



UNIVERSITE DE FIANARANTSOA
ECOLE NATIONALE D'INFORMATIQUE

**MEMOIRE DE FIN D'ETUDE POUR L'OBTENTION DU DIPLOME DE LICENCE
PROFESSIONNELLE EN INFORMATIQUE**

Mention : INFORMATIQUE

Parcours : Informatique Générale

Thème :

**ADMINISTRATION ET REPLICATION D'ACTIVE DIRECTORY AVEC MISE
EN PLACE DE VPN**

Présenté le **27 Juillet 2021**,

Par : Monsieur **RAHARISOLOFO Deddy**

Membre du jury :

Président : Monsieur **RAKOTOHASIMBAHOAKA Cyprien Robert**, Maître de Conférences

Examineur : Monsieur **RALAIVAO Jean Christian**, Assistant de l'Enseignement Supérieur et de Recherche

Rapporteurs :

- Monsieur **SIKA**, Assistant de l'Enseignement Supérieur et de Recherche
- Monsieur **RANDRIAMPARAMANIRAKA Lovasoa**, Administrateur et Architecte réseau d'UDITEC

Année Universitaire 2019-2020

CURRICULUM VITAE



RAHARISOLOFO Deddy

22ans, Célibataire, Malagasy

Lot 1116 D 131 MAHAZOARIVO-SUD-110 ANTSIRABE

+261 34 53 142 52

Raharisolofodeddy66@gmail.com

FORMATION

- **2020** : Troisième année d'étude en Formation Informatique Générale – Ecole Nationale d'Informatique.
- **2019** : Deuxième année d'étude en Formation Informatique Générale – Ecole Nationale d'Informatique.
- **2018** : Première année d'étude en Formation Informatique Générale – Ecole Nationale d'Informatique.
- **2016** : Obtention du Baccalauréat série C – Lycée Privée St Joseph.

EXPERIENCES PROFESSIONNELLES

- **2019-2020** : Stage pratique Networking au sein de l'entreprise UDITEC
- **2018-2019** : Stage pratique en développement d'application Web chez DSSI

PROJET REALISES

2018 :

- Création d'un site Web
- Réalisation de logiciel de gestion d'adresse IP avec C++ et Qt

COMPETENCES COMPLEMENTAIRES

- Langues :
 - Français : lu, écrit et parlée(couramment)
 - Anglais : lu, écrit et parlée(intermédiaire)
- Bureautique : Microsoft Word, Excel, PowerPoint
- Langage : C, C++, PHP, Python
- Développement web : HTML, CSS, JAVASCRIPT
- Protocole Réseaux : OSI, TCP/IP, ARP, SNMP
- Système d'exploitation : WINDOWS

CENTRE D'INTERET

- LOISIRS : Guitare, lecture
- SPORTS : Basketball, Football

REMERCIEMENTS

Je tiens à remercier toutes les personnes de par leur soutien, sans qui, l'aboutissement de ce stage n'aurait été. Cela se porte précisément sur :

Monsieur RAFAMANTANTSOA Fontaine, Professeur et président de l'université de Fianarantsoa, pour l'organisation de cette année universitaire.

Monsieur RAMAMONJISOA Bertin Olivier, Professeur titulaire et Directeur de L'Ecole Nationale d'Informatique.

Monsieur RABETAFIKA Louis Haja, responsable de mention de l'Ecole Nationale d'Informatique pour le bon déroulement et le bon fonctionnement de notre parcours.

Monsieur Gilante GESAZAFY, Responsable de parcours « Informatique General »

Monsieur Siaka Assistant de l'enseignement supérieur et de recherche pour son aide précieuse et ses conseils avisés.

Monsieur RANDRIAMPARAMANIRAKA Lovasoa Architecte réseau de l'entreprise UDITEC et également mon encadreur professionnel, pour sa disponibilité et son dévouement à transmettre ses connaissances du domaine professionnel.

Et enfin, mes parents, ma familles, amies et tous ceux qui ont participé de près ou de loin à la réussite de ce stage.

SOMMAIRE GENERALE

CURRICULUM VITAE.....	I
REMERCIEMENTS.....	III
SOMMAIRE GENERALE.....	IV
LISTE DES TABLEAUX.....	VII
LISTES DES ABREVIATIONS.....	VIII
INTRODUCTION GENERALE.....	1
PARTIE I : PRESENTATION GENERALE.....	2
CHAPITRE I - PRESENTATION DE L'ECOLE NATIONALE D'INFORMATIQUE	3
CHAPITRE II : PRESENTATION D'UDITEC.....	13
CHAPITRE III : DESCRIPTION DU PROJET.....	15
PARTIE II : ANALYSE ET CONCEPTION.....	17
Chapitre IV - ANALYSE DE L'EXISTANT.....	18
CHAPITRE V – CRITIQUE DE L'EXISTANT.....	22
PARTIE III : REALISATIONS.....	23
Chapitre VI - CHOIX DES OUTILS.....	24
Chapitre VII – MISE EN PLACE ET INSTALLATION.....	40
CONCLUSION.....	55
GLOSSAIRE.....	X
REFERENCES BIBLIOGRAPHIQUES.....	XI
REFERENCES WEBOGRAPHIQUES.....	XII
TABLE DES MATIERES.....	XIII
RESUME.....	XVII
ABSTRACT.....	XVII

LISTE DES FIGURES

Figure 1 : Organigramme de l'ENI	
Figure 2 : Organigramme d'UDITEC.....	14
Figure 3 : Topologie du réseau d'UDITEC.....	18
Figure 4 : Les objets d'Active Directory.....	26
Figure 5 : Forêt et arborescence.....	27
Figure 6 : Catalogue Global.....	29
Figure 7 : Réplication dans active directory.....	33
Figure 8 : Types de réplication dans Active Directory.....	34
Figure 9 : ajout des rôles et fonctionnalités.....	40
Figure 10 : ajout des rôles et fonctionnalités.....	40
Figure 11 : Attribution de rôles serveurs.....	40
Figure 12 : Ajout des Fonctionnalités requises.....	41
Figure 13 : Installation du service Active Directory.....	41
Figure 14 : Configuration de contrôleur de domaine.....	42
Figure 15 : Ajout de la forêt.....	42
Figure 16 : Options contrôleur de domaine.....	43
Figure 17 : Vérification du NetBios.....	43
Figure 18 : Vérification des options d'installation.....	44
Figure 19 : Vérification des prérequis.....	44
Figure 20 : Installation active de l'annuaire.....	45
Figure 21 : Administration des utilisateurs et ordinateurs.....	45
Figure 22 : Accès à la fenêtres Utilisateurs et Ordinateurs Active Directory.....	46
Figure 23 : ajout d'une nouvelle unité d'organisation.....	46

Figure 24 : Arborescence de compte utilisateur.....	47
Figure 25 : Ajout d'utilisateur.....	47
Figure 26 : Attribution de mot de passe utilisateur.....	48
Figure 27 : gestion des droits d'accès au compte.....	48
Figure 28 : Stratégie de groupe.....	49
Figure 29 : Attribution de nouvelle stratégie de groupe.....	49
Figure 30 : Paramètre de la GPO.....	50
Figure 31 : Méthode de déploiement.....	50
Figure 32 : Configuration de point d'accès.....	51
Figure 33 : Sélection du moyen de connexion.....	51
Figure 34 : Mise en place du groupe et ajout d'utilisateur du groupe.....	52
Figure 35 : Exemple de topologie d'usage du service.....	54

Liste des tableaux

Tableau 1 : Organisation du système de formation pédagogique de l'Ecole.....	6
Tableau 2 : Architecture des études correspondant au système LMD.....	7
Tableau 3 : Liste des formations existantes à l'ENI.....	8
Tableau 4 : Débouchés professionnels éventuels des diplômés	11
Tableau 5 : Chronogramme de travaux.....	15
Tableau 6 : Liste des moyens matériels.....	16
Tableau 7 : Types de réseau de UDITEC.....	19
Tableau 8 : Les différents équipements d'interconnexion.....	19
Tableau 9 : exemples de poste de travail.....	20
Tableau 10 : les différents serveurs.....	21

Liste des abréviations

AD	: Active Directory
AD DS	: Active Directory Domain Services
AD LDS	: Active Directory Lightweight Domain Services
AD CS	: Active Directory Certificate Services
AD FS	: Active Directory Federation Services
ADRMS	: Active Directory Rights Management Services
BTS	: Brevet de Technicien Supérieur
CPU	: Central Processing Unit
DEA	: Diplôme d'Etudes Approfondies
DTS	: Diplôme de Technicien Supérieur
DUT	: Diplôme Universitaire de Technicien
DHCP	: Dynamic Host Configuration Protocol
DC	: Domain Controller
ENI	: Ecole Nationale d'Informatique
ERP	: Enterprise Resources Planning
GPO	: Group Policy Object
HDD	: Hard Disk Drive
IT	: Information Technology
KCC	: Knowledge Consistency Checker
LDAP	: Lightweight Directory Access Protocol
LMD	: Licence – Master – Doctorat
LAN	: Local Area Network
OU	: Organizational Unit

PC	: Personal Computer
RAM	: Random Access Memory
SVM	: Shielded Virtual Machine
SAM	: Security Account Manager
WAN	: Wide Area Network
WLAN	: Wide Local Area Network
Wi-Fi	: Wireless Fidelity

INTRODUCTION GENERALE

La technologie de l'information est une évolution du système actuel qu'on ne peut éviter. Elle a permis l'épanouissement de la majorité des entreprises et société actuelle sur le chemin de l'expansion et d'élargissement du terrain d'influence.

Windows Server est aujourd'hui au cœur de l'informatique des entreprises. Déployé massivement dans les PME comme dans les grandes entreprises, Windows Server est le socle sur lequel s'appuie un grand nombre d'entreprises pour fournir à leurs utilisateurs une large palette de services d'infrastructure et de services applicatifs essentiels au bon fonctionnement du réseau. Il permet, grâce à ses outils de bien administrer les ressources du parc informatique auquel il est assigné.

Le travail décrit dans ce mémoire se portera sur l'Active Directory, qui permettra la fiabilité et la disponibilité ainsi que la robustesse et la cohérence du système que nous allons diviser en trois parties principales. La première consacrée à la présentation (Ecole Nationale d'Informatique), la seconde partie qui se porte sur l'analyse et la dernière ou l'on émettra la réalisation du projet.

Nous terminons ce mémoire par une brève conclusion ainsi que par des perspectives ouvertes.

PARTIE I :

Présentation Générale

CHAPITRE I - PRESENTATION DE L'ECOLE NATIONALE D'INFORMATIQUE

1.1. Information d'ordre générale

L'Ecole Nationale d'Informatique, en abrégé ENI, est un établissement d'enseignement supérieur rattaché académiquement et administrativement à l'Université de Fianarantsoa. Le siège de l'Ecole se trouve à Tanambao- Antaninarenina à Fianarantsoa.

Les coordonnées pour la prise de contact avec l'Ecole sont les suivantes :

Ecole Nationale d'Informatique (ENI)

Antaninarenina Tanambao

BP 1487 FIANARANTSOA (301)

Téléphones : 034 05 733 36 ou 033 42 302 02

Adresse mél : eni@eni-univ-fianar.mg. Site : www.eni-univ-fianar.mg

1.2. Missions et historiques

L'ENI se positionne sur l'échiquier socio-éducatif malgache comme étant le plus puissant secteur de diffusion et de vulgarisation des connaissances et des technologies informatiques.

Cette Ecole Supérieure peut être considérée aujourd'hui comme la vitrine et la pépinière des élites informaticiennes du pays.

L'Ecole s'est constituée de façon progressive au sein du Centre Universitaire Régional (CUR) de Fianarantsoa.

De façon formelle, l'ENI était constituée et créée au sein du (CUR) par le décret N° 83-185 du 24 Mai 1983, comme étant le seul établissement Universitaire Professionnalisé au niveau national, destiné à former des techniciens et des Ingénieurs de haut niveau, aptes à répondre aux besoins et exigences d'Informatisation des entreprises, des sociétés et des organes implantés à Madagascar.

L'ENI a pour conséquent pour mission de former des spécialistes informaticiens compétents et opérationnels de différents niveaux notamment :

En fournissant à des étudiants des connaissances de base en informatique ;

En leur transmettant le savoir-faire requis, à travers la professionnalisation des formations dispensées et en essayant une meilleure adéquation des formations par rapport aux besoins évolutifs des sociétés et des entreprises.

En initiant les étudiants aux activités de recherche dans les différents domaines des Technologies de l'information et de la communication (TIC).

L'implantation de cette Ecole Supérieure de technologie de pointe dans un pays en développement et dans une Province (ou Faritany) à tissu économique et industriel faiblement développé ne l'a pourtant pas défavorisée, ni empêchée de former des spécialistes informaticiens de bon niveau, qui sont recherchés par les entreprises, les sociétés et les organismes publics et privés sur le marché de l'emploi.

La filière de formation d'Analystes Programmeurs a été mise en place à l'Ecole en 1983, et a été gelée par la suite en 1996, tandis que la filière de formation d'ingénieurs a été ouverte à l'Ecole en 1986.

Dans le cadre du Programme de renforcement en l'Enseignement Supérieur (PRESUP) la filière de formation des Techniciens Supérieurs en Maintenance des Systèmes des informatiques a été mise en place en 1986 grâce à l'appui matériel et financier de la Mission Française de coopération auprès de l'Ambassade de France à Madagascar.

Une formation pour l'obtention de la certification CCNA et / ou NETWORK + appelée « CISCO Networking Academy » a été créée à l'Ecole en 2002-2003 grâce au partenariat avec CISCO SYSTEM et l'Ecole Supérieure Polytechnique d'Antananarivo (ESPA). Cependant, cette formation n'avait pas duré longtemps.

L'organisation de stage en entreprise continue non seulement à renforcer la professionnalisation des formations dispensées, mais elle continue surtout à accroître de façon exceptionnelle les opportunités d'embauche pour les diplômés de l'Ecole:

- Génie Logiciel et base de Données.
- Administration des Système et réseaux.

La mise en place à l'Ecole de ces deux options de formation devait répondre au besoin de basculement vers le système Licence – Master – Doctorat (LMD).

Mais la filière de formation des Techniciens Supérieurs en Maintenance des Systèmes Informatiques a été gelée en 2009.

En vue de surmonter les difficultés de limitation de l'effectif des étudiants accueillis à l'Ecole, notamment à cause du manque d'infrastructures, un système de « Formation Hybride » a été mise en place à partir de l'année 2010. Il s'agit en effet d'un système de formation semi-présentielle et à distance avec l'utilisation de la visioconférence pour la formation à distance.

Le système de formation hybride a été ainsi créé à Fianarantsoa ainsi qu'Université de Toliara.

1.3. Organigramme institutionnel de l'ENI

Cet organigramme de l'Ecole est inspiré des dispositions du décret N° 83-185 du 24 Mai 1983.

Sur cet organigramme, l'Ecole placée sous la tutelle académique et administrative de l'Université de Fianarantsoa, est dirigée par un Directeur élu par les Enseignants – Chercheurs permanents de l'Etablissement et nommé par un décret pris en Conseil des Ministres pour un mandat de 3 ans.

Le Conseil de l'Ecole est l'organe délibérant de l'Ecole.

Le Collège des Enseignants regroupant tous les enseignants-chercheurs de l'Ecole est chargé de résoudre les problèmes liés à l'organisation pédagogique des enseignements. Il propose et coordonne les programmes d'activités pédagogiques.

Le Conseil Scientifique propose les orientations pédagogiques et scientifiques de l'établissement, en tenant compte notamment de l'évolution du marché de travail et de l'adéquation des formations dispensées par rapport aux besoins des entreprises. Il coordonne les programmes de recherche à mettre en œuvre à l'Ecole.

Le Secrétariat principal coordonne les activités des services administratifs (Scolarité, Comptabilité, et Intendance).

Conformément aux textes en vigueur régissant les Etablissements malgaches d'Enseignement Supérieur, qui sont barrés sur le système LMD, les Départements de Formation pédagogique ont été ainsi remplacés par des Mentions et des parcours. Et les chefs des Départements ont été ainsi remplacés par des responsables des mentions et les responsables des parcours.

L'organigramme de l'Ecole Nationale d'Informatique est présenté par la Figure 1.

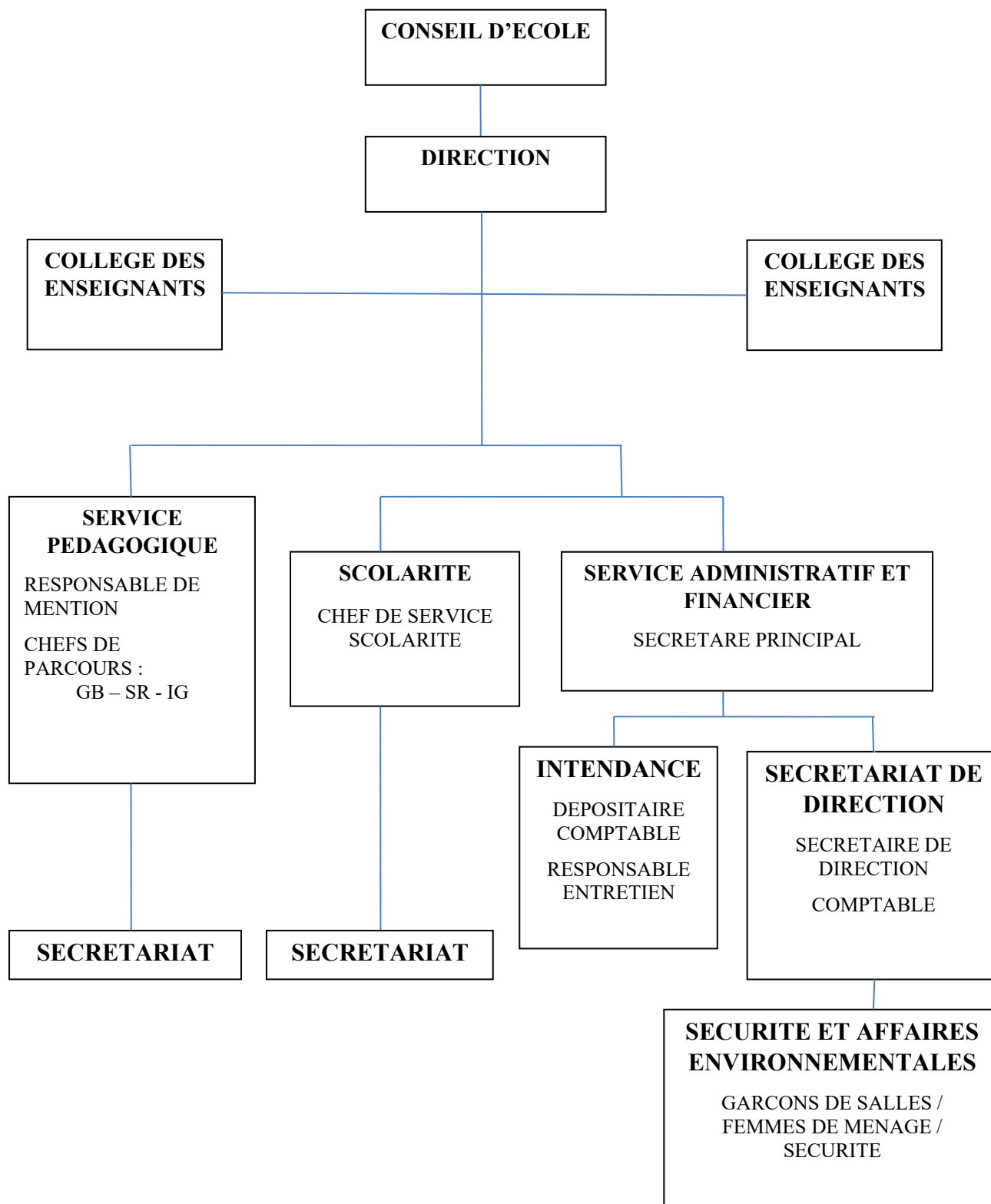


Figure 1: organigramme de l'ENI

1.4. Domaines et spécialisation

Les activités de formation et de recherche organisées à l'ENI portent sur les domaines suivants :

- Génie logiciel et Base de Données ;
- Administration des Systèmes et Réseaux ;
- Informatique Générale ;
- Modélisation informatique et mathématique des Systèmes complexes.

D'une manière plus générale, les programmes des formations sont basés sur l'informatique de gestion et sur l'informatique des Systèmes et Réseaux. Et les modules de formation intègrent aussi bien des éléments d'Informatique fondamentale que des éléments d'Informatique appliquée.

Le Tableau 1 décrit l'organisation du système de formation pédagogique de l'Ecole.

Tableau 1 Organisation du système de formation pédagogique de l'école

Formation Théorique	Formation Pratique
<ul style="list-style-type: none">- Enseignement théorique- Travaux dirigés- Travaux pratiques- Conférences	<ul style="list-style-type: none">- Etude de cas- Travaux de réalisation- Projets/ Projets tutoriels- Voyages d'Etudes- Stages en entreprise

1.5. Architecture des formations pédagogiques

Le recrutement des étudiants à l'ENI se fait uniquement par voie de concours d'envergure nationale en première année de Licence Professionnelle.

Les offres de formation organisées à l'Ecole ont été validées par la Commission Nationale d'Habilitation (CNH) auprès du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique selon les dispositions de l'Arrêté N°31.174/2012-MENS en date du 05 Décembre 2012.

Au sein de l'ENI, il existe une seule mention (INFORMATIQUE) et trois parcours :

- Génie logiciel et Base de Données,
- Administration des Systèmes et Réseaux,
- Informatique Générale.

L'architecture des études à trois niveaux conforme au système Licence-Master-Doctorat (LMD) permet les comparaisons et les équivalences académiques des diplômes au niveau international.

- L = Licence (Bac + 3) = L1, L2, L3 = 6 semestres S1 à S6
- M = Master (Bac + 5) = M1, M2 = 4 semestres S7 à S10

Le diplôme de licence est obtenu en 3 années des études après Baccalauréat. Et le diplôme de Master est obtenu en 2 ans après obtention du diplôme de LICENCE.

Le MASTER PROFESSIONNEL est un diplôme destiné à la recherche d'emploi au terme des études.

Le MASTER RECHERCHE est un diplôme qui remplace l'ancien Diplôme d'Etudes Approfondies (DEA), et qui permet de s'inscrire directement dans une Ecole Doctorale au terme des études.

- D = Doctorat (Bac +8)

Le Doctorat est un diplôme qu'on peut obtenir en 3 ans après l'obtention du diplôme de MASTER RECHERCHE.

Le Tableau 2 présente l'architecture des études correspondant au système LMD.

Tableau 2 Architecture des études correspondant au système LMD



La licence peut avoir une vocation générale ou professionnelle.

Le master peut avoir une vocation professionnelle ou de recherche.

Tableau 3 Listes des formations existantes à l'ENI

	FORMATION	
	LICENCE PROFESSIONNELLE	MASTER
Condition d'admission	Par voie de concours Formation Professionnelle : 100 candidats Formation hybride : 150 candidats	
Condition d'Accès	Bac de série C, D ou Technique	Etre titulaire de licence professionnelle
Durée de Formation	3 ans	2 ans
Diplôme délivré	Diplôme de Licence Professionnelle	Diplôme de Master Professionnel Diplôme de Master Recherche

L'accès en première année de MASTER se fait automatiquement pour les étudiants de l'École qui ont obtenu le diplôme de Licence Professionnelle.

Le Master Recherche permet à son titulaire de poursuivre directement des études en doctorat et de s'inscrire directement dans une École Doctorale.

Les Ecoles Doctorales jouissent d'une autonomie de gestion par rapport aux Etablissements de formation universitaire.

Il convient de signaler que par arrêté ministériel N° 21.626/2012 – MESupRES publié le 9 Août 2012 par la Commission Nationale d'habilitation (CNH), l'Ecole Doctorale « Modélisation – Informatique » a été habilitée pour l'Université de Fianarantsoa.

Depuis l'année universitaire 2010-2011, l'ENI s'est mise à organiser des formations hybrides en informatique dans les différentes régions (Fianarantsoa, Toliara) en raison de l'insuffisance de la capacité d'accueil des infrastructures logistiques. En effet, le système de formation hybride semi - présentielle utilise la visioconférence pour la formation à distance.

Bien qu'il n'existe pas encore au niveau international de reconnaissance écrite et formelle des diplômes délivrés par l'ENI, les étudiants diplômés de l'Ecole sont plutôt bien accueillis dans les instituts universitaires étrangers (Canada, Suisse, France...).

1.6. Relation de l'ENI avec les entreprises et organismes

Les stages effectués chaque année par les étudiants mettent l'Ecole en rapport permanent avec plus de 300 entreprises et organismes publics, semi-publics et privés, nationaux et internationaux.

L'Ecole dispose ainsi d'un réseau d'entreprises, de sociétés et d'organismes publics et privés qui sont des partenaires par l'accueil en stage de ses étudiants, et éventuellement pour le recrutement après l'obtention des diplômes par ces derniers.

Les compétences que l'Ecole cherche à développer chez ses étudiants sont l'adaptabilité, le sens de la responsabilité, du travail en équipe, le goût de l'expérimentation et l'innovation.

En effet, la vocation de l'ENI est de former des techniciens supérieurs de niveau LICENCE et des ingénieurs de type généraliste de niveau MASTER avec des qualités scientifiques, techniques et humaines reconnues, capables d'évoluer professionnellement dans des secteurs d'activité variés intégrant l'informatique.

Les stages en milieu professionnel permettent de favoriser une meilleure adéquation entre les formations à l'Ecole et les besoins évolutifs du marché de l'emploi. Les principaux débouchés professionnels des diplômés de l'Ecole concernent les domaines suivants :

L'informatique de gestion d'entreprise :

- les technologies de l'information et de la communication (TIC),
- la sécurité informatique des réseaux,
- l'administration des réseaux et des systèmes,
- les services bancaires et financiers, notamment le Mobile Banking,
- les télécommunications et la téléphonie mobile,
- les Big Data,
- le commerce, la vente et l'achat, le Marketing,
- l'ingénierie informatique appliquée,
- l'écologie et le développement durable.

Parmi les sociétés, entreprises et organismes partenaires de l'Ecole, on peut citer : ACCENTURE Mauritius, Air Madagascar, Ambre Associates, Airtel, Agence Universitaire de la Francophonie (AUF) , B2B, Banque Centrale, BFG-SG, BIANCO, BLUELINE, Bureau national de gestion des Risques et des catastrophes (BNGRC), CEDIIFianarantsoa, Data Consulting, Central Test, Centre National Antiacridien, CNRE, CHU, CNRIT, COLAS, Direction Générale des Douanes, DLC, FID, FTM, GNOSYS, IBONIA, INGENOSIA, INSTAT, JIRAMA, JOUVE, MADADEV, MEF, MEN, MESupRES, MFB, MIC, Min des

postes/Télécommunications et du Développement Numérique, NEOV MAD, Ny Havana, Madagascar National Parks, OMNITEC, ORANGE, OTME, PRACCESS, QMM Fort-Dauphin, SMMC, SNEDADRS Antsirabe, Sénat, Société d'Exploitation du Port de Toamasina (SEPT), SOFTWELL, Strategy Consulting, TELMA, VIVETEC, Société LAZAN'I BETSILEO, WWF ...

L'organisation de stage en entreprise continue non seulement à renforcer la professionnalisation des formations dispensées, mais elle continue surtout à accroître de façon exceptionnelle les opportunités d'embauche pour les diplômés de l'Ecole.

1.7. Partenariat au niveau international

Entre 1996 et 1999, l'ENI avait bénéficié de l'assistance technique et financière de la Mission Française de Coopération et d'action culturelle dans le cadre du Programme de Renforcement de l'Enseignement Supérieur (PRESUP) consacré à l'Ecole a notamment porté sur :

- une dotation en logiciels, micro-ordinateurs, équipements de laboratoire de maintenance et de matériels didactiques ;
- la réactualisation des programmes de formation assortie du renouvellement du fonds de la bibliothèque ;
- l'appui à la formation des formateurs ;
- l'affectation à l'Ecole d'Assistants techniques français.

De 2000 à 2004, l'ENI avait fait partie des membres du bureau de la Conférence Internationale des Ecoles de formation d'Ingénieurs et Technicien d'Expression Française (CITEF).

Les Enseignants-Chercheurs de l'Ecole participent régulièrement aux activités organisées dans le cadre du Colloque Africain sur la Recherche en Informatique (CARI)

L'ENI avait également signé un accord de coopération interuniversitaire avec l'Institut de Recherche en Mathématiques et Informatique Appliquées (IREMIA) de l'Université de la Réunion, l'Université de Rennes 1, l'INSA de Rennes, l'Institut National Polytechnique de Grenoble (INPG).

A partir du mois de Juillet 2001, l'ENI avait abrité le Centre de Réseau Opérationnel (Network Operating Center) du point d'accès à Internet de l'Ecole ainsi que de l'Université de Fianarantsoa. Grâce à ce projet américain qui a été financé par l'USAID Madagascar, l'ENI de l'Université de Fianarantsoa avait été dotées d'une ligne spécialisée d'accès permanent au réseau Internet.

L'ENI avait de même noué des relations de coopération avec l'Institut de Recherche pour le Développement (IRD).

L'objet du projet de coopération avait porté sur la modélisation environnementale du Corridor forestier de Fandriana jusqu'à Vondrozo (COFAV). Dans ce cadre, un atelier scientifique international avait été organisé à l'ENI en Septembre 2008. Cet atelier scientifique avait eu pour thème de modélisation des paysages.

Et dans le cadre du programme scientifique PARRUR, l'IRD avait financé depuis 2010 le projet intitulé « Forêts, Parcs et Pauvreté dans le Sud de Madagascar (FPPSM). Des étudiants en DEA et des Doctorants issus de l'ENI avaient participé à ce Programme.

Par ailleurs, depuis toujours la même année 2010, l'ENI de Fianarantsoa avait été sélectionnée pour faire partie des organismes partenaires de l'Université de Savoie dans le cadre du projet TICEVAL relatif à la certification des compétences en TIC ;

Le projet TICEVAL avait été financé par le Fonds Francophone des Inforoutes pour la période allant de 2010 à 2012, et il avait eu pour objectif de généraliser la certification des compétences en Informatique et Internet du type C2i2e et C2imi.

Dans le cadre du projet TICEVAL, une convention de coopération avec l'Université de Savoie avait été signée par les deux parties concernées. La mise en œuvre de la Convention de 13 Coopération avait permis d'envoyer des étudiants de l'ENI à Chambéry pour poursuivre des études supérieures en Informatique.

Enfin et non des moindres, l'ENI avait signé en Septembre 2009 un protocole de collaboration scientifique avec l'ESIROI – STIM de l'Université de la Réunion.

Comme l'ENI constitue une pépinière incubatrice de technologie de pointe, d'emplois et d'entreprises, elle peut très bien servir d'instrument efficace pour renforcer la croissance économique du pays, et pour lutter contre la Pauvreté.

De même que le statut de l'Ecole devrait permettre de renforcer la position concurrentielle de la Grande Ile sur l'orbite de la modélisation grâce au développement des nouvelles technologies.

1.8. Débouchés professionnels des diplômés

Le chômage des jeunes diplômés universitaires fait partie des maux qui gangrènent Madagascar. L'environnement socio-politique du pays depuis 2008 jusqu'à ce jour a fait que le chômage des diplômés est devenu massif par rapport aux établissements de formation supérieure existants.

Cependant, les formations proposées par l'Ecole permettent aux diplômés d'être immédiatement opérationnels sur le marché du travail avec la connaissance d'un métier complet lié à l'informatique aux TIC.

L'Ecole apporte à ses étudiants un savoir-faire et un savoir-être qui les accompagnent tout au long de leur vie professionnelle. Elle a une vocation professionnalisante.

Les diplômés en LICENCE et en MASTER issus de l'ENI peuvent faire carrière dans différents secteurs.

L'Ecole bénéficie aujourd'hui de 38 années d'expériences pédagogiques et de reconnaissance auprès des sociétés, des entreprises et des organismes. C'est une Ecole Supérieure de référence en matière informatique.

Par conséquent, en raison de fait que l'équipe pédagogique de l'Ecole est expérimentée, les enseignants-chercheurs et les autres formateurs de l'Ecole sont dotés d'une grande expérience dans l'enseignement et dans le milieu professionnel.

L'Ecole est fière de collaborer de façon régulière avec un nombre croissant d'entreprises, de sociétés et d'organismes publics et privés à travers les stages des étudiants. Les formations dispensées à l'Ecole sont ainsi orientées vers le besoin et les attentes des entreprises et des sociétés.

L'Ecole fournit à ses étudiants de niveau LICENCE et MASTER des compétences professionnelles et métiers indispensables pour les intégrer sur le marché du travail.

L'Ecole s'efforce de proposer à ses étudiants une double compétence à la fois technologique et managériale combinant l'informatique de gestion ainsi que l'administration des réseaux et systèmes.

Tableau 4 Débouchés professionnels éventuels des diplômés

LICENCE	<ul style="list-style-type: none">- Analyste- Programmeur- Administrateur de Site Web/ de portail Web- Assistant Informatique et Internet- Chef de projet Web ou MultiMedia- Développeur Informatique ou MultiMedia- Intégrateur Web ou Web Designer- Hot Liner/ Hébergeur Internet- Agent de référencement- Technicien/Supérieur de help desk sur Informatique- Responsable de sécurité web- Administrateur de réseau- Administrateur de cybercafé
---------	---

MASTER	<ul style="list-style-type: none"> - Administrateur de cyber café - Administrateur de réseau et système - Architecture de système d'information - Développeur d'application /web /java/Python/ IOS /Android - Ingénieur réseau - Webmaster /web designer - Concepteur Réalisateur d'applications - Directeur du système de formation - Directeur de projet informatique - Chef de projet informatique - Responsable de sécurité informatique - Consultant fonctionnel ou freelance
--------	--

1.9. Ressources humaines

Les ressources humaines affectées à l'Ecole Nationale d'Informatique sont composées de :

- Directeur de l'Ecole : Professeur RAMAMONJISOA Bertin Olivier
- Responsable de Mention : Monsieur RABETAFIKA Louis Haja
- Responsable de Parcours « Génie Logiciel et Base de Données » : Monsieur RALAIVAO Jean Christian
- Responsable de Parcours « Administration Systèmes et Réseaux » : Monsieur SIKA
- Responsable de Parcours « Informatique Générale » : Monsieur GILANTE Gesazafy
- Nombre d'Enseignants permanents : 12 dont un (01) Professeur Titulaire, un (01) Professeur, Cinq (05) Maîtres de Conférences et cinq (05) Assistants d'Enseignement Supérieur et de Recherche.
- Nombre d'Enseignants vacataires : 10
- Personnel Administratif : 23

Chapitre II : Présentation d'UDITEC

2.1 Présentation générale

UDITEC est une entreprise qui a connu ses débuts en septembre 2011. Elle siège à Akorondrano, rue Ravoninahitriniarivo à Antananarivo.

Téléphone : (+261) 20 22 217 83

2.2 Activité Principale

a) UDITEC

UDITEC se situe dans le secteur tertiaire, plus précisément dans la vente de Meubles, Electroménager, Téléphonie et MultiMedia, et cela par le biais de ses magasins officiels « COSMOS Madagascar ». Il s'engage sur de meilleurs services, le plus large choix et les offres les plus attrayants s'inscrivant sur une politique de proximité envers ses clients. Il se différencie dans son domaine par :

- Plus grand choix de produits
- Large réseau commercial
- Livraison et installation gratuite
- Services Apres Vente 100 % garanti
- Des conseils à l'achat, à l'installation et à l'utilisation
- Facilite de paiement

b) UMATEC

UMATEC est une branche du réseau d'UDITEC qui se centre sur la gestion des Ressources Humaines de l'entreprise. En tant que tel, ils s'organisent dans :

- L'administration du personnel :
 - L'enregistrement des données individuelles mais aussi collectives du personnel
 - Préparations des commissions et des réunions
 - Le maintien de l'ordre et contrôle de pointage
- La communication tel que :
 - La gestion des moyens de communication
 - La définition des publications orientées vers l'extérieur
- L'amélioration des conditions de travail

- L'hygiène et la sécurité au travail
- La prévention des risques psychosociaux et les maladies professionnelles
- La qualité de travail

2.3 Objectif

L'objectif principal de l'entreprise est d'entendre son influence sur toutes l'île en mettant toujours en avant les besoins de ses clients. Dans leur conquête de l'expansion du marché, ils visent à augmenter leurs chiffres d'affaires mais également inciter les marchés à se centrer sur leurs services.

2.4 Organigramme d'UDITEC

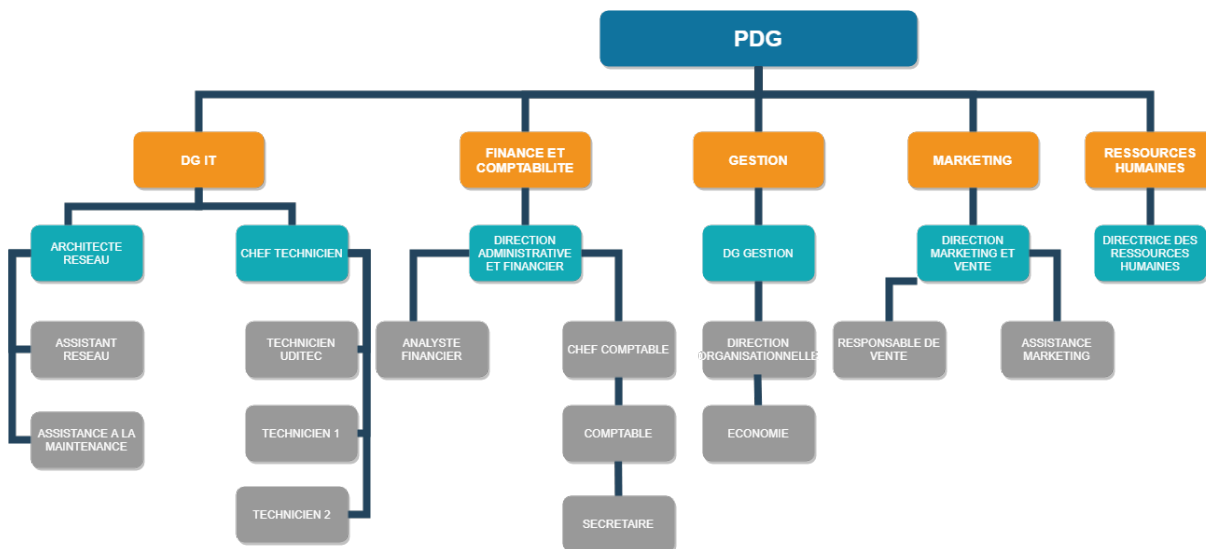


Figure 2 : Organigramme d'UDITEC

2.5 Réseau de vente

Compte tenu de son objectif pour mieux se rapprocher des Réseaux cibles de la clientèle dans les différentes régions de l'île, l'entreprise a mis en place des Unités de Production qui assurent la vente de ses produits. Elles se présentent sous la forme de ses magasins officielles dispersée à travers l'île.

Elles se localisent principalement :

- Antananarivo Analamanga :
 - Cosmos Zoom Ankorondrano
 - Avenue Fashion Zoom Ankorondrano
 - Cosmos Andranomena
 - Avenue Fashion Andranomena
 - Cosmos UCODIS
 - Avenue Fashion Analakely

- Cosmos Behoririka
- Antsirabe Vakinakaratra
- Cosmos Antsenakely
- Cosmos Toamasina
- Cosmos Diego Suarez
- Fianarantsoa
- Cosmos Ampasambazaha

2.6 Partenaires

L'entreprise UDITEC travaille personnellement avec la marque Samsung. On peut dire que c'est le représentant légal et agréé de Samsung à Madagascar. Outre ce grand producteur de marque, il y a également :

- ASUS
- LG
- Huawei
- TCL

Chapitre III : Description du projet

3.1 Descriptifs

UDITEC est une des entreprises avec le plus gros réseau de vente à travers toute l'île. Il s'est engagée à optimiser ses processus internes pour accroître l'efficacité et faciliter le quotidien de ses collaborateurs. Consciente des défis auxquels sont confrontés les employés, UDITEC a entrepris un projet ambitieux visant à simplifier les tâches administratives, réduire les erreurs potentielles et offrir un environnement professionnel propice à l'épanouissement.

3.2 Chronogramme de travaux

La réalisation du projet a été repartie suivant le tableau suivant :

Activités	Mai		Juin				Juillet	
	Semaine 3	Semaine 4	Semaine 1	Semaine 2	Semaine 3	Semaine 4	Semaine 1	Semaine 2
Intégration à la société et analyse de l'existant								
Recherche et proposition de solution								
Réalisation du projet								
Test et mise en								

place du projet								
-----------------	--	--	--	--	--	--	--	--

Tableau 5 : Chronogramme de travaux

3.3 Moyens nécessaires à la réalisation du projet

3.3.1 Moyens humains

- Encadreur Pédagogique :
- Encadreur professionnel : Monsieur RANDRIAMPARAMANIRAKA Lovasoa

Monsieur Ny MPANALINA Raneria

- Un stagiaire administrateur système et réseau

3.3.2 Moyens logiciels

Pour la réalisation de ce projet, il n'a pas été nécessaire d'utiliser de plusieurs logiciels. L'on a opté pour l'utilisation de Cisco Packet tracer 7.3.0 pour les tests de simulations réseaux.

3.3.2 Moyens Matériels

Divers moyens matériels ont été mis à disposition pour la réalisation du projet.

Désignation	Caractéristiques	Système d'exploitation	Nombres
HP EliteBook	CPU : Core i7 2.1GHz RAM : 4GB HDD : 160GB	Windows	01
NEC	CPU : Core i3 2.4GHz RAM : 4GB HDD : 500GB	Windows	01

Tableau 6 : Liste des moyens matériels

3.4 Objectifs

Les objectifs étant de

- Faciliter les tâches des architectes réseaux grâce à la centralisation d'identification et l'authentification du réseau.
- De permettre une mise à jour en temps réels des informations à la disposition des utilisateurs.

3.5 Résultats attendus

Au terme de ce stage, la société attend de pouvoir :

- Obtenir les détails concernant les postes clients du parc informatique.
- D'avoir les données centraliser et accessible par authentification
- Faciliter la gestion de résolution des problèmes.

PARTIE II :

ANALYSES

CHAPITRE IV : ANALYSE DE L'EXISTANT

4.1 Topologie du réseau d'UDITEC

Comme tout institut ou groupe existant, UDITEC utilise le modèle réseau en étoile qui facilite la communication des différents équipements réseau.

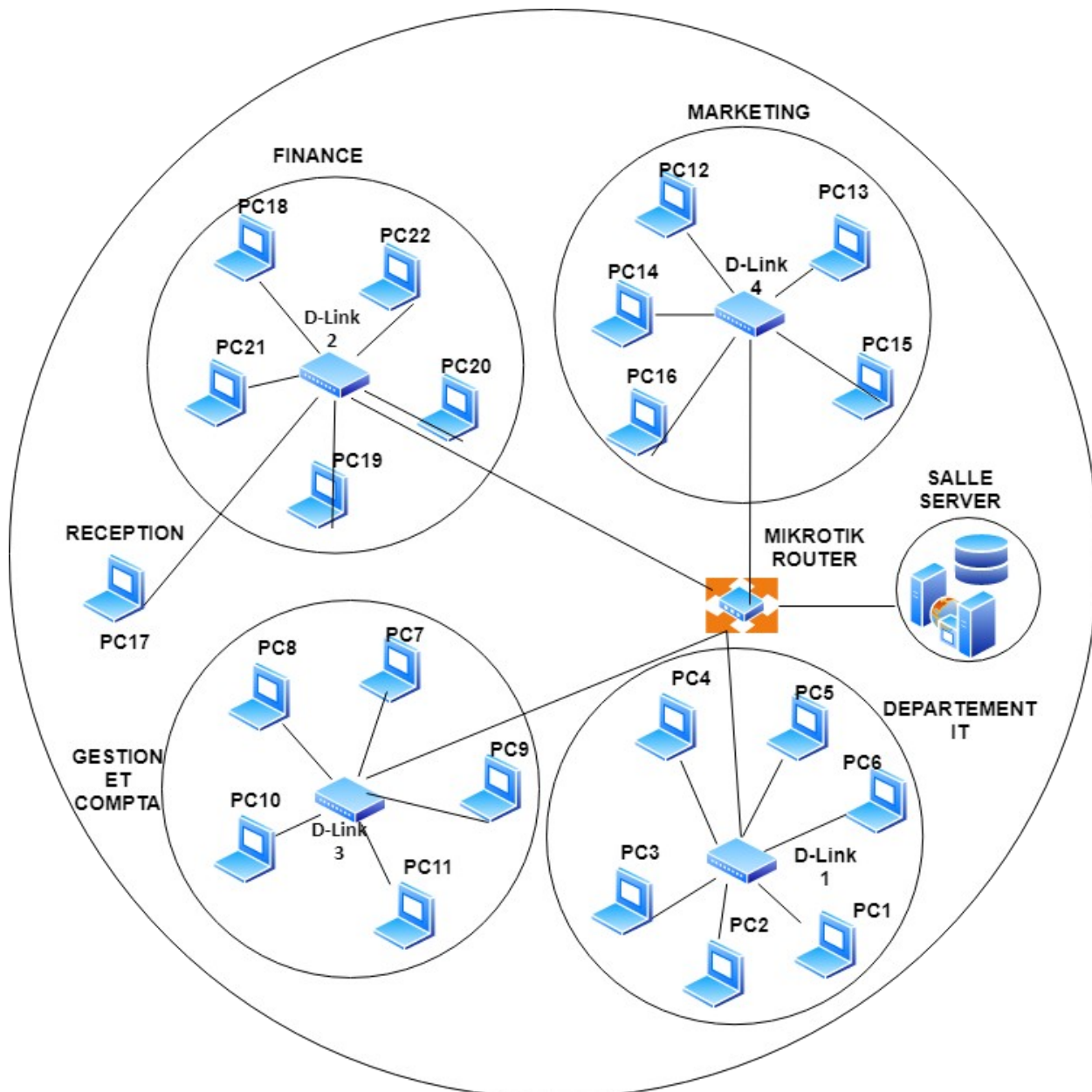


Figure 3 : topologie réseau du bâtiment d'UDITEC

4.2 types de réseau

Il existe plusieurs types de réseaux aux sein d'UDITEC récapituler dans le tableau suivant :

Types	Vitesse	Authentification
LAN	250Mb/s	Active Directory
WAN	4Mb/s	Active Directory
WLAN	25Mb/s	Active Directory

Tableau 7 : Types de réseau de UDITEC

Rôles :

- Le réseau LAN interconnecte les composants informatiques de l'entreprise pour le partage des ressources, des données et des programmes ainsi que l'information de messagerie.
- Le réseau WAN donne à certains utilisateurs un accès à des informations externes de l'entreprise ou dans l'internet.
- Le réseau WLAN appelé également Wi-Fi est le réseau sans fil qui permet aux utilisateurs de se connecter à internet à l'aide de communication sans fil.

4.3 Equipements d'interconnexions

Il existe plusieurs équipements d'interconnexions au sein de l'entreprise dans le tableau qui suit :

Désignation	Caractéristiques	Emplacements
Switch	D-Link DGS-1024D	A chaque étage et la salle serveur
Routeur Telma	Mikrotik BOARD 1200	Salle serveur et sur chaque sites
Firewall	pfSense	Salle seveur

Tableau 8 : Les différents équipements d'interconnexion

Rôles :

- Le Switch « D- Link DGS-1024D » relie tous les segments du réseau d'UDITEC et également au niveau de ses sites.
- « Le Mikrotik Board » sert à interconnecter les sites entre elles à travers toutes îles de Madagascar.
Par exemple UDITEC et CMZ
- Le firewall « pfSense » est un système de protection des ordinateurs ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers notamment Internet.

4.4 Postes de travaux

Il existe environ 200 machines utilisateurs Windows actives chez UDITEC dont on nommera quelques-unes.

Désignation	Caractéristiques	Système d'exploitation	Authentification
PC_IT	CPU : Intel Core i5 4.2GHz RAM : 8GB HDD : 1TB CPU : Intel Core i5 2.7GHz RAM : 4GB HDD : 500GB	Windows 10	Authentification de l'ordinateur et utilisation de l'annuaire Active Directory
PC_COMPTA	CPU : Intel Core i3 2.6GHz RAM : 4GB HDD : 1TB	Windows 10	Authentification de l'ordinateur et utilisation de l'annuaire Active Directory

PC_Marketing	CPU : Intel Core i5 3GHz RAM : 4GB HDD : 1TB	Windows 10	Authentification de l'ordinateur et utilisation de l'annuaire Active Directory
--------------	---	------------	--

Tableau 9 : exemples de poste de travail

4.5 Serveurs

Il existe plusieurs serveurs au sein de l'entreprise avec chacun d'eux leurs usages et leur rôles respectifs.

Désignation	Caractéristiques	Système	Usage
Serveur_1	CPU : E-2226GE 4.6GHz RAM : 16GB HDD: 6000TB	Windows Server	Serveur marché International
Serveur_2	CPU : E5-2274G RAM : 12GB HDD: 2400TB	Windows Server	Serveur UDITEC
Serveur_3	CPU : D-1649N, 3.00GHz RAM : 16GB HDD: 200TB	Windows Server	Serveur Cosmos
Serveur_4	CPU : W-1350, 5.00GHz RAM : 16GB HDD: 10TB	Windows Server	Serveur Avenue Fashion
Serveur_5	CPU : D-2166NT RAM : 16GB HDD: 4TB	Windows Server	Serveur test (exemple: test d'applications)

Tableau 10 : les différents serveurs

4.6 Disponibilités

Les serveurs d'UDITEC tournent 24h/24, 7j/7 pour assurer une accessibilité et une disponibilité des applications et des informations ou document utiles aux utilisateurs à tout moment. En cas de panne, la solution architecte font le nécessaire pour résoudre le problème pour qu'il y ait le moins d'impact possible sur la productivité. Le firewall, quant à lui, filtre le Trafic réseau pour ne laisser passer que les requêtes https.

4.7 Surveillance

La société utilise divers outils de supervision tels que Zabbix, Nagios. Leur mise en place est nécessaire afin de détecter les problèmes de performance liés à la saturation des ressources, ainsi que les diverses pannes.

CHAPITRE V : CRITIQUE DE L'EXISTANT

5.1 Critique de l'existant

A défaut de moyens matériels et logiciels nécessaires, les administrateurs réseaux et systèmes doivent se déplacer pour faire des inventaires et vérifier les informations des matériels et logiciels du parc informatique. Dans bien de cas, un responsable réseau est appelé à se rendre sur plusieurs sites pour différents réglages, ce qui paraît ardu.

Dans le cas de UDITEC, qui est un réseau qui s'étend à l'échelle Nationale, il est très difficile de le gérer dans ses conditions

5.2 Solution proposée

La solution proposée a été l'utilisation de l'annuaire Active Directory pour :

- Pour faciliter les interventions des responsables réseaux sur chaque site
- Faciliter la maintenance par assistances à distances des utilisateurs
- Administrer et authentifier les utilisateurs du domaine de la forêt.

PARTIE III :

REALISATIONS

Chapitre VI : CHOIX DES OUTILS

6.1 Windows Server

Le serveur est considéré comme le centre d'un réseau. C'est le cerveau du réseau.

Il existe 3 types de serveurs :

- **Serveur de fichier** : S'occupe de la gestion des fichiers. Il faut pour cela un très bon sous-système disque (contrôleur et disques), au moins 32 MB de RAM et une carte réseau très performante.
- **Serveur d'application** : Il contient les applications que les utilisateurs du réseau peuvent utiliser. Tous les traitements des logiciels se font sur le serveur donc la rapidité du m P et la quantité de RAM (au moins 64MB) sont primordiaux.
- **Serveur d'impression** : C'est lui qui gère les queues d'impression. Ce type de serveur est souvent couplé avec un serveur de fichiers ou un serveur d'applications car il ne demande pas un sous-système très performant.

« Windows server » est le système d'exploitation côté serveur de Microsoft. L'objectif est de fournir des services à de nombreux autres équipements. Notre choix s'est portée sur « Windows 2016 Server » [5].

Il existe trois éditions de Windows avec des cibles différentes :

- **Windows 2016 Server Essentials**

Cette édition se destine aux petites entreprises et organisations jusqu'à 25 utilisateurs et 50 équipements. Elle permet de faire fonctionner à moindre coût tous les services.

- **Windows 2016 Server Datacenter**

C'est une édition haute de gamme. On peut créer autant de machines virtuelles désirées. Elle se destine aux entités ayant de forts besoins de virtualisation, pour la mise en œuvre de centres de données gérés logiciellement.

- **Windows 2016 Server Standard Edition**

Elle est destinée à toute entité n'ayant pas de forts besoins de virtualisation.

6.2 Active Directory

6.2.1 Généralité

Active Directory est un annuaire d'entreprise qui existe depuis 1996 et est utilisable depuis Windows 2000 Server Edition sorti en 1999. Cet annuaire d'entreprise vient en remplacement des bases SAM (Security Account Manager) qui étaient exploitées avec NT4 et les groupes de travail.

Ces bases présentaient notamment des limitations d'administration. L'arrivée d'Active Directory a permis de passer des groupes de travail aux domaines Active Directory et ainsi de centraliser toute l'administration et la gestion des droits dans un annuaire de type LDAP. Tout logiciel utilisant LDAP sera capable de communiquer avec Active Directory : on peut, par exemple, gérer (partiellement) des postes Linux à partir d'un Active Directory. [6]

6.2.2 Description d'un service annuaire

Un service d'annuaire est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder. Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur.

a) Active Directory

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

La sécurité est intégrée dans Active Directory à travers l'authentification de l'ouverture de session et le contrôle d'accès aux objets de l'annuaire. Avec une connexion réseau unique les administrateurs réseau peuvent gérer les données et l'organisation de l'annuaire à travers leur réseau, et les utilisateurs autorisés

peuvent accéder aux ressources n'importe où sur le réseau. Une administration basée sur des stratégies facilite la gestion même du plus complexe des réseaux.

b) Protocole LDAP (Lightweight Directory Access Protocol)

LDAP est un protocole permettant l'interrogation et la modification des services d'annuaire. Les annuaires LDAP suivent le modèle X.500 et son architecture nativement multi-tenant :

- Un annuaire en arbre d'entrées
- Une entrée constituée d'un ensemble d'attributs
- Un attribut possède un nom, un type et un ou plusieurs values
- Les attributs sont définis dans des schémas

LDAP fournit aux utilisateurs des méthodes lui permettant :

- Se connecter
- Se déconnecter
- Rechercher des informations
- Comparer des informations
- Insérer des entrées
- Les modifier ou les supprimer

D'autre part, il propose des mécanismes de chiffrement et d'authentification (SASL) permettant de sécuriser l'accès aux informations stockées dans la base.

Les ordinateurs clients utilisent le protocole LDAP notamment, pour rechercher et modifier des objets dans une base de données Active Directory. Il utilise les informations portant sur la structure d'un annuaire pour trouver des objets individuels possédant chacun un nom unique.

Le protocole LDAP utilise un nom représentant un objet Active Directory par une série de composants concernant la structure logique. Cette représentation, appelée nom unique de l'objet, identifie le domaine dans lequel se trouve l'objet ainsi que le chemin complet permettant d'accéder à celui-ci. Un nom de ce type ne peut être qu'unique dans une forêt Active Directory.

Le nom unique relatif d'un objet identifie l'objet de manière unique dans son conteneur. Deux objets situés dans un même conteneur ne peuvent porter le même nom. Le nom unique relatif est toujours le premier composant du nom unique, mais il n'est pas toujours un nom usuel.

6.2.3 Structure logique d'active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans sa structure logique hiérarchique. Les objets Active Directory représentent des utilisateurs et des ressources, tels que des ordinateurs et des imprimantes. Certains objets en contiennent d'autres. [3]

La structure logique d'Active Directory inclut les composants suivants :

- **Les objets**

Il s'agit des composants les plus élémentaires de la structure logique. Chaque objet est une entité unique utilisateur, ordinateur, imprimante ou groupe ainsi que ses attributs. Un objet est identifié de manière unique dans Active Directory par son nom et possède son propre jeu d'attributs.



Figure 4 : Les objets d'Active Directory

- **Unité Organisationnelle (OU : Organizational Unit)**

Elle est un objet conteneur utilisé pour hiérarchiser Active Directory. On utilise ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte nos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. On peut également déléguer l'autorité de gestion d'une unité d'organisation. Les unités d'organisation peuvent être imbriquées les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.

- **Domaines**

Ils constituent les feuilles de l'arborescences. Les domaines sont un ensemble d'objets définis administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et des relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :

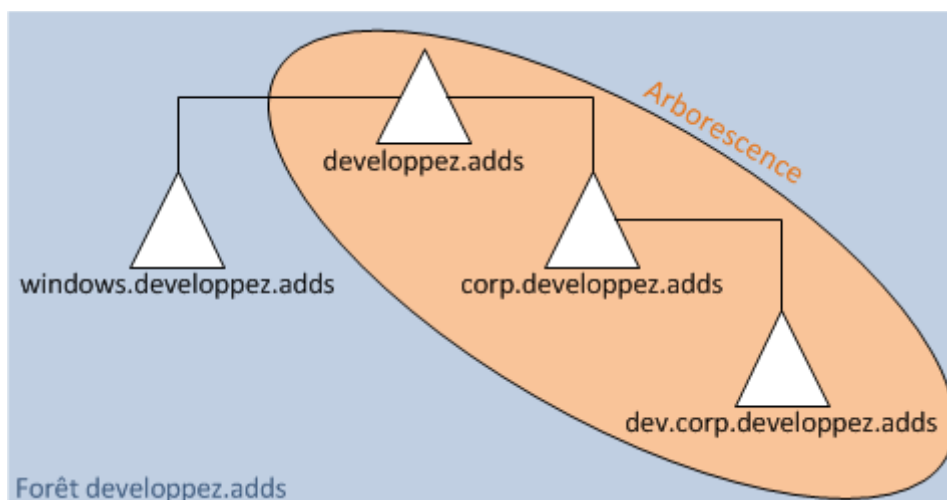
- Une limite d'administration pour objets
- Une méthode de gestion de la sécurité pour les ressources partagées
- Une unité de réplication pour les objets

• Les arborescences

Les domaines regroupés en structures hiérarchiques sont appelés arborescences de domaines. Lorsqu'on ajoute un second domaine à une arborescence, il devient enfant du domaine racine de l'arborescence. Le domaine auquel un domaine enfant est attaché et appelé domaine parent. Un domaine enfant peut à son tour avoir son propre domaine enfant. Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique. De cette manière, une arborescence a un espace de noms contigu.

• La Forêt

Elle est une structure hiérarchique d'un ou plusieurs domaines indépendants. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë. Le premier domaine de la forêt est appelé le domaine racine de la forêt. Le nom de ce domaine fait référence à la forêt. Par défaut, les informations dans Active Directory ne sont partagées qu'à l'intérieur de la forêt. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.



6.2.4 Structure physique d'active Directory

Contrairement à la structure logique, qui modélise des exigences administratives, la structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de répliquions. Pour optimiser l'utilisation par Active Directory de la bande passante du réseau, on doit en comprendre la structure physique. Les éléments de la structure physique d'Active Directory sont :

- **Les contrôleurs de domaine**

Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs des réseaux informatiques. Chaque contrôleur de domaine exécute des fonctions de stockage et de répliquion. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleurs de domaine.

- **Les sites AD**

Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsqu'on crée des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de latence de répliquion à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. On peut donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaines situés à des emplacements différents. Dans Active Directory, les sites facilitent la définition de la structure physique d'un réseau. Un ensemble de plages d'adresses de sous-réseaux TCP/IP définissent un site, qui à son tour définit un groupe de contrôleurs de domaine partageant les mêmes débits et coûts. Les sites sont composés d'objets serveurs, qui contiennent eux-mêmes les objets de connexion autorisant la répliquion.

6.2.5 Les services d'Active Directory

Au fil du temps, Microsoft a enrichi l'offre Active Directory de plusieurs services.

- **Active Directory Domain Services (AD DS) ou Service de Domaine**
Stocke les données et gère les communications entre utilisateurs et le contrôleur de domaine.
- **Active Directory Lightweight Domain Services (AD LDS)**

Une version allégée qui fait impasse sur certaines des fonctionnalités avancées qui compliquent l'usage de Domain Services pour intégrer les fonctions d'annuaire les plus rudimentaires, sans recours aux forêts ou aux domaines. C'est une version destinée aux réseaux de petite taille

- Active Directory Certificate Services (AD CS)

Le service de certificat permet à un contrôleur de domaine de servir des certificats et des signatures numériques, ainsi qu'un chiffrement à clé publique.

- Active Directory Federation Services (AD FS)

C'est un service Web d'authentification et d'autorisation unique (SSO) qui s'adresse en premier lieu aux entreprises. Un prestataire peut se connecter à son propre réseau et être habilité à accéder à celui de son client également

- Active Directory Rights Management Services (AD RMS)

Le service de gestion de droits contrôle les politiques en matière de droits à l'information et d'accès aux données. Les droits et restrictions sont associés aux documents plutôt qu'à l'utilisateur.

6.2.6 Catalogue Global

Le catalogue global est un annuaire central construit automatiquement sur la base de copies partielles des informations provenant de différents annuaires réseaux.

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparente pour l'utilisateur. Par exemple, si on recherche toutes les imprimantes présentes dans une forêt, un serveur de catalogue global traite la requête dans le catalogue global, puis renvoie les résultats. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Le catalogue global permet aux utilisateurs d'effectuer deux tâches importantes :

- Trouver les informations Active Directory en tout point de la forêt, indépendamment de l'emplacement des données ;
- Utiliser les informations d'appartenance au groupe universel pour se connecter au réseau.

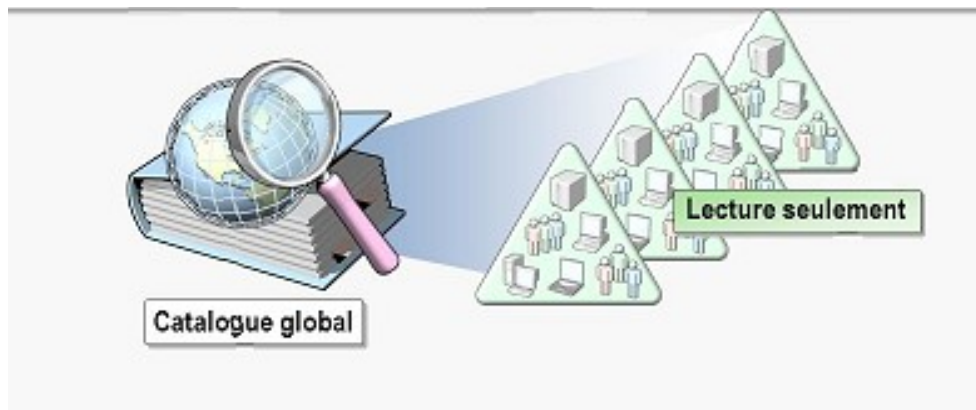


Figure 6 : Catalogue Global

Les membres du groupe Administrateurs du schéma peuvent modifier les attributs stockés dans le catalogue global, en fonction des impératifs d'une organisation.

Un serveur de catalogue global est un contrôleur de domaine qui traite efficacement les requêtes intraforêts dans le catalogue global. Le premier contrôleur de domaine qu'on crée dans Active Directory devient automatiquement un serveur de catalogue global. On peut configurer des serveurs de catalogue global supplémentaires pour équilibrer le trafic lié aux authentications de connexion et aux requêtes.

6.2.7 Domain Name System (DNS)

Active Directory contient des informations relatives à la localisation des objets stockés dans la base de données, mais il s'appuie sur le système DNS pour localiser les contrôleurs de domaine.

Le « Domain Name System » est le service informatique distribué utilisé pour traduire les noms de domaine internet en IP. On associe donc une adresse logique à une adresse physique. Le DNS permet à un message d'atteindre le destinataire et nom quelque'un d'autre avec un nom de domaine similaire. Il permet également d'entrer une adresse Web sans passer par une longue saisie d'adresse IP et accéder au site

Pour ces opérations, ce sont principalement deux types de serveurs qui sont utilisés :

- Serveur faisant autorité : Serveur DNS qui connaît le contenu d'un domaine
- Serveur récursif : Serveur DNS qui ne connaît pas le contenu d'un domaine mais pose des questions aux serveurs faisant autorité et mémorise les réponses.

Au sein de l'annuaire actif, tous les domaines ont un nom de domaine DNS et chaque ordinateur raccorde à un nom DNS au sein du même domaine.

6.2.8 DHCP (Dynamic Host Configuration Protocol)

DHCP est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant une adresse et un masque de sous-réseau. [1]

Il peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS, des serveurs de noms NBNS.

Cela permet de faciliter la tâche des administrateurs réseau qui autrefois devaient allouer statiquement des adresses aux machines.

6.2.9 Les types de comptes Active Directory

On peut créer trois types de comptes dans Active Directory : comptes d'utilisateurs, de groupes et d'ordinateurs. Les comptes d'utilisateurs et d'ordinateurs Active Directory représentent une entité physique, telle qu'un ordinateur ou une personne. On peut également utiliser les comptes d'utilisateurs comme comptes de services dédiés pour certaines applications.

a) Compte utilisateur

Un compte d'utilisateur est un objet stocké dans Active Directory qui permet une ouverture de session unique, autrement dit un utilisateur entre son mot de passe une seule fois lors de l'ouverture de session sur une station de travail pour obtenir un accès authentifié aux ressources réseau.

Il existe trois types de comptes d'utilisateurs, chacun ayant une fonction spécifique :

- Un compte d'utilisateur local : permet à un utilisateur d'ouvrir une session sur un ordinateur spécifique pour accéder aux ressources sur cet ordinateur.
- Un compte d'utilisateur de domaine : permet à un utilisateur de se connecter au domaine pour accéder aux ressources réseau, ou à un ordinateur individuel pour accéder aux ressources sur cet ordinateur.
- Un compte d'utilisateur intégré : permet à un utilisateur d'effectuer des tâches d'administration ou d'accéder temporairement aux ressources réseau.

b) Compte Ordinateur

À l'image des comptes d'utilisateurs, les comptes d'ordinateurs permettent d'authentifier et d'auditer l'accès d'un ordinateur aux ressources réseau et du domaine. Chaque compte d'ordinateur doit être unique.

c) Compte de groupes

C'est un ensemble d'utilisateurs, d'ordinateurs ou de groupes. On peut utiliser des groupes pour gérer efficacement l'accès aux ressources du domaine, et ainsi simplifier l'administration. Lorsqu'on utilise des groupes, on affecte en une fois des autorisations pour des ressources partagées, telles que des dossiers et des imprimantes, à des utilisateurs individuels.

Dans Active Directory, il existe deux types de groupes : les groupes de distribution et les groupes de sécurité. Tous deux possèdent un attribut d'étendue, qui détermine qui peut être membre du groupe et à quel endroit on peut utiliser ce groupe dans un réseau. On peut convertir à tout moment un groupe de sécurité en un groupe de distribution et inversement, mais uniquement si le niveau fonctionnel de domaine est défini sur Windows 2000 natif ou ultérieur.

i. Groupe de distribution

Ce groupe est plus utilisé par les applications de messageries, comme Microsoft Exchange, pour envoyer des messages à un ensemble d'utilisateurs. La sécurité n'est pas activée sur les groupes de distribution, ce qui signifie qu'ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire (DACL, Discretionary Access Control List).

ii. Groupe de Sécurité

Les groupes de sécurité sont les plus utilisés et manipulés plus souvent. Ils permettent d'utiliser les groupes pour gérer les droits et les autorisations d'accès aux ressources. Les droits déterminent les fonctions que les membres d'un groupe de sécurité peuvent effectuer dans un domaine ou une forêt. Les autorisations déterminent quelles ressources sont accessibles à un membre d'un groupe sur le réseau. Une méthode d'utilisation efficace des groupes de sécurité consiste à utiliser l'imbrication, c'est à dire, ajouter un groupe à un autre groupe. Le groupe imbriqué hérite des autorisations du groupe dont il est membre, ce qui simplifie l'affectation en une fois des autorisations à plusieurs groupes, et réduit le trafic que peut engendrer la réplication de l'appartenance à un groupe. Dans un domaine en mode mixte, on ne peut pas imbriquer des groupes possédant la même étendue de groupe.

Les groupes de distribution et de sécurité prennent en charge l'une des trois étendues de groupe suivantes : locale de domaine, globale ou universelle. Le niveau fonctionnel de domaine détermine le type de groupe qu'on peut créer.

6.2.10 Les stratégies de Groupes (GPO : Group Policy Object)

a) Définition

Une stratégie de groupe est un ensemble d'outils intégrés à « Windows Server » qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques.

Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou à des utilisateurs. Elles sont appliquées au démarrage de l'ordinateur et pendant l'ouverture d'une session de l'utilisateur. Les ordinateurs rafraichissent, de façon périodique, les paramètres transmis par les GPO, toutes les heures ou les deux heures.

Grâces aux stratégies de groupe, il est possible d'avoir une configuration homogène entre les différentes machines du parc informatique, mais aussi au niveau de l'environnement utilisateur. En effet, une stratégie de groupe peut servir à appliquer des paramètres sur Windows en lui-même, mais aussi à l'utilisateur directement, ou les deux.

Il est possible de forcer la mise à jour du GPO avec la commande « gpupdate /force ».

b) Les phases d'utilisation des GPO

Les stratégies de groupe peuvent être considérées en trois phase distinctes qui sont :

- Création et édition des stratégies de groupe

Les stratégies peuvent être éditées au travers de la Group Policy Management Console « gpmmc.msc ». Elle simplifie la gestion de stratégie de groupe en fournissant un outil permettant une gestion centralisée et collective des objets. Elle inclut de nombreuses fonctionnalités telles que la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration.

- Liaison des stratégies de groupe

Après avoir créé une stratégie de groupe, elle peut être liée à un site AD, à un domaine ou à une unité d'organisation.

- Applications des stratégies de groupe

Le client de la stratégie de groupe du poste récupère la configuration qui est applicable à l'ordinateur et à l'utilisateur connecté et l'applique en tenant compte des différents critères de filtres, de sécurité et d'héritage.

c) Différents choix de stratégies

1) Types de GPO

Il existe deux types de GPO :

- ✓ Les GPO **Utilisateur** : les règles de ces GPO vont être appliquées dès l'identification de l'utilisateur à l'ouverture de sa session, et nécessite dans certains cas, selon les opérations effectuées, d'être administrateur de leur machine.
- ✓ Les GPO **Ordinateur** : ces GPO vont s'appliquer au moment du démarrage de la machine et ne nécessite aucune authentification administrateur.

2) Les types de déploiement

On peut définir une GPO avec deux types de déploiement :

- ✓ Elles peuvent être **Publiées** : dans ce cas, l'installation du programme ne se fera pas automatiquement mais sera directement disponible dans les programmes et fonctionnalités du panneau de configuration.
- ✓ Elles peuvent être **Attribuées** : les programmes seront installés automatiquement, sans que l'utilisateur le lance manuellement.
- ✓ On peut également définir un type de déploiement avancé.

6.2.11 Réplication d'Active Directory

a. Généralité

La réplication est la méthode de transfert et de mise à jour d'objets Active Directory d'un contrôleur de domaine à un autre. Les connexions entre contrôleurs de domaine sont établies en fonction de leur emplacement dans une forêt ou un site. Le service de réplication garantit que tous les contrôleurs de domaine du réseau partagent le même catalogue et le même schéma.

Active Directory utilise plusieurs contrôleurs de domaine à diverses finalités, notamment pour la répartition des charges ou la tolérance aux pannes. Pour s'assurer ces fonctions, tous les contrôleurs de domaine doivent posséder une copie complète de la base de données AD du domaine lui-même. La réplication garantit que chaque contrôleur possède une copie actuelle de la base de données.

La réplication de confine aux frontières du domaine. Deux contrôleurs rattachés à des domaines différents ne répliquent pas les données de l'autre, même s'ils appartiennent à la même forêt.

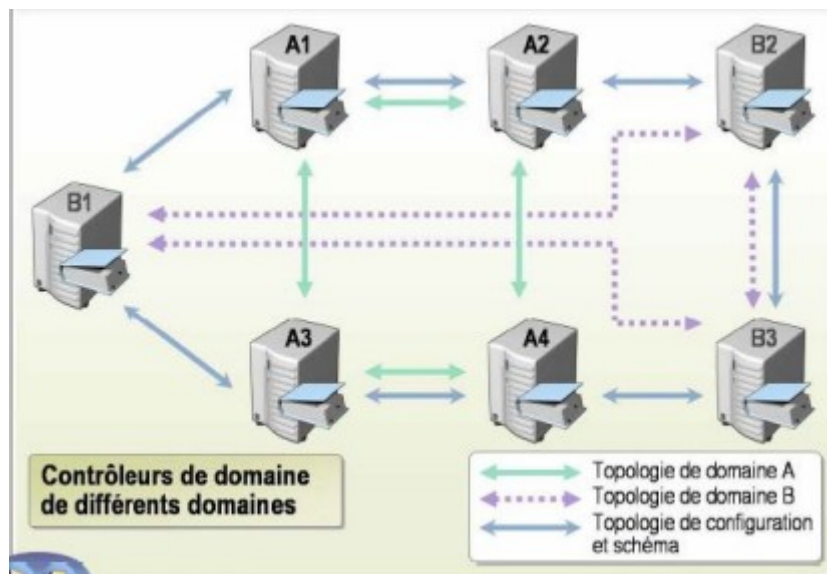


Figure 7 : Réplication dans active directory

b. Types de répliquions

Dans Active Directory, il existe de mode de répliquion.

- Répliquion intra-site : lien de répliquion entre les contrôleurs de domaine d'un même site.
- Répliquion inter-sites : repose sur des liens définis par l'utilisateur qui doivent être créés. Le KCC (Knowledge Consistency Checker) utilise ces liens pour créer une topologie, de manière à ce que la répliquion soit gérée via les liens de site a site.

Le KCC est un processus intégré capable de s'adapter dynamiquement à la topologie de la forêt numérique afin de contenir le plus efficacement possible les données fournies par les nouveaux contrôleurs de domaine.

Le KCC est responsable de la répliquion dans la forêt

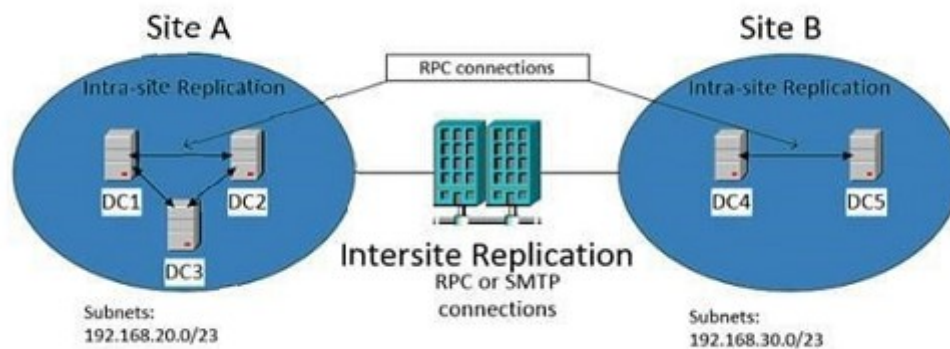


Figure 8 : Types de réplication dans Active Directory

6.3 Présentation du PGI (Progiciel de Gestion Intégré) ou ERP (Enterprise Resources Planning)

Un Progiciel est un ensemble de logiciel munis d'une documentation, conçus pour répondre à des besoins spécifiques et permettre une utilisation autonome. [5]

6.3.1 Introduction

Un ERP est un logiciel central dédié au pilotage de l'entreprise. Il permet de gérer toutes les activités de l'entreprise au sein d'un même outil et d'une base de données unique. Il est composé de plusieurs modules. Chaque module est dédié à une activité : gestion de ventes, gestion des stocks, comptabilité, finance, ressources humaines etc....

En d'autres termes, un ERP regroupe l'ensemble des processus opérationnels d'une organisation.

6.3.2 Caractéristiques

Pour être reconnu en tant qu'ERP, un logiciel doit rassembler les critères suivants :

- Le logiciel doit être issu d'un concepteur unique.
- Son système doit assurer une totale traçabilité des opérations effectuées
- L'ERP doit se reposer sur la synchronisation et la mise à jour des données en temps réel entre les modules.
- Garantit l'unicité des informations grâce à une base de données unique.

- Il peut couvrir l'intégralité de la gestion d'une entreprise

6.3.3 Types d'ERP

On retrouve deux catégories de produits sur le marché des ERP :

- **Les solutions Open Sources**

Une solution Open Source repose sur l'accessibilité de son code source. Implicitement, une entreprise peut modifier ce code source en fonctions de ses besoins.

Voici quelques exemples :

- ADempiere
- Apache OFBiz
- Odoo
- Axelor ERP

- **Les ERP propriétaire**

Un ERP propriétaire est commercialisé sous forme de licence qui définit les limites d'utilisation du logiciel sur une période fixée. L'éditeur propriétaire se charge de la partie technique s'assurant des mises à jour et de l'évolution de l'ERP.

Les principaux ERP propriétaires sont :

- GEAC
- Microsoft
- Oracle
- SAGE
- SAP
- SSA Global

La licence est ce qui différencie un ERP propriétaire des Open Source. Une licence est une forme de contrat par lequel une société

- Donne l'autorisation au client d'utiliser le PGI commercialisé ;
- Détermine les limites de l'utilisation du logiciel ;
- Liste les obligations et responsabilités du client et de la société

Ces deux types de ERP ont leurs avantages et inconvénients. Le choix doit être fait en fonction des besoins, des ressources et du budget de l'entreprise.

Les modules et les fonctionnalités d'un ERP propriétaire sont identiques aux ERP Open Source. Cependant, les ERP propriétaire incluent une prise en charge complète et un service personnalisable.

6.3.4 Objectifs et avantages

a) Objectif

L'objectif d'un ERP est de centraliser l'ensemble des outils de gestion dont l'entreprise a besoin. Il doit ainsi devenir le cœur du système d'information.

b) avantages

Les avantages des ERP sont multiples, elles participent :

- A l'amélioration des performances et de la productivité de l'entreprise pour optimiser la gestion des activités
- A l'amélioration de la communication et de la collaboration entre les services
- A l'amélioration de la prise de décision au sein d'une société.
- A la standardisation et à l'homogénéisation des processus de l'entreprise.

6.4 Réseau Privé Virtuel (VPN : Virtual Private Network)

Un réseau privé virtuel est un système permettant de créer un lien direct entre ordinateurs distants, qui isole leur échange du reste du trafic se déroulant sur des réseaux de télécommunications publics.

C'est le moyen plus facile et le plus efficace de protéger le trafic internet et de masquer l'identité d'une personne en ligne. Il permet notamment de modifier l'adresse IP de la machine pour masquer l'identité de la personne sur les sites web, applications et services. Grâce à une couche de chiffrement solide, un bon VPN masque également les activités vis-à-vis d'un fournisseur d'accès internet, opérateur téléphonique. [8]

Les simples individus utilisent un VPN dans le but de garder leurs activités en ligne privées et garantir l'accès à des sites et services qui sans cela pourraient être restreintes.

Pour les sociétés, un VPN est un moyen permettant de connecter des employés éloignés comme s'ils utilisaient tous le même réseau local dans un bureau central, mais avec moins d'avantages pour les personnes qu'un VPN personnel.

a) Types de VPN

Il existe plusieurs types de VPN. Les plus communs sont PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN, et Hybrid VPN. Nous parlerons de chaque type de VPN plus en détail ci-dessous.

- **VPN PPTP**

PPTP VPN signifie Point-to-Point Tunneling Protocol (protocole de tunnel point-à-point). Comme son nom l'indique, un VPN PPTP crée un tunnel qui capture les données. Les VPN PPTP sont utilisés par des utilisateurs éloignés pour se connecter à leur réseau VPN en utilisant leur connexion internet existante. Ce VPN est utile pour les professionnels et les particuliers. Pour accéder au VPN, les utilisateurs s'y enregistrent en utilisant un mot de passe préapprouvé. Les VPN PPTP sont idéaux autant pour une utilisation privée que professionnelle parce qu'il n'y a pas besoin d'installer de matériel supplémentaire et leurs fonctionnalités sont habituellement offertes dans un logiciel peu cher. Les VPN PPTP sont aussi les plus courants grâce à leur compatibilité avec Windows, Mac et Linux.

Même si les VPN PPTP possèdent de nombreux avantages, ils ont aussi des inconvénients. Le problème d'un VPN PPTP c'est qu'il n'offre pas de cryptage, ce qui est en général la raison pour laquelle les gens utilisent un VPN. Un des autres désavantages, c'est qu'il s'appuie sur le PP, ou le Point-à-point, pour les mesures de sécurité.

- **VPN site to site**

Un VPN Site-to-Site (site-à-site) est également appelé Router-to-Router (routeur-à-routeur), et on l'utilise principalement pour des opérations commerciales. Comme beaucoup d'entreprises possèdent des bureaux nationaux et internationaux, un VPN Site-to-Site sert à relier le réseau des bureaux principaux au reste des bureaux. Ce type de VPN est basé sur Intranet. Le contraire est aussi possible avec les VPN Site-to-Site. Certaines entreprises l'utilisent pour se connecter à d'autres entreprises, de la même façon, mais on appelle ça un VPN basé sur Extranet. Dans des termes simples, les VPN Site-to-Site construisent un réseau virtuel qui unit des réseaux issus de localisations variées pour les connecter à Internet et maintenir des communications sécurisées et privées entre eux.

Tout comme un VPN PPTP, les VPN Site-to-Site créent un réseau sécurisé. Toutefois, il n'y a pas de ligne dédiée, les autres sites d'une entreprise se connectent pour créer un VPN, comme mentionné ci-dessus.

Contrairement au PPTP, le routage, le cryptage et le décryptage sont effectués soit par du matériel informatique, soit grâce à un routeur basé sur logiciel situé des deux côtés.

- L2TP VPN

L2TP signifie Layer to Tunneling Protocol (protocole de tunnellation de niveau 2), développé par Microsoft et Cisco. Les VPN L2TP sont habituellement combinés à un autre protocole de sécurité VPN pour établir une connexion plus sécurisée. Un VPN L2TP forme un tunnel entre deux points de connexion L2TP, et un second VPN comme le protocole IPsec crypte les données et se concentre sur la sécurisation des données entre les tunnels.

Un L2TP est assez similaire au PPTP. Par exemple au niveau de leur manque de cryptage, et de leur fonctionnement avec un protocole PPP. La différence concerne la confidentialité et l'intégrité des données. Les VPN L2TP protège les deux, les VPN PPTP non.

- IPsec

IPsec est l'abréviation de Internet Protocol Security (protocole de sécurité internet). IPsec est un protocole VPN utilisé pour sécuriser les communications par internet sur un réseau IP. Un tunnel est mis en place dans un endroit éloigné et vous permet d'accéder à votre site central. Un IPsec sécurise le protocole de communication internet en vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toute la connexion. Il y a deux modes d'opération dans un VPN IPsec. Le mode transport et le mode tunnel. Les deux modes servent à protéger le transfert des données entre deux réseaux différents. Avec le mode transport, le message dans le paquet de données est crypté. Avec le mode tunnel, le paquet de données entier est crypté.

Un des avantages d'un VPN IPsec, c'est qu'il peut être utilisé en plus d'autres protocoles de sécurité pour un système de sécurité renforcé. Si un IPsec est un bon VPN à avoir, un des désavantages associés à l'utilisation de ce protocole est la grosse quantité de temps que le client doit passer à l'installer avant de pouvoir l'utiliser.

- SSL et TLS

SSL signifie Secure Sockets Layer et TLS Transport Layer Security. Ils fonctionnent ensemble comme un seul protocole. Les deux sont utilisés pour construire une connexion VPN. Dans cette connexion VPN, le navigateur internet sert de client et l'accès utilisateur est restreint à certaines applications seulement plutôt qu'un réseau entier. Les protocoles SSL et TLS sont principalement utilisés par des sites de vente en ligne et des fournisseurs de service.

Un VPN SSL et TSL vous offre une session sécurisée du navigateur de votre PC au serveur de l'application. C'est parce que les navigateurs internet passent facilement au SSL sans que l'utilisateur ait

besoin de faire grand-chose. Les navigateurs web possèdent déjà SSL et TLS de façon intégrée. Les connexions SSL commencent par https au début de l'URL au lieu de http.

- **MPLS VPN**

Un Multi-Protocol Label Switching (Multi-protocole de commutation d'étiquettes), ou un VPN MPLS, est utilisé pour des connexions de type Site-à-Site. C'est principalement dû au fait que les MPLS sont très flexibles et adaptables. Le MPLS est une ressource normalisée utilisée pour accélérer le processus de distribution de paquets de réseau avec de multiples protocoles. Les VPN MPLS sont des systèmes basés sur fournisseurs d'accès. On dit ça quand un site ou plusieurs sont connectés pour former un VPN avec le même fournisseur d'accès ISP.

Toutefois, le plus gros inconvénient des VPN MPLS c'est que le réseau n'est pas facile à mettre en place, par rapport aux autres VPN. Il est aussi très difficile à modifier. De plus, les VPN MPLS sont souvent bien plus chers.

- **Hybrid VPN**

Un VPN hybride combine à la fois un MPLS et un IPsec. Habituellement, ces deux types de VPN sont utilisés séparément. Mais il est possible de les utiliser en même temps. On peut par exemple utiliser le VPN IPsec comme soutien du VPN MPLS. Les VPN IPsec nécessitent de l'équipement du côté du client, comme mentionné ci-dessus. Habituellement, il faut un routeur ou un appareil de sécurité multi-tâches. Grâce à ces appareils, les données sont cryptées et forment le tunnel VPN comme évoqué précédemment. Les VPN MPLS sont utilisés par un porteur, ce qui signifie que l'équipement doit être dans le réseau du porteur.

Pour réussir à connecter ces deux VPN, un portail est établi pour éliminer le tunnel IPsec mais aussi le relier au VPN MPLS tout en préservant la sécurité qu'offrent ce réseau. Les VPN hybrides sont utilisés par les entreprises car c'est le choix le plus approprié pour leurs sites. Les MPLS ont beaucoup d'avantages par rapport aux connexions internet publiques, mais le coût est élevé. Utiliser un VPN hybride vous permet d'accéder au site central via un site secondaire. Les VPN hybrides coûtent assez cher mais sont très flexibles.

b) Service de routage et d'accès à distance

Dans Active Directory, le service Routage et accès distant prend en charge l'accès non traditionnel à un réseau. Vous pouvez configurer le service Routage et accès distant de manière à ce qu'il fasse office de serveur d'accès distant et connecter ainsi des télétravailleurs aux réseaux d'une entreprise. Il fournit la connectivité nécessaire aux clients d'accès à distance et VPN. [9]

Dans une infrastructure à plusieurs serveurs d'accès réseau, il est possible de centraliser l'authentification en utilisant le service RADIUS afin d'authentifier et d'autoriser les clients d'accès réseau. L'utilisation de ce service dispense chacun des serveurs d'accès du réseau d'effectuer les opérations d'authentification et d'autorisation.

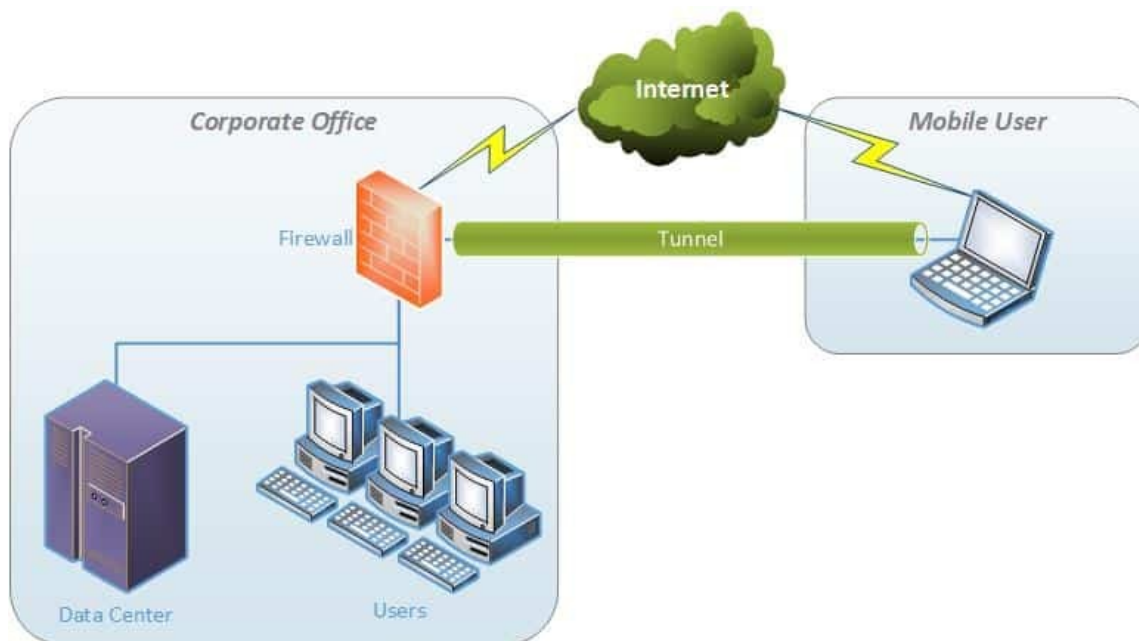


Figure 9 : Schéma d'utilisation de tunnel VPN

Un serveur d'accès réseau est un serveur qui fait office de passerelle vers un réseau pour un client. Dans ce module, le serveur d'accès réseau est un serveur configuré avec le service Routage et accès distant. Il peut également être qualifié de serveur d'accès distant (pour les connexions d'accès à distance) ou de serveur VPN, selon le type de connexion qu'il est habilité à négocier.

CHAPITRE 7 : MISE EN PLACE ET INSTALLATION

7.1. Installation et configuration

« Server Manager » est une console de gestion dans « Windows Server » qui aide les professionnels dans le domaine informatique à provisionner et à gérer les serveurs Windows locaux et distants à partir de leurs postes de travail, sans nécessiter un accès physique au serveur ou la nécessité d'activer les connexions RDP (Remote Desktop Protocol) à chaque serveur.

7.1.1 Installation d'active directory Domain Services

L'installation d'Active Directory est plutôt simple. Il suffit juste d'aller dans la console « Server Manager » et de cliquer sur « Manage » ou gérer, puis « add roles and features » pour commencer la configuration et l'installation des outils nécessaires [2].

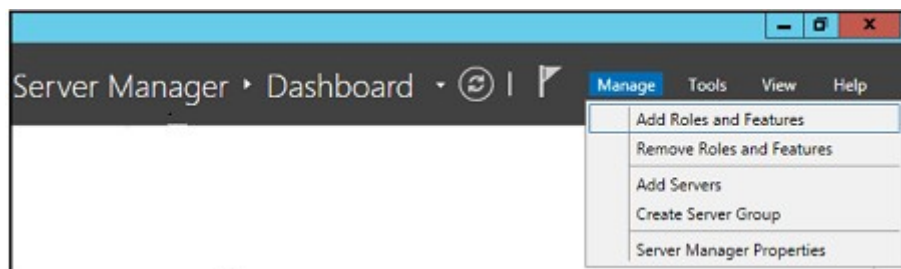


Figure 10 : ajout des rôles et fonctionnalités

Après cela, on passe à l'étape suivante qui est l'attribution des rôles.

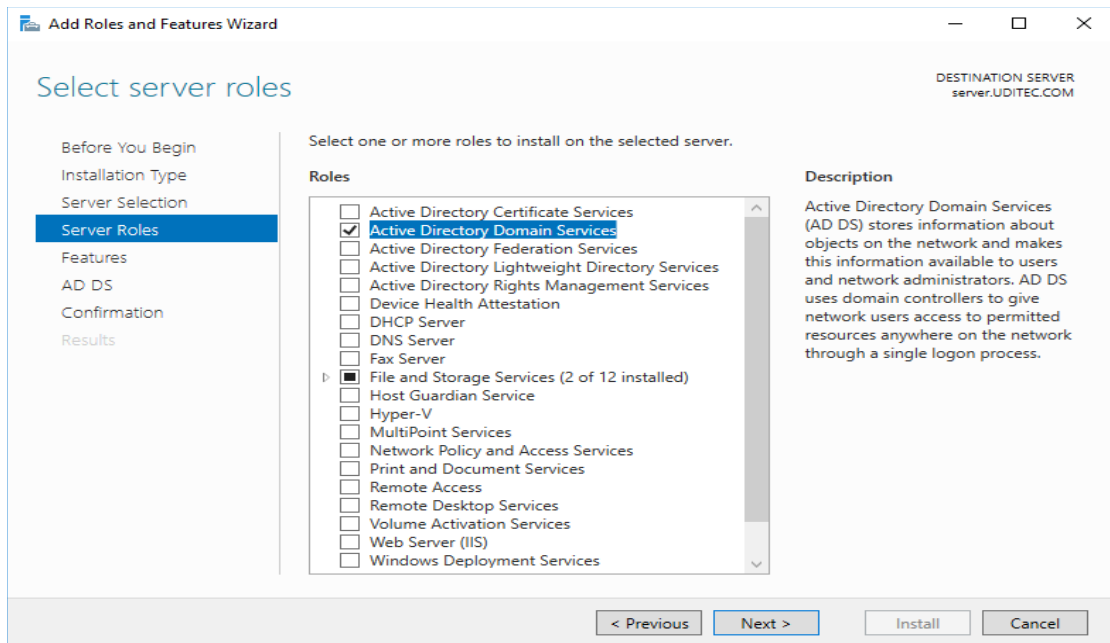


Figure 11 : Attribution de rôles serveurs

L'étape suivante marque l'attribution des fonctionnalités dans le service.

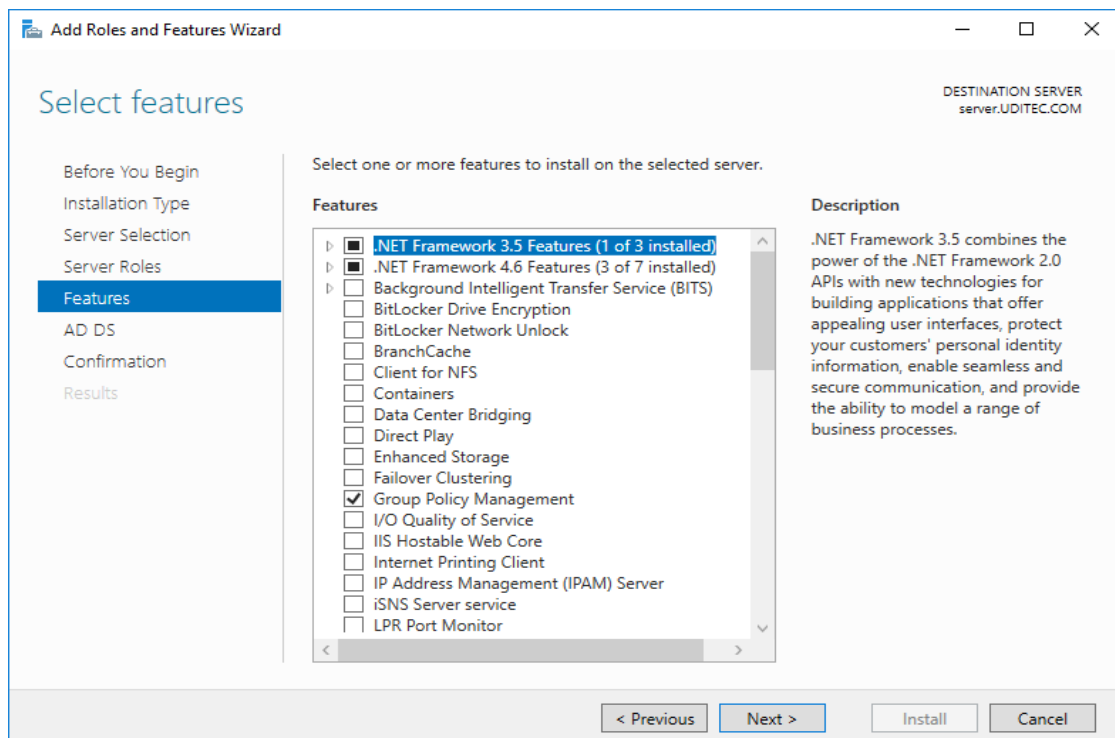


Figure 12 : Ajout des Fonctionnalités requises

L'étape suivante marque le début de l'installation d'Active Directory

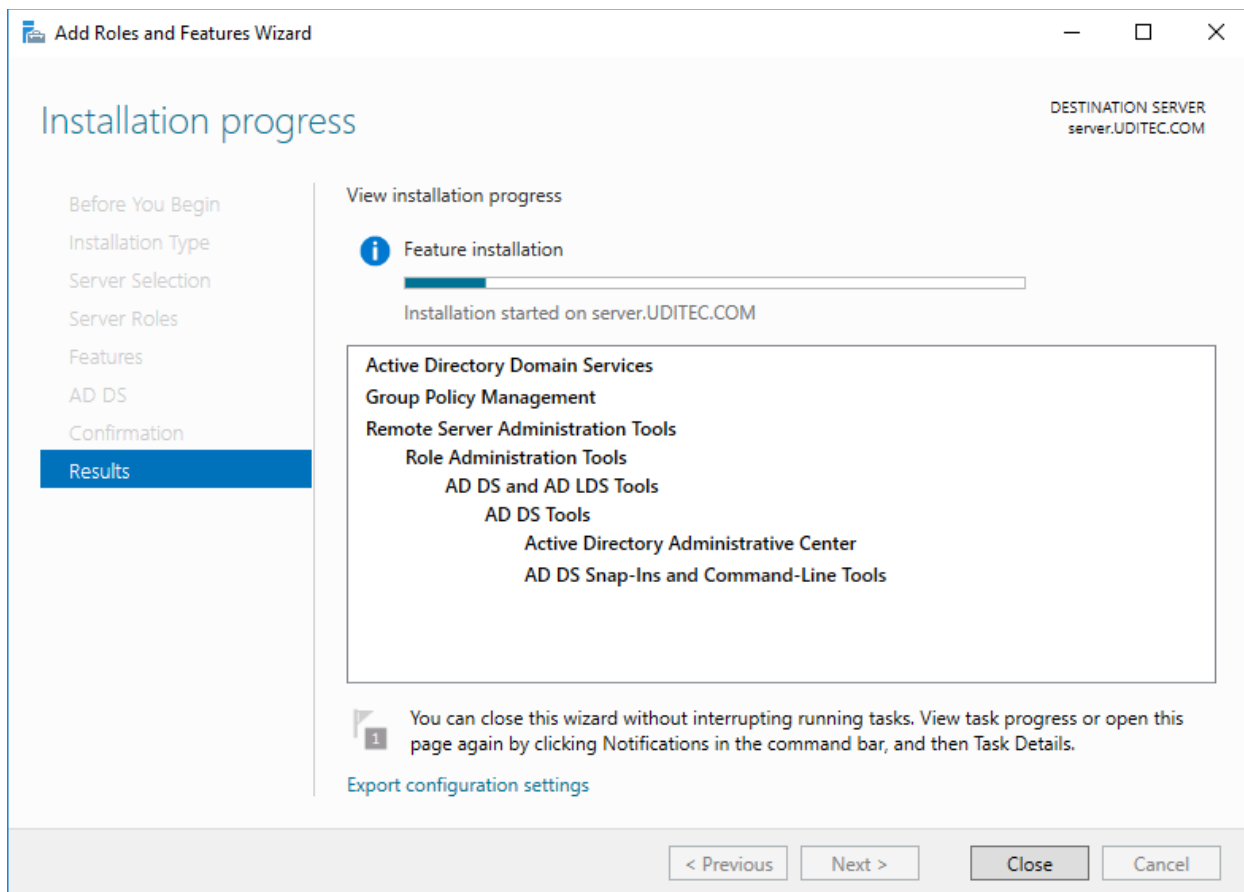


Figure 13 : Installation du service Active Directory

Rappelons que l'installation du service AD DS est importante pour pouvoir :

- Organiser les données de manière à répondre aux besoins de l'entreprise
- Fournir des fonctions intégrées de réplication et de redondance : si un contrôleur tombe en panne, un autre contrôleur de domaine prend la charge de son compte.
- Assurer la gestion centralisée des droits d'accès au réseau.

7.1.2 Installation de Domain Controller et de la forêt

La Mise en place de contrôleur de domaine et de la forêt n'a rien de bien sorcier non plus. Sur le menu « Server Manager », on cliquera sur la notification pour la configuration du serveur en tant que contrôleur de domaine en procédant par étapes :

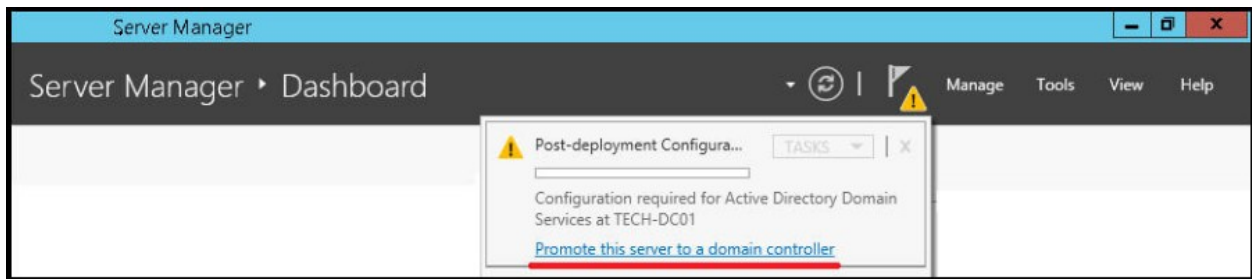


Figure 14 : Configuration de contrôleur de domaine

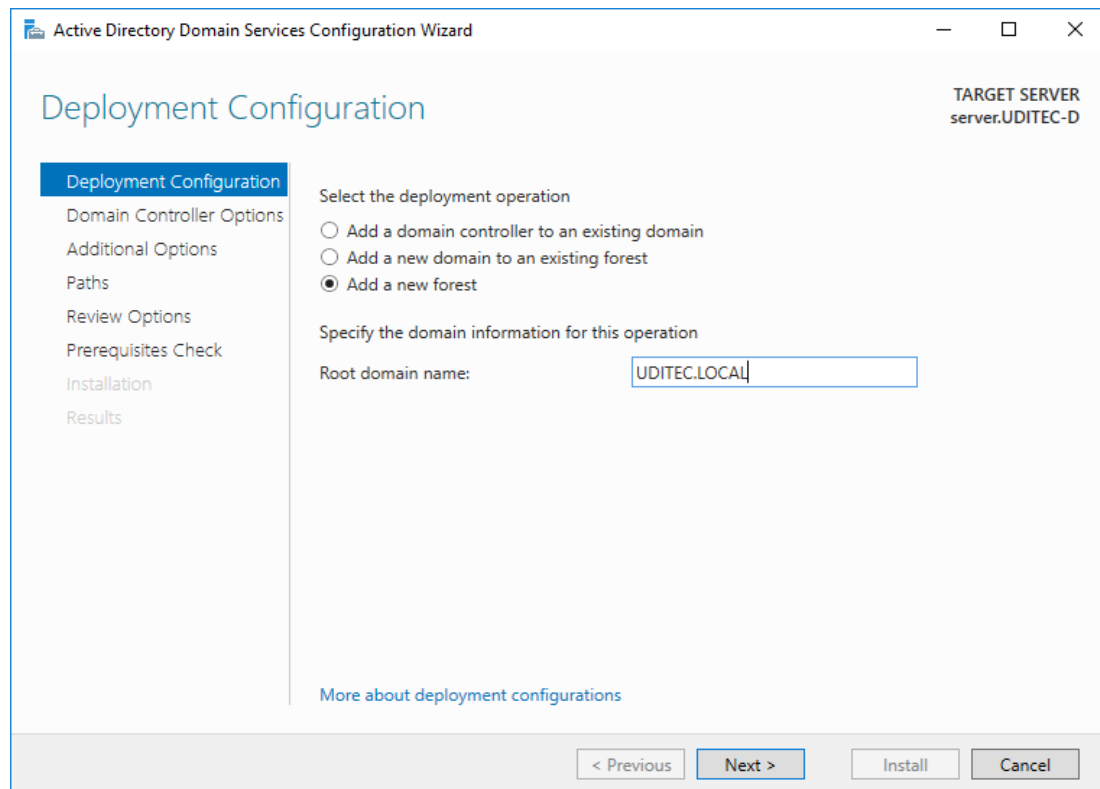


Figure 15 : Ajout de la forêt

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
server.UDITEC-D

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Figure 16 : Options contrôleur de domaine

Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
server.UDITEC-D

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: UDITEC

[More about additional options](#)

< Previous Next > Install Cancel

Figure 17 : Vérification du NetBios

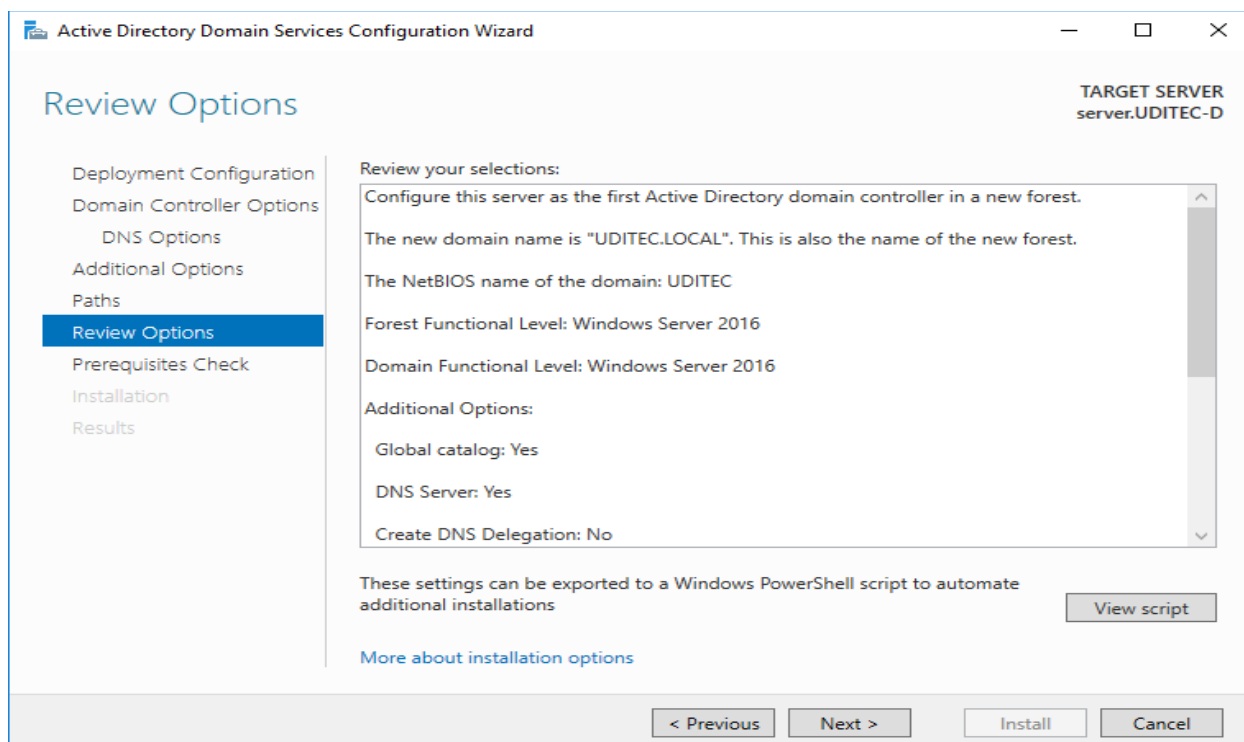


Figure 18 : Vérification des options d'installation

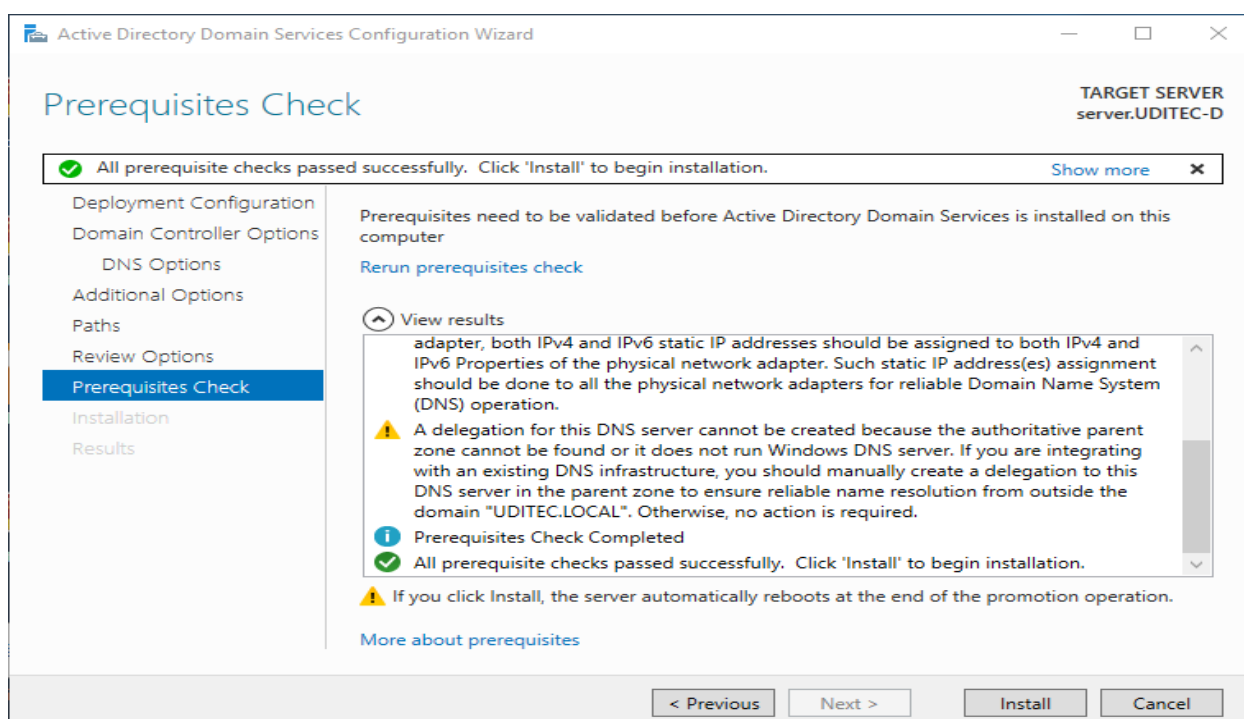


Figure 19 : Vérification des prérequis

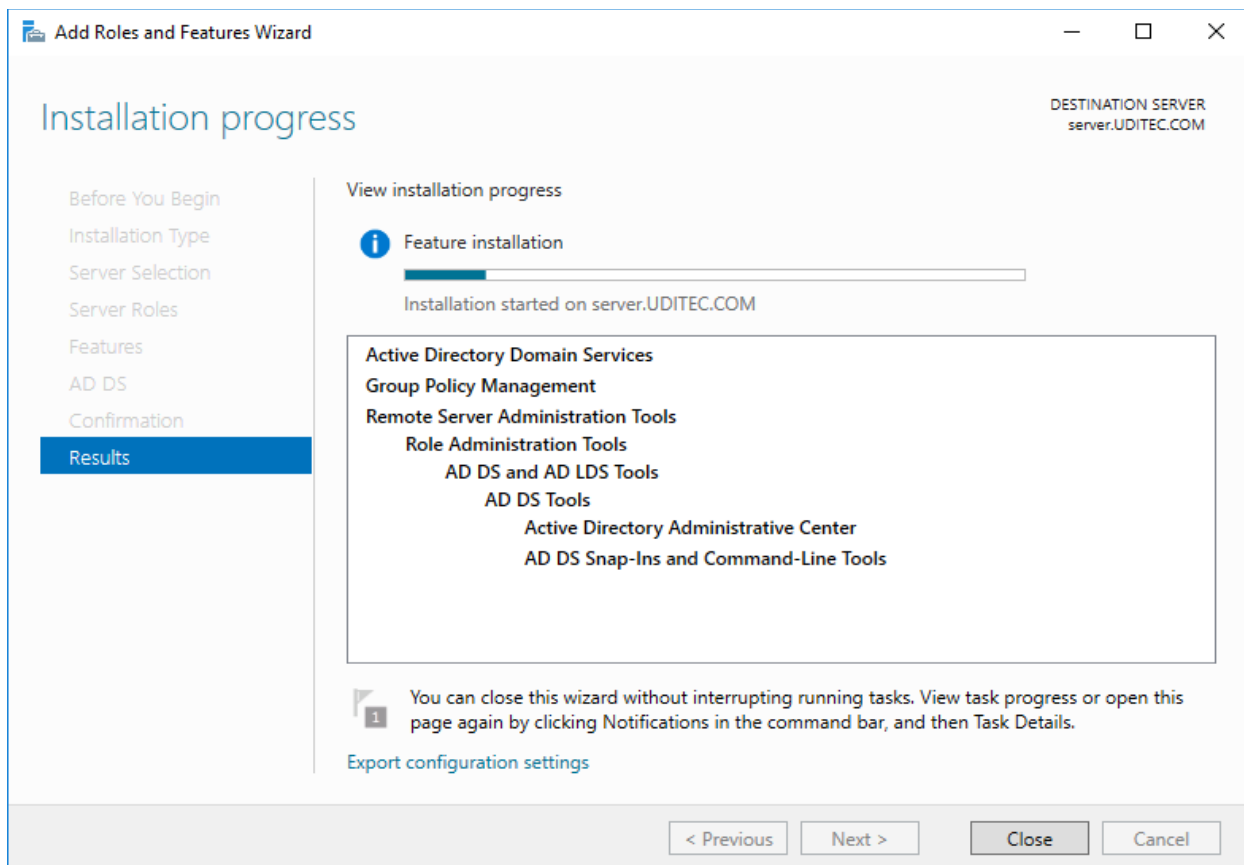


Figure 20 : Installation active de l'annuaire

Après l'installation, la machine redémarrera automatiquement.

7.1.3 Mise en place des Unités Organisationnelles

La mise en place des Unités Organisationnelles est une nécessité pour le une bonne administration du réseau du domaine de la forêt. Pour se faire, il faut accéder aux outils du « Server Manager » dans la section « Utilisateurs et ordinateurs Active Directory comme suit.

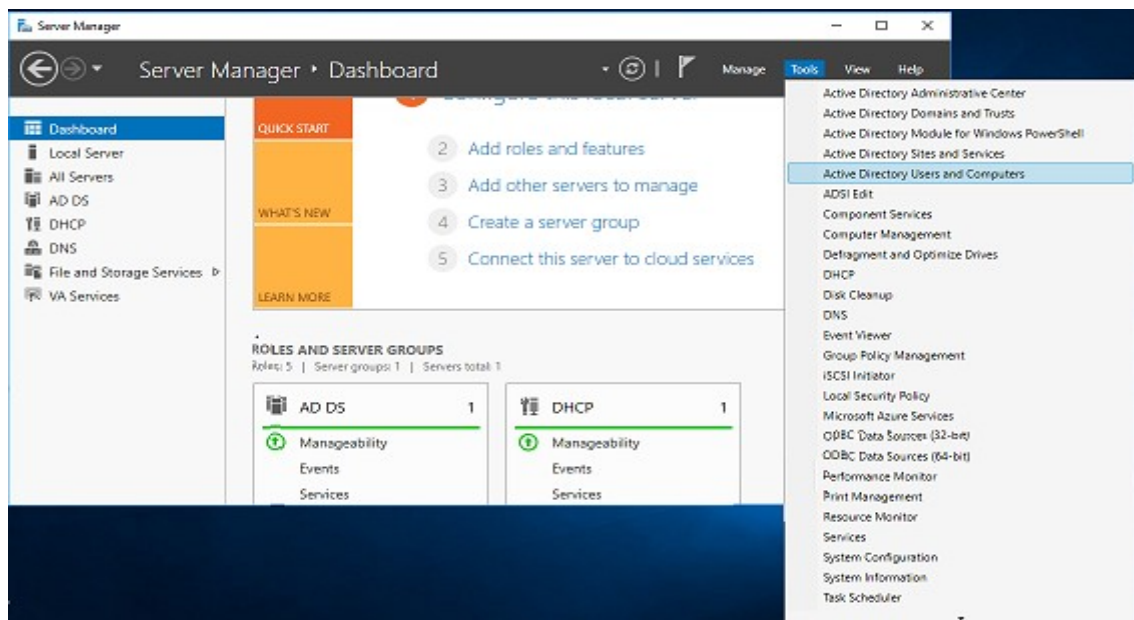


Figure 21 : Administration des utilisateurs et ordinateurs

Après cela, une fenêtre pour administrer les utilisateurs et les machines s'ouvrira.

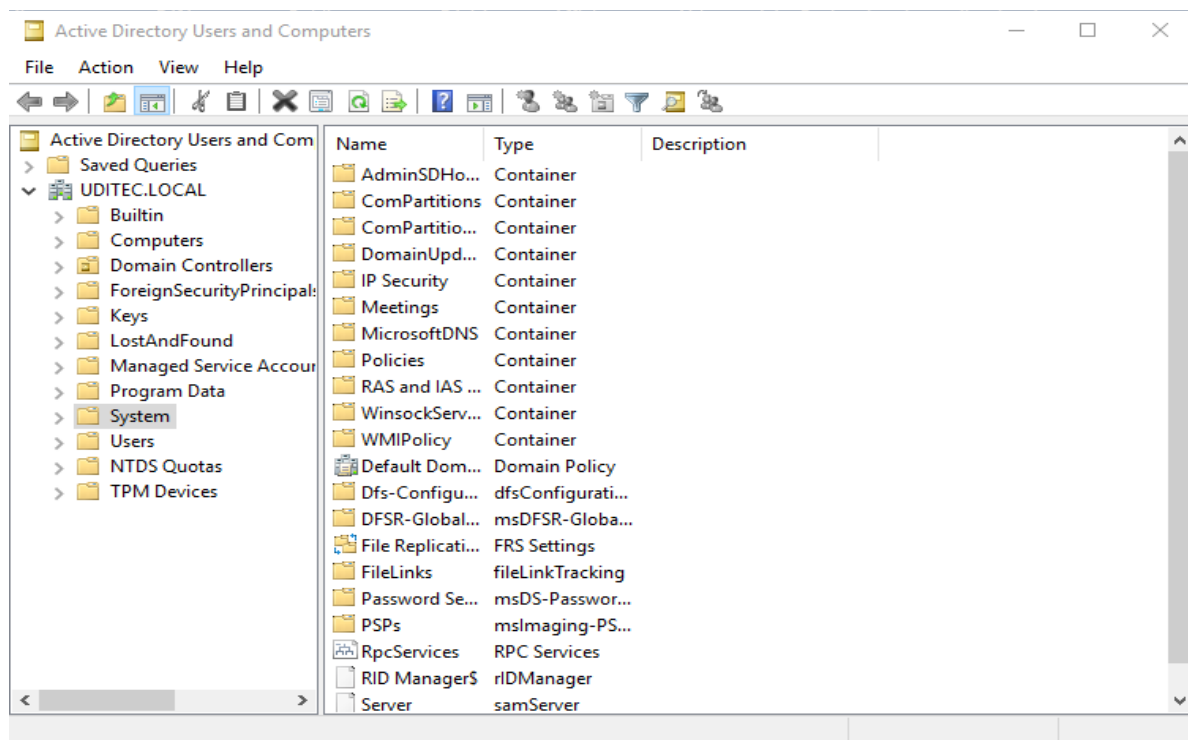


Figure 22 : Accès à la fenêtres Utilisateurs et Ordinateurs Active Directory

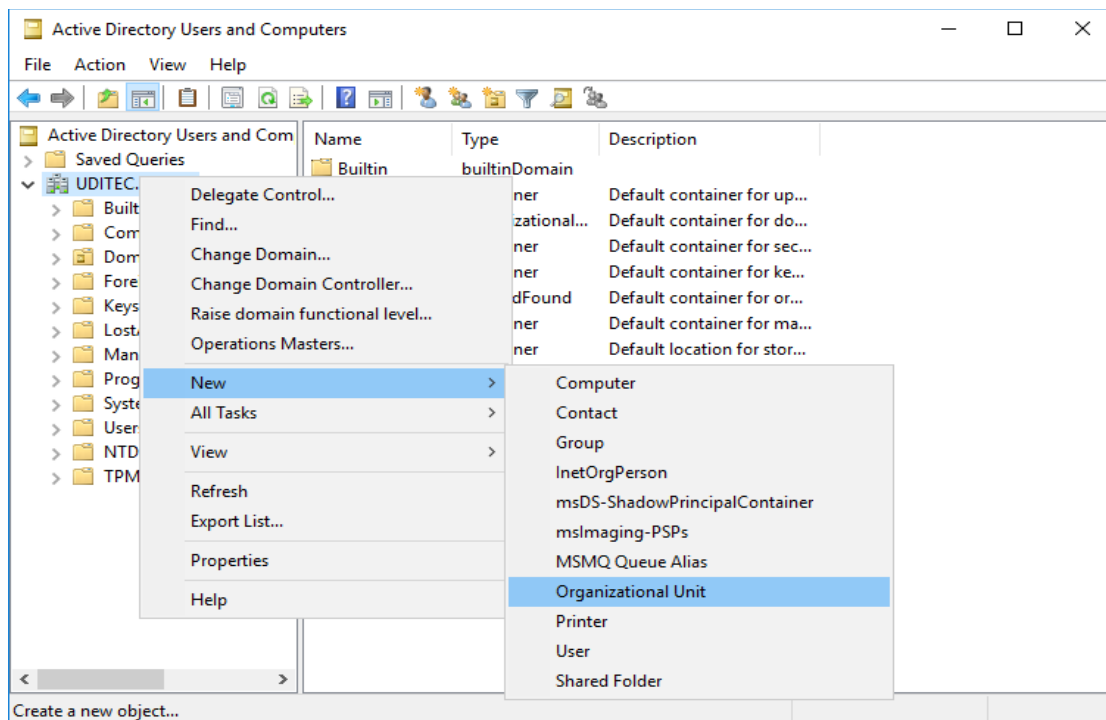


Figure 23 : ajout d'une nouvelle unité d'organisation

L'unité organisationnelle est un conteneur qui permet de déléguer les tâches d'administrations et de droits sur les objets Active Directory. On va créer une arborescence d'unité organisationnelle pour les comptes utilisateurs et ajouter de nouveaux utilisateurs pour chaque OU.

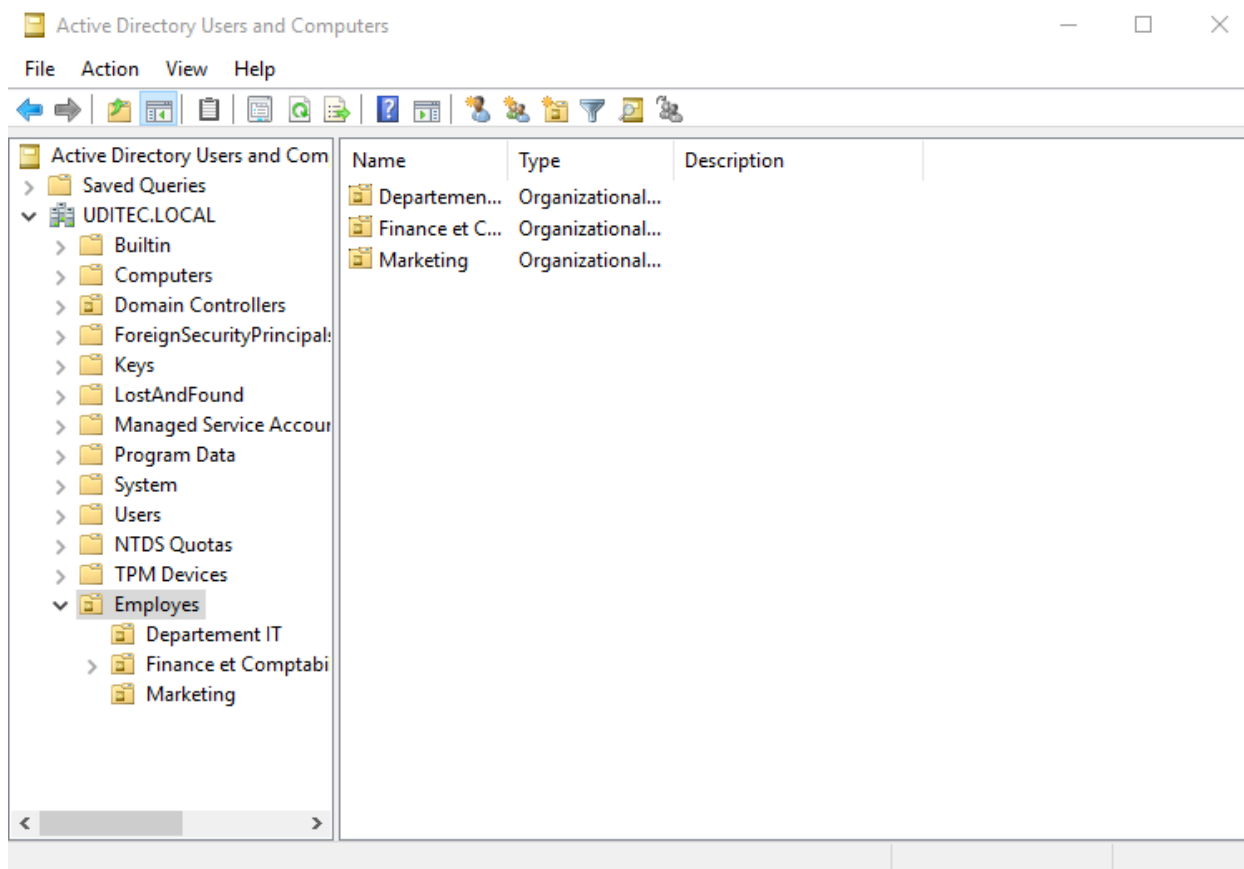


Figure 24 : Arborescence de compte utilisateur

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'UDITEC.LOCAL/Finances et Comptabilites/Comptabilite'. The 'First name' field contains 'Expert', 'Last name' contains 'Comptable', and 'Full name' is 'Expert Comptable'. The 'User logon name' is 'expertcomp' and the domain is '@UDITEC.LOCAL'. The 'User logon name (pre-Windows 2000)' is 'UDITEC\expertcomp'. The 'Next >' button is highlighted.

Figure 25 : Ajout d'utilisateur

Figure 26 : Attribution de mot de passe utilisateur

Règles de mot de passe :

- Ne pas contenir le prénom, nom, ou nom d'ouverture de session
- Doit être de 8 caractères au minimum
- Doit contenir au moins un caractère en majuscule, en minuscules et un chiffre

Il est possible d'y gérer les droits d'accès des utilisateurs par exemples les horaires d'accès

Figure 27 : gestion des droits d'accès au compte

Comme on peut le voir, il est possible de restreindre le temps d'activité des utilisateurs sur un intervalle donné.

7.1.4 Mise en place de la stratégie de groupe (GPO)

Les Stratégies de Groupes sont les moyens à la disposition de l'administrateur réseau pour limiter les zones d'actions des utilisateurs dans les domaines de la forêt.

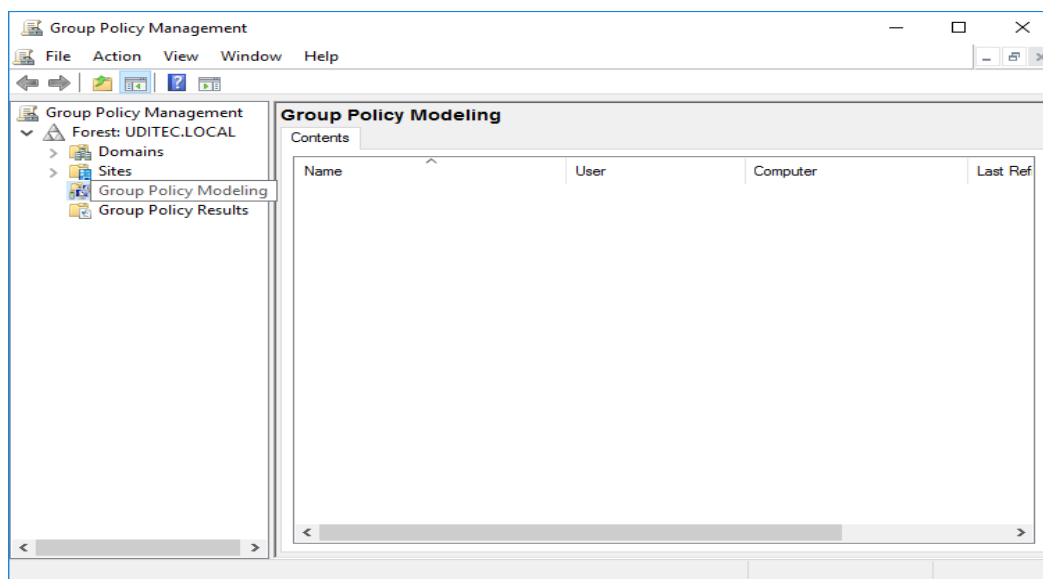


Figure 28 : Stratégie de groupe

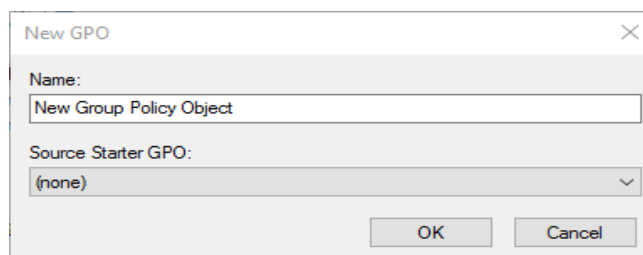
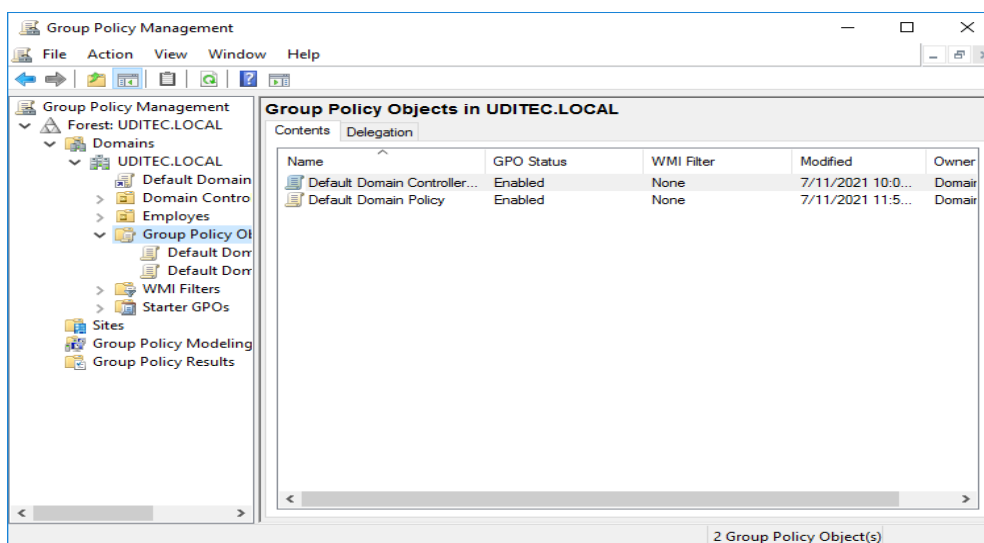


Figure 29 : Attribution de nouvelle stratégie de groupe

A partir de là, nous pouvons définir les possibilités d'accès de chaque utilisateur sur les sites. Par exemple, restreindre l'accès à certaines applications.

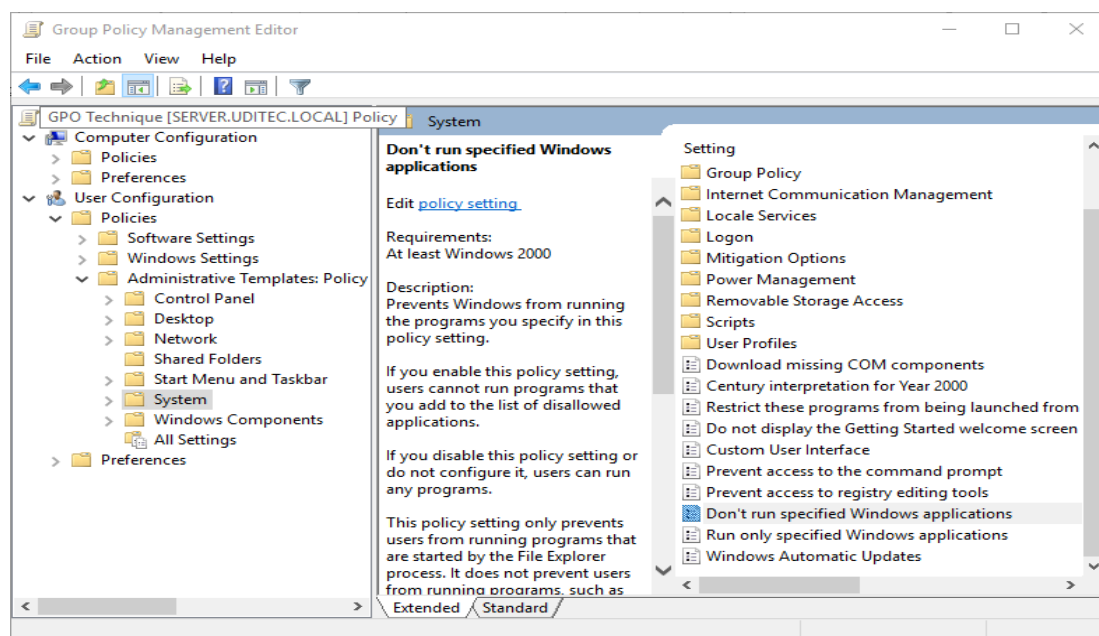


Figure 30 : Paramètre de la GPO

Comme on peut voir sur la figure 30, on peut définir plusieurs stratégies comme par exemple limité les applications pouvant être démarrées sur les machines du domaine.

7.1.5 Configuration de l'accès à distance par tunnel VPN

Active Directory permet, grâce à son accès de bureau à distance, de créer un réseau de tunnel.

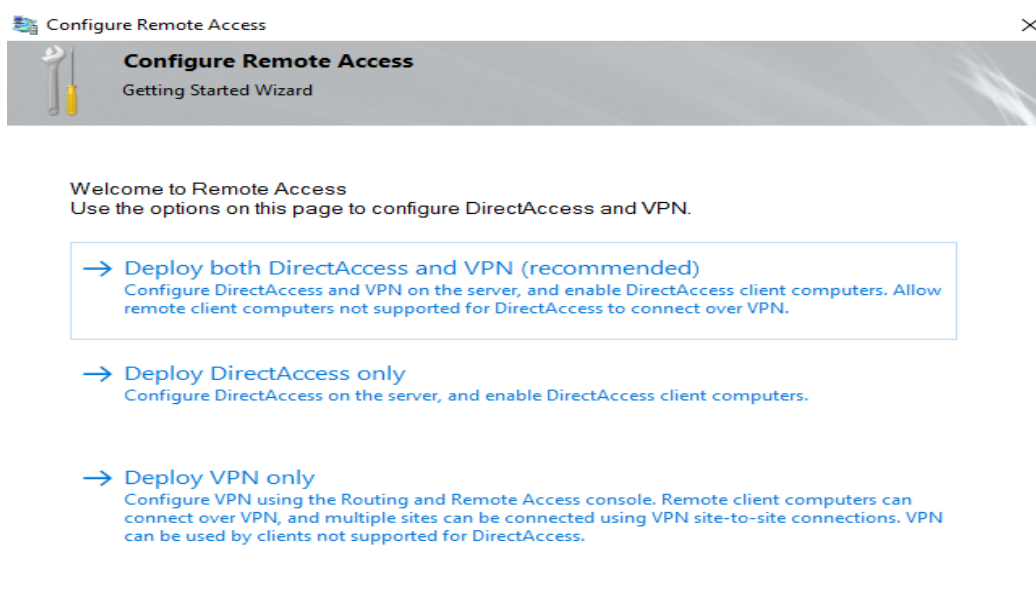


Figure 31 : Méthode de déploiement

Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

- ☐ Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
- ☐ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
- ☐ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
- ☐ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
- ☒ Custom configuration
Select any combination of the features available in Routing and Remote Access.

< Back

Next >

Cancel

Figure 32 : Configuration de point d'accès

Routing and Remote Access Server Setup Wizard

Custom Configuration

When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

- ☒ VPN access
- ☐ Dial-up access
- ☐ Demand-dial connections (used for branch office routing)
- ☐ NAT
- ☐ LAN routing

< Back

Next >

Cancel

Figure 33 : Sélection du moyen de connexion

Routing and Remote Access

Start the service

The Routing and Remote Access service is ready to use.

Start service

Cancel

Il suffit alors de cliquer sur « Start service » pour rendre opérationnel le service. Par la suite, on configurera les droits d'accès a tunnel en spécifiant les utilisateurs ou les groupes autorisés

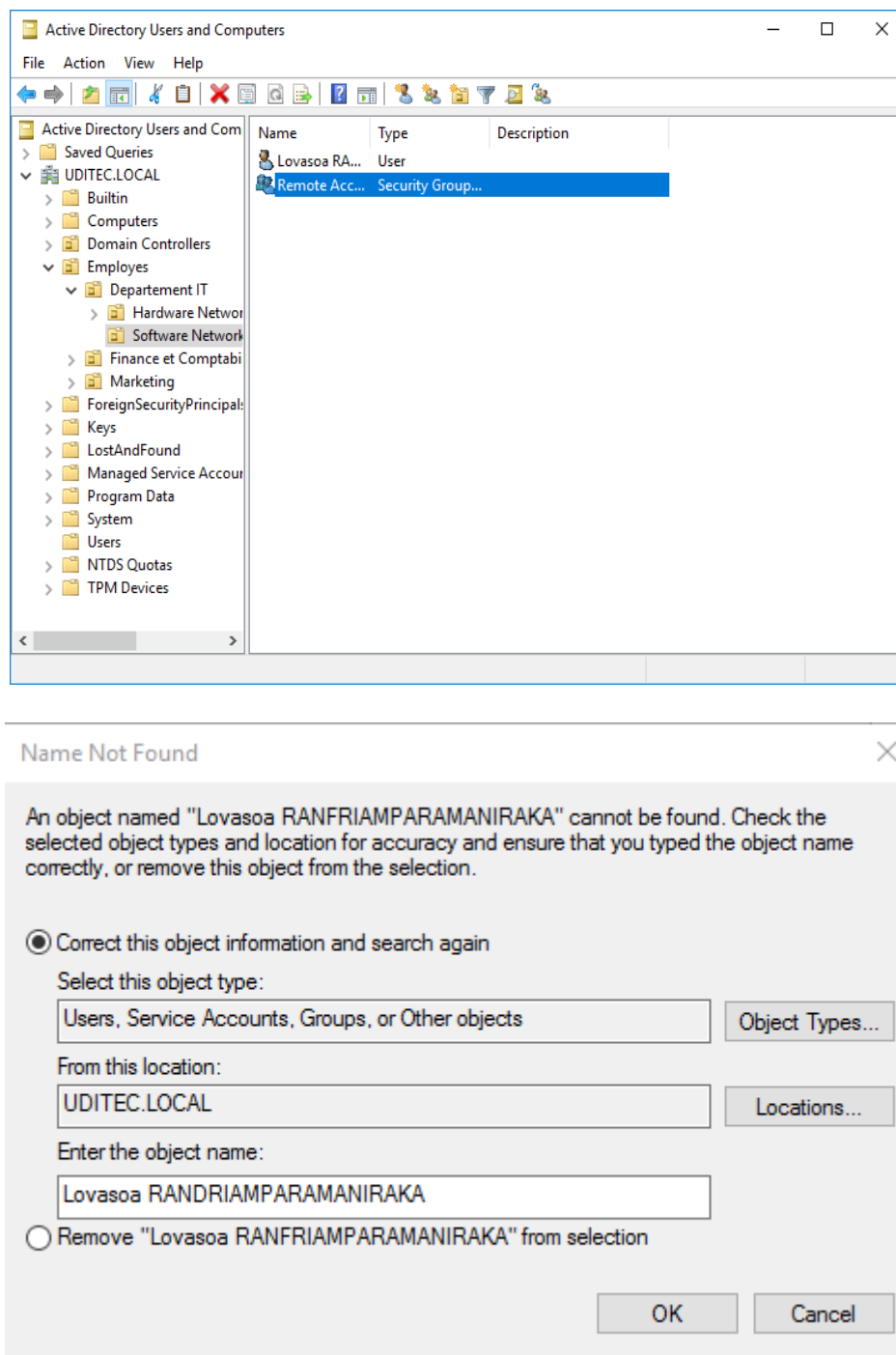


Figure 34 : Mise en place du groupe et ajout d'utilisateur du groupe

7.2 Présentation brève de l'usage du service au sein du réseau

Pour se faire une idée de l'utilisation des services mis en place, la figure suivante va nous informer le mécanisme.

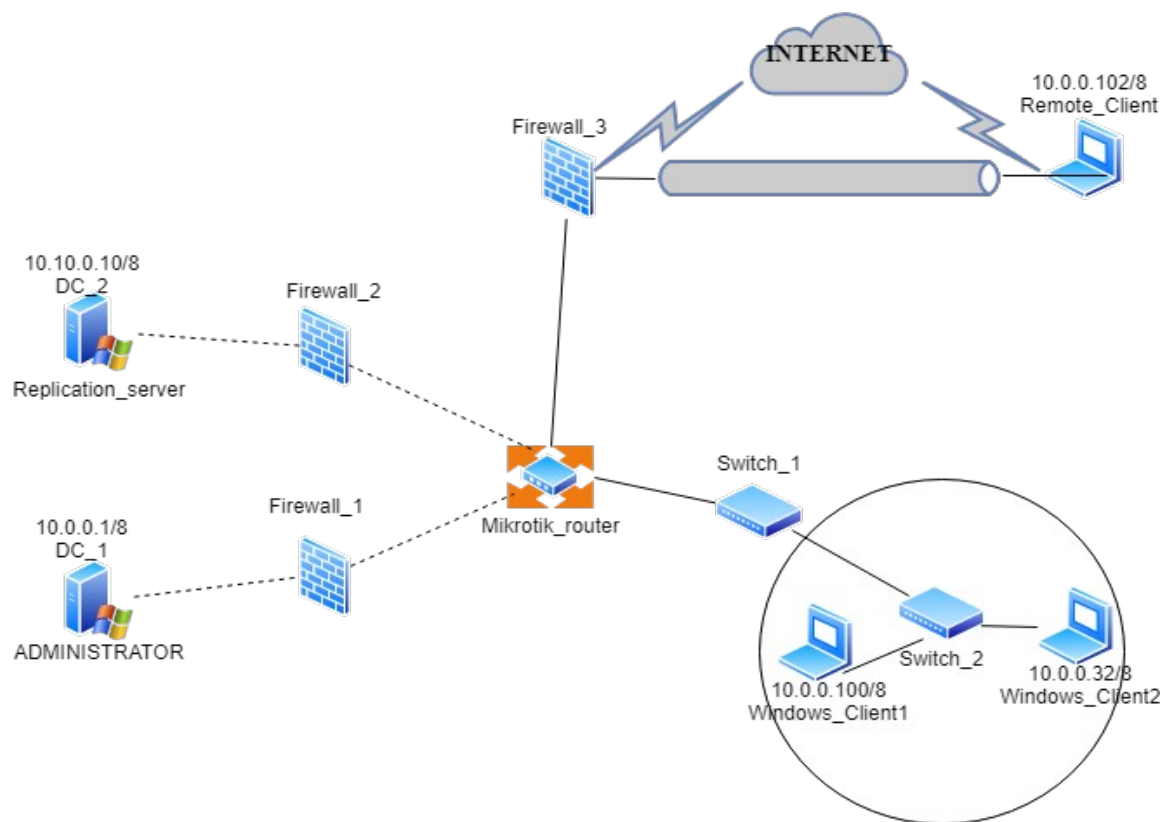


Figure 35 : Exemple de topologie d'usage du service

Sur cette image, on peut voir le client distant, qui est client hors domaine, accédant aux services de l'entreprise par tunnel sécurisé et également les postes clients. En cas de panne de l'un des serveurs, la réplication des données est assurée par le contrôleur actif ce qui permet une disponibilité parfaite des services et des données nécessaires aux utilisateurs.

CONCLUSION GENERALE

Pour conclure, ces deux mois de stage pratique a UDITEC Ankorondrano Antananarivo a permis de faire évoluer mes connaissances sur la gestion de réseau Informatique et aussi d'avoir eu beaucoup d'expériences dans le monde professionnel.

Durant la réalisation de ce projet qui se porte sur « La réplication d'Active Directory avec mise en place de VPN », l'utilisation de plusieurs de services ont été considéré pour la bonne gestion du réseau des domaines de la forêt. Il m'a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il m'a initié au monde de la recherche sur les réseaux informatiques et m'a également permis de découvrir les nouvelles technologies de Microsoft.

Le but étant de centraliser les services d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows afin de faciliter la gestion multiserveur et multi-utilisateurs sur plusieurs sites et ainsi faciliter les taches des administrateurs réseaux.

En perspective, des améliorations pourraient être ajouter au projet comme l'implémentation de progiciel pour la gestion des ressources de l'entreprise ou l'implémentation d'un nouveau server VPN en dehors de l'instance d'Active Directory.

GLOSSAIRE

Application : c'est un programme ou ensemble de logiciel directement utilisé pour réaliser une tâche ou ensemble de tâches élémentaires d'un même domaine, typiquement un éditeur de texte, un navigateur web, un jeu vidéo sont des applications.

Firewall : en français pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique ; Il surveille et contrôle les applications et les flux de données (Paquets).

Interface graphique : c'est un dispositif de dialogue homme-machine c'est-à-dire un langage d'échange entre humain et la machine (Ordinateur). Votre ordinateur affiche à l'écran des éléments que vous comprenez et que vous interprétez, chaque système dispose de sa propre interface graphique comme un smartphone, un distributeur de billet à la banque, ...

Inventaire : c'est une opération permettant de collecter le maximum d'informations sur les composants des matériels informatiques, ces performances et ressources dans un Parc Informatique d'une société.

Parc Informatique : c'est un ensemble des matériels et logiciels informatiques (Ordinateurs, imprimante, serveur...) relié en réseau dans une société.

Requête : c'est un moyen formel d'effectuer une recherche d'information dans un système d'information. Parc exemple dans un réseau informatique, un message envoyé par un client vers un serveur qui émet une réponse.

Système d'exploitation : souvent appelé OS (Operating System) en anglais, c'est un ensemble de programme chargé d'établir une relation entre les différentes ressources matérielles, les applications et les utilisateurs.

Simulation : c'est une représentation fictive de la réalité. Il s'agit d'imiter une situation, par exemple la simulation réseau c'est de reproduire l'architecture d'un réseau et cela sans utiliser de machine physique.

Serveur : c'est un dispositif informatique (matériel ou logiciel) qui offre des services à un ou plusieurs clients ; les services les plus courants sont l'accès au web (internet), le courrier électronique, le partage de périphériques (imprimantes, disque durs, ...), le partage des données, ...

REFERENCES BIBLIOGRAPHIQUES

[1] - « TCP-IP – Théories des réseaux » support de cours, Mr SIAKA

[2] - « Administration Microsoft » Support de cours, Mr SIAKA

[3] - « Windows Server 2016 – Architecture et gestion des services de domaine Active Directory (ADDS) »
Jean François Apréa

REFERENCES WEBOGRAPHIQUES

- [4] - <https://openclassrooms.com/fr/courses/2356306-prenez-en-main-windows-serveur/> “Apprehender Windows Server.”
- [5] - <https://www.cegid.com/fr/faq/quest-quun-erp/> “Qu’est-ce qu’un ERP?”
- [6] - <https://blog.varonis.fr/services-de-domaine-active-directory-ad-ds-presentation-et-fonctions/>
- [7] - <https://dll.ummto.dz> « Migration d’une infrastructure réseau de Windows »
- [8] - <https://www.futura-science.com/tech/definitions/connection-vpn-1819/> « VPN : Qu’est-ce que c’est ? »
- [9] - <https://www.inforatiweb-pro.net/admin-systeme/win-server/ws-2012-routage-et-serveur-vpn-2.html>
« Routage et serveur VPN sous Windows Server 2012 »

TABLES DE MATIERES

CURRICULUM VITAE

.....I

REMERCIEMENTS.....III

SOMMAIRE

GENERALE.....IV

Liste des figures.....V

Liste des tableaux.....VII

Liste des abréviations.....VIII

INTRODUCTION

GENERALE.....1

PARTIE I : Présentation Générale.....2

Chapitre I : Présentation de l'Ecole Nationale d'Informatique.....3

1.1. Information d'ordre général.....3

1.2. Missions et historique.....3

1.3. Organigramme institutionnel de l'ENI.....4

1.4. Domaine de spécialisation.....5

1.5. Architecture des formations pédagogiques.....6

1.6. Relations de l'ENI avec les entreprises et les organismes.....8

1.7. Partenariat au niveau international.....9

1.8. Débouchés professionnels avec des diplômés.....10

1.9. Ressources humaines.....12

Chapitre 2 : Presentation d'UDITEC.....13

2.1- Description Generale.....13

2.2- Activité principale.....13

2.3- Objectif..13

2.4- Organigramme.....14

2.5- Reseau de vente.....	14
2.6- Partenaires.....	14
Chapitre 3 : Description du projet.....	15
3.1. Descriptif.....	15
3.2.Chronogramme de travaux.....	15
3.3. Moyens nécessaires à la réalisation du projet.....	16
3.3.1 Moyens humains.....	16
3.3.2 Moyens logiciels.....	16
3.3.3 Moyens materiels.....	16
3.4. Objectifs.	16
3.5. Resultats attendus.....	16
PARTIE II : ANALYSE	17
Chapitre 4 : ANALYSE DE L’EXISTANT.....	18
4.1. Topologie d’UDITEC.....	18
4.2. Type de reseau.....	18
4.3. Equipements d’interconnexions.....	19
4.4. Postes de travaux.....	20
4.5. Serveurs.	20
4.6. Disponibilites.....	21
4.7. Surveillance.....	21
Chapitre 5 : Critique de l’existant.....	22
5.1. Critique de l’existant.....	22
5.2.Solutions proposees.....	22
PARTIE III : REALISATIONS	23
Chapitre VI : CHOIX DES OUTILS	24
6.1. Presentation de Windows Server.....	24

6.2. Active Directory.....	24
6.2.1. Generalite.....	24
6.2.2. Description d'un service d'annuaire.....	25
a. Active Directory.....	25
b. Protocole LDAP.....	25
6.2.3. Structure logique d'Active Directory.....	26
6.2.4. Structure physique d'Active Directory	28
6.2.5. Les services d'Active Directory	28
6.2.6. Catalogue Global.....	29
6.2.7. Domain Name System	29
6.2.8. Dynamic Host Configuration Protocol	30
6.2.9. Les types de comptes Active Directory	30
a. Compte utilisateur.....	30
b. Compte ordinateur.....	30
c. Compte de groupe.....	30
i. Groupe de distribution.....	31
i.i Groupe de securite.....	31
6.2.10. Les strategies de groupe.....	31
a. Definition.....	31
b. Les phases d'utilisation des GPO.....	32
c. Differents choix de strategies.....	32
1. Types de GPO.....	32
2. Types de deploiement.....	32
6.2.11. Replication d'Active Directory	32
a. Generalite.....	33
b. Types de replication.....	33
6.3. Presentation du PGI.....	34
6.3.1. Introduction.....	34

6.3.2. Caracteristiques.....	34
6.3.3. Types de ERP.....	34
6.3.4. Objectifs et avantages.....	35
a. Objectif.....	35
b. Avantages.....	35
6.4. Reseau Prive Virtuel.....	36
a) Types de VPN.....	36
b) Services de routage et d'accès a distance.....	39
Chapitre 7. Mise en place et installation.....	40
7.1. Installationet configuration.....	40
7.1.1. Installation d'Active Directory Domain Services.....	40
7.1.2. Installation du Domain Controller et de la forêt	42
7.1.3. Mise en place des Unites Organisationnelles.....	45
7.1.4. Mise en place des strategies de groupe	49
7.1.5. Configuration de l'accès à distance par tunnel VPN.....	50
7.2.Presentation breve de l'usage du service.....	54
CONCLUSION.....	55
GLOSSAIRE.....	X
BIBLIOGRAPHIE.....	X
I	
WEBOGRAPHIE.....	XII
TABLE DES MATIERES.	
.....	XIII
RESUME.....	XVII
ABSTRACT.....	XVII

RESUME

En guise de résumé, la mise en place du serveur actif de l'annuaire d'Active Directory, en y mentionnant la présentation, l'installation et la configuration des services utilisées, afin d'assurer bon fonctionnement des services. Le déploiement du serveur d'accès à distant et de routage permettra aux client distant d'accéder aux services de l'entreprise sans pour autant utiliser un poste client du domaine.

Durant le stage, mise à part la mise en place du projet, en œuvrant en tant qu'assistant, en contribuant et en participant à de nombreuses interventions et maintenances. Cela a permis d'acquérir des expériences professionnelles dans le domaine de maintenances des services informatiques et du parc mais également dans le domaine du travail en général. Et les interactions avec le personnel ont également été bénéfique pour l'adaptation aux échanges interpersonnels et l'accoutumance du milieu actif.

Mots Clés: Active Directory, Administration, Replication, VPN, Windows Server

ABSTRACTS

Summary, the establishment of Active Server of the Active Directory, mentioning the presentation, installation and configuration of the services used, in order to ensure the proper functioning of the services. The deployment of the routing and remote access server will allow remotes clients to access company services, through a secure tunnel, without using client workstation in the main domain.

During the internship, apart from the implementation of the project, I worked as an assistant, participating in many interventions and maintenances. That made me possible to acquire professional experience in the field of maintenances of IT services and also in the field of work in general. Interactions with staff were also beneficial for interpersonal exchanges adaptation and getting used to work environment.

Keywords: Active Directory, Administration, Replication, VPN, Windows Server