

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud MAMMARI de Tizi-Ouzou
Faculté de génie électrique et informatique
Département informatique



Mémoire de fin d'études

En vue d'obtention du Diplôme de Master en Informatique
Spécialité : Système informatique

Thème

**Conception et réalisation d'une infrastructure d'entreprise
client/serveur pour la gestion des utilisateurs.**

Présenté par : M^f. ABDELLAOUI Brahim

Devant le jury :

Présidente : M^f. DAOUI Mehammed U.M.M.T.O

Promoteur : M^f. DEMRI Mohamed U.M.M.T.O

Examinatrices : M^{me}. HADAOUI Rabiha. U.M.M.T.O

M^{me}. AOUDJIT Rachida. U.M.M.T.O

Année universitaire : 2014-2015

Remerciements

Ce travail a été effectué sous la direction scientifique de Monsieur M. DEMRI, Maitre de conférences à l'UMMTO. Je tiens à le remercier de m'avoir encadré. Je le remercie également pour la confiance qu'il a placée en moi en me donnant une certaine liberté afin d'organiser mon travail. Qu'il trouve ici l'expression de ma sincère reconnaissance et mon profond respect.

Monsieur le Professeur M. DAOUI, Professeur à l'UMMTO, me fait l'honneur de présider le jury de ce mémoire. Qu'il trouve ici la preuve de ma gratitude et sincères remerciements.

Mes remerciements vont également à Madame R. HADAoui (Maitre assistante à l'UMMTO) et Madame R. AOUDJIT (Maitre de conférences à l'UMMTO) qui ont accepté de juger ce modeste travail. Leurs conseils et leurs critiques seront sans aucun doute d'un grand apport scientifique.

Qu'il me soit permis de remercier tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Enfin, que tous ceux qui m'ont ouvert leur porte et offert leur amitié et leur aide soient assurés de ma profonde reconnaissance.

Sommaire

	Page
Introduction générale.....	01
Chapitre I. Généralités sur les Réseaux.....	03
I.1/ Définition des réseaux.....	03
I.1.1/ Les différentes topologies principales des réseaux.....	04
I.1.1.1/ Topologie en bus.....	04
I.1.1.2/ Topologie en anneau.....	04
I.1.1.3/ Topologie en étoile.....	05
I.1.2/ Les différents types de réseaux.....	06
I.1.2.1/ Les réseaux locaux.....	06
I.1.2.1.1/ Ethernet.....	06
Notation IEEE 802.3.....	06
La méthode d'accès à la parole : CSMA ICD.....	07
Limitations.....	07
Conclusion.....	07
I.1.2.1.2/ Token Ring.....	07
Principe.....	08
Topologie.....	08
Niveau physique.....	08
Trame.....	09
Protocol.....	09
Le moniteur (Le contrôleur du réseau).....	90
L'autotest matériel.....	10
Notion de priorité.....	10
Conclusion.....	10
I.1.2.2/ Objectifs des réseaux locaux.....	11
I.1.2.3/ Caractéristiques des réseaux locaux	11
I.2/ Modèle de transmission de données OSI.....	11
I.2.1/ Définition des couches du modèle OSI.....	12
La couche physique.....	12
La couche liaison de données.....	13
La couche réseau.....	14
La couche transport (routage).....	14
La couche session.....	15
La couche presentation.....	15
La couche application.....	15
I.3/ Les équipements réseaux	16
La carte réseau.....	16
Les adaptateurs (transceivers).....	16
Les ponts.....	17
Les commutateurs.....	17
Les routeurs.....	17

Les concentrateurs.....	17
Les passerelles.....	18
I.4/ Le protocole TCP/IP.....	18
I.4.1/ La couche application.....	19
I.4.2/ La couche transport.....	19
I.4.2.1/ Le protocole TCP.....	19
a. Fonctionnements.....	20
Transfert de donnée de base.....	20
Fiabilité.....	20
Contrôle de flux.....	20
Multiplexage.....	20
Connexion.....	21
b. Communication de données.....	21
C. Format de segment TCP.....	22
I.4.2.2/ Le protocole UDP.....	22
I.4.3/ La couche Internet.....	23
I.4.3.1/ Le protocole IP.....	23
I.5/ L'adressage IP.....	23
I.5.1/ Les classes d'adresses.....	24
Classe A.....	24
Classe B.....	24
Classe C.....	24
Chapitre II: Client/ Serveur.....	26
II.1/ Définition du Client/serveur.....	26
2.1. Paradigme Client/serveur.....	26
II.1.2/ Caractéristiques du Client/ Serveur.....	26
Service.....	26
Partage des ressources.....	26
Asymétrie des protocols.....	27
Transparence à la localisation.....	27
Assemblage multi vendeur.....	27
Echange de message.....	27
Encapsulation des services.....	27
Redimensionnement.....	27
Intégrité.....	27
II.1.3/ Evolution du Client/serveur.....	28
II.1.3.1/ Première génération.....	28
II.1.3.2/ Deuxième generation.....	29
II.2/ Intérêt du modèle Client/serveur.....	30
II.3/ Coexistence des modèles Client/serveur.....	31
II.4/ Extrémités du Client/serveur.....	31
II.5/ Principe de fonctionnement du client/serveur.....	32
Concepts de base.....	33

II.6/ Mise en œuvre du Client/serveur.....	34
II.6.1/ Les sockets.....	34
II.6.2/ Les TLIs.....	34
II.6.3/ Les RPCs.....	35
II.6.4/ Les MOMs.....	35
II.7/ Les modèles Client/serveur.....	35
II.7.1/ Types de serveurs.....	35
II.7.1.1/ Serveur de fichiers.....	35
II.7.1.2/ Serveur de base de données.....	36
II.7.1.3/ Serveur de transactions.....	36
II.7.1.4/ Serveur de groupware.....	36
II.7.1.5/ Serveur d'applications objet.....	36
II.7.1.6/ Serveur d'applications Web.....	36
II.7.2/ Orientation serveur & Orientation client.....	37
II.7.2.1/ Orientation serveur.....	37
II.7.2.2/ Orientation client.....	37
II.7.3/ Architecture Client/serveur multi tiers.....	37
II.7.3.1/ Architecture Client/serveur à deux niveaux.....	37
II.7.3.2/ Architecture Client/serveur à trois niveaux.....	38
II.7.3.3/ Principales fonctions du middleware.....	39
II.7.3.4/ Comparaison des architectures deux et trois niveau.....	40
II.7.3.5/ Architecture Client/serveur multi niveaux.....	40
II.8/ Avantages et inconvénients de l'architecture client serveur.....	41
II.8.1/ Avantages.....	41
II.8.2/ Inconvénients.....	42
Chapitre III: Système d'exploitation Windows.....	43
III.1/ Introduction.....	43
III.2/ Rôles du système d'exploitation.....	43
III.2.1/ Gestion du processeur.....	43
III.2.2/ Gestion de la mémoire vive.....	43
III.2.3/ Gestion des entrées/sorties.....	44
III.3/ Le système de fichiers.....	44
III.4/ Les types de systèmes d'exploitation.....	44
III.4.1/ Systèmes multitâches.....	44
III.4.2/ Systèmes multi-processeurs.....	44
III.4.3/ Systèmes embarqués.....	45
III.4.4/ Systèmes temps réel.....	45
III.5/ Microsoft Windows.....	46
III.5.1/ La gamme Windows est composée de 4 grandes branches.....	46
III.6/ Définition de la base de registre.....	47
III.6.1/ Avantages et inconvénients de la base de registre.....	47
III.6.2/ Editer la base de registres.....	48
III.6.3/ Répertoire de la base de registre.....	48
III.6.4/ Structure et contenu de la base de registre.....	49

Chapitre IV: Conception.....	52
IV.1/ Analyse.....	52
IV.1.1/Définition du besoin.....	52
IV.2.2/ Fonctionnalités.....	52
IV.2.3/ Identification des acteurs	53
IV.2.4/ Diagramme de contexte.....	53
IV.2.5/ Identification des espaces.....	53
IV.3/ Conception.....	54
IV.3.1/ La démarche de conception du système.....	54
Le niveau applicatif.....	54
Le niveau donné.....	54
IV.3.2/ Rôles et responsabilités.....	55
Administrateur.....	55
Utilisateur.....	55
IV.3.3/ Les fonctions globales du système.....	55
Fonction de l'administrateur.....	56
Fonction de l'utilisateur.....	56
IV.3.4/ Cas d'utilisation et diagrammes de cas d'utilisation.....	56
IV.3.4.1/ Administrateur.....	56
IV.3.4.2/ Utilisateur.....	57
IV.3.5/ Récapitulatif des diagrammes des cas d'utilisation.....	57
IV.3.6/ Spécification des scénarios.....	57
IV.3.6.1/ Définition.....	57
IV.3.7/ Description de cas d'utilisation.....	58
Chapitre V: Réalisation.....	64
V.1/ Objectif de l'application.....	64
V.2/ Les outils	64
V.2.1/ Environnement matériel	65
V.2.2/ Environnement de développement.....	65
V.2.2.1/ Système d'exploitation.....	65
V.3/ Routeur.....	65
V.3.1/ Installation et configuration de routeur.....	65
V.4/ Préparation des serveurs.....	70
V.4.1/ Serveur file.....	70
V.4.1.1/ Les droits des utilisateurs.....	70
1-Dossier Pere (Partage).....	71
2-Dossier sous pere (LABO).....	74
3-Dossier Lecteur Service (Achat).....	75
4-Dossier Responsable Service (achat D_achat).....	76
5-Dossier Partage Service (Achat achat).....	78
6-Dossier Utilisateurs (achat users).....	78
7-Dossier Partage tout le monde (Echange).....	80

8-Dossier Procedures Entreprise.....	82
9-Dossier Utilisateurs sans Service.....	38
V.4.2/ Serveur AD.....	85
V.4.2.1/ Créer un domaine.....	86
Installation.....	86
Configuration.....	90
V.4.2.2/ Réplication des données des AD (1 et 2).....	90
V.4.2.3/ Mettre toutes les machines dans le même domaine (AD).....	97
V.4.2.4/ Les cinq roles d'AD.....	98
V.4.3/ Serveur TMG.....	102
V.4.3.1/ Présentation du TMG.....	102
V.4.3.2/ Les composants du TMG.....	103
V.4.3.3/ Les principaux avantages et fonctionnalités de la TMG.....	103
V.4.4/ Serveur sauvegarde (symantec backup exe).....	106
V.4.4/ Serveur sauvegarde (symantec backup exe).....	106
V.4.5.1/ L'utilisation d'échange.....	107
V.4.5.2/ Création des groupe.....	109
V.4.6/ Serveur DHCP.....	109
V.4.7/ Serveur DNS.....	110
Installation et configuration d'un serveur DNS	112
V.4.8/ Réstriction des utilisateurs	130
Conclusion générale	133

Liste des figures

	Page
Figure I.1: Topologie en bus.....	4
Figure I.2: Topologie en anneau.....	5
Figure I.3: Topologie en étoile.....	5
Figure I.4 : Structure et les interactions entre les couches.....	12
Figure I.5: Modèle TCP/IP.....	19
Figure I.6: Diagramme d'une connexion TCP.....	21
Figure I.7: Le paquet TCP.....	22
Figure I.8 : Paquet UDP.....	22
Figure I.9 : Structure générale de l'adresse IP.....	23
Figure I.10 : Structure générale de la classe A.....	24
Figure I.11 : Structure générale de la classe B.....	24
Figure I.12 : Structure générale de la classe C.....	24
Figure II.1: La première génération de l'architecture Client/serveur.....	29
Figure II.2: La deuxième génération de l'architecture Client/serveur.....	30
Figure II.3 : Bornes du modèle Client/serveur.....	32
Figure II.4 : Principe de fonctionnement Client/serveur.....	32
Figure II.5: Le dialogue Client/serveur.....	34
Figure II.6 : Architecture Client/serveur 2-tiers.....	37
Figure II.7: Architecture Client/serveur 3-tiers.....	38
Figure II.8 : Architecture Client/serveur multi niveau.....	41
Figure III.1: Évolution du système d'exploitation Windows.....	46
Figure IV.1: Diagramme de contexte.....	53
Figure IV.2: Cycle de modélisation de l'application.....	55
Figure IV.3: Diagramme cas d'utilisation administrateur.....	56
Figure IV.4: Diagramme de cas d'utilisation de l'utilisateur.....	57
Figure IV.6: Cas d'utilisation «lancer le serveur».....	58
Figure IV.7: Cas d'utilisation «Ouvrir une session (AD) à utilisateurs».....	58
Figure IV.8: Cas d'utilisation «Ouvrir une session mail (EXCH) à utilisateurs».....	59
Figure IV.9: Cas d'utilisation «l'envoi des messages entre utilisateurs».....	59
Figure IV.10: Cas d'utilisation «Vérifier le système».....	60
Figure IV.11: Cas d'utilisation «se connecter aux serveurs».....	60
Figure IV.12: Diagramme de séquence « connecter au serveur AD».....	60
Figure IV.13: Diagramme de séquence « connecter au serveur EXCH».....	61
Figure IV.13: Diagramme de séquence globale.....	61
Figure IV.13: Diagramme de d'activité globale.....	62
Figure IV.14: Diagramme de classe globale.....	63
Figure V.1: Autorisations Spéciales Administrateur Local 1.....	71
Figure V.2: Autorisations Spéciales Administrateur Local 2.....	71
Figure V.3: Autorisations Spéciales Utilisateur Authentifiés 1.....	72
Figure V.4: Autorisations Spéciales Utilisateur Authentifiés 2.....	72
Figure V.5: Partage Administrateur.....	73

Figure V.6: Partage Utilisateur Authentifiés.....	73
Figure V.7: Partage Utilisateur du domaine.....	74
Figure V.8: Autorisations Spéciales Utilisateur Authentifiés 1.....	74
Figure V.9: Autorisations Spéciales Utilisateur Authentifiés 2.....	75
Figure V.10: Autorisation Spéciales Créateur Propriétaire 1.....	75
Figure V.11: Autorisation Spéciales Créateur Propriétaire 2.....	76
Figure V.12: Autorisation Spéciales Créateur Propriétaire 1.....	76
Figure V.13: Autorisation Spéciales Créateur Propriétaire 2.....	77
Figure V.14: Autorisation Spéciales GRP_RESP_Service.....	77
Figure V.15: Autorisation Spéciales GRP_SERVICE.....	78
Figure V.16: Autorisation Spéciales Créateur Propriétaire 1.....	78
Figure V.17: Autorisation Spéciales Créateur Propriétaire 2.....	79
Figure V.18: Autorisation Spéciales GRP_RESP_SERVICE.....	79
Figure V.19: Autorisation Spéciales Utilisateurs Authentifiés.....	80
Figure V.20: Autorisation Spéciales Créateur Propriétaire 1.....	80
Figure V.21: Autorisation Spéciales Créateur Propriétaire 2.....	81
Figure V.22: Autorisation Spéciales Utilisateurs Authentifiés.....	81
V.23: Autorisation Spéciales Créateur Propriétaire 1.....	82
Figure V.24: Autorisation Spéciales Créateur Propriétaire 2.....	82
Figure V.25: Autorisation Spéciales Utilisateurs Authentifiés.....	83
Figure V.26: Autorisation Spéciales Créateur Propriétaire 1.....	83
Figure V.27: Autorisation Spéciales Créateur Propriétaire 2.....	84
Figure V.28: Autorisation Spéciales Utilisateurs Authentifiés.....	84
Figure V.29 : Protection complète de la TMG.....	103
Figure V.30: Protection du réseau.....	104
Figure V.31: utilisation de DNS pour trouver l'adresse IP d'un ordinateur à partir de son nom	111
Figure V.33 : Editeur de stratégie de groupe local.....	130
Figure V.34 : Architecture de l'entreprise.....	131

Liste des tableaux

	Page
Tableau I.1: Couches physiques et leurs équipements	16
Tableau II.1 : Comparaison entre l'architecture Client/serveur deux et trois niveaux	40
Tableau III.1: Caractéristiques et types de systèmes d'exploitation	45

Introduction générale

L'évolution de l'informatique dans le monde des entreprises ces dernières années, a engendré la nécessité d'informatisation des processus de travail, afin d'assurer une bonne qualité de gestion des services dans l'entreprise.

Il est clair que l'informatique joue un rôle crucial au sein des entreprises dans lesquelles les systèmes doivent être de plus en plus performants du fait qu'elles sont soumises à une coriace et virulente concurrence. Pour la réalisation de tels systèmes, une méthode d'analyse des besoins, de conception et de réalisation s'impose.

Afin d'assurer le transfert des données d'une éternité à l'autre, il faut implanter une architecture logicielle permettant d'ordonner la transmission des informations et le stockage des données. L'architecture logicielle peut être définie par un ensemble de règles suivant une normalisation mondiale.

Les problèmes de stockage des données des utilisateurs et leurs gestions sont les plus réputés dans les entreprises en particulier, les problèmes qui relèvent de la sécurité des systèmes et de stockage posés par les anciens systèmes où les utilisateurs stockent leurs données sur les micro-ordinateurs. Ceci nous a incité à concevoir un système de stockage sécurisé et performant et à trouver un terrain d'application.

Notre projet de fin d'études porte sur la disposition d'un moyen efficace de gestion et de centralisation de l'information. Ce moyen permet de résoudre les problèmes des services de l'entreprise et offre aux futurs utilisateurs un environnement de communication et d'accès à l'information en toute simplicité et sécurité, sans se déplacer de son service pour avoir les informations nécessaires. Cela est assuré par notre conception en utilisant un serveur file sous un environnement Client/Serveur.

Pour mener à bien notre travail, nous avons structuré ce mémoire en cinq chapitres:

- Dans le premier, nous présenterons les principes des réseaux.
- Le second chapitre sera réservé aux notions du protocole de transmission de données TCP/IP.
- Le troisième chapitre sera consacré à l'étude de l'architecture client/serveur ainsi qu'à ses avantages et inconvénients.

- La conception de notre architecture ainsi que la réalisation et l'implémentation des différents modules dans un environnement client/serveur, seront abordées dans les quatrième et cinquième chapitres respectivement.

Nous terminerons enfin, par une conclusion générale et des perspectives relatives à notre travail.

Chapitre I: Généralités sur les Réseaux

Les réseaux informatiques ont pris peu à peu une importance considérable. Cet engouement provient essentiellement d'un besoin fondamental de communication. Ils sont nés d'un besoin d'échanger des informations de manière simple, rapide et sécurisé entre tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Dans une entreprise, il est important de communiquer et de partager l'information de manière sécurisée et rapide. Comme l'utilisation des réseaux informatiques évolue de plus en plus et prend de l'ampleur, les rondelles de communication se sont succédées depuis le début et leur performance n'a pas cessé d'augmenter. Les progrès technologiques en matière de conception de nouvelles techniques de communication et de la mise en place de nouveaux matériels plus adaptés ont permis de réaliser des architectures de réseaux aux caractéristiques très optimales afin de répondre aux exigences de la vie courante.

I.1/ Définition des réseaux :

Un réseau informatique est un système permettant à plusieurs appareils, d'échanger des informations. Bien sûr, les appareils en question sont souvent des ordinateurs. Cependant, il peut s'agir d'autres machines. Les automates d'une usine peuvent, par exemple, échanger des données afin d'exécuter des tâches particulières en fonction d'une situation.

Le réseau est souvent composé de câbles et d'éléments permettant d'envoyer les données sur câbles. C'est le cas d'un réseau filaire. Il peut également échanger les informations par l'intermédiaire des ondes. On parle alors de réseau sans fil.

La multitude des types de réseau a donné lieu à plusieurs classifications différentes. Une première manière de les classer est de les recenser par taille :

- ✓ Les petits réseaux locaux, restreints à une maison ou une entreprise par exemple, sont nommés LAN (Local Area Network) ou RLE (réseau local d'entreprise).
- ✓ Les réseaux repartis sur une surface moyenne, généralement de la taille d'une ville ou d'un campus universitaire, sont nommés MAN (Métropolitain Area Network).
- ✓ Enfin, les réseaux les plus importants, et en particulier Internet, sont appelés WAN (wide Area Network). Il s'agit là des réseaux d'opérateurs pouvant acheminer les informations sur plusieurs centaines, voire plusieurs milliers de kilomètres, et utilisant généralement la fibre optique.

I.1.1/ Les différentes topologies principales des réseaux :

Une topologie de réseau est une organisation physique et logique d'un réseau. L'organisation physique concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile, Maillé, Arborescence, ...). La topologie logique montre comment les informations circulent sur le réseau (diffusion, point à point).

I.1.1.1/ Topologie en bus :

Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau et les machines viennent s'y accrocher. Lorsqu'une station émet des données, celles-ci circulent sur toute la longueur du bus pour être, enfin, récupérées par la station destinataire. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

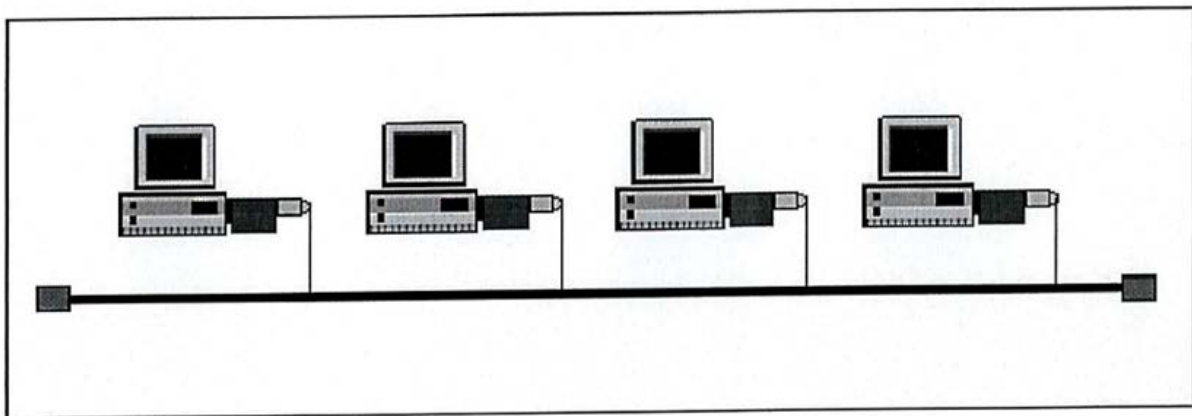


Figure I.1: Topologie en bus.

L'avantage de la topologie en bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est de plus, très facile à mettre en place. Par ailleurs, cette topologie présente un inconvénient majeur. En effet, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles.

I.1.1.2/ Topologie en anneau :

Développée par IBM, cette architecture principalement utilisée par les réseaux Token Ring, se base sur la technique d'accès par « jeton ». Les informations circulent de station en station suivant l'anneau autour duquel circule un jeton. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite ...

Le principe de la topologie en anneau est représenté dans la figure I.2.

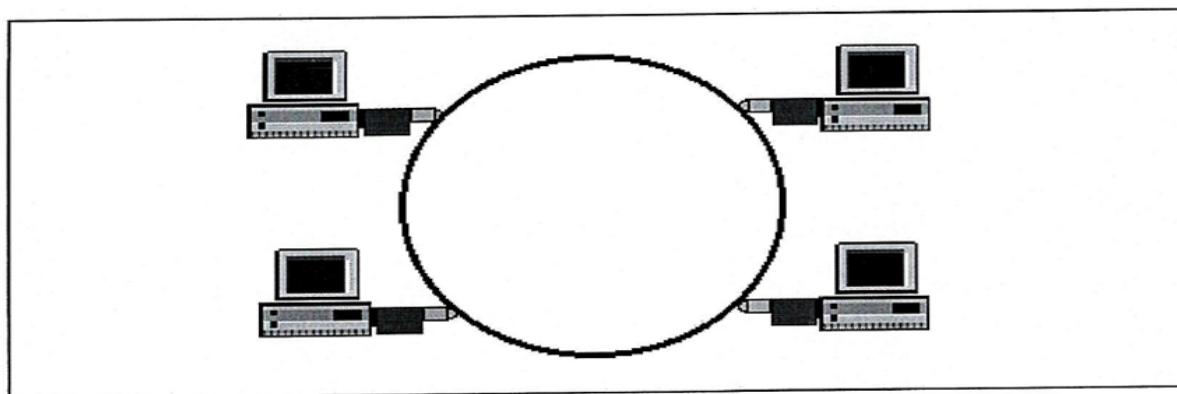


Figure I.2: Topologie en anneau

Cette topologie permet d'avoir un débit proche de 90% de la bande passante. Son avantage principal est que le signal qui circule est régénéré par chaque station. Néanmoins, la panne d'une station rend l'ensemble du réseau inutilisable. De plus, l'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre et à réaliser. Enfin, cette architecture étant la propriété d'IBM, les prix sont élevés et la concurrence est inexistante. Ce qui limite en fait, son utilisation.

I.1.1.3/ Topologie en étoile :

C'est la topologie la plus courante. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet des données vers le concentrateur, celui-ci les envoie à toutes les autres machines (hub) ou à celle qui en est le destinataire (Switch).

Ce type de réseau est facile à mettre en place et à surveiller. Son principal avantage est que la panne d'une station n'affecte pas l'ensemble du réseau. Par contre, si le concentrateur tombe en panne, tout le réseau est anéanti. Il est à noter que cette topologie nécessite plus de câbles que les autres avec un débit pratique moins bon. La figure I.3 représente le fonctionnement de cette topologie.

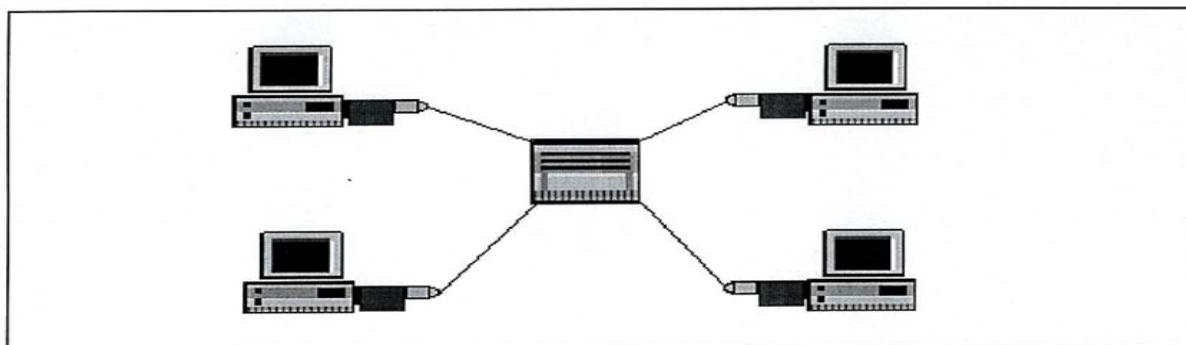


Figure I.3: Topologie en étoile

I.1.2/ Les différents types de réseaux:**I.1.2.1/ Les réseaux locaux :****I.1.2.1.1/ Ethernet :**

ETHERNET a été développé par Xerox vers le milieu des années 70. Ce réseau a fait suite au développement d'un projet de réseau de l'université d'Hawaii. Ce projet était novateur et prometteur car à cette époque, le concept de réseau local n'existait pas et la vitesse d'échange entre ordinateurs n'excédait guère 64 Kilobits par seconde.

Le principe est donc de mettre un support physique en commun et d'appliquer un bon débit sur des distances moyennes (> 100 m).

La spécification d'ETHERNET a été faite conjointement par DEC, Xerox et Intel. Un câble commun est utilisé pour relier des dizaines voir des centaines de machines. Ce câble commun va véhiculer les informations à destination de l'ensemble des stations. La méthode utilisée est le CSMA/CD (Carrier Sens Multiple Access / Collision Detection). L'architecture ETHERNET est aujourd'hui l'architecture la plus répandue dans le monde.

✓ Notation IEEE 802.3 :

Les réseaux Ethernet se nomment 10 base 5, 10 base T, 10 base 36, etc. Ce sont des notations IEEE, elles dépendent du débit utilisé, du mode de transmission et du câblage utilisé. Les débits possibles sont 1, 10, 100 Mbps et 1Gbps.

Les modes de transmissions sont :

- Bande de base (Base Band), transmission numérique.
- Large bande (Board Band), transmission analogique. Les câbles utilisés sont :
 - Gros coax.
 - Coax fin (cheapernet ou Ethernet fin).
 - UTP (unshieded twisted pair) 3 et 5, c'est-a-dire paire torsadée téléphonique et paire torsadée de meilleure qualité,
 - Fibre Optique MMF (Multi Mode Fiber) et SMF (Single Mode fiber).

✓ La méthode d'accès à la parole : CSMA ICD

Le principe d'Ethernet est que lorsqu'une station émet, tout le monde l'entend, par conséquent l'information est diffusée partout. Ce principe offre la possibilité de ne pas effectuer le routage.

Dans 802.3 et Ethernet, la méthode choisie est CSMA. Son principe est le suivant : on ne parle que quand personne ne parle.

Lorsqu' une station s'apprête à émettre, elle vérifie la liaison en écoutant. Si le câble est libre, elle émet et Si la voie est occupée, la station doit attendre et réessayer plus tard (CSMA persistant).

Une collision de signaux peut se produire, si deux machines transmettent simultanément. Pour palier à ce genre de problème, une détection des collisions sera effectuée (CD: collision detection). D'ou le nom de CSMA/CD.

✓ **Limitations :**

Si deux stations sont éloignées l'une de l'autre sur un RL, la première peut émettre une trame très courte, écouter son écho et penser que tout est bon. Cependant, il arrive parfois que la trame de cette première station n'arrive pas et ne soit pas écoutée par la seconde. Par conséquent, de l'autre coté, la deuxième station émet. Ce qui engendre une collision.

Pour contrecarrer ce problème, la norme impose une taille de trame Minimum de 512 bits et si le message n'est pas assez long, on rajoute des bits.

Cependant, il se trouve que parfois cette solution reste insuffisante. En effet, si la taille du réseau n'est pas limitée, le problème peut toujours se poser. On limite donc la taille du réseau en fonction de temps de retournement (Round Trip Delay) de la trame minimum et du débit. En résumé, pour éviter toute collision, il est nécessaire que le temps de mission d'une trame de 512 bits soit supérieur au temps d'un aller-retour du signal sur le réseau.

✓ **Conclusion :**

Les collisions que peut provoquer un réseau Ethernet sont remédiées par l'utilisation des Switch et des pongs. Ce qui fait d'Ethernet un réseau performant, rapide, peu couteux et facile à mettre en œuvre. C'est certainement pour ces raisons qu'il est utilisé dans la plupart des RL. Ethernet a donc réussi à imposer sa technologie.

I.1.2.1.2/ Token Ring :

Pour se démarquer d'Ethernet, IBM a promu un protocole portant le nom Token Ring et ayant au départ, un débit de 4Mbps ensuite, 16Mbps. En raison du manque d'organisation de l'accès à la parole initié par Ethernet: que chacun parle quand il veut, de sa méthode de détection des collisions qui se base sur le principe qu'on laisse se produire des erreurs et qu'on les traite quand elles arrivent, IBM n'as pas apprécié cette méthode et inventa l'anneau (RING) à jeton (Token) ou chacun parle quand on lui donne la parole.

✓ Principe :

Un jeton tourne, va de station en station. Lorsque l'on veut parler on attend que le jeton passe. S'il est libre on le marque occupé et on parle. Lorsque l'on reçoit un message on marque la trame pour signaler qu'on l'a lue et on la laisse continuer. L'émetteur reçoit donc la trame qu'il a émise en sachant si le destinataire l'a lue. Il libère le jeton et le passe à son voisin. Ceci évite l'émission simultanée de plusieurs trames et résout le problème de l'accès multiple. Soumis à de faibles charges, Token Ring est plus lent qu'Ethernet mais plus rapide (même 100Mbps) sur de lourdes charges car il ne s'écroule pas sous les collisions.

✓ Topologie :

En topologie logique c'est un anneau. C'est-à-dire une succession de liaisons point à point formant un cercle. Par contre sa topologie physique (qui peut aussi être un anneau) est souvent une étoile. L'étoile permet en fait, d'ajouter une station sur le réseau en service et d'assurer le bon fonctionnement de l'anneau en cas de panne d'une station.

Le TR était assez novateur pour le câblage car il utilise du matériel actif qui donne la configuration en étoile nommé MAU (Medium Access Unit) et c'est lui qui permet de détecter une coupure dans l'anneau et de la réparer immédiatement. C'est aussi cet équipement qui permet d'ajouter une station à « chaud ». Il est possible d'avoir un anneau d'étoiles en reliant plusieurs MAU ensemble. Le TR (Token Ring) peut compter jusqu'à 256 stations.

✓ Niveau physique :

La norme recommande d'utiliser des paires torsadées blindées bien qu'en théorie, on puisse aussi utiliser du coax ou de la fibre optique.

Les signaux de transmission sont en bande de base et utilisent les règles du codage Manchester Différentiel : un bit à 1 correspond à une transmission en début de l'intervalle temps du bit alors qu'un bit à 0 est caractérisé par l'absence de transmission. Cette méthode de codage est plus complexe mais offre une meilleure immunité aux bruits.

Les cartes TR sont conçues pour pouvoir émettre en même temps qu'elles reçoivent. En effet si l'anneau est court et que la trame est longue il se peut très bien que les premiers octets de la trame reviennent avant que les derniers ne soient émis.

✓ Trame :

La trame est constituée de :

- un en-tête
- un d'éliminateur de début de trame
- un contrôle d'accès pour indiquer la priorité de la trame pour signaler s'il s'agit du jeton ou d'une trame de données
- un contrôle de trame
- l'adresse réceptrice du destinataire
- l'adresse émettrice de l'expéditeur
- les données
- la queue
- une séquence de contrôle de trame, le CRC
- un d'éliminateur de fin de trame
- un état de trame, pour indiquer si la trame a été reconnue, copiée, ou si l'adresse de destination était indisponible,...

✓ Protocole :

La base du protocole est la capture de jeton lorsque l'on veut transmettre. Avant de procéder à l'émission de données, d'abord la station capture le jeton et peut le conserver pendant un certain temps appelé temps de maintien de jeton (THT : Token Holding Timer) dont la valeur est paramétrable (par défaut, la valeur de ce temps est de 10Ms).

Etant donné que le principe est basé sur un jeton, il est important de le surveiller pour éviter sa disparition. Une trame peut aussi tourner indéfiniment sur le réseau si son émetteur tombe en panne avant de la retirer. Afin d'échapper à ce problème, le réseau est doté d'une station appelée moniteur.

✓ Le moniteur (Le contrôleur du réseau) :

Le contrôleur de réseau est souvent la première machine allumée sur le réseau. Le contrôleur du réseau est responsable du bon fonctionnement du système Token Ring et ses tâches sont multiples :

- le contrôleur du réseau s'assure qu'il n'y a qu'un seul jeton qui circule.
- le contrôleur du réseau détecte si des trames ont fait plus d'une fois le tour de l'anneau.
- le contrôleur du réseau s'assure qu'il n'y a pas d'adresse en double. L'adresse de Chaque machine sur le réseau est unique.

-le contrôleur du réseau prévient les autres ordinateurs de l'arrivée d'une nouvelle station sur le réseau.

Mais il ne faut absolument pas qu'il ait plusieurs moniteurs. Car ceci provoquerait un retrait de trame non justifié. Pour cela, le moniteur va surveiller les trames AMP (Active Moniteur Présent) et s'il lui en arrive une qu'il n'a pas émise, c'est qu'il y a un autre moniteur.

✓ **L'autotest matériel :**

Le moniteur purge une trame qui boucle grâce à une trame PRG et cette solution est rappelée à chaque apparition d'un problème. Des fois la purge ne règle pas les problèmes. Dans ce cas, il y aura une élection d'un nouveau moniteur qui tente à son tour de purger l'anneau. Si le problème persiste, on fait appel à la phase d'autotest. Qui veut dire que toutes les stations du réseau se déconnectent et se font un test matériel complet. Ensuite, seules les stations s'étant reconnues comme saines se reconnectent et élisent un nouveau moniteur.

✓ **Notion de priorité :**

Le protocole de TR prévoit huit niveaux de priorité pour ses trames de zéro (trame courante) à sept (trame exceptionnelle et urgente). En fait, lorsqu'une station veut émettre, soit il n'y a pas du trafic, dans ce cas le niveau de priorité désiré est sans importance. Soit il y a du trafic et elle va utiliser le champ réservation (trois bits) de la trame qui passe devant elle en lui mettant son niveau de priorité. Si une autre station veut aussi émettre une réservation, elle ne pourra le faire que si son niveau de priorité est supérieur. Dans ce cas elle remplace l'ancienne réservation par la sienne. Cela signifie que lors d'un tour, c'est la plus prioritaire qui inscrit son niveau de priorité. Avant de procéder à la libération du jeton à la fin de l'émission, la station doit copier son niveau de réservation dans le champ priorité.

Les stations qui verront passer ce jeton libre, ne pourront le reprendre que si leur niveau de priorité est égal ou supérieur à celui indiqué dans le jeton. Par contre elles peuvent toujours effectuer des réservations avec les mêmes contraintes.

✓ **Conclusion :**

Les stations rattachées à un réseau token ring utilisent un court message spécial appelé « token » pour coordonner l'utilisation de l'anneau. Un seul token existe sur l'anneau à un moment donné. Pour émettre, un ordinateur doit attendre que le token lui parvienne, transmet exactement une trame et ensuite libère le token.

I.1.2.2/ Objectifs des réseaux locaux :

Le premier objectif d'un RL (Réseau Local) est économique. Il permet de partager les différentes ressources matérielles et logicielles entre les utilisateurs connectés aux réseaux.

L'avantage de partager des ressources matérielles est évident. Le besoin en nombre d'imprimantes, disques et même processeur est considérablement réduit. Celui des ressources logicielles n'est pas négligeable car on peut partager les logiciels à fin de ne pas acheter autant de licences que de postes. D'autres objectifs du LAN existent, tels que communiquer a haut débit, répartir les traitements et connecter tout le monde.

I.1.2.3/ Caractéristiques des réseaux locaux :

- ✓ Liaisons multipoint symétrique : multipoint signifie qu'il y a plusieurs entrées sur la liaison. Symétrique signifie que les équipements reliés peuvent discuter directement entre eux et sans intermédiaire.
- ✓ Distance limitée : pour obtenir des débits élevés, les RL limitent leurs tailles à une distance suffisante.
- ✓ Haut débit global: un LAN peut obtenir des débits élevés par exemple Ethernet peut avoir un débit de 10Mbps à 1 Gbps, par contre les WAN ont des débits relativement bas.
- ✓ Faible délais : les temps d'accès aux disques sont proches des temps d'accès à un disque Local.
- ✓ Diffusion : dans un RL quand un poste émet, toutes les adresses l'entendent. Dès qu'un poste entend un message qui ne lui est pas adressé, il l'ignore.
- ✓ Privé : les RL sont administrés par leurs propriétaires, par un opérateur.
- ✓ Grand nombre d'utilisateurs : les RL sont conçus pour accueillir un grand nombre de postes.

I.2/ Modèle de transmission de données OSI: [1]

Le modèle de référence pour l'échange de données informatiques est le modèle OSI (Open System Interconnexion) adopté par l'ISO (International Standards Organisation). Cette norme de communication repose sur l'empilement de 7 couches pouvant communiquer verticalement entre elles. Chacune des couches possède sa propre structure de données et sa propre terminologie. Le terme PDU (protocole data unit) est employé pour la description des données d'une couche.

Les couches basses présentent la manière dont la connexion physique est réalisée sur le câble alors que les couches hautes définissent l'interaction avec les applications finales et la communication entre nœuds s'effectuant virtuellement entre chaque couche.

La figure I. 4 résume la structure et les interactions entre les couches.

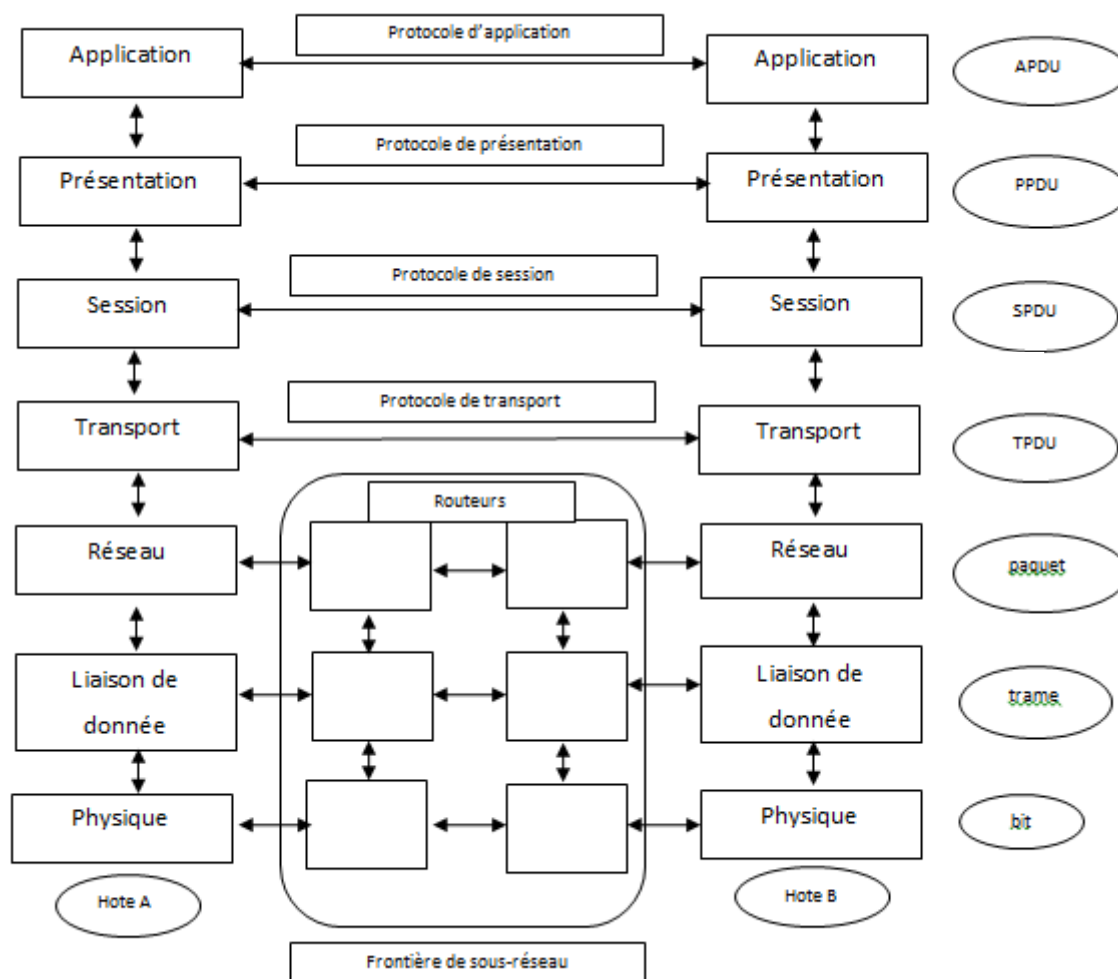


Figure 1.4 : Structure et les interactions entre les couches.

I.2.1/ Définition des couches du modèle OSI :

✓ **La couche physique :**

Cette couche se charge essentiellement de la transmission du bit à l'état brut sur un canal de transmission. L'objectif de conception de cette couche est d'assurer une transmission fiable d'un bit d'une éternité à une autre. Les questions posées portent généralement sur l'amplitude électrique associée aux différents niveaux du bit, la durée du bit et la possibilité de

transmission bidirectionnelle. Les problèmes de conception sont principalement des problèmes de télécommunication et concernent les interfaces mécaniques, la synchronisation et le support physique de transmission.

Cette couche fournit donc les moyens mécaniques, électriques et fonctionnels au maintien et à la désactivation des connexions physiques destinées à la transmission des éléments binaires (bits) entre entités de liaison.

La couche physique est constituée de :

- SUPPORT PHYSIQUE
- CONNECTEURS
- REPETEURS
- MODEMS
- MULTIPLEXEURS/DEMULTIPLIXEURS

✓ **La couche liaison de données :**

Le rôle principal de cette couche est de fournir à la couche supérieure (réseau) un moyen de communication fiable sans erreurs de transmission. Pour cela, les données sont décomposées en trams de données (quelques centaines ou milliers d'octets) puis envoyées en séquence. Le récepteur doit confirmer ou infirmer la réception de chaque trame. En général, des fonctions de gestions des erreurs y sont intégrées.

Cette couche doit aussi assurer qu'un récepteur lent ne soit pas submergé par des données émises par un émetteur rapide (régulation de flux).

Cette couche s'occupe des points suivants :

- Assure un transfert fiable des données.
- Adressage physique.
- Assure un contrôle de flux des données transmises.
- Utilise une procédure de transmission (HDLC, LLC, DSC).
- Gère la liaison des données.
- Données sous forme de trames.
- Transmission des trames en séquence.
- Reconnaissance des délimiteurs de trames (fanions) en réception.
- Gestion des trames d'acquittements.
- Détection des erreurs et reprise.

✓ **La couche réseau :**

Cette couche contrôle le fonctionnement des sous réseaux.

Le rôle essentiel de cette couche est de déterminer la manière dont les paquets sont routés de la source à la destination (routage).

De plus si le sous réseau est chargé (trop de paquets en circulation dans le sous réseau), des congestions auront lieu (freinage et éventuellement blocage de la circulation des paquets). C'est à la couche réseau de résoudre ces problèmes. Plus généralement, la couche réseau doit assurer la qualité de service 'QoS' (délais, temps de transit).

Etant donné que les réseaux interconnectés peuvent être hétérogènes, lorsqu'un paquet doit transiter par d'autres réseaux x pour atteindre sa destination les problèmes suivants peuvent surgir :

- La technique d'adressage peut différer d'un réseau à un autre.
- La taille de paquet gérée par les différents réseaux est différente ce qui peut résulter par un rejet du paquet au niveau d'un réseau car jugé trop grande.
- Les protocoles utilisés par différents réseaux peuvent être différents.

✓ **La couche transport (routage) :**

On distingue plusieurs classes de transport suivant la qualité des couches précédentes. Plus les couches inférieures sont complètes, moins la couche transport travaille et réciproquement.

Le rôle principal de cette couche est d'accepter des données de la couche supérieure, de les découper en paquets si nécessaire, de les transmettre à la couche réseau et d'assurer qu'elles arrivent correctement à destination.

C'est une authentique couche de bout en bout. En d'autres termes, un programme sur la machine source maintient une conversation avec un programme sur la machine destination (en utilisant les en-têtes de messages et des messages de contrôle).

En résumé cette couche s'occupe des fonctions suivantes :

- Assure les connexions de bout en bout.
- Accepte les données de la couche session et éventuellement les découpe.
- S'assure de l'ordonnancement.
- Fonctionnalité de bout en bout.
- Transport des données entre les unités hôtes.
- Assure la fiabilité du transport des données.
- Etablit, maintient et coupe les circuits virtuels.

- Détection et reprise sur incident.
- Contrôle de flux de l'information.
- Assure le multiplexage de plusieurs messages sur un canal donc nécessite d'indiquer quel message appartient à quelle connexion.
- Utilise les protocoles de transport : TCP, UDP.

✓ **La couche session :**

Cette couche s'occupe essentiellement de :

- Etablissement de la liaison avec le site distant.
- Ouverture et fermeture de session avec le site distant.
- Responsable de la synchronisation. On pose des points de resynchronisations (pour redémarrer en cas de problème sur un point précis).

Elle assure les fonctions du type:

- Gestion du dialogue (Bidirectionnel ou Unidirectionnel).
- Points de reprises.
- Retour arrière.
- Orchestration.
- Gestion des transactions.

✓ **La couche présentation :**

- S'intéresse à la syntaxe et à la sémantique des informations.
- Représentation des données transférées entre entités applications.
- Représentation de la structure de données et représentation de l'ensemble des actions effectuées sur cette structure de données.
- Encodage dans une norme agréée permettant à des équipements <ASCII> et <EBCDIC> par exemple de communiquer.
- Compression des données, chiffrement.

✓ **La couche application :**

- Fournit les services et interfaces de commutation aux utilisateurs. Elle contient une variété de protocoles qui sont utiles aux utilisateurs (http, Ftp, DNS ...).
- Offre au processus d'application le moyen d'accéder à l'environnement OSI. Les processus d'application échangent leurs informations par l'intermédiaire des entités

d'application (Terminal de réseau virtuel, Transfert de fichier, consultation des annuaires, courrier électronique...).

I.3/ Les équipements réseaux :

A chacun des trois premiers niveaux du modèle OSI correspondent des équipements réseaux spécifiques. Les niveaux supérieurs (du niveau 4 au niveau 7) sont traditionnellement traités de façon logicielle. Le tableau suivant regroupe les différentes couches physiques et leurs équipements.

Tableau I.1: Couches physiques et leurs équipements.

Niveau OSI	Equipement	Unité échangée
La couche application	-Serveur -Passerelle (Gateway)	
La couche réseau	-Routeur -Passerelle	Datagramme
La couche liaison de données	-Bridge (Pont) -Commutateur	Trame
La couche physique	-Répéteur -Concentrateur (Hub)	Bit

L'interconnexion de réseaux peut être locale : les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (répéteur, routeur, etc ...) suffit à réaliser physiquement la liaison. L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc ...)

✓ La carte réseau :

La carte réseau (appelée aussi carte d'interface réseau) en anglais NIC (network interface card). Il s'agit d'une carte connectée sur la carte mère de l'ordinateur et qui permet de l'interfacier au support physique permettant de transmettre l'information.

✓ Les adaptateurs (transceivers) :

Un répéteur (repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur

travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

✓ **Les ponts :**

Les ponts sont des dispositifs matériels permettant de relier des réseaux travaillant avec le même protocole. Le pont travaille également au niveau de la couche 2 du modèle OSI, c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées aux autres réseaux.

Cela permet de réduire le trafic sur chacun des réseaux et augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre bout.

✓ **Les commutateurs :**

Les commutateurs (switcher) sont similaires aux ponts, mais ils offrent une connexion plus directe entre les ordinateurs sources et destinations. Lorsqu'un commutateur reçoit un paquet de données, il crée une connexion interne séparée ou segmentée entre deux de ces ports et ne transmet le paquet de données qu'au port approprié de destination, en fonction des informations qui figurent dans l'en-tête de chaque paquet. Cette connexion est ainsi isolée des autres ports et permet aux ordinateurs sources et destinations d'accéder à la totalité de la bande passante d'un réseau.

✓ **Les routeurs :**

Un routeur est un périphérique qui joue le rôle de pont ou de commutateur, mais qui propose un plus grand nombre de fonctionnalités. Lorsqu'il transmet des données entre différents segments du réseau, le routeur examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet.

✓ **Les concentrateurs :**

Un concentrateur (hub) est un élément permettant de connecter le trafic provenant de plusieurs hôtes, et de régénérer le signal. Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.

Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé : répéteur multi ports.

✓ **Les passerelles :**

Les passerelles permettent à des architectures de réseaux différents de communiquer entre elles. Une passerelle peut réassembler différemment les données reçues d'un réseau pour permettre à chaque réseau de comprendre les données reçues d'un réseau ayant une architecture différente.

Une passerelle permet de relier deux systèmes qui n'utilisent pas:

- la même architecture.
- le même ensemble de règles de communication.
- la même structure de format de données.

I.4/ Le protocole TCP/IP: [2]

La Figure I.5 présente les différentes couches caractérisant les deux modèles TCP/IP et OSI. Il est à noter que le modèle OSI a été rapporté pour faciliter une comparaison entre les deux modèles.

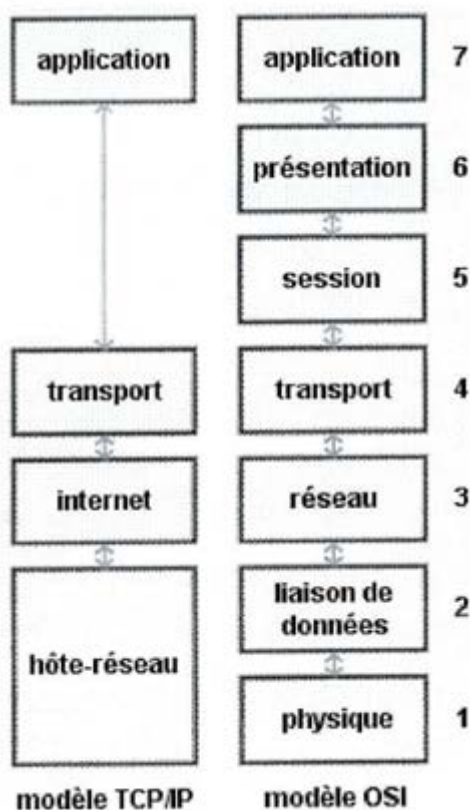


Figure 1.5: Modèle TCP/IP.

I.4.1/ La couche application :

C'est à ce niveau que les applications et utilitaires accèdent au réseau avec des protocoles. Ces derniers permettent la mise en forme et l'échange des informations utilisateur. Parmi les protocoles de cette couche : le FTP (File transfert protocole) fournit un moyen de transfert de fichiers, le HTTP (hyper text transfert Protocol) assure un transfert interactif de fichiers, le SMTP (Simple mail transfert Protocol) utilise pour le transfert de courrier électronique.

I.4.2/ La couche transport :

Dans cette couche se fait le contrôle de la méthode de remise de données grâce au protocole TCP (Transmission Control Protocol) et UDP (user datagramme protocol).

I.4.2.1/ Le protocole TCP :

Le TCP fournit un service fiable de connexion entre deux machines seulement. Cela signifie que le TCP/IP établit d'abord une connexion entre l'émetteur et le récepteur avant la remise de données, ainsi garantit le transfert de données par le biais d'un accusé de réception.

a. Fonctionnements :

Pour pouvoir assurer un service de communication de données fiable, au-dessus d'une couche de protocole TCP.

✓ Transfert de donnée de base :

Le protocole TCP a la capacité de transférer un flux continu découpé en paquets. Il assure le suivi de chaque octet reçu ou envoyé.

Les données envoyées par TCP, sous forme de flux d'octets, ne contiennent pas un véritable marqueur de fin de message dans le flux. Pour s'assurer de la transmission de toutes les données soumises au module TCP, une fonction PUSH est nécessaire. Celle-ci fait que TCP envoie rapidement toute donnée reçue en provenance d'une application.

✓ Fiabilité :

Le protocole doit prendre en considération et traiter les cas de données perdues, erronées, dupliquées, ou arrivées dans le désordre. Pour réaliser cela, le protocole TCP insère un numéro de séquence et oblige le TCP destinataire à l'émission d'un accusé de réception (ACK).

La rémission d'un paquet est ordonnée si l'accusé de réception n'est pas reçu au bout d'un temps prédéfini. L'élimination des erreurs physiques de transmission se fait par cette élimination des paquets pour lesquels les deux dernières valeurs ne correspondent pas.

✓ Contrôle de flux :

TCP met un moyen au destinataire pour contrôler le débit de données de l'émetteur. Cela est réalisé en retournant une information de fenêtre avec chaque accusé de réception. Cette fenêtre indique la capacité de réception instantanée en terme de numéro de séquence; c'est-à-dire, elle indique le nombre d'octets que l'émetteur peut émettre avant une autorisation ultérieure d'émettre.

✓ Multiplexage :

Plusieurs tâches d'une même machine peuvent communiquer simultanément par le biais des sockets et la combinaison d'une adresse IP et d'un numéro de port TCP ou UDP (un port est l'identificateur d'une application dans une machine).

Chaque machine affecte les numéros de port à ces applications indépendamment des autres machines. Cependant, il existe des ports réservés pour des services caractérisés et souvent utilisés.

✓ **Connexion :**

Une connexion nécessite la mise en place de deux sockets. Le numéro de port seul ne suffirait pas car chaque modèle TCP choisit indépendamment les numéros de ports et on pourra avoir un numéro identique pour deux applications différentes situées sur des machines distinctes lors d'une connexion TCP. On appelle ce mécanisme la poignée de main en trois temps. Le schéma suivant illustre cet échange :

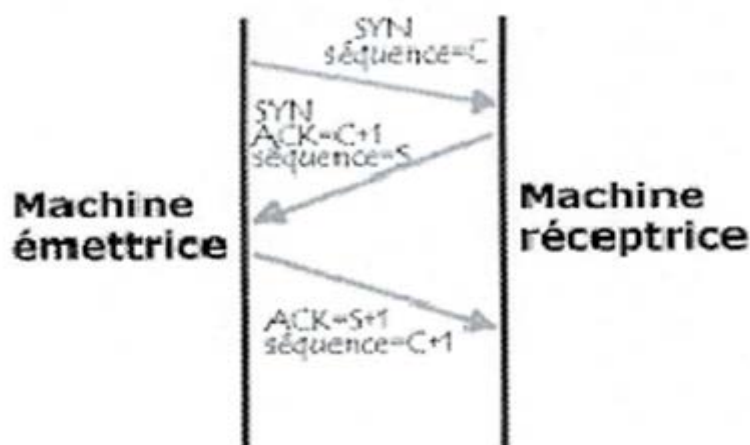


Figure I.6: Diagramme d'une connexion TCP.

b. Communication de données :

Les données circulant dans une connexion ouverte sont considérées comme un flux d'octets. TCP est libre de stocker les données soumises par l'application pour les émettre à sa convenance jusqu'à ce que le signal PUSH soit actif. Dans ce cas, toutes les données non émises doivent être émises immédiatement, Symétriquement lorsque le TCP récepteur voit le flag PUSH marqué. Il devra passer immédiatement toutes les données collectées à l'application destinataire. TCP dispose d'un moyen d'avertir l'application que dans le flux de données qu'il est en train de lire, au delà de la position de lecture courante, des données de caractère urgent sont apparues.

C. Format de segment TCP :

La figure I.7 représente le paquet TCP.

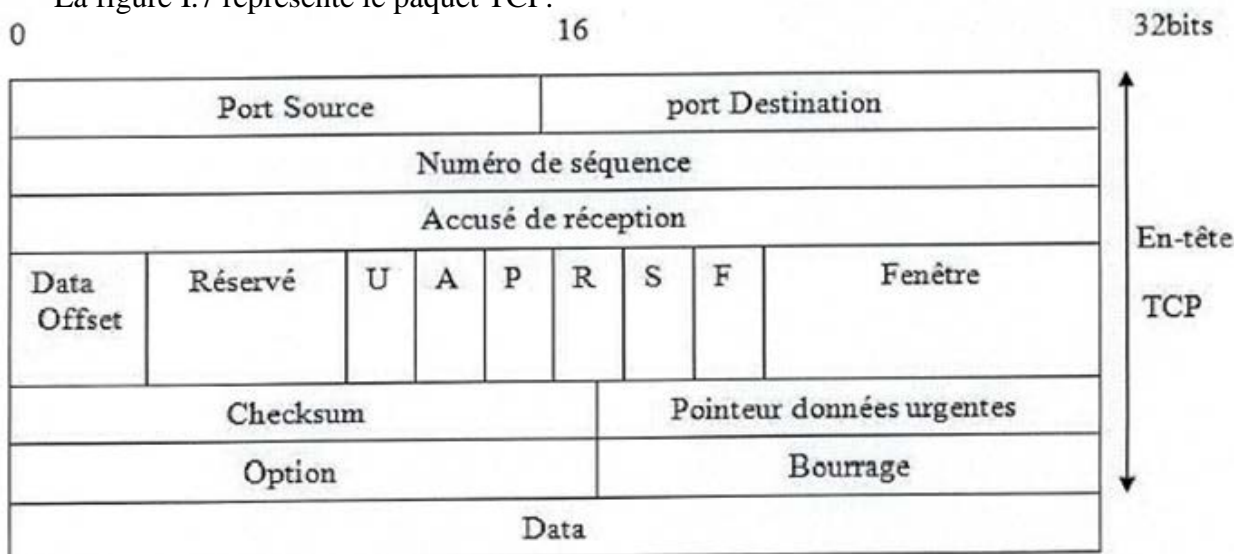


Figure 1.7: Le paquet TCP.

I.4.2.2/ Le protocole UDP :

Le protocole UDP offre un service en mode non connecté, qui se caractérise par une remise de donnés rapide mais non fiable. La figure suivante présente un paquet UDP.

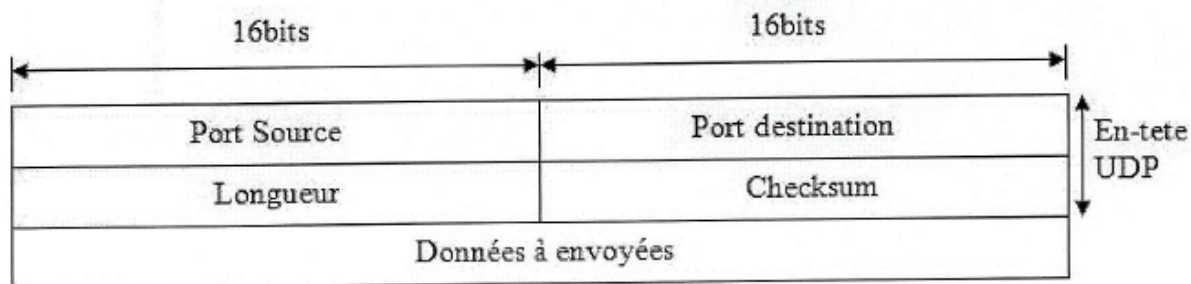


Figure I.8 : Paquet UDP.

La notion de port est utilisée dans UDP car l'application source doit fournir son numéro de port UDP ainsi que celui de l'application de destination. Le champ longueur donne le nombre de paquet UDP en octets, et grâce au champ Checksum les erreurs sont détectées sans pouvoir les corriger.

Parmi l'application qui nécessite l'utilisation d'UDP on distingue les applications au temps réel (cas d'une vidéo, conférence directe) et la multidiffusion.

I.4.3/ La couche Internet :

Cette couche est la plus importante du modèle TCP/IP. Elle est chargée d'adressage, du conditionnement et du routage. C'est à ce niveau que réside l'un des plus importants protocoles qui est le protocole IP ainsi que d'autres tels que :

- ARP (Adress Résolution Protocol) chargé d'identifier l'adresse MAC (Media Acces Control) de la carte réseau de l'ordinateur de destination à partir de son adresse IP.
- ICMP (Internet Control Message protocol) qui offre des fonctions de diagnostic et de signalement des erreurs dues à un échec de remise des données.
- IGMP (InternetGroup management protocol) responsable de la multidiffusion dans le TCP/IP.

I.4.3.1/ Le protocole IP:

Le protocole IP a été conçu pour réaliser l'interconnexion des réseaux informatiques et les communications entre systèmes. Le protocole IP est un protocole sans connexion non fiable qui est principalement chargé de l'adressage et du routage des paquets entre les ordinateurs mis en réseau. Il s'occupe également de la fragmentation des données.

I.5/ L'adressage IP :

Chaque composant impliqué dans une communication réseau doit posséder une adresse IP codée sur 32 bits, Permettant d'identifier un réseau unique et une machine particulière connectée sur ce réseau.

Une adresse IP est codée sur quatre octets représentés conventionnellement par quatre IP. Elle est composée d'un identificateur réseau suivi d'un identificateur machine, tel que montré par la figure I.10.

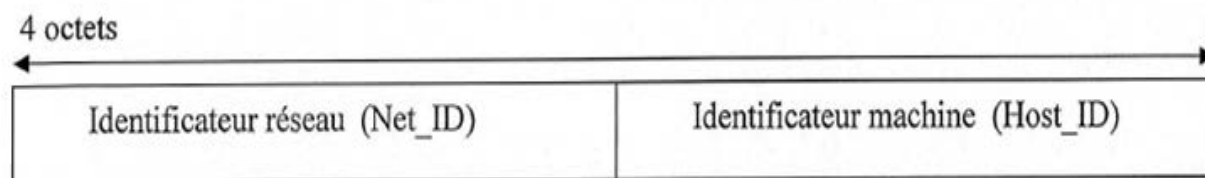


Figure I.9 : Structure générale de l'adresse IP.

I.5.1/ Les classes d'adresses :

La répartition des octets entre Net_ID et host_ID a généré des classes d'adresses IP et ces dernières sont distinguées par les premiers bits de poids fort du champ Net_ID.

✓ **Classe A :**

Cette classe A, représentée dans la figure I.11, est caractérisée par le premier bit de Net_ID qui égal à zéro et un espace d'adressage compris entre les adresse 1.0.0.1.Et126.255.255.254.

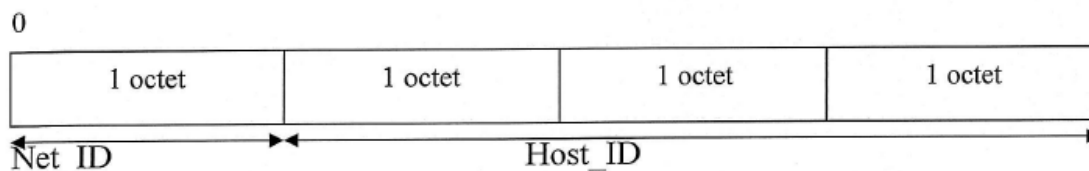


Figure I.10 : Structure générale de la classe A.

✓ **Classe B :**

La classe B (figure I.12) est caractérisée par les deux premiers bits Net_ID qui sont respectivement égaux à 10 et une plage d'adresse qui s'étale de 128.0.0.1 jusqu'à 191.255.255.254.

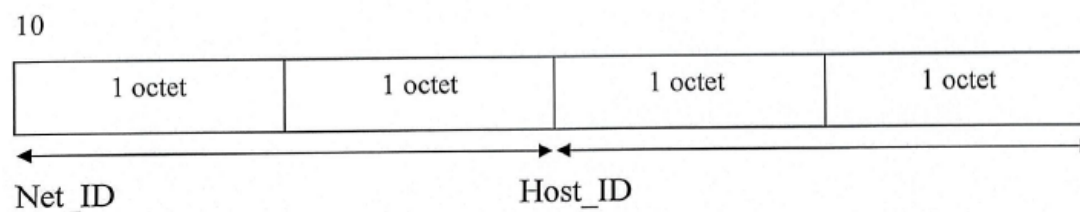


Figure I.11 : Structure générale de la classe B.

✓ **Classe C :**

Cette classe (figure I.13) est caractérisée par les trois premiers bits Net_ID qui sont respectivement égaux à 110 et une plage d'adresse comprise entre les adresses 192.0.0.1 et 123.255.255.254

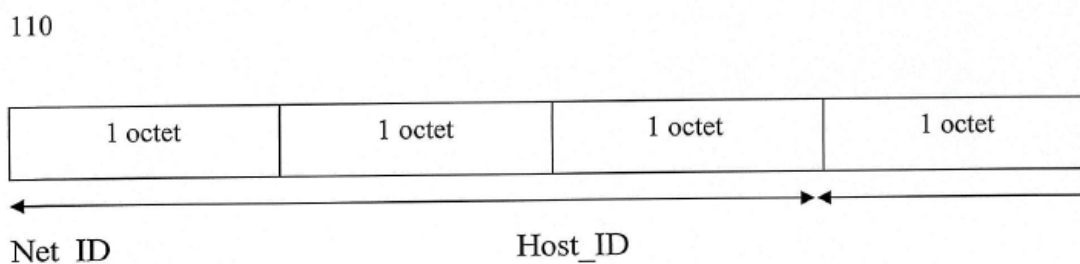


Figure I.12 : Structure générale de la classe C.

En conclusion:

Nous avons détaillé dans ce chapitre tout ce qui concerne le réseau de point de vu architecture, topologie, constitution, méthodes d'accès. L'un des composants software

constituant le réseau, le logiciel appelé Protocole. Pour développer notre application sous réseau nous avons utilisé le protocole sécurisé orienté connexion, supportant le fonctionnement de réseau qui est TCP/IP.

Le chapitre suivant est consacré à l'étude précise de l'architecture et du fonctionnement de ce dernier.

Chapitre 2: Client/ Serveur

L'informatique client/serveur est un mouvement irrésistible qui restructure l'utilisation de l'ordinateur. Malgré sa relative jeunesse, il est actif et ne laisse aucune facette de l'industrie informatique. «client/serveur» possède une particularité unique, c'est celle d'avoir des supporters à tous les échelons de cette industrie.

II.1/ Définition du Client/serveur :

Quoique le terme Client/serveur soit devenu un mot très répandu en informatique, il n'existe aucun consensus quant à sa signification exacte. Comme l'indique le terme : Client et Serveur sont des entités fonctionnant en harmonie sur un réseau afin d'accomplir une tâche bien définie.

II.1.1/ Paradigme Client/serveur :

La plupart des applications réseau modernes se fondent sur le paradigme Client/serveur. Le Client/serveur est un mode de dialogue entre deux entités. La première appelée client qui demande des services à l'entité serveur qui les exécute et envoie les résultats en retour. Le Client/serveur est souvent employé dans deux contextes : physique et logique. Dans le premier contexte, clients et serveurs représentent des systèmes physiques (machines) tandis que dans le second, ils relèvent du domaine logiciel et données donc à des processus. Dans ce cas, on peut avoir une application Client/serveur qui tourne sur une seule machine physique qui assurera le rôle de client et serveur en même temps.

II.1.2/ Caractéristiques du Client/ Serveur : [3]

Bien que le Client/ Serveur soit une forme d'informatique distribuée, il n'est supposé d'appeler systèmes Client/ Serveur que ceux qui partagent les caractéristiques suivantes :

✓ **Service** : Le modèle Client/ Serveur est essentiellement une relation entre des processus tournant sur des machines séparées. Le processus Serveur est un fournisseur de services. Le Client est le consommateur de ces services. Le modèle Client/serveur établit ainsi une séparation claire des rôles à partir de la notion du service.

✓ **Partage des ressources** : Un serveur est sensé pouvoir traiter plusieurs clients à la fois et contrôler leurs accès au ressources.

✓ **Asymétrie des protocoles** : La relation entre clients et serveur est de type plusieurs vers un. Toutefois le client est le déclencheur du dialogue en demandant un service alors que le serveur attend passivement les requêtes.

Notons que dans certains cas, quand un client invoque un service, il peut transmettre une référence de type callback à un objet, ce qui permet au serveur de le rappeler. Le client devient à son tour un serveur.

✓ **Transparence à la localisation** : Les processus client et serveur peuvent résider sur la même machine ou, par l'intermédiaire d'un réseau, sur deux machines différentes. Le logiciel Client/ Serveur masque aux clients la localisation du serveur en redirigeant les demandes de service si nécessaire. Un programme peut être client, serveur ou les deux.

✓ **Assemblage multi vendeur** : Le Client/ Serveur idéal est indépendant de la plate forme matérielle ou du système d'exploitation. On doit toujours pouvoir mélanger et appairer les plates formes Client/ Serveur.

✓ **Echange de message** : Clients et serveurs sont des systèmes à liaison épisodique qui interagissent au moyen de messages. Le message est un mécanisme d'émission de demandes de services et de réponses à celles-ci.

✓ **Encapsulation des services** : Le serveur est spécialiste, un message lui indique quel service est requis et c'est à lui de décider comment rendre ce service. Les serveurs peuvent être mis à niveau sans effet sur les clients tant que l'interface des messages reste la même.

✓ **Redimensionnement** : Les systèmes Client/ Serveur peuvent être redimensionnés horizontalement ou verticalement. Le redimensionnement horizontal correspond à l'ajout ou au retrait de stations clientes alors que le redimensionnement vertical correspond à la migration du serveur vers une machine plus puissante ou la distribution des charges de traitement sur plusieurs serveurs.

✓ **Intégrité** : Le code et les données du serveur sont gérés de façon centralisée, chose qui garantit un moindre cout de maintenance et une meilleure intégrité des données tandis que les clients restent individuels et indépendants.

II.1.3/ Evolution du Client/serveur :

Les architectures mainframe, apparues dans les années 60 dans lesquelles tout était centralisé et les utilisateurs n'étaient équipés que de simples terminaux passifs, ont vite montré leurs limites d'utilisation car elles ne pouvaient absorber les nouvelles technologies.

Une nouvelle orientation est apparue donnant naissance à une génération d'informatique axée sur les concepts de flexibilité et d'interopérabilité ainsi que la mouvance des applications et l'ouverture aux nouvelles technologies. Cette génération est celle du Client/serveur.

Apparu pour répondre aux problèmes que posaient les systèmes centralisés, le Client/serveur permet, par l'utilisation de nouvelles méthodes et techniques, de surpasser les limites de l'environnement mainframe et procurer ainsi à l'entreprise certains avantages tels que la souplesse et le pouvoir d'adaptation aux mutations. Le Client/serveur a connu deux stades de générations :

II.1.3.1/ Première génération :

Apparue vers la fin des années 80 et connue sous le vocable du client/serveur de données, elle est basée sur des applications clientes opérant autour d'un SGBD relationnel. La base de données est implémentée au niveau du serveur avec le langage SQL et l'application est développée au niveau du client. Le code source est exécuté sur la machine du client. L'architecture globale de cette génération est donnée dans la figure suivante:

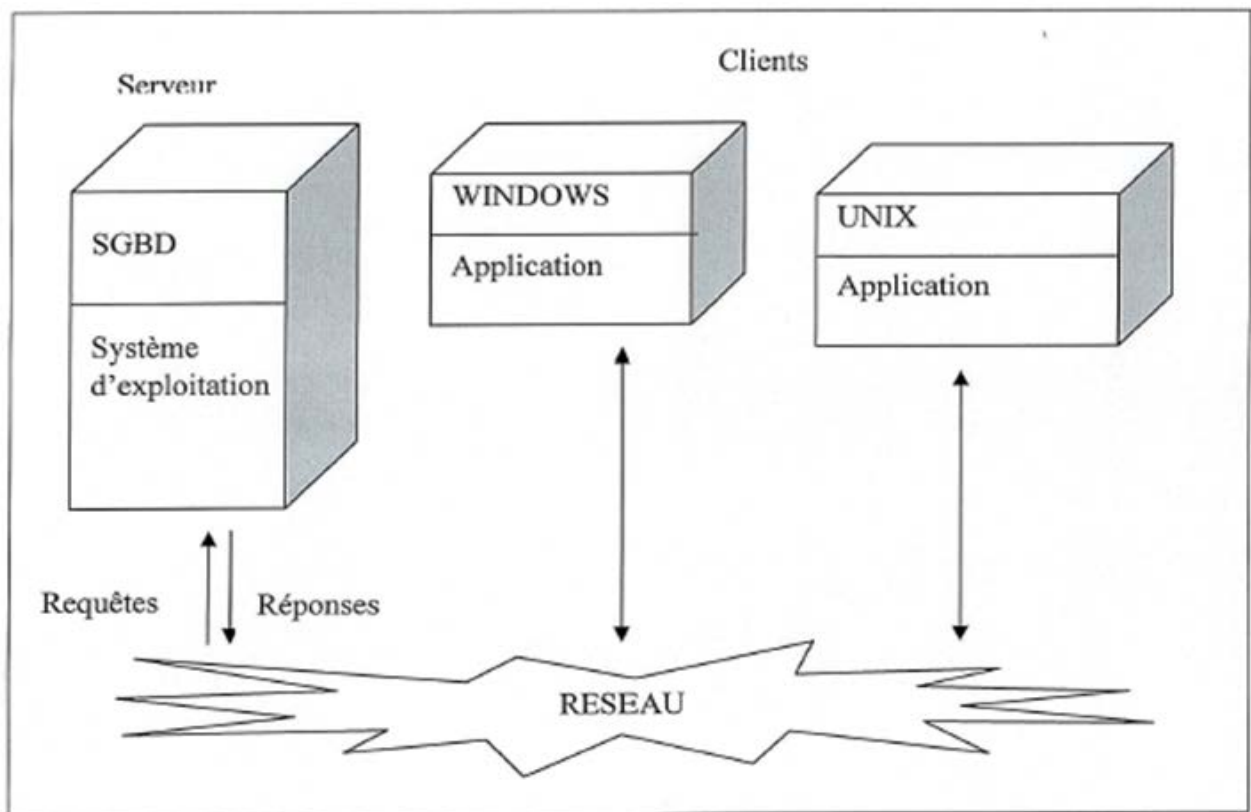


Figure II.1: La première génération de l'architecture Client/serveur.

II.1.3.2/ Deuxième génération :

Cette génération a connu une grande évolution où de nouveaux outils apparaissent. Ces derniers permettent l'optimisation des performances, facilitent la réutilisation des composants ainsi que la gestion des configurations complexes (nombre important de clients).

Trois caractéristiques marquent cette génération à savoir:

- Le traitement applicatif se fait au niveau du serveur et implémenté sous forme de procédures et fonctions.
- Le déploiement des applicatifs se fait automatiquement entre le serveur et le client et ce avec la gestion d'un référentiel des objets de l'application ce qui réduit le trafic sur le réseau.
- L'utilisation intensive de l'approche objet

Le Client/serveur de la deuxième génération est représenté dans le schéma suivant:

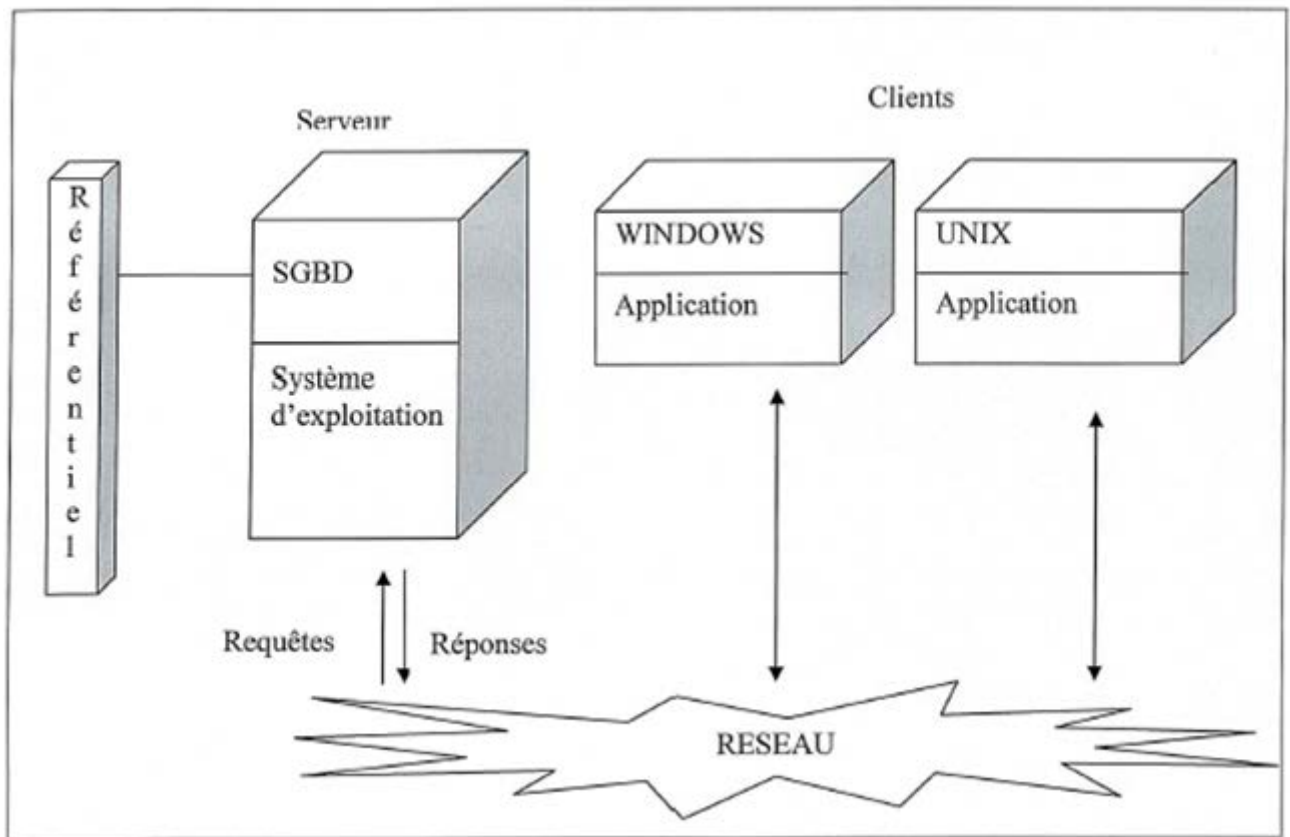


Figure II.2: La deuxième génération de l'architecture Client/serveur.

II.2/ Intérêt du modèle Client/serveur :

Le modèle Client/serveur s'impose dès lors que l'on souhaite décomposer l'exécution d'une application et faire en sorte que différentes machines (au sens large; matérielles et logicielles) y participent et ce par opposition aux techniques de calcul centralisées sur mainframe où tout se fait au niveau du serveur central.

Les intérêts d'une telle décomposition sont multiples:

- Exploitation : Il est alors facile d'utiliser (préparer) les entrées et comprendre les sorties d'un système ou d'un composant. Ceci implique une meilleure maîtrise du système d'information.

- Flexibilité : Il est possible de modifier un système ou un composant pour le réutiliser dans des applications et environnements autres que ceux pour lesquels il a été conçu.

- Interopérabilité : Les systèmes ou les composants peuvent communiquer, échanger les informations et les utiliser facilement.

- Mise à l'échelle : Il est aisé de mettre à l'échelle le système ou le composant selon la dimension du problème à résoudre.

II.3/ Coexistence des modèles Client/serveur : [4]

Les modèles d'extrémité relativement simples peuvent coexister. En effet, pour éviter le cumul sur un même bureau de deux postes de travail physiques (poste passif et microordinateur), les micro-ordinateurs disposent de logiciels leur permettant de se comporter vis à vis du réseau et des applications centrales comme s'ils étaient des terminaux passifs. Ces logiciels ont pour nom générique "émulateur de terminal" (sous-entendu de terminal passif). Grâce à ces logiciels, le micro-ordinateur peut cumuler les fonctions de traitement local et le rôle de poste de travail passif. Ainsi, le schéma centré sur le serveur n'est pas affecté car les applications existantes continuent à dialoguer avec le logiciel d'émulateur de microordinateur comme s'il s'agissait d'un terminal passif. Il y a coexistence sur un même poste physique, du monde de la micro-informatique et du monde centré sur le serveur.

Cette coexistence des modèles d'extrémité sur un même système (micro) doit être soigneusement distinguée des modèles dans lesquels plusieurs systèmes coopèrent pour exécuter un système interactif. Le mécanisme de coopération entre ordinateurs s'est instauré dans différentes directions. Une branche s'est développée dans le monde des micro-ordinateurs qui partagent des données entre eux ou avec mainframes. Parallèlement, le monde des micro-ordinateurs a montré ses limites car le besoin de mettre en commun des documents est devenu important. Des techniques, permettant de rendre accessible les données et fichiers par des micro-ordinateurs connectés à un réseau sont apparues, et avec elles, le terme Client/serveur s'est vulgarisé.

II.4/ Extrémités du Client/serveur : [5]

Les systèmes de traitement interactifs se situent entre deux bornes appelées aussi modèles d'extrémité. L'une des extrémités repose sur un schéma selon lequel la totalité des traitements interactifs s'effectue sur un ordinateur puissant et spécialisé dont les ressources sont partagées par des ordinateurs passifs, l'autre extrémité est matérialisée par des microordinateurs fonctionnant en mode isolé.

La figure suivante montre les modèles d'extrémité du Client/serveur

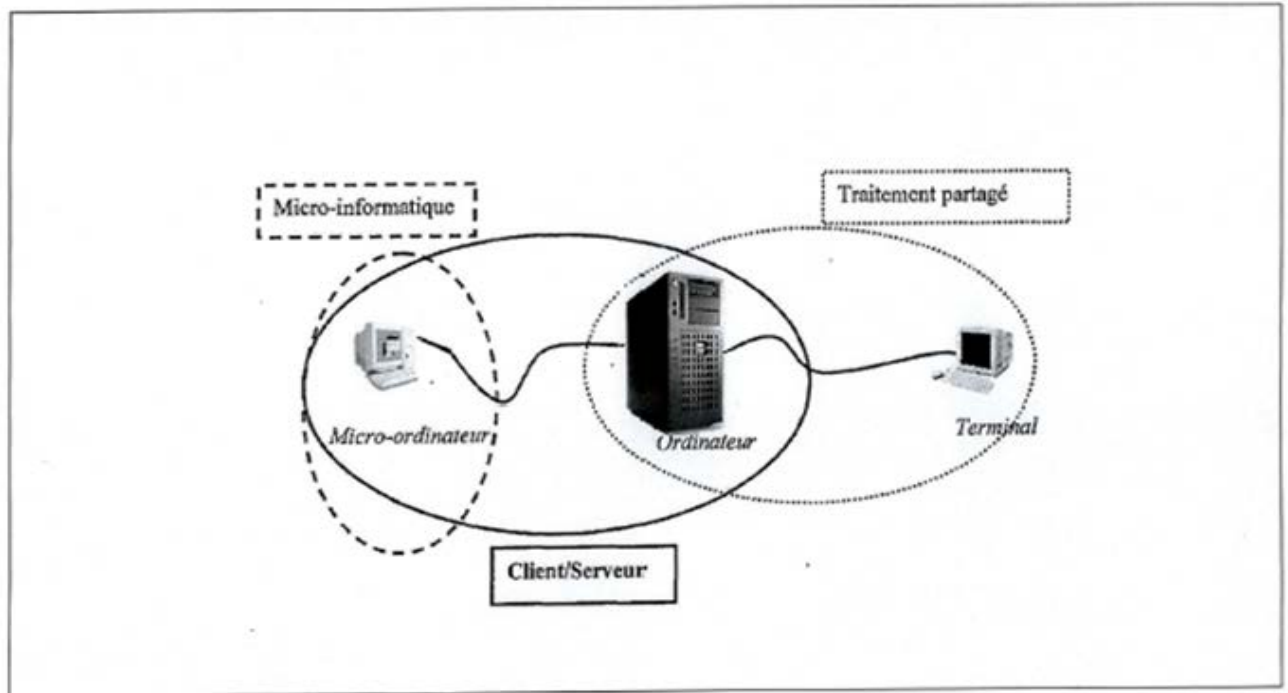


Figure II.3 : Bornes du modèle Client/serveur.

II.5/ Principe de fonctionnement du client/serveur:

Le Client/serveur est avant tout un mécanisme de dialogue entre deux processus. Ce modèle de communication est basé sur la fourniture de services par le processus serveur au processus client qui les demandent.

Le dialogue entre client et serveur consiste en l'envoi d'une requête au serveur qui l'exécute puis renvoie en retour la réponse appropriée (résultats) au client.

Le principe de fonctionnement du Client/serveur est illustré dans la figure suivante

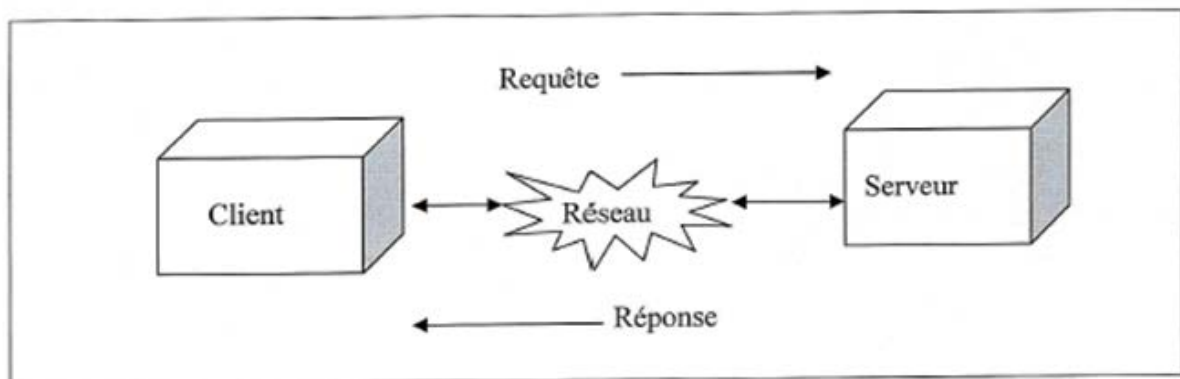


Figure II.4 : Principe de fonctionnement Client/serveur.

Concepts de base

Le vocabulaire de base de l'informatique Client/serveur manipule plusieurs concepts dont nous citons les notions de, Client, Serveur, Requête, Réponse, Middleware.

- ✓ Client : processus demandant l'exécution d'une opération à un autre processus par envoi d'un message contenant le descriptif de l'opération à exécuter et attendant la réponse à cette opération par un message en retour.
- ✓ Serveur: processus accomplissant l'opération sur demande d'un client et transmettant la réponse à ce client.
- ✓ Requête (requête) : message transmis par un client à un serveur décrivant l'opération à exécuter pour le compte du client.
- ✓ Réponse (reply): message transmis par le serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'application.
- ✓ Middleware: c'est le logiciel qui, situé au milieu, assure les dialogues entre les clients et les serveurs. Il est souvent hétérogène. En d'autres termes il constitue l'ensemble des services logiciels construits au-dessus du protocole de transport afin de permettre l'échange Requête-réponse de manière transparente en cachant l'hétérogénéité des composants mis en jeu (SGBD, réseau).

Notons au passage que le client est toujours le premier à engager la conversation en sa qualité de demandeur et ce par envoi d'une requête au serveur qui l'attend puis réalise l'opération demandée et fournit la réponse au client.

Les appels aux services de transport mis en jeu sont au nombre de quatre :

- **SEND REQUEST ()**: permet au client d'émettre le message décrivant la requête.
- **RECEIVE REQUEST ()** : permet au serveur de recevoir la requête en sa porte d'écoute.
- **SEND REPLY ()**: permet au serveur d'envoyer la réponse sur la porte d'écoute du client.
- **RECEIVE REPLY ()**: permet au client de recevoir la réponse en prévenance du serveur.

La figure suivante illustre le dialogue Client/serveur

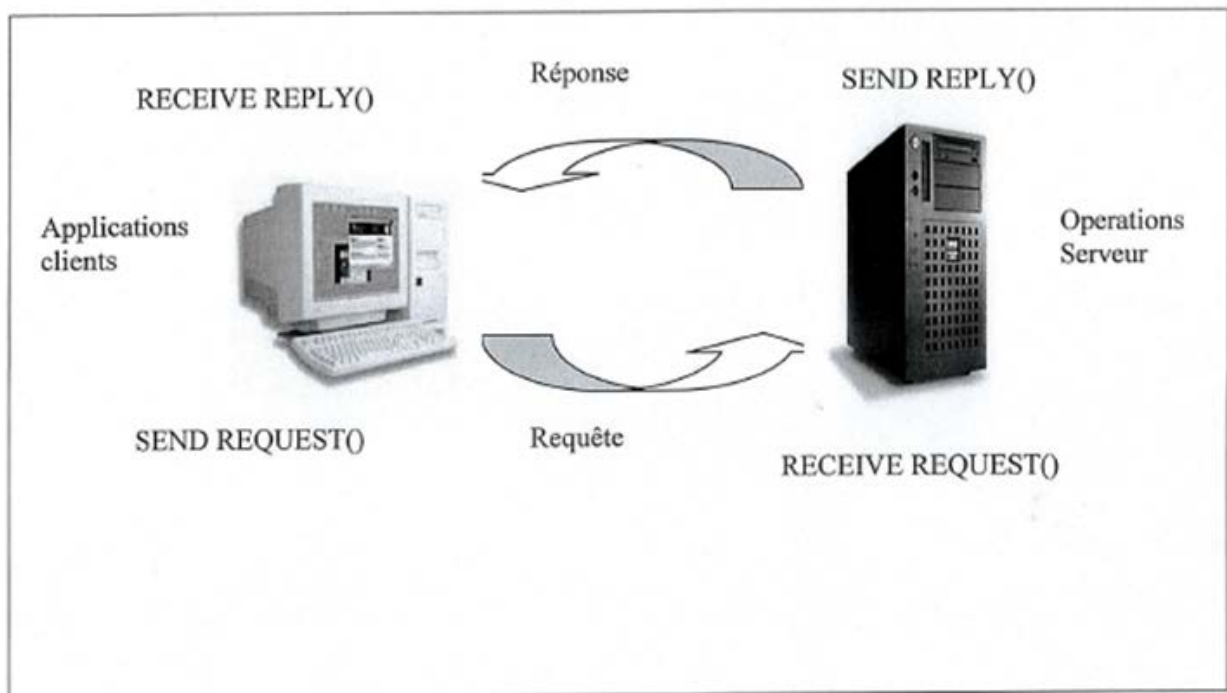


Figure II.5: Le dialogue Client/serveur.

II.6/ Mise en œuvre du Client/serveur:

Tandis que le Client/serveur est bâti sur l'idée de partage d'une application de chaque côté d'une frontière entre client et serveur pour créer diverse solutions sur des réseaux locaux; la mise en œuvre de sa partie communication s'appuie sur plusieurs mécanismes parmi lesquels nous citons : les API-sockets, les RPCs, les TLIs, les OREs, les MOMs,...etc.

II.6.1/ Les sockets :

Un socket, appelle aussi API (Application Program Interface), est l'interface entre les programmes d'application et la couche transport. Les APIs sont utilisées dans la programmation réseau, elles fournissent un accès aux protocoles de transport et par conséquent, elles forment un point de communication par lequel un processus peut émettre et recevoir des informations.

II.6.2/ Les TLIs :

Une TLI (Transport Layer Interface) fournit une interface à la couche transport du modèle OSI, en s'appuyant sur le mécanisme général d'E/S par Stream (image du flot de données établi entre l'utilisateur et un périphérique d'E/S via son driver).

II.6.3/ Les RPCs :

Les RPCs (Remote Procedure Call) fournissent le mécanisme d'appel de procédures distantes (s'exécutants sur d'autres machines).

L'utilisation des RPCs permet au programmeur d'applications distribuées de ne pas se préoccuper des détails de l'interface réseau. L'indépendance des RPCs vis-à-vis du transport sépare complètement l'application des éléments physiques et logiques de la communication des données.

II.6.4/ Les MOMs :

(Message Oriented Middleware); protocole de communication assurant La gestion d'envoi de messages en environnement réseau, permet une communication d'égal à l'égal notamment la diffusion d'événements vers les acteurs connectés.

Les MOMs offrent plusieurs avantages; tels que:

- Intégration de multiples protocoles et plates formes.
- Définition des messages par les utilisateurs.
- Equilibrage des charges.
- Tolérance aux pannes.
- Support pour plates formes hétérogènes.

II.7/ Les modèles Client/serveur : [6]

Alors que certains différencient les applications Client/serveur selon les services qu'elles offrent (Le selon les types de serveurs), et d'autres préfèrent les distinguer par la façon dont les fonctions distribuées se partagent entre le client et le serveur et utilisent plutôt les termes Orientation client, Orientation serveur; les préteurs du Client/serveur préfèrent utiliser les termes d'architectures Client/serveur à deux ou trois niveaux.

II.7.1/ Types de serveurs :**II.7.1.1/ Serveur de fichiers :**

Dans le cas de serveur de fichiers, le client requiert des enregistrements de fichiers en émettant des requêtes au serveur de fichiers. Les serveurs de fichiers sont utiles pour partager des fichiers sur un réseau et ils sont indispensables pour créer des banques de documents d'images, etc...Sa faiblesse réside dans l'obtention de l'information qui nécessite de nombreux échanges de messages sur le réseau.

II.7.1.2/ Serveur de base de données :

Dans le cas de serveur de base de données, le client émet des requêtes SQL sous forme de messages en direction du serveur. Le résultat de chaque requête est renvoyé au client. Les données ainsi que le code qui traite les requêtes, résident sur la même machine (serveur). Le serveur utilise sa propre capacité de traitement pour rechercher les données demandées au lieu de transmettre tous les articles au client et de le laisser en faire la sélection. Ainsi la puissance répartie est utilisée de façon beaucoup plus efficace.

II.7.1.3/ Serveur de transactions :

Dans ce modèle, les clients invoquent des procédures distantes résidant sur le serveur qui comporte un moteur de base de données SQL. Ces procédures distantes exécutent un ensemble d'instructions SQL. L'échange sur le réseau consiste en un seul message de Requête/Réponse (une réponse pour un bloc de requête SQL). Pour ce type de serveur l'application Client/serveur nécessite du code source au niveau du serveur.

II.7.1.4/ Serveur de groupware :

Le groupware s'intéresse à la gestion d'informations semi structurées telles que le texte, l'image, le courrier, la messagerie et l'ordonnancement des tâches. Ces systèmes Client/serveur mettent les utilisateurs en contact direct les uns avec les autres, Microsoft Exchange est un exemple de ce type.

II.7.1.5/ Serveur d'applications objet :

Dans ce type de serveur, l'application Client/serveur est écrite sous forme d'un jeu d'objets communicants. Les objets clients communiquent avec les objets serveurs au moyen d'un courtier d'objet ou ORB (Object Request Broker). Le client invoque une méthode sur un objet distant, l'ORB localise une instance de la classe, appelle la méthode demandée et envoie les résultats à l'objet Client.

II.7.1.6/ Serveur d'applications Web :

L'internet est la plus grande application Client/serveur dite intergalactique. Ce nouveau modèle consiste en des clients légers et portables qui communiquent avec de très gros serveurs. Le serveur web par exemple, renvoie des documents lorsque le client les

demande par leurs noms. Clients et serveurs communiquent via un protocole de type RPC appelé HTTP (Hyper Text Transmission Protocol).

II.7.2/ Orientation serveur & Orientation client :

II.7.2.1/ Orientation serveur :

Le modèle orienté serveur place plus de fonctionnalité sur le serveur sur lequel tourne le gros de l'application. Les serveurs de groupware, de transaction et les serveurs web sont des cas exemples des modèles orientes serveur.

II.7.2.2/ Orientation client :

La forme la plus traditionnelle est le modèle orienté client, dans lequel le gros de l'application tourne du coté client. Dans les modèles serveurs de bases de données et serveurs de fichiers, les clients connaissent l'organisation et la localisation des, données sur le serveur.

II.7.3/ Architecture Client/serveur multi tiers : [7]

II.7.3.1/ Architecture Client/serveur à deux niveaux :

L'architecture à deux niveaux (2-tiers) est l'architecture la plus classique, elle décrit les systèmes Client/serveur dans lesquels, la logique applicative est enfouie soit dans l'interface utilisateur chez le client, soit dans la base de données chez le serveur (ou dans les deux à la fois).

Dans cette architecture, le serveur exécute la requête du client et fournit directement le service, sans faire appel à d'autres intermédiaires.

L'architecture Client/serveur à deux niveaux est schématisée comme suit:

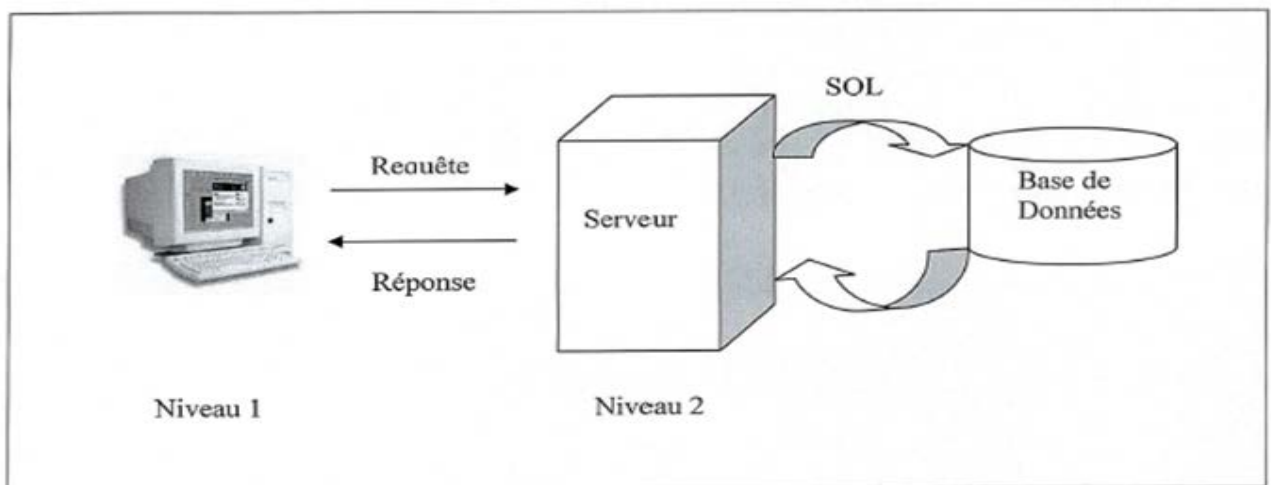


Figure II.6 : Architecture Client/serveur 2-tiers.

II.7.3.2/ Architecture Client/serveur à trois niveaux :

Dans cette architecture; la logique applicative réside dans un niveau intermédiaire, séparément des données et de l'interface utilisateur. Les trois niveaux de cette architecture sont:

- Le client (niveau 1) : demandeur de ressources.
- Le serveur d'application (niveau 2) : appelé aussi middleware, il est chargé de fournir les ressources mais en faisant appel à un autre serveur.
- Le serveur de base de données (niveau 3) :c'est celui qui fournit le service au serveur d'application.

La figure ci-jointe montre les niveaux de l'architecture 3-tiers :

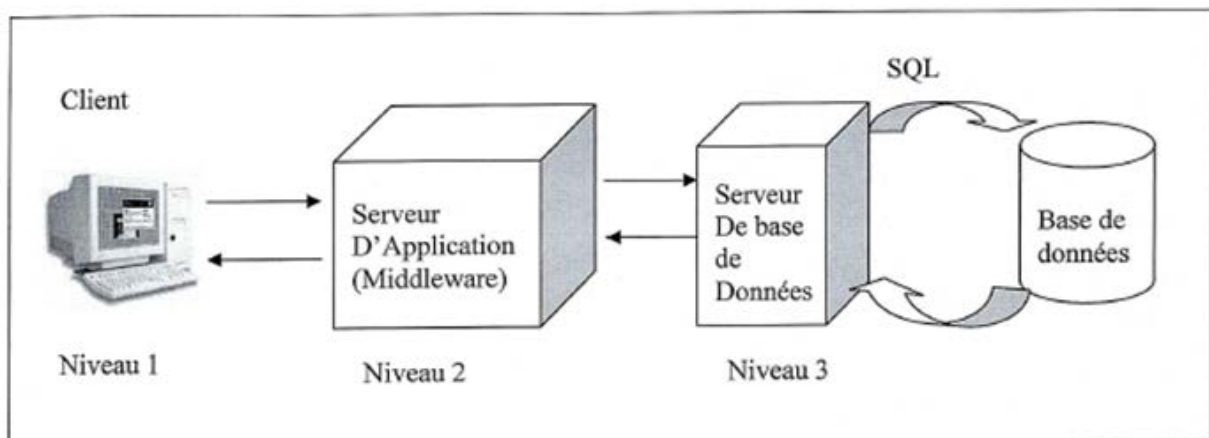


Figure II.7: Architecture Client/serveur 3-tiers.

En théorie, les systèmes à trois niveaux sont, contrairement à ceux de deux niveaux, mieux dimensionables, plus robustes et plus souples.

Le modèle à trois niveaux est recommandé si l'application possède une des caractéristiques suivantes :

- Nombreux services ou nombreuses classes (plus de 50).
- Application écrite dans plusieurs langages ou par différentes organisations.
- Sources de données multiples et hétérogènes.
- Application évolutive (modifications et ajouts), de longévité supérieure à 3ans.
- Importante charge de traitement; plus de 50 000 transactions par jour ou plus de 300 utilisateurs accédant simultanément à la même base de données,
- Importante communication inter applications.
- Croissance de l'application susceptible d'amener l'une des conditions ci-dessus.

Remarque

Le niveau intermédiaire de la plupart des applications à trois niveaux n'est pas implémenté comme un programme monolithique, mais d'une façon modulaire. Chaque composant se charge d'une fonction spécifique et relativement petite. Un composant peut en appeler un autre pour satisfaire une requête du client. Ainsi, le modèle à trois niveaux est en fait à N niveaux.

Cependant, il faut noter que la vulnérabilité du système augmente en fonction du nombre de niveaux. Remarquons qu'en architecture, 2-tiers le serveur de données est le maillon faible au sein du système, étant donné que toute l'application est architecturée autour de lui. En architecture 3-tiers l'arrêt du Middleware induit celui de tout le système; cela s'ajoute au fait que le serveur de données est toujours maillon faible comme en architecture 2-tiers.

II.7.3.3/ Principales fonctions du middleware :

- Procédures d'établissement de connexion.
- Récupération des résultats.
- Procédure de fermeture de connexion.
- Conversion de données organisées (tables structurées, objets reliés entre eux du fait de l'hétérogénéité des plates forme).
- Exécution des requêtes.
- Gestion des accès concurrents.
- Accès aux données à distance.
- Initialisation des processus.
- Terminaison des processus.

Le tableau II.1 résume une comparaison entre l'architecture Client/serveur deux et trois niveaux.

II.7.3.4/ Comparaison des architectures deux et trois niveau :

Tableau II.1 : Comparaison entre l'architecture Client/serveur deux et trois niveaux.

	Deux niveaux	Trois niveaux
Administration du système	Complexe	Moins complexe.
Sécurité	Faible ; sécurité au niveau des données.	Importante ; au niveau du service, méthodes ou type objet.
Encapsulation des données	Faible : les tables de la base de données sont accessibles.	Important : le client invoque des services ou méthodes.
Performance	Faible : de nombreuses instructions SQL transitent sur le réseau	Bonne : seules les requêtes et réponses sont échangées.
Changement d'échelle	Difficile : gestion limitée des liens de communication des clients	Facile : charges partagées sur plusieurs serveurs.
Réutilisation	Faible : le client est monolithique	Importante : réutilisation possible des services et des objets.
Infrastructure serveur-serveur	Non.	Oui : via le middleware.
Support de BDs hétérogènes	Non.	Oui : utilisation de plusieurs base de données.
Souplesse de l'architecture matérielle	Limitée.	Excellence : le second niveau peut être reparté sur plusieurs serveurs, le 2 ^e et le 3 ^e sur la même machine.
Support de l'internet	Faible : limitation de la bande passante.	Excellence : utilise des petits clients facilement téléchargés (beans....).
Choix de communication	Non : seule les appels synchrones orientés connexion.	Oui : support d'appels de type RPC, files d'attente,...etc.
Disponibilité	Faible.	Excellence : relance possible du niveau intermédiaire sur d'autres serveurs.
Facilité de développement	Importante.	En voie d'amélioration vu l'utilisation d'outils.

II.7.3.5/ Architecture Client/serveur multi niveaux :

Dans l'architecture à trois niveaux, chaque serveur (niveau 1 et 2) effectue une tâche (un serveur) spécialisée. Ainsi, un serveur peut utiliser le service d'un ou plusieurs autres serveurs afin de fournir son propre service par conséquent, l'architecture à trois niveaux est potentiellement une architecture à N niveaux.

Le schéma suivant illustre ce type d'architecture.

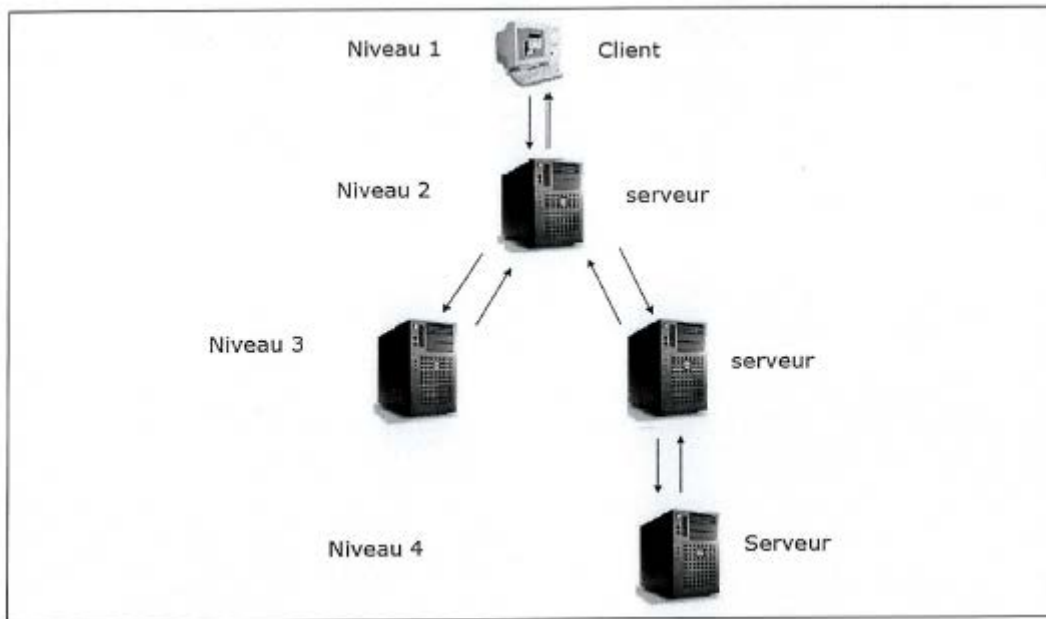


Figure II.8 : Architecture Client/serveur multi niveaux

II.8/ Avantages et inconvénients de l'architecture client serveur :

II.8.1/ Avantages :

Le modèle client/serveur s'impose dès que l'on souhaite composer l'exécution d'une application et faire en sorte que différentes machines (matérielles et logicielles) y participent et ce par opposition aux techniques de calcul centralisés sur mainframe, au tout se fait au niveau du serveur central.

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux avantages sont :

- Des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisées afin d'éviter les problèmes de redondances et de contradiction.

- Une meilleure sécurité : car le nombre de points d'entrée permettant l'accès aux données est moins important.

- Une administration au niveau serveur: les clients ont peu d'importances dans ce modèle, ils ont moins besoins d'être administrés.

- Un réseau évolutif grâce à cette architecture, on peut supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures.

II.8.2/ Inconvénients :

L'architecture client/serveur à tout de même quelques lacunes parmi lesquelles:

- Un cout élève : du à la technicité du serveur.
- Un maillon faible: le serveur est seul maillon faible du réseau, étant donné que tout le réseau est construit autour de lui.

A l'issue de ce chapitre, nous concluons que l'informatique Client/serveur est l'un des divers modèles d'informatique en réseau visant l'utilisation de multiples ordinateurs dans un même système. Le réseau utilisé pour le développement de notre application est configuré en architecture Client/serveur, le serveur est configuré sous le système d'exploitation Windows, les machines se connecte via le protocole de transmission de données TCP/IP, la majorité des traitements s'effectuent au niveau du client et les résultats sont renvoyés au serveur ce qui permet de dire que le réseau est orienté vers le client et le serveur est de type serveur de fichier.

En se basant sur les connaissances théoriques que nous venons présenter, une étude conceptuelle de notre architecture, où nous définirons briefèrent l'approche orientée objets et les différents modules implémentés pour développement de notre application, sera menée dans le chapitre suivant.

Chapitre III: Système d'exploitation Windows

III.1/ Introduction

Pour qu'un ordinateur soit capable de faire fonctionner un programme informatique (appelé parfois application ou logiciel), la machine doit être en mesure d'effectuer un certain nombre d'opérations préparatoires afin d'assurer les échanges entre le processeur, la mémoire, et les ressources physiques (périphériques).

Le système d'exploitation (noté SE ou OS, abréviation du terme anglais Operating System) est chargé d'assurer la liaison entre les ressources matérielles, l'utilisateur et les applications (traitement de texte, jeux vidéo,...etc). Ainsi lorsqu'un programme désire accéder à une ressource matérielle, il ne lui est pas nécessaire d'envoyer des informations spécifiques au périphérique. Il lui suffit d'envoyer les informations au système d'exploitation, qui se charge de les transmettre au périphérique concerné via son pilote. En l'absence de pilotes, il faudrait que chaque programme reconnaisse et prenne en compte la communication avec chaque type de périphérique.

Le système d'exploitation permet ainsi de "dissocier" les programmes et le matériel, afin de simplifier la gestion des ressources et d'offrir à l'utilisateur une interface homme-machine (notée «IHM») qui lui permet de s'affranchir de la complexité de la machine physique.

III.2/ Rôles du système d'exploitation : [8]

Les rôles du système d'exploitation sont divers, citons essentiellement :

III.2.1/ Gestion du processeur:

Le système d'exploitation est chargé de gérer l'allocation du processeur entre les différents programmes grâce à un algorithme d'ordonnancement. Le type d'ordonnanceur est totalement dépendant du système d'exploitation, en fonction de l'objectif visé.

III.2.2/ Gestion de la mémoire vive:

Le système d'exploitation est chargé de gérer l'espace mémoire alloué à chaque application et, le cas échéant, à chaque usager. En cas d'insuffisance de mémoire physique, le système d'exploitation peut créer une zone mémoire sur le disque dur appelée «mémoire virtuelle». Cette dernière permet de faire fonctionner des applications nécessitant plus de mémoire qu'il n'y a de mémoire vive disponible sur le système. En contre partie, cette mémoire est beaucoup plus lente.

III.2.3/ Gestion des entrées/sorties:

Le système d'exploitation permet d'unifier et de contrôler l'accès des programmes aux ressources matérielles par l'intermédiaire des pilotes (appelés également gestionnaires de périphériques ou gestionnaires d'entrée/sortie).

III.3/ Le système de fichiers:

Le système de fichier, en anglais «file system» note FS, permet d'enregistrer les fichiers dans une arborescence.

III.4/ Les types de systèmes d'exploitation:**III.4.1/ Systèmes multitâches:**

Un système d'exploitation est dit «multi-tâche» (en anglais multithread) lorsque plusieurs «tâches» (également appelées processus) peuvent être exécutées simultanément. Les applications sont composées en séquence d'instructions que l'on appelle «processus légers» (en anglais «threads»). Ces threads seront tour à tour actifs, en attente, suspendus ou détruits, suivant la priorité qui leur est associée ou bien exécutés séquentiellement.

Un système est dit préemptif lorsqu'il possède un ordonnanceur (aussi appelé planificateur), qui répartit, selon des critères de priorité, le temps machine entre les différents processus qui en font la demande.

Le système est dit à temps partagé lorsqu'un quota de temps est alloué à chaque processus par l'ordonnanceur. C'est notamment le cas des systèmes multi-utilisateurs qui permettent à plusieurs utilisateurs d'utiliser, simultanément et sur une même machine, des applications différentes ou bien similaires : Le système est alors dit «système transactionnel». Pour ce faire, le système alloue et consacre à chaque utilisateur une tranche de temps.

III.4.2/ Systèmes multi-processeurs

Le multiprocessing est une technique consistant à faire fonctionner plusieurs processeurs en parallèle afin d'obtenir une puissance de calcul plus importante que celle obtenue avec un processeur haut de gamme. Cette synergie de processeurs permet d'augmenter la disponibilité du système (en cas de panne d'un processeur).

On appelle SMP (Symmetric Multiprocessing ou Symmetric Multiprocessor) une architecture dans laquelle tous les processeurs accèdent à un espace mémoire partagé. Un système multiprocesseur doit donc être capable de gérer le partage de la mémoire entre plusieurs processeurs mais également de distribuer la charge de travail.

III.4.3/ Systèmes embarqués

Les systèmes embarqués sont des systèmes d'exploitation prévus pour fonctionner sur des machines de petite taille telles que des PDA (personal digital assistants ou en français assistants numériques personnels) ou des appareils électroniques autonomes (sondes spatiales, robot, ordinateur de bord de véhicule, etc.), possédant une autonomie réduite. Ainsi, une caractéristique essentielle des systèmes embarqués est leur gestion avancée de l'énergie et leur capacité à fonctionner avec des ressources limitées.

Les principaux systèmes embarqués «grand public» pour assistants numériques personnels sont:

- PalmOS
- Windows CE/Windows Mobile/Windows Smartphone.

III.4.4/ Systèmes temps réel:

Les systèmes temps réel (real time systems), essentiellement utilisés dans l'industrie, sont des systèmes dont l'objectif est de fonctionner dans un environnement contraint temporellement. Un système temps réel doit ainsi fonctionner de manière fiable selon des contraintes temporelles spécifiques, c'est-à-dire qu'il doit être capable de délivrer un traitement correct des informations revues à des intervalles de temps bien définis (réguliers ou non). Voici quelques exemples de systèmes d'exploitation temps réel :

- OS-9.
- RTLinux (RealTime Linux).
- QNX.
- VxWorks.

On distingue plusieurs types de systèmes d'exploitation, selon qu'ils sont capables de gérer simultanément des informations d'une longueur de 16 bits, 32 bits, 64 bits ou plus. Le tableau III.1 résume des caractéristiques de quelques types de systèmes d'exploitation.

Tableau III.1: Caractéristiques et types de systèmes d'exploitation.

Système	Codage	Mono-utilisateur	Multi-utilisateur	Mono-tâche	Multitâche
DOS	16 bits	X		X	
Windows3.1	16/32 bits	X			non préemptif
Windows95/98/Me	32 bits	X			coopératif
WindowsNT/2000	32 bits		X		préemptif
Windows XP	32/64 bits		X		préemptif
Unix / Linux	32/64 bits		X		préemptif
MAC/OS X	32 bits		X		préemptif
VMS	32 bits		X		préemptif

III.5/ Microsoft Windows : [9]

Windows est une Gamme de systèmes d'exploitation développés par Microsoft et destinés aux ordinateurs compatibles PC.

La caractéristique principale de Windows est une gestion cohérente, normalisée, à l'aide de symboles, menus et champs de dialogue graphiques que l'on active généralement par un clic de la souris. Il n'est donc plus nécessaire de saisir les commandes manuellement, comme c'était le cas avec MS-DOS.

Le nom "Windows" provient du fait que l'on utilise des fenêtres pour représenter la surface de travail sur laquelle on exploite les programmes d'application et les documents. Les tâches générales, telles que l'impression et la gestion des éléments du système (disque dur, carte graphique, etc.), sont gérées centralement par Windows et mises à la disposition de tous les programmes d'application.

Windows est devenu le système d'exploitation le plus utilisé dans le monde.

La figure III.1 illustre l'évolution du système d'exploitation avant Windows7 .

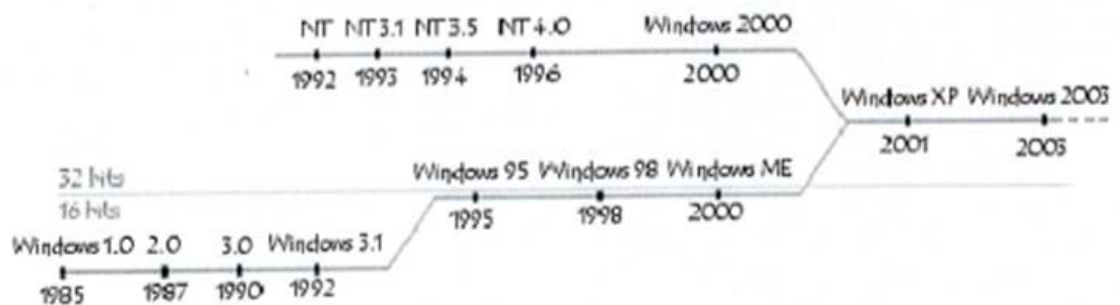


Figure III.1: Évolution du système d'exploitation Windows.

III.5.1/ La gamme Windows est composée de 4 grandes branches:

- ✓ La première (1985 - 1993), de Windows 1.0 à Windows 3.11

Interface utilisateur graphique (OUI) développée pour les ordinateurs compatibles PC basés sur le système d'exploitation MS-DOS.

- ✓ La seconde (1993 - 2003), de Windows NT 3.1 à Windows 2000 SP4

Principalement à destination des serveurs et des stations de travail professionnelles. Cette gamme n'était pas basée sur MS-DOS ce qui la rendait, à l'origine, incompatible avec de nombreux jeux.

- ✓ La troisième, (1995), à partir de Windows 95

Gamme de systèmes d'exploitation qui résultent de l'évolution 32 bits de la première gamme et reprenant certains avantages de la seconde. Windows 95 apportait comme principales évolutions le multitâche, la mémoire virtuelle et une nouvelle interface graphique.

- ✓ La quatrième (1996 et plus), à partir de Windows CE 1

Destinée aux appareils mobiles (PDA, téléphone mobile, GPS..). Cette gamme est adaptée aux contraintes de ces machines (affichage, mémoire) et offre une interface graphique similaire aux systèmes d'exploitation PC bien que son noyau soit différent.

III.6/ Définition de la base de registre : [10]

La base de registre est une base de données utilisée par le système d'exploitation Windows. Elle contient les données de configuration du système d'exploitation et des autres logiciels installés désirant s'en servir. Microsoft utilise aujourd'hui plutôt le terme Registre Windows pour parler de cette base de données.

Le plus souvent, les utilisateurs modifient la base de registre de façon transparente, via une interface graphique. Il existe des cas où aucune interface graphique n'est prévue; il est alors nécessaire d'utiliser l'outil Regedit, mais dans ce cas, il n'y a pas de garde-fou, le logiciel ne vérifie aucun des paramètres modifiés par l'utilisateur...

III.6.1/ Avantages et inconvénients de la base de registre:

Le but de cette base de registre est de regrouper toutes les informations de configuration, pour d'une part, créer un semblant d'organisation et d'autre part limiter le nombre de fichiers de configuration sur le disque dur.

La base de registre est un fichier contenant une arborescence dans laquelle les paramètres sont classés par critère. A chaque critère correspond une branche qui peut encore être subdivisée en autres branches (une arborescence...). Chaque élément de configuration est situé tout au bout d'une branche dans ce que l'on nomme "une clé".

Le problème majeur de cette base de registre est que, suite à l'installation d'un programme, il se crée plusieurs clés dans divers endroits de la base de registre, or, à la désinstallation, les clés sont effacées (dans le meilleur des cas) mais l'arborescence reste. Lorsque vous installez des programmes à la pelle et que vous les effacez...le système ralentit...il faut donc, au bout d'un certain temps réinstaller Windows.

III.6.2/ Editer la base de registres

Il est possible de modifier ce gigantesque capharnaüm, mais cela ne se fait pas sans précautions (la base de registre est le cœur de Windows-pas de base de registre, pas de Windows) :

- Avant toute chose, il faut faire une copie de la base de registre, qui vous permettra de revenir à vos paramètres initiaux en cas d'erreur!!
- Il faut ensuite désactiver les attributs des fichiers system.dat et user.dat
- enfin, il faut lancer le programme "c:\windows\regedit.exe"

Il ne vous reste plus qu'à modifier les clés que vous voulez éditer.

III.6.3/ Répertoire de la base de registre : [11]

Un système comme Windows est entouré d'un nombre de logiciels et de matériel.

La gestion qui en résulte est assez importante : pilotage des périphériques (processeur, BIOS, cartes PCI...), gestion des logiciels, gestion des différents profils...Les informations nécessaires sont alors stockées dans une structure particulière, le registre.

- ✓ Sous Windows server2008, Windows XP, Windows Server2000 et NT

Par défaut, c'est dans le répertoire %SystemRoot% \System32 \Congig que sont stockés les fichiers de ruche suivant :

- SAM (Security Account Manager)
- Security
- Software
- System

Les informations concernant un utilisateur sont stockées dans le répertoire correspondant à la variable d'environnement **%Userprofile%**. Par exemple, pour un utilisateur dont le login est «dupont», la valeur %Userprofile% sera par défaut "C:\Documments and settings\dupont". Il y a un fichier de ruche **NTUSER.DAT** par utilisateur.

Le répertoire %SystemRoot% \repair contient une sauvegarde de la base de registre. Elle est utilisée par Windows pour certains cas de figure. De plus, sous Windows XP, la restauration du système les stocke dans le répertoire \System Volume Information du disque système.

Des fichiers journaux (extension.LOG) et des fichiers de sauvegarde (extension.SAV) sont utilisés en interne par Windows pour pallier aux coupures de courant intempestives, ou à toute autre forme d'arrêt brutal.

III.6.4/ Structure et contenu de la base de registre

La base de registre est partagée en différentes sections logiques. Elles sont généralement connues par les noms les définissant quand on y accède via l'interface graphique de Windows. Les noms commencent tous par 'HKEY' (une abréviation de Handle to a KEY, gestionnaire de clé). Les deux HKEY de base sont :

- **HKEY_LOCAL_MACHINE (hklm)** contient les informations qui sont générales à tous les utilisateurs de l'ordinateur :
- ✓ **HARDWARE** : Description, informations sur le processeur de l'ordinateur, le coprocesseur mathématique et les adaptateurs SCSI ou multifonctions, informations plug and play et sur les ressources système (taille mémoire). Toutes ces données sont initialisées à chaque démarrage du PC, une modification manuelle n'a donc aucun intérêt.
- ✓ **SOFTWARE**: Cette branche contient les informations sur les applications et les composants systèmes de Windows.

Software\Classes : Cette clé du registre contient une copie intégrale de la branche HKEY_CLASSES_ROOT. Elle gère les classes et les objets (voir plus haut).

Software\Microsoft : Les composants et les applications Microsoft se gèrent sous cette clé.

Software\Microsoft\Shared Tools : Modules complémentaires, composants utilisés simultanément par plusieurs programmes.

Software\Microsoft\Windows : Cette clé regroupe les paramètres d'exécution de Windows (composants, programmes, etc).

Software\Microsoft\Windows\CurrentVersion\App Paths : cette clé gère les chemins d'accès à Windows ainsi qu'à des applications.

Software\Microsoft\Windows\CurrentVersion\Uninstall : regroupe les informations nécessaires pour désinstaller Windows et les applications (nom des programmes, chemin d'accès du logiciel de désinstallation).

✓ **SAM** : Dans cette branche sont gérés les paramètres de sécurité pour les comptes des utilisateurs et des groupes, ainsi que des domaines de serveur (SAM, Security Account Management). Ces paramètres n'ont pas besoin d'être fixés par le registre. Il est beaucoup plus facile de les régler par l'explorateur.

✓ **SECURITY**: Vous trouvez à cet endroit les paramètres de la sécurité locale.

✓ **SYSTEM** : Les paramètres de cette branche sont nécessaires au démarrage de Windows, mais ils ne sont pas initialisés à chaque démarrage. Ils contiennent les options de configuration du système d'exploitation ainsi que des applications et composants installés. Une partie de cette branche est mirée dans la branche HKEY _ CLASSES _ ROOT.

System\CurrentControlSet : Dans cette branche figure tous les paramètres vitaux du système et les services installés.

System\CurrentControlSet\Control\ComputerName: Ici figure le nom de l'ordinateur dans le réseau.

System\CurrentControlSet\Control\InstalledFiles : Cette clé contient la liste des fichiers actuellement installés de Windows 98. Examiner le contenu est très instructif, mais évitez de le modifier.

- **HKEY_USERS**: La branche HKEY_USERS décrit un environnement de système d'exploitation par défaut et contient une clé pour chaque utilisateur ayant ouvert une session locale ou via une connexion réseau. Il contient tous les profils utilisateurs chargés activement, y compris HKEY_CURRENT_USER, déjà désigné comme enfant de HKEY_USERS et profil par défaut.

Les trois autres HKEY sont :

- **HKEY_CURRENT_CONFIG**: La branche HKEY_CURRENT_CONFIG contient des informations sur le profil matériel utilisé par l'ordinateur local au démarrage. Ces informations sont utilisées pour configurer des paramètres tels que les pilotes de périphérique à charger et la résolution d'écran à adopter. N'y modifiez rien sous peine de tout réinstaller ou de dysfonctionnement grave.

C'est une copie de HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ HardwareProfiles\ Current.

- **HKEY_CLASSES_ROOT(HKCR)** : contient des informations sur les applications enregistrées. Cela inclut, entre autres, les associations entre extensions de fichiers et identifiants de classe d'objet OLE. Ce qui permet de lancer automatiquement l'exécutable correspondant. Cela correspond à HKEY_LOCAL_MACHINE\SOFTWARE\Classe. Exemple: ".bat" et "XML" sont respectivement associés à "batfile" et "XML script engin".

- **HKEY CURRENT USER:** contient les informations concernant l'utilisateur connecté, Ce n'est qu'une sous-branche de HKEY_USER.

En définitive, dans ce chapitre, nous avons décrit en premier lieu la notion des systèmes d'exploitation ainsi que leurs caractéristiques. Nous avons, par la suite, présenté la base de registre.

Cette partie du mémoire nous a permis de nous familiariser avec le système d'exploitation Windows et d'acquérir un tas de connaissances des produits. Elle nous a également permis d'évaluer la puissance de ce système. En effet, ce chapitre est une initiation, dans le détail, aux différents langages et technologies de programmation à utiliser pour lancer le développement et l'implémentation des composants de l'application (interfaces et application Client/serveur).

Chapitre IV: Conception

Dans le but d'une meilleure organisation et une bonne maîtrise du travail, tout processus de développement d'applications ou systèmes informatiques doit suivre une méthode ou démarche bien définie.

Dans ce chapitre, nous allons entamer un processus qui mettra en évidence les différents acteurs intervenant dans le système cible ainsi que leurs besoins. Pour ce faire, notre démarche va s'appuyer sur une architecture logicielle permettant d'ordonner la transmission des informations et le stockage des données.

IV.1/ Analyse:

Cette partie à pour objectif la spécification de manière claire de la conception des projets informatiques. Pour ce faire, il est nécessaire de déterminer globalement ce qui se trouve dans les champs du projet. De ce fait, on s'intéressera dans cette phase à la définition des besoins ainsi qu'au domaine couvert par notre projet.

IV.1.1/Définition du besoin:

Les besoins principaux du système à réaliser sont les suivants :

- Offrir des moyens de communication entre les machines des réseaux locaux.
- Offrir des mécanismes d'envoi et de réception des messages ainsi que des fichiers.
- Appliquer des restrictions sévères sur les utilisateurs pour protéger le système.
- Offrir une sauvegarde pour les données des utilisateurs (symantec backup exec 2010).
- Offrir une sécurité internet avec les TMG.
- Offrir une réplication des données.
- Offrir des mécanismes de consultation et de listage et même de modification si nécessaire selon les besoins des utilisateurs.
- Offrir des interfaces conviviales pour faciliter la tâche au serveur.
- être extensible de telle sorte que de nouvelles fonctionnalités peuvent lui être ajoutées.

IV.2.2/ Fonctionnalités:

Le système qu'on se propose de réaliser va intégrer une solution qui optimisera le processus de gestion des utilisateurs, tout on s'inspirant des besoins des futurs utilisateurs et en tirant l'épingle du jeu des différentes procédures de gestion de configuration des PC d'un réseau.

Sur ce, on se fixe comme but le processus de gestion des utilisateurs (client/serveur) au niveau d'une entreprise, par la mise en place d'un espace d'échange interactif qui va faciliter et donner aux différents agents des moyens efficaces et conviviaux pour la gestion.

IV.2.3/ Identification des acteurs

Durant le stage que nous avons effectué au sein de la direction informatique de la **Grande distribution**, nous avons procédé en premier lieu, à la localisation des centres d'activité potentielle de la gestion de la configuration des PC d'un réseau LAN.

- L'administrateur.
- Utilisateur.

IV.2.4/ Diagramme de contexte:

Le diagramme de contexte est un modèle conceptuel de flux qui permet d'avoir une vision globale des interactions entre le système et les liens avec l'environnement extérieur. Il permet aussi de bien délimiter le champ de l'étude.

Pour notre cas le contexte est donné par la figure suivante :



Figure IV.1: Diagramme de contexte.

IV.2.5/ Identification des espaces :

A chaque acteur est attribué un espace qui regroupe toutes les tâches qu'il peut effectuer. Pour notre cas nous avons identifié deux espaces :

- Espace administrateur.
- Espace utilisateur.

Remarque : Les activités de chaque agent seront définies de manière détaillée dans les diagrammes de cas d'utilisation.

IV.3/ Conception:

IV.3.1/ La démarche de conception du système:

Le processus de conception de notre projet se caractérise par deux niveaux : Le niveau applicatif et le niveau donné.

✓ **Le niveau applicatif :**

Il s'appuie essentiellement sur quelques diagrammes du langage de modélisation UML. Donc, après avoir identifié les principaux acteurs ainsi que leurs besoins, à travers des entretiens, choses qui nous ont permis d'identifier les différentes fonctions du système à concevoir, nous avons opté pour la démarche suivante :

- Mettre en évidence les cas d'utilisation mis en œuvre par les utilisateurs futurs du système. Les diagrammes des cas d'utilisation sont élaborés, ainsi que le détail de chaque cas d'utilisation.
- A l'aide du diagramme de séquence, on formalise graphiquement le ou les scénarios qui décrivent chaque cas d'utilisation.
- Les classes sont définies par synthèse des diagrammes de séquence. Une fois les classes manipulées, on passe à l'élaboration du diagramme de classes.

✓ **Le niveau donné**

Ce niveau concerne l'organisation conceptuelle, logique et physique des données manipulées. Durant la partie analyse nous avons pu identifier les données nécessaires et indispensables au bon fonctionnement de l'application et à travers la conception du niveau applicatif nous allons dégager les classes significatives. Dès lors on pourra élaborer la conception de base de données.

Pour la conception de notre projet nous allons adopter une démarche qui s'appuie sur quatre étapes :

Etape 1 : identification des acteurs et des besoins.

Etape 2 : identification et représentation des cas d'utilisation.

Etape 3 : élaboration des diagrammes de séquence.

Etape 4 : élaboration du diagramme d'activités.

Etape 5 : élaboration du diagramme classes.

La figure suivante illustre la représentation graphique de la démarche de modélisation choisie pour concevoir notre application

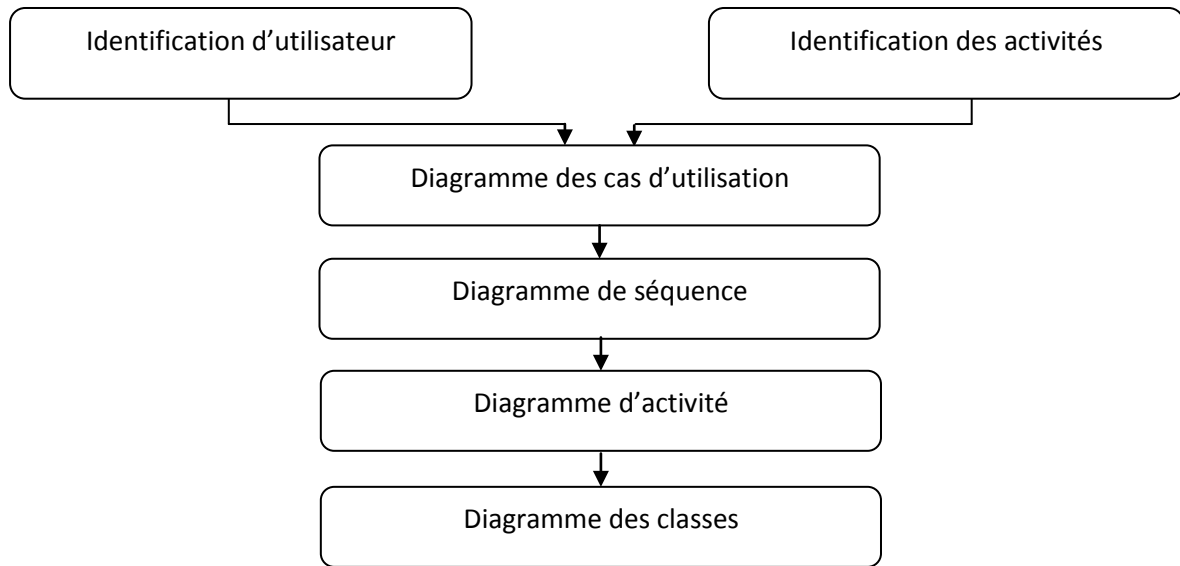


Figure IV.2: Cycle de modélisation de l'application.

IV.3.2/ Rôles et responsabilités:

- ✓ **Administrateur** : il est chargé de :
 - Consulter, installer, désinstaller, modifier des applications sur les postes.
 - Contrôler les accès des utilisateurs.
 - Affecter les profils aux utilisateurs.
 - Gérer les utilisateurs.
 - Ajouter des utilisateurs dans l'AD et EXCHANGE.
- ✓ **Utilisateur**: il est chargé de :
 - Utiliser les applications.
 - Signaler les problèmes.
 - Demande des besoins.
 - L'envoi des messages.
 - Stocker les données.

IV.3.3/ Les fonctions globales du système :

- Consulter la liste des utilisateurs.
- Assurer un environnement sûr aux utilisateurs.
- Consulter la configuration hardware des utilisateurs.
- Consulter la liste des applications des utilisateurs.

- Installer une application.
- Désinstaller une application.
- Création des sessions outlook des utilisateurs (AD).
- Création des sessions mail des utilisateurs (EXCHANGE).
- Stocker les données des utilisateurs dans le serveur file.
- ✓ **Fonction de l'administrateur**
- Lancer le serveur.
- L'ajout des utilisateurs dans l'AD et EXCHANGE.
- Assurer le bon fonctionnement des serveurs et applications.
- Consulter la configuration (hardware et software) des utilisateurs.
- Consulter la liste des applications des utilisateurs.
- Installer des applications.
- Désinstaller des applications.
- Modifier des applications.
- Consulter la liste des fichiers utilisateur.
- ✓ **Fonction de l'utilisateur**
- Se connecter au serveur.
- Signaler les problèmes.
- Envoyer de messages.
- Demander des fonctionnalités supplémentaires (tout dépend des profils).

IV.3.4/ Cas d'utilisation et diagrammes de cas d'utilisation:

Pour décrire les cas d'utilisations et acteurs de ce système, nous allons recenser les acteurs intervenants dans le système et décrire les rôles et responsabilités de chacun.

IV.3.4.1/ Administrateur:

La figure suivante représente le diagramme de cas d'utilisation administrateur.

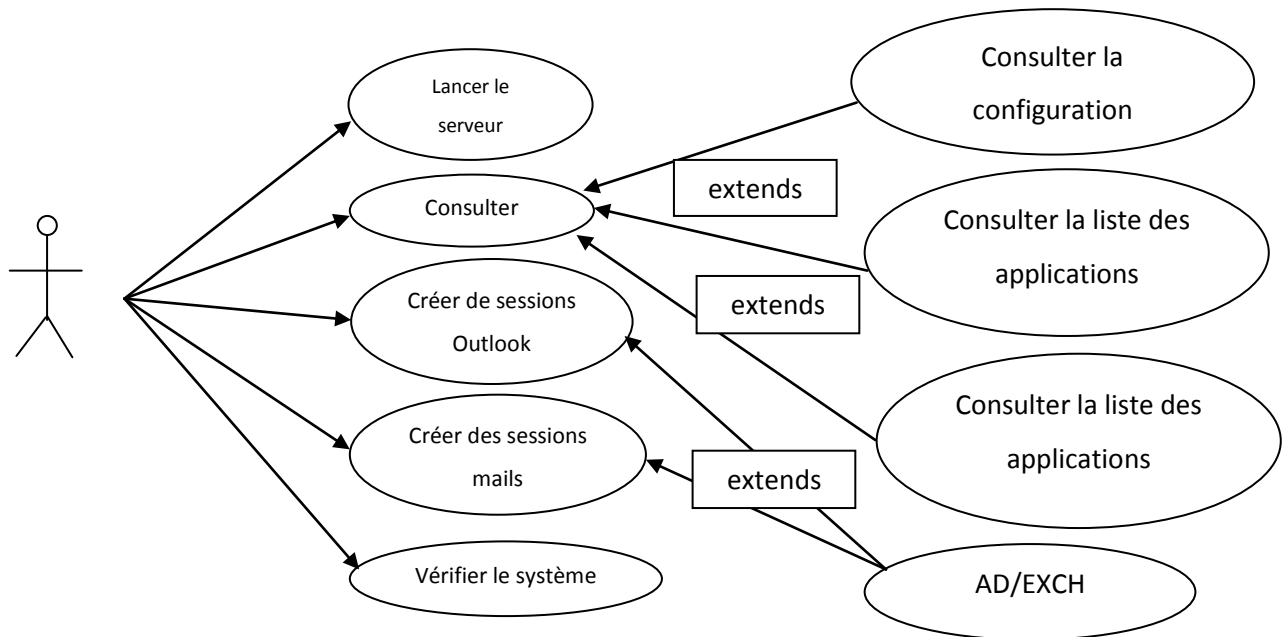


Figure IV.3: Diagramme cas d'utilisation administrateur.

IV.3.4.2/ Utilisateur:

La figure IV.4 représente le diagramme de cas d'utilisation d'utilisateurs.

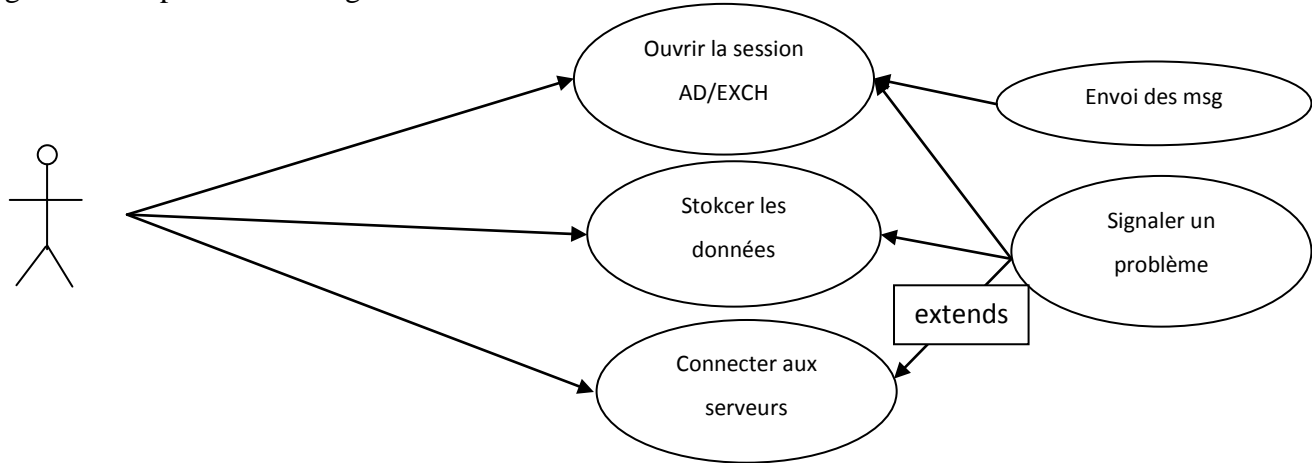


Figure IV.4: Diagramme de cas d'utilisation de l'utilisateur

IV.3.5/ Récapitulatif des diagrammes des cas d'utilisation :

L'utilisateur s'identifie pour ouvrir la session de Outlook ou il y'a tous les lecteurs ou il pourra stocker ses données en toute sécurité.

L'utilisateur s'identifie et ouvre le session mail pour envoyer des messages aux autres utilisateurs

Les sessions sont créées au départ par l'administrateur. C'est un espace propre à l'utilisateur qui lui permettra de trouver son environnement.

IV.3.6/ Spécification des scénarios:

IV.3.6.1/ Définition:

Un scénario représente une succession particulière d'enchaînements, s'exécutant du début à la fin du cas d'utilisation, un enchaînement étant l'unité de description de séquences d'actions. Un cas d'utilisation contient en général un scénario nominal et plusieurs scénarios alternatifs (qui se terminent de façon normale) ou d'erreur (qui se terminent en échec).

IV.3.7/ Description de cas d'utilisation:

Les figures IV.6 – IV.14 mettent en évidence la description des différentes séquences d'actions des cas d'utilisation.

1. Identification de cas d'utilisation

Cas d'utilisation : lancer le serveur.

Objectif : permettre à l'administrateur de lancer le serveur pour permettre aux utilisateurs de se connecter.

Acteur : administrateur.

2. Description fonctionnelle

Pré condition: se connecter en tant que administrateur.

Description du cas d'utilisation

L'administrateur lance serveur,

Le système en attente de connexion des clients.

Figure IV.6: Cas d'utilisation «lancer le serveur».

1. Identification du cas d'utilisation

Cas utilisation : ouvrir une session Outlook.

Objectif : avoir un espace propre à utilisateur.

Acteur : administrateur.

2. Description fonctionnelle

Pré condition : se connecter en tant que administrateur et créer une session Outlook (AD).

Description du cas d'utilisation

Le système n'affiche pas d'erreur.

L'utilisateur est ajouté dans le serveur (AD).

Figure IV.7: Cas d'utilisation «Ouvrir une session (AD) à utilisateurs».

1. Identification du cas d'utilisation

Cas d'utilisation : ouvrir une session mail.

Objectif : avoir un espace mail propre à utilisateur.

Acteurs : administrateur.

2. Description fonctionnelle

Pré condition : se connecter en tant que administrateur et créer une session mail (EXCH).

Description du cas d'utilisation

Le système n'affiche pas d'erreur.

L'utilisateur est ajouté dans le serveur (EXCH).

Figure IV.8: Cas d'utilisation «Ouvrir une session mail (EXCH) à utilisateurs».

1. Identification du cas d'utilisation

Cas d'utilisation : l'envoi et réception des messages.

Objectif : une communication entre utilisateurs.

Acteur : utilisateurs.

2. Description fonctionnelle

Pré condition: l'existence de l'utilisateur dans les serveurs (AD et EXCH).

Description du cas d'utilisation

L'utilisateur se connecte au serveur.

L'ouverture des sessions.

L'envoi des messages.

Réception des messages.

Figure IV.9: Cas d'utilisation «l'envoi des messages entre utilisateurs».

1. Identification du cas d'utilisation

Cas d'utilisation : Vérifier le système des fichiers.

Objectif : vérification de système des fichiers.

Acteur: administrateur.

2. Description fonctionnelle

Pré condition: avoir le scripte des fichiers.

Description du cas d'utilisation

Le système affiche la liste des fichiers.

Figure IV.10: Cas d'utilisation «Vérifier le système».

Figure IV.11: Cas d'utilisation «se connecter aux serveurs».

1. Identification du cas d'utilisation
Cas d'utilisation : se connecter au serveur.
Objectif : connexion au serveur.
Acteur : utilisateur.

2. Description fonctionnelle
Pré condition: serveur en attente de connexion.
Description du cas d'utilisation
 Connexion au serveur «connexion effectuée».

Par ailleurs, la figure IV.12 représente un diagramme de séquences «connecter au serveur AD».

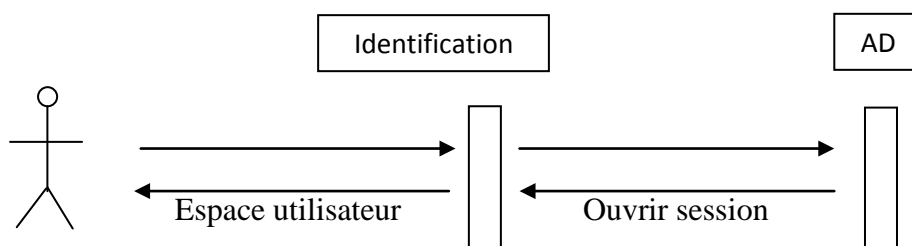


Figure IV.12: Diagramme de séquence « connecter au serveur AD».

Cette étape est réalisée dans l'ordre chronologique suivant:

1. L'utilisateur s'identifie.
2. AD vérifie l'identification d'utilisateur pour ouvrir la session.
3. Entrer dans l'espace d'utilisateur.
4. Avoir la possibilité de stockage dans le serveur file en toute sécurité.

La figure IV.13 représente un diagramme de séquences «connecter au serveur EXCH».

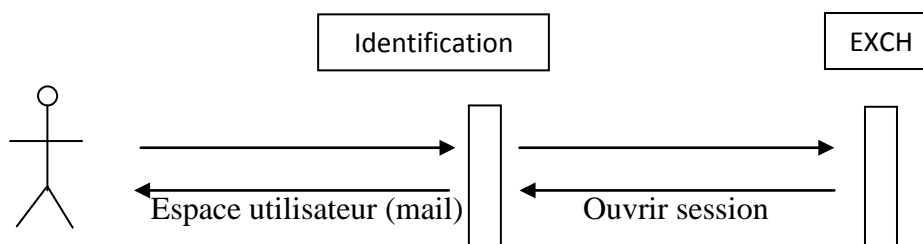


Figure IV.13: Diagramme de séquence « connecter au serveur EXCH».

Cette étape est réalisée dans l'ordre chronologique suivant:

1. L'utilisateur s'identifie sur Outlook.
2. Exchange vérifie l'identification d'utilisateur pour ouvrir la session de messagerie.
3. Avoir l'accès dans l'espace d'utilisateur messagerie.
4. Avoir la possibilité d'envoyer et de recevoir des messages.

La figure IV.14 représente un diagramme de séquences globales.

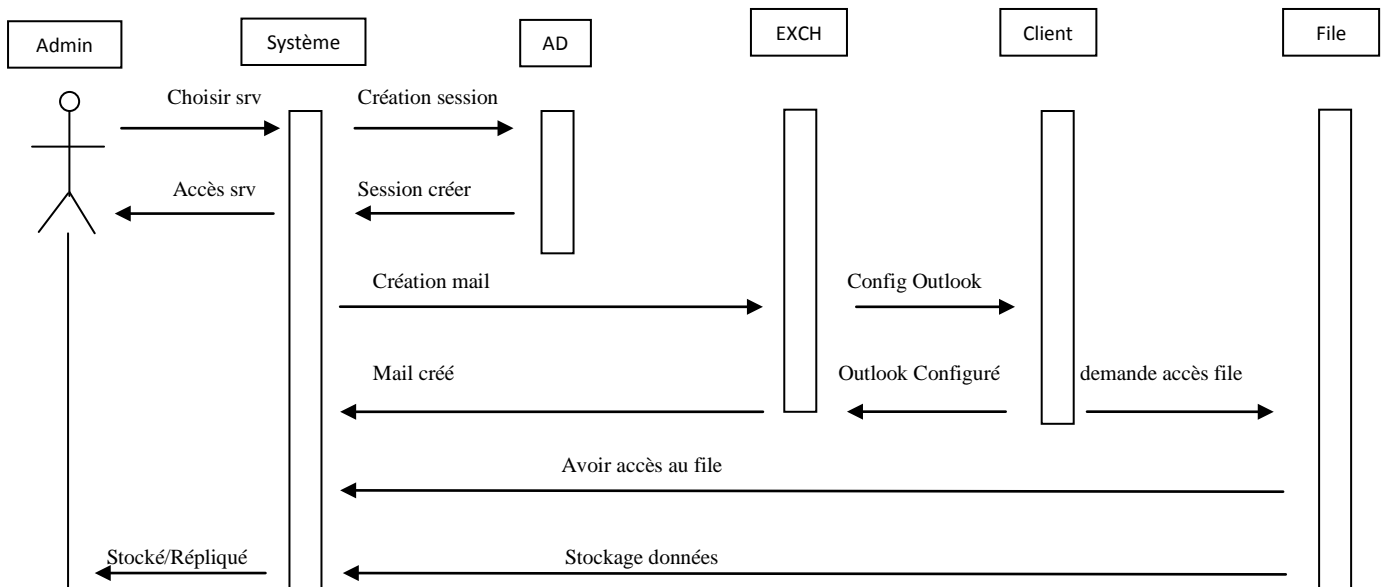


Figure IV.13: Diagramme de séquence globale.

1. L'administrateur se connecte au serveur.
2. L'administrateur choisit le serveur AD pour l'ouverture de session Outlook.
3. Création de session Outlook pour l'utilisateur.
4. L'administrateur choisit le serveur Exchange pour l'ouverture de session mail.
5. L'administrateur configure la session mail à l'utilisateur.
6. L'utilisateur a l'accès à la ressource partagée (file).
7. L'utilisateur peut stocker ses données en toute sécurité
8. Réplication des données et sauvegarde

1. Diagrammes d'activités

Le diagramme d'activités fait partie des cinq diagrammes d'UML utilisés pour la modélisation des aspects dynamiques des systèmes. Un diagramme d'activités est principalement un organigramme qui montre le flot de contrôle d'une activité à l'autre.

C'est-à-dire la modélisation des étapes séquentielles (voire concurrentes) dans un processus de calcul.

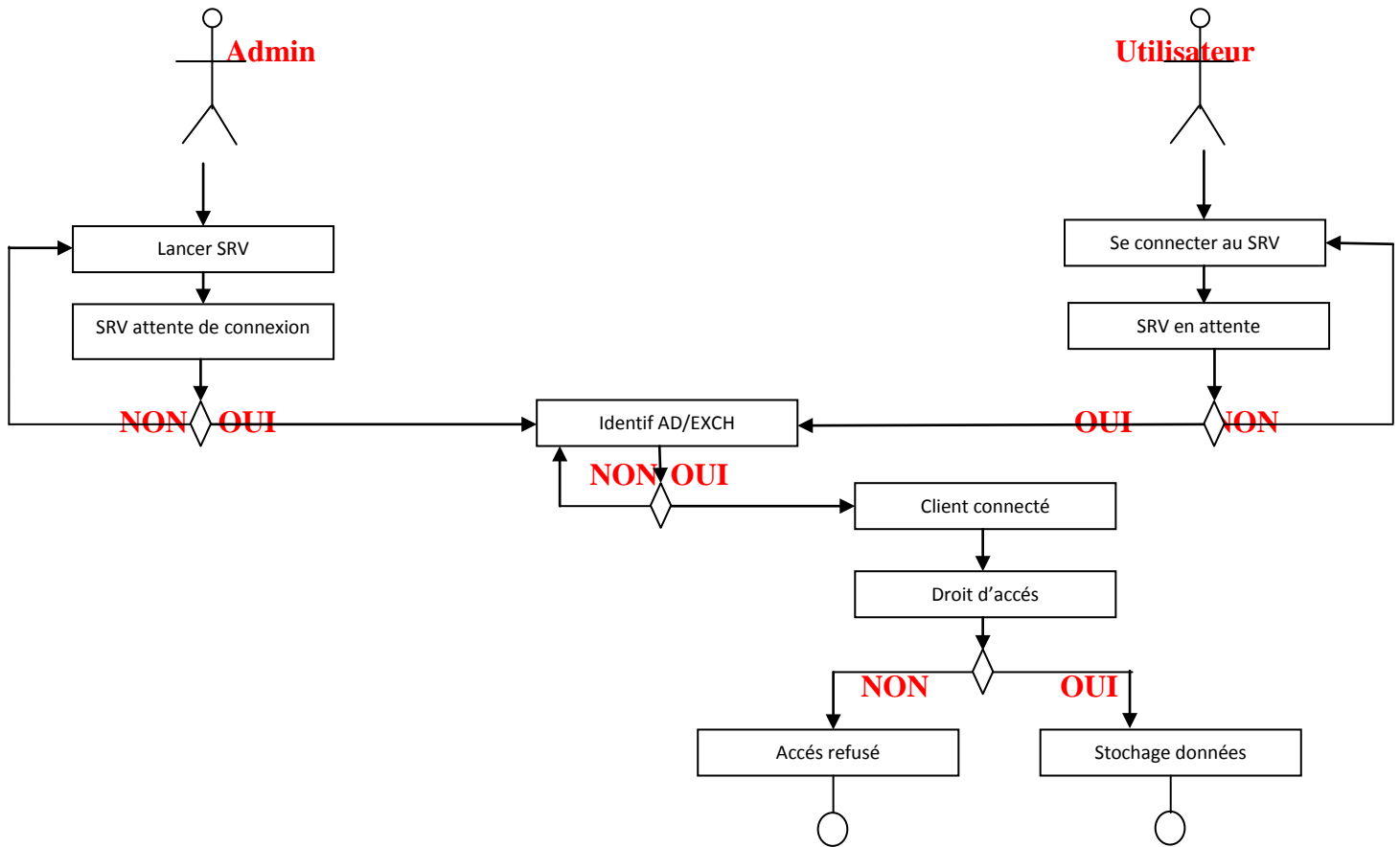


Figure IV.13: Diagramme de d'activité globale.

2. Diagramme de classes

Les diagrammes de classes sont les plus courants dans la modélisation des systèmes orientés objet. Ils représentent un ensemble de classes, d'interfaces et de collaborations ainsi que leurs relations. Ces diagrammes sont utilisés pour modéliser la vue de conception statique.

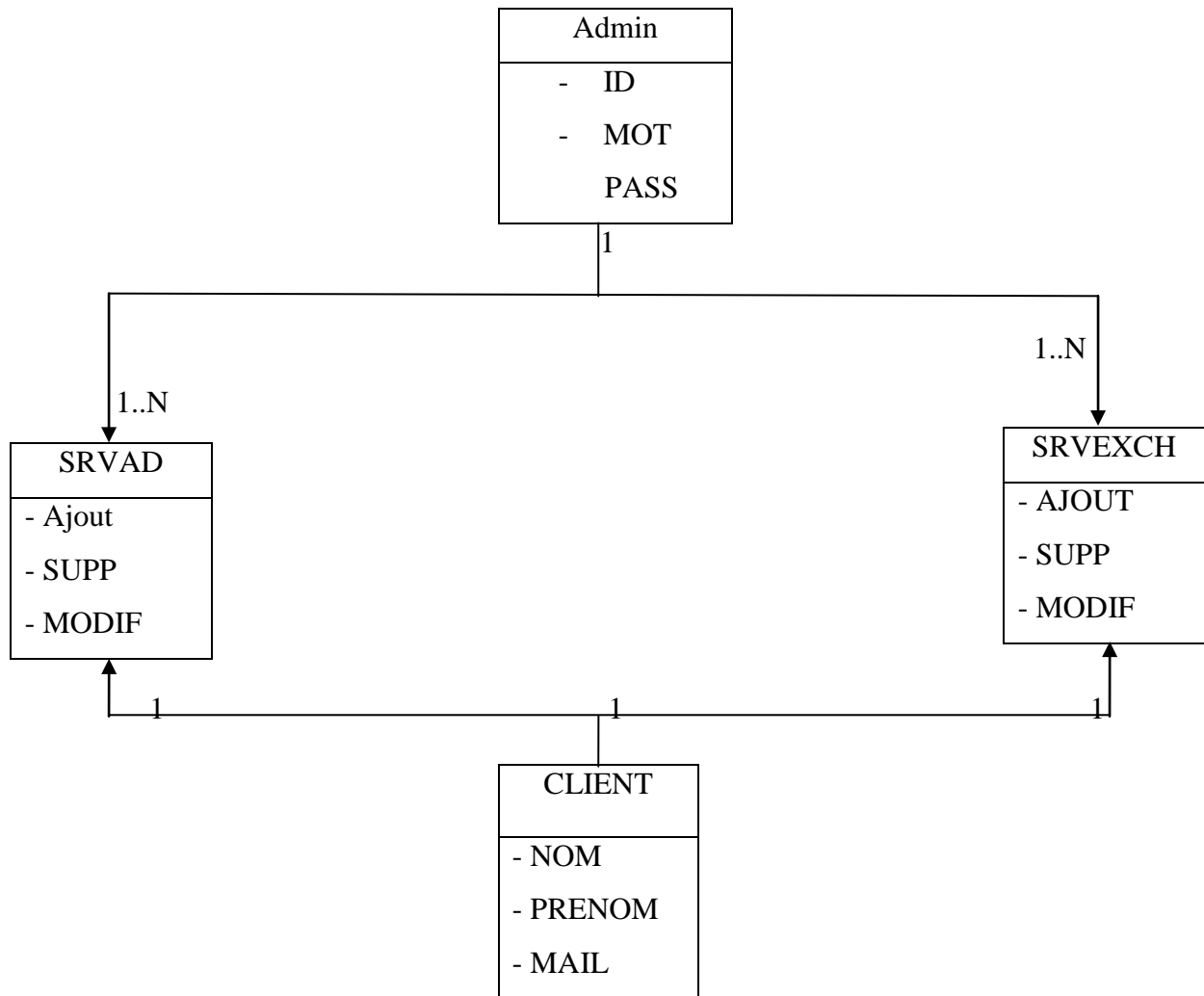


Figure IV.14: Diagramme de classe globale.

Le présent chapitre a été consacré pour la conception de notre thème et d'éclaircir les principales définitions des besoins ainsi qu'au domaine couvert par notre projet.

Chapitre V: Réalisation

Dans l'aire ou nous vivons, les périphériques mobiles sont devenus partie intégrante dans la vie quotidienne aussi bien professionnelle que personnelle engendrant différents risques de sécurité.

Dans ce contexte et afin de protéger et garantir les données des entreprises tout en facilitant le travail aux employés (utilisateurs), la mise en œuvre d'un environnement sécurisé, utilisant différents moyens et outils, s'avère indispensable.

Dans une première étape de ce travail, nous présenterons les différentes méthodes et matériels utilisés pour la réalisation de l'architecture système de notre entreprise.

V.1/ Objectif de l'application :

L'objectif de ce projet est de concevoir une application simple et efficace afin d'assurer aux utilisateurs un environnement de travail sécurisé et fiable, offrant toutes les commodités telles que: système de messagerie, stockage de leurs données, accès à des ressources ...etc, en imposant une certaine politique associée aux outils utilisés tel que :

- ✓ FILE : Les données des utilisateurs de la société.
- ✓ TMG : Offrir une connexion en toute sécurité.
- ✓ Exchange : La messagerie.
- ✓ Active Directory : Création de session des utilisateurs.
- ✓ GPO : Politique des restrictions pour les utilisateurs.
- ✓ DHCP : Fournir la configuration IP.
- ✓ DNS : Consiste à trouver l'adresse IP d'un ordinateur à partir de son nom.

V.2/ Les outils :

- ✓ Serveur 2008 2R.
- ✓ Serveur 2012 2R.
- ✓ TMG.
- ✓ Symantec backup exec 2010.
- ✓ Un routeur.
- ✓ Exchange 2010 messagerie.
- ✓ Visual basic.
- ✓ Windows 7.

V.2.1/ Environnement matériel :

- ✓ Une baie de stockage.
- ✓ Micro-ordinateur.
- ✓ Routeur.
- ✓ Switch.
- ✓ Serveur (machine puissante).

V.2.2/ Environnement de développement:

Pour réaliser ce projet, notre choix s'est posé sur un environnement de Windows qui assure la gestion des ordinateurs et de leurs périphériques. Les systèmes d'exploitation interactifs offrent à l'utilisateur un environnement de travail intuitif et performant et la possibilité d'assurer la sécurité des données.

V.2.2.1/ Système d'exploitation :

Windows est le système d'exploitation moderne pour les ordinateurs personnels. Il permet de faciliter l'utilisation des ordinateurs grâce, en particulier: à une présentation graphique des applications sous la forme d'icônes et de fenêtres, à un système de menus, à une gestion simplifiée des fichiers, à la possibilité d'exécuter simultanément plusieurs applications, etc. **WINDOWS** est l'un des plus répandus.

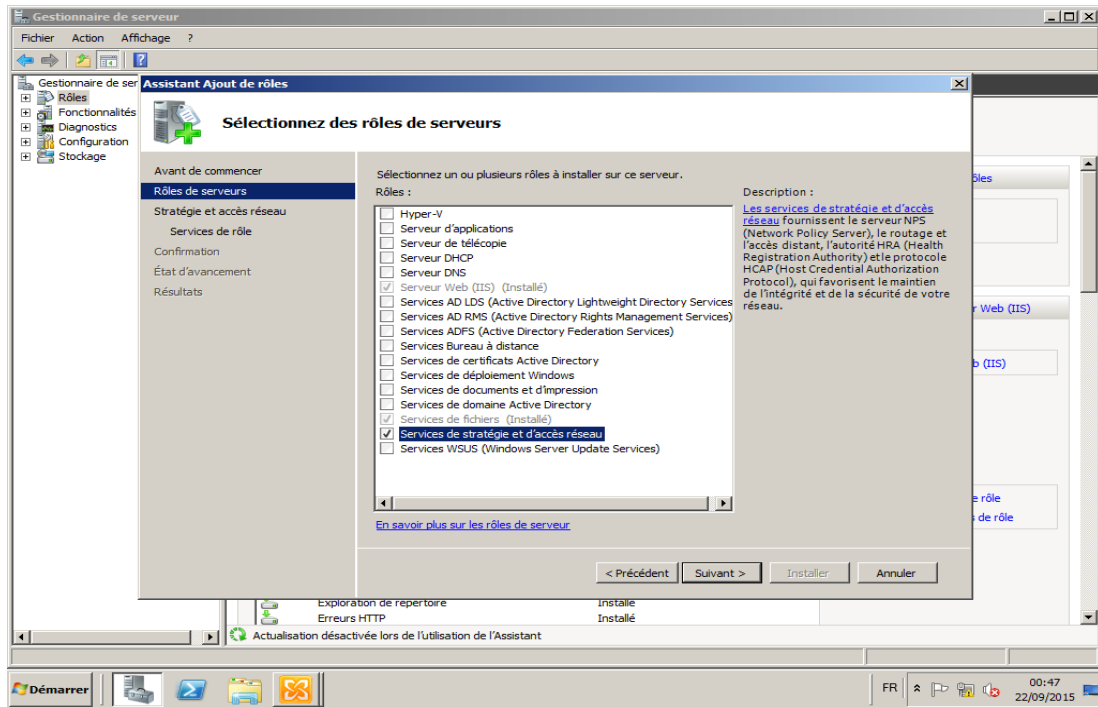
V.3/ Routeur :

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles.

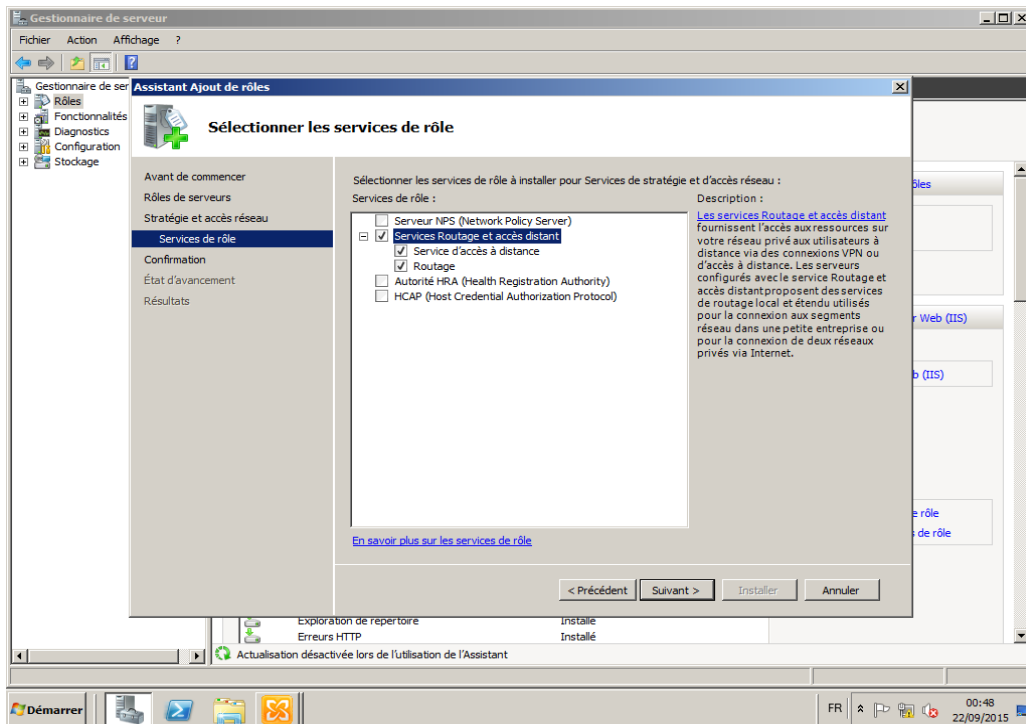
Comme on a utilisé des réseaux différents dans notre cas (ALGER / 10.10.10.0 et Oran : 20.20.20.0), on été dans l'obligation d'utiliser un routeur pour que toutes les machines communique entre elles.

V.3.1/ Installation et configuration de routeur :

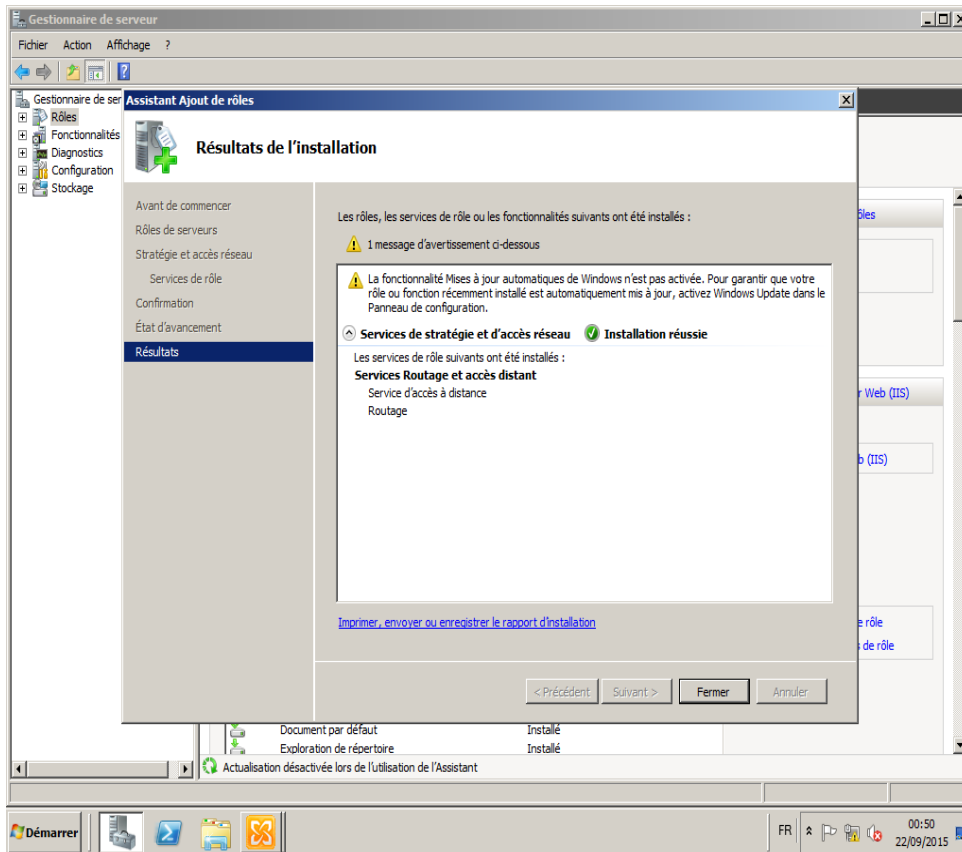
- Installation de windows 2008R2.
- Installation de deux cartes réseaux (10 et 20).



- L'ajout du role Service de stratégie et d'accès réseau (installé).

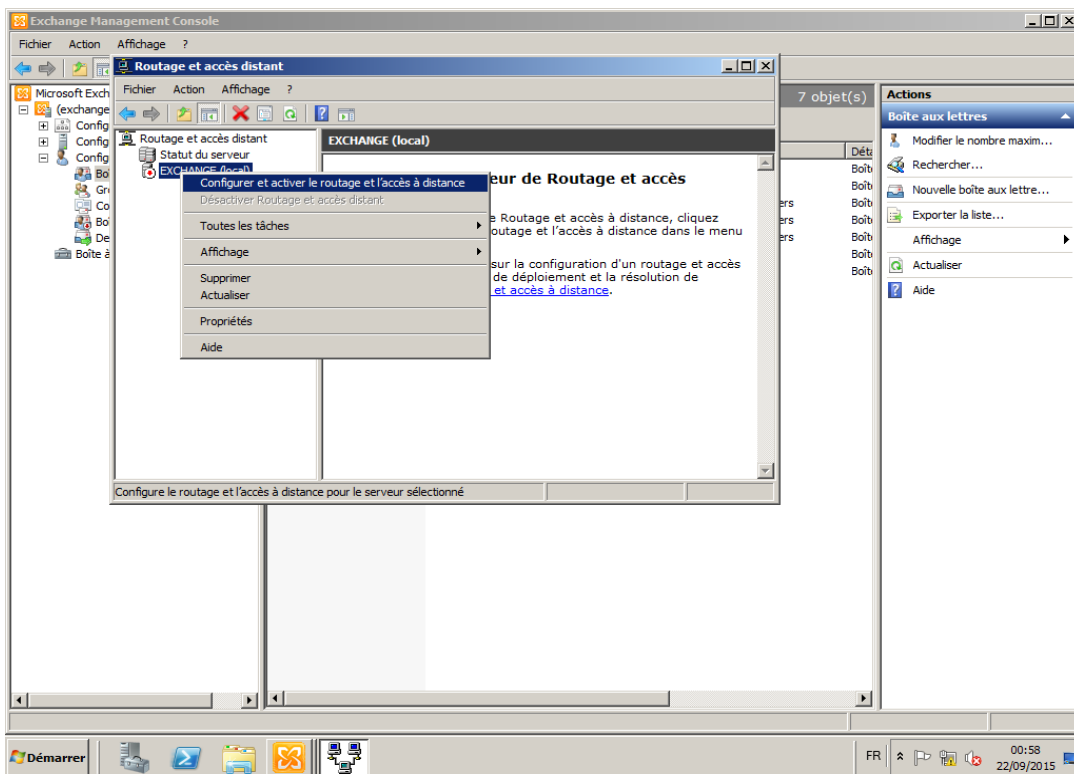


- Cocher Routage et accès distant



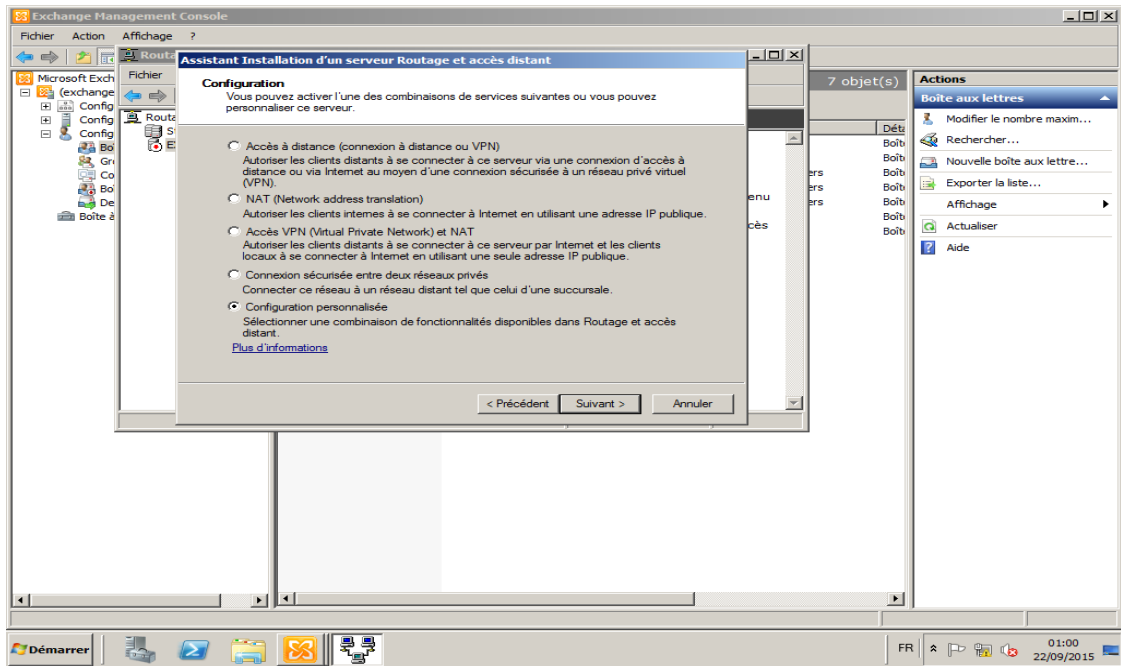
- l'installtion réussie

- Aller à Demarrer --> Outils d'administration --> Routage et accès distant --> clic droit Configurer et activer le routage et accès à distance



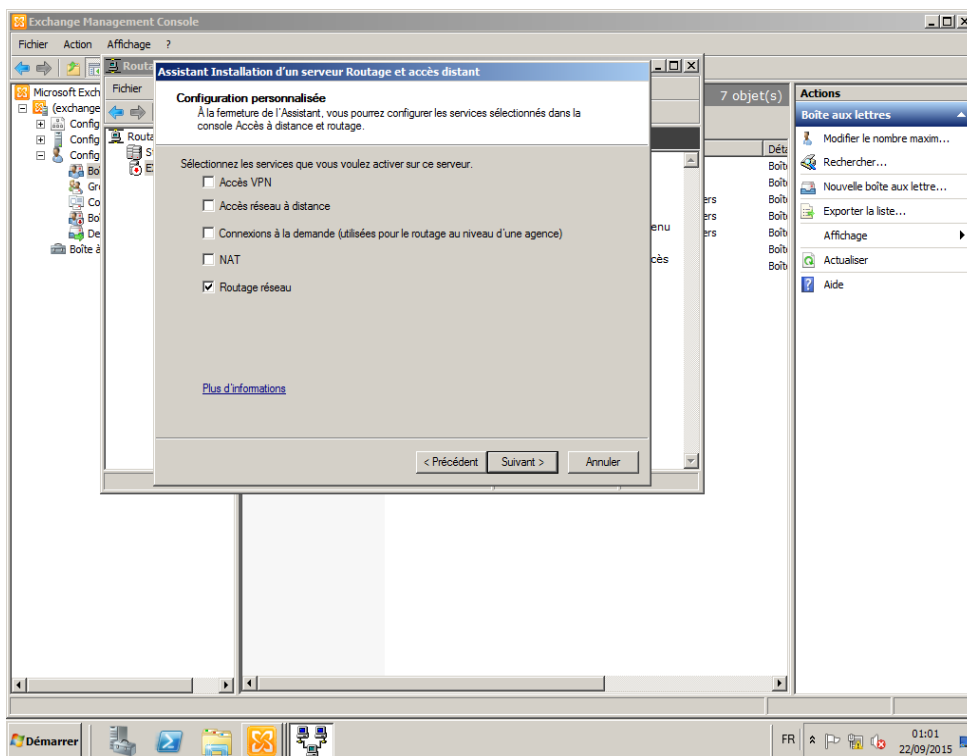
Configurer et activer le routage et accès à distance

Cocher Configuration personnalisée



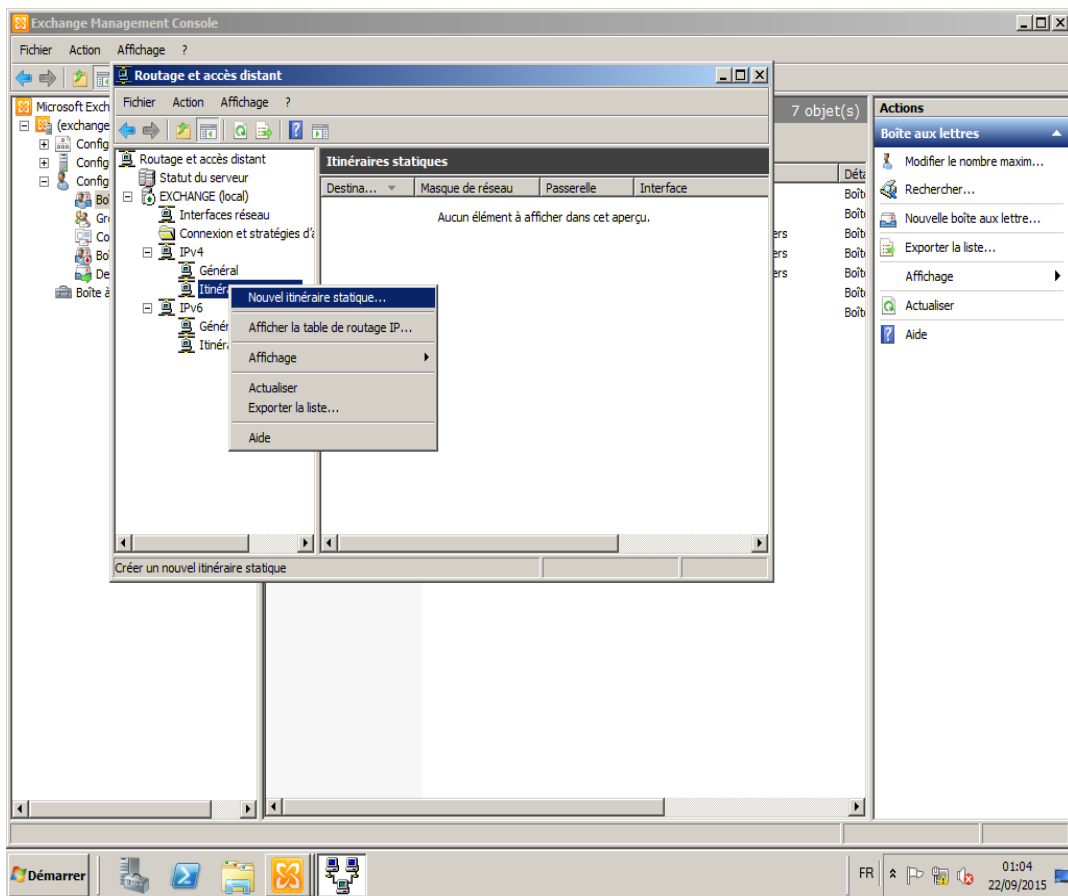
Configuration personnalisée

Cocher Routage réseaux



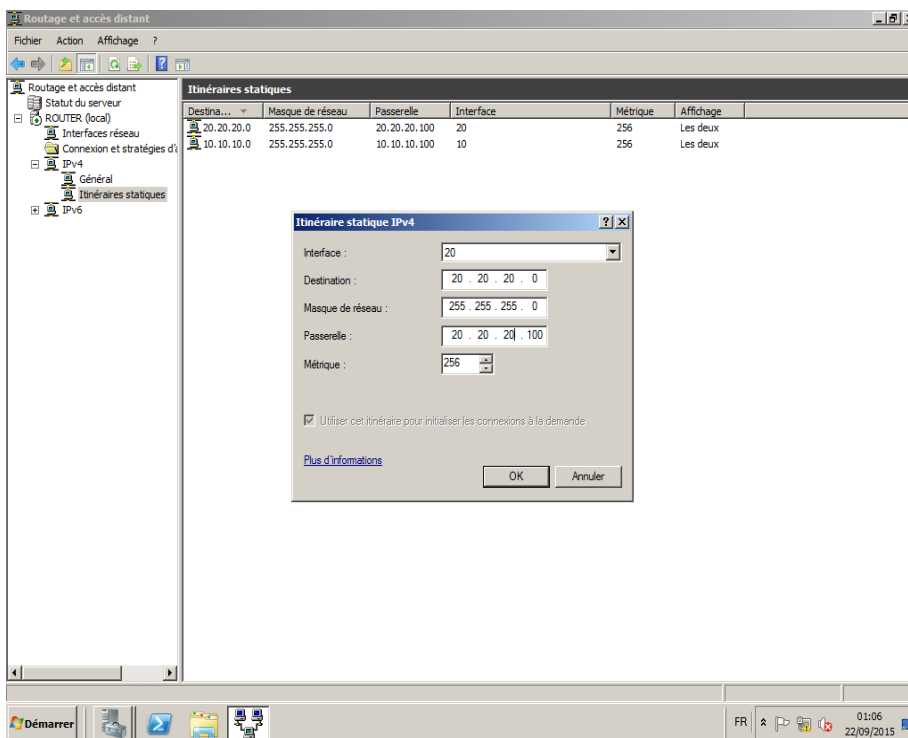
Routage réseau

Aller a IPv4 --> Itinéraires statiques --> Clic droit Nouvelle itinéraire statique



Nouvelle itinéraire statique

Ajouter les deux réseaux (10 et 20).



V.4/ Préparation des serveurs:

Dans notre projet, nous avons utilisé plusieurs serveurs, entre autres: le serveur de fichier (server file) mis en œuvre avec tous les privilèges (droits).

V.4.1/ Serveur file :

Un serveur de fichiers fournit un emplacement central sur le réseau qui permet de stocker et partager des fichiers avec des utilisateurs de notre réseau. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent, par conséquent, accéder aux fichiers sur le serveur de fichiers au lieu de devoir les transférer entre les ordinateurs individuels. Ils peuvent ensuite, les récupérer au moyen d'un protocole de partage de fichier selon les droits affectés par l'administrateur système.

V.4.1.1/ Les droits des utilisateurs :

Avant de parler des droits ou des privilèges, on doit donner l'architecture de notre serveur file qui est comme suite :

Partage->LABO->Achat----->Achat

D_achat

Users

CDG----->CDG

R_CDG

Users

INFORMATIQUE--->D_INFO

Informatique

Users

MARKETING----->D_Marketing

Marketing

Users

RH----->D_RH

RH

Users

SECURITE----->D_sécurité

Sécurité

Users

1- Dossier Père (Partage) :

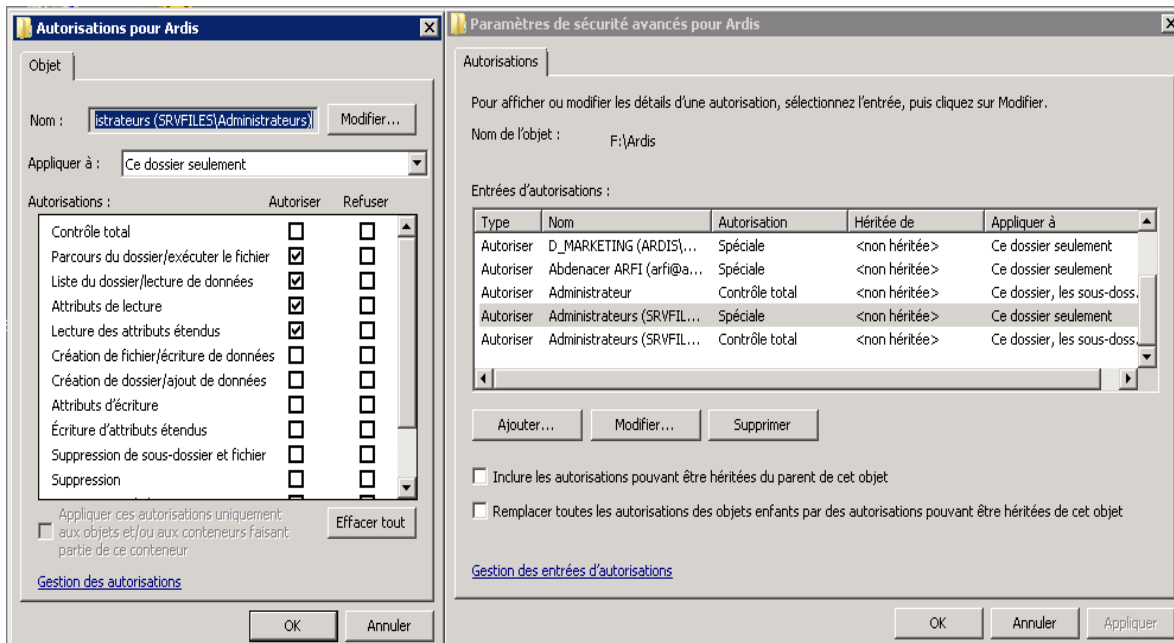


Figure V.1: Autorisations Spéciales Administrateur Local 1.

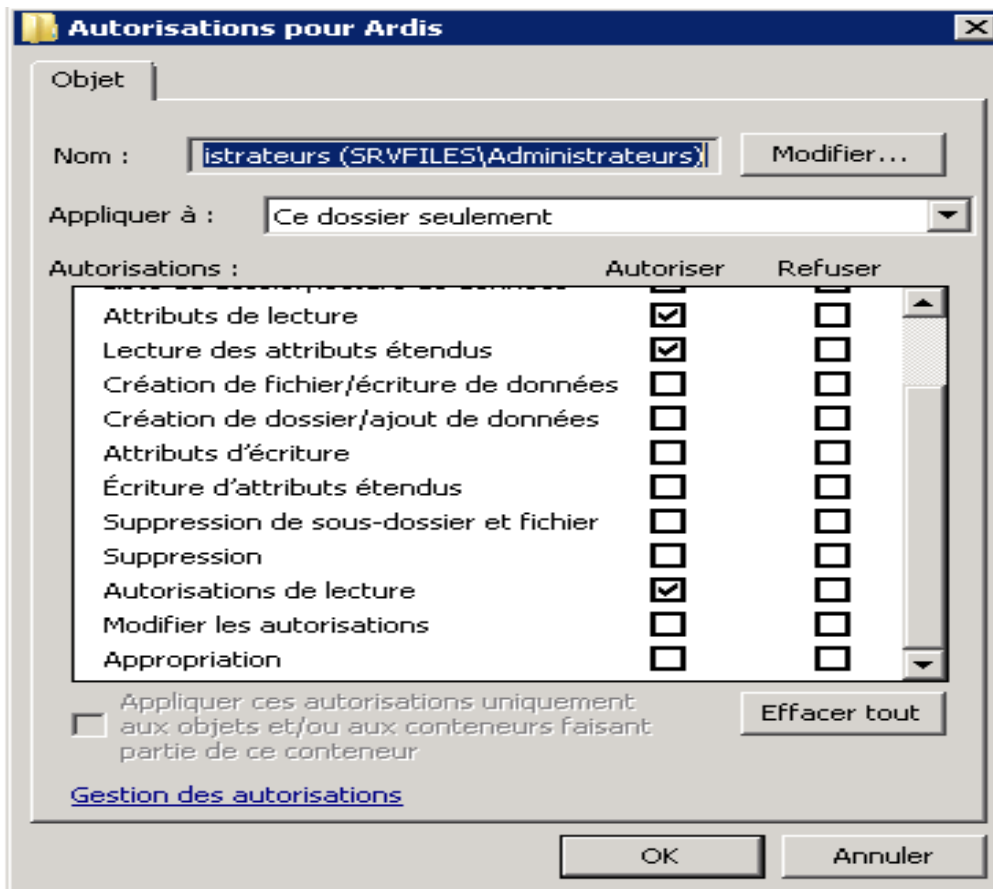


Figure V.2: Autorisations Spéciales Administrateur Local 2.

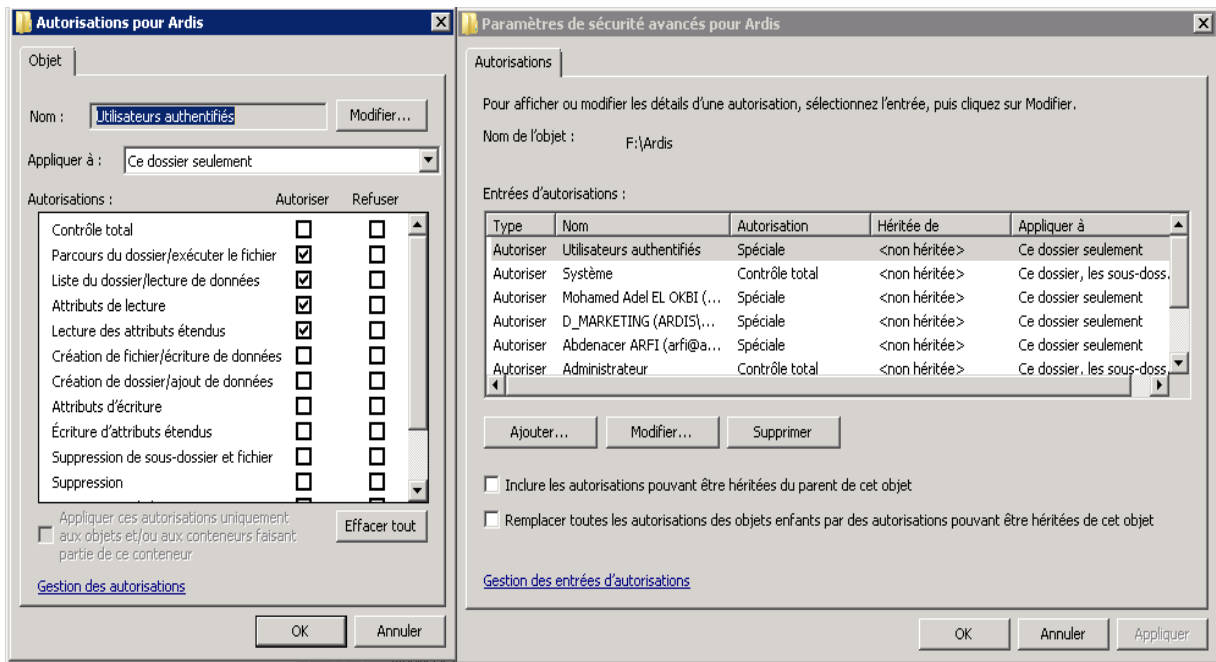


Figure V.3: Autorisations Spéciales Utilisateur Authentifiés 1.

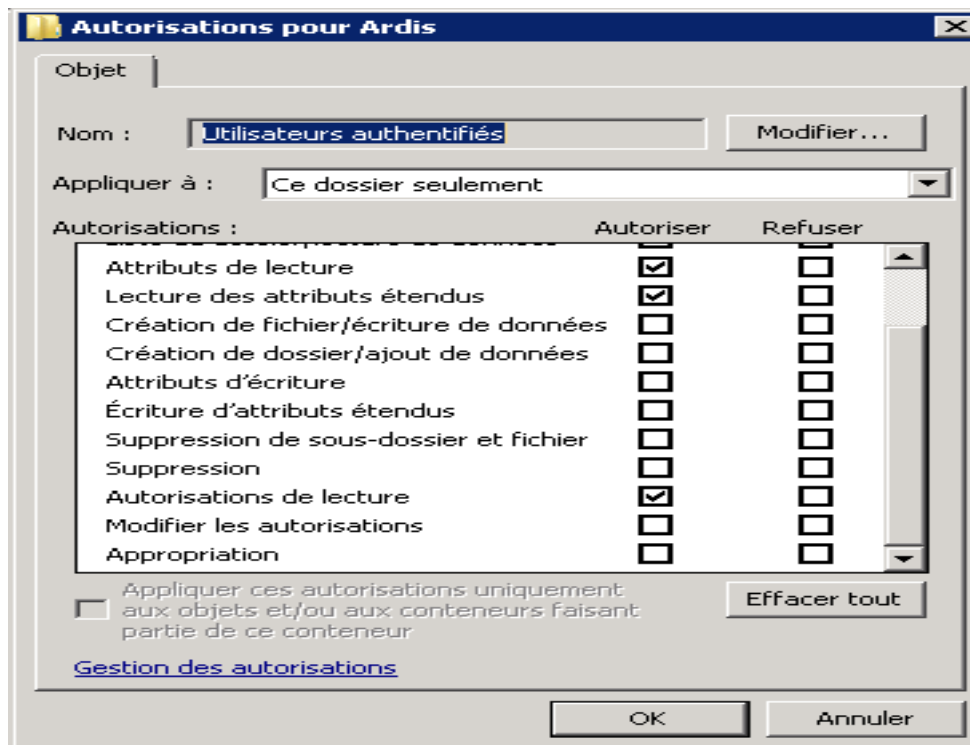


Figure V.4: Autorisations Spéciales Utilisateur Authentifiés 2.

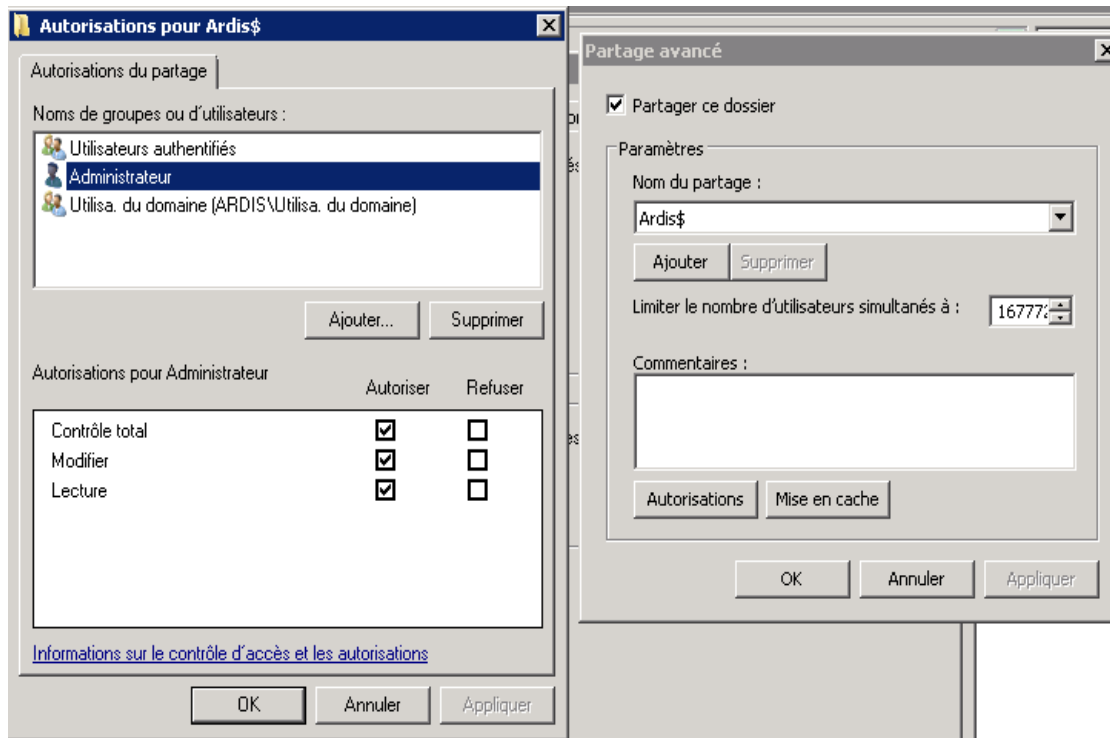


Figure V.5: Partage Administrateur.

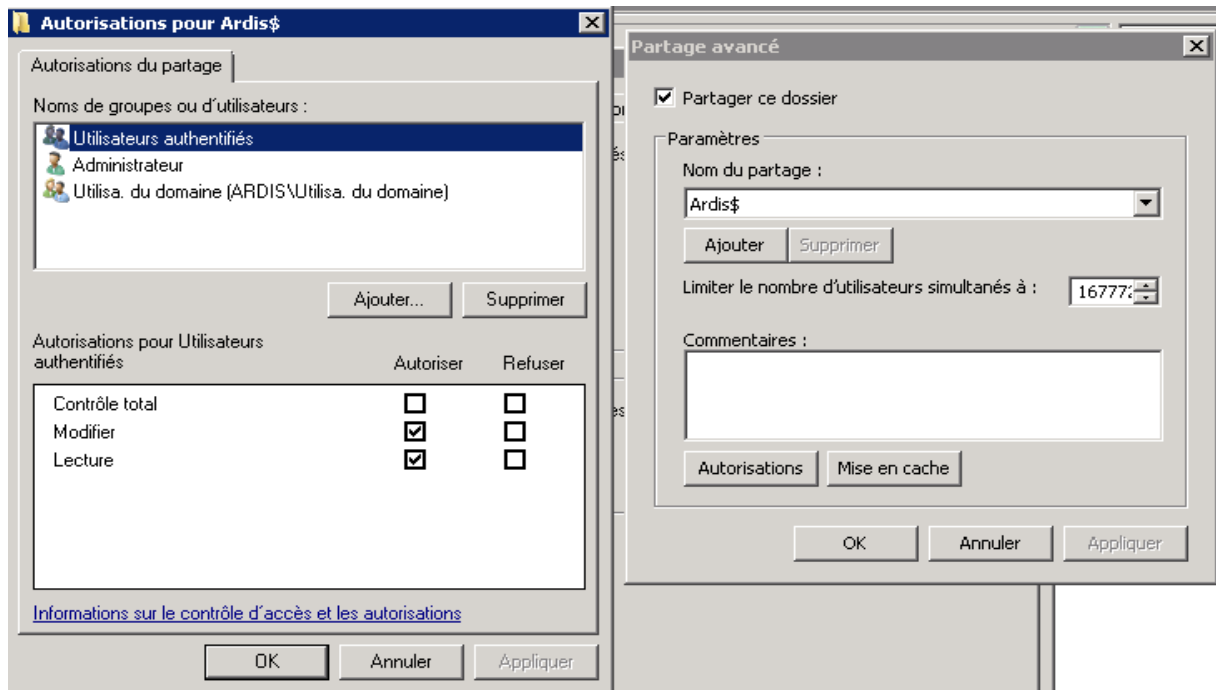


Figure V.6: Partage Utilisateur Authentifiés.

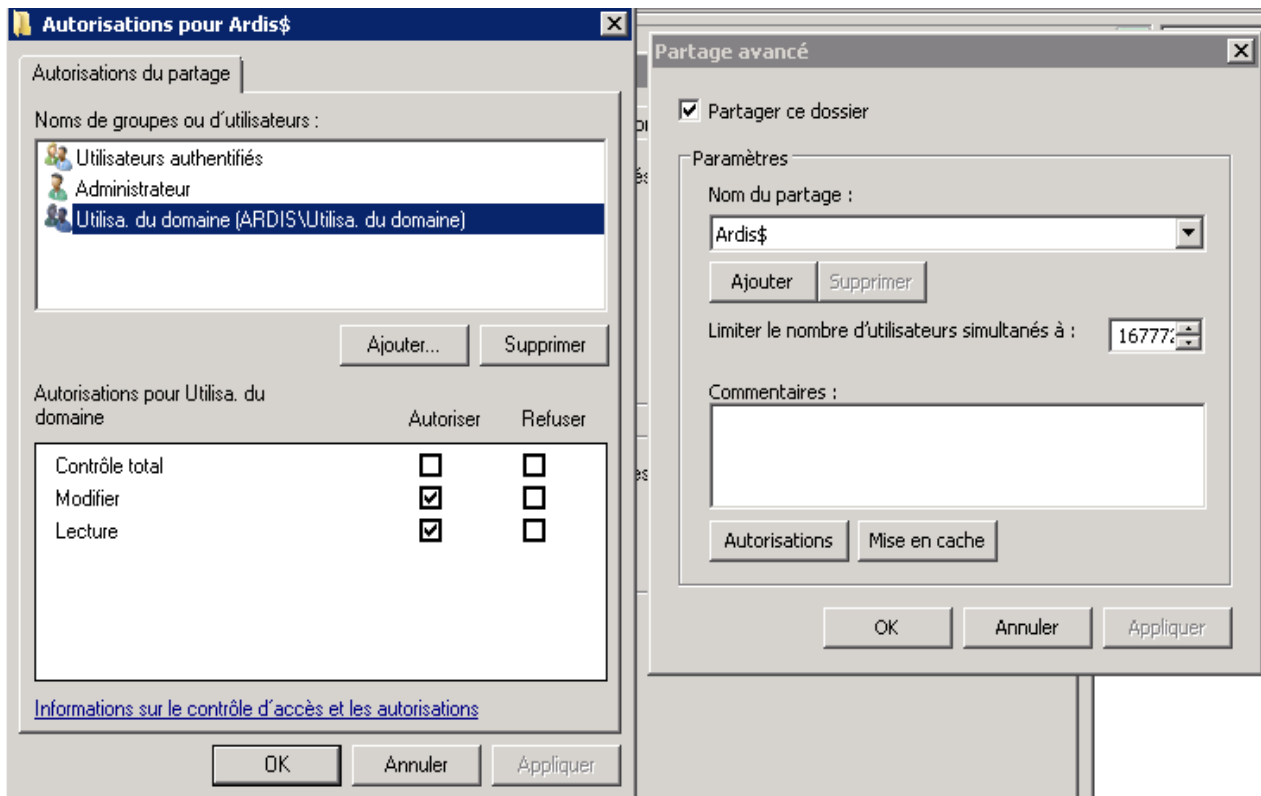


Figure V.7: Partage Utilisateur du domaine.

2- Dossier sous père (LABO) :

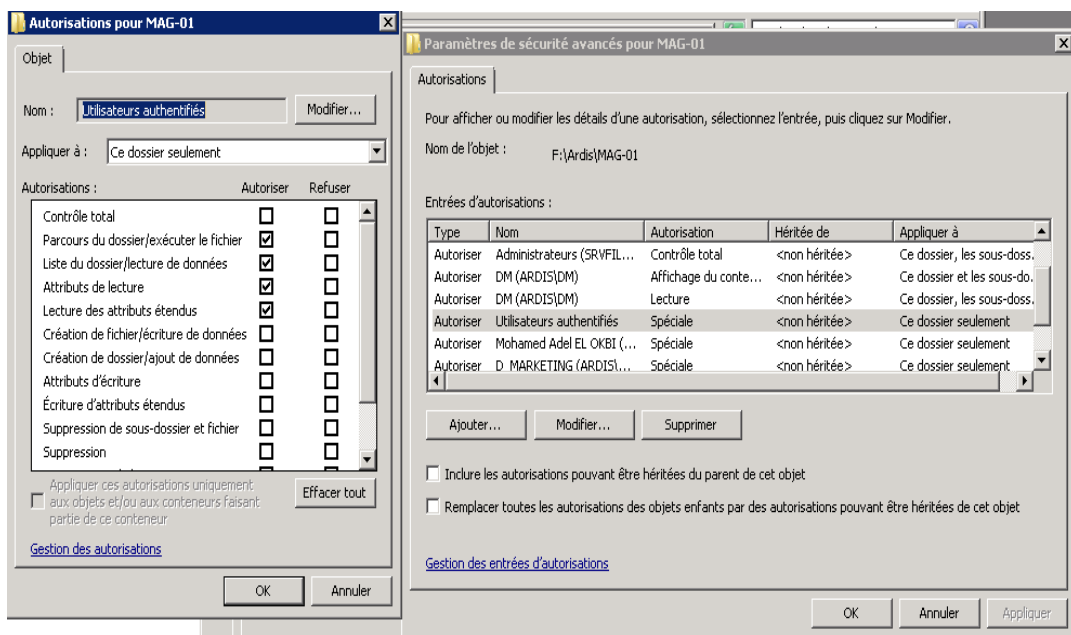


Figure V.8: Autorisations Spéciales Utilisateur Authentifiés 1.

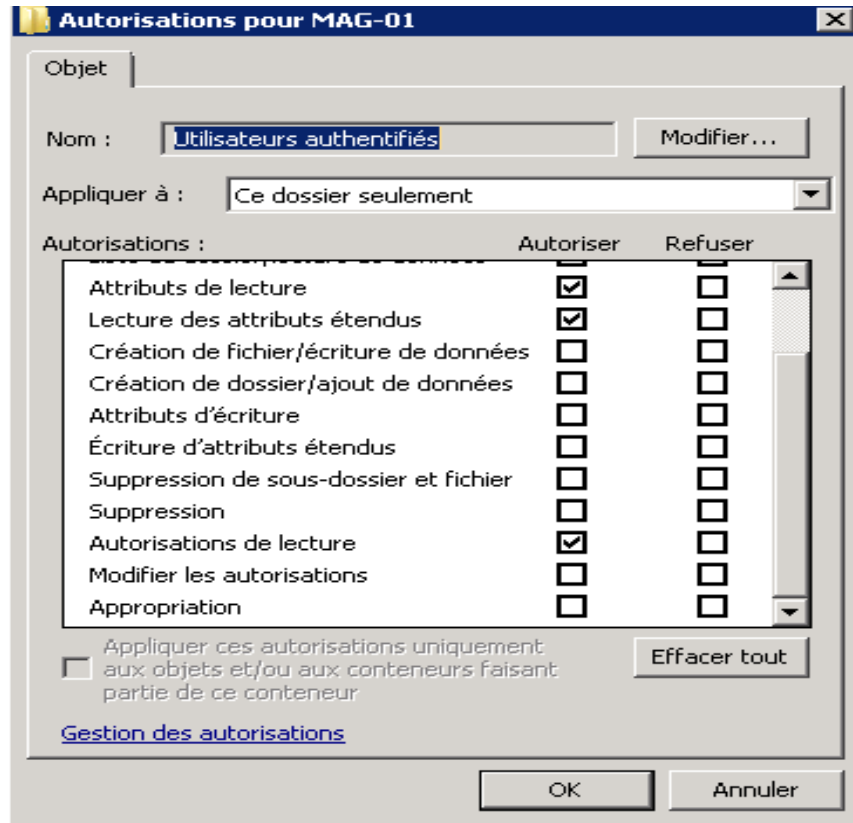


Figure V.9: Autorisations Spéciales Utilisateur Authentifiés 2.

3- Dossier Lecteur Service (Achat) :

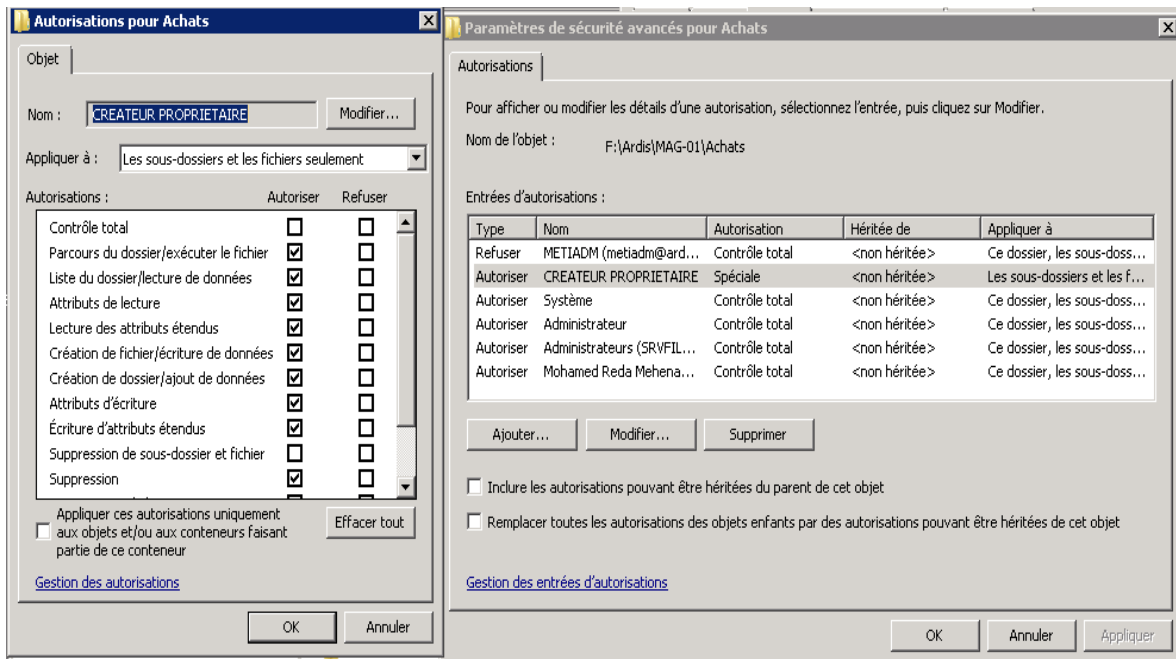


Figure V.10: Autorisation Spéciales Créateur Propriétaire 1.

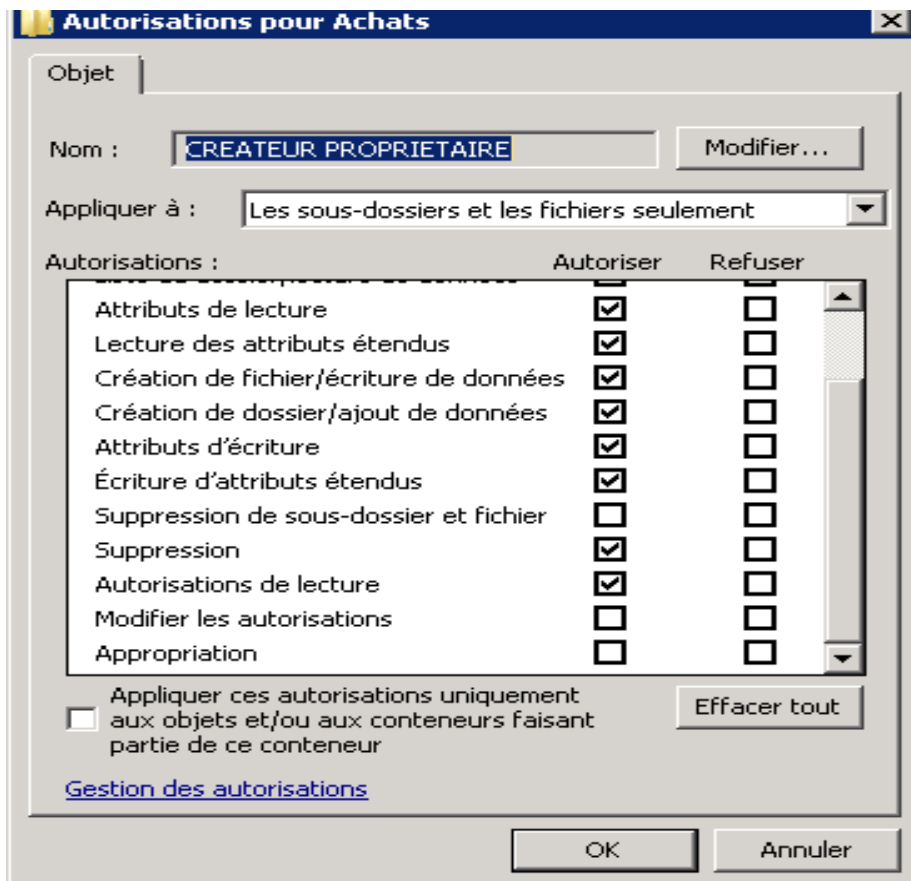


Figure V.11: Autorisation Spéciales Créateur Propriétaire 2.

4- Dossier Responsable Service (achat D_achat) :

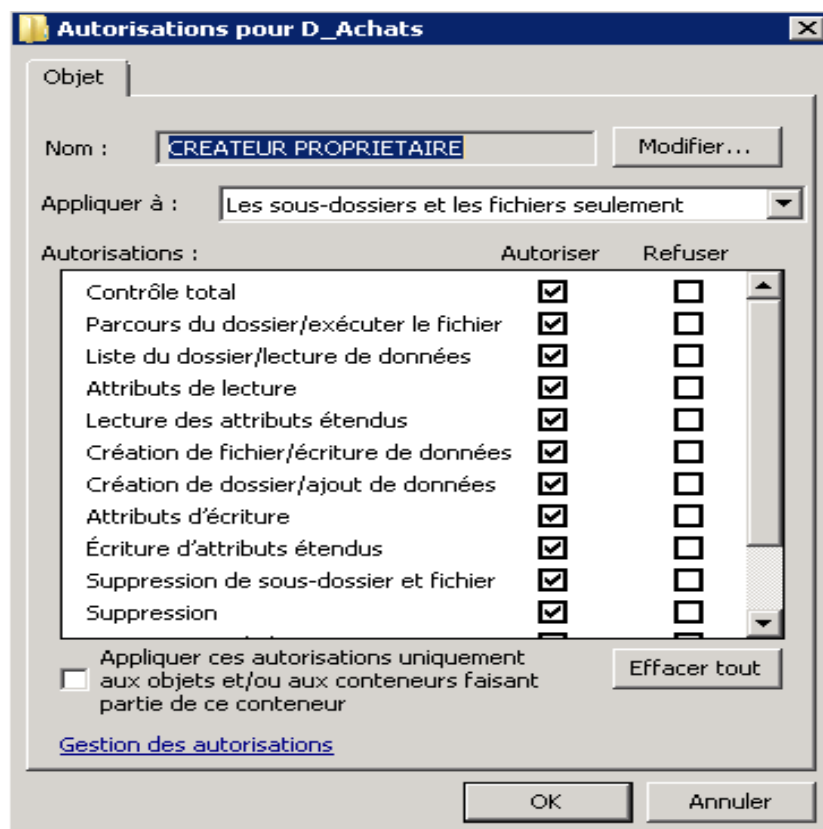


Figure V.12: Autorisation Spéciales Créateur Propriétaire 1.

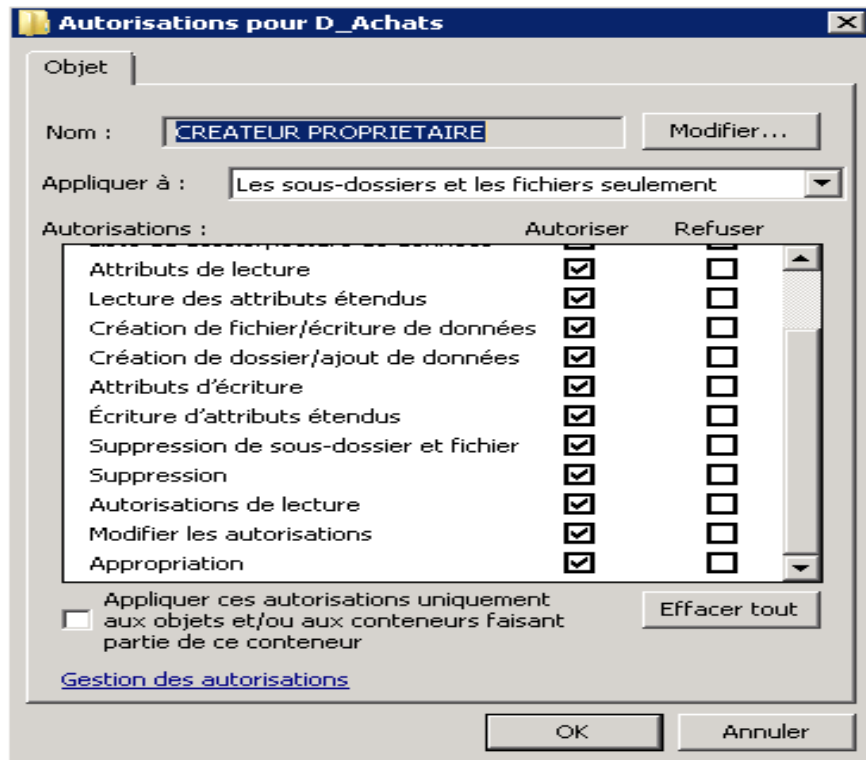


Figure V.13: Autorisation Spéciales Créateur Propriétaire 2.

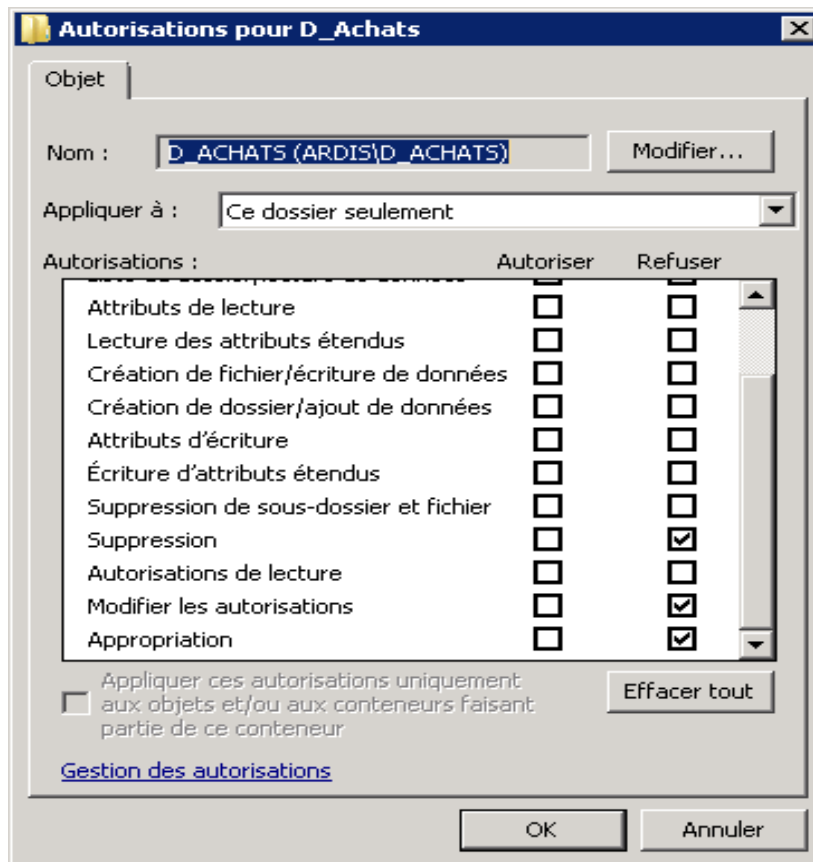


Figure V.14: Autorisation Spéciales GRP_RESP_Service.

5-Dossier Partage Service (Achat achat) :

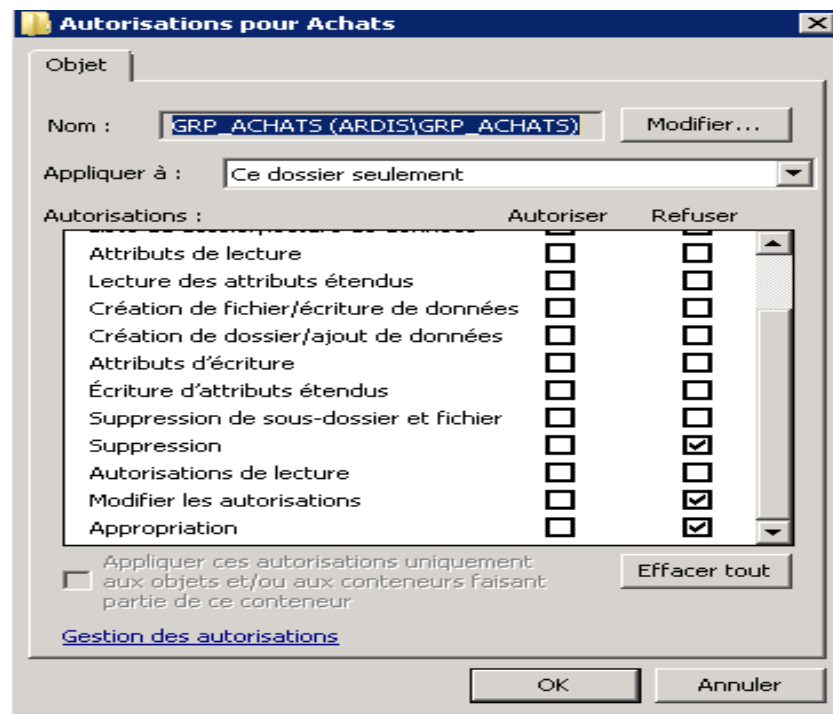


Figure V.15: Autorisation Spéciales GRP_SERVICE.

6-Dossier Utilisateurs (achat users) :

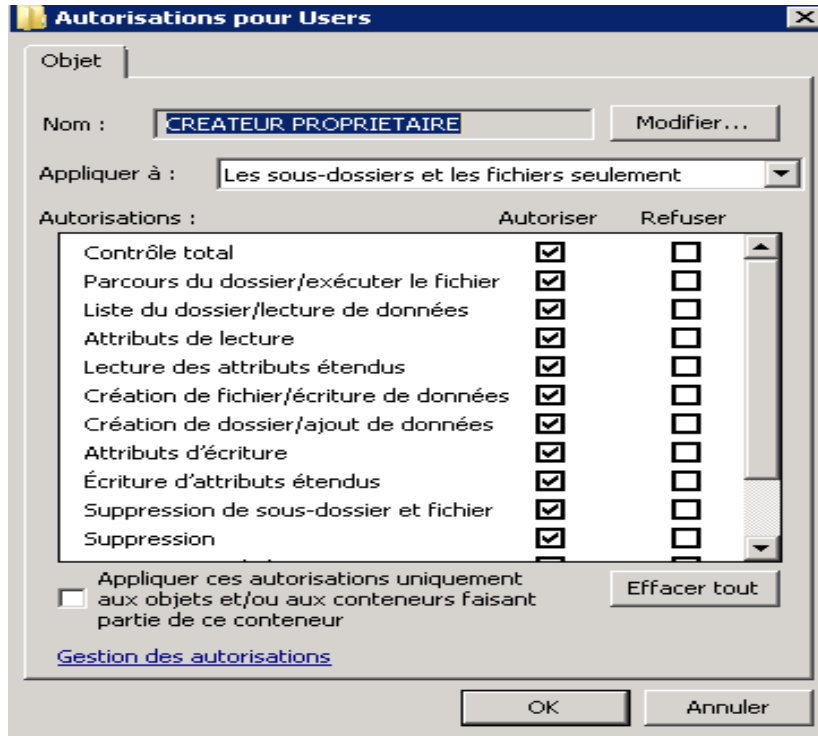


Figure V.16: Autorisation Spéciales Créateur Propriétaire 1.

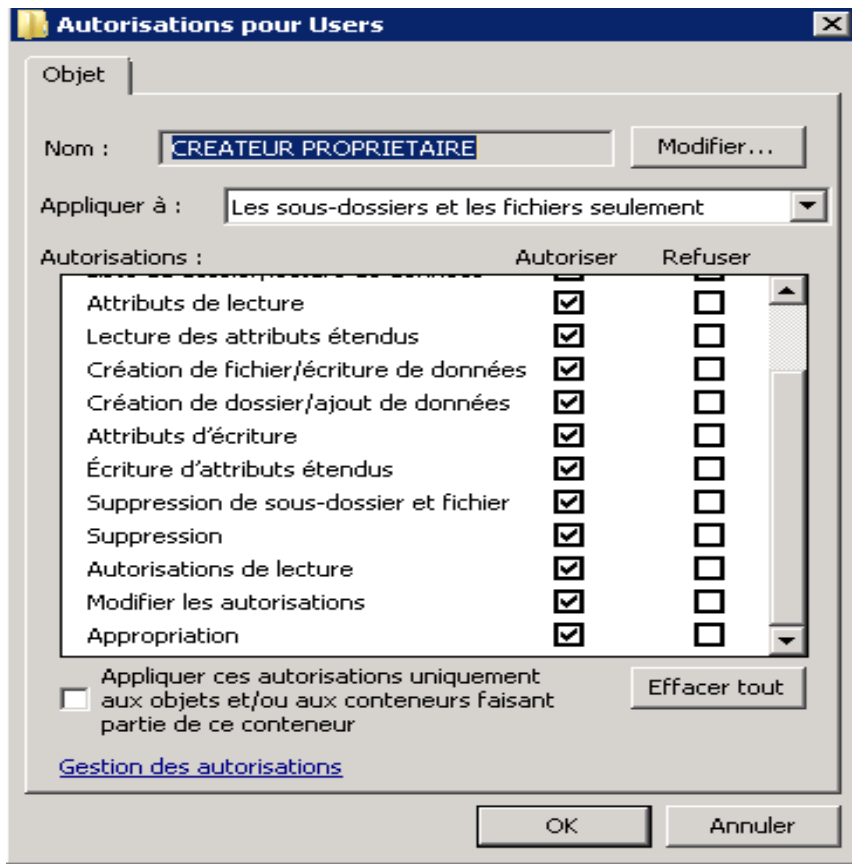


Figure V.17: Autorisation Spéciales Créateur Propriétaire 2.

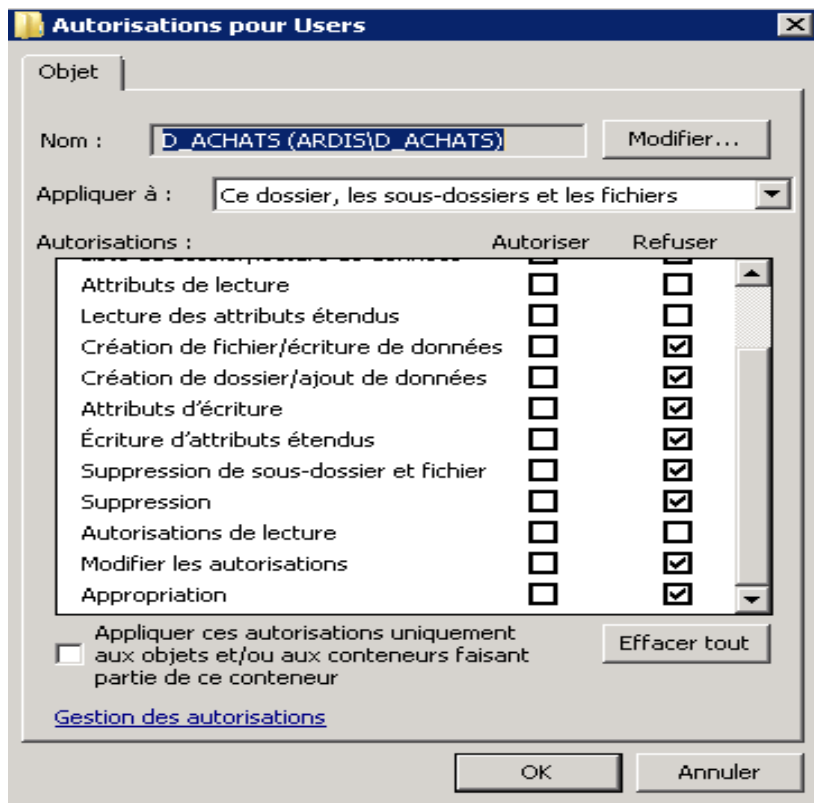


Figure V.18: Autorisation Spéciales GRP_RESP_SERVICE.

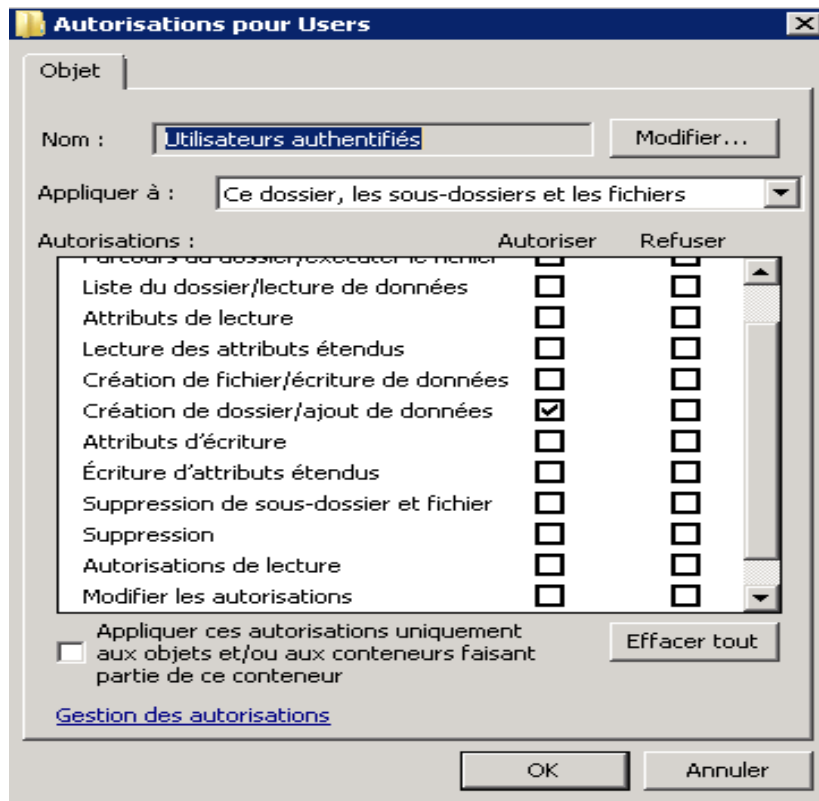


Figure V.19: Autorisation Spéciales Utilisateurs Authentifiés.

7-Dossier Partage tout le monde (Echange) :

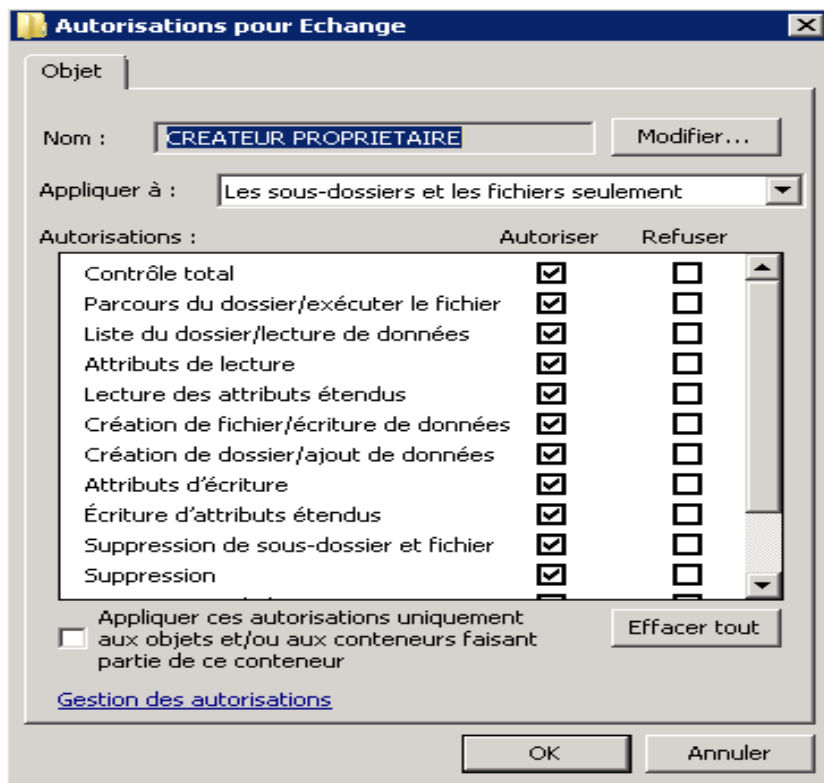


Figure V.20: Autorisation Spéciales Créateur Propriétaire 1.

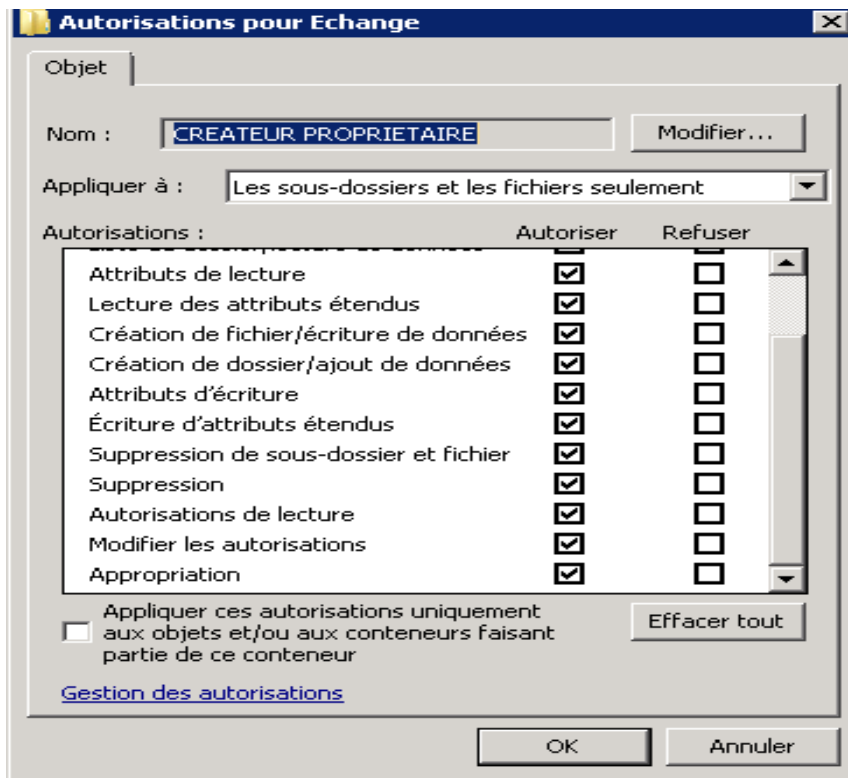


Figure V.21: Autorisation Spéciales Créateur Propriétaire 2.

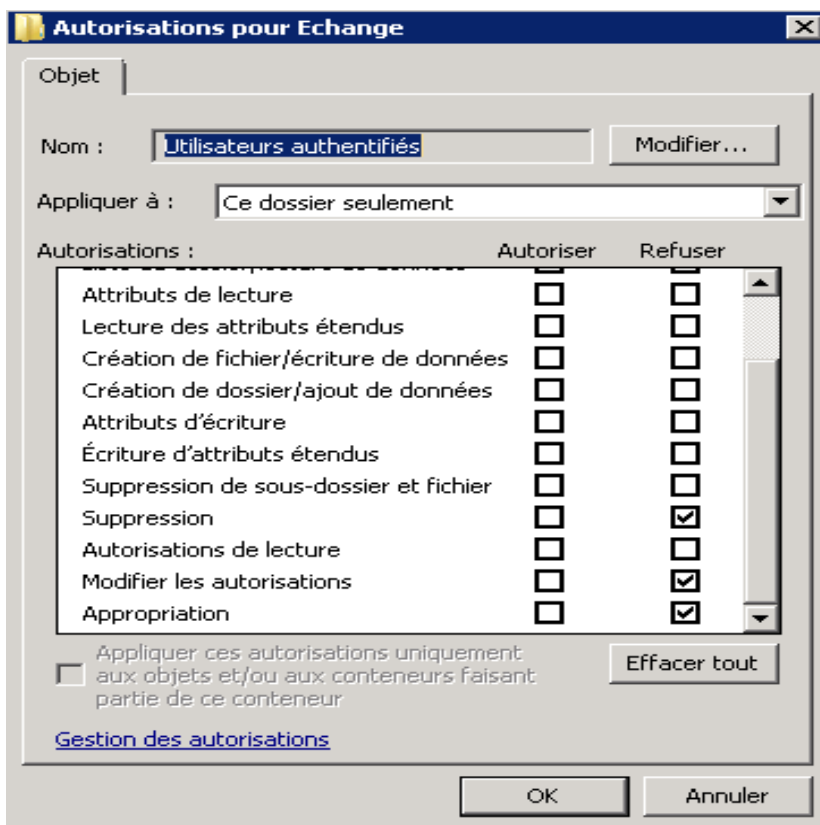


Figure V.22: Autorisation Spéciales Utilisateurs Authentifiés.

8-Dossier Procedures Entreprise :

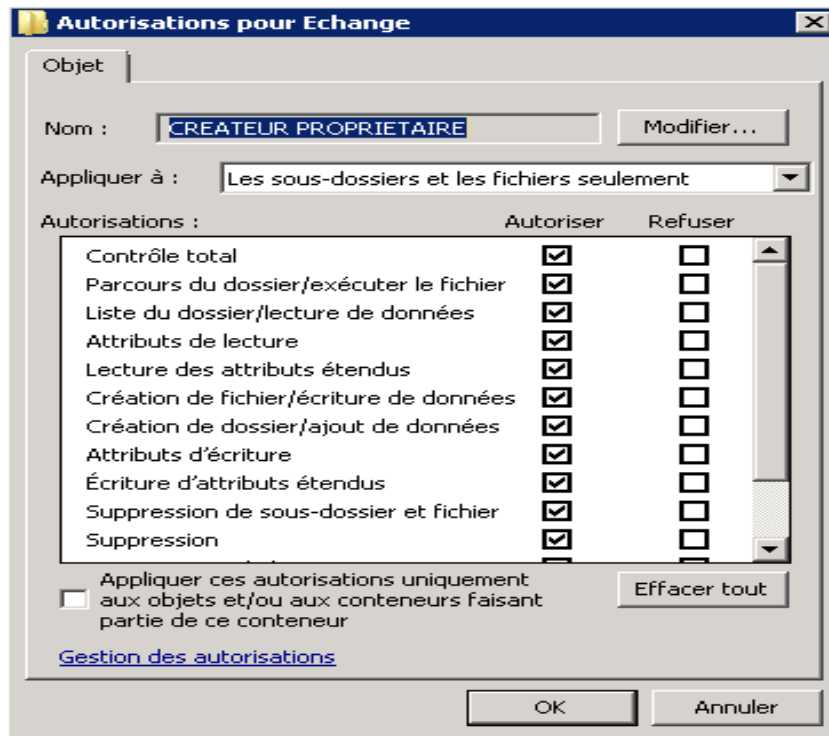


Figure V.23: Autorisation Spéciales Créateur Propriétaire 1.

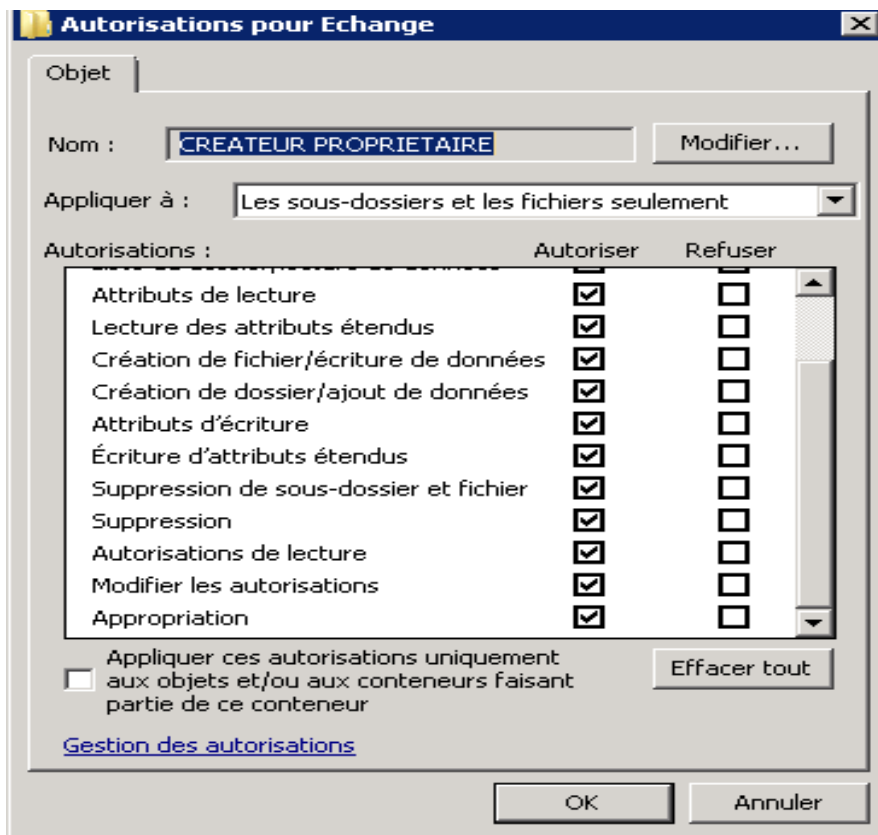


Figure V.24: Autorisation Spéciales Créateur Propriétaire 2.

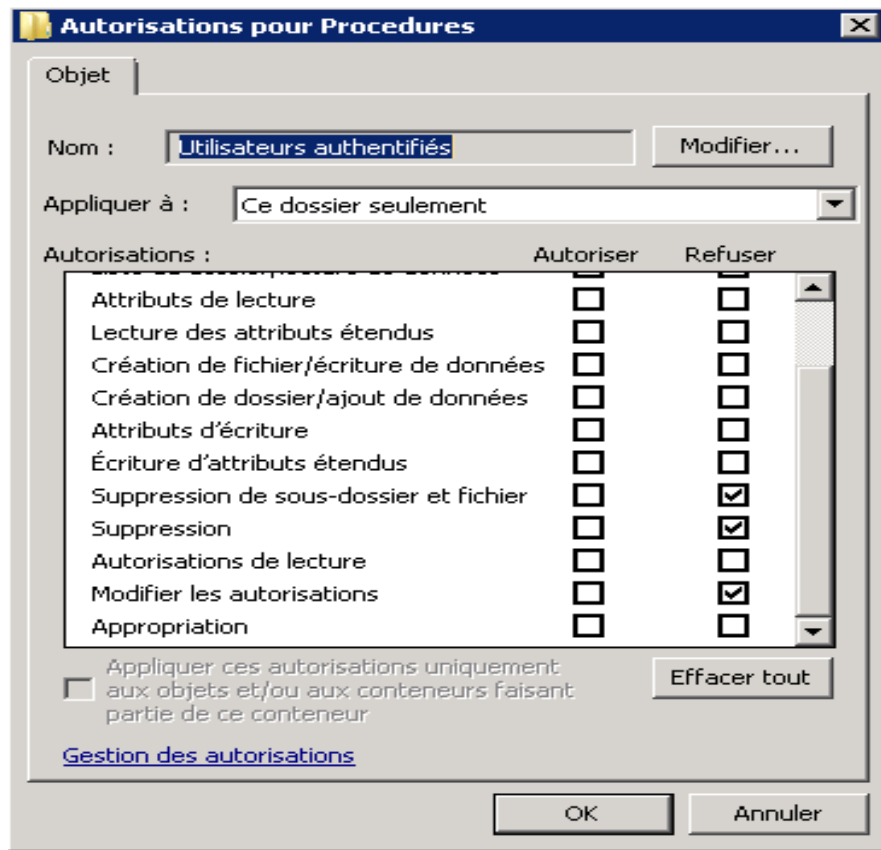


Figure V.25: Autorisation Spéciales Utilisateurs Authentifiés.

9-Dossier Utilisateurs sans Service :

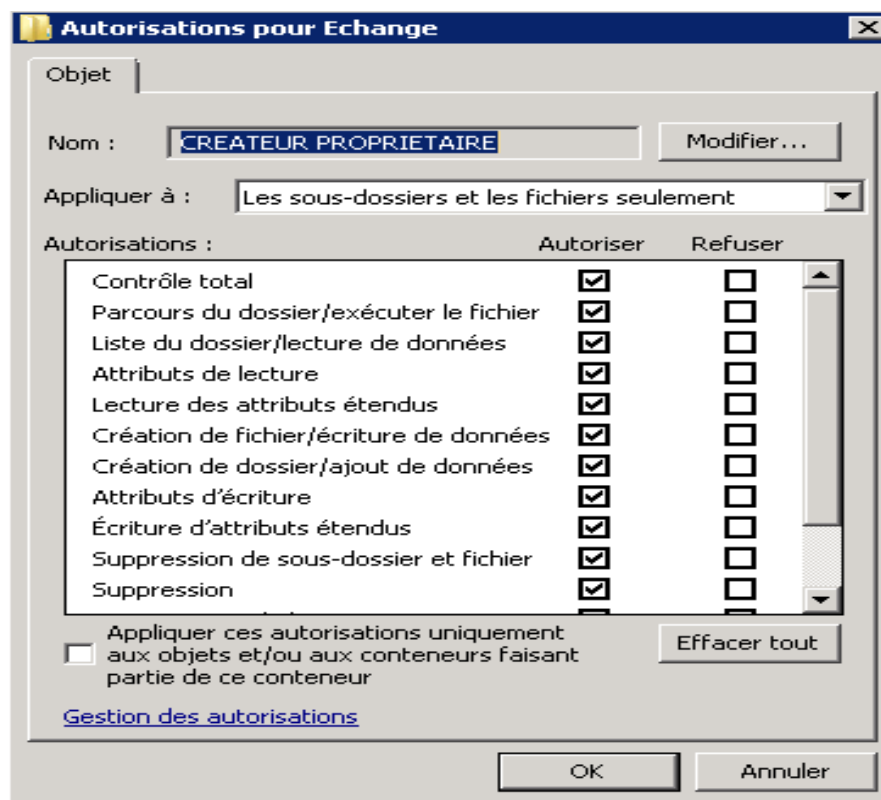


Figure V.26: Autorisation Spéciales Créateur Propriétaire 1.

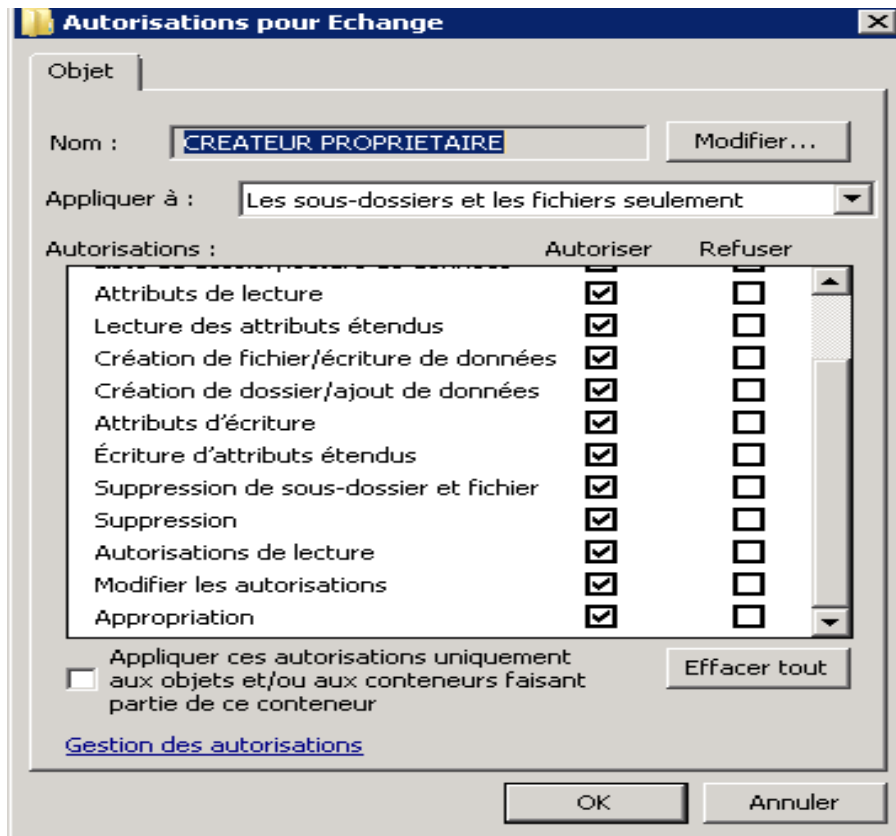


Figure V.27: Autorisation Spéciales Créateur Propriétaire 2.

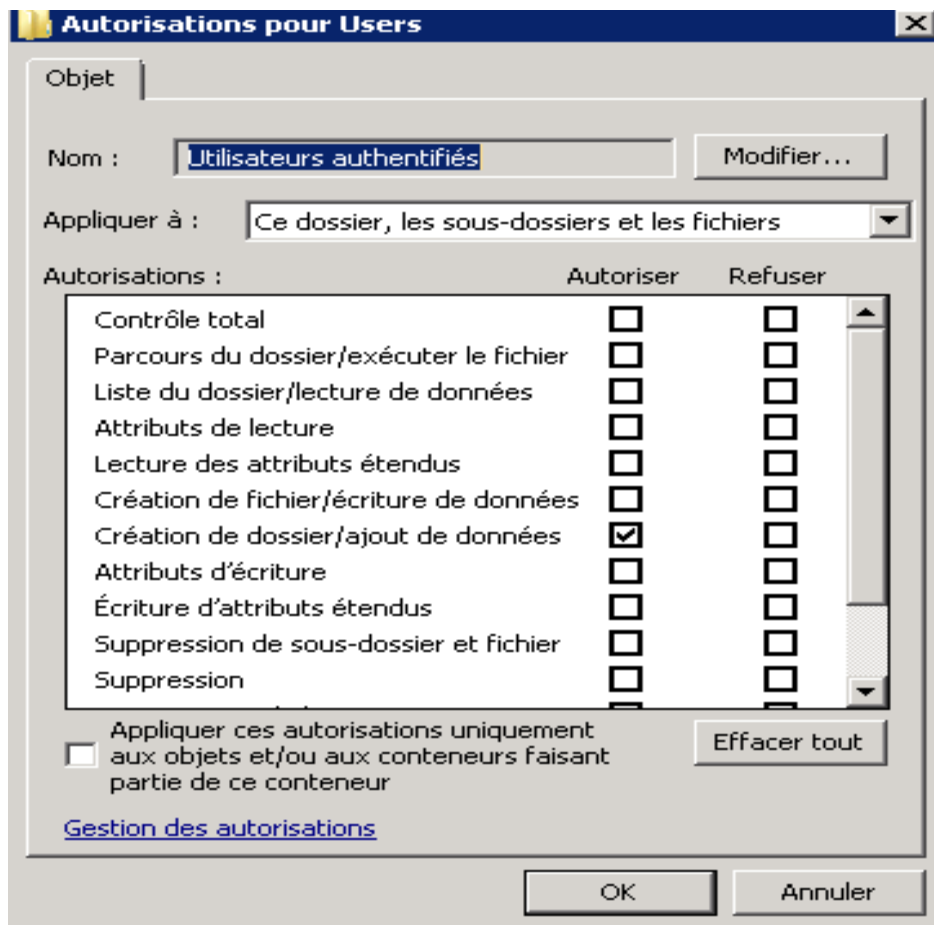


Figure V.28: Autorisation Spéciales Utilisateurs Authentifiés.

Il est bien connu que le serveur file compte parmi les serveurs les plus importants et intéressants dans une société puisqu'il permet de stocker toutes les données des utilisateurs. Une sauvegarde est donc nécessaire pour éviter la perte des données ou tout autre incident qui peut stopper l'entreprise.

Pour procéder à la sauvegarde réciproque du file on procède comme suite :

Demarrer → outils d'administration → Gestion du système distribué DFS → clic droit → Nouveau groupe de réplication → Groupe de réplication multi-usage → ENTRER LE NOM → Ajouter les deux serveurs → suivant → Serveur à Répliquer (endroit de la Réplication) → Créer un dossier de réplication → Créer.

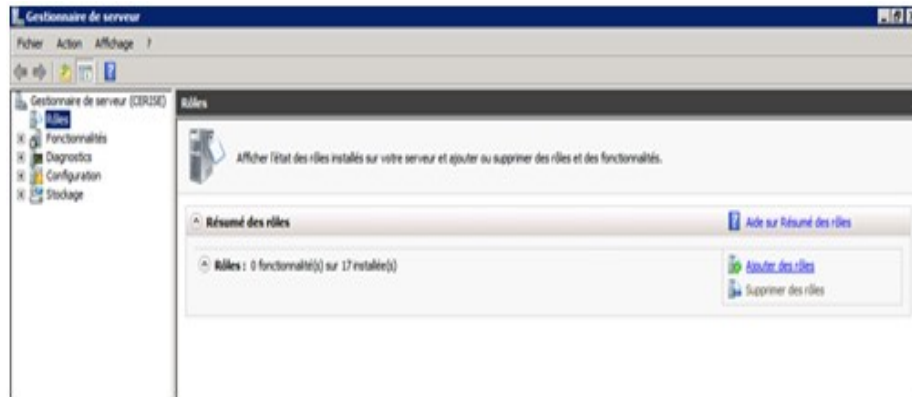
V.4.2/ Serveur AD :

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

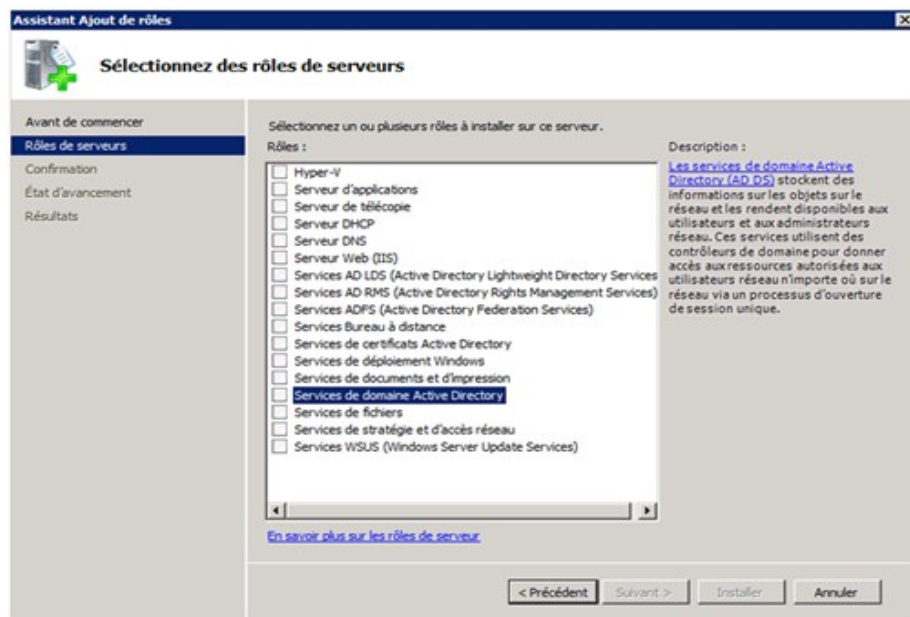
V.4.2.1/ Créer un domaine :

✓ Installation :

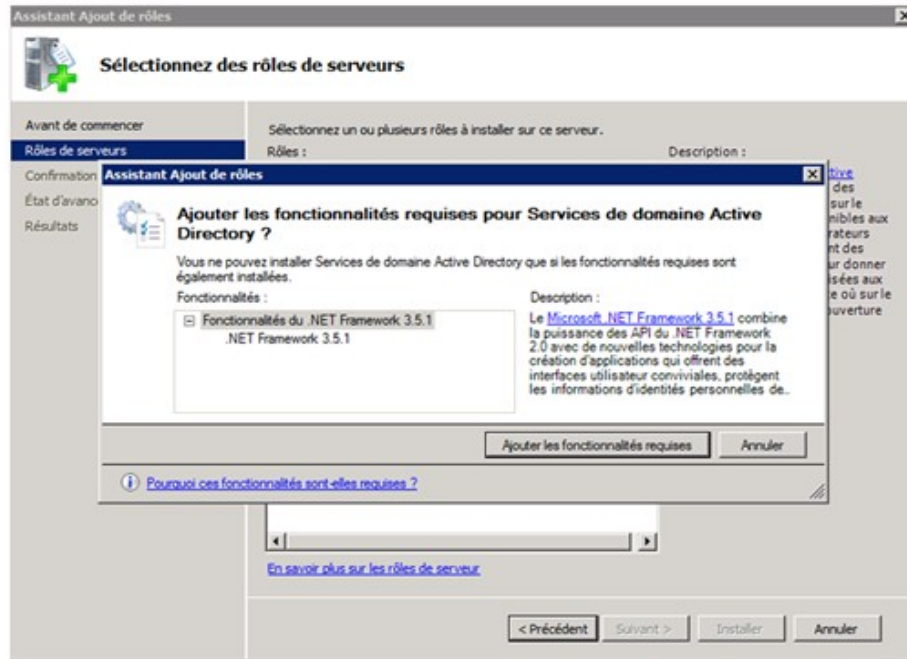
Commencez par ouvrir le “Gestionnaire de serveur” et cliquez sur “Ajouter des rôles”.



Cochez la case “Services de domaine Active Directory”.



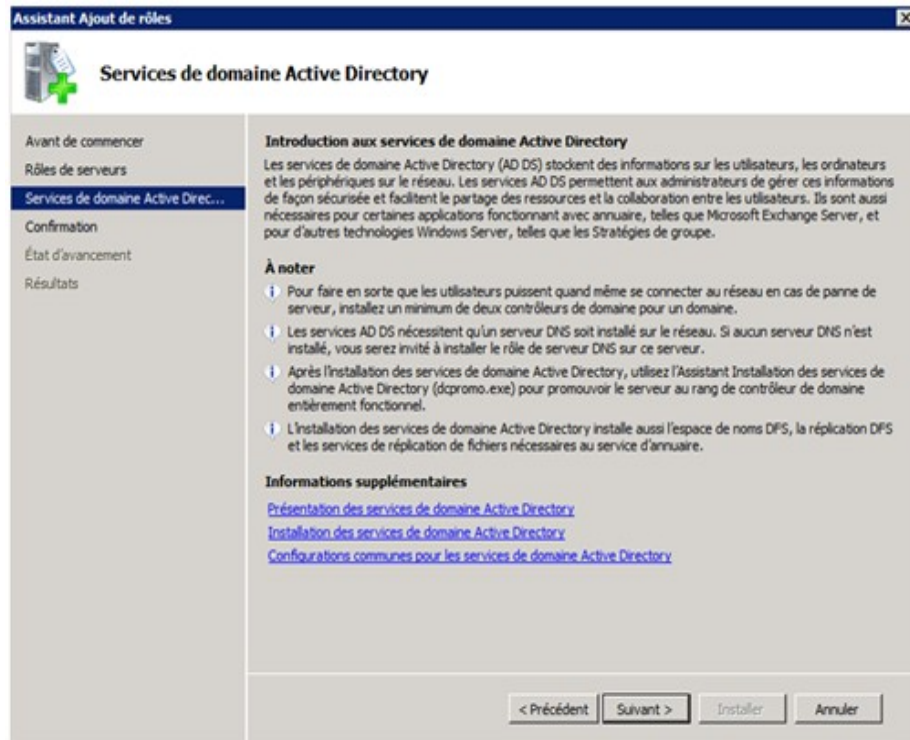
Si votre serveur vous demande d’installer “.NET Framework”, cliquez sur ‘Ajouter les fonctionnalités requises’.



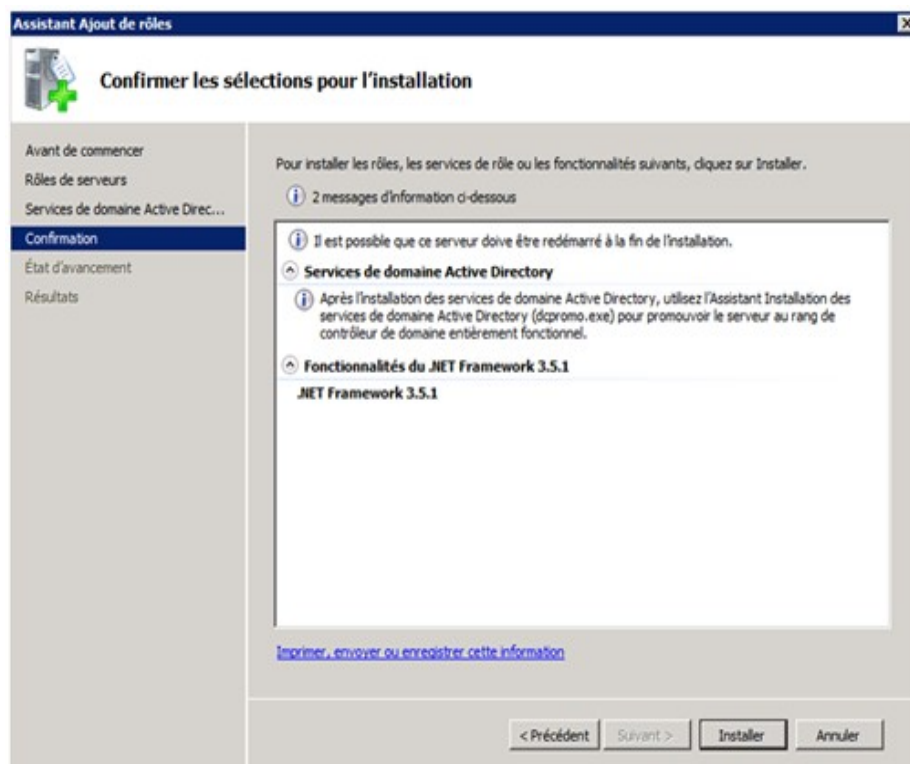
Cliquez sur “Suivant”.



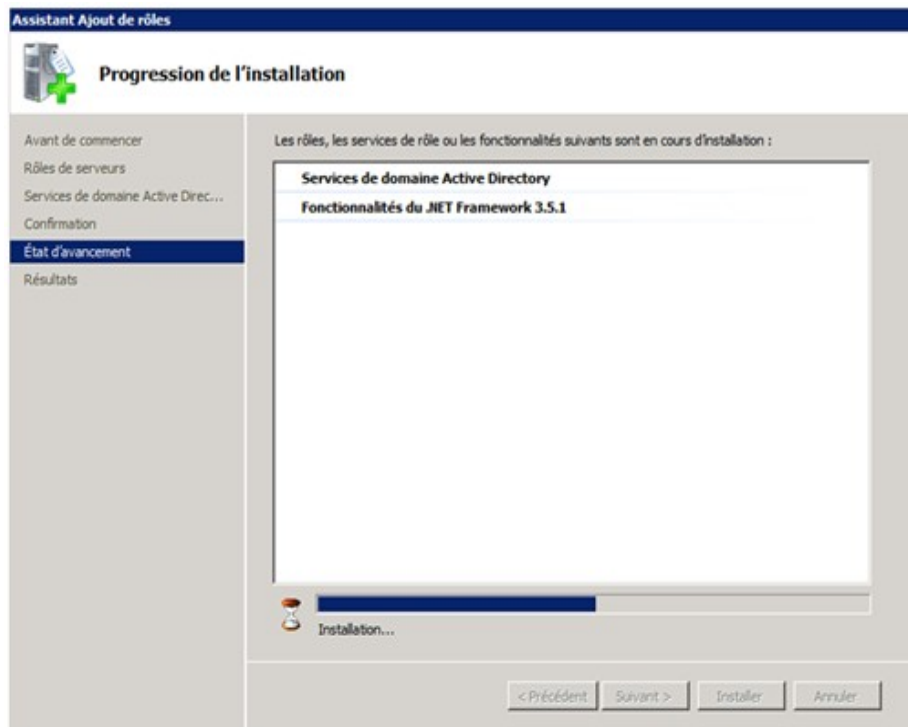
Cliquez sur “Suivant”.



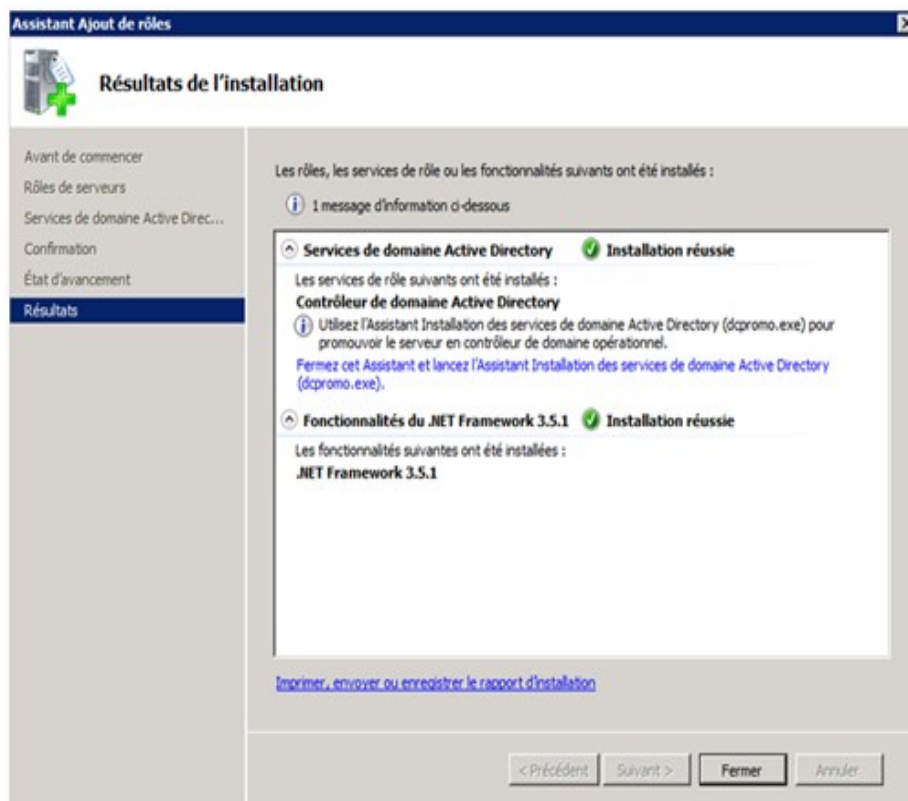
Cliquez sur "Installer".



Patiencez pendant l'installation.

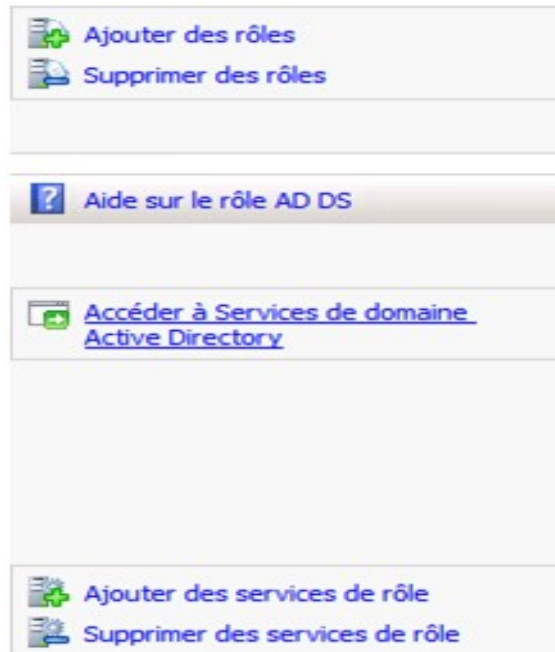


Cliquez sur “Fermer”.



✓ **Configuration :**

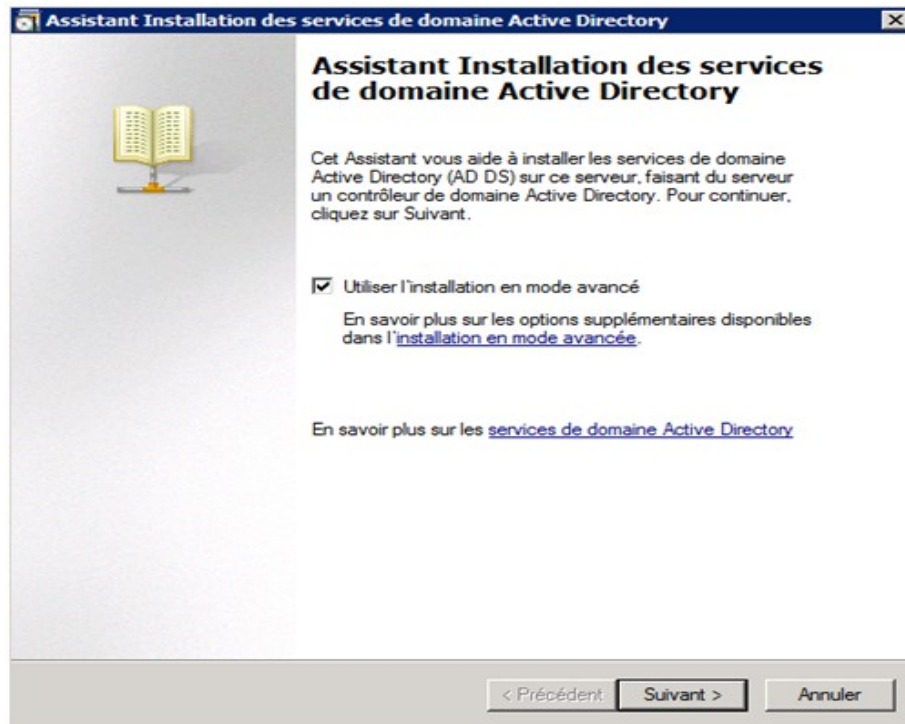
Retournez ensuite sur le “Gestionnaire de serveur”, puis cliquez sur “Accéder à services de domaine Active Directory”.



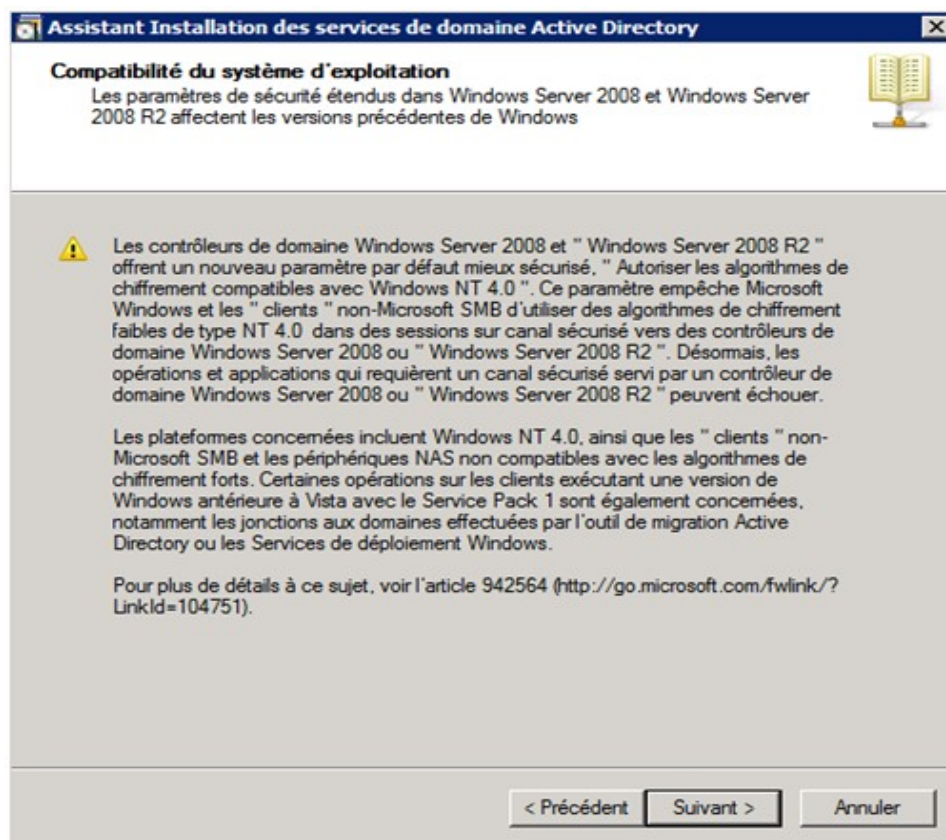
Cliquez sur “Dcpromo.exe”.



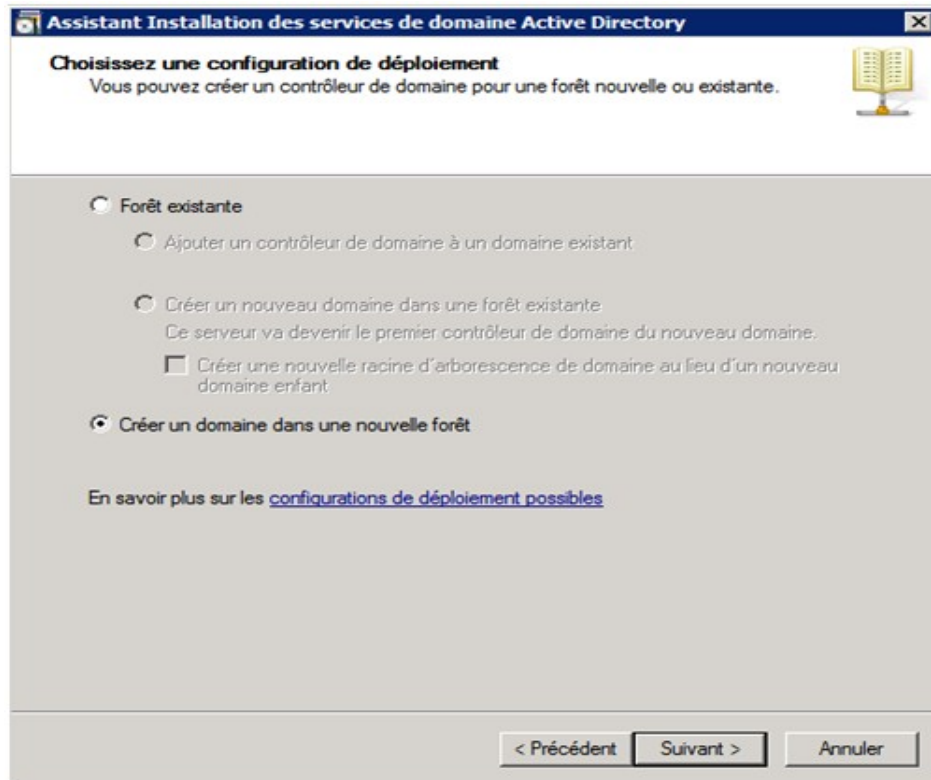
Cochez sur “Utiliser l’installation en mode avancé”, puis sur “Suivant”.



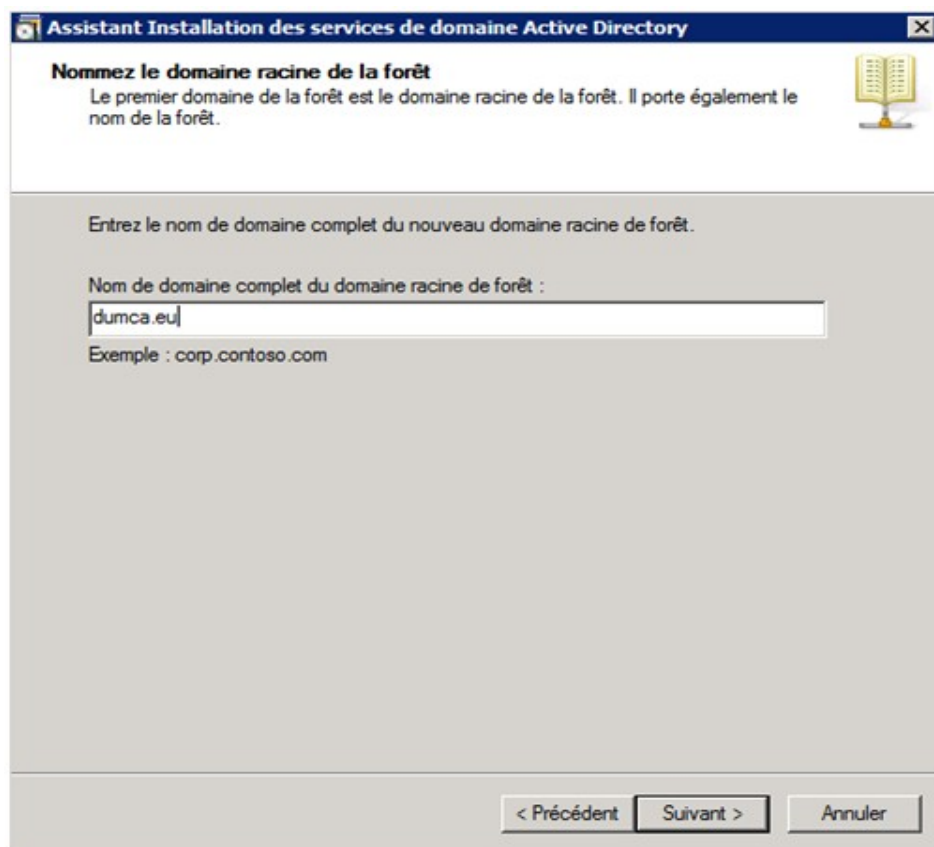
Cliquez sur “Suivant”.



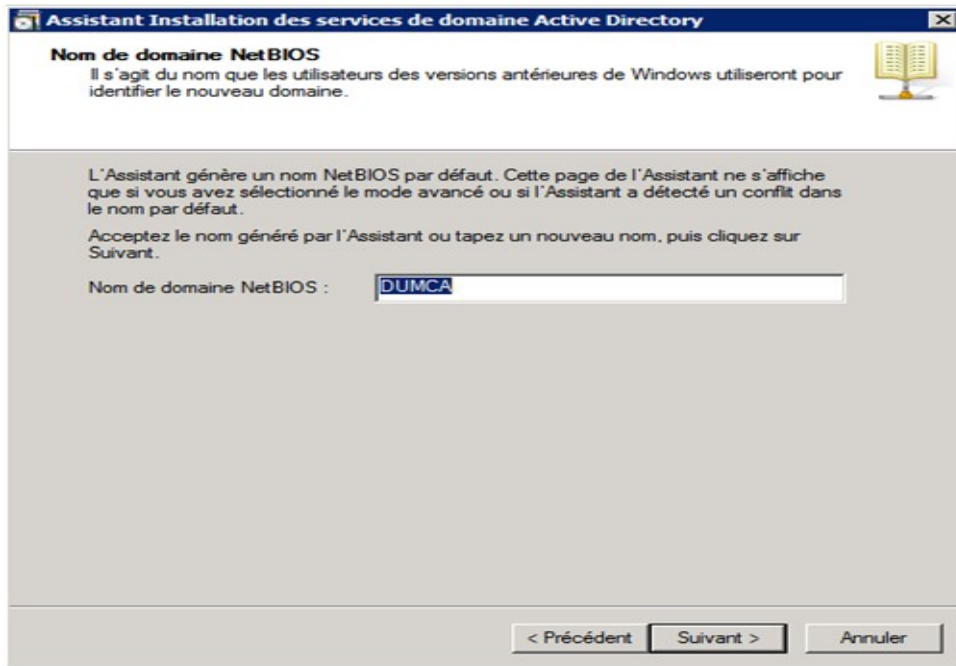
Sélectionnez “Crée un domaine dans une nouvelle forêt”, puis cliquez sur “Suivant”.



Entrez le nom de votre domaine, puis cliquez sur “Suivant”.

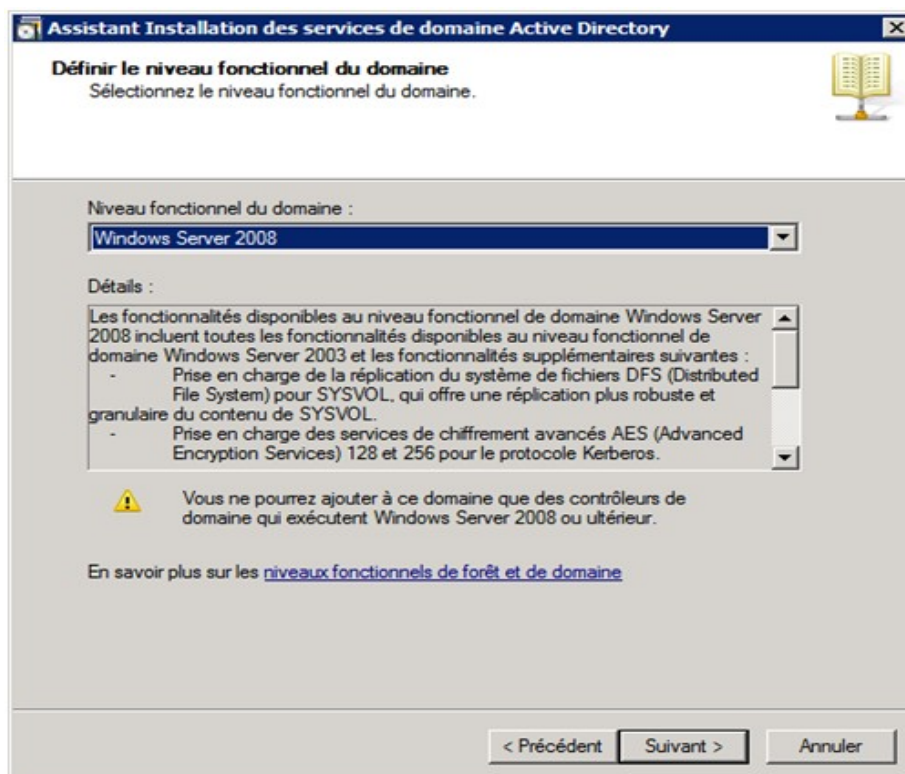


Entrez le nom NETBIOS, puis cliquez sur “Suivant”.

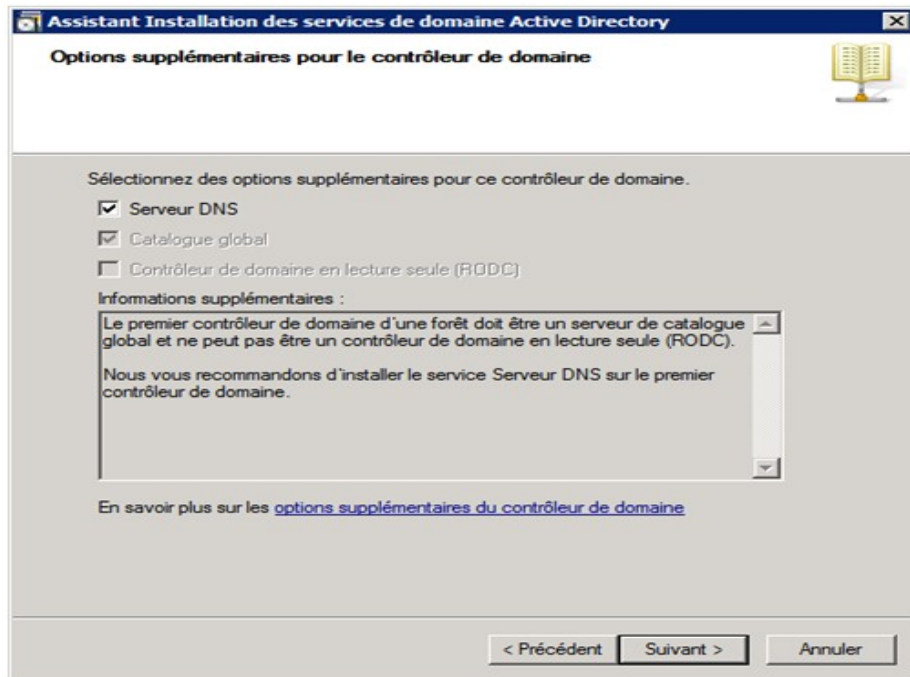


Ensuite vous devez choisir le niveau de fonctionnalité de la forêt. Le plus simple, est d'indiquer le système d'exploitation le plus configuré des serveurs que l'on trouve dans votre forêt. Pour ma part, ayant deux serveurs Windows 2008R2 et un serveur Windows 2008, j'indique un niveau de fonctionnalité : "Windows Server 2008".

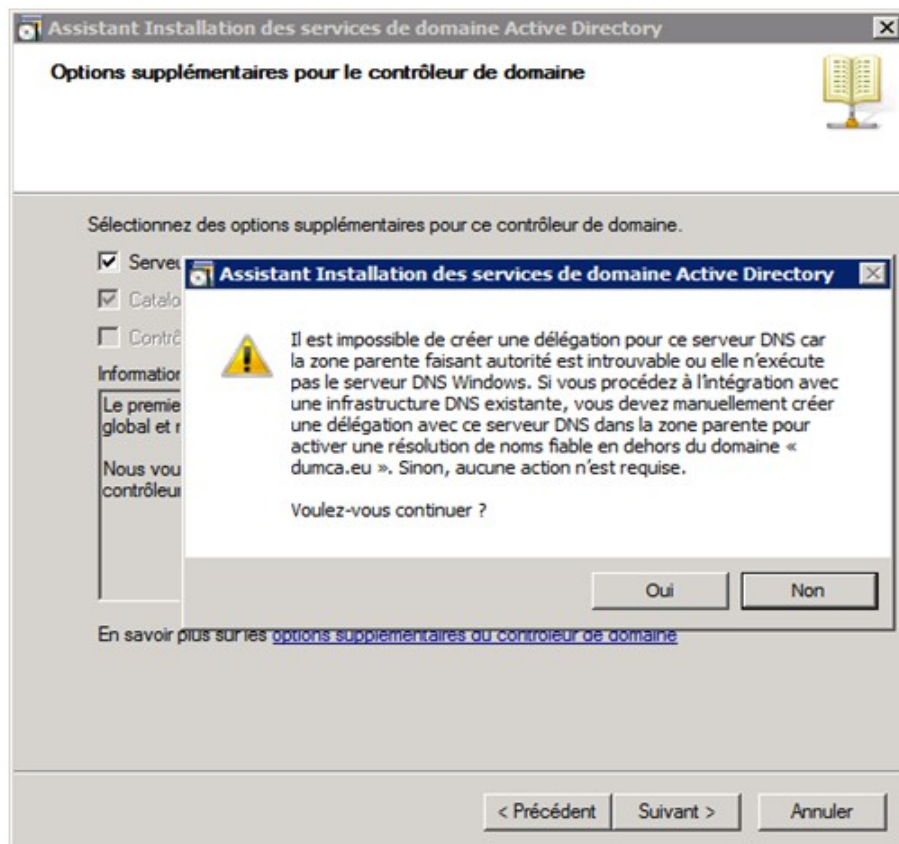
Même question mais concernant le domaine.



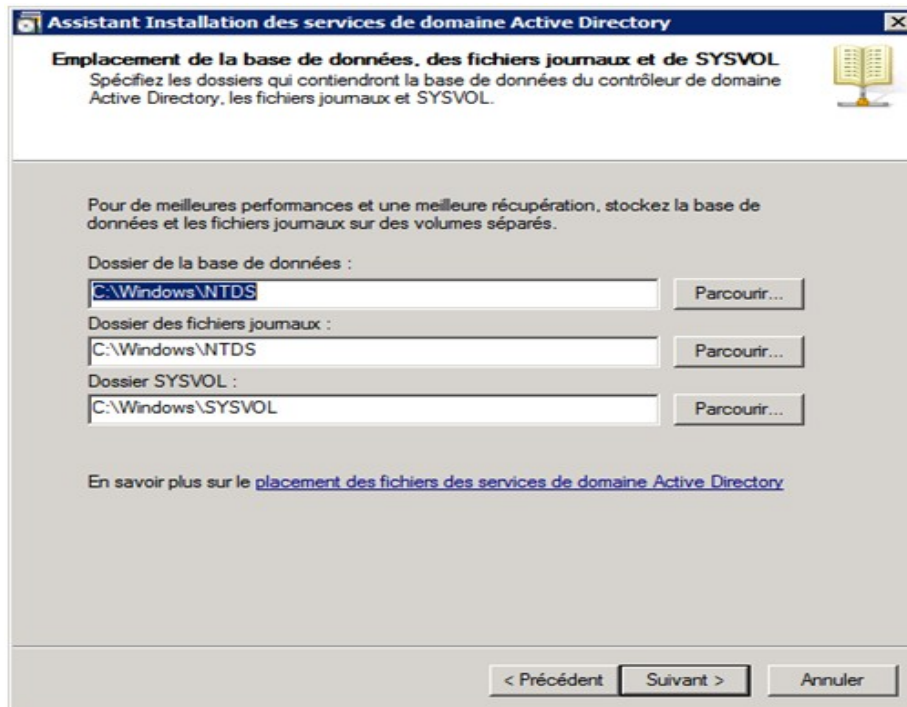
Si vous n'avez pas de Serveur DNS sur votre réseau alors cochez "Serveur DNS".



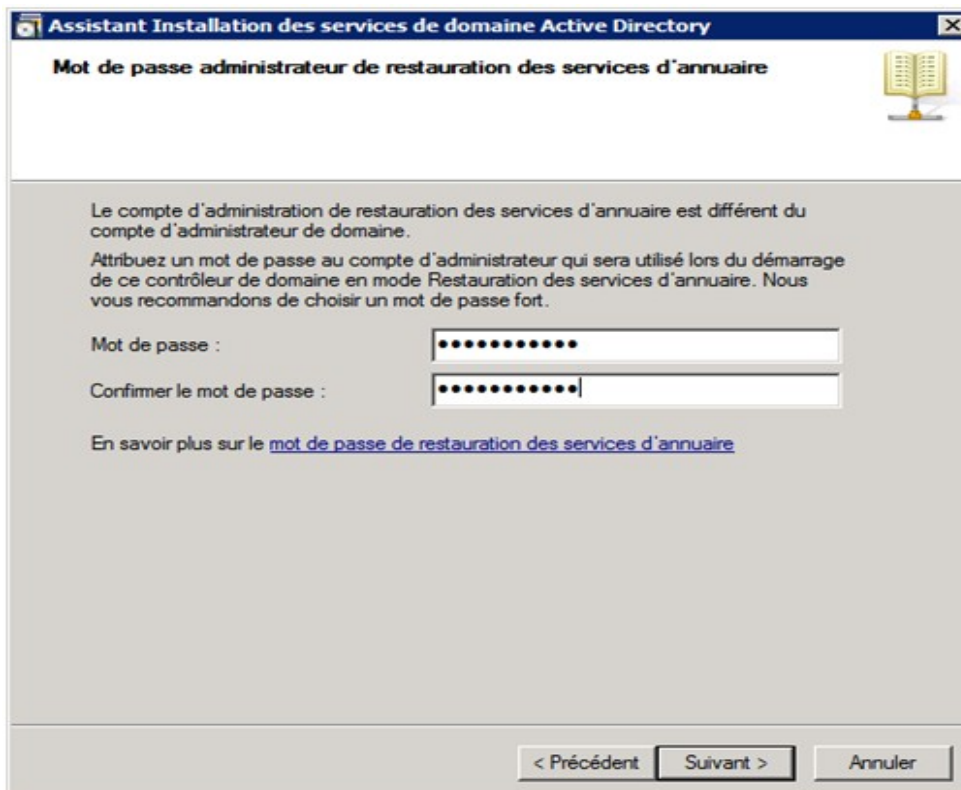
Si vous avez coché l'option, la fenêtre suivante va apparaître cliquez sur "Oui".



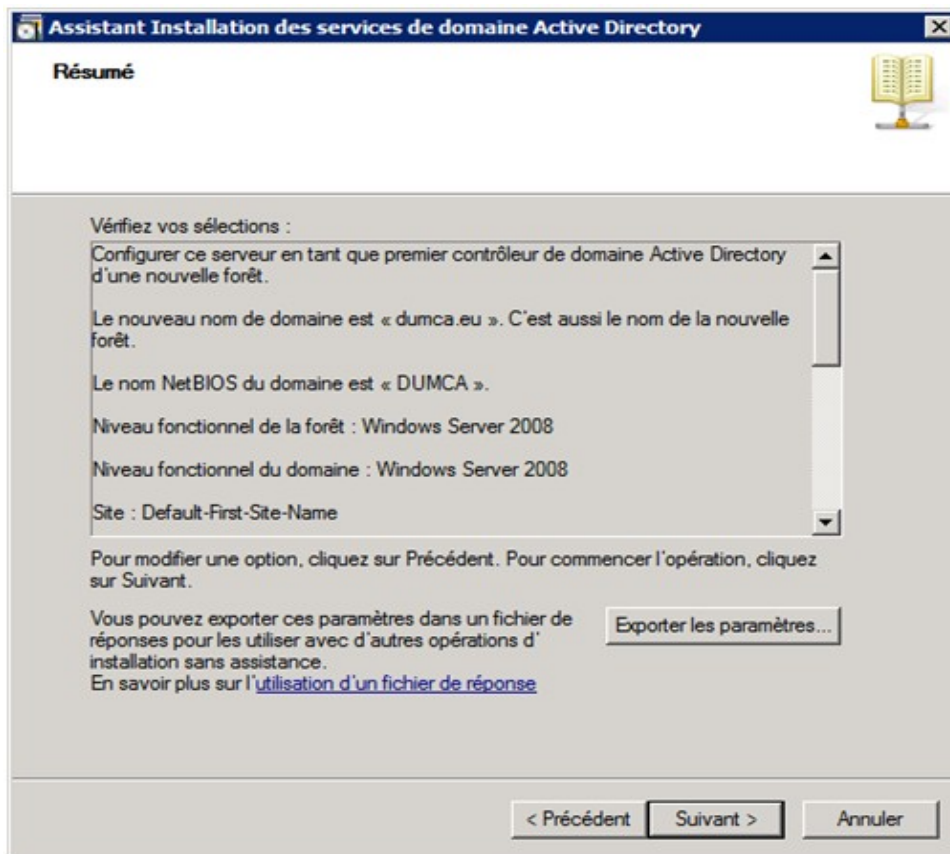
Indiquez les configurations des dossiers où seront stockés les fichiers journaux et les BDD. Pour une installation simple laissez les paramètres par défaut.



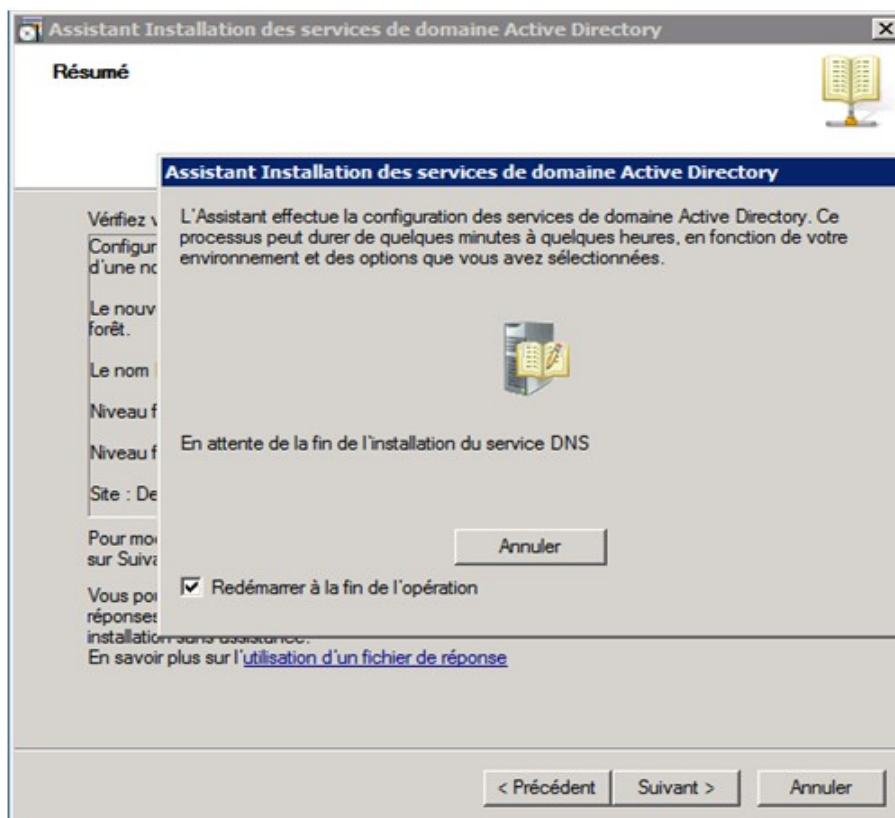
Maintenant l'assistant va vous demander de configurer un mot de passe qui servira en cas de restauration.



Vérifiez les paramètres et cliquez sur "Suivant".



Cochez la case “Redémarrer à la fin de l’opération”, puis patientez pendant la configuration.



V.4.2.2/ Réplication des données des AD (1 et 2) :

En informatique, la **réplication** est un processus de partage d'informations pour assurer la cohérence de données entre plusieurs sources de données redondantes, pour améliorer la fiabilité, la tolérance aux pannes, sauvegarde ou la disponibilité. On parle de *réplication de données* si les mêmes données sont dupliquées sur plusieurs périphériques.

Pour éviter toute surprise du serveur AD, nous avons utilisé la réplication de ce dernier qui est comme suite :

Démarrer --> outils d'administration --> sites et service AD --> ORON/ALGER--> servers --> SRVAD-ALGER/SRVAD-ORAN --> clic droit replication à partir de du domaine sélectionner /réplication sur le domaine sélectionner.

Clic droit sur le domain répliqué maintenant.

En fin, nous utilisons l'invite de commande pour forcer le Knowledge Consistency Checker (KCC) sur chaque contrôleur de domaine ciblé pour recalculer immédiatement la topologie de réplication entrante.

Par défaut, chaque contrôleur de domaine effectue ce calcul toutes les 15 minutes.

Exécutez la commande suivante pour résoudre les erreurs KCC après la suppression de conditions de panne suspectée ou réévaluer si de nouveaux objets de connexion doivent être créés au nom de contrôleurs de domaine ciblé.

Les commandes :

```
repadmin /kcc
```

```
repadmin /syncall
```

V.4.2.3/ Mettre toutes les machines dans le même domaine (AD) :

Dans une architecture centralisée, toutes les machines doivent être reliées au même domaine pour qu'elles puissent partager ou accéder à toutes les ressources de l'entreprise. Pour cela, nous devons les mettre dans le domaine approprié comme suit :

Démarrer --> clic droit sur ordinateur --> propriétés --> Paramètres système avancés --> Nom de l'ordinateur --> Modifier --> allez à la case « Domaine » --> écrire notre domaine et cliquer sur OK.

Une case de sécurité apparaît pour mettre le nom de l'administrateur et le mot de passe. Enfin un démarrage est demandé.

V.4.2.4/ Les cinq rôles d'AD :

Dans un environnement de domaine Windows Server 2003, les contrôleurs de domaine contiennent une réplique de la base de données Active Directory. Ce système de réplication est dit multimaître car, chaque contrôleur de domaine a la possibilité de modifier cette base de données et de transmettre ces modifications aux autres contrôleurs de domaine afin que tous possèdent la même base de données Active Directory.

Les rôles les plus importants du AD sont mentionnés dans le tableau V.1.

Tableau V.1: Les principaux rôles du AD:

FSMO	Emplacement	Rôle
Maître d'attribution des noms de domaine	Unique au sein d'une forêt	Inscription de domaines dans la forêt
Contrôleur de schéma	Unique au sein d'une forêt	Gère la modification du schéma Active Directory
Maître RID	Unique au sein d'un domaine	Distribue des plages RID pour les SIDs
Maître d'infrastructure	Unique au sein d'un domaine	Gère le déplacement des objets
Emulateur CPD	Unique au sein d'un domaine	Garantie une compatibilité avec les anciens systèmes

✓ Transfert des rôles du serveur ADx à Ady :

Les rôles définis au niveau de la forêt sont :

- Contrôleur de schéma.
- Maître d'attribution des noms de domaine.

Les rôles de domaine :

- Contrôleur de domaine principal.
- Maître RID.
- Maître d'infrastructure.

Il est à noter que les transferts de ces rôles se fait par la méthode invite de commande :

I. Présentation :

Transférer des rôles FSMO d'un contrôleur de domaine vers un autre. On peut transférer un seul rôle ou plusieurs (maximum 5). Nous procéderons avec l'utilitaire ntdsutil.exe.

Dans notre cas, nous avons un premier serveur appelé "**AD-ALGER**" et un second serveur appelé "**AD-ORAN**". Le premier serveur est le maître d'opération pour tous les rôles FSMO. Par ailleurs, nous voulons que le second serveur le devienne pour les 5 rôles suscités. Nous allons donc les transférer. Il est à signaler que l'ensemble de ce qui est réalisé dans cette fiche se fait sur le premier serveur c'est à dire celui qui possède les rôles.

II. Exécuter NTDSUTIL :

Pour cela il suffit d'aller dans le menu Démarrer, Exécuter puis de saisir :
« **ntdsutil.exe** ».

III. Obtenir de l'aide :

Cette option est utilisée en cas d'oubli. Il suffit de saisir "?" pour que toutes les commandes disponibles deviennent activées.

```

ntdsutil: ?
?
Authoritative restore - Imprime ces informations d'aide
                        - Restauration faisant autorité de la base
                        de données DIT
Domain management - Préparer la création d'un nouveau domaine
Files - Gère les fichiers de base de données NTDS
Help - Imprime ces informations d'aide
IPDeny List - Gestion de la liste de refus LDAP IP
LDAP policies - Gérer les stratégies de protocole LDAP
Metadata cleanup - Nettoyer les objets des serveurs désaffectés
Popups %s - Activez ou désactivez les messages avec "on" ou
"off"
Quit - Quitter l'utilitaire
Roles - Gérer les jetons du propriétaire du rôle NTDS
Security account management - Gérer la base de données de comptes de sécurité
- Dupliquer le nettoyage SID
Semantic database analysis - Vérificateur sémantique

```

IV. Mode «fsmo maintenance» :

Pour passer en mode fsmo maintenance il faut saisir la commande suivante :

« Roles ».

V. Voir les commandes disponibles :

Même principe qu'à l'étape précédente, il suffit de saisir un « ? » pour afficher les commandes disponibles.

```

ntdsutil: roles
fsmo maintenance: ?
?
Connections - Imprime ces informations d'aide
              - Connexion à un contrôleur de domaine spécifique
Help - Imprime ces informations d'aide
Quit - Revenir au menu précédent
Seize domain naming master - Remplace le rôle de domaine sur le serveur conn
ecté
Seize infrastructure master - Remplace le rôle d'infrastructure sur le serveu
r connecté
Seize PDC - Remplace le rôle PDC sur le serveur connecté
Seize RID master - Remplace le rôle RID sur le serveur connecté
Seize schema master - Remplace le rôle de schéma sur le serveur conne
cté
Select operation target - Sélection des sites, serveurs, domaines, rôles
et contextes de nommage
Transfer domain naming master - Faire du serveur connecté le maître de nommage
de domaine
Transfer infrastructure master - Faire du serveur connecté le maître d'infrastr
ucture
Transfer PDC - Désigne le serveur connecté comme PDC
Transfer RID master - Faire du serveur connecté le maître RID
Transfer schema master - Faire du serveur connecté le maître de schéma

```

VI. Connexion au second serveur :

Il faut établir une connexion avec le serveur auquel nous voulons transférer un ou des rôles. Pour cela, dans le mode «fsmo maintenance », tapez la commande : « Connections ».

Nous sommes désormais en mode « **server connections** ». Pour établir la connexion avec le serveur, tapez la commande :

« **Connect to server nom_serveur** ».

« **Connect to server AD-ALGER** » (pour notre cas)

Patiencez le temps que la connexion s'établisse.

VII. Retourner au mode fsmo maintenance :

Pour quitter le mode connections et retourner au mode fsmo maintenance, tapez la commande : « **q** ».

VIII. Transfert du rôle de Maître RID :

« **transfer RID master** ».

Une boîte de dialogue apparaît pour qu'on confirme vouloir transférer le rôle sur le serveur avec lequel on avait établie une connexion. Elle apparaîtra pour le transfert de chacun des rôles.

IX. Transfert du rôle de contrôleur de schéma :

Pour cela, saisissez cette commande afin de transférer le rôle :

« **transfer schema master** ».

X. Transfert du rôle de Maître d'infrastructure :

Sur le même principe que la commande précédente, saisissez celle-ci :

« **transfer infrastructure master** ».

XI. Transfert du rôle de Maître d'attribution des noms de domaine :

Dans ce cas, la commande suivante est utilisée : « **transfer domain naming master** ».

Si la commande ci-dessus ne fonctionne pas, utilisez celle-ci :

« **transfer naming master** ».

XII. Transfert du rôle d'Émulateur PDC:

Pour effectuer ce transfert, la commande « **transfer pdc** » est recommandée.

Remarque : Il est à signaler qu'à chaque fois que l'on transfère un rôle, NTDSUTIL mentionne le résumé sur l'appartenance des rôles. Nous devons donc vérifier si le rôle a bien été transféré.

XIII. Quittez NTDSUTIL:

Pour quitter correctement le programme, saisissez “**q**” dans le mode fsmo maintenance sur l'invite de commande ntdsutil.

Enfin, on peut vérifier si les rôles sont bien transférés grâce à la commande suivante :
« **NETDOM QUERY /Domain:<votre-domaine> FSMO** »

V.3.3/ Serveur TMG :

V.3.3.1/ Présentation du TMG :

Le TMG (Threat Management Gateway) est une passerelle Web qui permet aux entreprises d'utiliser Internet de façon sécurisée et efficace, sans crainte des logiciels malveillants ou autres menaces. Pour mieux bloquer les menaces récentes en provenance du Web, ce produit multiplie les couches de protection (filtrage d'URL, recherche de logiciels malveillants et prévention des intrusions) et les met à jour en permanence. Il protège les utilisateurs contre les menaces du Web en intégrant plusieurs couches de sécurité dans une solution simple à administrer. Placé comme passerelle dans le réseau de l'entreprise, il inspecte le trafic Web aux niveaux réseau, application et contenu pour assurer une sécurité Web cohérente. De plus, il améliore les performances du firewall en répartissant la charge de certaines fonctions sur plusieurs processeurs, comme l'inspection des logiciels malveillants.

[24-25]

V.3.3.2/ Les composants du TMG :

Le TMG se compose de quatre composants :

✓ **Le serveur Forefront TMG :**

Il fournit plusieurs technologies d'inspection, des firewalls applicatifs et réseau, une prévention d'intrusion et un filtrage de logiciels malveillants. Il se connecte à Forefront TMG Web Protection Service pour le filtrage des URL et les mises à jour des signatures des logiciels malveillants.

✓ **Forefront TMG Web Protection Service :**

Il assure les mises à jour des signatures et le filtrage des URL Internet en temps réel, il peut aussi servir à surveiller ou à bloquer l'usage fait par les employés du Web.

✓ **La console d'administration :**

Il permet une gestion locale et à distance des serveurs.

✓ **Un serveur d'administration :**

Inclus dans Forefront TMG Enterprise Edition, il permet la création de stratégies à l'échelle de toute l'entreprise et les applique à des ensembles de serveurs TMG.

V.3.3.3/ Les principaux avantages et fonctionnalités de la TMG :

Forefront TMG fournit aux entreprises plusieurs avantages en matière de connectivité à Internet :

a. Protection complète



Figure V.29 : Protection complète de la TMG.

Le filtrage des URL dans TMG Web Protection Service consolide les données en provenance de plusieurs fournisseurs.

TMG bloque efficacement l'accès aux sites malveillants : Il utilise des données en provenance de différents fournisseurs de filtres d'URL, et des technologies contre les logiciels malveillants et l'usurpation d'identité qui équipent déjà Internet Explorer 8. Le filtrage des sites Web permet aussi de bloquer l'accès aux sites inappropriés selon les choix d'entreprise.

Empêche l'exploitation de vulnérabilités : Il empêche les intrusions qui exploiteraient des vulnérabilités du navigateur ou de ses modules additionnels.

Détecte les logiciels malveillants du Web : Il assure une détection précise grâce à un moteur d'analyse qui combine des signatures génériques pour anticiper la diffusion de nouvelles variantes n'ayant pas de signatures spécifiques.

b. Interface de sécurité Web unifiée :

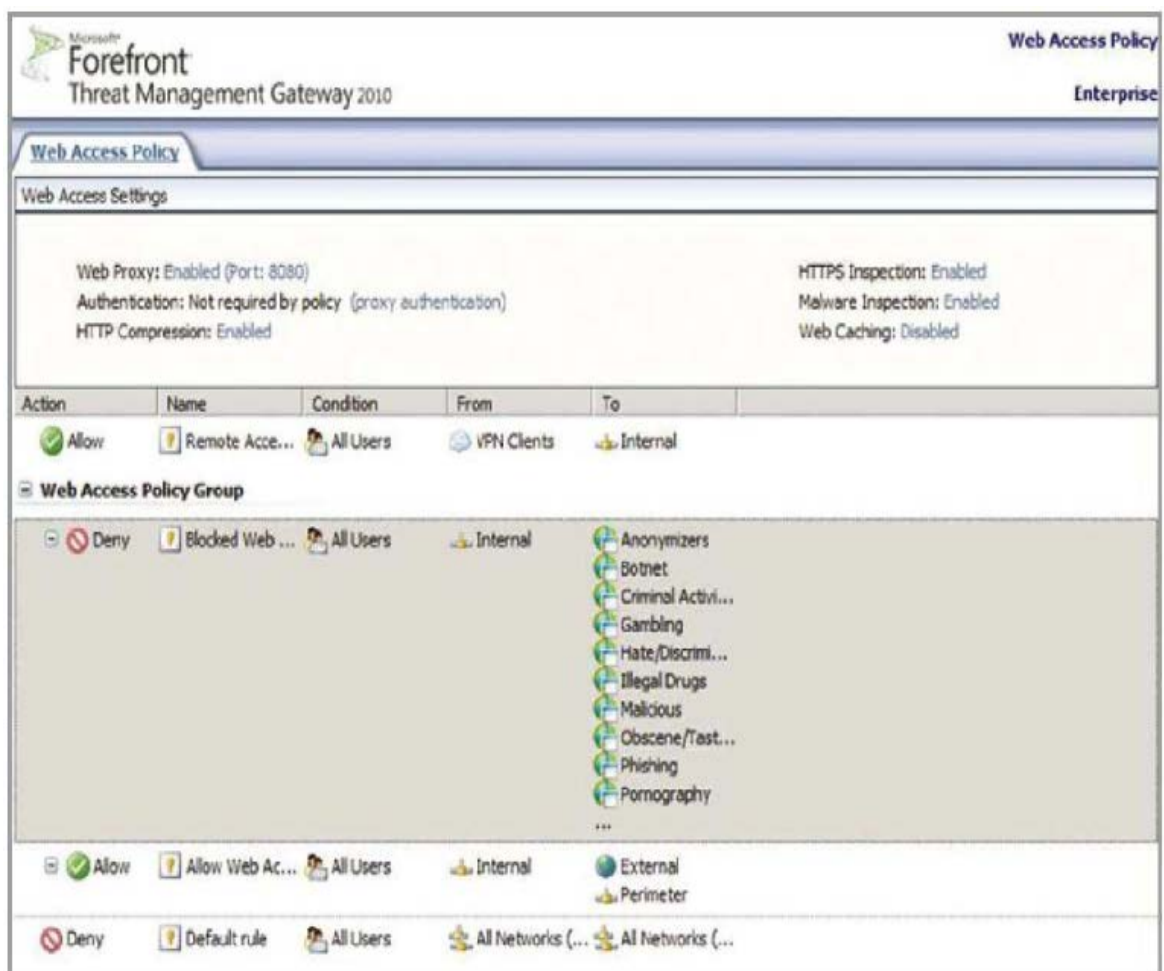


Figure V.30: Protection du réseau.

La console d'administration Forefront TMG simplifie la création de stratégies et assure les principales fonctions de protection du réseau : Il reprend les technologies de protection du réseau de Microsoft ISA Server 2006, la version précédente de Forefront TMG. Cela permet de déployer un firewall de périmètre et une passerelle sécurisée pour des applications comme Microsoft Exchange Server.

Inspecte le trafic Web chiffré : Il examine le trafic Web chiffré SSL, ce que ne fait pas un firewall. Dans ces sessions chiffrées, Forefront TMG peut détecter un logiciel malveillant et contrôler l'accès à des sites interdits par l'entreprise.

c. Sécurité intégrée :

Une source unique pour la sécurité Web : Il combine sur un seul serveur le filtrage des URL, des services de réputation, le blocage des intrusions, le proxy Web, des firewalls applicatifs et réseau, la détection de logiciels malveillants et l'inspection HTTP/HTTPS.

Réduit les coûts : Il assure un rôle de cache pour améliorer la rapidité de navigation et réduire les coûts en bande passante. La possibilité de déployer Forefront TMG comme une appliance virtuelle permet d'économiser sur le matériel.

Exploite les investissements d'infrastructure existants : Il simplifie l'authentification et l'application des stratégies en s'intégrant dans Active Directory. Par exemple, Forefront TMG simplifie l'inspection HTTPS en distribuant son certificat via Active Directory. Il utilise aussi l'infrastructure Windows Update pour diffuser rapidement de nouvelles protections à tous les serveurs Forefront TMG.

d. Administration simplifiée :

Centralise la gestion sur une seule console simple d'emploi : Il permet aux administrateurs de créer et de gérer toutes les fonctions de sécurité Web à partir d'une seule console dans des environnements distribués.

Fournit des rapports complets : Il génère rapidement des rapports de sécurité qui peuvent être adaptés pour répondre à des besoins spécifiques de l'entreprise.

✓ **TMG Client :** Le TMG client est un outil qui s'installe dans la machine client pour qu'il contacte le TMG serveur.

✓ **TMG Serveur :** Le TMG serveur est un outil de gestion des utilisateurs.

V.4.4/ Serveur sauvegarde (symantec backup exe) : Backup Exec™ 15 offre des fonctions de sauvegarde et de restauration puissantes, flexibles et conviviales pour l'ensemble de notre infrastructure quelle que soit la plateforme : virtuelle, physique ou cloud. L'intégration avancée avec les versions les plus récentes de VMware et Hyper-V assure une restauration rapide et efficace. La récupération se fait en quelques minutes, y compris des machines virtuelles, des applications, des bases de données, des fichiers, des dossiers et des objets d'applications granulaires.

V.4.5/ Serveur de messagerie (exchange) :

Dans les sociétés, les utilisateurs communiquent avec des messages, donc un serveur mail est nécessaire, pour notre projet on a choisi l'échange qui est un outil de communication et de collaboration pour les entreprises, basé sur la messagerie électronique (outlook) qui va leur offrir un environnement de communication.

AD et l'échange travaillent en synchronisation, c-à-d l'échange peut importer des données des utilisateurs du serveur AD.

- Les pré-requis d'échange

Dans le Gestionnaire de serveur il faut ajouter les fonctionnalités suivantes pour le fonctionnement d'échange:

- Net framework 3.5.1 features.
- Net framework 3.5.1.
- RPC over HTTP Proxy.
- WCF Activation.
- HTTP Activation.
- remote server administration tools.
- roles administration tools.
- AD DS and AD LDS Tools.
- AD DS snap-tra and command-line tools.

Mettre les services suivants en mode automatique et les démarrer :

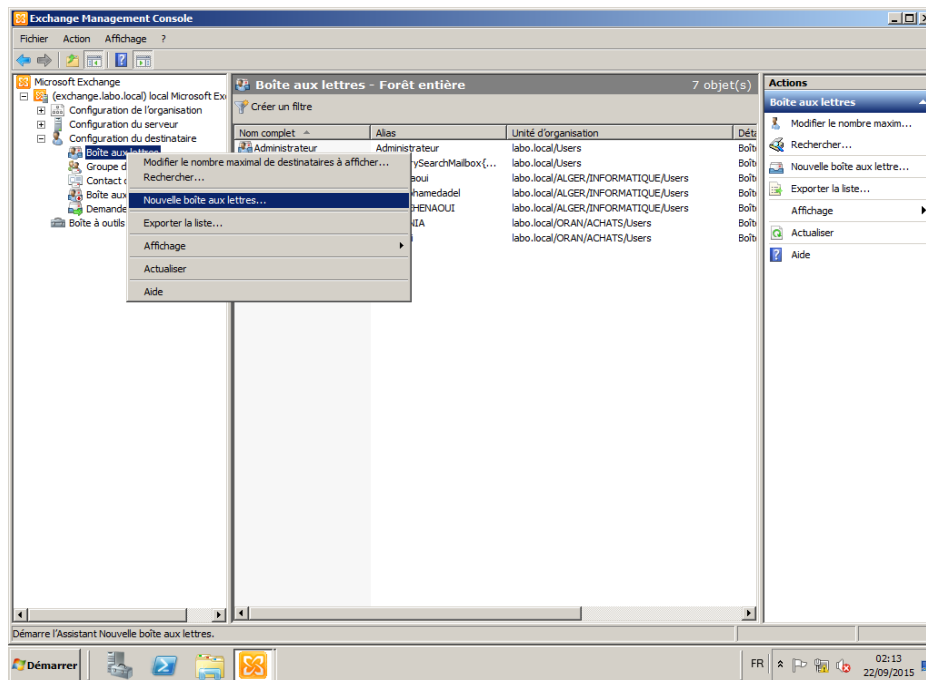
- Microsoft Exchange IMAP.
- Microsoft Exchange POP3.
- Service d'accès client RPC Microsoft Exchange.
- Service de partage de ports Net.TCP
- Topologie Active Directory Microsoft Exchange.

Après avoir installé l'échange et mettre les services nécessaires en mode automatique on entame la méthode d'utilisation.

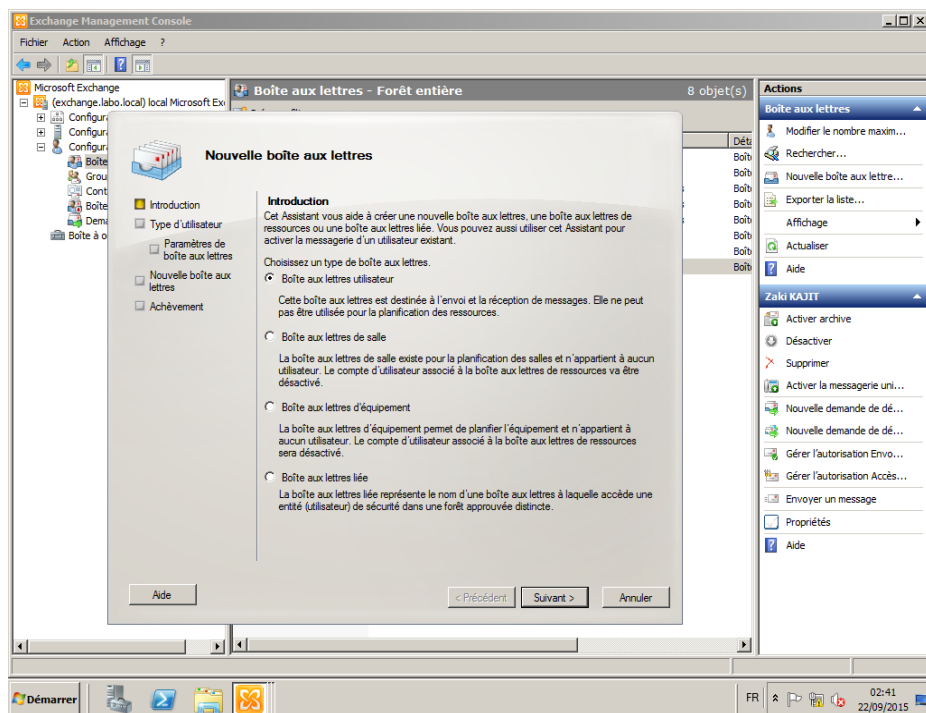
V.4.5.1/ L'utilisation d'échange :

Pour créer des utilisateurs dans l'échange on procède comme suite :

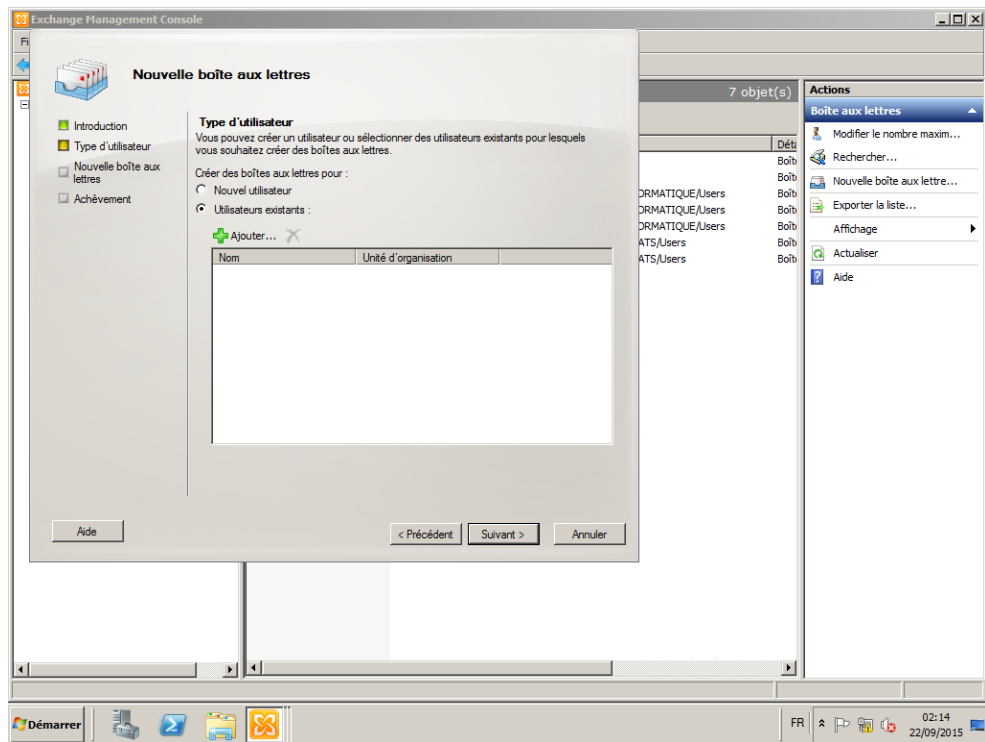
- Création mail de l'utilisateur sur l'échange (boîte aux lettres).



Nouvelle boîte aux lettres

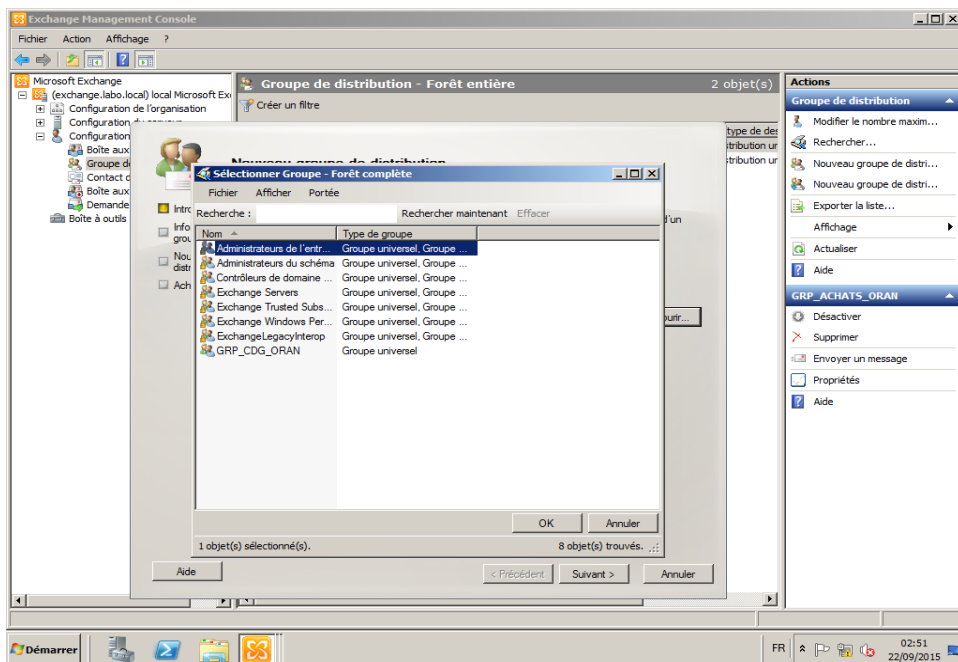


Boîte aux lettres utilisateur

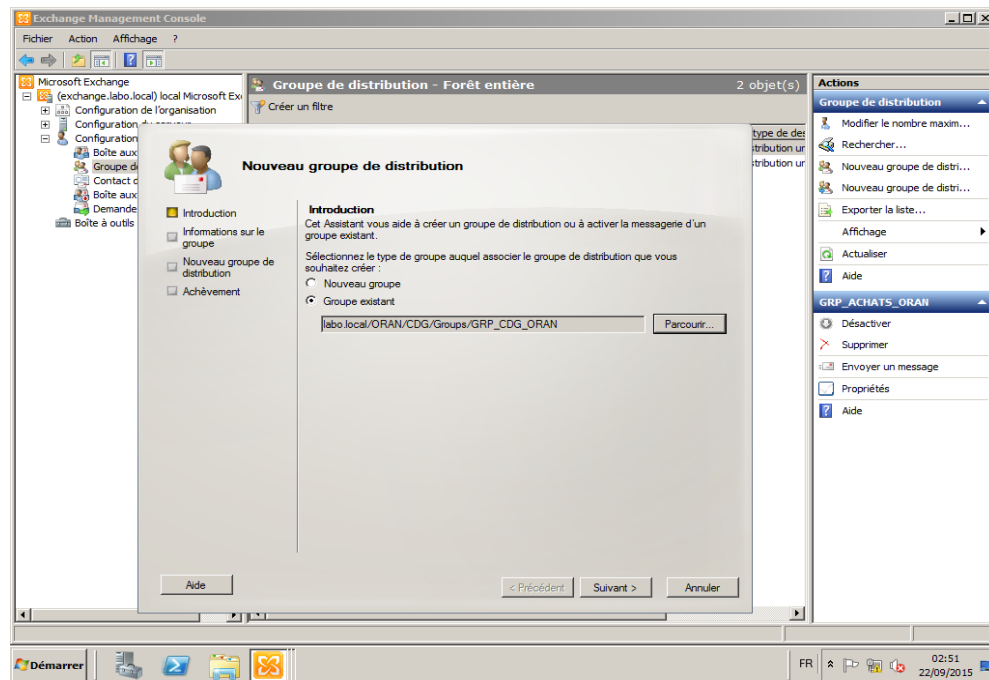


Utilisateur existant (il va l'importer directement d'AD) --> Ajouter et choisir le nom

- Groupe de distribution --> nouveau groupe distribution



**Groupe existant
Choisir le GRP_ CDG_ ORAN**



- Création utilisateur AD (groups / users).
- Aller a active directory --> clic droit sur le groupe (GRP_INFORMATIQUE).
- > etude de groupe (Universelle) --> Type de groupe (Distribution).

V.4.5.2/ Création des groupe :

Pour envoyer des messages à des groupes d'utilisateurs, On peut créer les groupes dans AD et mettre les utilisateurs des services dans les groupes appropriés.

V.4.6/ Serveur DHCP :

✓ **Configuration du serveur :** Un serveur DHCP, en plus de fournir la configuration IP "de base" (Adresse et masque), peut aussi transmettre un nombre plus ou moins grand de paramètres supplémentaires. Nous aurons donc au moins deux choses à configurer :

- La réserve d'adresses dont le serveur pourra disposer pour les attribuer aux clients.
- les paramètres optionnels à leur communiquer dans la foulée, comme l'adresse d'un DNS et de la passerelle par défaut. Dans le cas d'un réseau domestique; ce sera suffisant, mais il y a beaucoup d'autres options, plus ou moins spécifiques aux divers systèmes d'exploitation.

Nous avons vu qu'un seul serveur DHCP pouvait être utilisé pour plusieurs réseaux logiques interconnectés, pourvu que les interconnexions disposent d'un agent de relais DHCP. Dans un tel cas, le serveur DHCP devra disposer d'au moins une étendue d'adresses IP par réseau logique dont il aura la charge.

En ce qui concerne les options, nous disposons d'une architecture hiérarchique :

- Nous pouvons définir des options globales, qui seront les mêmes pour tous les clients du DHCP, tous sous réseaux confondus,
- nous pouvons définir également des options propres à chaque sous réseau, celles-ci écrasent les options globales, en cas de conflit.
- Si l'on veut aller encore plus loin, sachez que DHCPd peut créer des groupes distincts de machines dans un même sous réseau et même gérer des clients de façon indépendante.

Client DHCP :

✓ Configuration des clients :

Aller dans la configuration TCP/IP, enlever tout ce qu'il y a concernant l'IP, le masque de sous réseau, DNS, passerelle et juste dire que vous voulez une configuration dynamique (DHCP). Relancez vos services réseaux, la méthode la plus simple et la plus bestiale étant le "reboot", et voilà. Une fois le système remonté, vous devez avoir hérité d'une configuration automatique.

Commandes `ipconfig` permet également :

- ✓ De réilier le bail : `ipconfig /release`.
- ✓ De renouveler le bail : `ipconfig /renew`.

V.4.7/ Serveur DNS :

Le DNS est un protocole qui permet d'associer un nom de domaine (ex : `www.clashinfo.com`) à une adresse IP, ce qui évite aux utilisateurs d'entrer une adresse IP dans la barre de leur navigateur, `www.clashinfo.com` étant tout de même bien plus facile à retenir que `193.19.217.38` !

DNS (Domain Name System, système de noms de domaine) est un système de noms pour les ordinateurs et les services réseau organisé selon une hiérarchie de domaines. Le système DNS est utilisé dans les réseaux TCP/IP tels qu'Internet pour localiser des ordinateurs et des services à l'aide de noms conviviaux. Lorsqu'un utilisateur entre un nom DNS dans une application, les services DNS peuvent résoudre ce nom en une autre information qui lui est associée, par exemple une adresse IP.

La plupart des utilisateurs préfèrent en effet un nom convivial comme *exemple.microsoft.com* pour accéder à un ordinateur tel qu'un serveur de messagerie ou un serveur Web dans un réseau. Un nom convivial est plus facile à retenir. Cependant, les ordinateurs utilisent des adresses numériques pour communiquer sur un réseau. Pour faciliter

l'utilisation des ressources réseau, des systèmes de noms comme DNS fournissent une méthode qui établit la correspondance entre le nom convivial d'un ordinateur ou d'un service et son adresse numérique.

L'illustration suivante représente une utilisation élémentaire de DNS qui consiste à trouver l'adresse IP d'un ordinateur à partir de son nom.

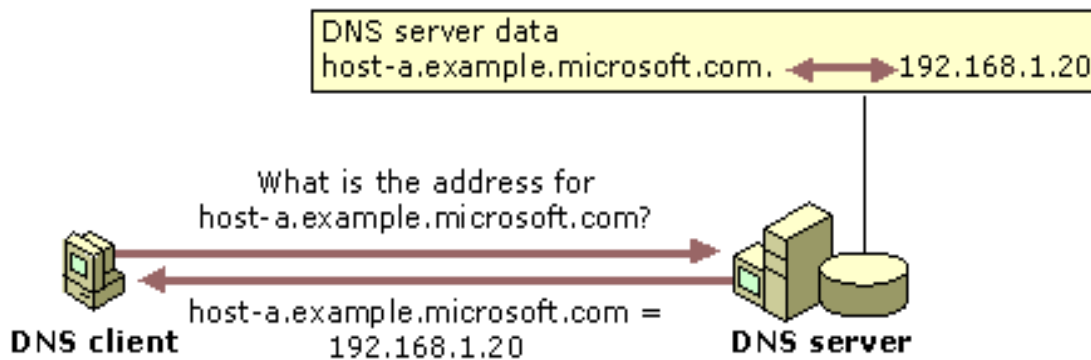
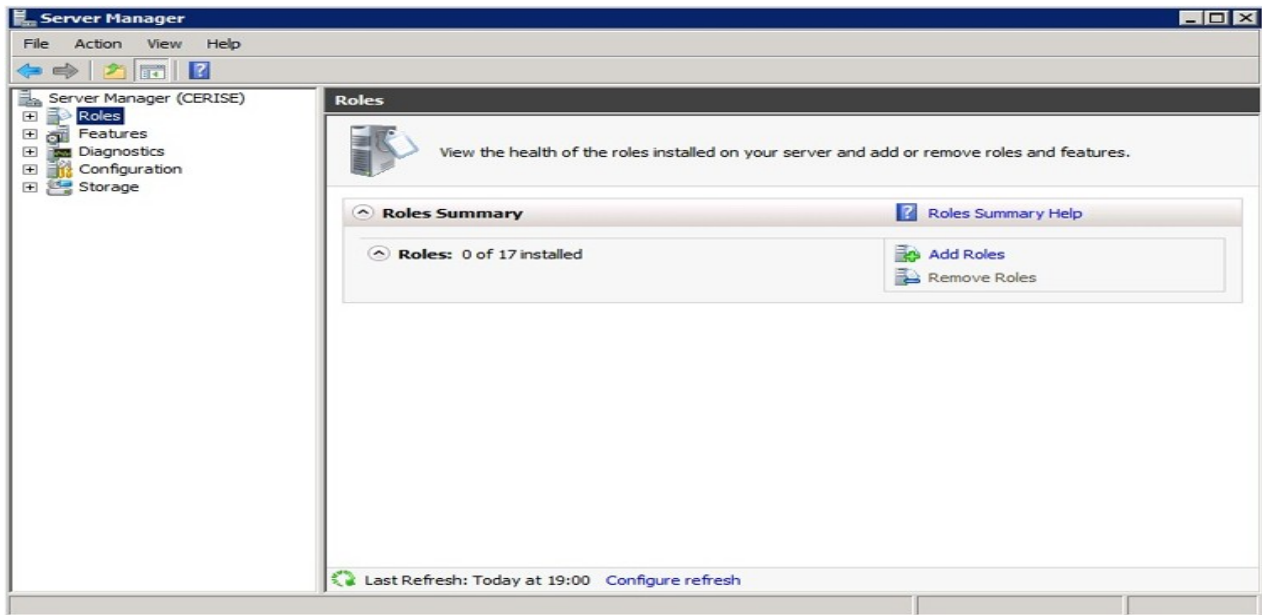


Figure V.31: utilisation de DNS pour trouver l'adresse IP d'un ordinateur à partir de son nom.

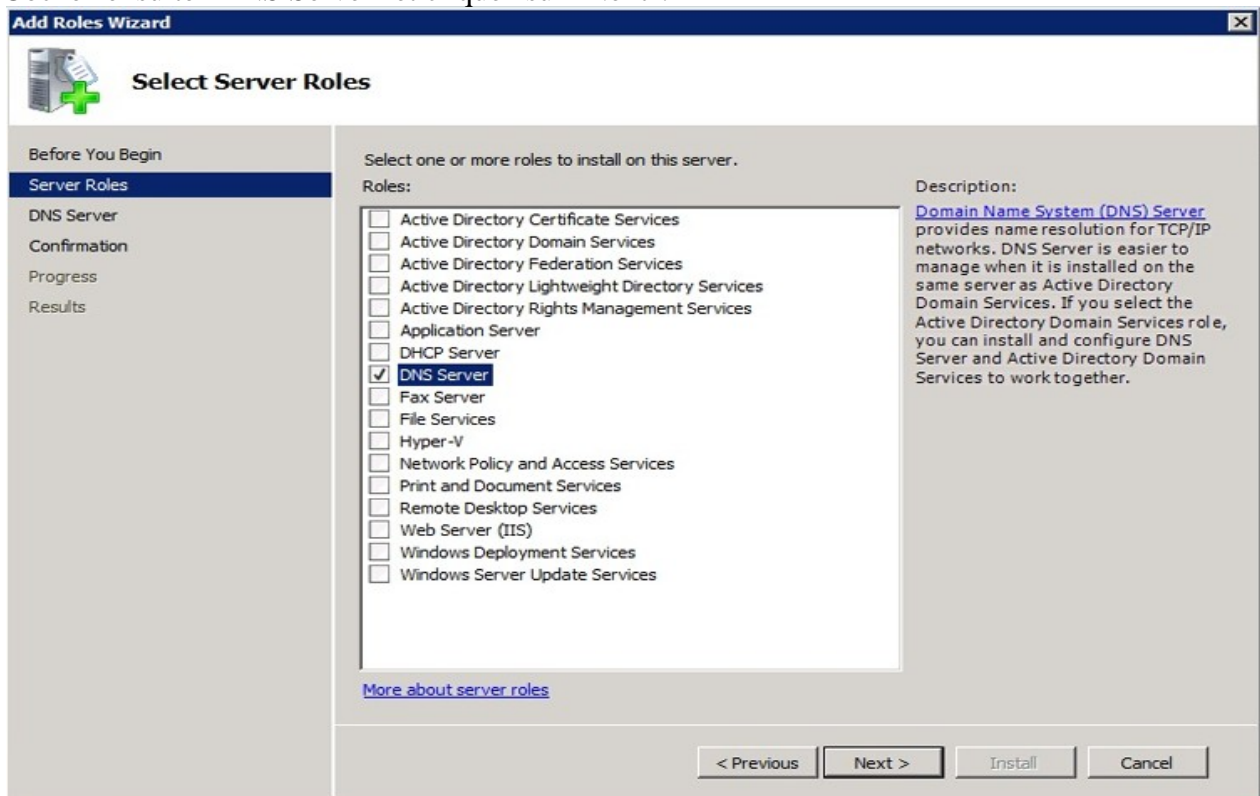
Dans cet exemple, un ordinateur client interroge un serveur DNS pour lui demander l'adresse IP d'un troisième ordinateur configuré pour utiliser le nom de domaine DNS *hôte-a.exemple.microsoft.com*. Le serveur DNS étant en mesure de répondre à cette requête en interrogeant sa base de données locale, il renvoie une réponse qui fournit l'information demandée, c'est-à-dire un enregistrement de ressource A (adresse d'hôte) contenant l'adresse IP correspondant à *hôte-a.exemple.microsoft.com*.

Cet exemple illustre une requête DNS simple entre un client unique et un serveur DNS. En pratique, les requêtes DNS sont souvent plus complexes que celle-ci et comprennent des étapes supplémentaires.

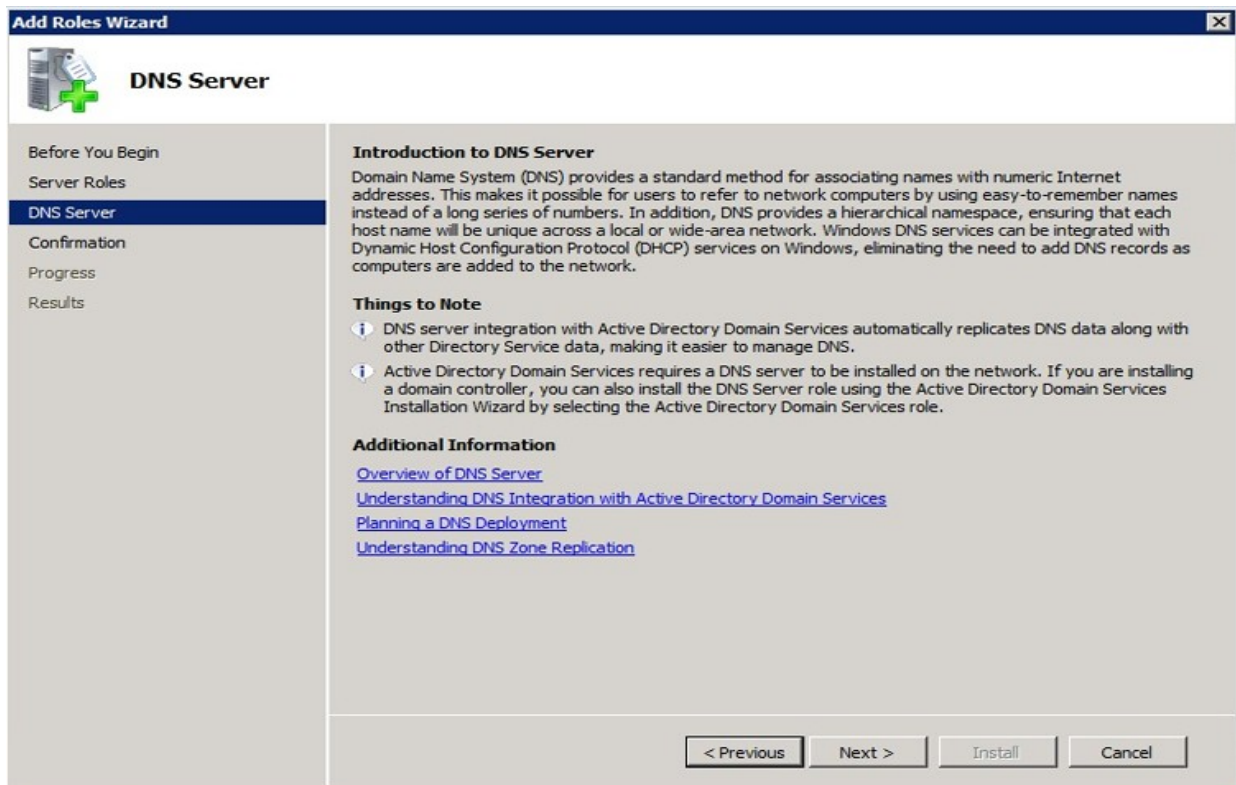
Installation et configuration d'un serveur DNS :



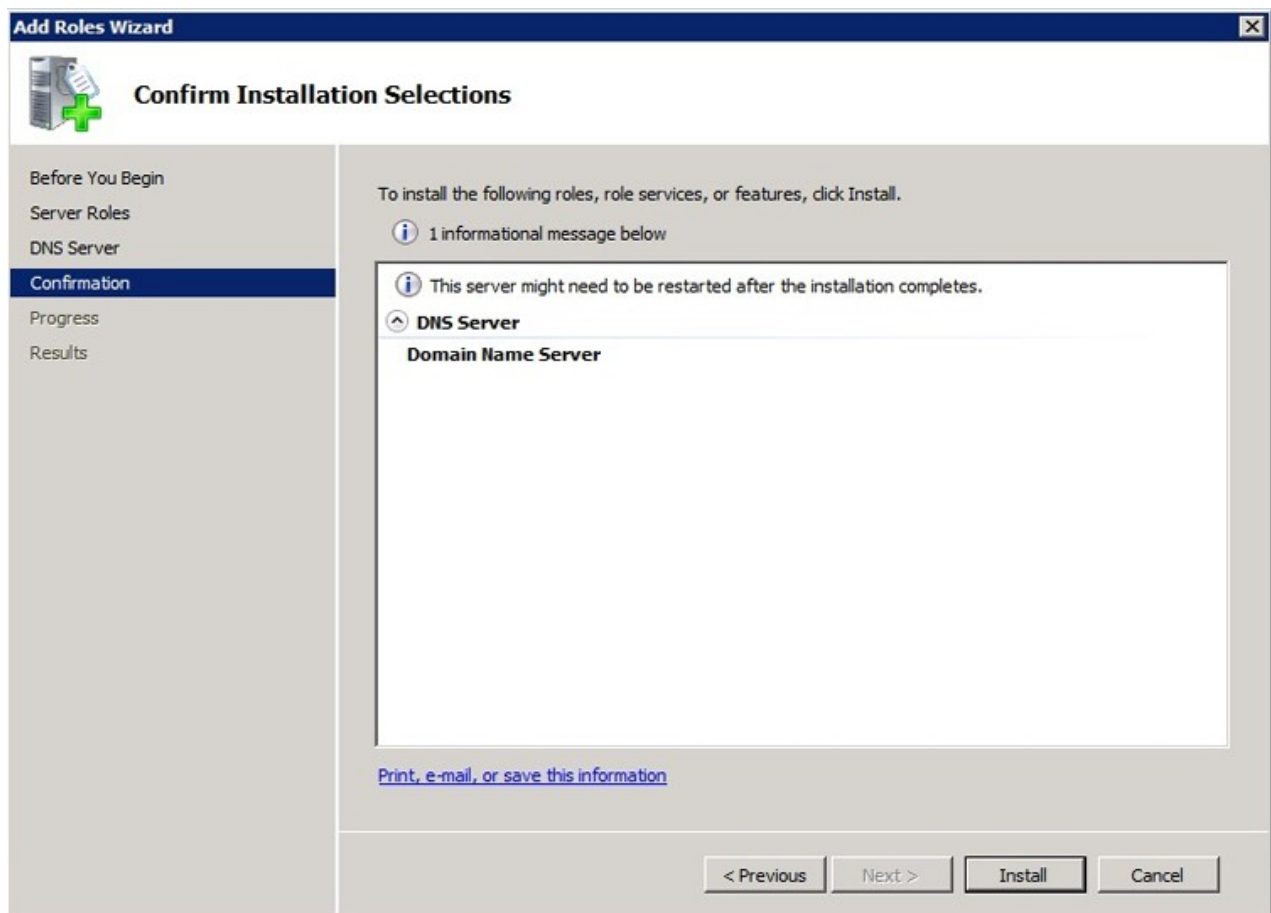
Cochez ensuite "DNS Server" et cliquez sur "Next".



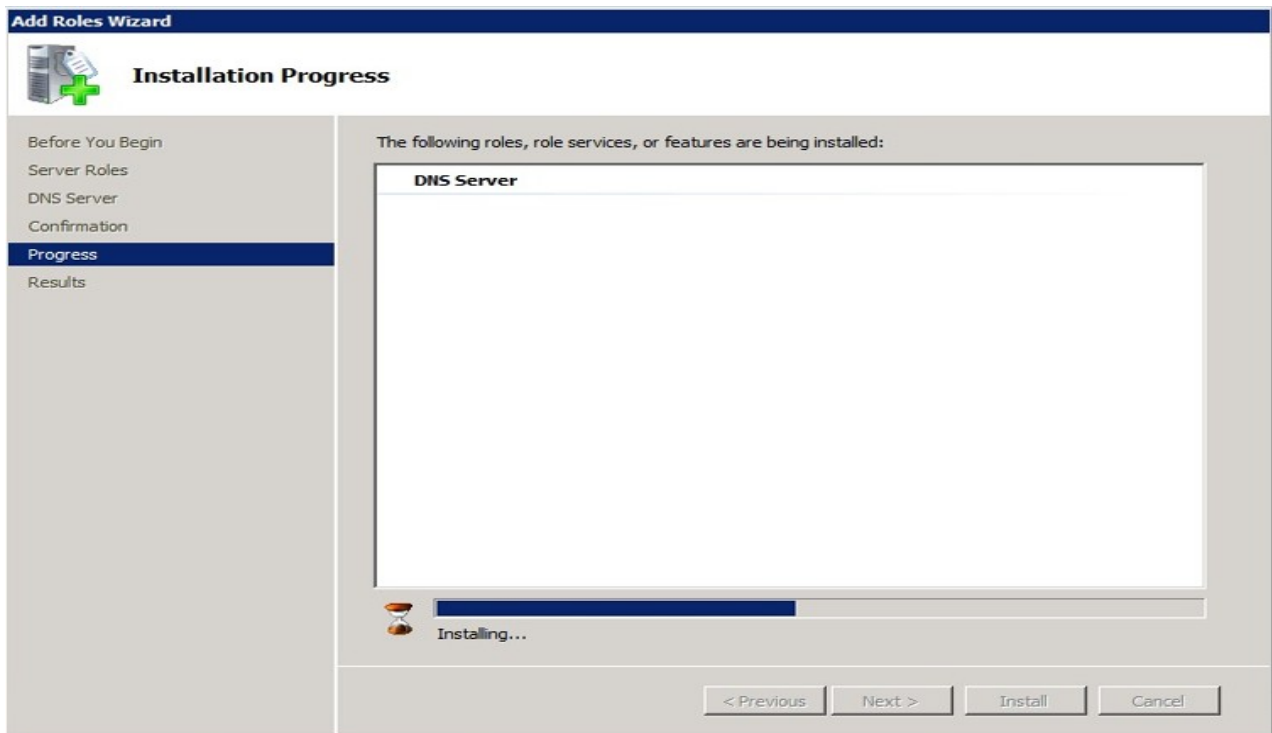
Cliquez sur "Next".



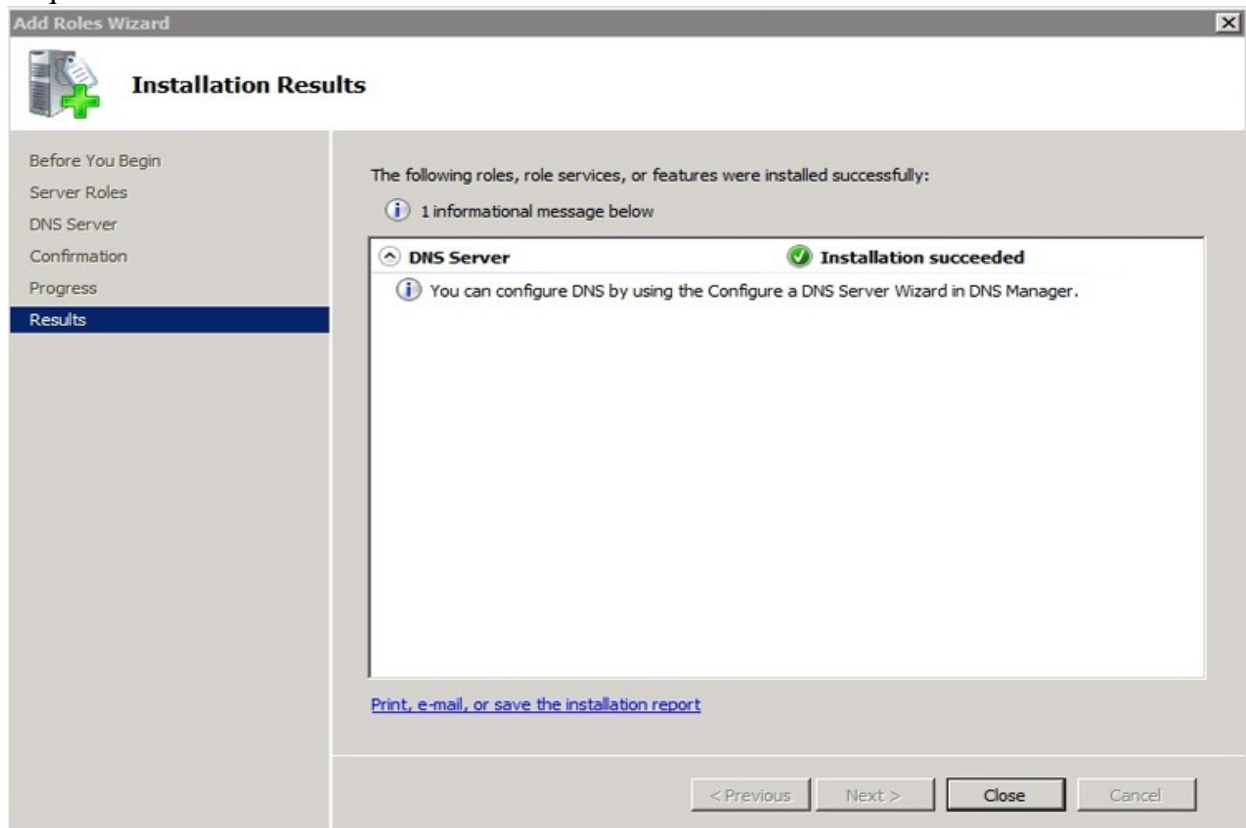
Cliquez sur "Install".



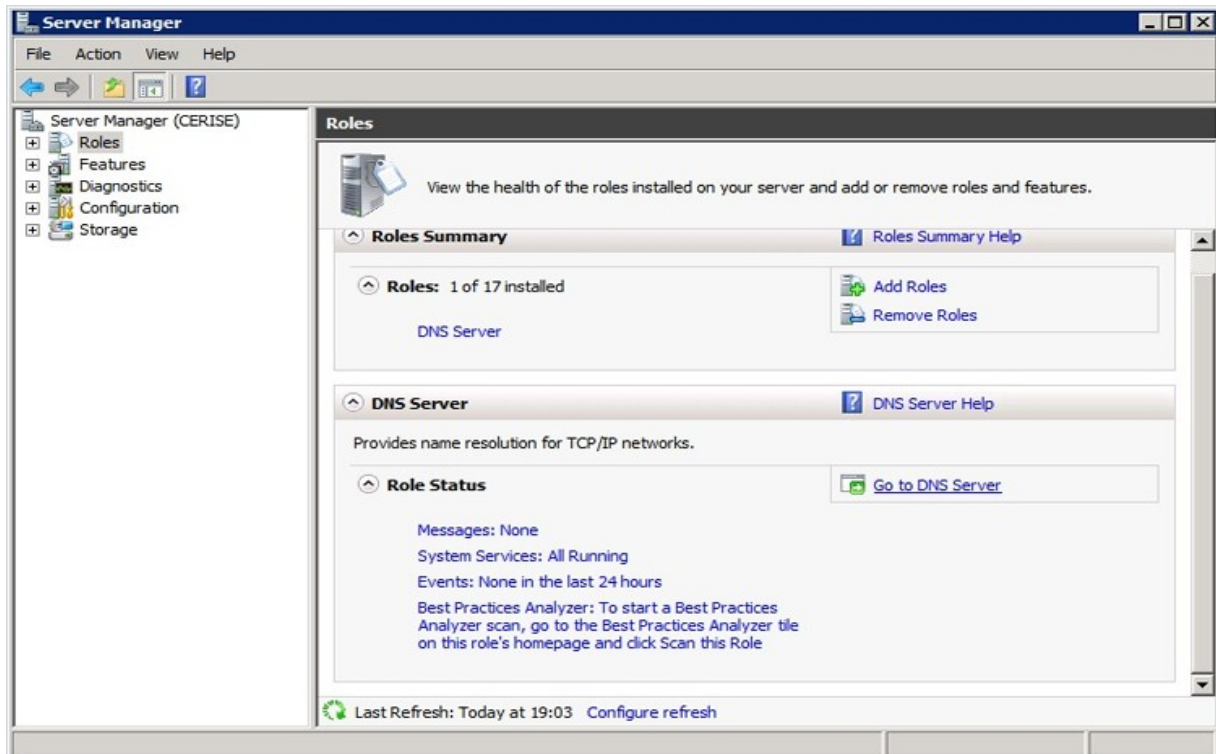
Patientez pendant l'installation.



Cliquez sur "Close".

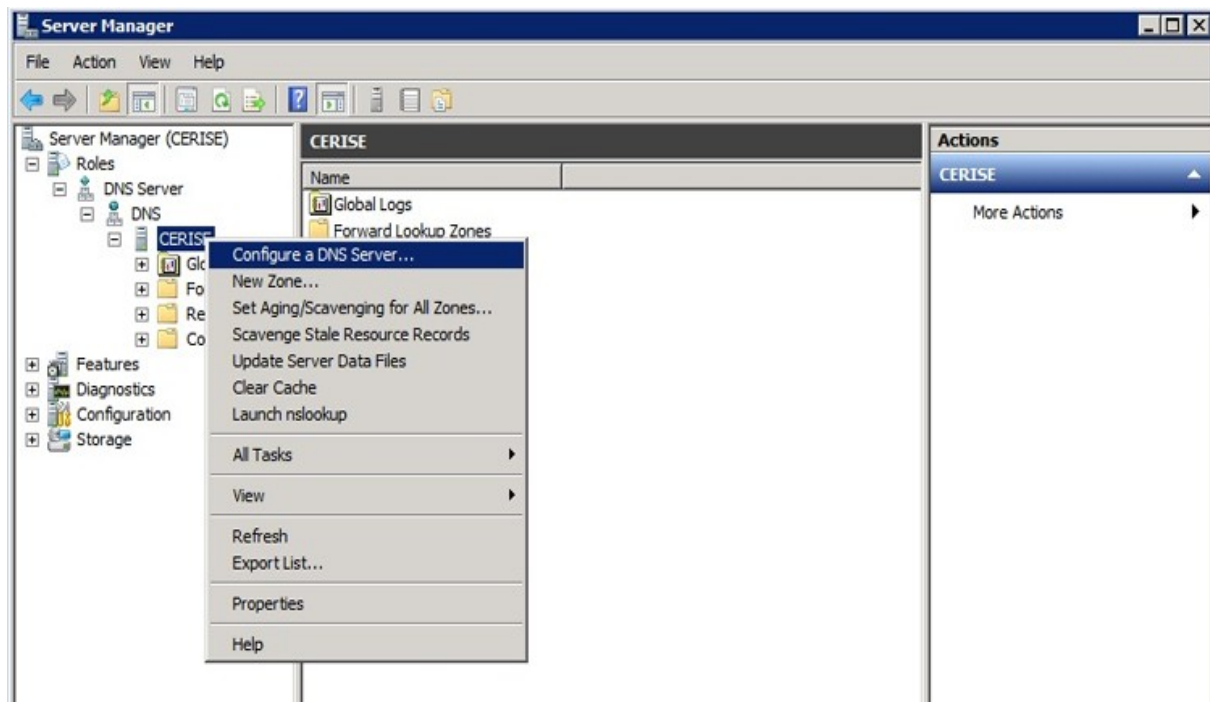


Comme vous pouvez le constater dans le "Server Manager" le rôle DNS a bien été ajouté.



I) Configuration

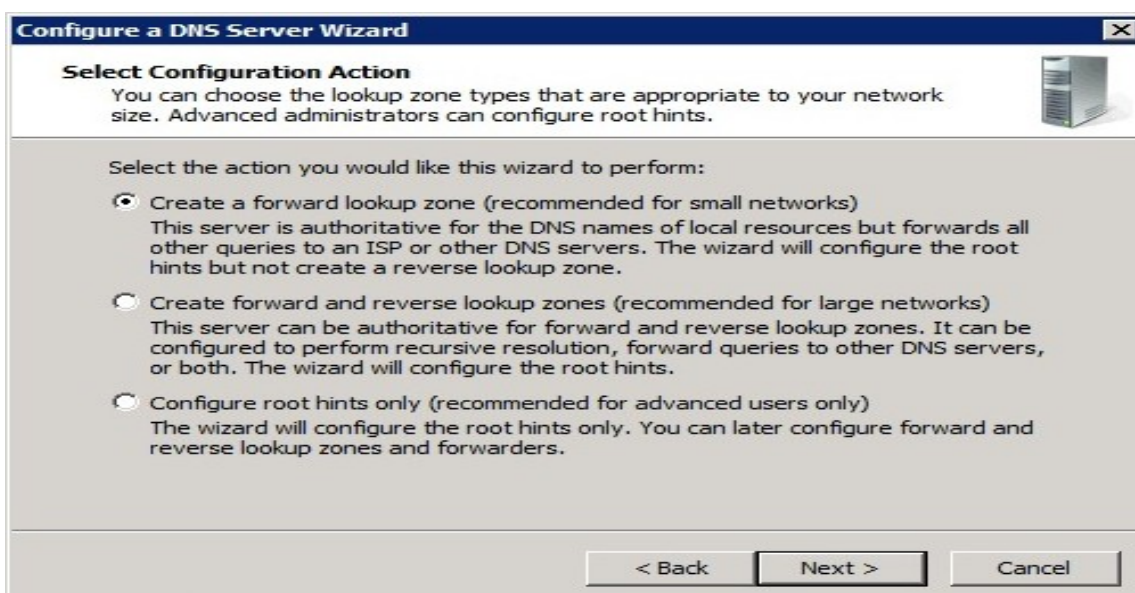
Cliquez sur le "+" devant "Roles" puis devant "DNS" pour développer. Faites ensuite un clic droit sur le nom de votre serveur (dans notre cas "CERISE") puis cliquez sur "Configure a DNS Server...".



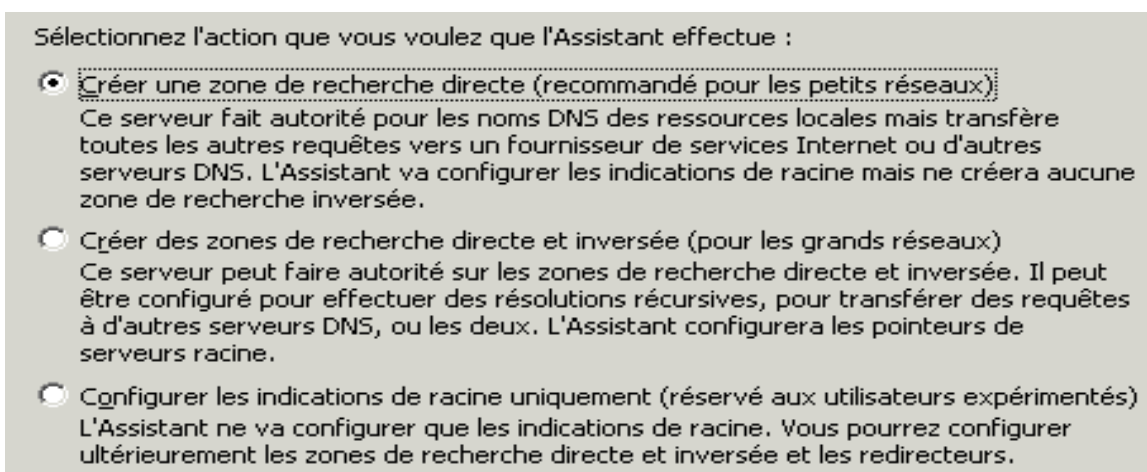
L'assistant de configuration se lance, cliquez sur "Next".



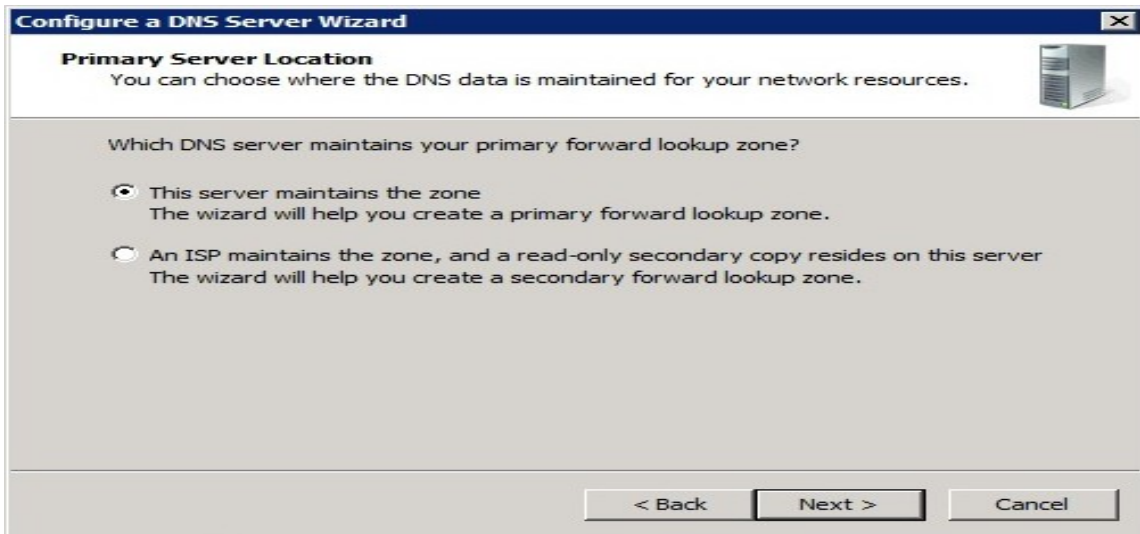
Sélectionnez maintenant le type de serveur dont vous avez besoin. Nous utiliserons le premier choix recommandé pour les petits réseaux :



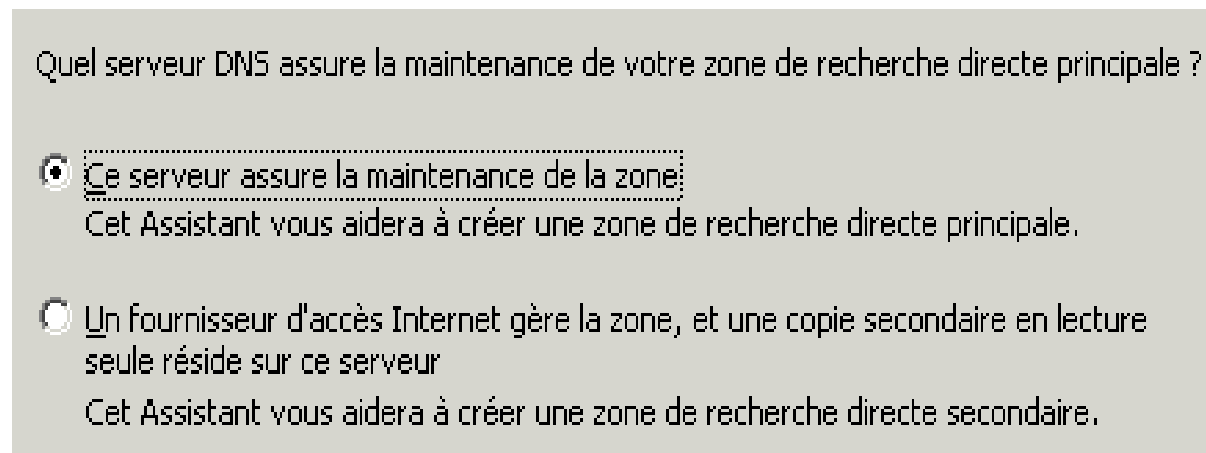
Voici la traduction pour vous aider à faire votre choix:



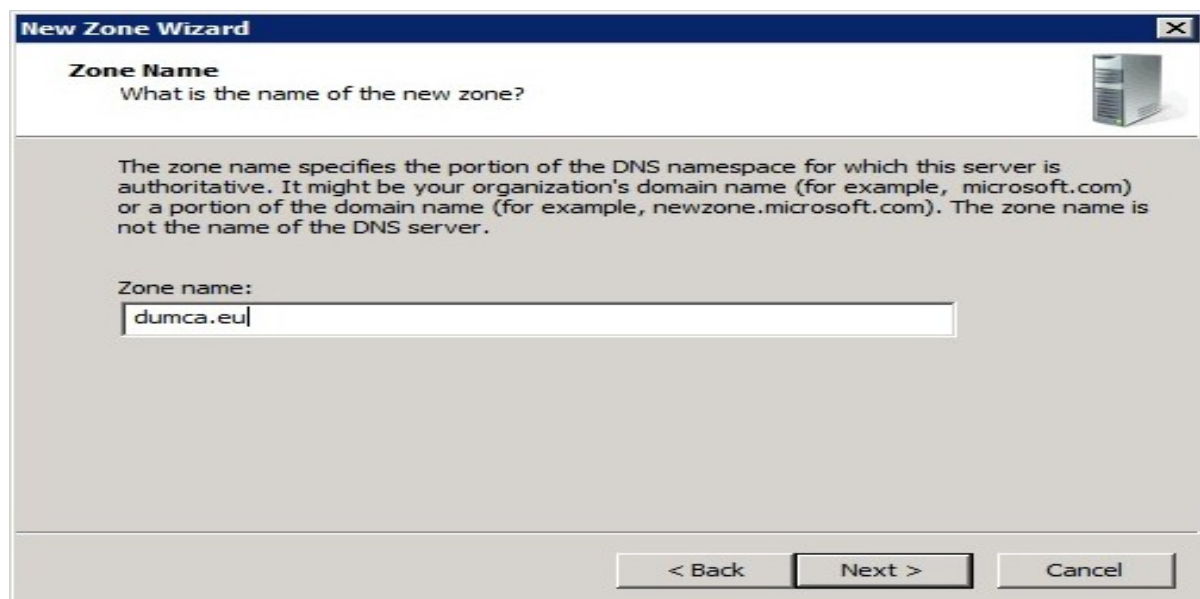
Sélectionnez ensuite le premier choix, pour que votre serveur soit le serveur primaire.



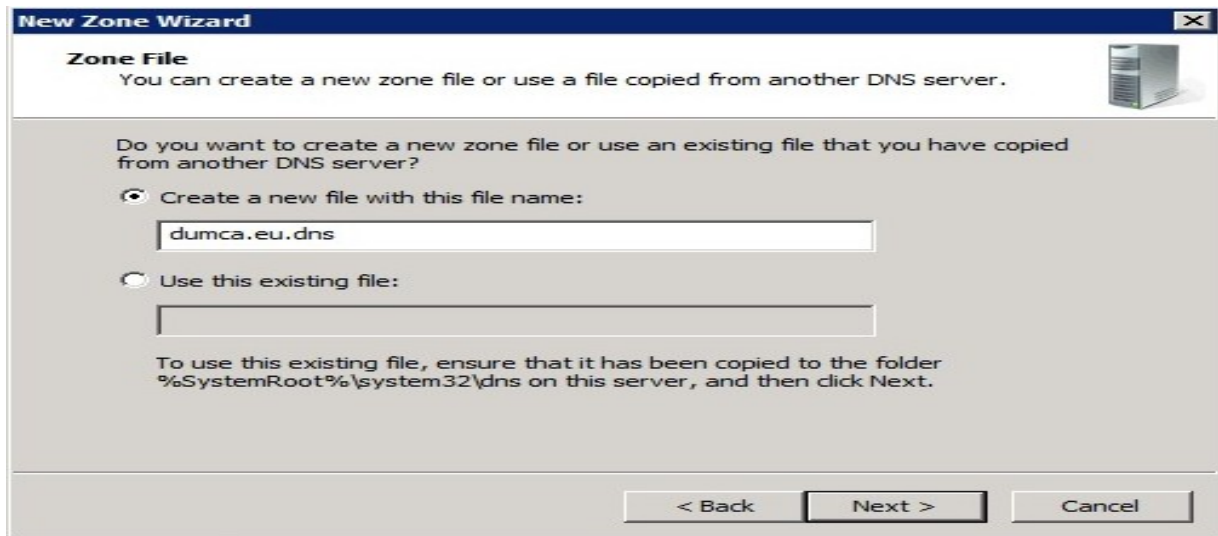
Voici la traduction pour vous aider à faire votre choix :



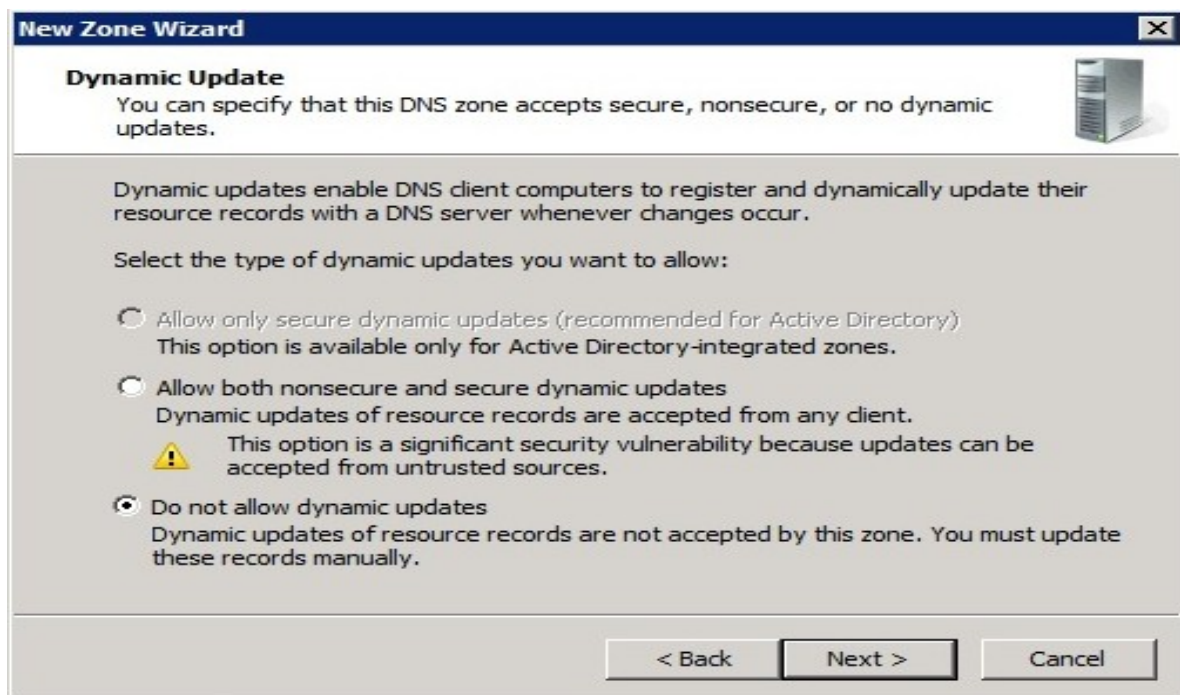
Déclarer le nom de votre domaine dans notre cas nous utiliserons "dumca.eu".



Donnez un nom au fichier de configuration de votre serveur DNS, je vous conseille de laisser celui par défaut.

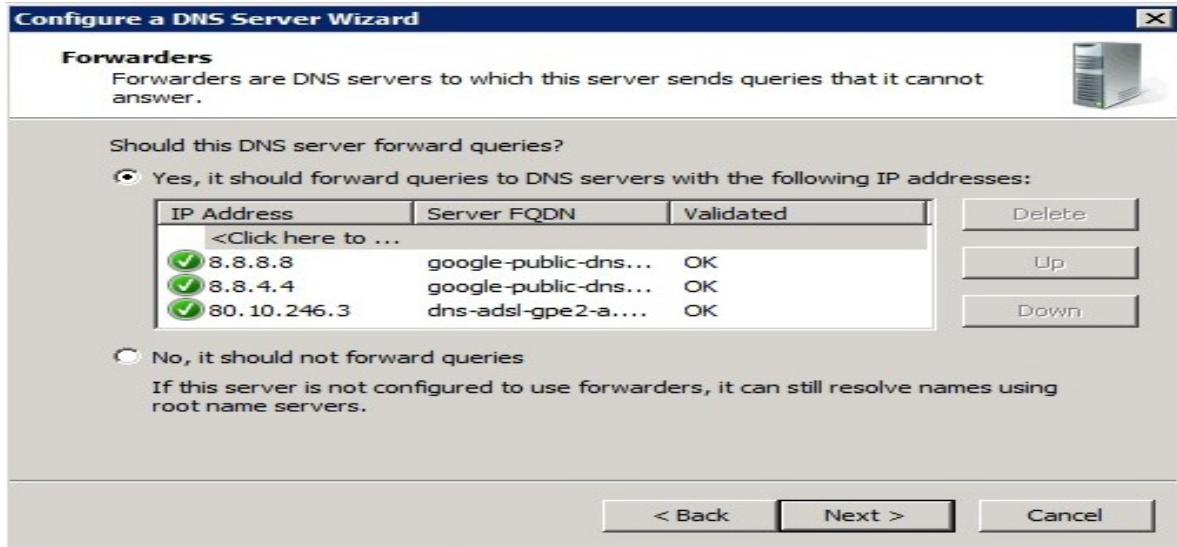


On vous propose maintenant d'accepter ou de ne pas accepter les mises à jour dynamiques, si vous avez installé "Active Directory" sélectionnez la première option "Allow only secure dynamic updates". Sinon sélectionnez "Do not allow dynamic updates" pour ne pas autoriser les mises à jour dynamiques pour plus de sécurité.

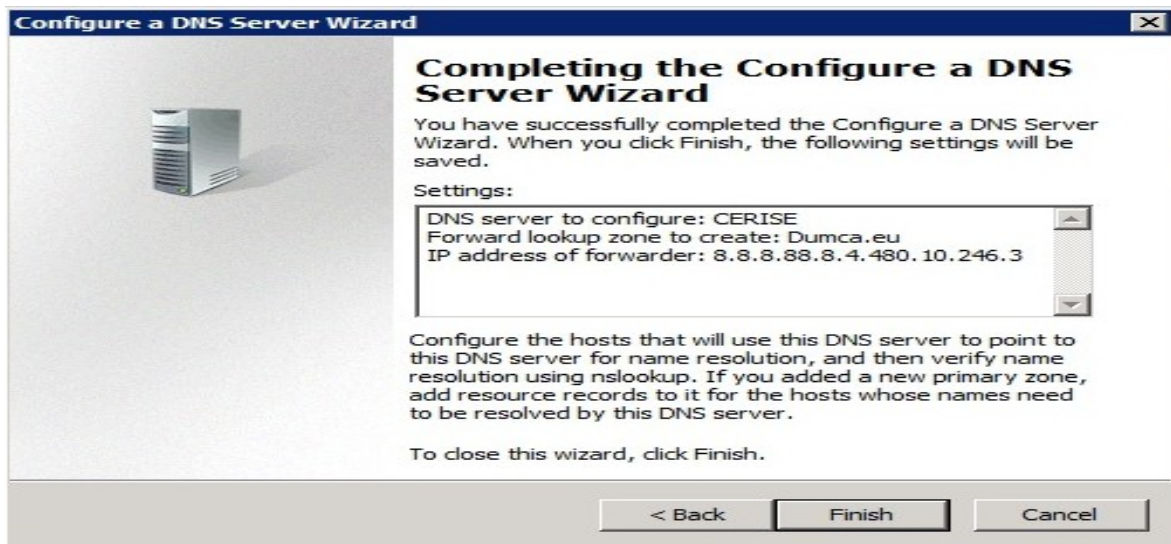


Nous allons maintenant configurer les adresses des DNS public sur lesquels notre serveur cherchera les noms de site internet (exemple google.com). Nous avons ajouté 3 adresses:

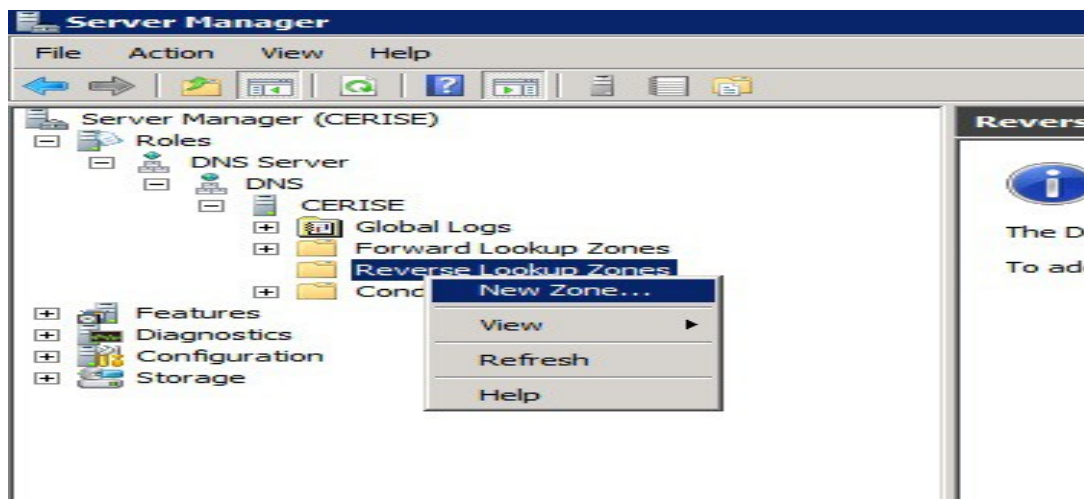
- 8.8.8.8
- 8.8.4.4
- 80.10.246.3



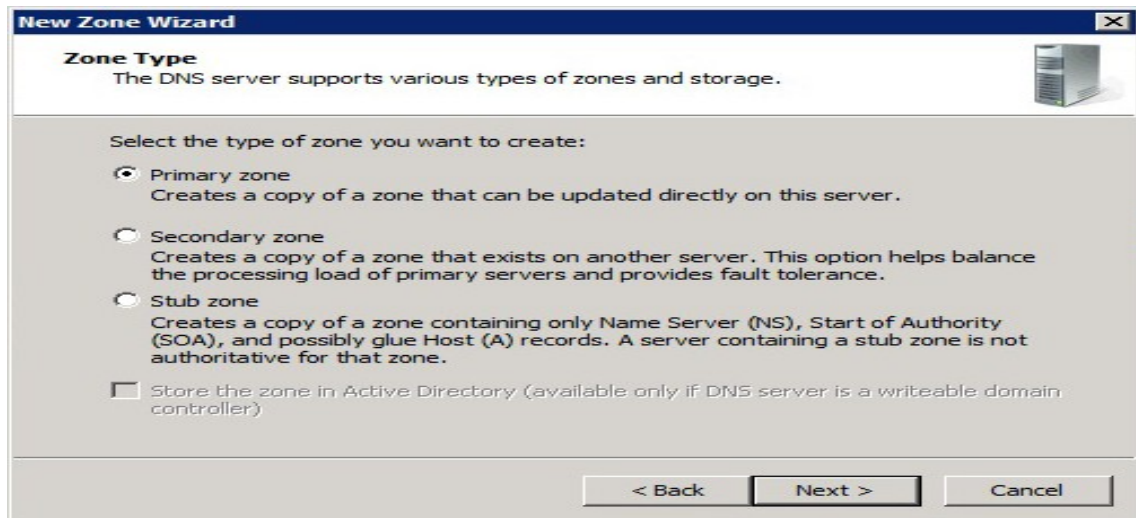
Il ne vous reste plus qu'à cliquer sur "Finish".



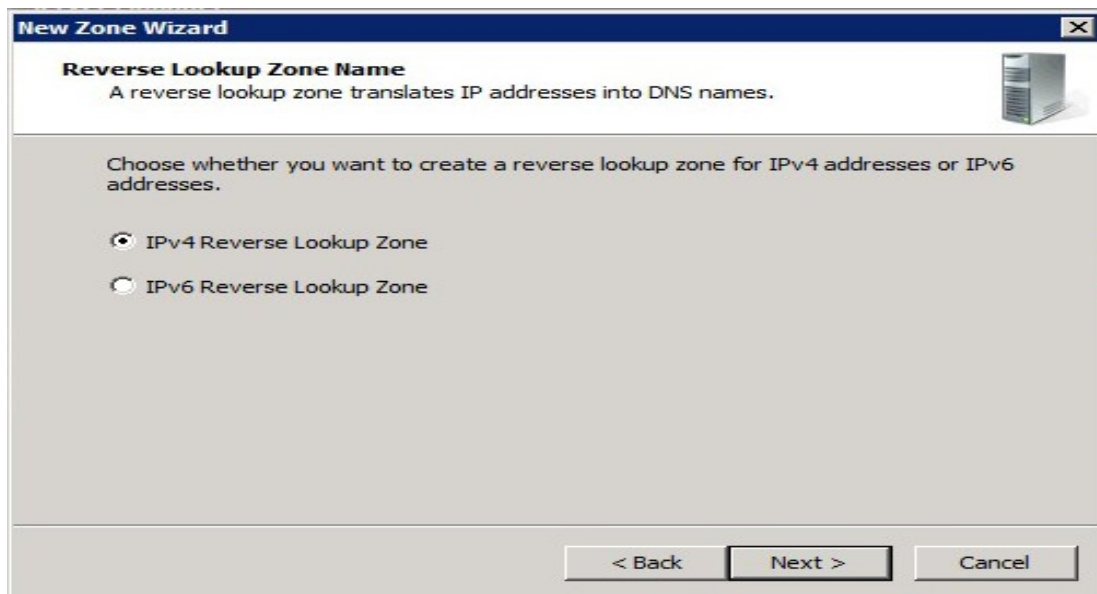
Nous nous retrouvons de nouveau sur la fenêtre du "Server Manager", faite un clic droit sur "Reverse Lookup Zones" puis "New Zone ...".



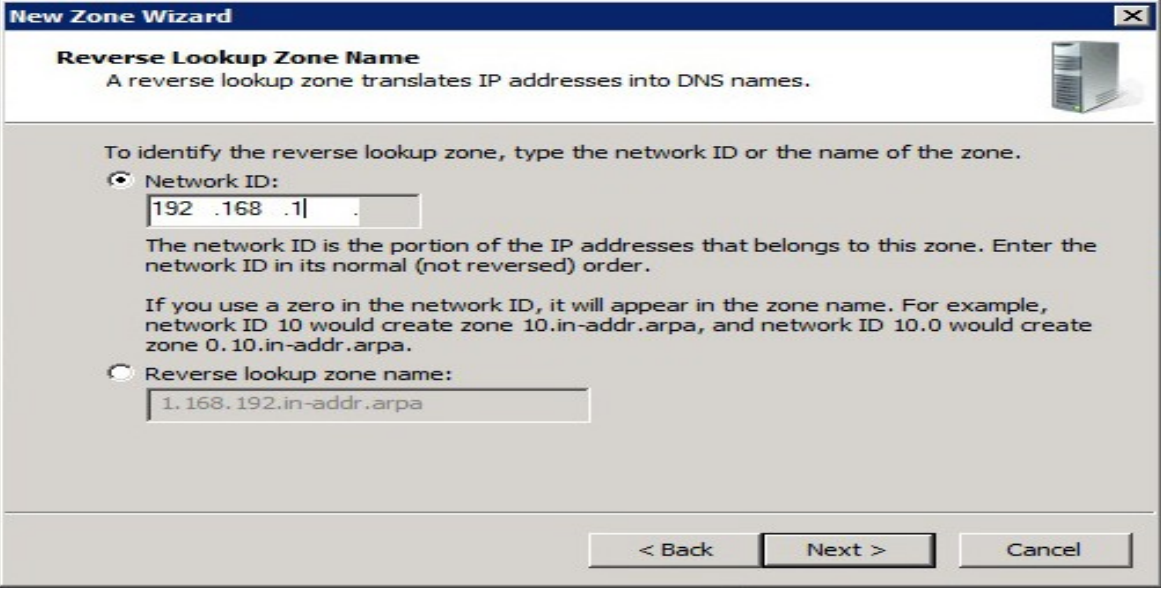
Sélectionnez "Primary zone".



Suivant votre réseau sélectionnez "IPv4 Reverse Lookup Zone" ou "IPv6 Reverse Lookup Zone", dans mon cas je choisi la première option.



Entrez maintenant l'adresse réseau.



New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:
[192 .168 .1] .

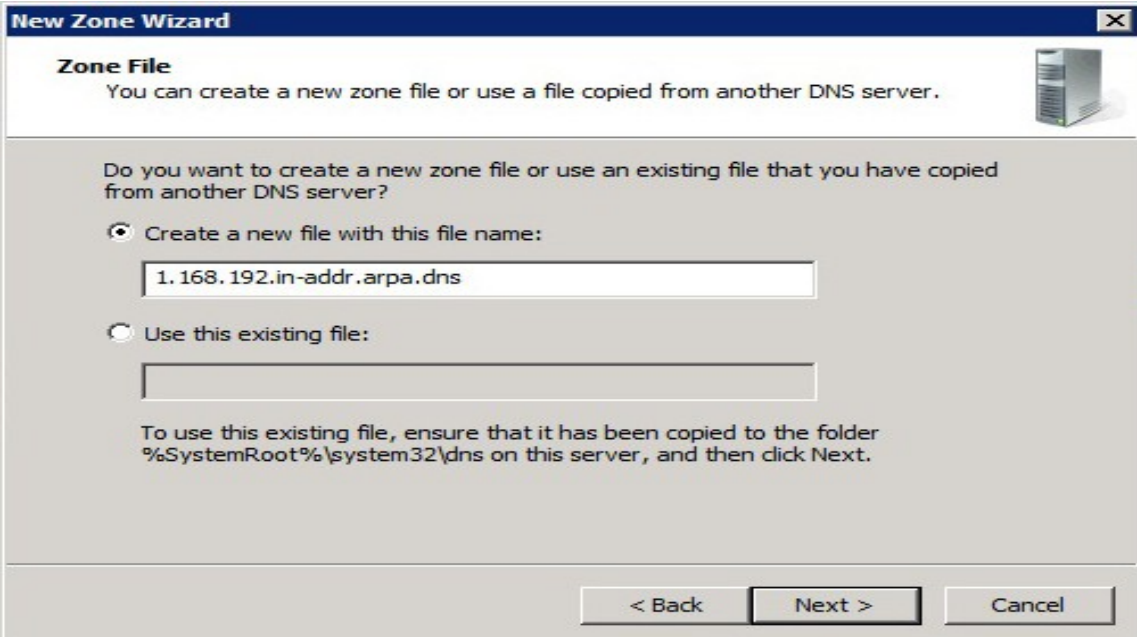
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

Reverse lookup zone name:
[1.168.192.in-addr.arpa]

< Back Next > Cancel

Donnez un nom au fichier de configuration de votre zone arpa, je vous conseille de laisser celui par défaut.



New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

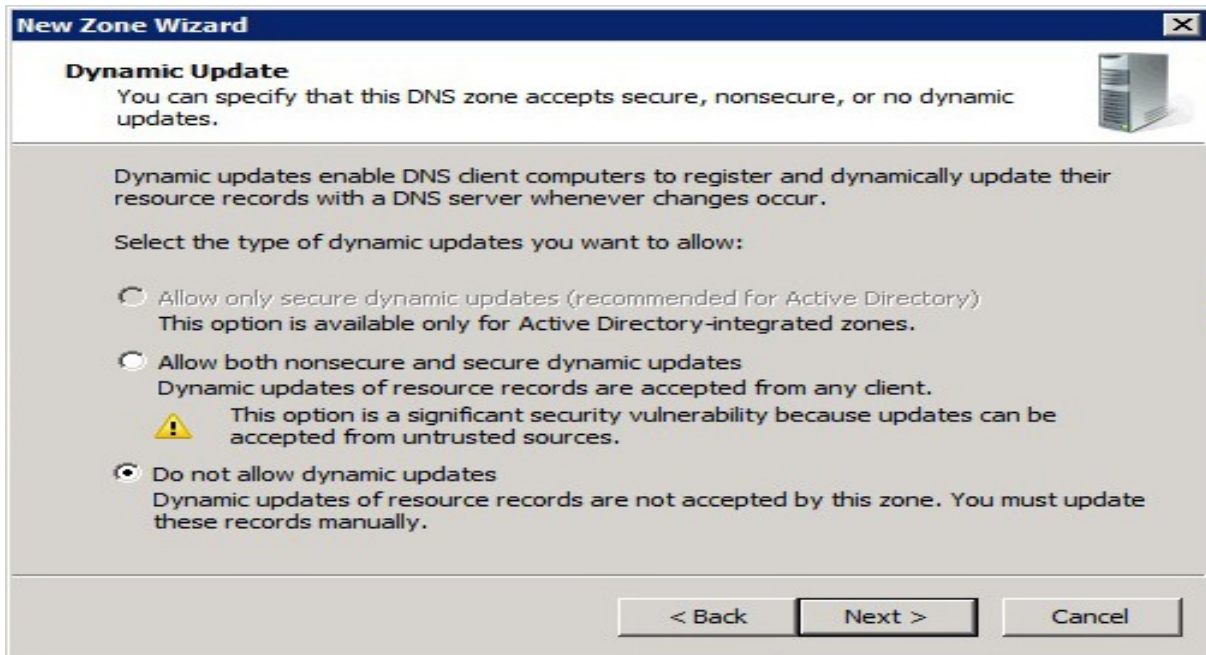
Create a new file with this file name:
[1.168.192.in-addr.arpa.dns]

Use this existing file:
[]

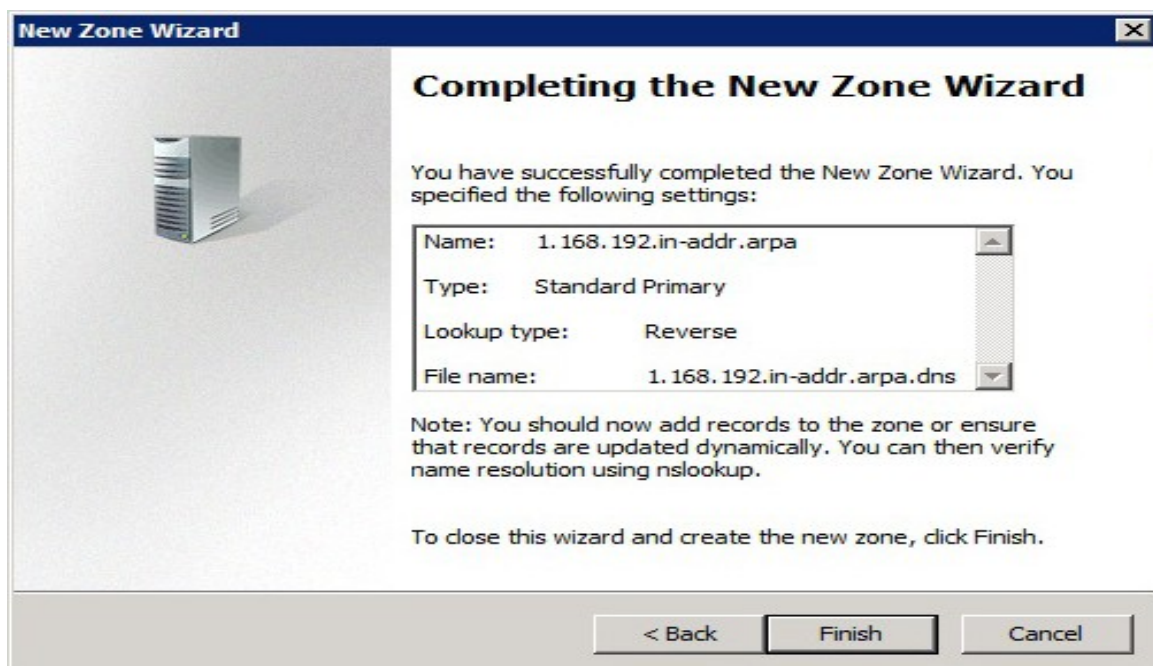
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back Next > Cancel

On vous propose maintenant d'accepter ou de ne pas accepter les mises à jour dynamiques, si vous avez installé "Active Directory" sélectionnez la première option "Allow only secure dynamic updates". Sinon sélectionnez "Do not allow dynamic updates" pour ne pas autoriser les mises à jour dynamiques pour plus de sécurité.

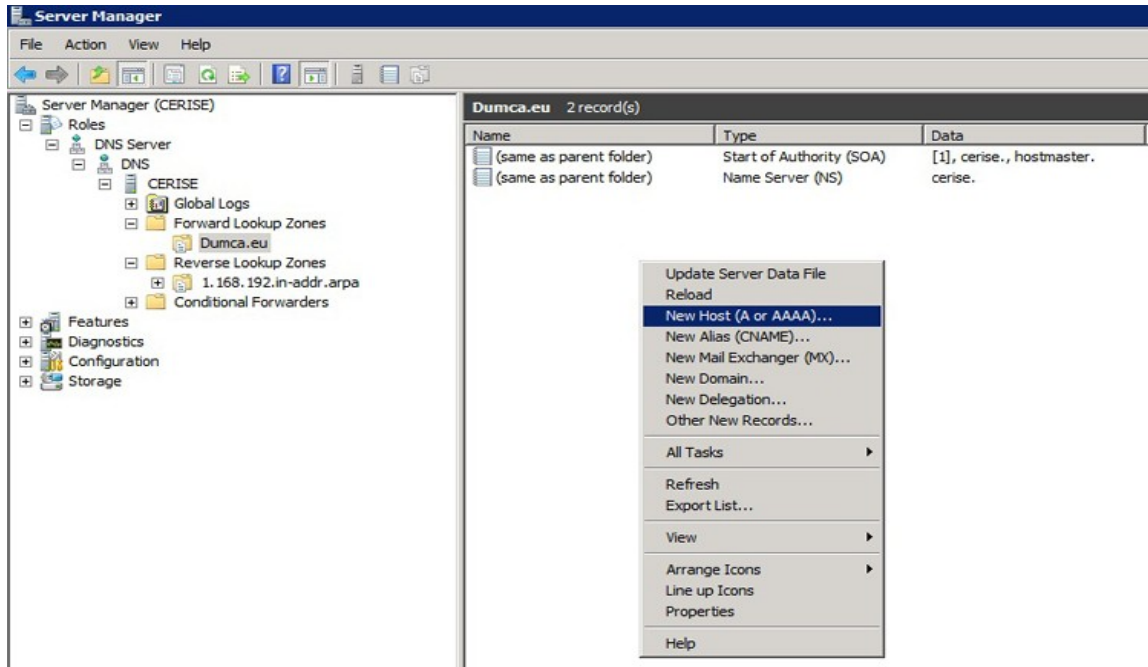


Il vous reste plus qu'à cliquer sur "Finish".

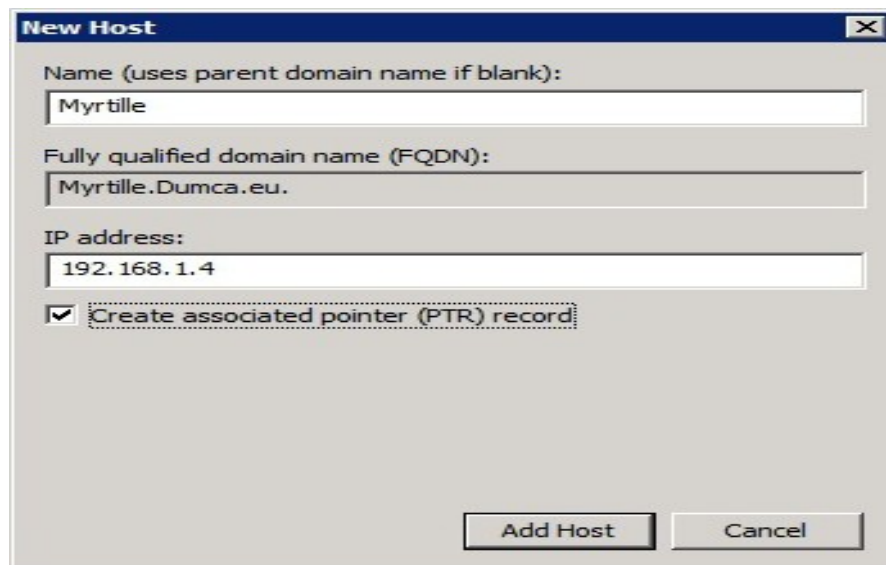


II) Ajout d'une machine :

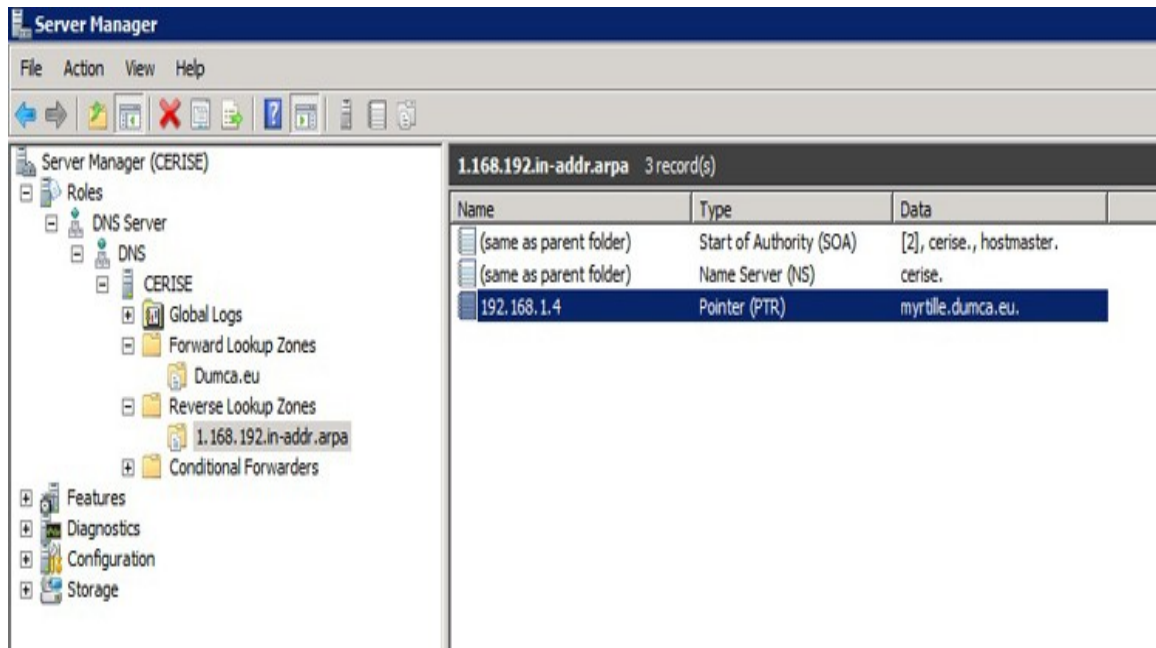
Maintenant nous allons ajouter manuellement un nom de machine : Faites un clic droit sur la partie droite comme sur l'image ci-dessous, puis cliquez sur "New Host (A or AAAA)".



Entrez le nom de machine, puis son adresse IP sans oublier de cocher "Create associated pointer (PTR) record".

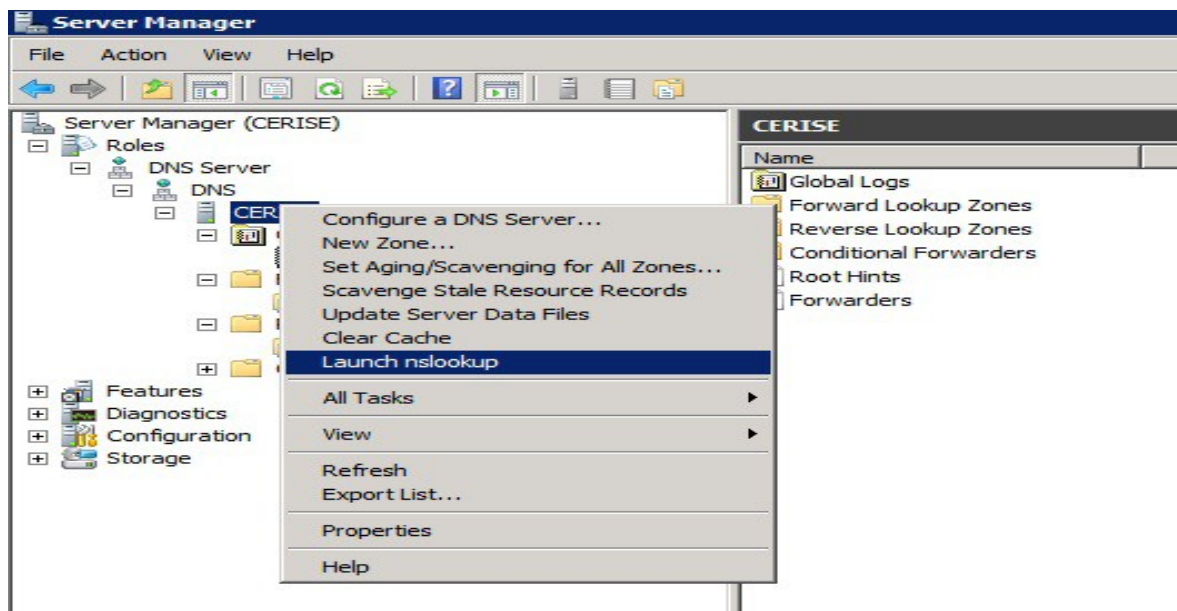


Comme vous pouvez le voir sur la photo ci-dessous nous avons bien ajouté un nouveau nom de machine.

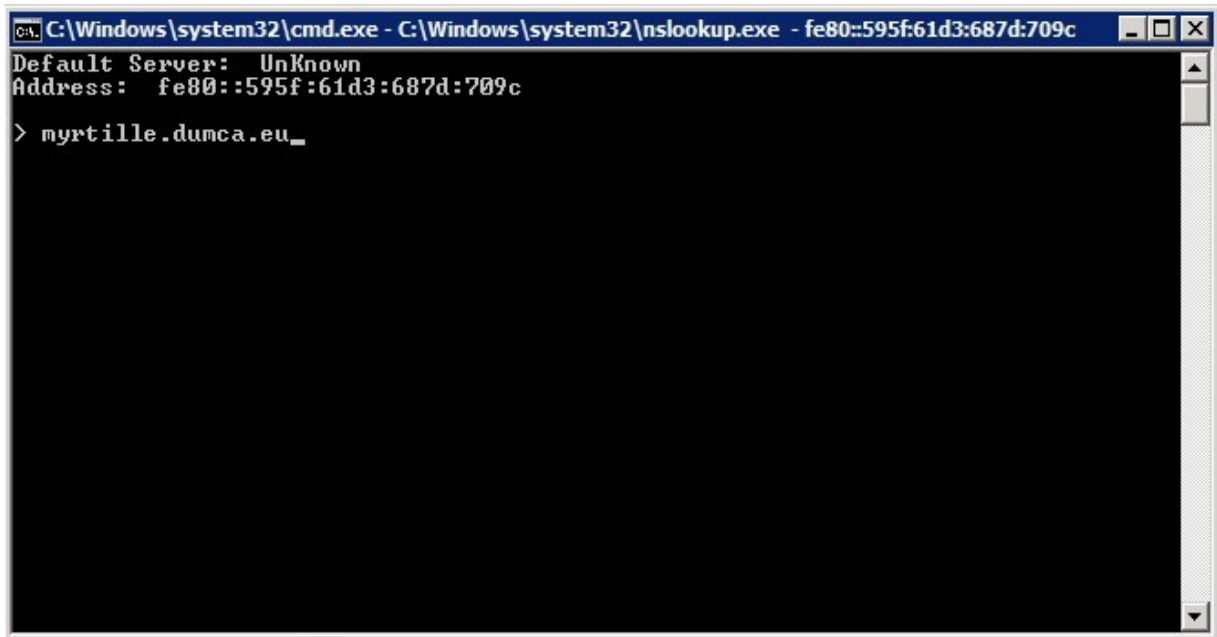


III) Test du serveur :

Nous allons essayer maintenant de faire une résolution de DNS pour savoir si notre serveur fonctionne : faite un clic droit sur le nom du serveur à gauche comme ci-dessous, puis cliquez sur "Launch nslookup".



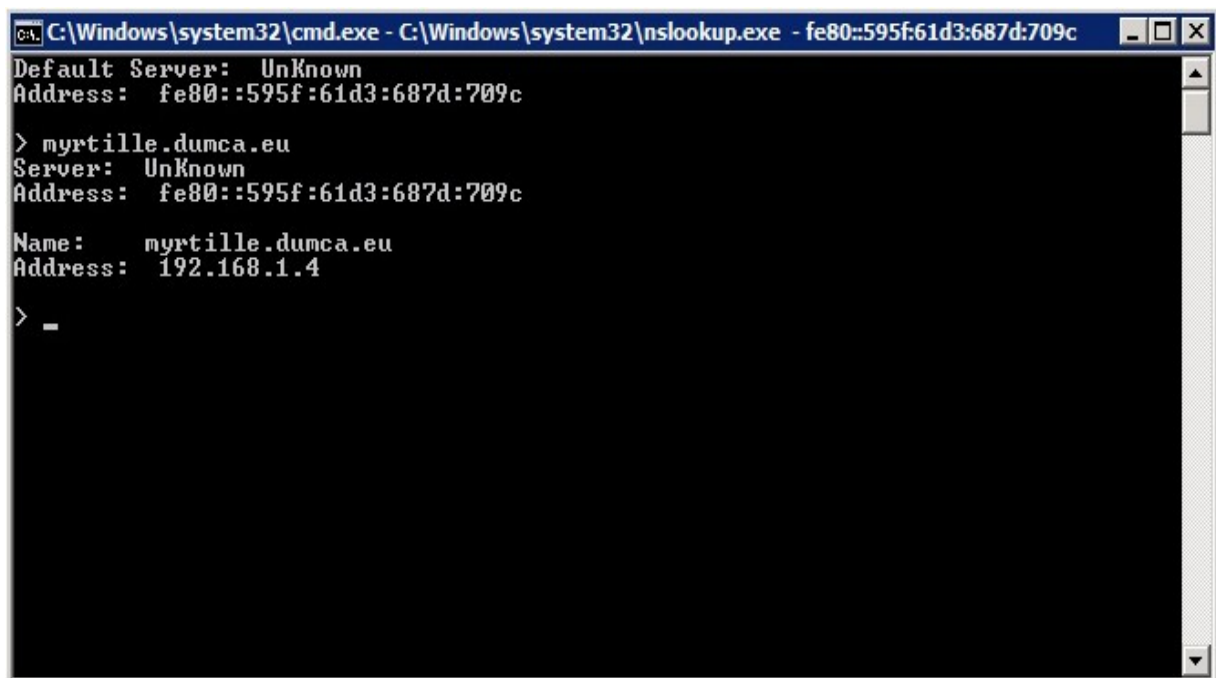
Une fenêtre de commande MS-DOS s'ouvre, tapez le nom complet (nom de machine + nom de domaine) de la machine que vous venez d'ajouter.



```
C:\Windows\system32\cmd.exe - C:\Windows\system32\nslookup.exe - fe80::595f:61d3:687d:709c
Default Server: UnKnown
Address: fe80::595f:61d3:687d:709c
> myrtille.dunca.eu_
```

Comme vous pouvez le remarquer il y a un petit problème de configuration, les informations retourné par le serveur ne sont pas complètes :

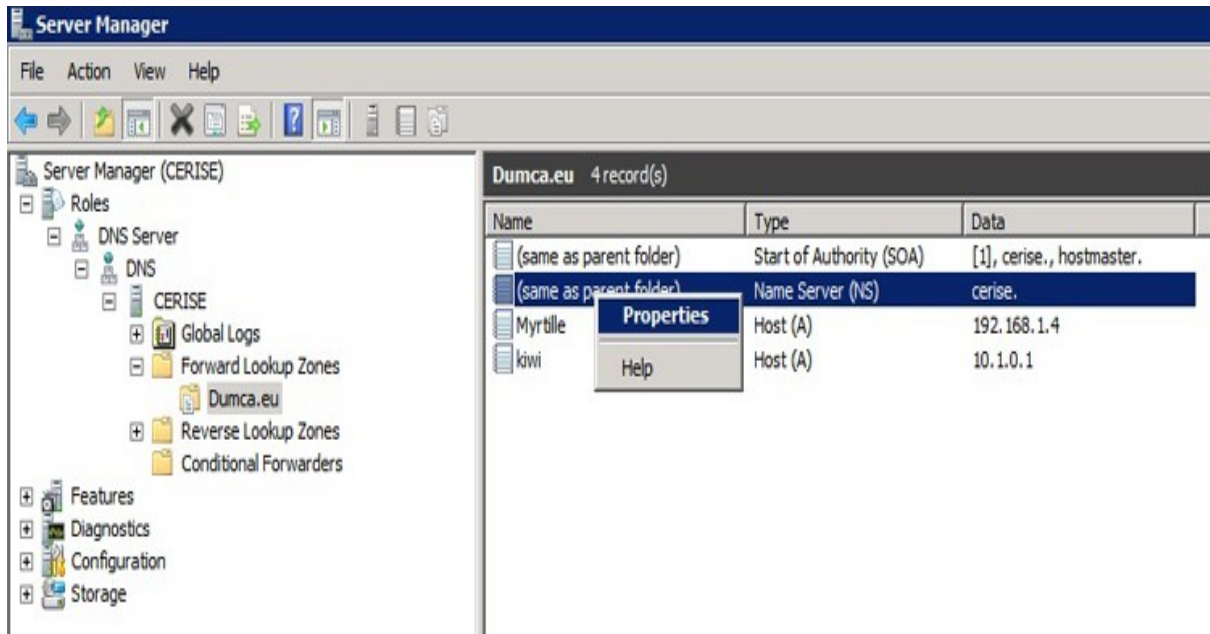
- ✓ Server : UnKnown
- ✓ Address : fe80 ::595f:61d3:687d:709c



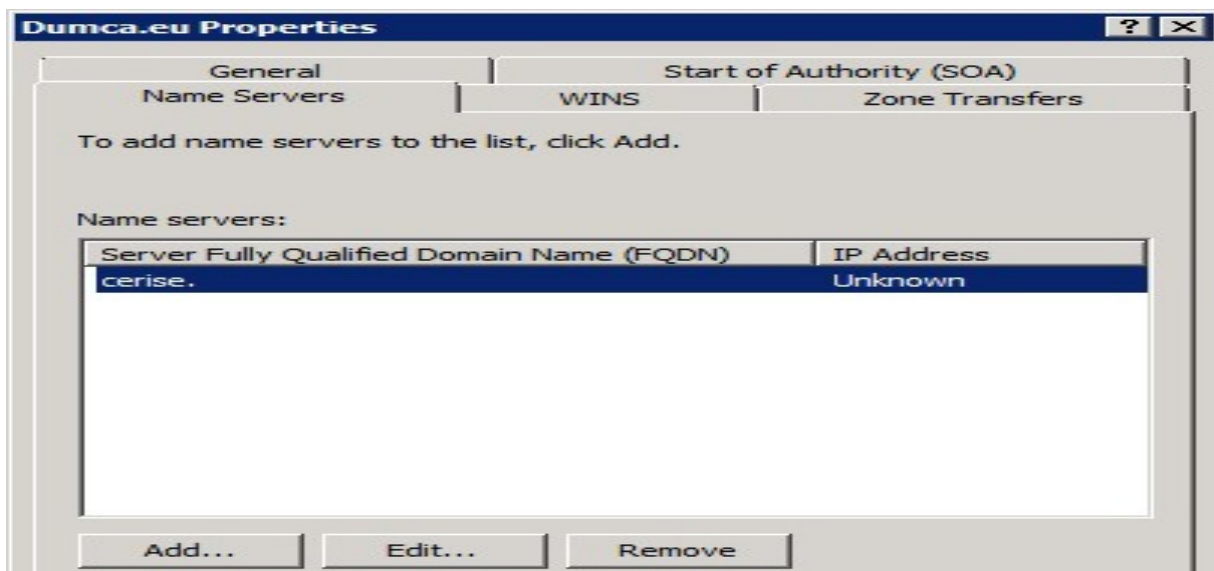
```
C:\Windows\system32\cmd.exe - C:\Windows\system32\nslookup.exe - fe80::595f:61d3:687d:709c
Default Server: UnKnown
Address: fe80::595f:61d3:687d:709c
> myrtille.dunca.eu
Server: UnKnown
Address: fe80::595f:61d3:687d:709c
Name: myrtille.dunca.eu
Address: 192.168.1.4
> _
```

IV) Configuration des informations du serveur DNS :

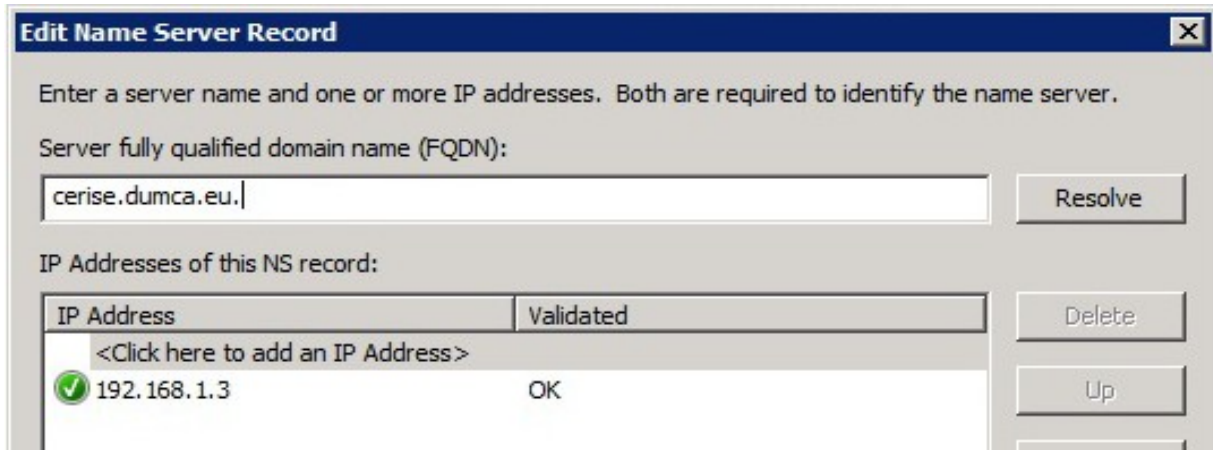
Dans la "Forward Lookup Zone" faite un clic droit sur "Name Server (NS)" dans la partie de droite, puis "Properties".



Vous obtenez cette fenêtre (ci-dessous), cliquez sur "Edit".



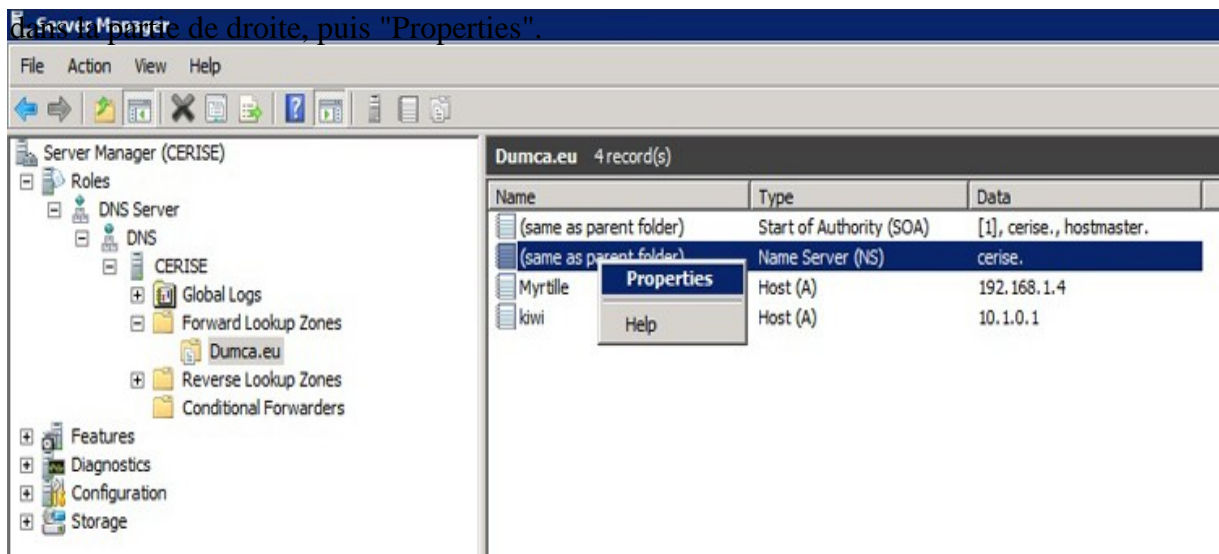
Entrez le nom FQDN ou nom complet du serveur (nom de machine + nom du domaine), puis ajoutez au moins une adresse IP avant de cliquer sur "OK".



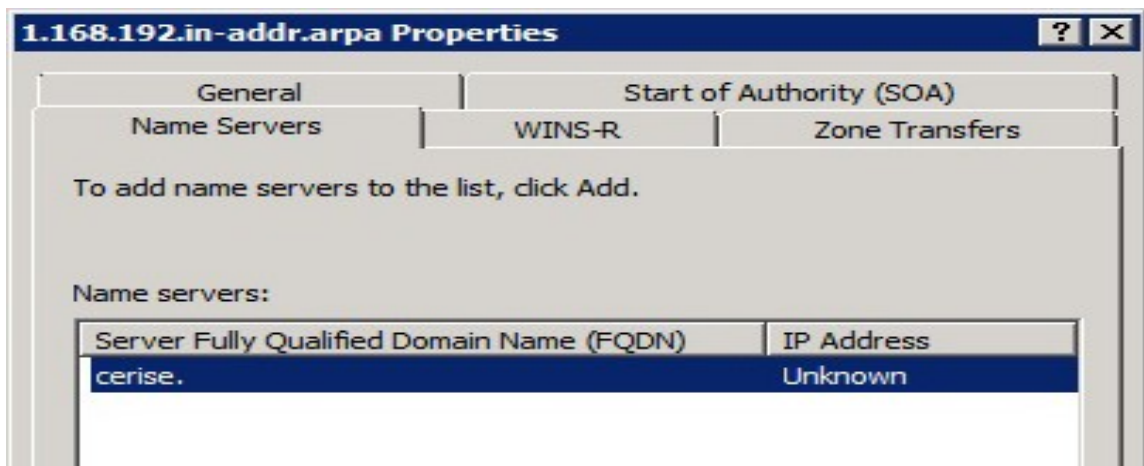
Cliquez maintenant sur l'onglet "Start of Authority (SOA)", Configurez les paramètres suivants puis fermez cette fenêtre.



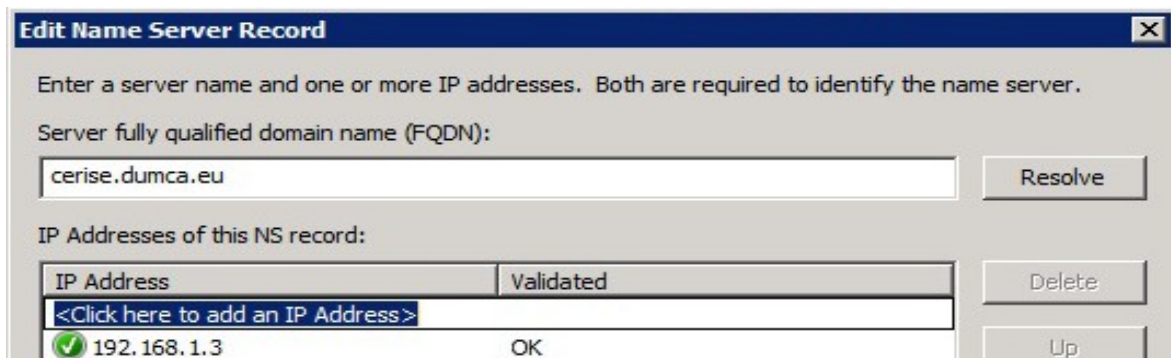
Recommencez avec la "Reverse Lookup Zone" faite un clic droit sur "Name Server (NS)" et cliquez sur "Propriétés".



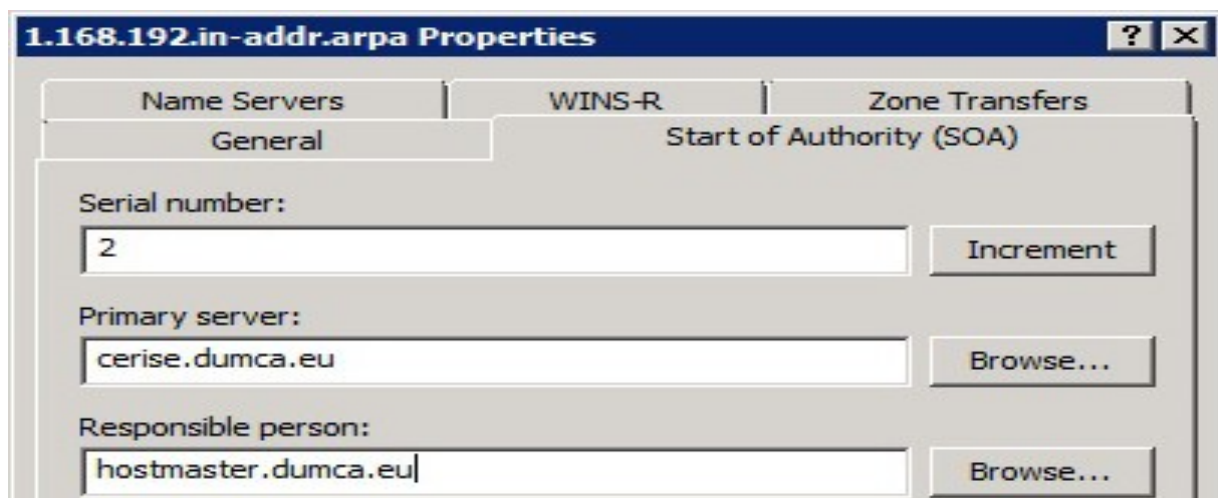
Vous obtenez cette fenêtre (ci-dessous), cliquez sur "Edit".



Entrez le nom FQDN ou nom complet du serveur (nom de machine + nom du domaine), puis ajoutez au moins une adresse IP avant de cliquer sur "OK".

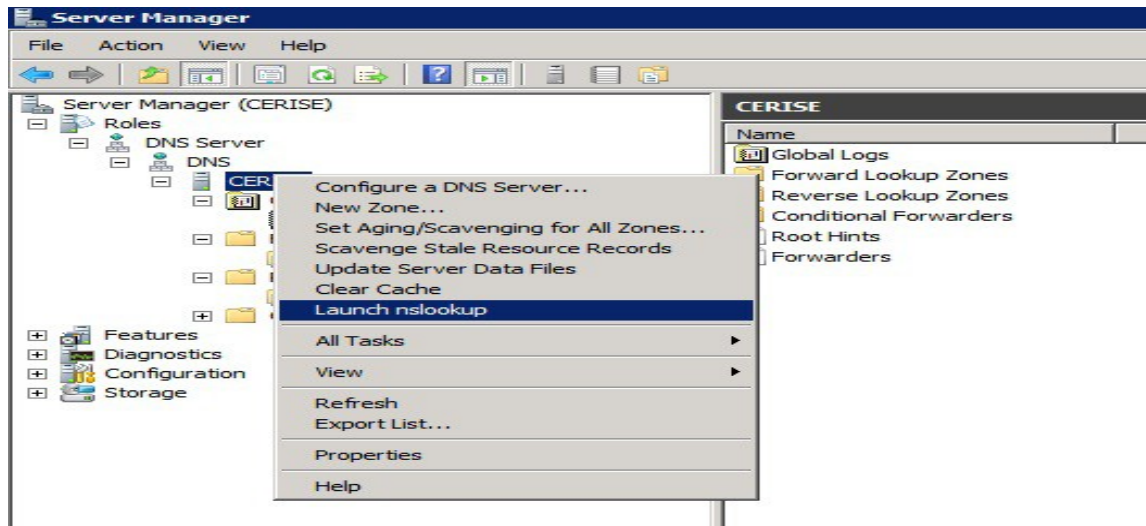


Cliquez maintenant sur l'onglet "Start of Authority (SOA)", Configurez les paramètres suivants puis fermez cette fenêtre.



V) Test du serveur :

Nous allons réessayer la résolution de DNS pour savoir si notre serveur fonctionne. Faites un clic droit sur le nom du serveur à gauche comme ci-dessous, puis cliquez sur "Launch nslookup".



Une fenêtre de commande MS-DOS s'ouvre, tapez le nom complet (nom de machine + nom de domaine) de la machine que vous venez d'ajouter.



Vous pourrez remarquer que cette fois, nous n'avons plus d'erreur.



Il est clair que notre serveur fonctionne. Vous pouvez ajouter l'adresse IP de votre serveur comme serveur de noms dans les configurations IP de vos stations de travail.

V.4.8/ Réstriction des utilisateurs:

✓ Group Policy Object (GPO) :

GPO est un stratégie de sécurité qui refuse ou non les accès à des périphérique des ordinateurs ou/et d'utilisateurs (c-à-d appliquer des restrictions). Tout dépend des choix de l'administrateur et les besoin de l'entreprise et cela pour des multiples causes.

Exemple :

Dans notre cas, mettre en œuvre une GPO qui refuse l'accès :

- ✓ Accès au stockage amovible (conf ordi/model admin/système/accès stock).
- ✓ Sauvegarde dans les emplacements locaux (conf ordi/mod admi/comp windows/sauvegarde).
- ✓ Désactiver le panneau de configuration d'affichage (conf utili/modél admini/affichage).

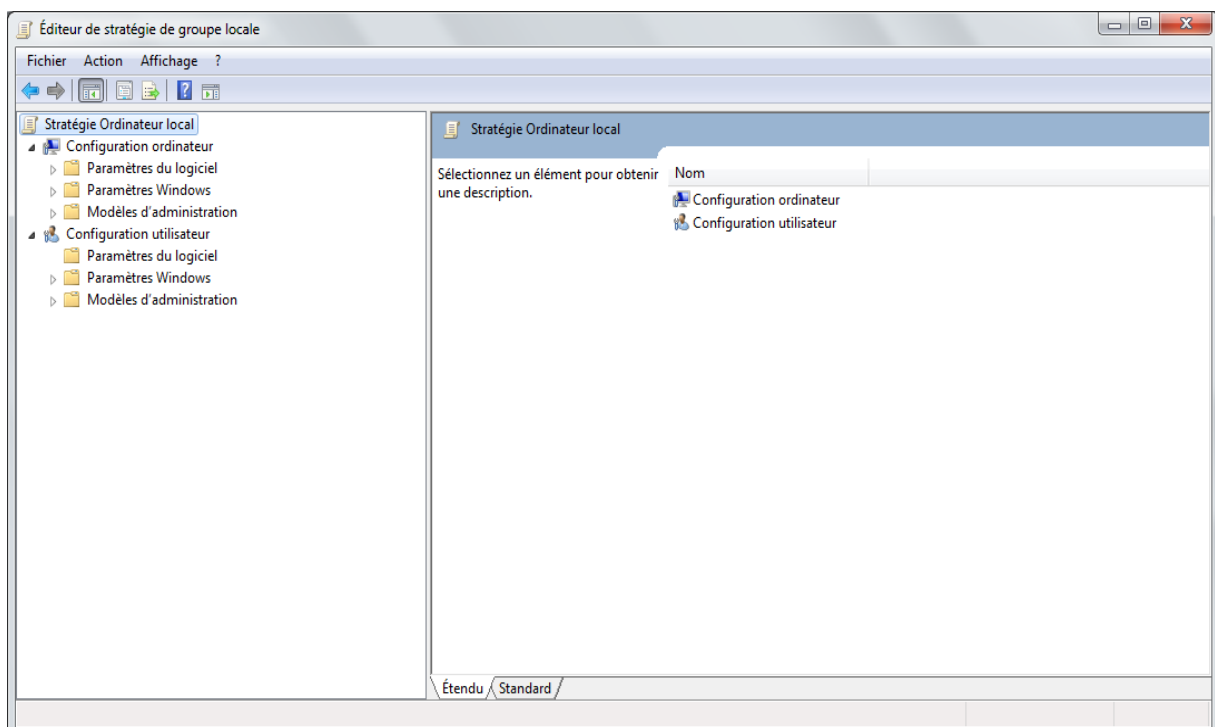


Figure V.33 : Editeur de stratégie de groupe local.

Architecture de l'entreprise :

La figure V. 34 représente l'architecture de l'entreprise.

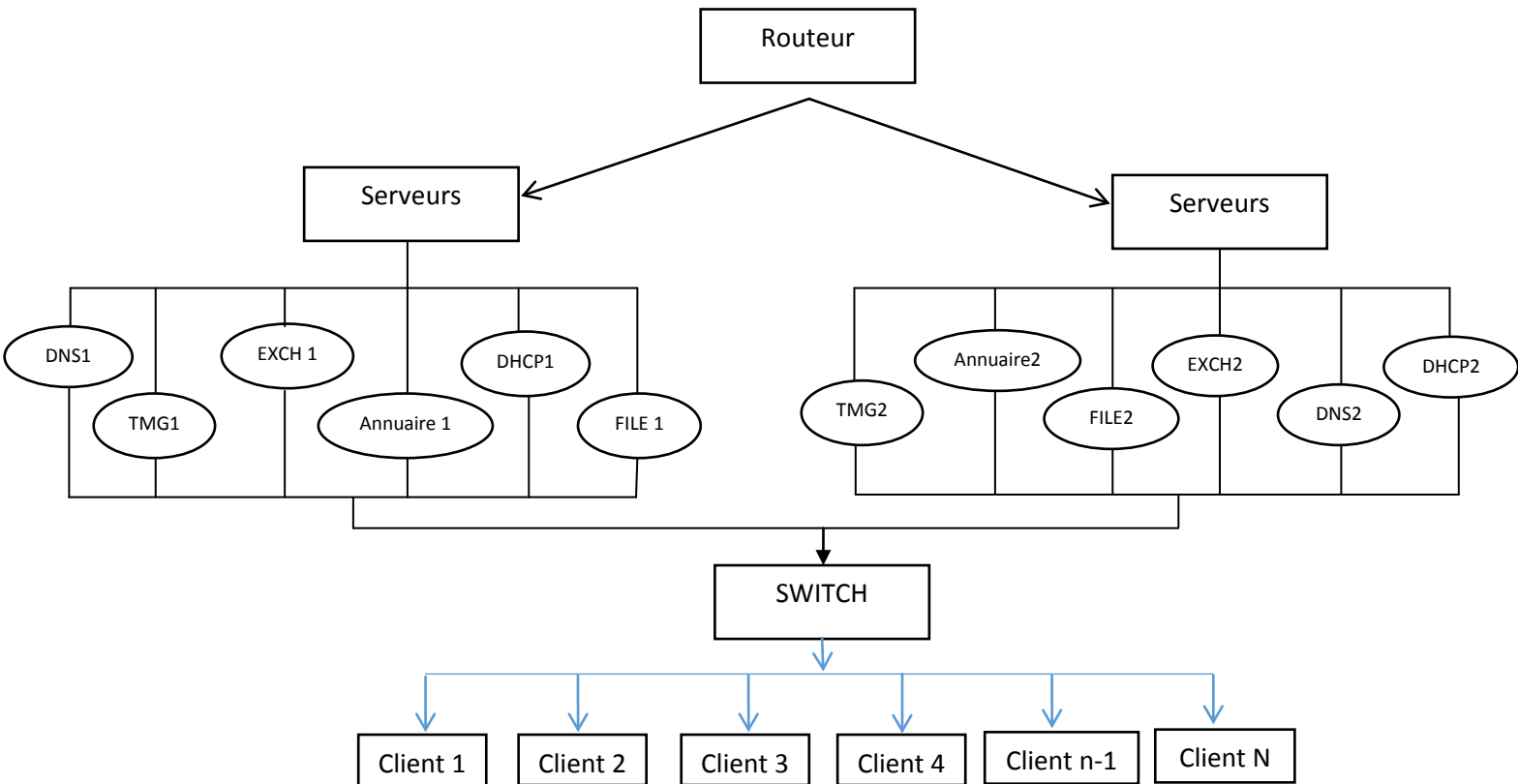


Figure V.34 : Architecture de l'entreprise.

Conclusion

En définitive, ce travail cible essentiellement la conception d'une infrastructure d'une entreprise afin d'assurer le bon déroulement du travail de tous les utilisateurs et afin de faciliter le travail aux administrateurs système. A cet effet, nous avons utilisé des outils de sauvegarde de données et de gestion des utilisateurs, tels que l'Active Directory (AD), EX change et le serveur de fichiers (file), de façon à ne pas affecter le système.

Notre étude a permis de gérer les utilisateurs de système et de stocker leurs données en toute sécurité et fiabilité mettant en évidence un aspect pratique pour cette conception. Notre investigation a offert aux utilisateurs un moyen de communication de messagerie rapide, efficace et sécurisé. Elle leur offre, également, un environnement de partage des ressources puisqu'elle permet à plusieurs utilisateurs de tirer profit des mêmes infrastructures et à plusieurs fins en même temps.

En perspective, il serait intéressant et judicieux d'étaler cette étude à d'autres systèmes plus modernes à savoir le RAID, pour conserver des données dans une baie de stockage qui gère l'espace intelligemment.

Bibliographie et webographie

- 1. Anonyme, 2010. Réseaux informatiques. Modèle OSI et protocole TCP/IP.**
- 2. CALECA C., 2005. TCP/IP. <http://christian.caleca.free.fr/tcpip/>**
- 3. BELKHOUCHE souhila., 2011., Tlemcen Caractéristique des modèle client/serveur.**
- 4. OLIVIER Gluck 2014**
- 5. CHRISTIAN Bulfone., <http://www.gipsa-lab.fr/~christian.bulfone/IC2A-DCISS/>**
- 6. BELKHOUCHE souhila., 2011., Tlemcen Caractéristique des modèle client/serveur.**
- 7. OLIVIER Gluck 2014.**
- 8. MICHEL Simatic 2012.**
- 9. Site officiel de Microsoft Windows.**
- 10. <http://idecibel.tuxfamily.org/courswinxp/Bases%20du%20registre.>**
- 11. <http://idecibel.tuxfamily.org/courswinxp/Bases%20du%20registre.>**