateur sécurisé

Vérification de la connectivité réseau entre les différentes VMs

2-1-3 Configuration initiale du serveur

Avant toute installation de rôle :

Attribution d'une adresse IP statique :
Exemple :

Adresse IP	Masque	Passerelle
192.168.0.10	255.255.255.0	192.168.0.1

Renommage du serveur (ex : MIAGEPFE)

Installation des mises à jour Windows

Désactivation temporaire du pare-feu pour simplifier les tests et configurations

2-2 Mise en place de l'Active Directory

2-2-1 Création du domaine

Installation du rôle Active Directory Domain Services (AD DS) via Server Manager Une fois installé, promotion du serveur en contrôleur de domaine via l'assistant :

Création d'un domaine : miagepfe.mr

Niveau fonctionnel : Windows Server 2012

Configuration du service DNS intégré

Définition du mot de passe pour le Directory Services Restore Mode (pass123@)

Redémarrage du serveur à la fin de l'installation

2-2-2 Ajout des utilisateurs et groupes

Après la création du domaine :

Création d'Unités d'Organisation (OU) :

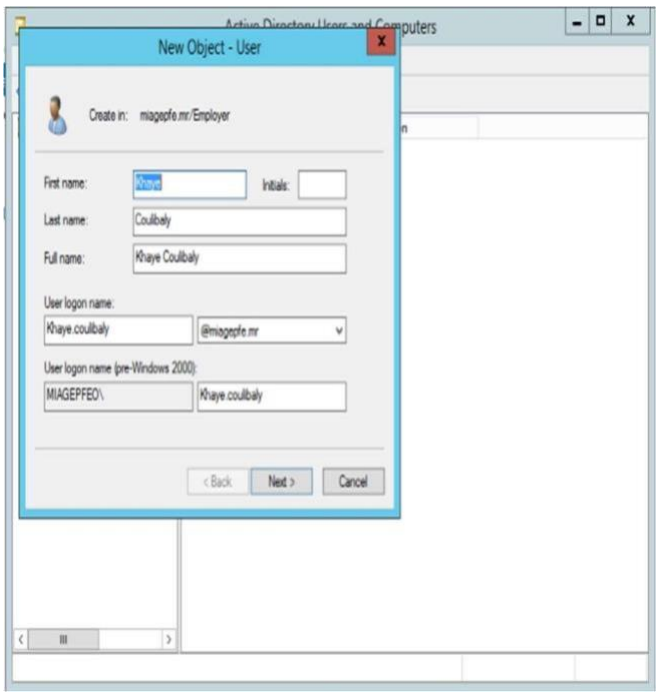
Utilisateurs, Groupes et Postes Clients

Création de comptes utilisateurs : Exemple

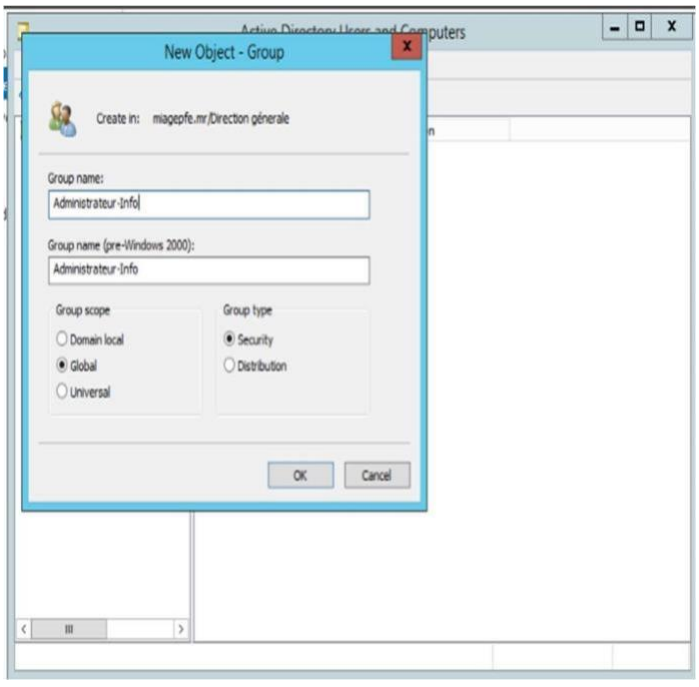
: user: Aly, user: khaye coulibaly Création

de groupes de sécurité :

CREATION UTILISATEUR



CREATION DE GROUPE



Exemple :

Technicie

Comptabilité etc.....

Affectation des utilisateurs dans les groupes respectifs selon leur service

2-3 Services réseaux

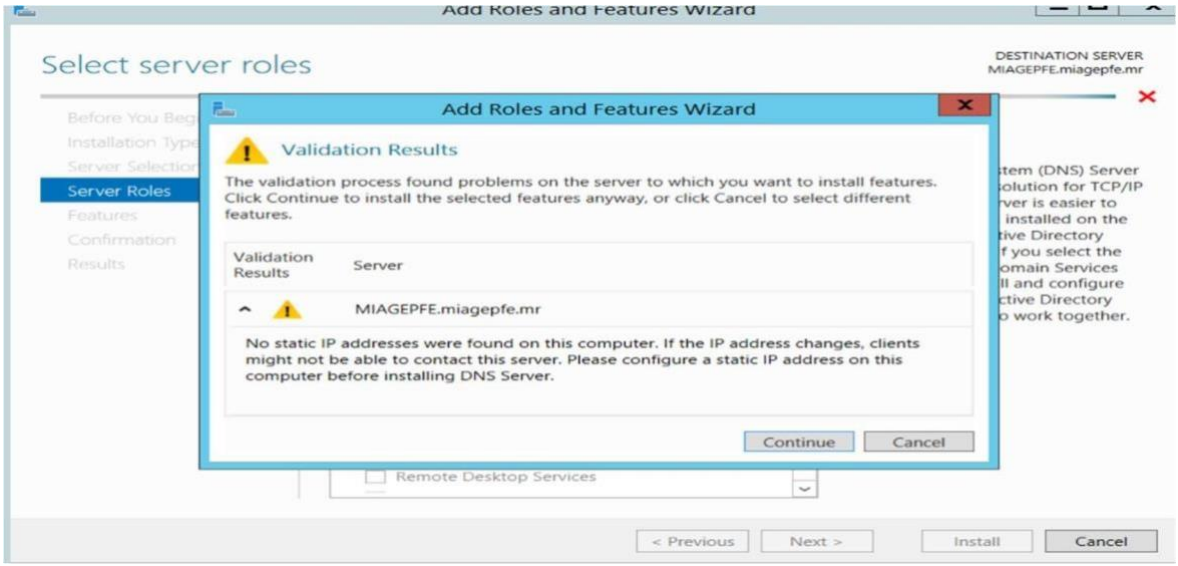
2-3-1 Configuration du DNS

Le rôle DNS est automatiquement installé lors de la promotion du serveur AD DS. Les actions suivantes ont été effectuées :

Vérification de la zone de recherche directe miagepfe.com

Ajout manuel des enregistrements A (par exemple pour les clients)

Test de la résolution DNS via nslookup



2-3-2 Configuration du DHCP

Pour la gestion dynamique des adresses IP :

Installation du rôle DHCP via Server Manager

Création d'une étendue :

Adresse IP	Plage	Masque	Passerelle
Début	192.168.0.100	255.255.255.0	192.168.0.254
Fin	192.168.0.150		

Activation de l'étendue et autorisation du serveur DHCP dans Active Directory

Test sur les clients pour vérifier l'attribution automatique d'IP

2-3-3 Mise en place des GPO (Group Policy Object)

Les stratégies de groupe ont été mises en œuvre pour contrôler et sécuriser les postes clients

Vérification **:**

Création de GPO via la console Group Policy Management Exemples

de stratégies configurées :

Politique de mot de passe : longueur minimale, complexité, durée de validité

Désactivation du panneau de configuration

Blocage des périphériques USB

Déploiement d'un fond d'écran d'entreprise

Liaison des GPO aux OU appropriées

Mise à jour des stratégies sur les clients avec la commande gpupdate /force

2-3-4 Partages de fichiers sécurisés

Pour assurer le stockage et le partage sécurisé des documents :

Création de dossiers partagés sur le serveur :

Exemple : \\ MIAGEPFE \Mapremierepartage

Exemple : \PartageIT
Introduction

Attribution des droits NTFS :

Lecture seule pour certains utilisateurs, lecture/écriture pour d'autres et configuration des permissions de partage.

Test des accès à partir des clients :

Vérification de la visibilité des dossiers partagés et Contrôle des autorisations en lecture et écriture.

Chapitre 3 : Tests et Validation

Ce chapitre présente l'ensemble des tests réalisés afin de vérifier la bonne installation, la configuration correcte et le fonctionnement des différents services mis en place dans le cadre de ce projet. Les tests permettent de s'assurer que l'infrastructure Active Directory et les services réseau associés répondent aux besoins définis.

3-1 Test de connectivité réseau

Afin de valider la communication entre les différentes machines virtuelles :

Commande ping :

Depuis le serveur, ping vers les clients Windows 10

Depuis les clients, ping vers le serveur Active Directory

Résultat attendu :

Les paquets sont envoyés et reçus sans perte, prouvant que la connectivité réseau est opérationnelle.

Commande nslookup :

Test de résolution DNS des noms de machines du domaine Résultat

attendu :

Les noms des machines sont bien résolus en adresses IP par le serveur DNS.

3-2 Vérification du bon fonctionnement d'Active Directory

Pour s'assurer que le service Active Directory Domain Services (AD DS) fonctionne correctement :

Création de nouveaux utilisateurs via la console Active Directory Users and Computers

Authentification sur les postes clients avec les comptes utilisateurs créés dans le domaine

Résultat attendu :

Les utilisateurs peuvent se connecter sans erreur sur les postes clients avec leurs identifiants Active Directory.

3-3 Tests DNS et DHCP

Pour le DNS :

Vérification des zones DNS

Résolution correcte des noms en IP avec nslookup Pour

le DHCP :

Vérification que les clients reçoivent bien une adresse IP automatique dans la plage définie par le serveur DHCP

Commande ipconfig /all sur les clients pour vérifier :

Adresse IP attribuée

Masque de sous-réseau

Passerelle

Serveur DNS

Résultat attendu :

Les clients reçoivent les bonnes informations réseau automatiquement.

3-4 Validation des GPO appliquées sur les postes clients

Pour contrôler l'application des stratégies de groupe (GPO) :

Exécution de la commande gpupdate /force sur les clients Vérification

:

Politique de mot de passe (test à la création/modification du mot de passe)

Blocage de l'accès au panneau de configuration ou à certains périphériques (clé USB)

Application du fond d'écran personnalisé (le cas échéant) Résultat attendu :

Les restrictions et personnalisations définies dans les GPO sont bien appliquées sur les postes clients.

3-5 Test des droits d'accès aux dossiers partagés

Pour tester la sécurité des partages de fichiers :

Connexion à un dossier partagé depuis un poste client (\\MIAGEPFE\Mapremierpartage)

3-6 Test des droits :

Lecture seule pour certains groupes

Lecture/écriture pour les groupes autorisés

3-7 Résultat attendu :

Les utilisateurs accèdent uniquement aux dossiers qu'ils sont autorisés à consulter et selon les droits définis**.**

3-8 Récapitulatif des résultats des tests

Test effectué	**Résultat**	**Observation**

Ping entre serveur et client	Réussi	Pas de perte de paquets
Résolution DNS (nslookup)	Réussi	Résolution de nom
Attribution d'IP via DHCP	Réussi	IP attribuées dans la bonne plage
Authentification utilisateur du Domaine	Réussi	Connexion possible avec AD
Application de GPO	Réussi	Politiques de mot passe appliquée
Accès aux dossiers partages	Réussi	Droits NTFS et partages respectés

CONCLUSION GENERALE

La mise en œuvre de ce projet de création et de configuration d'une infrastructure Active Directory sous Windows Server 2012 dans un environnement virtualisé a permis d'atteindre les objectifs fixés en début de projet. Grâce à cette réalisation, l'ensemble des services réseau essentiels au bon fonctionnement d'un système d'information en entreprise ont été déployés et testés avec succès.

Ce projet a démontré l'importance d'une gestion centralisée des ressources informatiques et des utilisateurs au sein d'un domaine Active Directory. Il a permis de :

Structurer un environnement réseau sécurisé et organisé.

Automatiser l'attribution des adresses IP via DHCP.

Assurer la résolution des noms de machines par le service DNS.

Appliquer des stratégies de sécurité via les GPO pour standardiser les configurations et limiter les risques.

Mettre en place des partages de fichiers sécurisés, accessibles selon des droits définis par groupe d'utilisateurs.

Les différents tests effectués sur les fonctionnalités mises en place ont confirmé la fiabilité et l'efficacité de l'infrastructure. Les utilisateurs peuvent se connecter au domaine, obtenir des adresses IP dynamiques, accéder aux ressources partagées selon leurs droits et subir les restrictions de sécurité prévues par les stratégies.

✞ Compétences acquise

À travers ce projet, plusieurs compétences techniques et organisationnelles ont été consolidées :

Installation et configuration d'un serveur Windows Server 2012

Déploiement et administration d'un domaine Active Directory

Gestion des services DNS et DHCP

Mise en place et application des Group Policy Objects (GPO)

Configuration de partages sécurisés et attribution de droits NTFS

Réalisation de tests et validation d'une infrastructure réseau virtualisée.

Bibliographie / Webographie

✞ **Bibliographie**

- Jean-Philippe Bay, Michel Martin — Windows Server 2012 R2 – Installation, configuration et administration — Éditions ENI, 2014.
- Sébastien Rohaut — Active Directory : Concepts, administration et mise en œuvre — Éditions ENI, 2017.
- Microsoft Press — Windows Server 2012 Inside Out — Ed Bott, 2013. ✞ **Webographie**
- Microsoft Learn

Documentation officielle et tutoriels sur Windows Server et Active Directory.

https://learn.microsoft.com/fr-fr/windows-server/

• Documentation Active Directory — Microsoft Docs

https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual- dc/active-directory-domain-services-overview

• Comment ça marche.net (CCM)

Guides et astuces pour administrateurs systèmes.

https://www.commentcamarche.net/

- Developpez.com

Forum et tutoriels en administration système et réseau.

https://www.developpez.com/

- IT-Connect.fr

Articles et tutoriels sur Windows Server, Active Directory et les GPO.

https://www.it-connect.fr/