République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique

Option

Administration et Sécurité des Réseaux

Thème

Configuration sécurisée d'un contrôleur de domaine pour une gestion centralisée des utilisateurs au sein d'une entreprise cas « Tchin-Lait»

Réalisé par :

ADJOUADI Ouardia

IKHLEF Yasmina

Devant le jury:

Président : M[r] TOUAZI Djoudi

Examinateur : M[r] AISSANI Sofiane

Examinatrice : M[me] SAADI Nora

Promoteur : M[r] BAADACHE Abderahmane

Promotion: 2016/2017

Remerciements

Nous remercions Dieu le tout puissant de nous avoir donné la force nécessaire et la patience qui nous a permis de mener à bien ce modeste travail ;

Nous tenons à remercier :

Particulièrement nos familles et nos amis(es) qui ont su nous soutenir, nous encourager, nous aider et nous supporter tout au long de l'année.

Nous exprimons notre profonde reconnaissance à notre promoteur Mr BAADACHE Abderahmane pour son suivit, ces encouragements et sa disponibilité toute au long de la réalisation de notre mémoire.

Non sincères remercîments vont à Mr BAROUDJI Raid et à Mr MERRABETTE nos encadreurs de l'entreprise Tchin-Lait CANDIA, pour leur encadrement avec patience. Leur encouragement et leurs remarques pertinentes nous ont permis de mieux structurer ce travail. Nous les remercions aussi de nous avoir fait profiter de leurs expériences, leurs orientations et leurs conseils nous ont énormément aidés.

Nous remercions également notre président TOUAZI Djoudi de nous avoir fait l'honneur de présider notre jury, ainsi que l'examinateur Mr AISSANI Sofiane et l'examinatrice Melle SAADI Nora pour avoir accepter d'examiner notre travail.

En fin nous exprimons nos vifs remerciements, et notre profonde gratitude à la promotion M2 informatique, ainsi à l'égard de tous ceux qui ont contribués de prés ou de loin à la réalisation de ce travail.

Merci

Dédicaces

Je dédie ce modeste travail à :

A l'homme de ma vie, mon exemple eternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, qui éclaire mon chemin et m'illumine de douceur et d'amour, que dieu te garde pour nous PAPA.

A ma très chère maman en signe d'amour, de reconnaissance et de gratitude pour tous les soutiens et les sacrifices dont elle a fait prévue à mon égard.

A mon frère qui a tout fait pour m'encourager durant toutes mes études, et sa femme Ghania.

Aux êtres chers auxquelles je ne saurais exprimer ma gratitude et ma reconnaissance, mes sœurs Zahra et Souad et leurs maris.

A la prunelle de mes yeux, mes niéces Alouiz et maylisse, mes neveux Youdass et Maxime-massillasse, qui sont la lumière de la maison.

Aussi à un homme, une personnalité brillante, qui m'a toujours inspiré fort de ses qualités et de son parcours et qui est pour moi un modèle, il s'agit de mon fiancé Yazid qui m'a toujours soutenue dans la vie, et à toute sa famille.

A ce qui j'aime beaucoup, qui m'ont toujours soutenus et étaient toujours à mes cotés, mes chères amies spécialement : Katia, Miha et Celia.

A les personnes que j'ai passé des beaux moments avec eux, qui étaient toujours à mes cotés, mes copines de chambres : Hanane, Nedjma et sara.

A ma binôme et à toute sa famille.

Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

Ouardia

Dédicaces

Je dédie ce mémoire à :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

Mon mari, l'homme de ma vie qui m'a toujours soutenu qui m'a offert tous les moyens pour réussir, son amour sa gentillesse source de mon bien être.

Mon frère et mes deux sœurs qui n'ont cessé d'être pour moi des exemples de générosité.

Ma binôme, pour sa sympathie et son sérieux.

Mes professeurs de l'université qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

Yasmina

Table des matières

Table des figures

Liste des tableaux

Glossaire

AD *Active Directory*
Service d'annuaire inclus dans Microsoft Windows. Il stocke des informations sur les objets d'un réseau et met celle-ci à la disposition des utilisateurs et des administrateurs réseau.

DHCP *Dynamic Host Control Protocol*
Permet de configurer une machine de manière automatique à son démarrage.

DMZ *DeMilitarized Zone*
Correspond en informatique à un sous-réseau encadré de pare-feu, situé généralement entre le réseau local et l'Internet. Cet emplacement héberge les serveurs qui seront accessibles depuis l'Internet en passant le pare-feu externe généralement au travers d'un mécanisme de translation d'adresses ou de port.

DNS *Domain Name Système*
Service disponible dans un environnement TCP/IP permettant de résoudre des noms du type www.eni.fr en adresse IP.C'est le service d'annuaire « machines » de l'Internet.

FTP *File Transfer Protocol*
Est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP.

HDLC *High-level Data Link Protocol*
Est un protocole de niveau 2 (couche de liaison) du Modèle OSI, son but est de définir un mécanisme pour délimiter des trames de différents types, en ajoutant un contrôle d'erreur.

HTTP *Hyper Text Transfer Protocol*
Protocole de transfert de fichiers permettant d'acheminer tous types d'informations.

ICMP *Internet Control Message Protocol*
Protocole Internet permettant de véhiculer des messages d'erreur et autres informations.

ISO Organisme de normalisation mondialement reconnu, l'origine de très nombreuses normes.

LAN *Local Area Network*
Réseau à l'étendue géographique limitée.

MAN *Metropolitan Area Network*
Réseau dont l'étendue géographique est relativement importante, à l'échelle d'une ville.

NAT *Netrwork Address Translation*
Mécanisme qui permet de traduire systématiquement les datagrammes en modifiant les en-têtes IP, voire TCP et UDP pour protéger les postes de l'intranet.

OSI *Open System Interconnection*
Modèle de sept couches de référence de l'ISO.

SARL *Statut de la société à Responsabilité Limitée*
Comme son nom l'indique, la Sarl est une société qui se caractérise par la responsabilité limitée des associés : leur perte potentielle se limite au montant de leurs apports respectifs. Il s'agit de la forme de société la plus répandue en France.

SMTP *Simple Mail Transfer Protocol*
Est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

SSH *Secure Shell*
est à la fois un programme informatique et un protocole de communication sécurisé.

TCP/IP *Transmission Control Protocol/ Internet Protocol*
Familles de protocoles mondialement connue, indépendante de la couche Physique utilisée.

UDP *User Datagram Protocol*
protocole de la couche transport de la pile TCP/IP proposant un mode non fiable.

VPN *Virtual Private Network*
Connexion privée (c'est –à-dire protégée, dont le contenu des échanges est chiffré) en général sur un réseau public(tel qu'Internet).

WAN *Wide Area Network*
Terme désignant un réseau étendu géographiquement.

WDS *Wireless Distribution System*
Un système permettant l'interconnexion de plusieurs points d'accès sans fil. Il désigne également l'interconnexion sans fil entre les points d'accès Wi-Fi.

WINS *Windows Internet Naming Service*
Service dynamique permettant de r2soudre en inter-réseau les noms NetBIOS en adresse IP.

WMS *Warehouse Management System*
Une catégorie de progiciels destinés à gérer les opérations d'un entrepôt de stockage.

Introduction générale

Avec l'arrivée de l'internet, le savoir-faire de l'administration des réseaux informatiques évolue sans cesse et il s'affirme aujourd'hui comme une activité-clé de toute entreprise. En plus d'être constamment en fonction, ces outils d'échange de données et de partage d'information en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve.

La mise en place d'une infrastructure réseau comportant un service d'annuaire géré par un contrôleur de domaine ou plusieurs deviens une nécessité dans la mesure, ou on veut gérer en même temps les données des utilisateurs et les accès utilisateurs à ces données. L'enjeu principal d'un contrôleur de domaine, est de pouvoir réglementer les accès aux ressources du réseau tant à partir du réseau local qu'à l'extérieur, tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations afin d'accroître la sécurité du réseau local.

Dans le but de permettre une meilleure gestion des utilisateurs et des droits d'accès, plusieurs solutions se sont présentées. C'est dans ce cadre que nous somme choisie le Windows server 2012 de Microsoft pour sa convivialité, son niveau de sécurité et de sa flexibilité. Afin de mettre en place un serveur contrôleur de domaine qui permettra de résoudre les problèmes constatés à notre organisme d'accueil Tchin-lait « Candia».

Ce mémoire sera subdivisé en quatre chapitres dont le premier sera consacré à présenter des généralités sur l'administration et la sécurité des réseaux informatique.

Dans le deuxième chapitre, nous intéressons à la description de l'environnement de notre travail, en outre, notre organisme d'accueil qui est l'entreprise Tchin-Lait «Candia » dans laquelle nous avons effectué notre stage.

Par la suite, le troisième chapitre qui présente une vue générale sur l'Active Directory tout en présentant ces concepts fondamentaux.

Enfin, dans le dernier chapitre nous le consacrons pour la réalisation de notre travail, qui consiste à la description des étapes suivie pour l'installation et la configuration de Windows server et ses différents services, ainsi que les étapes à suivre pour l'utilisation de ces derniers.

Chapitre I

Généralités sur Administration, Sécurité et Réseau informatique

Introduction

Ce chapitre est une introduction aux réseaux informatiques, leur classification, topologies, architectures et leurs objectifs. Ensuite, nous introduirons quelques notions de la sécurité informatique telle que menace, sécurisation de l'interconnexion de réseaux (routeur filtrant, Nat, pare-feu, proxy et la zone démilitarisée). Enfin, nous parlerons sur administration des systèmes et des réseaux informatiques.

I. Généralités sur les réseaux informatiques

Un réseau informatique est un ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

L'ensemble de ces moyens matériels et logiciels permet de faire circuler des données informatiques et ainsi échanger du texte, des images, de la vidéo ou du son entre chaque équipement, selon des règles et des protocoles bien définit. **[1]**

I.1. Objectifs des réseaux

Beaucoup d'organisations ont un nombre important d'ordinateurs souvent fort distants, l'intérêt de l'interconnexion de ces ordinateurs est résumé dans les points suivants :

- Le partage de fichiers et de périphériques ;
- La communication entre personne grâce au courrier électronique et à la vidéo conférence ;
- La décentralisation de la gestion de l'information, par exemple : les bases de données distribuées ;
- Le contrôle à distance tel que l'assistance médicale et les systèmes de sécurité domotiques.

I.2. Architecture des réseaux

Le transfert d'information entre deux logiciels informatiques sur deux équipements réseaux différents se base sur deux modèles théoriques : le modèle OSI et le modèle TCP /IP. Dans cette partie nous définissons ces deux modèles comme suit :

I.2.1. Modèles OSI

OSI signifie *Open Systems Interconnection*, ce qui se traduit par *Interconnexion de systèmes ouverts*. Ce modèle a été mis en place par l'ISO afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs. Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

Le modèle OSI est composé de 7 couches d'abstractions qui répondent aux critères suivants:

- *Couche physique* : Assure le transfert de bits, on trouve dans cette couche :

- L'étude des interfaces de connexion.
- L'étude des modems, des multiplexeurs et concentrateurs.

➢ *Couche liaison de données* : Responsable de l'acheminement d'unités de données appelées trames en assurant la meilleure qualité de transmission possible. Le protocole standard est HDLC.

➢ *Couche réseaux* : Transporte des unités de données de taille fixe appelée paquets.

➢ *Couche transport* : Transport des unités de données appelées messages. Le protocole TCP et UDP et TCP/IP.

➢ *Couche session* : Assure l'établissement et le contrôle de séances de communication.

➢ *Couche présentation* : Présentation globale et unifiée de l'information, interprétation, cryptage, compression de données.

➢ *Couche Application* : Application spécifiques, comme Telnet, FTP, SSH…. **[17]**

I.2.2. Modèle TCP/IP

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fractionnement des messages en paquets ;
- L'utilisation d'un système d'adresses ;
- L'acheminement des données sur le réseau (routage) ;
- Le contrôle des erreurs de transmission de données.

Nous décrivons brièvement chacune des 4 couches du modèle TCP/IP :

➢ *La couche accès réseau*

Cette couche regroupe les couches physiques et liaison de données du modèle OSI.

✓ *La couche Internet*

Le but de cette couche est de permettre d'injecter des paquets dans n'importe quel réseau et de faire en sorte qu'ils arrivent à destination.

➢ *La couche Transport*

Tout comme pour le modèle OSI, la couche de transport permet aux hôtes source et destination de faire une conversation.

➢ *La couche Application*

Le modèle TCP/IP n'a pas besoin des couches Session ni Présentation. La couche application contient des protocoles haut-niveaux : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine. **[18]**

I.3. Protocoles réseaux

Un protocole réseau est un ensemble de règles et de procédures de communication utilisées de part et d'autre par toutes les stations qui échangent des données sur le réseau.

I.3.1. Protocole DHCP

Un serveur DHCP (Dynamic Host Configuration Protocol ou protocole de configuration dynamique) a pour rôle de distribuer des adresses IP à des clients d'une maniere dynamique pour une durée déterminée.

- ✓ **Mode de fonctionnement**

  Lorsqu'une application cliente DHCP est lancée sur une machine non configurée, protocole TCP/IP est mis en action comme aucune adresse IP ne lui a été introduite. Le logiciel ne peu envoyer ou recevoir des datagrammes que par diffusion (broadcast). Lorsqu'un client DHCP initialise un accès à un réseau TCP/IP.

- ✓ **Avantages de DHCP dans l'administration d'un réseau**

- Offre une configuration de réseau TCP/IP fiable et simple ;
- Facilite la configuration des machines portables ;
- Economie d'adresse.

I.3. 2. Serveur DNS

DNS (Domain Name Service). Un server DNS (Unix, Windows, AS400...) associe des noms aux adresses IP des terminaux ou des PCs. L'utilisation d'un serveur DNS simplifie la gestion du réseau car les utilisateurs ont simplement besoin de connaître le nom des machines sans se préoccuper des adresses IP.

- ✓ **Avantages**
  - Existence d'un cache DNS qui accélère la recherche des noms ;
  - Possibilité d'en avoir plusieurs sur différents serveurs afin de garantir son service en cas d'arrêt d'un des serveurs ;
  - Fiabilité de mise en place ;
  - Une entreprise peut disposer de son propre DNS. **[5]**

I.4. Adressage réseau

Une adresse IP est constituée de deux parties : l'adresse du réseau et l'adresse de la machine, elle permet donc de distinguer une machine sur un réseau. Deux machines se trouvant sur un même réseau possèdent la même adresse réseau, mais pas la même adresse machine.

On distingue deux situations pour assigner une adresse IP à un équipement :

1. **De manière statique** : l'adresse est fixée et configurée le plus souvent manuellement puis stockée dans la configuration de son système d'exploitation.
2. **De manière dynamique** : l'adresse est automatiquement transmise et assignée grâce au protocole DHCP.

I.5.Sécurité des réseaux informatiques

Comme des informations confidentielles circulent dans les réseaux, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

I.5.1. Définition

C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles, auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées

uniquement dans le cadre où il est prévu qu'elles le soient. Les exigences fondamentales de la sécurité Informatiques se résument à assurer:

- ✓ **Disponibilité** : L'information sur le système doit être toujours disponible aux personnes autorisées.
- ✓ **Confidentialité** : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- ✓ **Intégrité** : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées. **[6]**

I.5.2. Menaces informatiques

Les systèmes et les réseaux informatiques sont confrontés à des menaces intempestives qui peuvent endommager sérieusement un système (ou un réseau), ses services ou ses informations. Une attaque est une action qui compromet la sécurité des informations tandis qu'une menace informatique est la possibilité de mener à bien de telles attaques. Parmi les menaces courantes, nous relevons : le refus de service (déni de service), l'interception, la manipulation, l'identité et la répudiation.

Les attaques réseau peuvent être classées en deux grandes catégories :

- *les attaques passives* consistent à écouter sans modifier les données et /ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.

- *les attaques actives* consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau et/ou à perturber le bon fonctionnement d'un réseau.

Il existe une deuxième classification des attaques selon l'effet qu'elle causent.Elle comprend :

- *l'interruption* des services d'un réseau qui constitue un danger sur la disponibilité du système ;

- *l'interception* du trafic véhiculé sur le réseau par une entité non autorisée ; elle constitue un danger pour la confidentialité ;

- *la modification* du trafic véhiculé ; ceci constitue un danger pour l'intégrité des données ;

- l'injection du trafic dans le réseau ; ceci constitue un danger pour l'authenticité des données. **[7]**

I.5. 3. Sécurisation de l'interconnexion de réseaux

Il est devenu très rare que le réseau local de l'entreprise soit isolé. Son interconnexion avec internet, ou tout autre réseau, est devenue chose courante. Il est donc nécessaire de protéger les entrées et sorties sur le réseau interne privé. Différents équipements peuvent être mis en place pour réaliser cette sécurisation, Parmi eux nous sélections :

I.5.3.1. Routeur filtrant

Les mécanismes de filtrage qui peuvent être associés à l'équipement routeur autorisent des analyses de la couche3 (réseau) du modèle OSI.

L'examen des paquets entrants ou sortants porte ainsi, par exemple, sur l'entête IP, ce qui permet des actions comme :

_ Le blocage d'adresses IP (source et destination).

_ L'interdiction de transmission de protocoles de couche Réseau ou Transport utilisés (UDP, TCP, ICMP)… **[8]**

I.5.3.2. Translateur d'adresse

La technique de translation d'adresses (NAT en anglais) est une pratique courante qui est apparue à l'origine pour palier au manque croissant d'adresses IPv4 libres. En effet, ces adresses sont codées sur 4 octets et sont du type 0.0.0.0 à 255.255.255.255 (certaines valeurs étant réservées et par conséquence inutilisables); il y a donc peu d'adresses disponibles en comparaison du nombre croissant de machines sur Internet. Il fut donc décidé de réserver des intervalles d'adresses à des usages privés uniquement. Ce sont les adresses :

- ✓ **10.0.0.0 - 10.255.255.255**
- ✓ **172.16.0.0 - 172.31.255.255 (172.16/12prefix)**
- ✓ **192.168.0.0 - 192.168.255.255 (192.168/16prefix)**

En conséquence, ces adresses ne sont pas routables sur Internet et ne doivent pas être utilisées par des machines de ce réseau. Par contre, tous les réseaux privés peuvent utiliser ces adresses sans restrictions. Comme ces adresses ne sont pas routables sur le réseau public, la translation d'adresse est utilisée pour permettre aux machines du réseau privé d'accéder à Internet, et de façon générale à d'autres réseaux. Le principe de base est simple puisqu'il s'agit de remplacer à la volée les champs d'adresses dans les paquets qui sont destinés à un autre réseau (ce qui implique que le NAT soit effectué entre les 2 interfaces réseau, entre le réseau privé et les autres). **[8]**

I.5.3.3. Pare-feu

Un pare-feu ou coupe-feu (firewall) est comme son nom l'indique, un équipement dont l'objectif est de séparer le mode extérieur du mode intérieur à protéger. Son rôle est de laisser entrer que les paquets dont l'entreprise est sûre qu'ils ne posent pas de problème.

Les pare-feu offrent de nombreuses fonctions dont la principale est de trier ce qui entre et ce qui sort et de décider d'une action lorsque la reconnaissance a été- effectuée. Les actions peuvent du rejeter du paquet à sa compression-décompression en passant par son examen par un antivirus, son accélération, etc. **[8]**

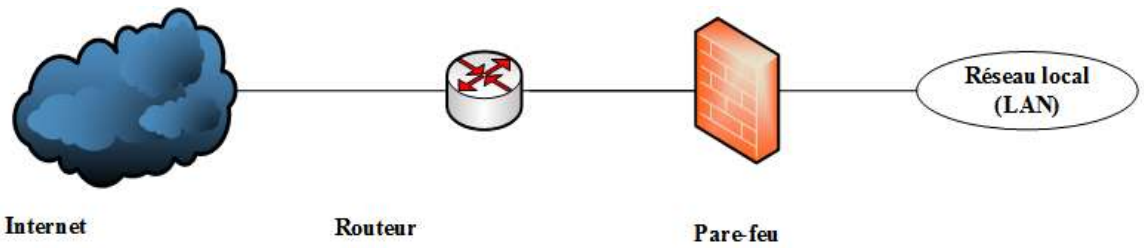


Figure I-1 : Par-feu.

I.5.3.4. Proxy

Le serveur mandataire, ou proxy, est particulièrement utilisé dans le cadre de trafics *Hyper Text Transfer Protocol* (HTTP), voire *File Transfer Protocol* (FTP) entre le réseau LAN et l'internet. Nous pouvons considérer qu'il complète l'équipement pare-feu.

Interceptant une demande vers l'extérieur, le proxy la fait en son propre nom, puis stocke les données renvoyées. Ensuite, il les retransmet au demandeur initial. L'intérêt du proxy est double. Tout d'abord, il camoufle les adresse IP internes, puisque la demande n'est pas prolongée jusqu'à l'Internet. Ensuite, il autorise des filtrages, par exemple pour interdire l'accès à certains sites web.

Un troisième avantage du proxy est sa capacité à gérer une mémoire cache. Ainsi, il est possible d'éviter de redemander un fichier ou un site sur internet. Au niveau web, une telle fonction est à relativiser. En effet, un site dynamique change tellement régulièrement qu'on peut souvent considérer qu'il est rechargé à chaque demande. **[8]**

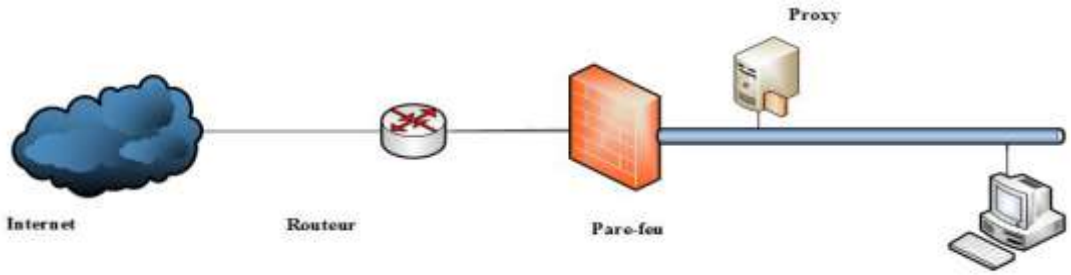


Figure I-2 : Proxy.

I.5.3.5. Zone démilitarisée

L'interconnexion entre le réseau public Internet et le LAN utilise très souvent une zone publique tampon, hébergée dans l'entreprise. Ce sas est nommé zone démilitarisé ou DeMilitarized Zone (DMZ). Elle héberge différents serveurs accessibles depuis l'Internet, tels que :

- Serveur proxy.
- Serveur web hébergeant le site de l'entreprise.
- Relais de messagerie, chargé de réaliser un tri des messages…

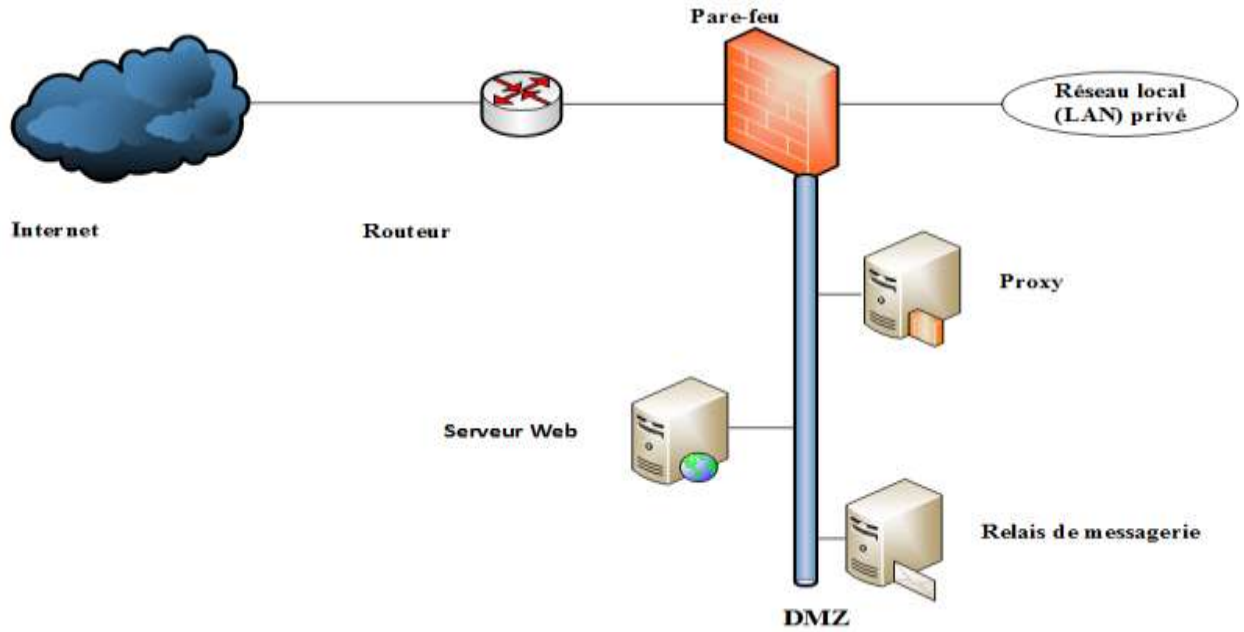


Figure I-3 : Zone démilitarisée.

La frontière de cette DMZ est concrétisée par au moins un pare-feu. Dans des infrastructures de petite taille, il est souvent unique. Dans ce cas, il est qualifié de tri résident. **[8]**

I.6. Administration des systèmes et des réseaux

L'administration des systèmes et des réseaux consiste à contrôler, cordonner et surveiller les différentes ressources mises en œuvre afin de fournir des services opérationnels aux utilisateurs : ces ressources sont les équipements, le réseau, les applications, Internet, les services offerts par les différents serveurs qui peuvent être :

- Accès aux données et aux ressources informatiques partagées (bases de données, annuaires, etc.) ;
- Consultation des sites Internet ;
- Accès au réseau informatique. **[9]**

I.6.1. Rôle d'un administrateur réseau

Le rôle d'un administrateur réseau consiste à :

- Mettre en place et maintenir l'infrastructure du réseau (organisation, . . .) ;
- Installer et maintenir les services nécessaires au bon fonctionnement du réseau ;
- Assurer la sécurité des données internes au réseau ;
- S'assurer que les utilisateurs n'outrepassent pas leurs droits ;
- Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, . . .) ;
- Sauvegarder les données ;
- Contrôler l'accès au réseau (accès interne, accès à distance et interconnexion avec des tierces parties);
- Surveiller et assurer la fiabilité générale du réseau. **[9]**

I.6.2. Objectifs de l'administration des réseaux pour un administrateur

Les objectifs de l'administration des réseaux pour un administrateur sont :

- Supervision du fonctionnement des réseaux ;
- Optimisation pour l'utilisation des ressources ;
- Détection et prévision des erreurs ;
- Signalisation des pannes ;
- Calculs de facturations à l'utilisation des ressources ;
- Support technique pour utilisateurs. **[9]**

Conclusion

Nous avons essayé à travers ce chapitre de mettre le point sur les réseaux informatiques, comment ils sont classés, leurs objectifs et topologies. Ainsi que, nous avons donné un aperçu sur ce qu'est la sécurité des réseaux et nous avons cité quelques équipements qui peuvent être mis en place pour réaliser cette sécurisation .Enfin, nous avons parlés sur l'administration des systèmes et des réseaux.

Après avoir discuté les principaux points de ce chapitre, nous allons passer à une autre partie « Présentation de l'organisme d'accueil », où nous présentons l'entreprise de Tchin-Lait, son histoire et situation géographique, son organisation et ses équipements.

Chapitre II

Présentation de l'organisme d'accueil

Introduction

Ce chapitre est consacré pour la présentation de l'organisme d'accueil qui nous a accueillies dans le cadre de notre stage de fin de cycle, afin de faire une configuration sécurisé d'un contrôleur de domaine pour centraliser la gestion des utilisateurs au sein de l'entreprise Tchin-Lait.

II.1. Présentation de l'unité Tchin- Lait « CANDIA»

Tchin-lait est une société privée de droit Algérien (SARL), fondée par M. Fawzi BERKATI (gérant de la société) en 1999, implanté sur l'ancien site de la limonaderie Tchin-Tchin. Cette dernière était à l'origine d'une entreprise familiale spécialisée dans les boissons gazeuses depuis 1952, ayant de fait une longue expérience dans le conditionnement des produits sous forme liquide.

C'est à l'arrivée des grandes firmes multinationales sur le marché des boissons gazeuses, qu'elle a révisée sa stratégie d'où l'idée de reconversion vers le lait UHT (Ultra Haute Température) qui a donné naissance à Tchin lait sous label « Candia », depuis mai 2001.

Cette laiterie construite sur une superficie totale de 6000 m^2, situé sur la route nationale n°12 à l'entrée ouest de la ville de Bejaïa (Bir-Slam). **[10]**

Figure II-1 : Carte géographique.

II.1.1. Organisation de TCHIN-LAIT

TCHIN-LAIT est une laiterie moderne, construite sur une superficie totale de 6000m^2, comprenant : une direction générale des sous directions (direction systèmes information, direction laboratoire, direction production, direction marketing et vente, direction finance et comptabilité, direction recherche et développement, direction ressources humaines et administration, direction technique) et des sites de stockages (annexe, BOUAOUADIA, SIMB,YAICI,BERAKI). **[10]**

Elle emploie 412 personnes (dont 29 femmes), 10% d'entre eux sont des cadres, 37% des agents de maîtrise et le reste sont des agents d'exécution.24/24 heures avec trois équipes de production :

- Première équipe, 5 heures du matin à 13 heures.
- Deuxième équipe, 13 heures à 21 heures.
- Troisième équipe, 21 heures à 5 heures du matin.

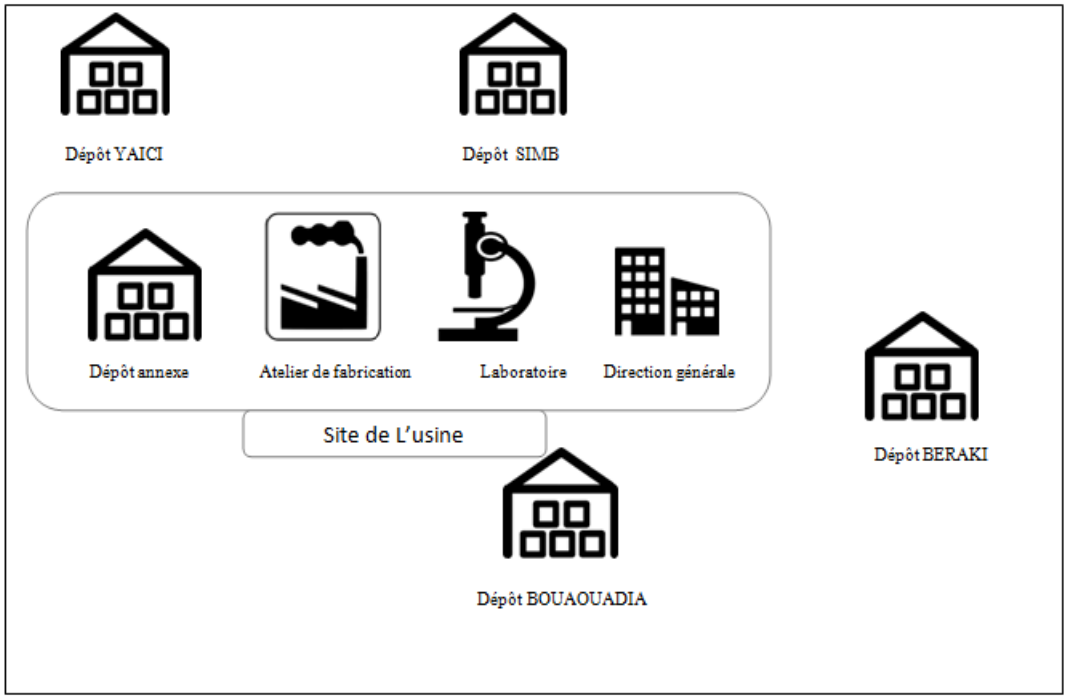


Figure II-2: Organisation de Tchin-Lait.

II.2. Description de l'organigramme Tchin-Lait

II.2.1. Direction finance et comptabilité

- Etablir tous les états financiers (bilans, tableau des comptes des résultats).
- Assure la bonne comptabilité générale.
- Etablir les listes planaires de tous les nouveaux projets.
- Gérer les dépense par département et par produit entrant dans le cadre du contrôle de gestion. **[10]**

II.2.2. Direction ressources humaines et administration

Cette section assure la gestion administrative des travailleurs et la gestion du personnel, tout en veillant aux relations avec les organismes extérieurs.

II.2.3. Direction laboratoire

Contrôle de la qualité du produit, à toutes les étapes de la production, de la matière première aux produits finis. Il existe deux laboratoires :

- Physico-chimie : contrôle des paramètres physico-chimiques du produit.
- Microbiologie : contrôle de stérilité du produit. **[10]**

II.2.4. Direction marketing et vente

Elle a pour mission d'établir le lien entre l'entreprise et son marché, cette section se compose de trois sous sections :

- Marketing : étude de marchés, lancement de nouveaux produit, publicité et communication.

- Force de vente : elle s'occupe de tout ce qui est prospection et promotion des ventes, elle a pour missions de relayer les actions marketing sur le terrain et veille concurrentielle.
- Centre de distribution : elle s'occupe du suivi des commandes clients et assure les expéditions et la bonne gestion des stocks produits finis. **[10]**

II.2.5. Direction production

Cette direction prend en charge l'ensemble des opérations liées à la production, maintenance, qualité, performance, hygiène et la sécurité. Ces opérations permettent la réalisation de produit selon les normes internationales. On distingue deux sections :

- Process : assure la bonne réception, reconstitution et traitement thermique du produit.
- Packaging : assure le bon conditionnement des produits finis, sur emballage (fardelage et palettisation). **[10]**

II.2.6. Direction technique

Elle s'occupe de l'entretient mécanique, électrique et électronique des machines de traitement et conditionnement du lait, de la gestion des stocks des pièces de rechange et de l'entretient des utilités (chaudières compresseurs bacs a eau glacées chambre froide, station de traitement des eaux). **[10]**

II.2.7. Direction systèmes d'information

La direction informatique de TCHIN-LAIT est située au deuxième étage de la direction générale. Elle contient la salle machine ou sont entreposé les armoires des serveurs et de brassage ainsi que les bureaux des responsables informatiques :

- Responsables des bases de données ;
- Responsables du système d'informations et de l'administration du réseau informatique ;
- Ingénieur support. **[10]**

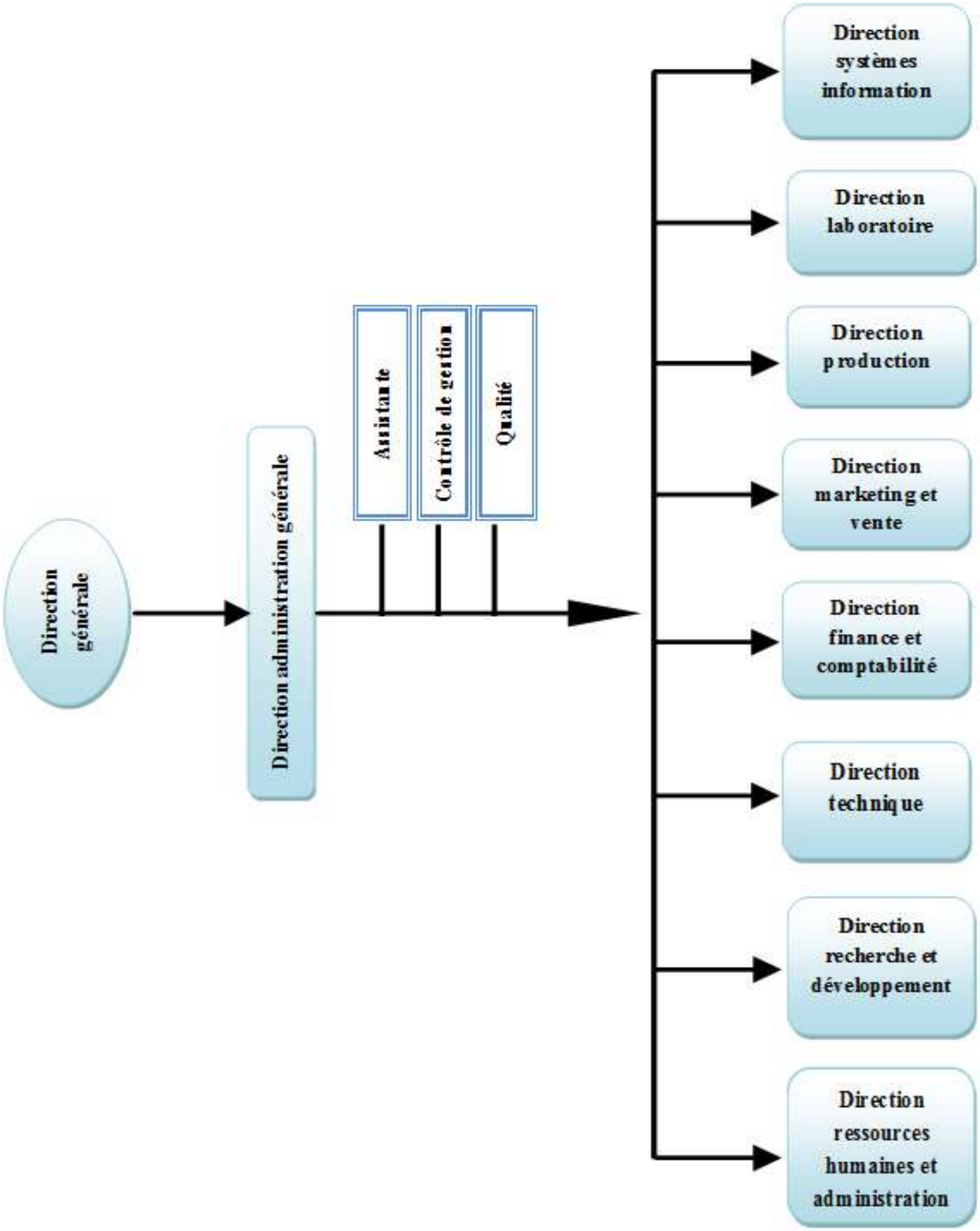


Figure II-3 : Organigramme de l'organisation de la laiterie TCHIN-LAIT

II.2.7.1. Architecture du réseau informatique Tchin-Lait

Tchin-Lait dispose d'un réseau de taille importante composé de 5 sites reliés par VPN et WDS. Il est constitué de plusieurs équipements, des Switch, des routeurs, des firewalls, pour la plupart de marque Cisco.

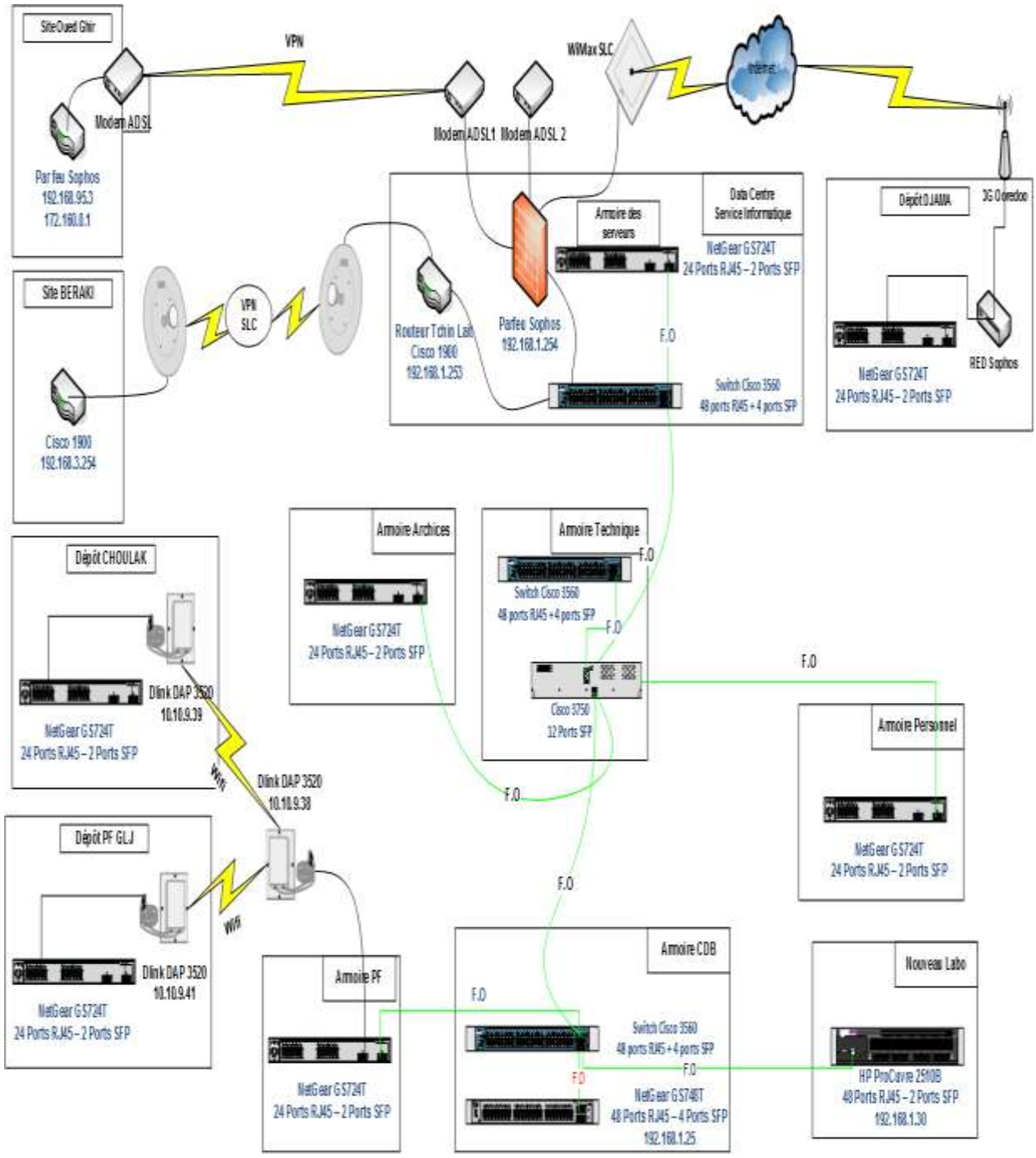


Figure II-4: Architecture du réseau informatique Tchin-Lait.

II. 2.7.2. Parc informatique Tchin-Lait

Le réseau Tchin-Lait contient un parc informatique composé d'une centaine ordinateurs (portables et bureaux), leurs configurations est illustré dans le tableau suivant :

Système d'exploitation	RAM	Processeur
Windows 7	4 GO	INTELL I3
Windows 10	2GO	INTELL Dual Core
Windows XP	2GO	INTELL Dual Core

Tableau II-1 : Configuration des ordinateurs de Tchin-Lait.

II. 2.7.3. Applications de Tchin-Lait

Les applications de Tchin-Lait sont diverses installées sur les serveurs contenu en salle machine, d'autres sur les machines des employées. Nous citons deux dans le tableau suivant :

Nom d'application	**Rôle**	**Description**
The Dude	Surveillance de réseau	The Dude est une application gratuite qui offre une très grande panoplie d'outils de surveillance de l'environnement réseau. Et en saisissant uniquement l'adresse d'une passerelle, The Dude est capable de dresser la carte de tous les composants réseau et d'en indiquer l'état ainsi que son Ping et éventuellement sa bande passante. Par simple glisser/déposer, il est possible de disposer les différents éléments selon leur configuration géographique et de les plaquer sur une carte pour une parfaite lisibilité.
WMS	Système de gestion d'entrepôts	C'est un logiciel qui sert a aider dans la gestion d'un entrepôt en utilisant les codes barre affecter aux lots de production, matières premières, etc.

Tableau II-2- Applications de Tchin-Lait.

II. 2.7.4. Serveurs Tchin-Lait

Un serveur est un dispositif informatique matériels et logiciels, qui offre des services à différents clients.

Les serveurs dont nous disposons dans le réseau de Tchin-Lait, présentent différentes caractéristiques énumérées comme suit :

Nom du serveur	**Rôle de serveur**	**Type de serveur**
Serveur FP	Serveur de base de données et fichiers partagés.	Serveur HP ProlLiant ML350p Gen8
Serveur VID	Serveur de vidéo surveillance.	Serveur HP ProlLiant ML350p Gen8
Serveur DOM	Contrôleur de domaines.	Serveur HP ProlLiant ML350p Gen8

Serveur DON	serveurde base de données(ERP).	Serveur HP ProlLiant ML350p Gen8
Serveur ENT	Serveur du système de gestion d'entrepôts.	Serveur HP ProlLiant ML350p Gen8
Serveur KAS	Serveur kaspersky.	Serveur HP ProlLiant ML350p Gen8
Serveur MES	Serveur messagerie.	Serveur HP ProlLiant ML350p Gen8
Serveur APP	Serveur qui contient quelques applications.	Serveur HP ProlLiant ML350p Gen8

Tableau II-3 : Serveurs du réseau Tchin-Lait.

II.2.7.5. Sites de stockages

Tchin-Lait se compose de plusieurs sites de stockages tels que site Usine, site Bouaoudia site de Simb, site de Yaici et site de Beraki ou sont stockés les produits finis qui sortes de la production et aussi les matières premières que vont être utilisées. Nous intéressons dans notre mémoire au site Usine qui est considéré comme la partie centrale du réseau.

Le site Usine se compose de trois sites à savoir : direction générale, service technique, annexe qui sont reliés entre eux par fibre optique.

- ***Liste des équipements de la direction générale***

1. ***Equipements d'interconnexion de la direction générale***

Nom d'équipement	Type d'équipement	Modèles
Forti Gate	Routeur	Cisco
Routeur Cisco	Routeur	Cisco
Switch serveurs	Switch	Switch Cisco
Cisco Informatique	Switch	Switch Cisco
WDS usine	Assiette wifi	Bridge wifi
WMS DG	Point d'accès	AP-Motorola

Tableau II-4: Equipements d'interconnexion de la direction générale.

2. ***Equipements terminaux fixes de la direction générale***

Non d'équipement	Type d'équipement	Modèles
CLP 620	DG Imprimante IP	SAMSUNG CLP 620
ZEBRA	Imprimante IP	ZEBRA

Tableau II-5 : Equipements terminaux fixes de la direction générale.

- ***Liste des équipements du service technique***
  1. ***Equipements d'interconnexion du service technique***

Non d'équipement	Type d'équipement	Modèles
Cisco fédérateur	Switch	Switch Cisco
Cisco Technique	Switch	Switch Cisco
Cisco DAG	Switch	Switch Cisco
NetGear Archives	Switch	Switch Cisco
WMS Usine 1	Point D'accès	AP-Motorola
WMS Usine 2	Point D'accès	AP-Motorola
WMS Usine 3	Point D'accès	AP-Motorola
WMS Usine 4	Point D'accès	AP-Motorola
WMS Usine 5	Point D'accès	AP-Motorola

Tableau II-6: Equipements d'interconnexion du service technique.

  2. ***Equipements terminaux fixes du service technique***

Non d'équipement	Type d'équipement	Modèles
Prod 1	Imprimante IP	ZEBRA
Prod 2	Imprimante IP	ZEBRA
ML2850 Technique	Imprimante IP	SAMSUNG 2850
CLP620 Personnel	Imprimante IP	SAMSUNG CLP 620
MFC7460 DAG	Imprimante IP	BROTHER 7460
ML3470 Chefs	Imprimante IP	SAMSUNG 3470

Tableau II-7: Equipements terminaux fixes du service technique.

- ***Liste des équipements de l'annexe***
  1. ***Equipements d'interconnexion de l'annexe***

Non d'équipement	Type d'équipement	Modèles
Cisco CDB	Switch	Switch Cisco
Switch	Switch	Switch Cisco
Switch	Switch	Switch Cisco
ProCure Switch	Switch	Switch Cisco
AP DMV	Point D'accès	AP-Motorola
WMS CDB1	Point D'accès	AP-Motorola
WMS CDB2	Point D'accès	AP-Motorola
WMS CDB3	Point D'accès	AP-Motorola
WMS CDB4	Point D'accès	AP-Motorola
WMS CDB5	Point D'accès	AP-Motorola
WMS CDB6	Point D'accès	AP-Motorola
WMS CDB7	Point D'accès	AP-Motorola

Tableau II-8: Equipements d'interconnexion de l'annexe.

1. Equipements terminaux fixes de l'annexe

Non d'équipement	Type d'équipement	Modèles
ML3710 CDB	Imprimante IP	SAMSUNG 3710
Zebra CDB	Imprimante IP	ZEBRA
HL22370 DMV	Imprimante IP	BROTHER 2270
CLP660 DMV	Imprimante IP	SAMSUNG 660
CLP660 Appros	Imprimante IP	SAMSUNG 660
ML3710 GDS	Imprimante IP	SAMSUNG 3710
ML2850 DFC	Imprimante IP	SAMSUNG 2850
HL2270Idjraoui	Imprimante IP	BROTHER 2270
ML 3470 Bounia	Imprimante IP	SAMSUNG 3470
Pointeuse Annexe	Pointeuse	ZKSOFTWARE

Tableau II-9 : Equipements terminaux annexes.

II.3. Problématique

Dans les entreprises, tel que Tchin-Lait, échanger des informations devient une nécessité absolue. Malgré la complexité de gestion des ressources systèmes de l'administration réseaux, les besoins se multiplient pour élargir les tâches administratives de chaque entreprise quel que soit sa taille. Cependant la gestion des comptes utilisateurs est l'un des tâches absolument essentiels dévolus aux administrateurs pour assurer les problèmes de connexion, d'authentifier des utilisateurs, donner des droits d'accès. En effet, les ressources de l'entreprise tendent de plus en plus à une centralisation des informations.

L'administrateur réseau gère les postes de travail et les serveurs de l'entreprise, pour mettre en place les moyens et les procédures en garantissant les performances et la disponibilité des systèmes. Tchin-Lait

Pour une meilleure gestion des utilisateurs et des droits d'accès, Tchin-Lait utilise Windows server 2008.

Le problématique générale de notre travail portera sur: commet gérer tous les comptes des employés ainsi que les comptes des clients ,Comment donner l'accès aux documents et les partager entre les employés en utilisant une nouvelle version de Windows server.

II.4. Objectif

Notre objectif est de mettre en place un serveur contrôleur de domaine, qui sera en mesure de rependre aux critères habituellement utilisés par un administrateur réseau de Tchin-Lait, tels que :

-L'authentification des utilisateurs.

-La gestion de droits d'accès.

-Les partages des fichiers ou répertoires.

A l'issu de ce travail, nous serons en mesure de faire une configuration sécurisée d'un contrôleur de domaine, afin de centraliser la gestion des utilisateurs au sein d'une entreprise sous Windows server 2012.

Conclusion

La présentation de l'entreprise et l'étude de l'existant est une étape nécessaire pour voir les problèmes que Tchin-Lait fréquente (la gérance des comptes utilisateurs, d'accès à internet, des mails, des droits d'accès aux documents).

Windows server est un groupe de systèmes d'exploitation conçu par Microsoft, qui prend en charge la gestion au niveau de l'entreprise, le stockage de données, les applications et les communications. Ce logiciel va nous permettre de résoudre le problème de l'entreprise Tchin-Lait et de répondre à ces besoins.

Dans le chapitre suivant, nous allons présenter le service d'annuaire Active Directory, pour gérer les comptes utilisateurs et sécuriser en générale le réseau de l'entreprise.

Chapitre III

Service annuaire Active Directory

Introduction

Dans de grands réseaux, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre aux utilisateurs et aux applications d'accéder à ces ressources et aux informations les concernant, une méthode cohérente est nécessaire pour nommer, décrire, localiser, accéder, gérer et sécuriser les informations concernant ces ressources. Un service d'annuaire remplit cette fonction.

III .1. Service d'annuaire

Un annuaire est un moyen de stockage des informations. Un service d'annuaire comprend à la fois l'annuaire même et la méthode utilisée pour le stocker sur le réseau afin qu'il soit accessible à partir de tous les clients et serveurs. Les types d'informations stockées dans un annuaire peuvent être répartis en trois catégories :

- ressources ;
- services ;
- comptes.

Dans un réseau Windows Server (2000, 2003, 2008, 2012,…), le service d'annuaire s'appelle Active Directory. **[11]**

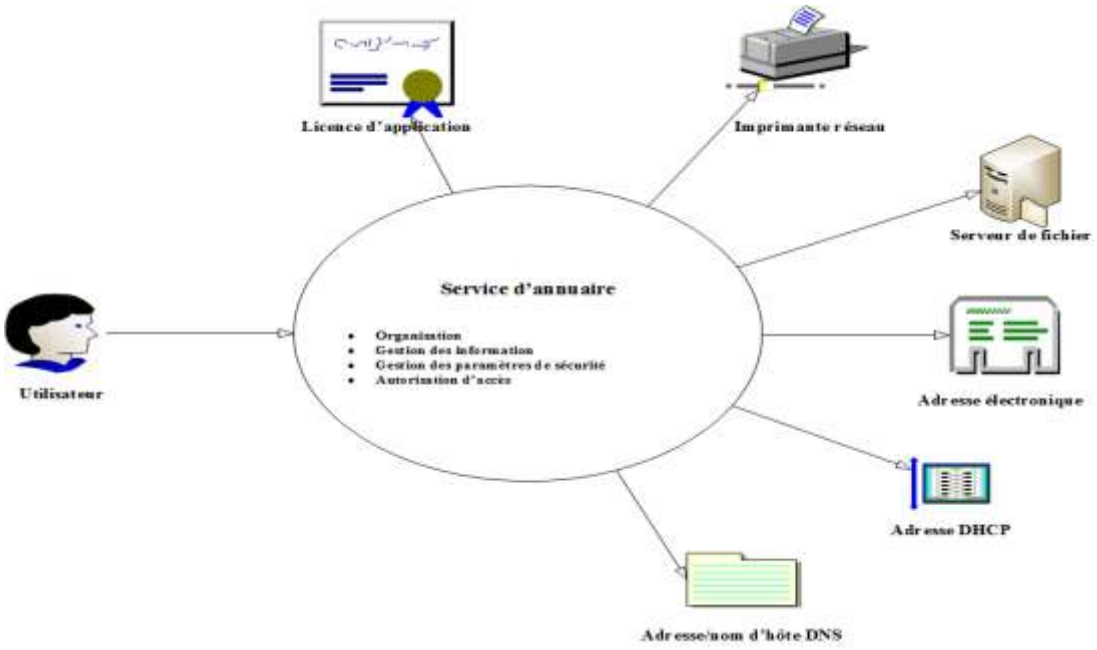


Figure III-1 : Structure d'un service d'annuaire.

III.2. Active Directory

Un Active directory est un rôle[1] disponible sur Windows Server qui permet la mise en place d'un service d'annuaire (d'utilisateurs, d'ordinateurs, etc.), et de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows (ex : création de session individuelles), il permet également l'attribution et

[1] Rôle : Collection nommée de tâches définissant les opérations disponibles sur un serveur.

l'application de stratégies de groupe (Interdiction : de changer de fond d'écran, d'installation d'applications ou de paramétrage en tout genre). **[16]**

Active directory s'appuie sur le protocole le plus connu du domaine LDAP (Lightweight Directory Access Protocol) pour l'interrogation des bases de données Active Directory. Ce protocole fonctionnant en TCP/IP, Microsoft a du utiliser cette pile de protocoles en standard et faire reculer au second plan ses protocoles historiques : NetBIOS, WINS, etc.

Les domaines qui utilisent les services Active Directory sont nommés domaines Active Directory. Si les domaines Active Directory ne peuvent fonctionner qu'avec un contrôleur de domaine, il convient de configurer plusieurs contrôleurs pour le domaine. Si un contrôleur tombe en panne, les autres prennent le relais pour gérer l'authentification et les autres tâches critiques. **[5]**

III.2.1. Famille Active Directory

Microsoft a regroupe la fonctionnalité d'annuaire et a créé une famille de services connexes qui comprend notamment :

- *Active Directory Certificate Services (AD CS).*

  Fournissent des services personnalisables pour l'émission et la gestion de certificats dans des systèmes de sécurité logicielle employant des technologies de clé publique. Pour obtenir des informations techniques d'ordre général à propos du chiffrement par clé publique et des avantages offerts par une infrastructure à clé publique (PKI).
- *Active Directory Domain Services (AD DS)*

  Les Services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine, y compris le magasin de données qui stocke les informations sur les objets du réseau et les met à la disposition des utilisateurs. Les Services AD DS font appel aux contrôleurs de domaine pour gérer l'accès aux ressources du réseau. Une fois que les utilisateurs s'authentifient en se connectant à un domaine, leurs informations d'identification stockées peuvent être exploitées pour accéder aux ressources du réseau. Comme les Services AD DS constituent le cœur d'Active Directory et qu'ils sont indispensables aux applications et technologies qui fonctionnent avec l'annuaire, nous emploierons simplement le terme Active Directory pour désigner les Services AD DS ou Services de domaine Active Directory.
- *Active Directory Federation Services (AD FS)*

  . Les services AD FS complètent les fonctionnalités d'authentification et de gestion d'accès des services AD DS en les développant pour le WWW. Les services AD FS font appel à des agents Web pour donner aux utilisateurs un accès aux applications Web et aux proxys, hébergés en interne, qui gèrent l'accès client. Une fois les services AD FS configurés, les utilisateurs emploient leur identité numérique pour s'authentifier sur le web et accéder aux applications Web hébergées en interne à l'aide d'un navigateur Web comme Internet Explorer.
- *Active Directory Lightweight Directory Services (AD LDS)*

  Fournissent un magasin de données pour les applications fonctionnant avec l'annuaire qui ne nécessitent pas les services AD DS et qui n'ont pas besoin d'être déployées sur des contrôleurs de domaine. Ce service ne fonctionne pas comme un service de système d'exploitation et il peut être utilisé autant dans des environnements de domaine que de groupe de travail. Chaque application qui s'exécute sur un serveur dispose de son propre magasin de données implémenté via les services AD LDS.

- *Active Directory Right Management Services (AD RMS)*

Permettent de renforcer la stratégie de sécurité d'une organisation en protégeant les informations en appliquant en permanence des stratégies d'utilisation aux informations, même ces dernières sont déplacées. Nous pouvons utiliser AD RMS pour renforcer la protection des informations sensibles, telles que les rapports financiers, les spécifications de produits, les données des clients et les messages électronique confidentiels, afin d'empêcher des personnes non autorisées d'avoir accès à ces information accidentellement ou non. **[5]**

III.2.2. Objets Active Directory

Active Directory stocke des informations sur les objets du réseau.

Chaque objet possède un ensemble d'attributs regroupant diverses informations permettant par exemple d'effectuer des recherches précises dans l'annuaire (trouver l'emplacement physique d'une imprimante, le numéro de téléphone ou l'adresse de messagerie d'un utilisateur, le système d'exploitation d'un serveur…).

Les principaux types d'objets que nous rencontrons sont :

- ***Serveurs :*** il s'agit des machines du réseau disposant d'un système d'exploitation Windows Server dont la version est un attribut.
- ***Domaines :*** pour chacun des domaines de notre forêt Active Directory, nous allons avoir un objet domaine (dans notre exemple *Candia.local*).
- ***Sites :*** les sites Active Directory permettent de définir une segmentation reflétant la topologie physique du réseau en se basant sur les sous-réseaux. Ainsi, deux sites de la même entreprise éloignés géographiquement et reliés par une liaison louée à faible débit pourront constituer deux sites Actives Directory : ceci permettra entre autres d'optimiser le trafic lié à la réplication des objets Actives Directory à travers la liaison.
- ***Utilisateurs :*** ces objets représentent ce que l'on dénomme communément les comptes d'utilisateurs (le compte utilisateur est en fait un attribut de l'objet utilisateurs, tout comme le mot de passe). Il s'agit des principales entités de sécurité administrées au sein d'Actives Directory.
- ***Groupes :*** ces objets facilitent l'administration d'Actives Directory. Ce sont des entités de sécurité dans les quelles nous retrouvons des utilisateurs, ordinateurs ou des groupes.
- ***Ordinateurs :*** Il s'agit des comptes d'ordinateurs rattachés à un domaine. Comme les utilisateurs, ce sont également des entités de sécurité auxquelles il est possible d'affecter des permissions.
- ***Imprimantes :*** Ce type d'objet représente une imprimante publiée dans l'annuaire Actives Directory. **[12]**

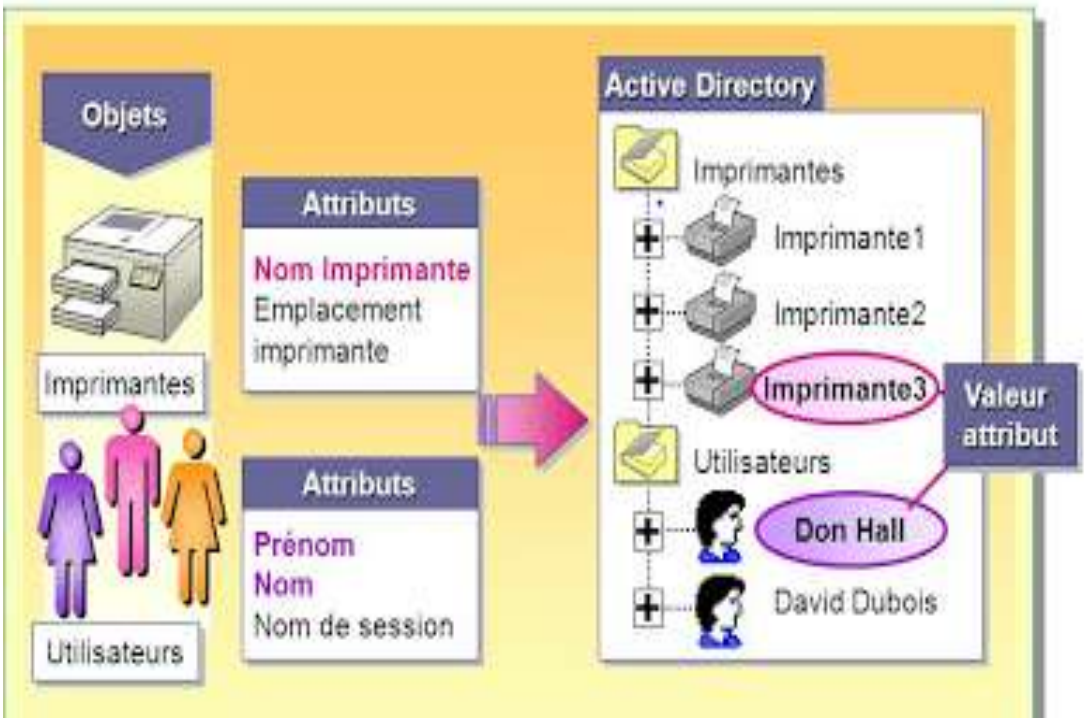


Figure III-2 : Objets Active Directory et leurs attributs.

III.2.3. Exploitation des structures de domaines

Active Directory fournit à la fois les structures logiques et physiques pour des composants réseau. Les structures logiques aident à organiser les objets d'annuaire et à gérer les comptes réseau et les ressources partagées. Les structures logiques incluent les éléments suivants :

- ***Unités d'organisation* :** sous groupes de domaines qui reflètent souvent la structure fonctionnelle ou professionnelle de l'organisation.
- ***Domaine (ou sous-domaine)* :** Groupe d'ordinateurs qui partagent la même base de données d'annuaire. Le domaine au sens de l'AD est le niveau le plus bas. Il contient au moins un contrôleur de domaine (Ldap + Kerberos). Il représente une organisation ou une partie d'une organisation.
- ***Arborescence* :** Un ou plusieurs domaines qui partagent un espace de noms contigu.
- ***Forêt :*** Ensemble d'arborescences qui appartient à la même organisation et partagent les même informations d'annuaire. Au choix de l'architecte réseau, deux arborescences peuvent appartenir à une même forêt ou pas. **[16]**

Exemple :

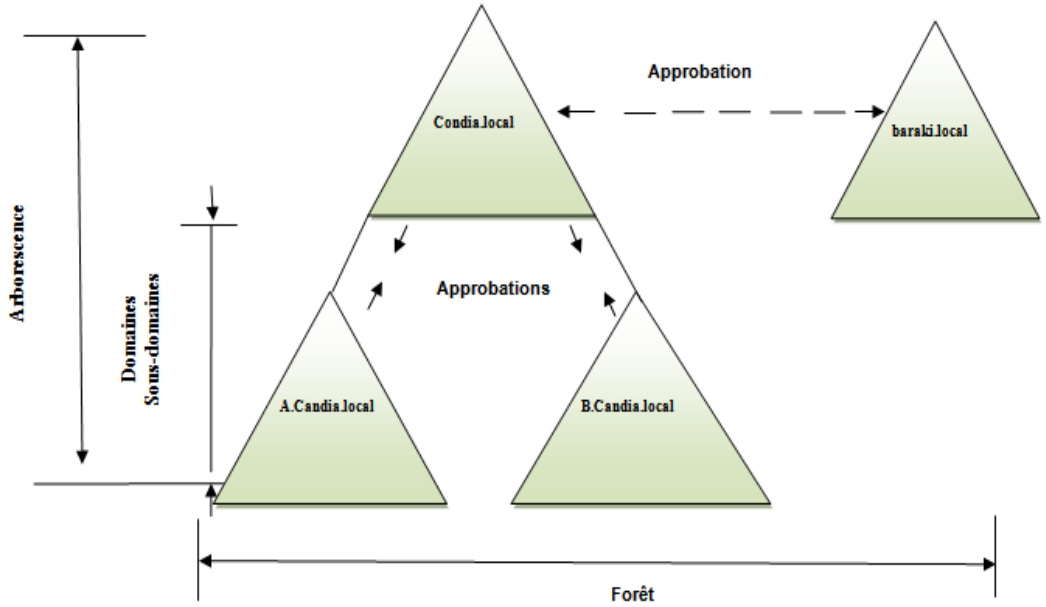


Figure III-3: Exemple sur les concepts d'organisation d'Active Directory.

Les structures physiques servent à faciliter la communication réseau et à définir des limites physiques des ressources réseau. Les structures physiques qui aident à mapper la structure du réseau physique incluent les éléments suivants :

- ***Sous-réseaux* :** groupes de réseaux avec une plage spécifique d'adresses IP et de masque réseau.
- ***Sites* :** un ou plusieurs sous-réseaux. Les sites servent à configurer la réplication et l'accès à l'annuaire. **[16]**

III.2.4. Fonctionnalités Active Directory

Active Directory dispose des fonctionnalités suivantes :

- *Accès pour les utilisateurs et les applications aux informations concernant des objets*. Ces informations sont stockées sous forme de valeurs d'attributs. Vous pouvez rechercher des objets selon leur classe d'objet, leurs attributs, leurs valeurs d'attributs et leur emplacement au sein de la structure Active Directory ou selon toute combinaison de ces valeurs.
- *Transparence des protocoles et de la topologie physique du réseau*. Un utilisateur sur un réseau peut accéder à toute ressource, une imprimante par exemple, sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.
- *Possibilité de stockage d'un très grand nombre d'objets.* Comme il est organisé en partitions, Active Directory peut répondre aux besoins issus de la croissance d'une organisation. Par exemple, un annuaire peut ainsi passer d'un serveur unique contenant quelques centaines d'objets à des milliers de serveurs contenant des millions d'objets.

- *Possibilité d'exécution en tant que service indépendant du système d'exploitation.* AD/AM (Active Directory in Application Mode) est une nouvelle fonctionnalité de Microsoft Active Directory permettant de résoudre certains scénarios de déploiement liés à des applications utilisant un annuaire. AD/AM s'exécute comme un service indépendant du

système d'exploitation qui, en tant que tel, ne nécessite pas de déploiement sur un contrôleur de domaine. L'exécution en tant que service indépendant du système d'exploitation signifie que plusieurs instances AD/AM peuvent s'exécuter simultanément sur un serveur unique, chaque instance étant configurable de manière indépendante. **[5]**

Le tableau suivant résume les fonctionnalités d'active Directory et ses avantages par apport à l'entreprise :

Fonctionnalités Active Directory	Avantages pour l'entreprise
Système de stockage réparti.	Stockage des données d'annuaire unifié nécessitant peu de tâches administratives.
Extensibilité de l'annuaire	Intégration d'applications tierces avec extension du schéma Active Directory.
Administration centralisée et délégation.	Contrôles des privilèges d'administration et des paramètres de sécurité de manière hiérarchique à l'échelle de l'entreprise.
Disponibilité des informations de l'annuaire, tolérance de panne, hautes performances.	L'annuaire peut être mis à jour à partir de tout contrôleur de domaine et ce, même lorsqu'un contrôleur de domaine est indisponible. La disponibilité et la gestion des flux de réplication sont contrôlées grâce l'ajustement dynamique de la topologie de réplication et au mode de réplication multi-maître. La structure de foret Active directory les arbres, les domaines et les contrôleurs de domaine – supporte des structures comportant des milliers de sites géographiques et des millions d'objets.
Gestion des configurations et des changements de configuration à l'aide de la technologie IntelliMirror.	Cohérences des paramètres appliqués et opérations réalisées grâce aux stratégies de groupe.
Services de sécurité à l'échelle des entreprises de toutes tailles via le support de Kerberos v5, SSL, TLS et les services de clés publiques (PKI).	Servies d'authentification et de contrôle des accès assurent une prise en charge au sein du réseau privé et aussi sur internet.
Gestion de la sécurité et délégation de gestion de l'administration.	Granularité descend jusqu'à l'attribut et l'étendue de management s'exerce sur les objets de types Site, Domaine et OU.
Support des standards de l'internet: un domaine Windows est un domaine DNS, un domaine d'authentification est un royaume Kerberos, les certificats sont utilisables de manière naturelle pour l'authentification.	Entreprise est assurée d'une pérennité de ses choix de par la participation active de Microsoft aux standards de l'industrie. TCP/IP, DNS, IPSec, DHCP,…

Tableau III-1 : Point Clés Qui caractérisent L'Active Directory.

III.2.5. Base de données Active Directory

Active Directory est un annuaire, il lui faut donc enregistrer les informations qu'il contient dans une base de données. Cette dernière est modélisée sous la forme d'un seul fichier, appelé **ntds.dit**, et localisé dans %systemroot%\NTDS\ntds.dit. L'extension de ce fichier, DIT, signifie Directory Information Tree, ou arborescence d'informations de l'annuaire. Cette base de données est basée sur la base *ESE* (Extensible Storage Engine), Elle peut stocker plusieurs millions d'objets.

Trois sections, ou partitions, composent donc la structure d'Active Directory. Ces sections sont appelées *Naming Contexts*, ou Contextes de Nommage. Ces trois contextes sont :

• Le *Domain Naming Context*, Contexte de Nommage du Domaine contient les informations qui, la majorité du temps, sont assimilées à Active Directory. C'est à dire la partie concrète de l'annuaire, les informations auxquelles Active Directory permet d'accéder, telles que la description des domaines et des Unités d'Organisation.

• Le *Configuration Naming Context*, Contexte de Nommage de la Configuration contient les informations concernant les sites, les sous-réseaux, les media de réplication, les permissions, les données de configuration du service de réplication de fichiers, du service Active Directory, ainsi que la configuration de divers autres services reposant sur Active Directory.

• Le *Schema Naming Context*, Contexte de Nommage du Schéma définit la structure abstraite d'Active Directory. Cette structure est extrêmement importante, c'est grâce à elle que les informations sont organisées de façon consistante à l'intérieur de l'annuaire. Y sont définis les structures et les types de données des objets et des propriétés contenus dans Active Directory. Un parallèle simple peut être fait entre le schéma d'Active Directory et la définition des classes d'un programme orienté objet. **[13]**

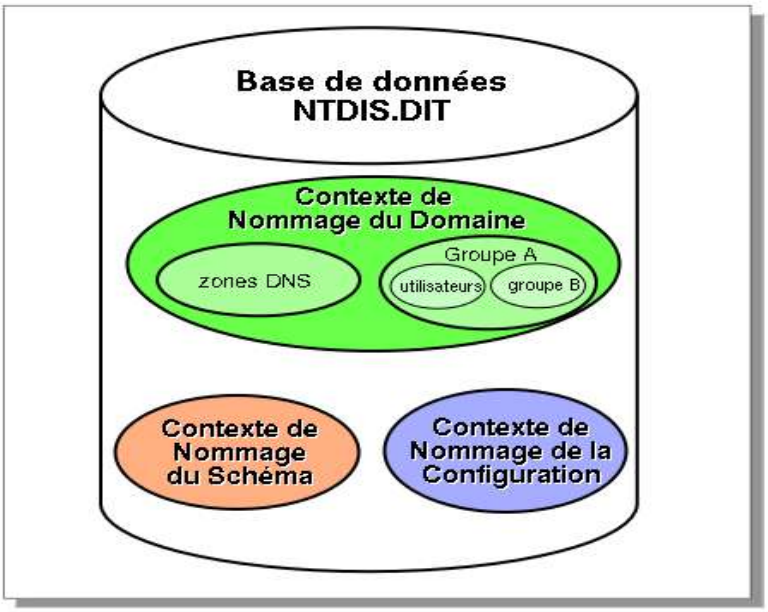


Figure III-4 : Contenu de la base de données Active Directory.

III.2.6. Définition d'un schéma Active Directory

Le schéma Active Directory contient les définitions de tous les objets, comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory.

Le schéma possède deux types de définitions : les classes d'objets et les attributs. Les classes d'objets comme utilisateur, ordinateur et imprimante décrivent les objets d'annuaire possibles que nous pouvons créer. Chaque classe d'objet est un ensemble d'attributs.

Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets. Par exemple, l'attribut **Description** est utilisé dans de nombreuses classes d'objets, mais il n'est défini qu'une seule fois dans le schéma afin de préserver la cohérence. **[12]**

III.2.7. Définition d'un catalogue global Active Directory

Le catalogue global ou GC (Global Catalog) est une liste de tous les objets d'un annuaire Active Directory. Il comprend assez d'informations pour qu'une réplique d'une partition Active Directory contenant l'objet recherché puisse être trouvée, sans que l'utilisateur ou l'application n'ait besoin de connaitre l'emplacement de l'objet dans la hiérarchie Active Directory. L'utilisateur ou l'application doit connaitre un ou plusieurs attributs de l'objet pour pouvoir effectuer une recherche. **[14]**

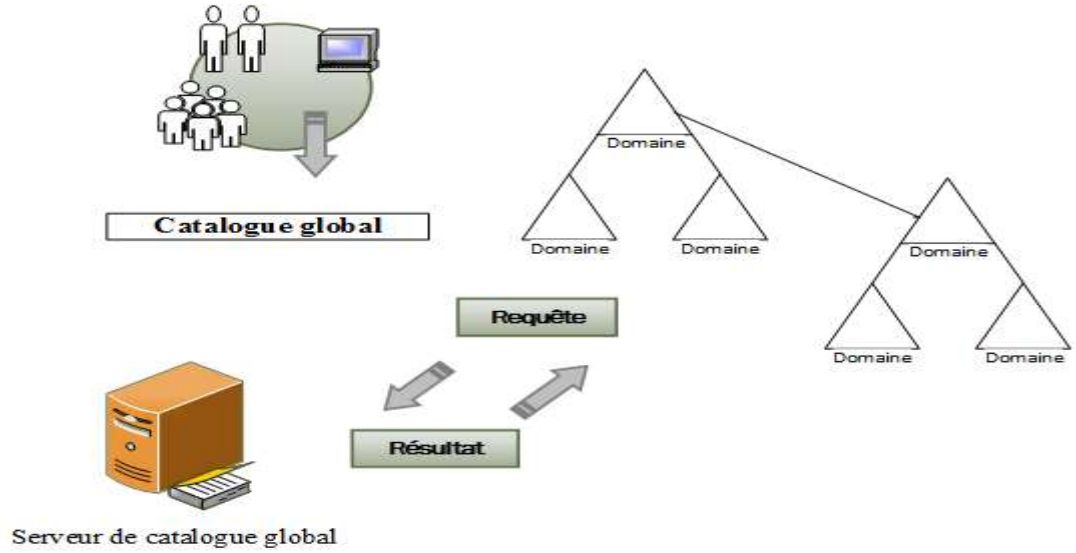


Figure III-5 : Catalogue global Active Directory.

III.2.8. Active Directory et DNS

Il est indispensable pour un contrôleur de domaine Active Directory de pouvoir contacter un serveur DNS compatible. Lorsqu'un serveur Windows est transformé en contrôleur de domaine, il doit avoir un serveur DNS à sa disposition. Si aucun serveur DNS n'est pas trouvé sur le réseau, le service DNS est installé par défaut sur le nouveau contrôleur de domaine.

Pour Active Directory, l'importance de service DNS se situe à deux niveaux :

a) Pour qu'un client puisse se connecter à Active Directory, le DNS doit être disponible pour localiser le contrôleur de domaine. Le service NetLogon nécessite

la présence d'un serveur DNS prenant en charge les RR SRV, ces derniers servant à enregistrer et à identifier les contrôleurs de domaine dans l'espace de noms DNS.

b) L'annuaire Active Directory peut stocker les informations de zone DNS et les propager dans l'entreprise. **[15]**

III.2.9. Active Directory et DHCP

Le service Serveur DHCP est intégrer dans Active Directory pour fournir l'autorisation pour les serveurs DHCP. Un serveur DHCP contrôleur de domaine ou membre d'un domaine Active Directory interroge Active Directory pour obtenir la liste des serveurs autorisés (identifiés par leur adresse IP). Si sa propre adresse IP ne figure pas dans la liste des serveurs DHCP autorisés, le service Serveur DHCP ne termine pas sa séquence de démarrage et se ferme automatiquement. **[15]**

Conclusion

Dans ce chapitre, nous avons présenté les concepts fondamentaux d'Active Directory, qui sont particulièrement nécessaire pour la suite de notre travail sur l'administration réseau sous Windows, et la mise en place d'un serveur contrôleur de domaine Active Directory de Microsoft.

Nous traiterons dans ce qui suit, la configuration d'Active Directory sous Windows serveur 2012 ainsi que les autres services requis : DNS et DHCP.

Chapitre IV

Réalisation

Introduction

Afin de bien mener notre objectif de mettre en place un serveur contrôleur de domaine Active Directory de Microsoft pour l'entreprise Tchin-Lait, nous irons détailler dans ce chapitre toutes les étapes de l'installation et la configuration de Windows server 2012 et ses différents services (Active Directory, DNS, DHCP).

Dans le cadre de notre travail, nous avons fait appel au logiciel VMware Workstation qui permet de simuler plusieurs machines.

IV.1. Installation et configuration de Windows server 2012 et ses différents services

Au premier lieu, nous allons introduire les différentes étapes à suivre pour installer et configurer Windows server, à la fin de cette installation, nous allons installer les différents services offerts par ce dernier.

IV.1.1. Windows server 2012

Installer un Windows Server 2012 est utile si l'on souhaite créer un domaine pour mettre en réseau des postes de travail. Ce serveur deviendra donc contrôleur de domaine, un rôle minimum qu'il convient de bien configurer. Dans le cas de l'unique serveur d'une petite entreprise, ce contrôleur de domaine aura les rôles de serveur Active Directory**,** serveur DNS et serveur DHCP.

- ✓ **Installation Windows server 2012**

L'installation de base est classique, nous bootons sur l'image ISO d'installation de Windows Server 2012.

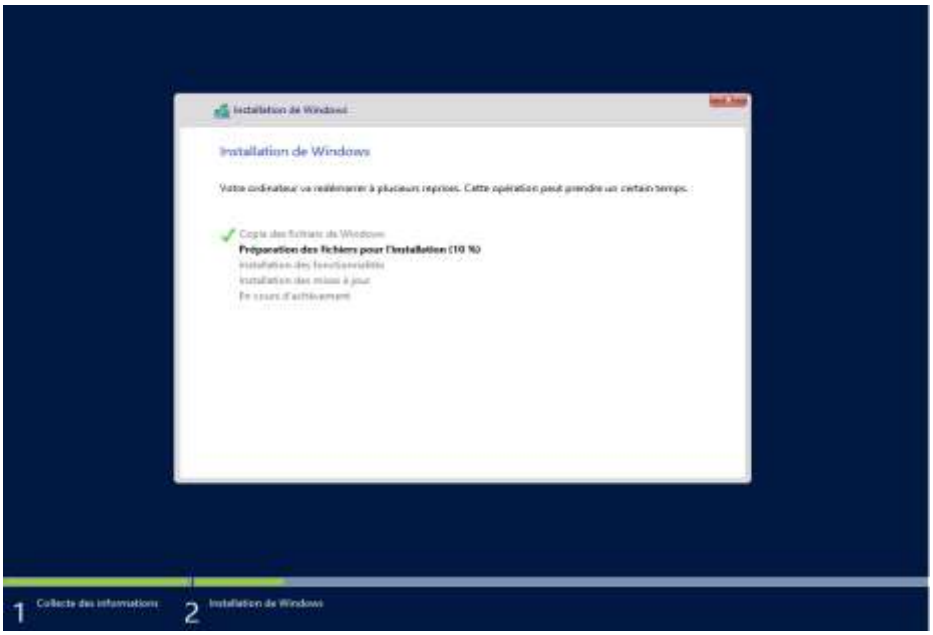


Figure IV-1 : Installation en cours.

Après redémarrage, il faut paramétrer la date et l'heure, Définissons un mot de passe pour le compte Administrateur. Il faut utiliser un mot de passe complexe pour répondre à la stratégie de complexité des mots de passe définie par défaut dans les éditions serveurs de Windows. Cliquons sur "**Terminer**" pour confirmer et continuer.

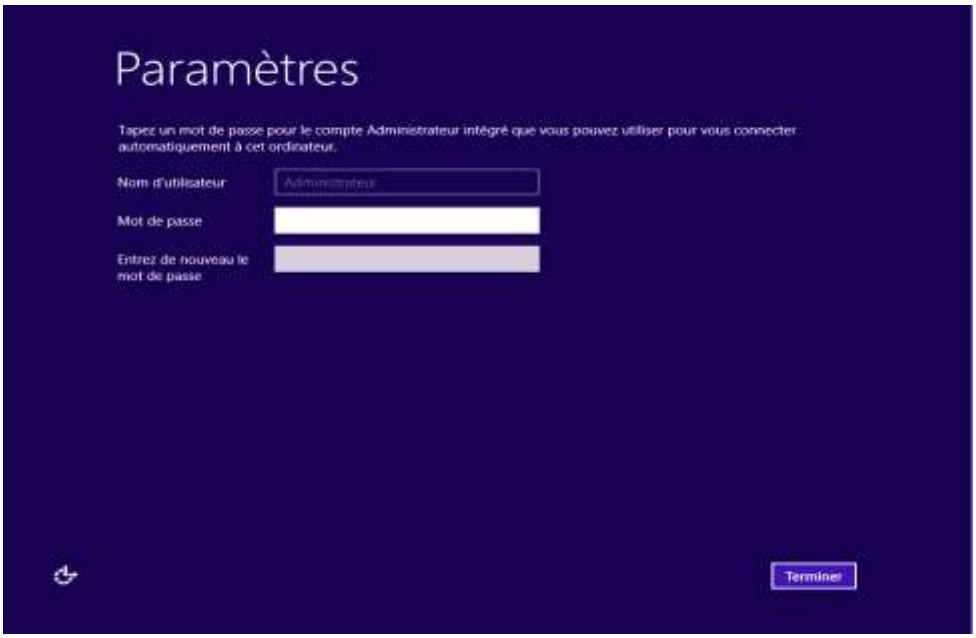


Figure IV-2: Définition d'un mot de passe pour le compte Administrateur.

Ouvrez la session Administrateur en appuyant sur "**Ctrl+Alt+Suppr**".

Figure IV-3 : Session administrateur.

L'installation est terminée.

- ✓ **Configuration de Windows Server 2012**

Une fois que nous avons terminé l'installation, nous allons passer aux étapes de configuration l'ensemble des paramètres généraux de Windows Server 2012 à l'aide de la page d'accueil du gestionnaire de serveur.

Notons que le gestionnaire de serveur de Windows server 2012 est automatiquement chargé lors de l'ouverture de la session.

La fenêtre principale Gestionnaire de serveur permet d'afficher un instantané détaillé des informations d'identité du serveur, des options de configuration de sécurité sélectionnées, ainsi que des rôles et fonctionnalités installés.

a. Configuration des paramètres TCP/IP

Nous accédons au **centre de réseau et partage**, ensuite aux propriétés de notre connexion réseau. Par default, celle-ci est nommée **connexion au réseau local** ou **Ethernet**, nous cliquons sur voir sur le statut **propriétés** puis nous accédons aux propriétés du protocole TCP/IP et affectons les initialisations.

Dans notre cas, nous avons choisi les adresses IP (IPv4) suivantes :

- Adresse IP : 192.168.10.1
- Masque de sous réseau : 255.255.255.0
- Serveur DNS : 192.168.10.1

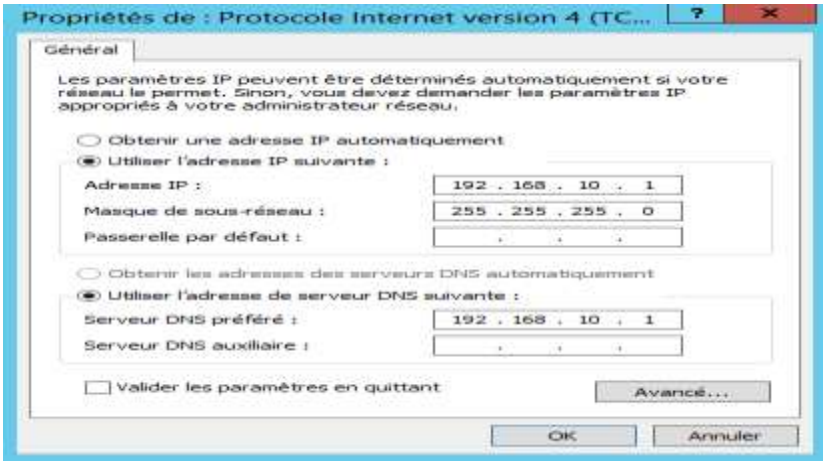


Figure IV-4 : Configuration du protocole TCP/IP.

b. Vérification de la configuration TCP/IP

Nous utilisons l'invite de commande sur lequel nous tapons la commande **IP config/all**, et nous aurons comme résultat ce qui est affiché sur la **Figure IV-8**

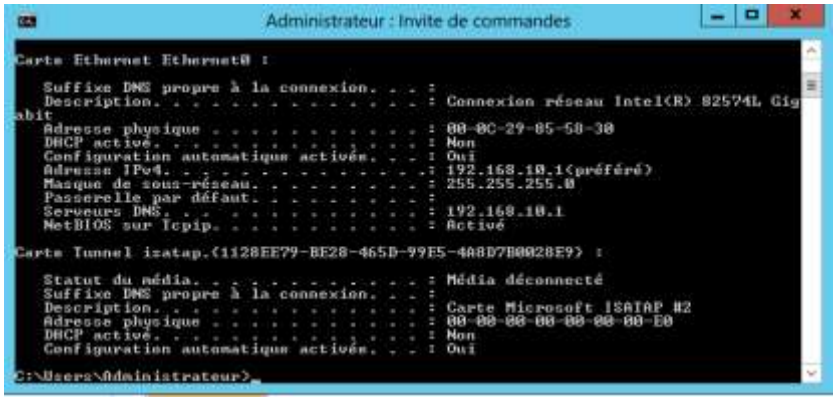


Figure IV-5 : Vérification de protocole TCP/IP.

c. Test de connectivité

Dans cette partie, nous testons notre adresse TCP/IP en tapant la commande **Ping 192.168.10.1**

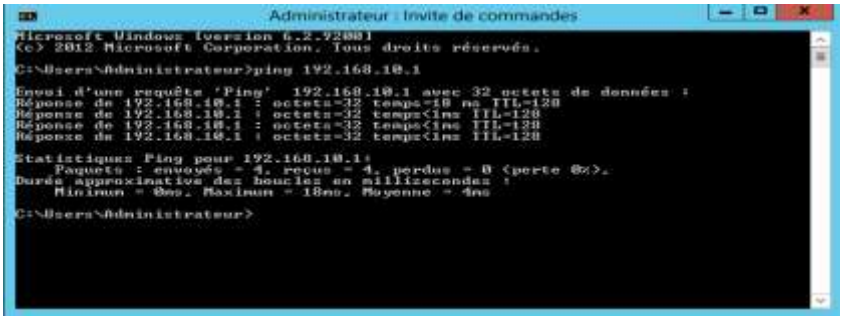


Figure IV-6 : Test de connectivité

Dans ce qui suit, nous passons à l'installation des différents services de Windows server.

IV.1.2. Active Directory sous Windows Server 2012

Windows server 2012 propose un nombre important d'améliorations, tant d'un point de vue fonctionnel que technique et Active Directory n'échappe pas à la règle.

Ainsi le traditionnel **dcpromo** utilisé pour promouvoir un serveur en tant que contrôleur de domaine a été mis au rebut.

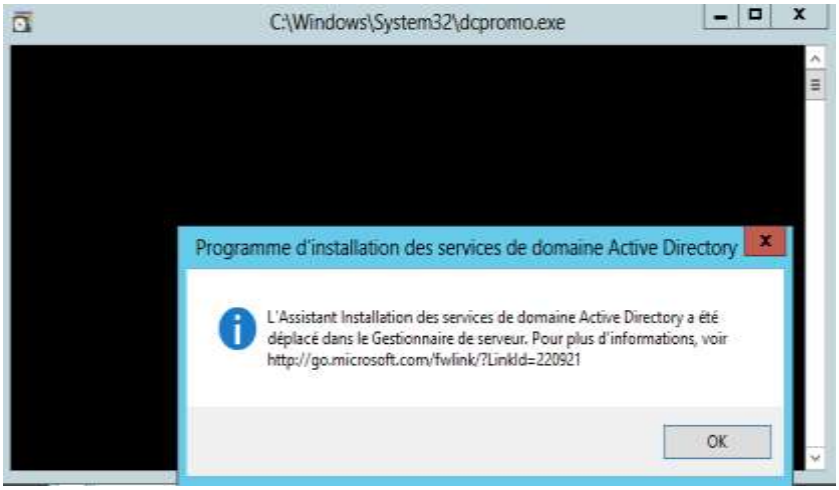


Figure IV-7 : Message qui affiche lors de Louverture de dcpromo dans WS 2012.

Deux options s'offrent désormais à nous pour installer Active Directory sur un serveur Windows 2012 : le gestionnaire de serveur ou PowerShell.

✓ **Installation d'Active Directory via PowerShell**

Pour déployer une forêt ainsi que un domaine racine via Power Shell, nous devons procéder ainsi :

- Charger le rôle Active Directory, les services implicites requis pour ce rôle ainsi que les outils d'administration associés :
  - Install-WindowsFeature –Name AD-Domain-Services IncludeManagementTools
- Installer le domaine (exemple: Condia.local) :
  - Install-addsforest –domainName: Condia.local
- Saisir le mot de passe de restauration des services d'annuaires et sa confirmation ;
- Valider l'installation et le redémarrage.

Tous les composants nécessaires à Active Directory seront installés automatiquement (notamment le service DNS).

✓ Installation d'Active Directory via le gestionnaire de serveur

Sous Windows Server 2012, le menu Démarrer n'existe plus. Les outils de gestion et d'administration sont désormais disponibles dans le Gestionnaire de serveur dont l'icône est située à gauche sur la barre des tâches

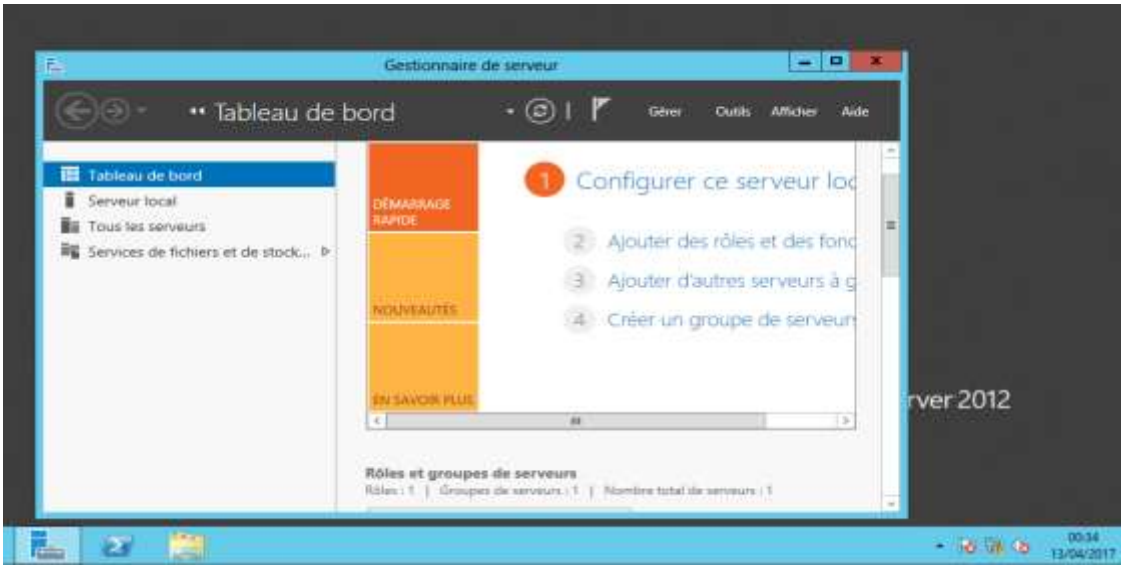


Figure IV-8 : Le Gestionnaire de serveur.

D'autre part, si nous étions familiers du traditionnel **dcpromo** sous les versions antérieures de Windows au travers duquel Active Directory était installé, sachons désormais, nous devons procéder en deux étapes :

- En premier lieu, nous devrons ajouter le rôle Active Directory – Directory Services (AD DS) via l'icône **Gérer –Ajouter des rôles et des fonctionnalités.**

Figure IV-9 : Ajout des rôles et fonctionnalités.

- Dans la fenêtre **Assistant Ajout de rôles et de fonctionnalités**, cliquons sur **Suivant.**

- Sur la page **Sélectionner le type d'installation,** cliquons sur **Suivant** pour accepter l'option par défaut **Installation basée sur un rôle ou une fonctionnalité.**

- Sur la page **Sélectionner le serveur de destination,** cliquons sur **Suivant** pour accepter l'installation locale sur ce serveur.

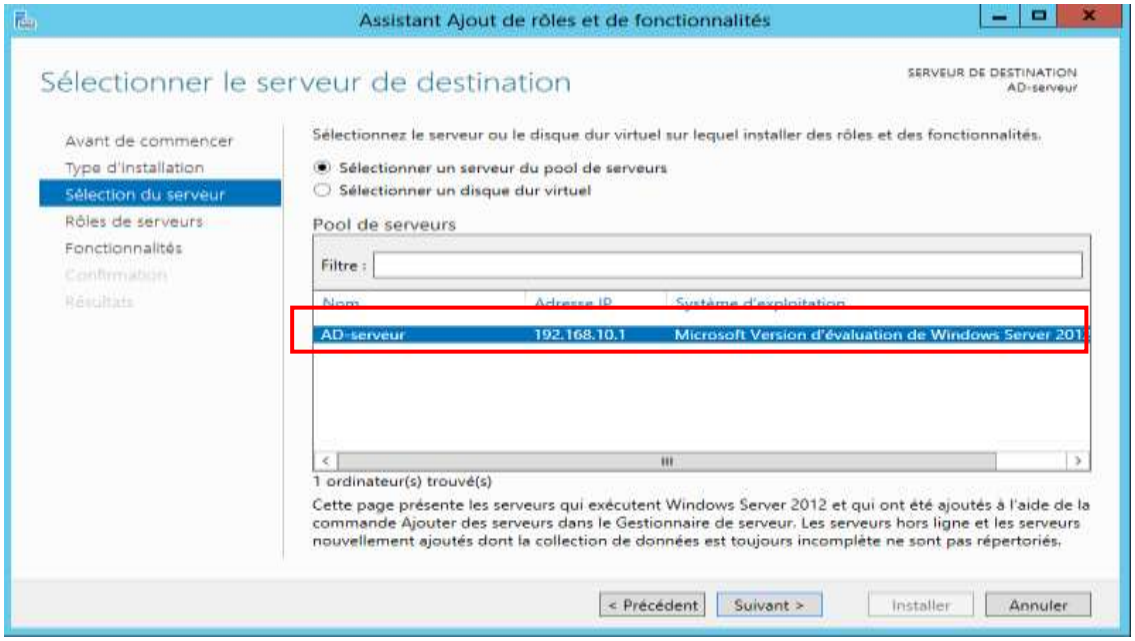


Figure IV-10: Sélection de serveur de destinataire.

- Sur la page **Sélectionner des rôles de serveurs,** parcourons la liste **Rôles** et cliquons sur **Services AD DS.**

- Dans la fenêtre **Ajouter les fonctionnalités requises pour Services AD DS** qui apparaît, cliquons sur **Ajouter des fonctionnalités.**

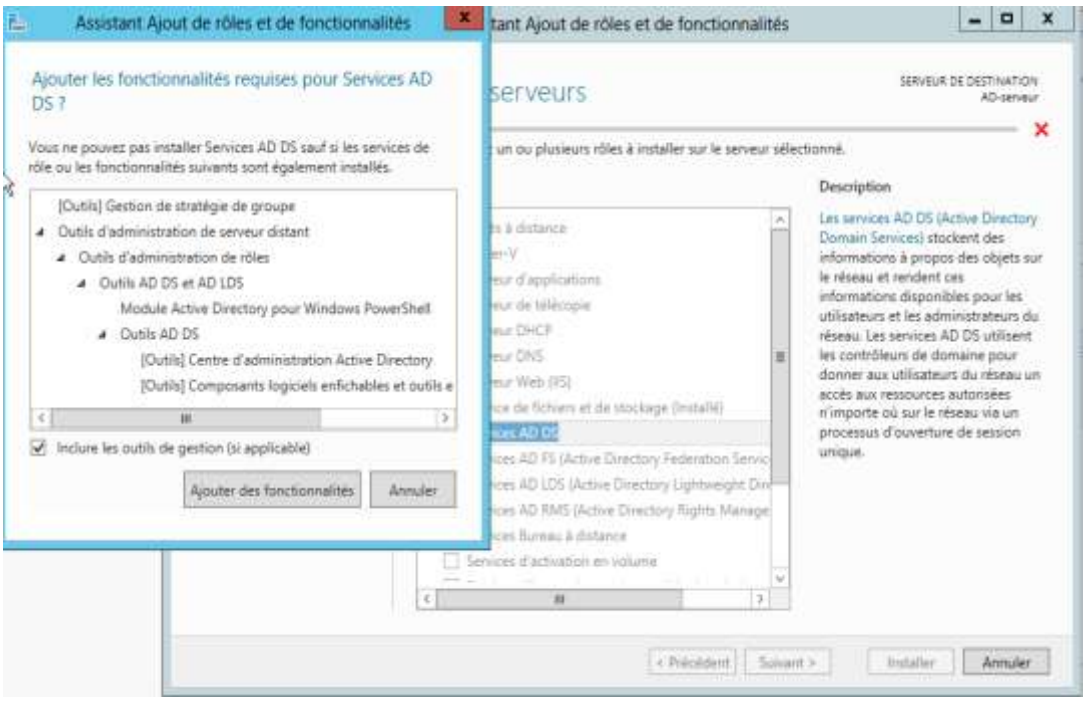


Figure IV-11 : Ajout des fonctionnalités requises pour Services AD DS.

- De retour dans la page **Sélectionner des rôles de serveurs** cliquons sur **suivant**.

- Dans la page **Sélectionner des fonctionnalités**, cliquons sur **suivant** (les fonctionnalités nécessaires ont été présélectionnées automatiquement lors de l'étape précédente).

- Sur la page **Services de domaine Active Directory**, cliquons sur **Suivant.**

- Sur la confirmation, cliquons sur **Installer.**

- Sur la page **Progression de l'installation,** lors les composants ont été installés, cliquons sur **Fermer.**

IV.1.2.1. Configuration du rôle Active Directory

Apres avoir ajouté le rôle Active Directory (ainsi que les fonctionnalités requises par ce rôle comme le service DNS), nous devons configurer ses services en exécutant la Configuration post-déploiement" et lui donner un nom de domaine, ici nous allons créer notre domaine «candia.local» comme la figure suivante le montre :

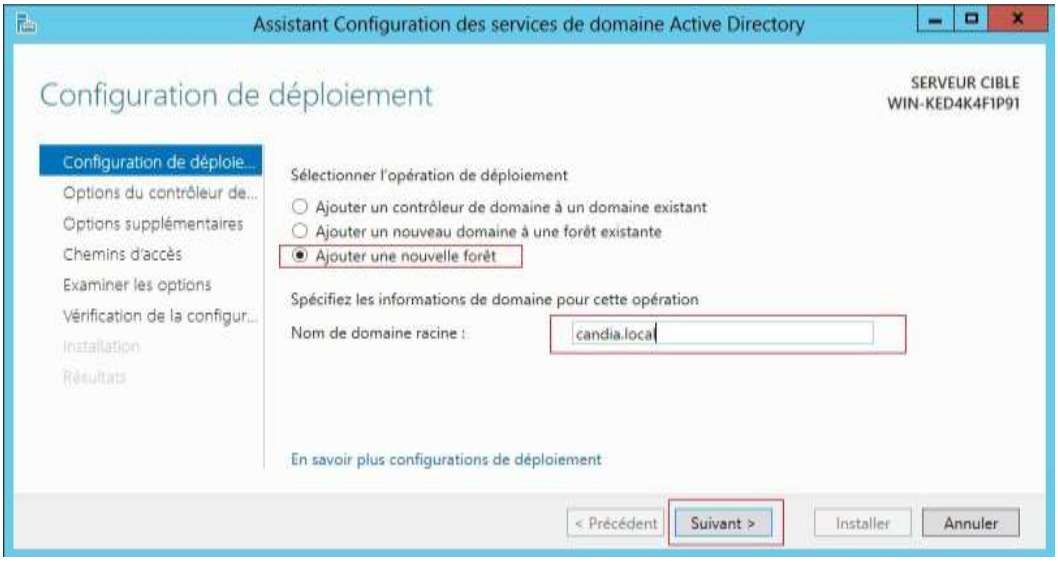


Figure IV-12 : Ajout d'une nouvelle forêt.

Après configuration, le serveur redémarre automatiquement. À présent, les outils de gestion d'Active directory sont présents dans le menu Outils. Notre domaine est ainsi créé. L'ouverture de session s'effectue avec le compte administrateur de domaine « CANDIA\Administrateur ».

Figure IV-13 : Session administrateur CANDIA**.**

IV.1.2.2. Vérification de l'installation des services Active Directory

- Dans l'explorateur de fichiers, naviguons vers le répertoire c:\windows\ntds.
- Confirmons la présence du fichier de base donnée Active Directory NTDS.DIT.

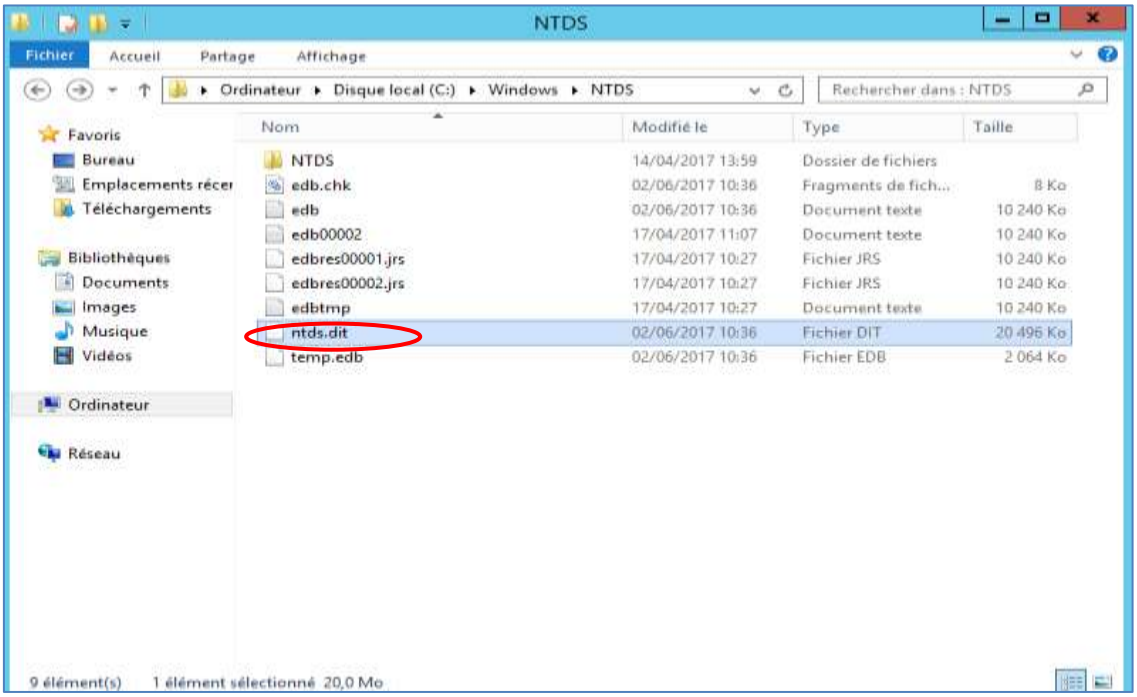


Figure III-14 : Fichier de base donnée Active Directory NTDS.DIT.

- Pour **DNS**
- Dans la console **Gestionnaire DNS**, développons l'arborescence de notre serveur puis les zones de recherches directes**.**
- Confirmons la présence des espaces de noms msdcs.Candia .local et Candia .local.

- Développons ces zones et confirmons la présence d'enregistrement DNS.
- Fermons la console **Gestionnaire DNS**.
- Dans le menu Outils du Gestionnaire de serveur, cliquons sur Utilisateurs et ordinateurs Active Directory.
- Développons l'arborescence Candia .local.
- Vérifions que dans le conteneur **Domain Controllers**, nous retrouvons bien un objet représentant notre contrôleur de domaine **AD-serveur.**

IV.1.3. Installation et configuration du serveur DNS

Pour l'installation du service DNS, nous procéderons comme suit :

✓ **Installation du serveur DNS**
Pour l'installation du service DNS, nous procéderons comme suit :

a. Connectons-nous sur l'ordinateur en tant qu'administrateur local de l'ordinateur ;
b. A l'aide du **Gestionnaire de Serveur**, via **Rôles**, **Ajouter des rôles**, sélectionnons le rôle **Serveur DNS** à l'aide de l'assistant, puis cliquons sur **suivant**.

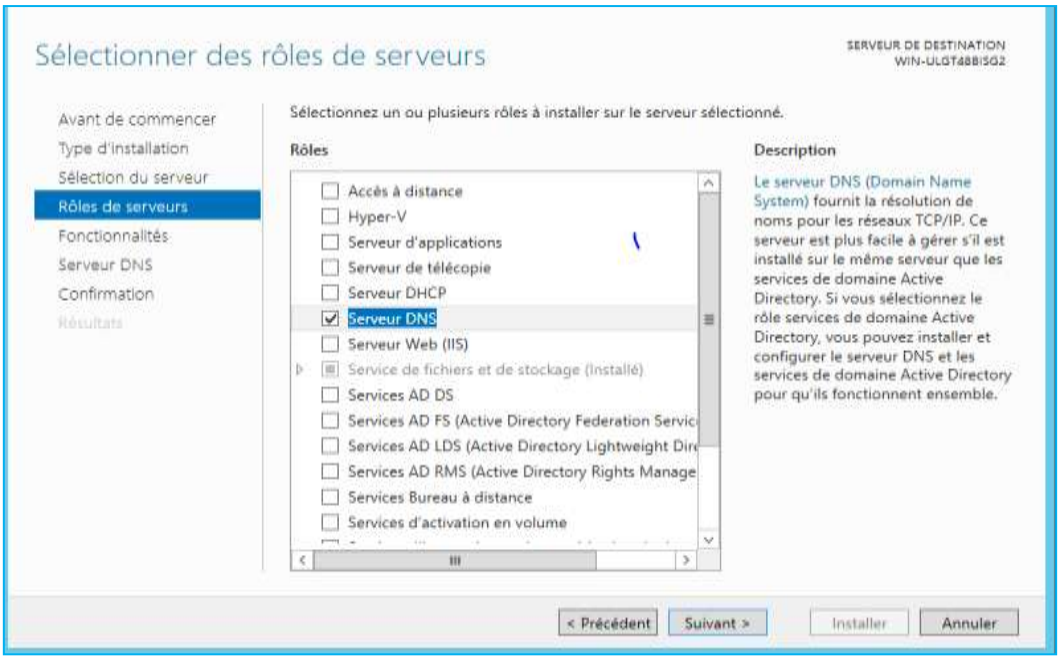


Figure III-15 : Ajout du rôle DNS.

c. Cliquons sur **installer**, et patienter pendant l'installation puis cliquons sur **Fermer** une fois que l'installation est terminée.

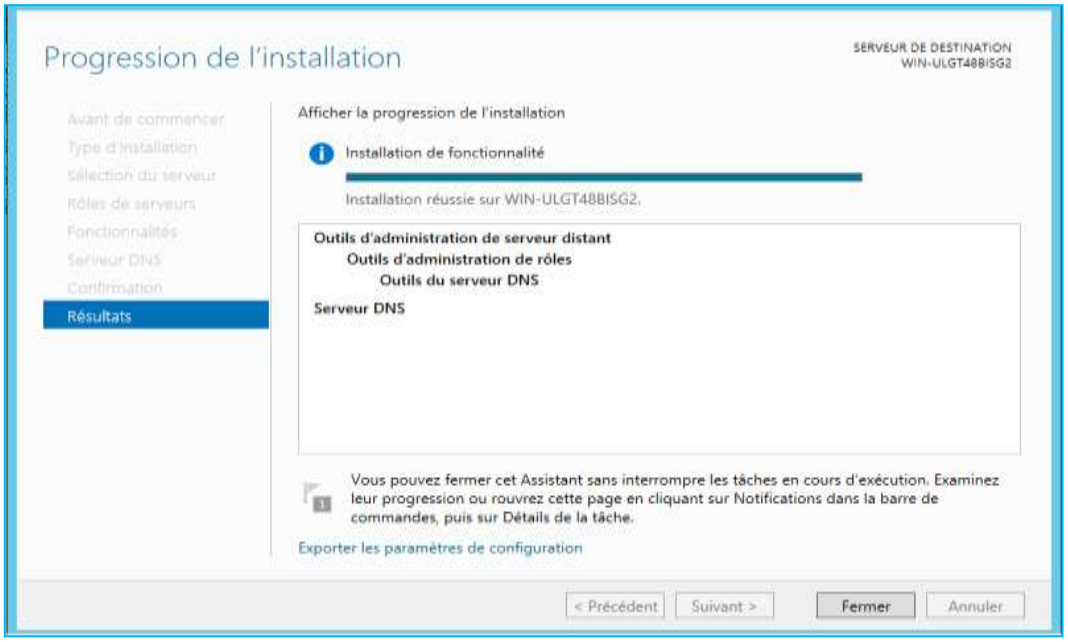


Figure III-16: Progression de l'installation.

✓ **Configuration du serveur DNS**

Une fois le service DNS installé, nous pouvons le configurer grâce à une console dédiée accessible dans les outils d'administration.

IV.1.4. Installation et configuration du serveur DHCP

- Pour l'installation du service DHCP, nous procéderons comme suit :

1. Lancement de l'ajout de rôle depuis la console Gestion de l'ordinateur, cliquons sur Ajouter des rôles et cochons serveur DHCP.

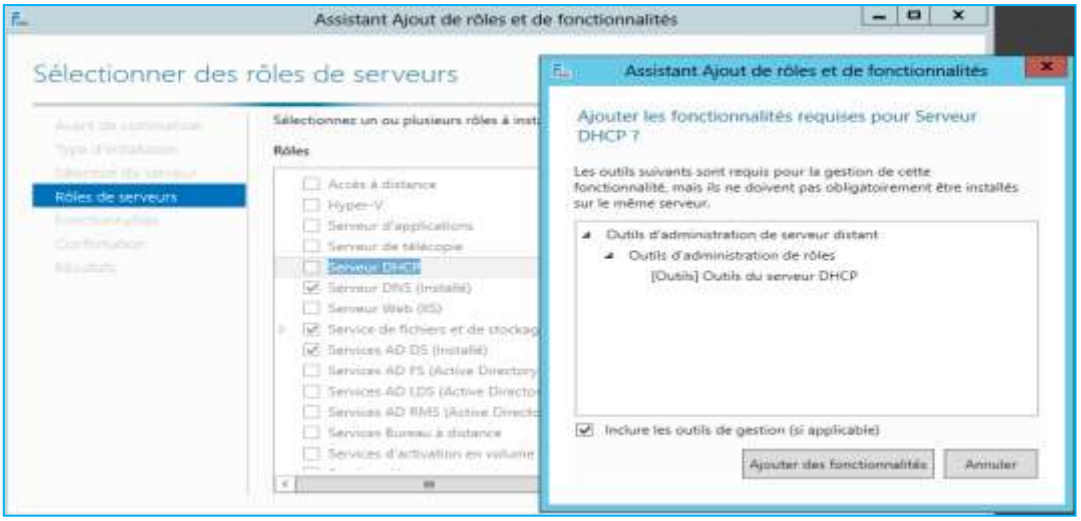


Figure III-17 : Ajout du rôle DHCP.

2. Cliquons sur **installer** et patienter pendant l'installation puis cliquons sur **Fermer** une fois que l'installation est terminée.

- **Configuration du serveur DHCP**

1. Une fois le service DHCP est installé, nous passons à l'étape de la configuration :
   Nous devons démarrer et configurer le serveur DHCP en créant une étendue qui est une plage d'adresses IP qui peut être allouée aux clients DHCP sur le réseau. Les propriétés d'une " étendue " sont les suivantes :
   - Identificateur de réseau ;
   - Masque de sous réseau ;
   - Plage d'adresses IP de réseau ;
   - Durée de bail ;
   - Passerelle ;
   - Nom de l'étendue ;
   - Plage d'exclusion.

   Pour créer une nouvelle étendue, démarrons la console DHCP, faisons un clic droit sur **IPV4** du serveur où nous voulons créer une nouvelle étendue.

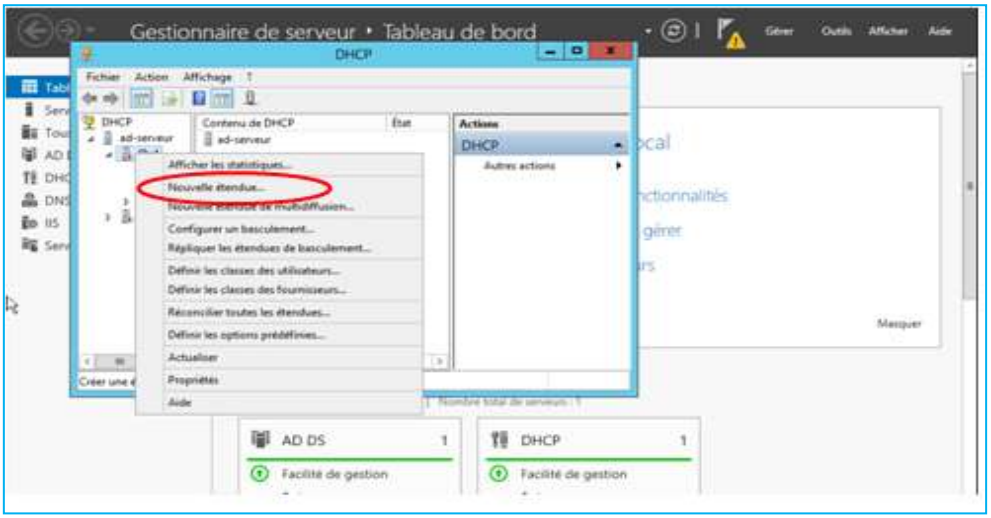


Figure IV-18: Création d'une nouvelle étendue.

Puis cliquons sur **nouvelle étendue** et Cliquons sur **suivant**.

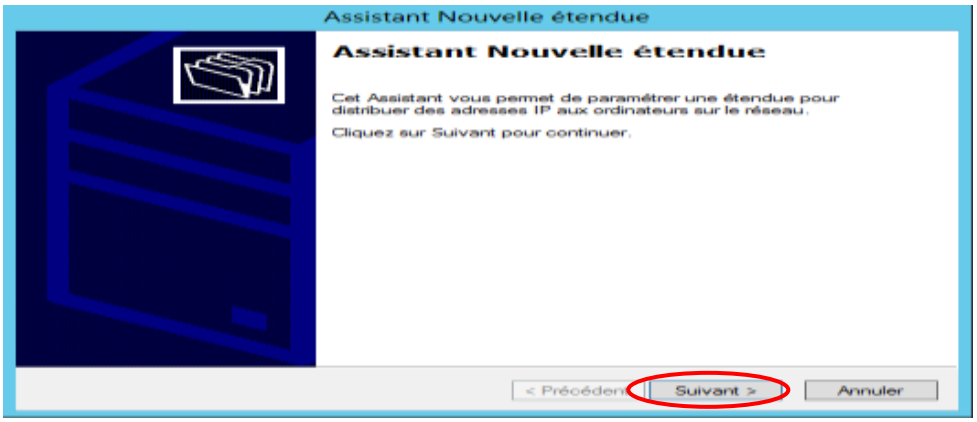


Figure IV-19: Création d'une nouvelle étendue.

2. Dans l'assistant de création d'une nouvelle étendue. Entrons un nom d'étendue dans la zone Nom, ce nom doit être explicite. Dans notre cas nous avons choisi comme nom « **stage** ».

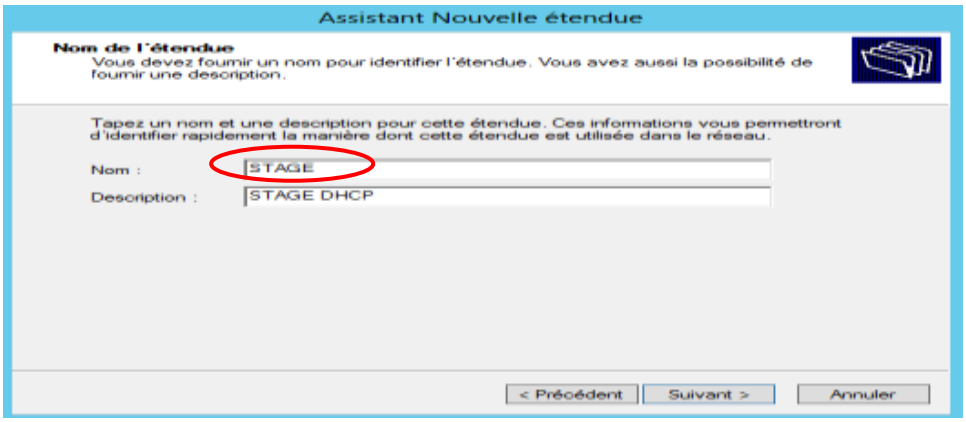


Figure IV-20 : Nom de l'étendue.

3. Cliquons sur **suivant**, ensuite, saisissons la plage d'adresses qui sera alloué. Ces adresses vont être par la suite attribuées aux clients, elles doivent être valides et ne doivent pas être utilisées.
   Spécifions ensuite le masque de sous-réseau choisi et cliquons sur **suivant**.

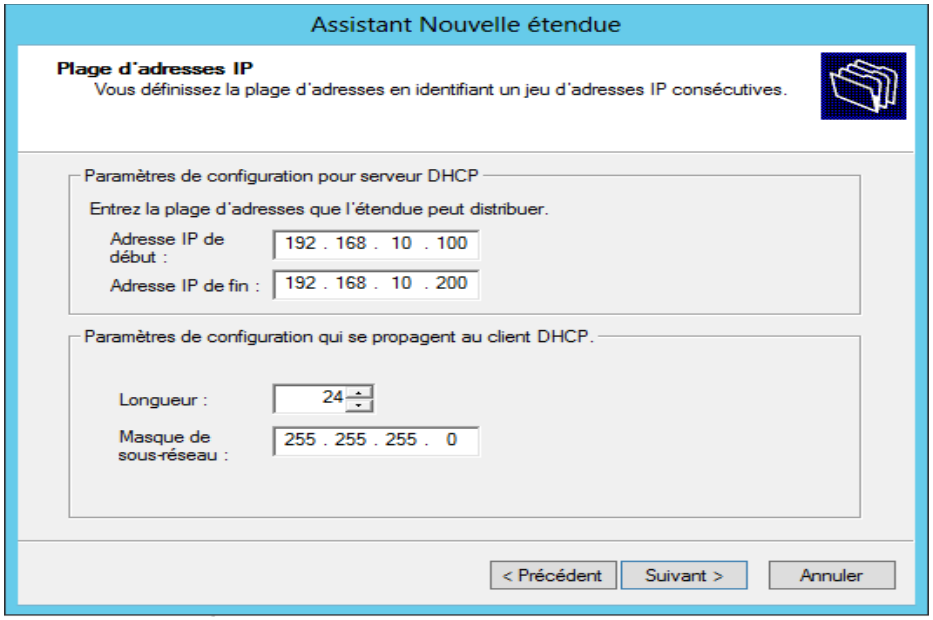


Figure IV-21 : Plage d'adresse allouée aux machines clientes.

4. Spécifions ensuite la durée de bail DHCP : cette durée spécifie la durée pendant laquelle un client peut utiliser une adresse IP de l'étendue .Pour les réseaux stables la durée du bail peut être longue, alors que pour les réseaux mobiles constitués de nombreux ordinateurs portables des durées courtes de bail son utiles.

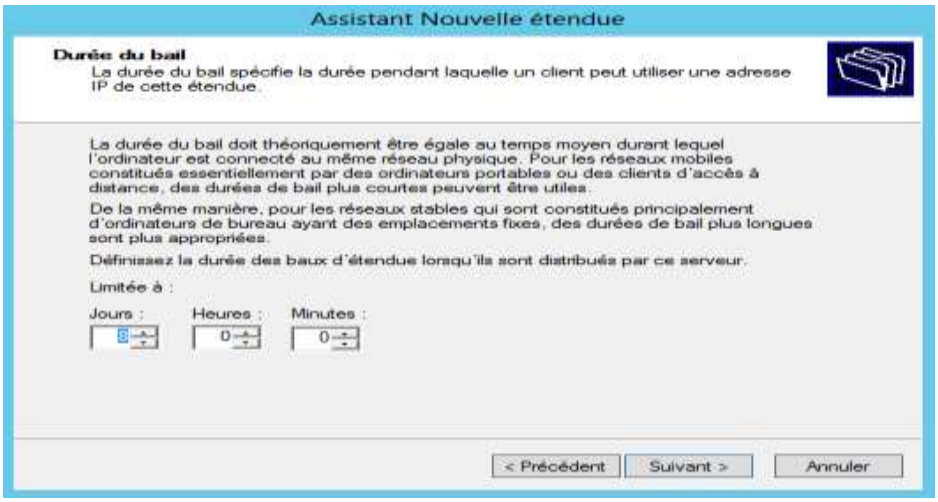


Figure IV-22: Durée de bail.

5. Cliquons sur **« Oui, je veux configurer ces options maintenant** » afin que l'assistant configure l'étendue avec les options les plus courantes puis cliquons sur **suivant**.

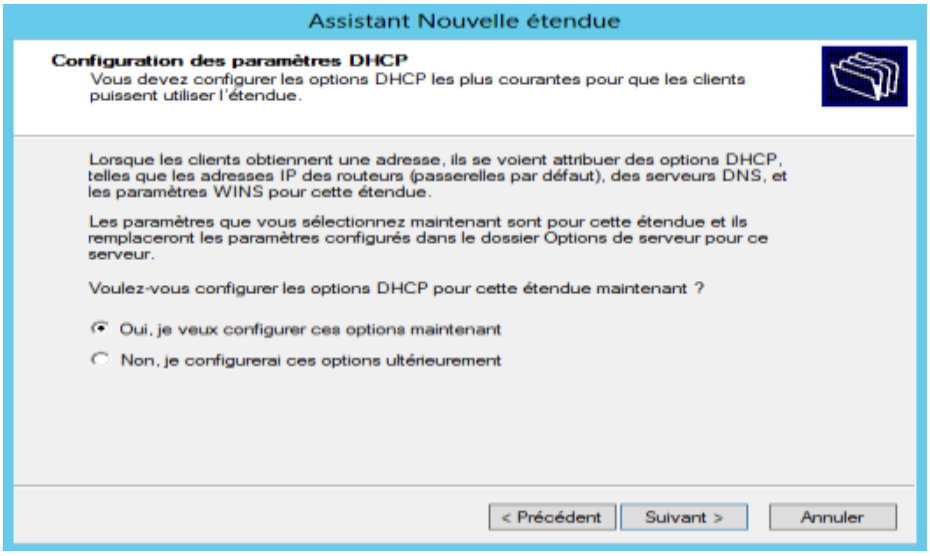


Figure IV-23: Configuration des paramètres DHCP.

6. Cliquons sur **suivant**.

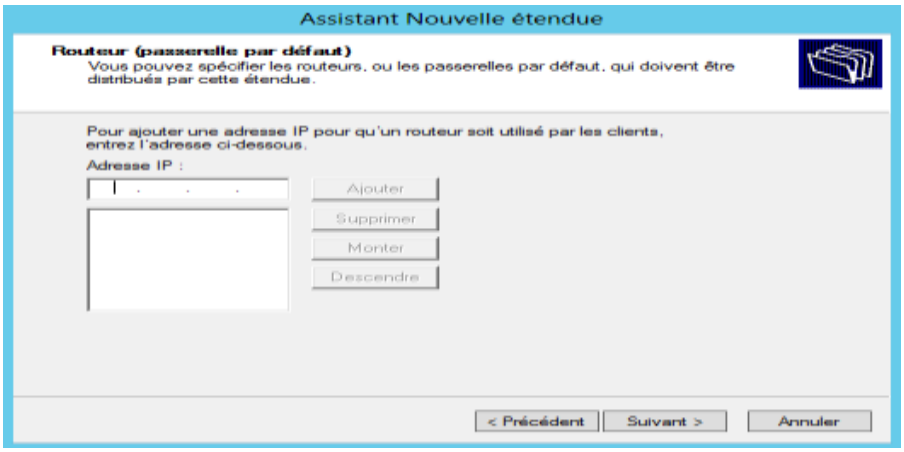


Figure IV-24: Ajout d'une adresse IP à un routeur.

7. Si nous utilisons un serveur DNS, saisissons le nom du serveur puis cliquons sur **Résoudre**.
   Cliquons sur **Ajouter** pour inclure ce serveur dans la liste des serveurs DNS affectés aux clients DHCP puis cliquons sur **suivant**.

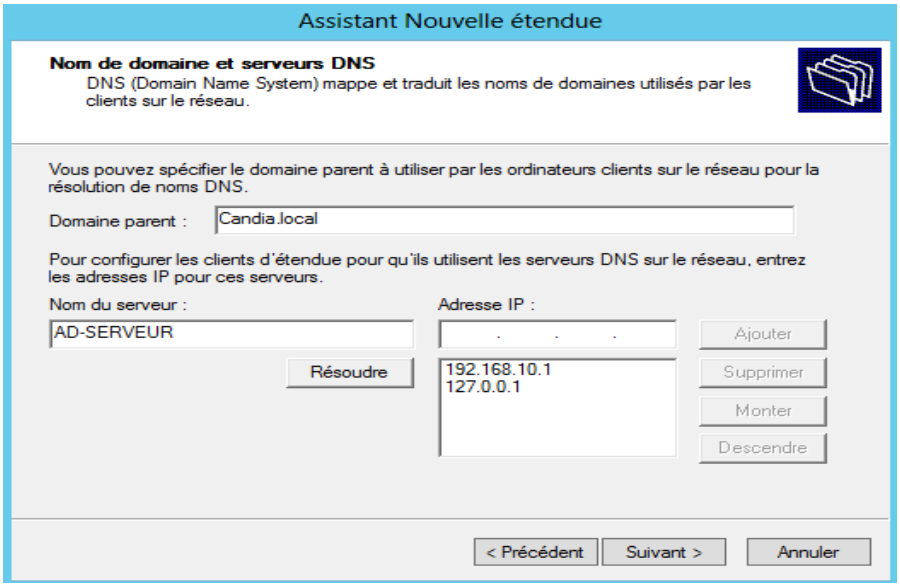


Figure IV-25 : Ajout du nom de domaine server DNS.

8. Cliquons sur **Oui, je veux activer cette étendue maintenant** pour activer l'étendue et ainsi délivrer des baux aux clients de l'étendue, puis cliquons sur **suivant**.
9. Notre serveur DHCP est à présent configuré.

Figure IV-26 : Fin de l'assistant.

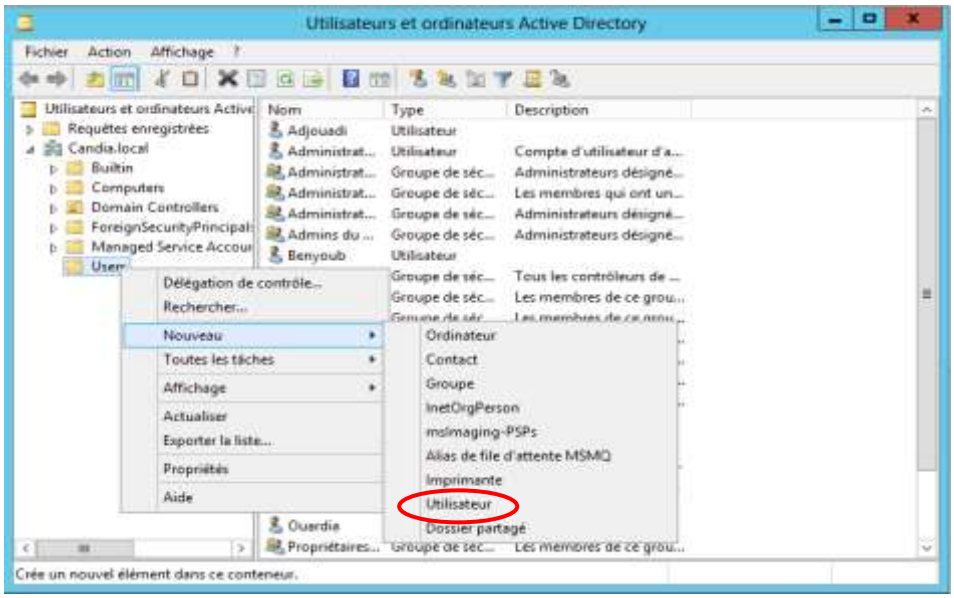
IV.2. Gestion des utilisateurs

Une fois que nous avons installé Windows server et ses services, nous passons à la gestion des utilisateurs.

IV.2.1. Création d'un Compte utilisateur

Pour créer un nouveau compte utilisateur à l'aide de l'interface Windows, nous devons :

- Dans l'arborescence de la console, faisons un clic droit sur le dossier sélectionner **User** ;
- Pointons sur **Nouveau** puis cliquons sur **Utilisateu**r ;



- Après nous remplions les champs qui il faut.

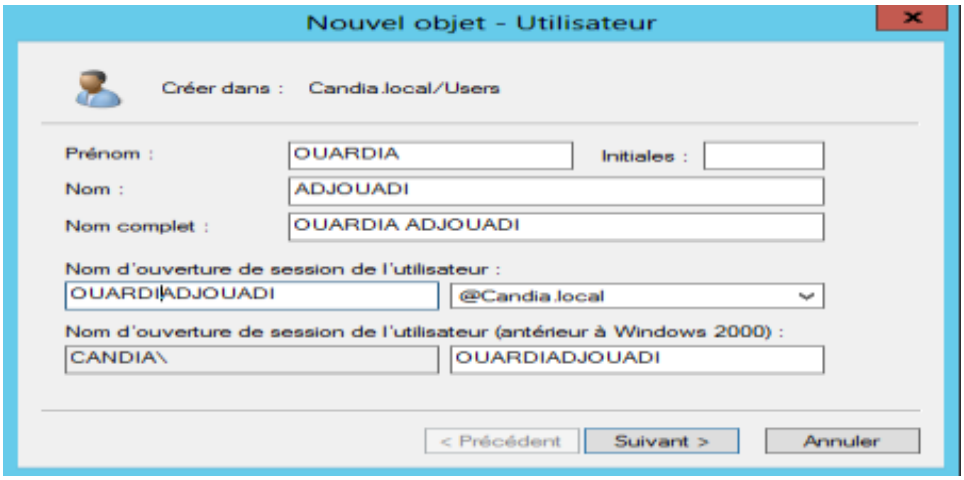


Figure IV-27 : Ajout d'un utilisateur.

- Dans **Mot de passe** et **Confirmer le mot de passe**, entrons le mot de passe de l'utilisateur, puis sélectionnons les options appropriées du mot de passe.

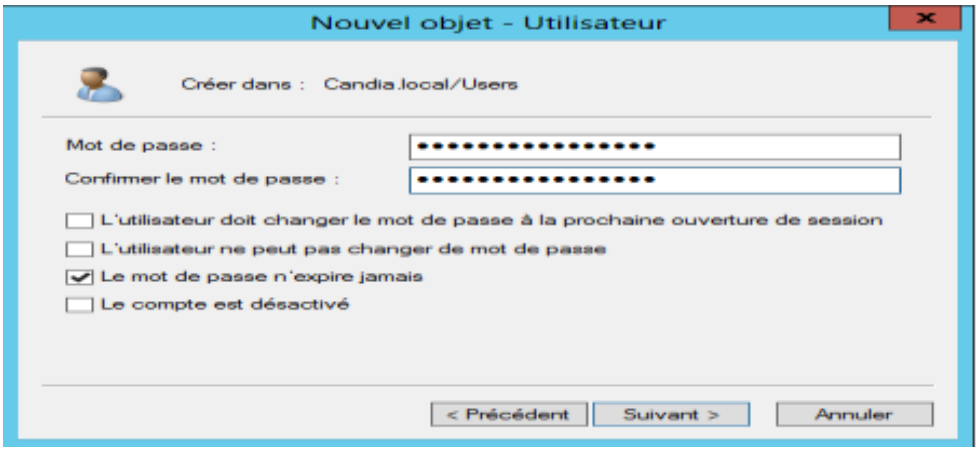


Figure IV-28 : Insertion et confirmation du mot de passe.

IV.2.2. Désactiver et activer un compte utilisateur

Afin d'activer ou désactiver un compte utilisateur à l'aide de l'interface Windows, il faut que :

- Dans l'arborescence de la console, cliquons sur **Utilisateurs** ; nous devons ensuite cliquons sur le dossier qui contient le compte utilisateur ;
- Dans le volet d'information et sur l'utilisateur, cliquons sur le boutons droit;
- En fonction du statut du compte, effectuons l'une des opérations suivantes :
  - Pour désactiver le compte, cliquons sur **Désactiver le compte**.
  - Pour activer le compte, cliquons sur **Activer le compte**.

IV.2.3. Supprimer un compte utilisateur

- Dans la liste des comptes d'utilisateur, sélectionnez le compte d'utilisateur à supprimer.

- Cliquons avec le boutons droit puis cliquons sur **Supprimer le compte d'utilisateur**.
- Le compte est supprimé.

IV.2.4. Afficher un compte utilisateur

La section **Utilisateurs** du tableau de bord Windows Server 2012 affiche une liste des comptes d'utilisateur réseau. La liste fournit également des informations supplémentaires sur chaque compte.

Pour afficher une liste des comptes d'utilisateur :

- Sur le **Gestionnaire de Serveur** cliquons sur **outils**, puis sur **Utilisateurs et ordinateurs Active** Directory ;
- Dans l'arborescence de la console, cliquons sur **Utilisateurs ;**
- Le tableau de bord affiche la liste actuelle des comptes d'utilisateur.

Pour afficher ou changer les propriétés d'un compte d'utilisateur

- Nous allons sur **propriétés**. La page **Propriétés** du compte d'utilisateur s'affiche ;

Figure IV-29: propriétés d'un utilisateur.

IV.2.5. Changer le nom du compte utilisateur

Le nom complet est le nom qui apparaît dans la colonne **Nom** de la page **Utilisateurs**. Le changement du nom complet ne change pas le nom d'ouverture de session ou le nom de connexion d'un compte d'utilisateur.

Pour changer le nom complet d'un compte d'utilisateur :

- Sélectionnez le compte d'utilisateur à modifier ;
- Cliquons sur le boutons droit puis sur **Renommer** et nous modifions;

Le nouveau nom complet s'affiche dans la liste des comptes d'utilisateur.

IV.2.6. Définition des horaires d'accès

Windows server permet de contrôler les périodes pendant les quelles les utilisateurs se connectent au réseau. Par défaut, il permet un accès 24 heures sur 24 heures et 7 jours sur 7 jours.

Pour configurer les horaires d'accès, voici les étapes à suivre :

- Sur le **Gestionnaire de Serveur** cliquons sur **outils**, puis sur **Utilisateurs et ordinateurs Active** Directory ;
- Nous pouvons à présent définir des heures d'accès valides et invalides en utilisant la boite de dialogue illustrée à la figure c'est dessous. Dans cette boite de dialogue, nous pouvons activer ou désactiver chaque heure du jour ou de la nuit.
  - Les heures autorisées sont de couleur bleu.
  - Les heures interdites sont banches.

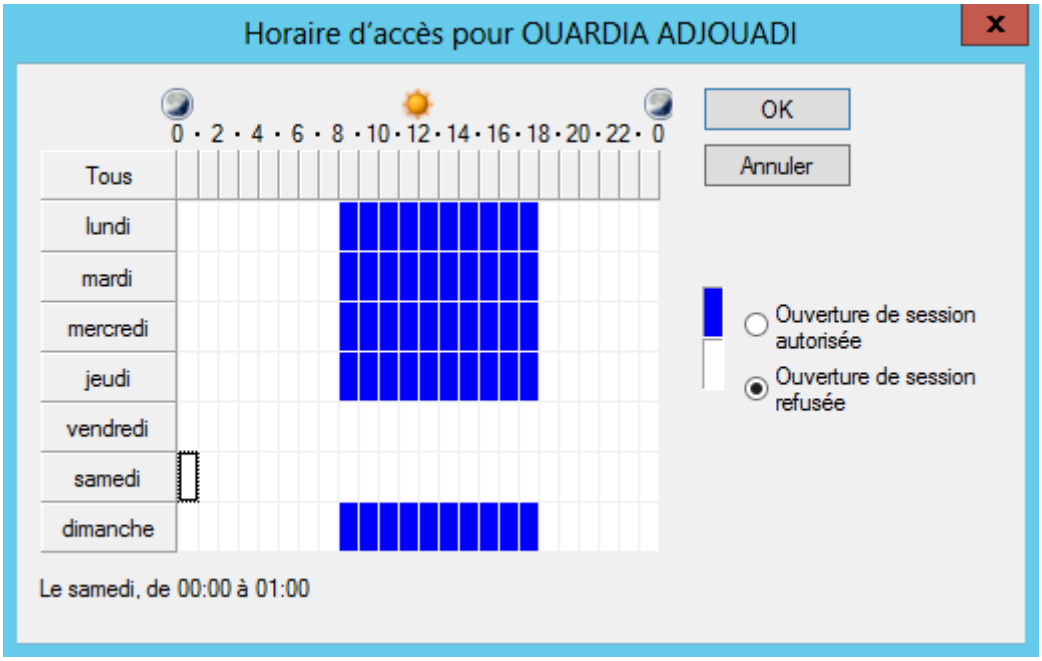


Figure IV-30 : Boite de dialogue Horaires d'accès.

IV.3. Stratégies de groupe

En plus des comptes d'utilisateur, Windows server fournit des groupes. En règle générale, nous utilisons des groupes pour accorder des autorisations aux mêmes types d'utilisateurs, et pour simplifier l'administration des comptes, en nous permettant d'attribuer des autorisations et des droits à un groupe d'utilisateurs plutôt qu'à chaque compte d'utilisateur individuel.

Dans cette partie, nous allons voir comment créer des groupes, les supprimer et leurs ajouter des membres.

IV.3.1. Créer un groupe utilisateur

Pour créer un groupe :

- Sur le **Gestionnaire de Serveur** cliquons sur **outils**, puis sur **Utilisateurs et ordinateurs Active** Directory ;
- Dans l'arborescence de la console, faisons un clique droit sur le dossier sous lequel créer un nouveau groupe ;
- Pointons sur **Nouveau,** puis cliquons sur **Groupe ;**
- Tapons ensuite le nom du nouveau groupe ;

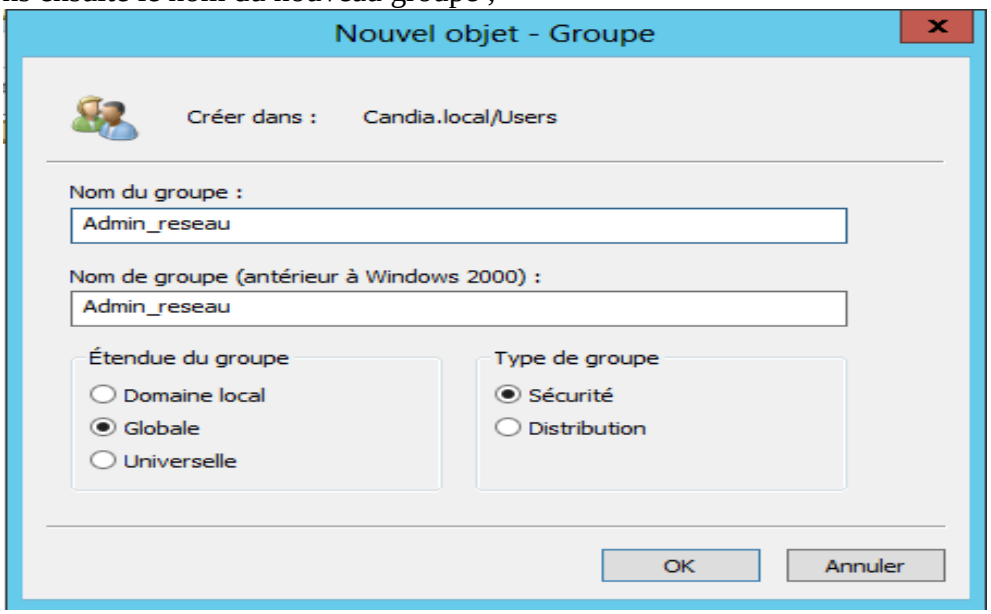


Figure IV-31: Ajout de nouveau groupe.

Par défaut, le nom que nous tapons est aussi entré comme le nom antérieur à Windows 2000 du nouveau groupe.

- Dans **Etendue du groupe,** cliquons sur l'une des options ;
- Dans **Type du groupe,** cliquons sur l'une des options ;
- Enfin nous cliquons sur **OK**.

IV.3.2. Ajouter un membre à un groupe

- Sur le **Gestionnaire de Serveur** cliquons sur **outils**, puis sur **Utilisateurs et ordinateurs Active** Directory ;
- Dans l'arborescence de la console, cliquons sur le dossier qui contient le groupe auquel ajouter un membre ;
- Dans le volet d'information, faisons un clic droit sur le groupe, puis cliquons sur **propriétés** ;
- Sous l'onglet **Membres,** cliquons sur **Ajouter** ;
- Dans entrons les noms des objets à sélectionner, tapons le nom de l'ordinateur, du groupe ou de l'utilisateur que nous voulons ajouter au groupe, puis cliquons sur OK.

IV.3.3. Suppression d'un groupe

- Cliquons sur le dossier qui contient le groupe à supprimer ;

- Dans le volet d'informations, faisons un clic droit sur le groupe, puis cliquons sur supprimer ;
- Un message de confirmation s'affiche ;

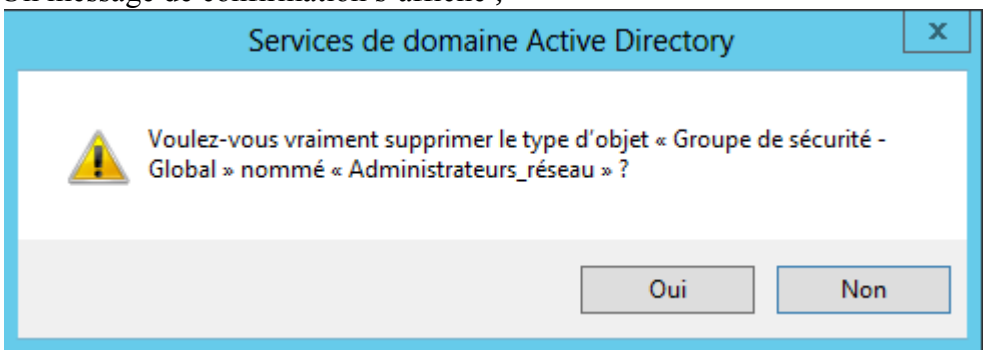


Figure IV-32 : Suppression d'un groupe.

- Cliquons sur **Oui** pour supprimer le groupe.

IV.4. Connexion d'un ordinateur au domaine client Windows

Pour permettre au client de se connecter au domaine, nous allons suivre les étapes suivantes :

- Dans propriétés de « Ordinateur » et dans l'anglé « nom de l'ordinateur » nous avons cliqué sur le bouton «modifier» puis nous avons spécifié le nom du domaine«Candia».
- Le système demande une authentification avec le nom d'utilisateur et le mot de passe de domaine.

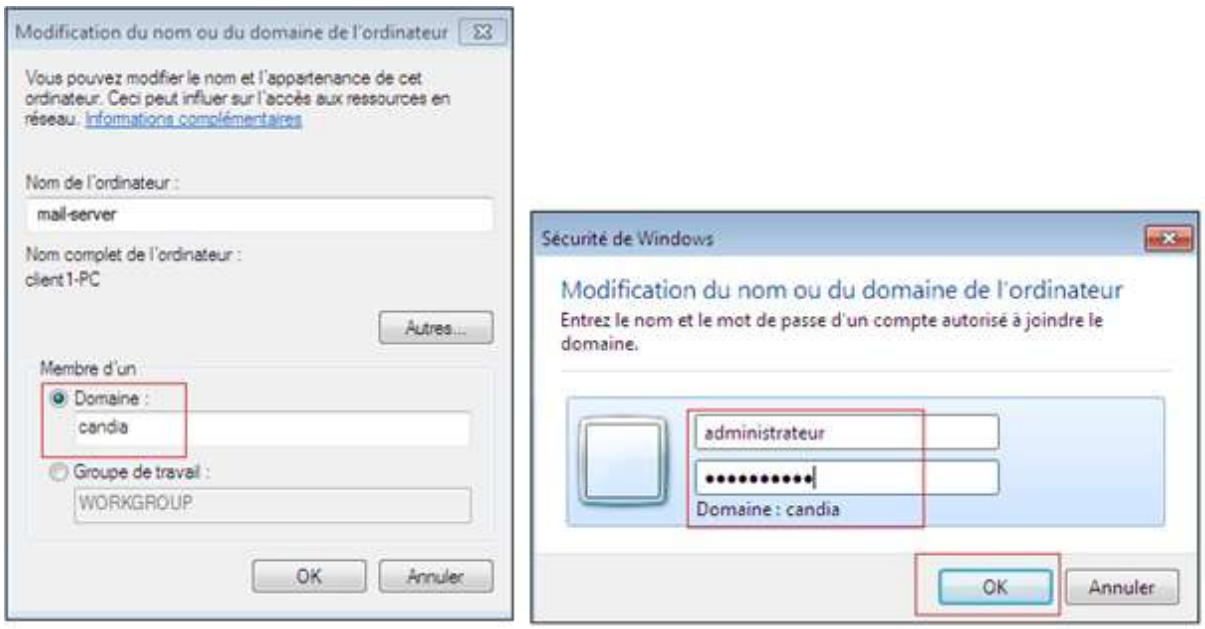


Figure IV-33: Demande d'authentification au domaine Candia.

Si tous s'est bien passé, le message « Bienvenue dans le domaine Candia »apparait :

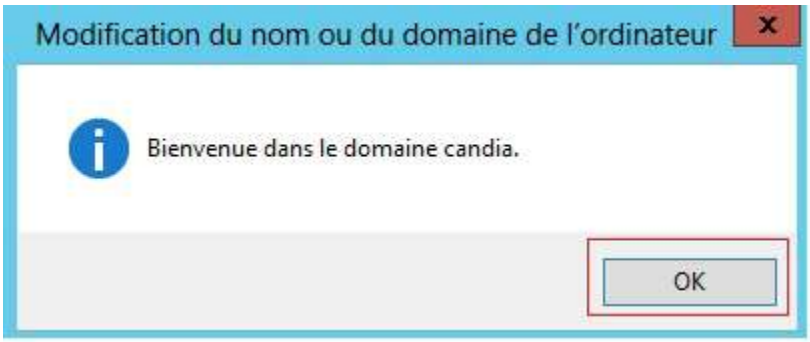


Figure IV-34: Intégration au domaine Candia.

IV.5. Partage de fichiers

Les dossiers partagés offrent aux utilisateurs un accès centralisé aux fichiers sur le réseau. Lorsqu'un dossier partagé, tous les utilisateurs peuvent par défaut s'y connecter et accéder à son contenue.

- ✓ **partage d'un dossier**
  Pour partager un dossier :
  - Sous l'onglet sécurité, cliquons sur le bouton **Avancé** et désactiver l'héritage,

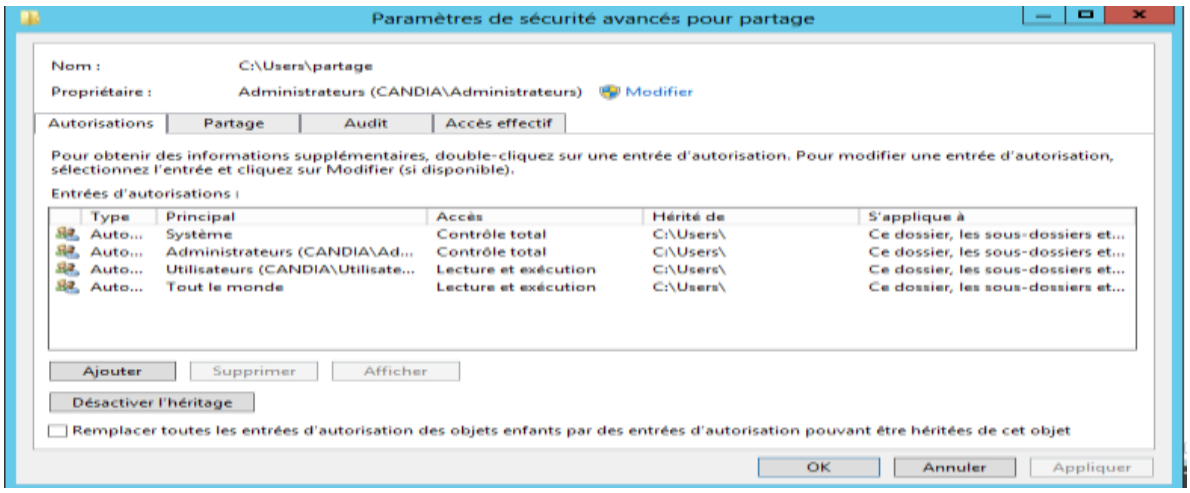


Figure IV-35: Désactivation de l'héritage.

- Dans le même onglet sécurité, ajouter les groupe ou appartient l'utilisateur qui a l'autorisation d'accès à ce fichier ;
- Sur l'onglet **Partager**, cochons la colonne **Partager ce dossier** puis cliquons sur le bouton **Autorisation ;**

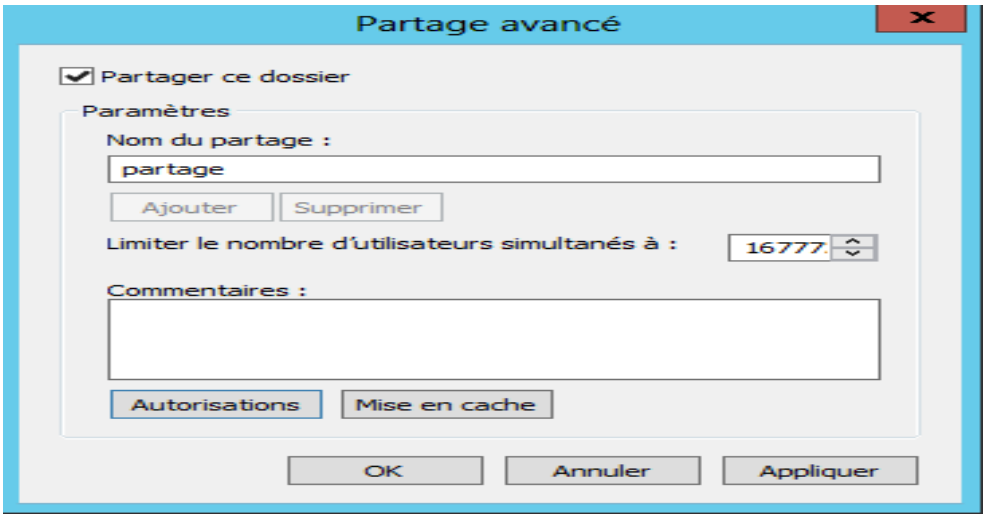


Figure IV-36: Partage avancé.

- Cliquons sur **Ajouter** pour ajouter l'utilisateur qui va avoir l'accès à ce dossier partagé ;.

✓ **attribution d'autorisations sur les dossiers partagés**

Dans cette partie nous allons vérifier le partage de fichiers

- Dans **Démarrer** et sur **Ordinateur**, cliquons sur le bouton droit de la souris;
- Ensuite, Cliquons sur **Connecter un lecteur réseau.** Cela affiche la boite de dialogue **Connecter un lecteur réseau ;**

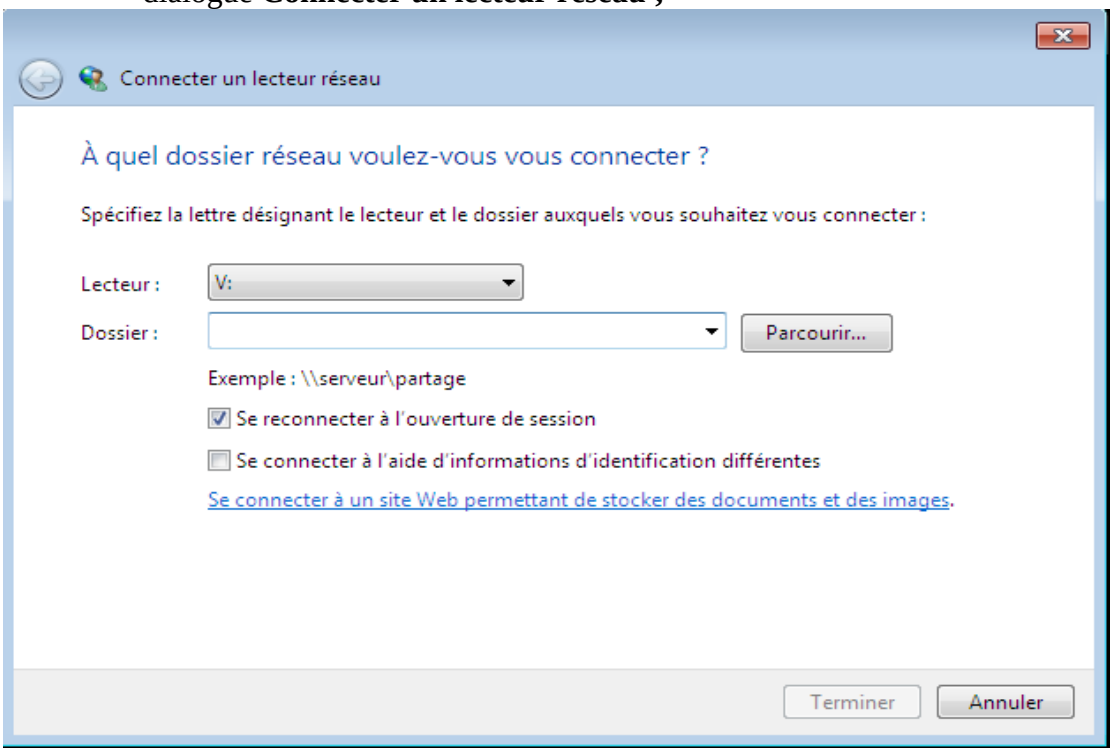


Figure IV-37: Boite de dialogue Connecter un lecteur réseau.

- Cliquons sur le bouton **Parcourir** pour chercher le dossier partagé dans le réseau ;

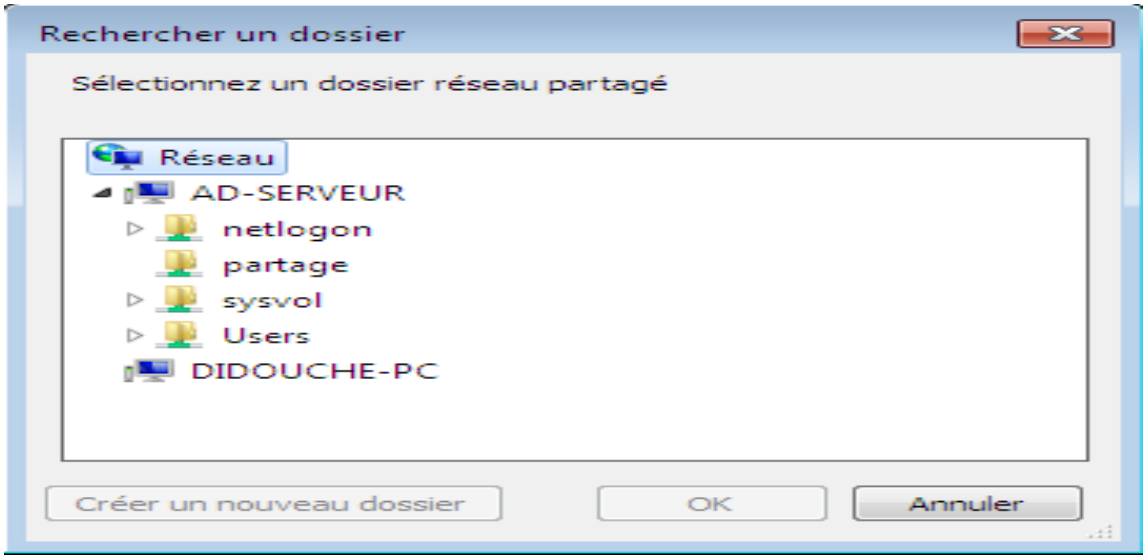


Figure IV-38: Recherche d'un dossier sur le réseau.

- C'est l'utilisateur à le droit d'accès au dossier partagés, il accède ou' il peut ajouter, modifier ou supprimer un dossier, sinon un message d'erreur lui affiche.

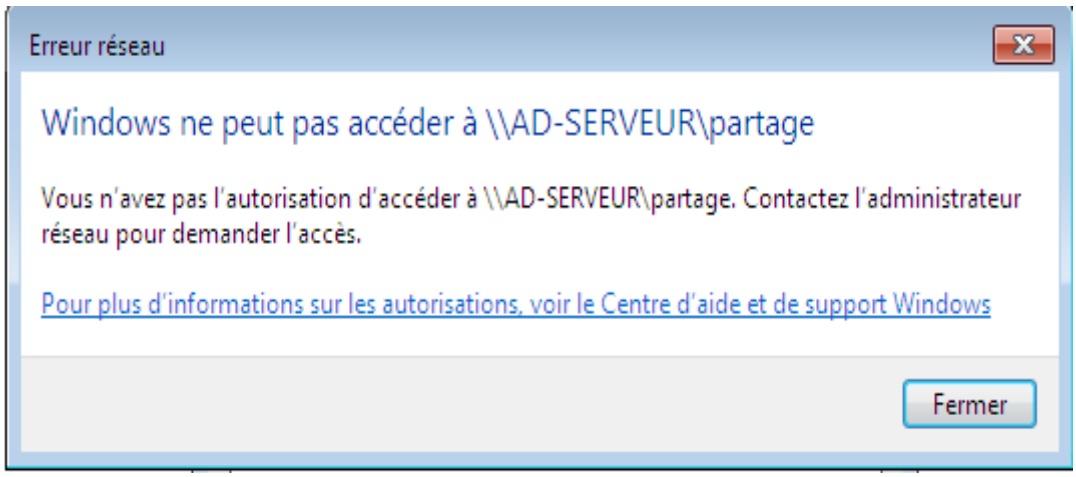


Figure IV-39: Message d'erreur de ne pas avoir l'accès a un dossier partagé.

Conclusion

Dans ce chapitre, nous avons décrit brièvement les étapes d'installation et de configuration du système Windows server 2012 ainsi que ses différents services (AD, DNS, DHCP).

Cette étape nous a permis de réaliser notre objectif de résoudre le problème de l'entreprise Tchin-Lait qui consiste à créer le serveur contrôleur de domaine.

Conclusion générale et perspectives

Le travail présenté dans ce projet, réalisé dans le cadre du projet de fin de cycle a été le fruit d'une longue réflexion pendant laquelle il a fallu répondre à la demande de l'entreprise Tchin-Lait « Candia », celle de mettre en place un contrôleur de domaine afin de centraliser la gestion des utilisateurs. Ce mémoire nous a permis d'approfondir ainsi de pratiquer nos nouvelles acquisitions théoriques durant notre cycle de stage. Ce dernier était une occasion pour nous de côtoyer le monde professionnel.

Pour mettre en œuvre ce projet, nous avons dans un premier temps passé en revue les généralités et les notions théorique relative à l'administration et la sécurité des réseaux informatique, ainsi qu'au service d'annuaire Active Directory, fondamental pour le fonctionnement de la solution choisie.

Puis , nous avons mis en œuvre la solution choisie sur un environnement de réalisation composée de machines virtuelles, et nous avons réalisé toutes les taches nécessaires à sa configuration pour ensuite explorer les fonctions d'administration et de configuration d'une infrastructure de service d'annuaire Active Directory à base de Windows server 2012.

Afin d'accomplir ce projet et aboutir au résultat prévue, nous avons choisis d'utiliser Windows server2012 qui nous l'avons installé sur VMWare.

C'est avec un réel enthousiasmé que nous nous somme lancés dans ce projet. Ce dernier nous a permis d'avoir une idée très claire sur les services d'annuaire ainsi leur importance. L'élaboration de ce travail nous a permis d'une part d'approfondir les connaissances acquises durant les années d'études à l'université, et d'une autre part de préparer notre intégration à la vie professionnel.

Par ailleurs, les perspectives dégagées pour ce travail c'est que nous souhaitons faire une réalisation réel avec des équipements physiques, ainsi d'ajouter d'autre services à savoir :

- ❖ service de résolution de nom WINS, LLMNR.
- ❖ sauvegarde et restauration des données.
- ❖ Connexion à distance.

Références bibliographiques

[1] : Philippe.A, Réseaux informatiques notions fondamentales, Edition ENI, Mai 2009.

[2] : Yang.B and Garicia-Molina.H, Comparing Hybrid peer-to-peer systems, in proceedings of the 27th international conference on very large Data Bases, September 2001.

[3]: Olivier .D, Frédéric.G, Julian.M, Stéphane.P. Analysis of Failure Correlation in Peer-to-Peer Storage Systems. *Rapport de recherche N°6771, INRIA December*.

[4] : AUTRIVE.P, La théorie des réseaux locaux et étendus, 7 octobre 2006 IN http :// hautrive.devloppez.com/réseau /page=page_5.

[5] : William.R. S, Guide de l'administrateur Windows server 2012, Edition Dunod, 2007.

[6] : AMAN.V, Concevoir la sécurité informatique en entreprise, Edition Creative Commons, 2014.

[7] : Labiod.H et Afifi.H, Sécurité, qualité de service et aspects pratiques, Edition Lavoisier, paris, 2004.

[8] : Drdoigne.J, Réseau informatique, notions fondamentales, Edition ENI, France, Janvier 2013.

[9] : LAHFA.N et HENAOUI.A, Administration Réseaux informatiques, mémoire de l'obtention du diplôme Master en Informatique, Modèle Intelligent et Décision. Université Abou Bakr Belkaid– Tlemcen, 2013.

[10] : TCHIN -LAIT, « DOCUMENT D'ENTREPRISE» ,2017.

[11] : Rizcallah. M, Annuaires LDAP, 2éme édition, édition ENI, 2011.

[12] : Vinnaza.E, Exchange server 2010, édition ENI, 2010.

[13] : Brahim.N et Loïc.T, Exchange Server 2013 « Préparation à la certification MCSE messaging», Edition ENI, France, février 2014.

[14] : Aprea .J .F, configuration d'une infrastructure Active Directory avec Windows server, édition ENI, 2008.

[15] : CRAFT.M, Active Directory pour Windows 2000 Server, Edition EYROLLES, Paris, 2002.

[16] : Microsoft press, Windows 2000, Active Directory Services, France, Mai 2000.

[17] : DORDOIGNE.J, Réseaux informatiques "Notions fondamentales et administrations sous windows server ou linux", Edition ENI, France, Novembre 2014.

[18] : LOHIER.S et QUIDELLEUR.A, Le reseau Internet, Edition DUNOD, Paris, 2010.

Résumé

Le réseau est devenu une ressource indispensable au bon fonctionnement d'une organisation, une entreprise, une université,... L'administration du réseau met en œuvre un ensemble de moyens pour offrir aux utilisateurs une certaine qualité de service, permettre l'évolution du système en incluant de nouvelles fonctionnalités ,contrôler l'accès au réseau et aux ressources par les utilisateurs, gérer la gestion des comptes des utilisateurs et assurer la sécurité et la disponibilité des ressources du réseau à tout moment.

C'est ceci qui nous a poussés à faire une configuration sécurisé d'un contrôleur de domaine afin de centraliser la gestion des utilisateurs au sein de l'entreprise « Tchin-Lait » sous Windows server. Ce dernier est une plateforme qui offre un outil familier pour gérer les comptes des utilisateurs, groupes et règle de partage, et d'une autre part, il facilite pour l'administrateur réseau de gérer le parc informatique dans un plus bref délai et cela depuis son poste de travail ou de n'importe quel poste configuré pour l'accès à distance.

Pour la réalisation de ce projet, nous avons utilisées des différents logiciels informatiques tels que Windows server 2012, VMware.

Mot clés: Administration réseau, Windows server 2012, Active Directory, VMware.

Abstract

The network has become an indispensable resource for the proper functioning of an organization, a company, a university, etc. The administration of the network implements a set of means to offer users a certain quality of service, Of the system by including new features, controlling users access to the network and resources, managing user account management, and ensuring the security and availability of network resources at all times.

This is what prompted us to make a secure configuration of a domain controller in order to centralize the management of users within the company "Tchin-Lait" under Windows server. The latter is a platform that provides a familiar tool for managing user accounts, groups and sharing rules, and on the other hand, it makes easy for the network administrator to manage the computer park within a shorter period of time its workstation or any extension configured for remote access.

For the realization of this project, we used different computer software such as Windows Server 2012, VMware.

Keywords: Network administration, Windows server 2012, Active Directory, VMware.