Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Virtuelle de Tunis

UVT
جامعة تونس الافتراضية
UNIVERSITÉ VIRTUELLE DE TUNIS

MEMOIRE

DE STAGE DE FIN D'ETUDES

Pour l'obtention du

«Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)»

Présenté par :

Henda Azzouzi

Titre

Exploitation des différents services sous server 2008 et gestion de certificat

Soutenu le : 29 octobre 2016

Devant le jury :

Président : Mr. (Mme.)

Encadreur : Mr. (Mme.) Hela Bouceta

Rapporteur : Mr. (Mme.)

Membre : Mr. (Mme.)

Année Universitaire : 2015 - 2016

Remerciement:

Je tiens à présenter mes reconnaissances et mes remerciements à mon encadrante madame Hela Bouceta, pour le temps consacré à la lecture et aux réunions qui ont Rythmées les différentes étapes de mon mémoire. Les discussions que nous avons partagées ont Permis d'orienter mon travail d'une manière pertinente.

Je le remercie aussi pour sa disponibilité à encadrer ce travail à travers ses critiques et ses propositions d'amélioration.

Je remercie également Mr.Sadok Ghanmi et Mr. Chameseddine Halaouet, pour leurs patiences, leur amabilités, leur coopérations et pour tous les conseils et les informations qu'ils m'ont Dispensé afin que ce stage se passe dans les meilleures conditions.

Je remercie également toute L'équipe de l'entreprise qui a essayé de créer une ambiance favorable au bon déroulement de ce stage.

Je remercie évidement tous les membres du jury qui ont accepté d'évaluer ce travail

Enfin je remercie toutes les personnes qui ont contribué de prés ou de loin à la

Réalisation de ce mémoire, ainsi qu'au bon déroulement du stage, et dont les noms ne figurent Pas dans ce document.

Dédicaces

A Mes Très Chers Parents

Tous les mots du monde ne sauraient exprimer l'immense amour que je vous porte, ni la profonde gratitude que je vous témoigne pour tous les efforts et les sacrifices que vous n'avez jamais cessé de consentir pour mon instruction et mon bien-être.

C'est à travers vos encouragements que j'ai opté pour cette profession, et c'est à travers vos critiques que je me suis réalisé.

J'espère avoir répondu aux espoirs que vous avez fondés en moi.

Je vous rends hommage par ce modeste travail en guise de ma reconnaissance éternelle et de mon infini amour.

Que Dieu tout puissant vous garde et vous procure santé, bonheur et longue vie pour que vous demeuriez le flambeau illuminant le chemin de vos enfants

Je dédie aussi ce travail à :

Mes sœurs pour leurs encouragements incessants.

Tous mes amis et spécialement Mounir Hamdi pour leur soutien continu, leur aide précieuse

Table de matières

Liste des Figures

Liste des acronymes

[A]:

AD: Active Directory

A, G, U, DL, P: A: **A**ccount, **G**: **G**lobal Group, **U**: **U**niversal group,

DL: **D**omain **L**ocal group, **P**: **P**ermissions

ADS: **A**ctive **D**irectory **S**ervice

ACL: **A**ccess **C**ontrol **L**ist

[C]:

CA: **C**ertificate **A**uthorities

CS: **C**ertificat **S**ervices

CRL: **C**ertificate **R**evocation **L**ist

[D]:

DNS: **D**omain **N**ame **S**ystem

DHCP: **D**ynamic **H**ost **C**onfiguration **P**rotocol

DC-Promo : **D**omain **C**ontroller **P**romotion

[E]:

EFS: **E**ncrypting **F**ile **S**ystem

[F]:

FQDN: Fully **Q**ualified **D**omain **N**ame

FTP: File Tranfert **P**rotcole

[I]:

IIS: **I**nternet **I**nformation **S**ervices

[K]:

KDC: **K**ey **D**istribution **C**enter

[L]:

LDAP : Lightweight **D**irectory **A**ccess **P**rotocol

[M]:

MD5 : Message **D**igest 5

MMC : Microsoft **M**anagement **C**onsol

[N]:

NTFS: New **T**echnology **F**ile **S**ystem

[P]:

PKI: **P**ublic **K**ey **I**nfrastructure

PDC: **P**rimary **D**omain **C**ontroller

PGP : Pretty **G**ood **P**rivacy

[R]:

RSA : **R**ivest, **S**hamir et **A**dleman

RID: **R**elative **I**dentifier

[S]:

SAM: **S**ecurity **A**ccount **M**anager

SA: **S**ervice d'**A**uthentification

SHA-1: **S**ecure **H**ash **A**lgorithm

SID: **S**ecurity **Id**entifier

ST: **S**ervice **T**icket

SSL: Secure **S**ocket **L**ayer

[T]:

TCP/IP: Transmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol

TGS: **T**icket-**G**ranting **S**ervice

TGT: **T**icket **G**ranting **T**icket

[U]:

UO: **U**nite **O**rganizationally

[V]:

VP: **V**irtual **M**achine

Introduction générale

Les entreprises ont développé le modèle traditionnel du réseau local (LAN, Local Area Network*)*. C'est pourquoi, il est plus important que jamais de renforcer la sécurité de ses systèmes informatiques. Pour renforcer la sécurité au sein des entreprises déployant Windows Server, Microsoft Windows Server 2008 propose une plate-forme plus sécurisée : **PKI.**

Une PKI (Public Key Infrastructure), aussi appelée IGC (Infrastructure de Gestion de Clés) est donc une infrastructure qui se construit. C'est une structure à la fois technique et administrative. Le domaine des PKI est intéressant : il est possible de les utiliser pour des applications tels que mail chiffré, web sécurisé, VPN, commerce électronique …

Dans ce cadre, nous allons mettre en place un exemple d'implémentation d'une PKI dans un environnement Microsoft Windows Server 2008. Son but final est de renforcer la sécurité dans notre réseau. Donc, ce rapport va présenter les pré-requis nécessaires à cette implémentation, essentiellement la préparation d'un environnement ADS (Active Directory Services).

Pour ce faire, il apparaît logique de présenter à titre préalable dans un premier chapitre Cadre général et spécifications des besoins, puis dans un deuxième chapitre, nous allons détailler l'infrastructure Microsoft Active Directory et les différents services telque Dns, DHCP, Ftp. Ensuite un Troisième chapitre l'infrastructure de clé publique, qu'est un ensemble de technologies, procédures et pratiques qui supportent l'implémentation et l'exploitation des certificats basés sur la cryptographie à clé publique. Et un dernier chapitre configuration des différents services et implémentation de service de certificats sera consacrée à la gestion de certificats dans des systèmes de sécurité (autorité de certification, une demande de certificat…).

Ce travail sera réalisé au sein de Tunisie Télécom (Elghazala) L'élaboration de ce rapport a pour principale source, les différents enseignements tirés à la pratique journalière des tâches auxquelles nous étions affectés. Enfin, les nombreux entretiens que nous avons pu avoir avec les employés des différents services de l'entreprise, nous ont permis de donner une cohérence à ce rapport.

Chapitre1 :

Cadre général et spécification des besoins

Ce chapitre est consacré pour la présentation de l'entreprise d'accueil, la précision du cadre du projet et la problématique puis l'énumération des étapes de travail à réaliser pour achever ce projet.

1. Tunisie Telecom

1.1. Présentation générale :

L'office national des télécommunications est créé suite à la promulgation de la loi N°36 du 17 avril 1995. L'office a ensuite changé de statut juridique, en vertu du décret N°30 du 5 avril 2004, pour devenir une société anonyme dénommée « Tunisie Telecom ». Tunisie Telecom compte dans ses rangs plus de 6 millions abonnés dans la téléphonie fixe et mobile, en Tunisie et à l'étranger. Elle joue en outre un rôle important dans l'amélioration du taux de pénétration de l'Internet en Tunisie, ce qui lui permit d'atteindre le nombre 140 mille abonnés à la toile à la fin du mois d'avril 2008. Tunisie Telecom se compose de 24 directions régionales de plus de 13 mille points de vente privés. Elle emploie plus de 8000 agents

1.1.1 Organigramme de l'entreprise :

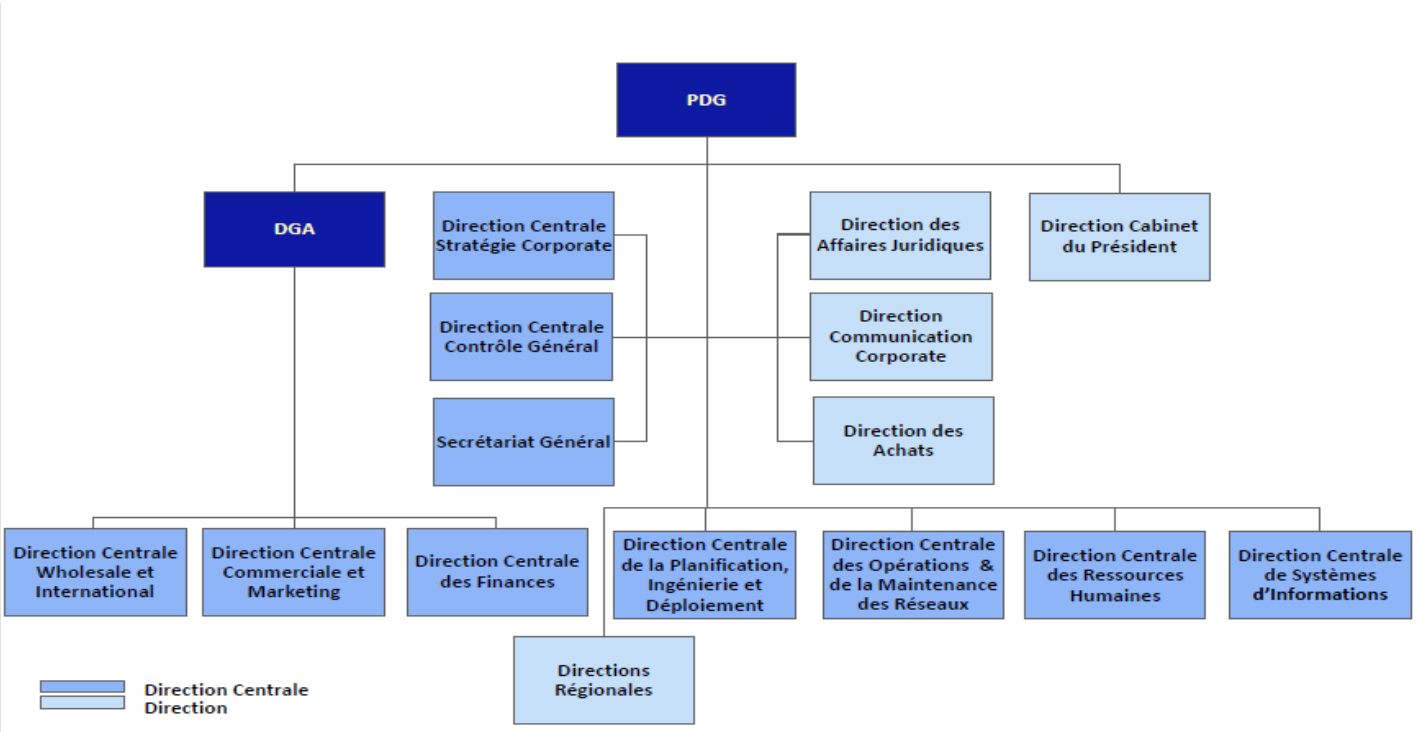

Figure 1: organigramme de Tunisie Télécom

1.2. Direction centrale des systèmes d'information (DCSI) :

Présentation de DCSI:

La Direction Centrale du système d'information (DCSI) a pour mission de :

- Piloter le système d'information de l'établissement (applications et infrastructures) en s'appuyant sur le Comité stratégique du système d'information (COSSI), instance principale de gouvernance du SI.
- Fais une liste avec des tirets pour les activités
- Être moteur dans l'élaboration du schéma directeur du système d'information (SDSI) et dans sa révision au fil des années
- Assister la direction et les services de l'établissement dans la définition de leurs besoins et dans la conduite des projets SI (fonction d'assistance à maîtrise d'ouvrage)
- Conduire la mise en œuvre des applications et des infrastructures informatiques dans le cadre de projets (fonction de maîtrise d'œuvre)
- Maintenir en condition opérationnelle et faire évoluer les infrastructures (réseau,¬ serveurs...) et les applications informatiques
- Fournir et maintenir en condition opérationnelle l'ensemble des postes informatiques ainsi que les moyens d'impression associés
- Accompagner les usages du numérique par l'assistance, la formation et la veille technologique
- Maintenir en condition opérationnelle et faire évoluer les salles informatiques pour l'enseignement (matériels et logiciels)
- Fournir aux étudiants un ensemble de services informatiques : accès au wi-fi, postes en libre-service, services de photocopie et d'impression, assistance...
- Tenir à jour l'inventaire physique de l'ensemble des matériels informatiques de l'établissement Mettre tous les moyens en œuvre pour garantir la sécurité du système d'information (SSI)

2. Etude de l'existant

2.1. Critique de l'existant et problématique

Avec le développement de l'utilisation d'Internet, de plus en plus d'entreprises ouvrent leur Système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet. On remarque qu'il y a une perte de temps et une disponibilité pas totale de l'information, alors ce type de projet qui à était lancer pour la première fois chez Tunisie Télécom permet de résoudre ses types de problèmes et d'ajouter des services locaux. Tunisie télécom dispose d'une multitude d'outils qui facilitent le travail en entreprise telque :

- **Serveur web**

1. Il permet à tous vos collaborateurs ou clients d'accéder aux applications et documents présents sur le serveur de votre entreprise via un simple navigateur internet. L'utilisateur à distance devra au préalable télécharger un logiciel pour accéder au serveur à distance. Idéal pour le télétravail. Le serveur web rend aussi votre accès à internet plus sécurisé.
2. Sauvegarder régulièrement la totalité de vos fichiers : Permet de limiter les risques de pertes de fichiers qui signifient perte de temps et d'argent pour votre entreprise. Évite aussi la nécessaire et régulière sauvegarde des fichiers sur un autre support qui avait pour but de limiter les risques de perte
3. Sécuriser les données, avec notamment la mise en place d'un mécanisme d'identification des utilisateurs (identifiant et mot de passe)

- **Serveur DNS**

DNS veut dire « Domain Name System » ou système de nom de domaine. un serveur DNS est un annuaire pour ordinateur. Lorsque vous voulez accéder à un ordinateur dans le réseau, votre ordinateur va interroger le serveur DNS pour récupérer l'adresse de l'ordinateur que vous voulez joindre. Une fois, que votre ordinateur aura récupéré l'adresse du destinataire, il

pourra le joindre directement avec son adresse IP. Le serveur DNS va permettre de faire la relation entre nom d'ordinateur et adresse

- **Serveur DHCP**

DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.

- **Autorité de Certification**

Utilisé dans le protocole HTTPS qui sert à accéder à un site internet de manière sécurisé car les données échangées entre le client et le serveur sont cryptées avec un algorithme de chiffrement asymétrique à clé publique / clé privée.

Du coup si un pirate récupère les informations échangées entre le client et le serveur (par exemple entre un acheteur et un site de vente en ligne au moment du paiement), il ne pourra rien en faire car il ne sera pas en mesure de déchiffrer les données.

La clé de voute de ce système c'est justement ce fameux certificat SSL qui est utilisé pour générer les clés de chiffrement (clé publique) et de déchiffrement (clé privée, qui ne transite par sur le réseau).

HTTPS ne peut pas fonctionner sans certificat SSL, les deux sont complètement liés, SSL fait partie du protocole https.

- **Problématiques**

On va essayer de répondre aux questions suivantes :

Comment résoudre les problèmes de transfert de fichier sur un réseau local ?

Comment résoudre les problèmes de configuration automatique de machine ?

Comment résoudre les problèmes de configuration dynamique de machine ?

2.2. Solution proposée

Dans un souci de gain de temps et de productivité de l'équipe Tunisie télecom, nous nous sommes donc intéressées à trouver une solution qui permet d'accélérer la procédure de déploiement d'un poste et la rendre totalement automatique, pour l'agent du ressource humaine qui traite tous les tâches d'intégration d'un nouvel employé

-La gestion des DNS est primordiale pour le bon fonctionnement des sites Web

-Les serveurs DHCP gèrent de façon centralisée les adresses IP et les informations associées et les fournissent automatiquement aux clients.

-Autorité de certification

Une Autorité de certification offre à un demandeur plusieurs types de certificats, selon les certificats qu'elle est habilitée à émettre et les autorisations de sécurité du demandeur. Elle utilise les informations disponibles pour faciliter la vérification de l'identité du demandeur. Elle publie sa liste de révocation dans un répertoire partagé.

-Infrastructure de Gestion de Clés

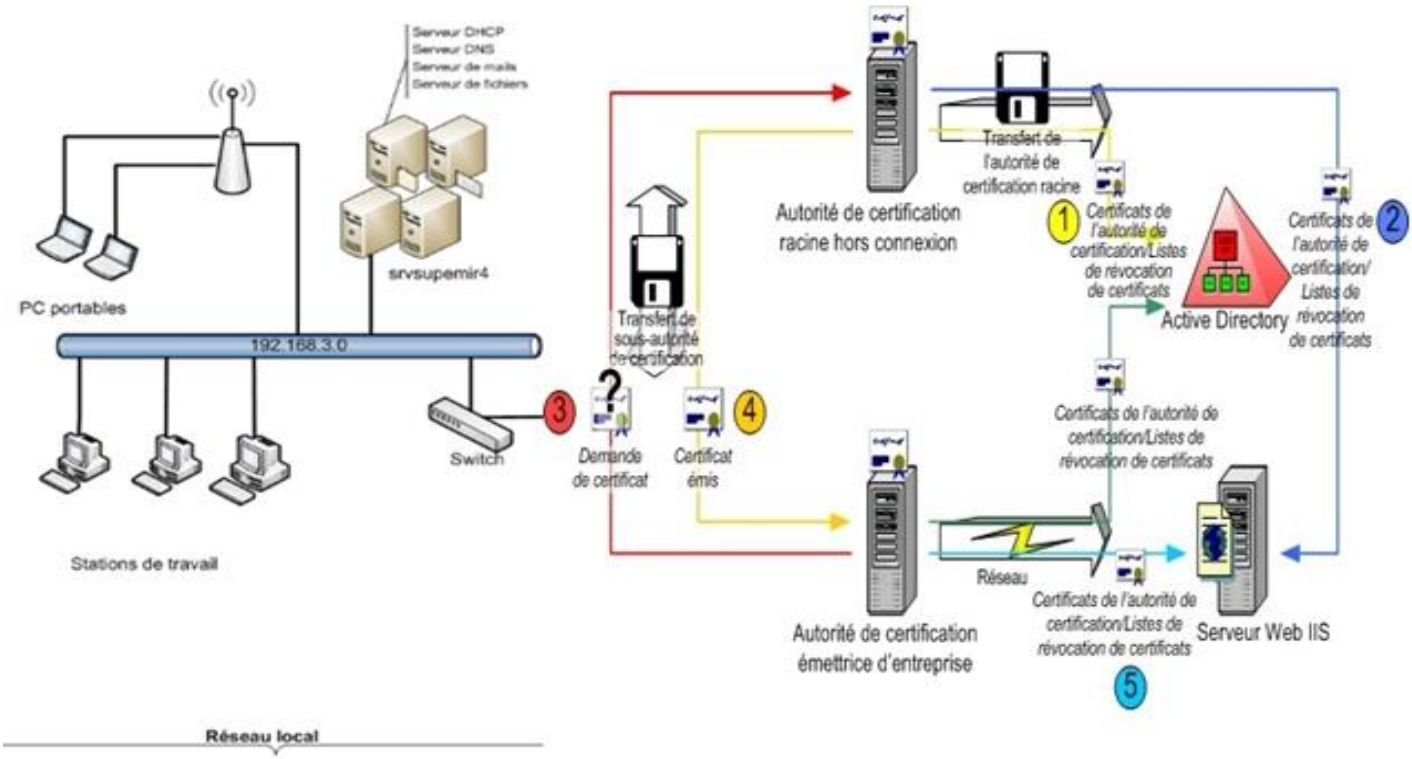

Figure 2:Architecture de la solution proposée

La solution est :

- préparer Active Directory pour l'infrastructure de clés publiques ;
- sécuriser les serveurs Windows pour les services de certificats ;
- installer et configurer une autorité de certification racine ;
- installer et configurer une autorité de certification émettrice ;
- activer l'inscription automatique des clients.

3 .Spécifications des besoins

3.1. Besoin fonctionnels

Les besoins fonctionnel Ces besoins peuvent concerner les contraintes d'implémentation :

Configuration d'un serveur DNS

Configuration d'un serveur DHCP

Configuration d'un serveur FTP

Configuration d'un serveur web

Configuration d'une autorité de certification

3.2. Besoin non fonctionnels

Les besoins non fonctionnels concernent les contraintes à prendre en considération pour mettre en place une solution adéquate aux attentes des concepteurs et des utilisateurs

Notre projet doit nécessairement assurer les besoins suivantes :

- La convivialité : La génération des certificats est simple

  L'interface du client FTP est facile à utiliser

- La performance : Réponse des serveurs FTP, DNS, et web est rapide

La génération des certificats est simple à manipuler

- Maintenable / flexible : la solution doit prendre en compte les évolutions.
- Exploitable : la solution doit être extensible et ouverte pour toute autre évolution ou ajout d'une autre fonctionnalité

4. Conclusion

Dans ce chapitre, on a présenté les besoins généraux de l'entreprise. On a essayé de proposer une solution adaptée à ces besoins. La spécification de cette solution nous a permis de bien comprendre les fonctionnalités attendues.

Chapitre 2 :
Etat de l'art

Dans ce chapitre nous allons détailler l'infrastructure Microsoft Active Directory. Cette section va englober le système d'annuaire Windows 2008, en l'introduisant par montrer le cadre général d'Active Directory, cette dernière permet de centraliser, de structurer, d'organiser et de contrôler les ressources réseau dans les environnements Windows server 2008. Et la présentation des différents services.

1. Active Directory

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP (Lightweight Directory Access Protocol un protocole du service d'annuaire utilisé pour interroger et mettre à jour Active Directory) pour définir comment s'établit la communication (Client-serveur) 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.

Le service d'annuaire AD peut être mis en œuvre sur Windows Server 2003 , il résulte de l'évolution de la base de compte plane SAM (Security Account Manager).

Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine .

2. Structure Active Directory

La structure logique et physique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie.

Dans cette section, nous s'allons vous proposer un aperçu des principaux outils de construction d'entreprise d'Active Directory bénéficient de tous les outils, mais également d'une panoplie supplémentaire, dont font parties Structure logique et physique. [1]

2.1. Structure logique

Les composants logiques de la structure d'Active Directory sont les suivants :

2.2. Domaine

Unité de base de la structure Active Directory, un domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine à un nom unique sur le réseau, doit concevoir une liste d'information concernant les utilisateurs (nom, Mot de passe et personne autorisés à utiliser les systèmes). Des que vous avez plusieurs

ordinateurs vous allez tomber sur un système d'exploitation : « Comment partager cette liste avec tous les ordinateurs de l'entreprise ? ».

- Il faut pour cela installé un petit nombre de serveurs appelés contrôleur de domaine, avec une base de données de vos utilisateurs.
- La notion de sécurités intervient lorsque vous avez plusieurs domaines.

Un domaine regroupe un ensemble de ressources qui seront administrées de manière centralisée par le biais des contrôleurs de domaine. Le domaine Active Directory est basé sur le service DNS (Domain Name System), ainsi un domaine sera délimité par un nom DNS commun.

Afin d'assurer la compatibilité avec les clients (membres d'un domaine) antérieurs à Windows 2008, Active Directory supporte également un nom NetBIOS de domaine, ce type de domaine contient uniquement des objets de type utilisateur, groupe ou ordinateur et ne comprend qu'un seul niveau.

2.3. Construire des structures multi-domaine : « les arbres de domaine »

Un arbre Active Directory est composé de plusieurs domaines reliés par le biais d'approbations transitives bidirectionnelles.

- Le premier domaine Active Directory que vous créez est appelé : racine de l'arbre.
- Les domaines situés au dessous sont appelés : domaines enfants.

Tous les domaines d'un arbre partagent une définition formelle de tous les types d'objets appelée Schéma. Par ailleurs, le catalogue global (GC) est partagé par tous les domaines de n'importe quel arbre.

Active Directory vous aide en créant automatiquement des relations d'approbation entre chaque domaine et ces domaines enfants. Cette relation d'approbation bidirectionnelle permet à deux domaines de s'approuver mutuellement. Ainsi le domaine A approuve le domaine B et le domaine B approuve le domaine A.

On dispose de trois domaines nommés A, B et C. A approuve B et B approuve C. La relation d'approbation transitive implique donc que A approuve C.

Vous pouvez décider de diviser votre organisation de différente manière ou autrement dit suivant des critères de décomposition qui peut être :

- Le critère géographique, consiste à représenter chaque zone géographique de l'entreprise par un réseau logique différente.

- Le critère organisationnel, chaque organisation correspond à un réseau logique.
- Le critère fonctionnel, chaque fonction de l'entreprise correspond à un réseau logique.
- Le critère hybride, consiste à faire la création des réseaux logiques sur la base d'une combinaison des critères de décomposition.

2.4. Structure physique

Les concepts évoqués précédemment décrivent la structure logique d'Active Directory, ensuite les composants physiques de la structure d'Active Directory sont les suivants :

2.5. Contrôleur de domaine

Un contrôleur de domaine est un ordinateur exécutant Windows 2008 qui stocke les données de l'annuaire et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches d'annuaire.

Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Dans le cas d'une société constituée de plusieurs entités dispersées géographiquement, on aura besoin d'un contrôleur de domaine dans chacune de ses entités.

Lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, le premier site et vous installez Active Directory.

⇨ Les contrôleurs de domaine sont créés à l'aide de l'Assistant Installation de Active Directory. [3]

3. Infrastructure Active Directory

Active Directory fournit un emplacement central pour l'administration réseau et de sécurité. Il authentifie et autorise tous les utilisateurs et les ordinateurs dans un domaine de type réseau Windows-attribution et l'application de politiques de sécurité pour tous les ordinateurs et l'installation ou la mise à jour du logiciel.

Active Directory utilise DNS et KERBEROS.

3.1. Domain Name System

Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

Le système DNS fournit les principales fonctions ci-dessous sur un réseau exécutant Active Directory :

- Résolution de noms : le système DNS résout les noms d'hôtes en adresses IP. Par exemple, un ordinateur nommé labo-1 désirant se connecter à un autre ordinateur nommé labo-2 enverra une requête au serveur DNS qui lui renverra l'adresse IP de labo-2. Le système DNS peut aussi effectuer une résolution de nom inversée, c'est-à-dire fournir le nom d'hôte à partir de l'adresse IP qui lui est communiquée.

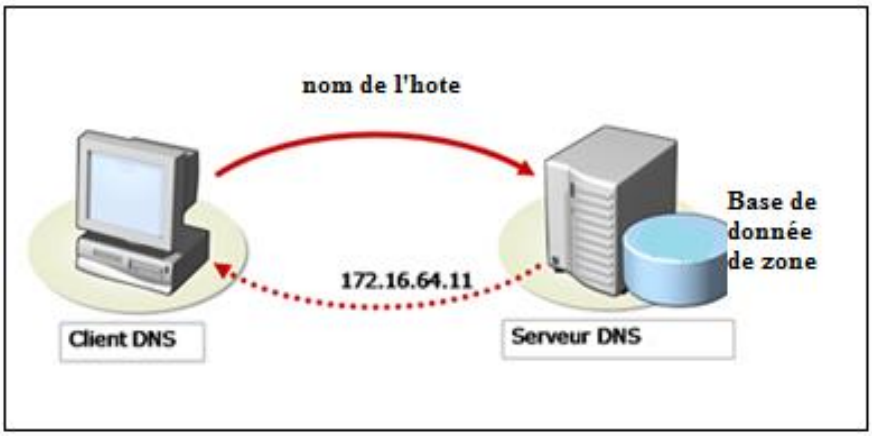

Figure 3:Résolution de nom

- Convention de dénomination : Active Directory emploie les conventions de dénomination du système DNS.
- Localisation des composants physiques d'Active Directory : Le système DNS identifie les contrôleurs de domaine par rapport aux services spécifiques qu'ils proposent comme l'authentification d'une connexion ou la recherche d'informations dans Active Directory. Lors de l'ouverture d'une session, une machine cliente doit s'adresser à un contrôleur de domaine, seul capable de l'authentifier. Le système DNS pourra lui fournir l'emplacement de l'un de ces contrôleurs de domaine. [10]

3.1.1. Les enregistrements de ressource

Dans un environnement Microsoft, les mappages nom d'hôte / adresse IP et adresse IP / nom d'hôte sont appelés enregistrements de ressources. On distingue plusieurs types d'enregistrements de ressources. Voici la liste des principaux types :

- **A** : qui fait correspondre un nom d'hôte à une adresse IPv4.
- **CNAME** : qui permet de faire un alias vers un enregistrement A.

- **MX** : qui définit les serveurs de messagerie.
- **PTR** : qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit « reverse » puisque il fait exactement le contraire du A record.
- **NS** : qui définit les serveurs DNS de ce domaine.
- **SOA** : donne les informations générales de la zone.
- **SRV** : permettent de mapper un nom d'hôte à un type de service donné.
- **HINFO** : spécifient le type de processeur et le système d'exploitation correspondant à un nom d'hôte.
- **WINS** : indiquent au serveur DNS l'adresse IP d'un serveur WINS a contacté en cas d'échec lors de la résolution de nom d'hôte. Les enregistrements WINS ne peuvent être crée que dans une zone de recherche directe.
- **WINS-R** : ne peuvent être crée que dans une zone de recherche inversée. [4][5]

3.1.2. Les différentes zones Domain Name System

Une zone de noms ou zone DNS est un ensemble d'enregistrements de ressources appartenant à la même portion de l'espace de noms DNS. Par exemple une zone DNS peut contenir l'ensemble des enregistrements de ressource de type A (c'est-à-dire des mappages noms d'hôte / adresses IP) du domaine Mydomain.intra. Il existe quatre types de zones DNS :

- **Zone principale:** peuvent ajouter, modifier et supprimer des enregistrements de ressource.
- **Zone secondaire:** sont des copies en lecture seule d'une zone principale donnée. Un serveur DNS qui héberge une zone secondaire ne peut pas ajouter ni modifier d'enregistrements de ressource. Les zones secondaires ont donc pour seul intérêt de garantir une tolérance aux pannes.
- **Zone de stub:** sont des copies partielles d'une zone. Elles contiennent uniquement les enregistrements de ressource de type SOA, NS et A.
- **Zone intégrée à Active Directory**: Les données d'une zone intégrée à Active Directory peuvent être répliquées sur des contrôleurs de domaine, même si le rôle DNS n'est pas installé sur le contrôleur de domaine.

  Si le serveur est un contrôleur de domaine en lecture seule, un processus local ne peut pas écrire dans les données.
- émet un TGT pour le client. . [4][6]

3.1.3. Groupe d'utilisateurs et ordinateurs

L'Active Directory offre un bien, qui consiste à crées un type de compte spéciale qui n'est ni un compte utilisateur ni un compte ordinateur, et qui parle le nom de groupe. Les groupes sont utilisés pour simplifier l'administration. Ils contiennent un ensemble de comptes d'utilisateurs et d'ordinateurs possédant des besoins identiques en termes d'administration sont également appelés entités de sécurité.

Un compte d'utilisateur ou d'ordinateur permet d'effectuer les opérations suivantes :

- Authentifier l'identité de l'utilisateur ou de l'ordinateur par un Mot de passe.
- Autoriser ou refuser l'accès aux ressources du domaine en fonction des autorisations explicites qui lui sont attribuées pour chaque ressource
- Administrer d'autres entités de sécurité par le domaine local, Active Directory crée un objet « entité de sécurité externe » qui représente chaque entité de sécurité d'un domaine externe approuvé.

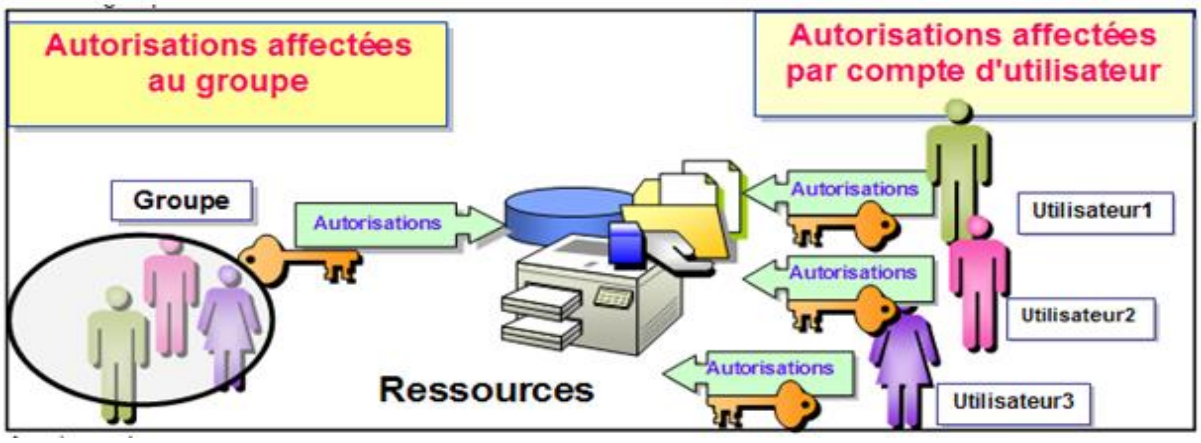

Figure 4:Autorisation affectées au groupe et par compte utilisateur

Ainsi, un administrateur pourra simplement donner des permissions au groupe plutôt que de les donner individuellement à chaque utilisateur.

Les permissions et droits assignés à un groupe sont répercutés sur tous les utilisateurs de ce même groupe. De la même manière, un utilisateur cumule les droits ou restrictions des groupes auxquels il appartient.

3.1.4. KERBEROS

C'est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.

Le protocole KERBEROS fournit une authentification mutuelle plus rapide et une approbation transitive pour l'authentification en n'importe quel point d'une arborescence d'un domaine.

Dans un réseau simple utilisant KERBEROS, on distingue plusieurs entités :

- le client (C).
- le serveur (S).
- le service d'émission de tickets (TGS pour Ticket-Granting Service).
- le centre de distribution de clés (KDC pour Key Distribution Center).

Un ticket est une structure de données constituée d'une partie chiffrée et d'une partie claire.

Les tickets servent à authentifier les requêtes des principaux. Il existe 2 types de Tickets :

- Ticket Granting Ticket (TGT)
- Service Ticket (ST).

➢ Les services KERBEROS

Deux types de services sont requis :

- Un service d'authentification (AS): le client se connecte en envoyant La requête initiale contient (en clair) l'identité du requérant et les serveurs pour lequel on demande un TGT. Le serveur alors émet un TGT pour le client.

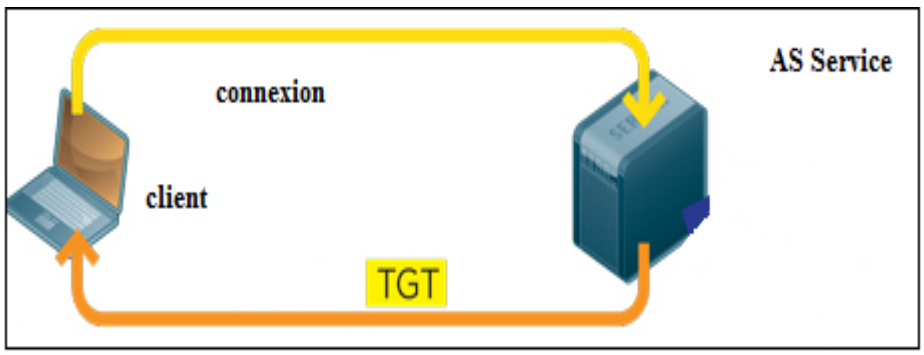

Figure 5:Demande d'un ticket

- Un service d'octroi de tickets (TGS) : le client utilise le TGT obtenue précédemment pour requérir un ST. Le serveur alors émet un ST.

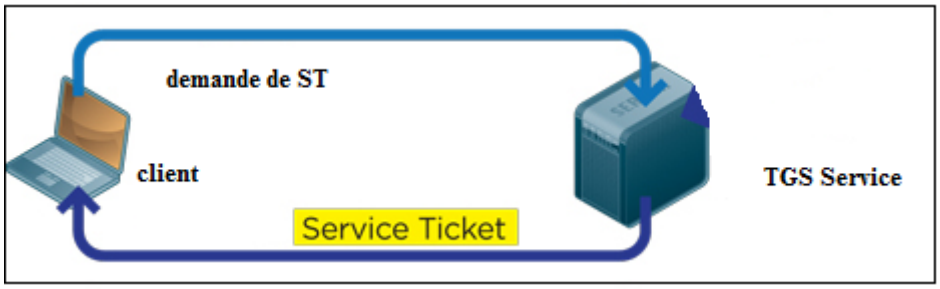

Figure 6:Demande d'un ticket ST

Ces services ne tournent pas nécessairement sur le même serveur. [7][8][9]

4. FTP

a. Définition

Le File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de Communication destiné à l'échange de fichiers sur un réseau. Il permet de copier des fichiers du Serveur vers le client et inversement (selon les droits).Il est notamment utilisé pour d'alimenter les pages d'un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur [11].

b.Rôle de FTP

Permettre le transfert de fichiers entre deux ordinateurs distants. Il sert essentiellement au partage de fichiers sur machines distantes. Il permet surtout de procéder au transfert des données de manière efficace. En effet, en plus de faire transiter des données, ce protocole contrôle et gère la qualité des opérations effectuées. [11]

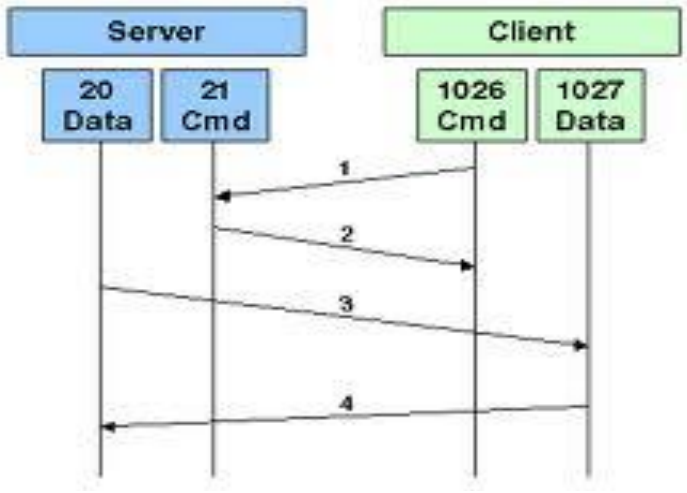

Figure 7:Principe de fonctionnement du FTP

c.Authentification

L'authentification permet de déterminer qui peut accéder aux ressources sur un serveur Web. FTP 7.5 prend en charge les méthodes d'authentification basée sur les stimulations suivantes :

- Authentification anonyme (désactivée par défaut)
- Authentification de base (désactivée par défaut)

5. DHCP

a. Rôle d'un service DHCP

Un serveur DHCP (Dynamic Host Configuration Protocol) a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée. Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau), un serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin. Tous les nœuds critiques du réseau (serveur de nom primaire et secondaire, passerelle par défaut) ont une adresse IP statique ; en effet, si celle-ci variait, ce processus ne serait plus réalisable [12].

Figure 8:Principe de fonctionnement du DHCP

6. web

a. Définition

Un serveur Web est un ordinateur disposant d'un logiciel spécifique qui lui permet d'accepter des demandes d'ordinateurs clients et de renvoyer des réponses à ces demandes. Un serveur Web permet de partager des informations via Internet ou via des réseaux intranet et extranet [13].

b. Rôle d'IIS

Le rôle de Serveur Web (IIS) dans Windows Server 2008 vous permet de partager des informations avec des utilisateurs sur Internet, sur un intranet ou un extranet. Windows Server 2008 met à votre disposition IIS, qui est une plateforme Web unifiée intégrant IIS, ASP.NET et Windows Communication Fondation. Les principales fonctionnalités et améliorations dans IIS sont les suivantes :

- Extensions intégrées
    - WebDAV et FTP
    - Filtrage des demandes
    - Modules Pack d'administration
- Améliorations de la gestion

- Sécurisation renforcée des services
- Comptes de services gérés
- Instance principale Web

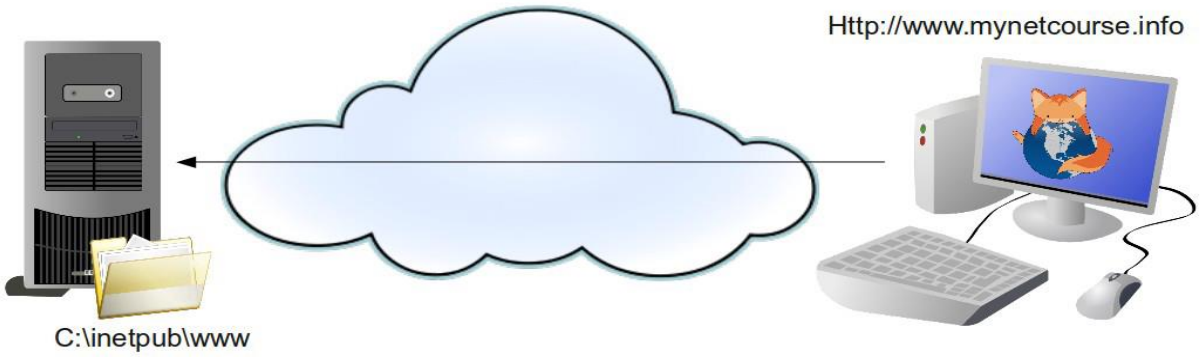

Figure 9:Principe de fonctionnement du web IIS

7. Conclusion

Avec ce chapitre on conclure la partie théorique et dans un deuxième temps nous allons développer la partie pratique dont on commence l'implémentation du service Active Directory.

Chapitre3 :

Infrastructure de clé publique

L’objectif de ce chapitre est de mettre en œuvre l’infrastructure de clé publique (PKI), ainsi que ça structure, ces composantes et son organisation. Il s’agit ici de faire une étude détaillée de cette infrastructure et de la présenter comme une infrastructure qui se construit, donc une structure à la fois technique et administrative.

1. Infrastructure de clé publique

PKI (Public Key Infrastructure) est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur.

Donc l’infrastructure PKI fournit trois services principaux:

- Certification de clé publique et publication de certificats.
- Révocation de certificats.
- Gestion la fonction de certification.

Techniquement l’infrastructure à clé publique utilise des mécanismes de signature et certifie des clés publiques qui permettent de chiffrer et de signer des messages ainsi que des flux de données.

PKI délivre des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique qui offrent les garanties suivantes lors des transactions électroniques :

- Confidentialité : seul le destinataire (ou le possesseur) légitime d'un bloc de données ou d'un message pourra en avoir une vision intelligible ;
- Authentification : lors de l'envoi d'un bloc de données ou d'un message ou lors de la connexion à un système, on connaît sûrement l'identité de l'émetteur ou l'identité de l'utilisateur qui s'est connecté ;
- Intégrité : on a la garantie qu'un bloc de données ou un message expédié n'a pas été altéré, accidentellement ou intentionnellement ;
- Non-répudiation : l'auteur d'un bloc de données ou d'un message ne peut pas renier son œuvre. [14][15]

1.1. Certificat numérique

Un certificat numérique aussi appelé certificat électronique ou certificat de clé publique peut-être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier une entité physique ou morale, mais aussi pour chiffrer des échanges.

Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique.

Le standard le plus utilisé pour la création des certificats numériques est le

Les certificats contiennent des informations telles que :

- Un nom qu'indique à qui ou à quoi il appartient. Si le certificat est émis par une autorité de certification intégrée aux services d'annuaire d'Active Directory.
- Une copie de clé publique issue d'une paire de clé cryptographique.
- Le nom de l'autorité de certification qui à émis le certificat.
- La ou les raisons pour lesquelles on utilise un certificat.
- La signature de l'autorité de certificat qui à émis le certificat. [16]

1.1.1. Cryptographie

L'art et la science de garder un secret est appelé cryptographie. La cryptographie dans les applications téléinformatiques doit assurer la confidentialité, l'authentification, l'intégrité des données et le non désaveu.

Il existe deux types de cryptage : le cryptage symétrique et le cryptage asymétrique. Seul le cryptage asymétrique nécessite l'utilisation de certificats numériques.[16]

1.1.1.1. Cryptage symétrique

Les algorithmes à clé symétrique ou secrète sont des algorithmes où la clé de cryptage peut être calculée à partir de la clé de déchiffrement. Dans la plupart des cas, la clé de cryptage et la clé de décryptage sont identiques. Pour de tels algorithmes, l'émetteur et le destinataire doivent se mettre d'accord sur une clé à utiliser avant d'échanger des messages cryptés.

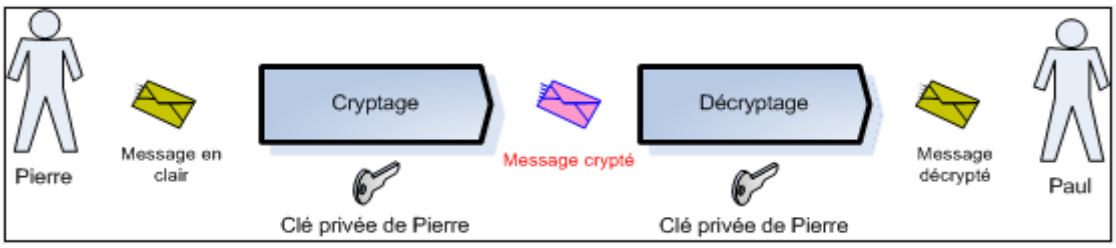

Figure 10:clé symétrique

Dans cette figure la clé doit être gardée secrète. La sécurité d'un algorithme à clé symétrique repose intégralement sur non divulgation de cette clé : si celle ci est dévoilée, n'importe qui peut chiffrer ou déchiffrer les messages.

1.1.1.2. Cryptage asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

Les PKI permettent l'obtention de ces garanties par l'application de processus de vérification d'identité rigoureux et par la mise en œuvre de solutions cryptographiques fiables (éventuellement évaluées), conditions indispensables à la production et à la gestion des certificats numérique.

Le cryptage asymétrique s'appui sur un couple de clés composé d'une clé publique permettant à n'importe qui de crypter un message, un destinataire muni de sa propre clé privée. La clé publique est donc largement diffusée dans le réseau (local, Internet, …) et permet le cryptage du message alors que la clé privée, qui doit rester confidentielle, permet à son possesseur de déchiffrer tous les messages encryptés à l'aide de la première.

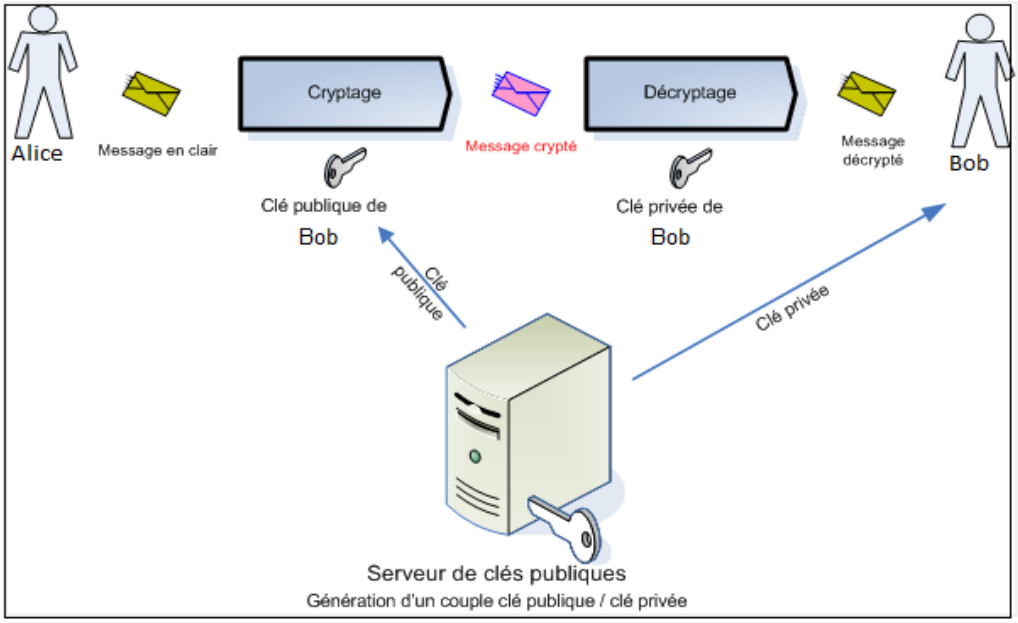

Figure 11:Clé asymétrique

Sur ce schéma on constate que le serveur de clés publiques va générer à la demande de Bob un couple de clé publique / clé privée. Il transmettra la clé privée à Bob et partagera à tout le monde la clé publique. Alice crypte le message avec la clé publique de Bob obtenu sur le serveur et transmet le message sur le réseau. Lorsque Bob le reçoit, il pourra le déchiffrer grâce à sa clé privée.

Un message chiffré avec une clé publique donnée ne peut être déchiffré qu'avec la clé privée correspondante.

- RSA exemple d'algorithme à clé asymétrique.

Il existe différents algorithmes asymétriques. L'un des plus connus est le **RSA** (de ses concepteurs Rivest, Shamir et Adleman). Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés et pour chiffrer les emails. Il est dans le domaine public.

Un utilisateur de RSA crée et publie ensuite le produit de deux grands nombres premiers , avec une valeur auxiliaire, comme leur clé publique. Les facteurs premiers doit être gardée secrète. N'importe qui peut utiliser la clé publique pour chiffrer un message, mais avec des méthodes actuellement publiés, si la clé publique est assez grande, seule une personne ayant connaissance des facteurs premiers peuvent en pratique en décoder le message.

En fait, on utilise jamais les algorithmes asymétriques pour chiffrer toutes les données, car ils sont trop longs à calculer : on chiffre les données avec un simple algorithme symétrique dont la clé est tirée au hasard, et c'est cette clé qu'on chiffre avec un algorithme asymétrique comme le RSA.

1.1.1.3. Pourquoi utiliser un certificat numérique ?

Un certificat numérique permet, lors d'un cryptage asymétrique, de garantir lorsque cela s'avère nécessaire, l'identité des différents intervenants. Prenons l'exemple de l'envoi d'un message crypté de manière asymétrique entre trois utilisateurs.

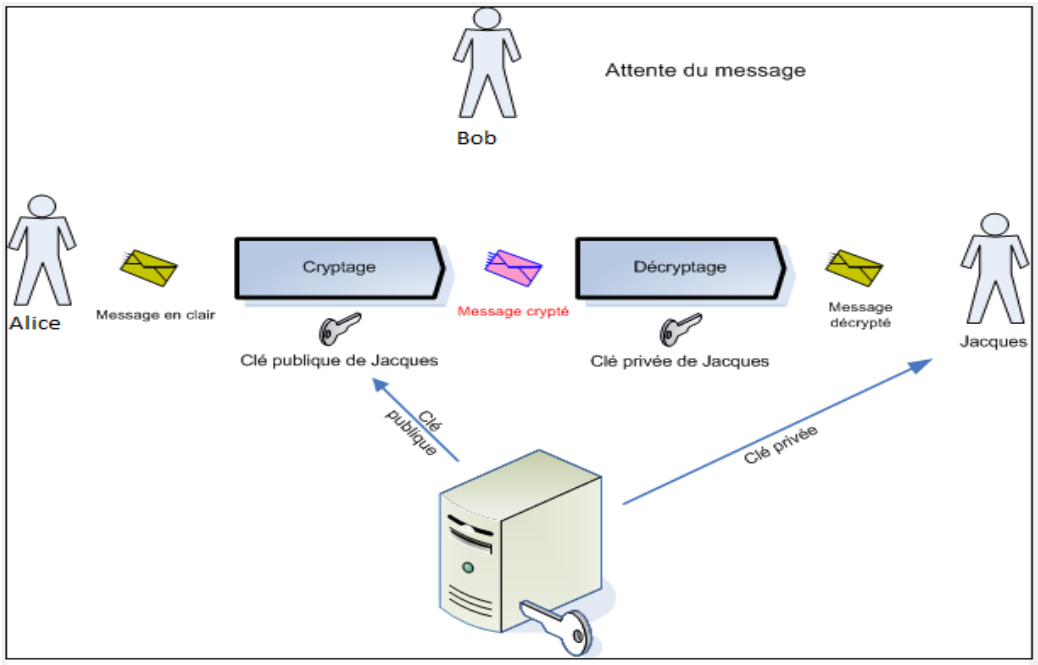

Figure 12:Serveur des clés publiques sans certificat numérique

Dans ce cas, Alice veut transmettre des informations confidentielles à Jacques. Il va donc récupérer auprès du serveur de clés publiques la clé de cryptage qu'il pense être celle de Jacques. Malheureusement, sans certificat (donc sans carte d'identité) l'identité du propriétaire de la clé publique n'est pas garantie. Alice va donc crypter le message avec la clé publique qu'il pensera être celle de Jacques mais qui appartiendra en réalité à Bob le pirate. Bob n'aura donc plus qu'à récupérer le message et pourra le décrypter sans aucun problème avec sa propre clé privée.

Dans le cas de l'utilisation d'un certificat numérique, Alice se serait aperçu que la clé publique ne pouvait pas appartenir à Jacques et n'aurait donc pas transmis son message. [15][16][17]

2. La norme X.509

Il existe un nombre considérable de normes et de standards qui régissent les certificats, la signature électronique, l'identification des algorithmes cryptographiques, les messages signés, etc. Nous nous focaliserons dans ce paragraphe sur celles qui seront utiles dans la suite.

Les PKI reposent initialement sur la norme X.509 de cryptographie de l'Union internationale des télécommunications . X.509 établit entre autres les formats standards de certificats numériques et un algorithme pour la validation de chemin de certification.

X.509 a été créé en 1988 dans le cadre de la norme X.500. Il repose sur un système hiérarchique d'autorités de certification, à l'inverse des réseaux de confiance (comme PGP Pretty Good Privacy en français : « Assez Bonne Intimité » ou « Assez Bonne Vie privée », plus connu est un logiciel de chiffrement et de déchiffrement cryptographique), où n'importe qui peut signer (et donc valider) les certificats des autres. Il existe un nombre considérable de normes et de standards qui régissent les certificats, la signature électronique, l'identification des algorithmes cryptographiques, les messages signés, etc. Nous nous focaliserons dans ce paragraphe sur celles qui seront utiles dans la suite. [18][19]

Figure 13:Certificat X.509 au format PEM

2.1. Signature numérique

La signature numérique (parfois appelée signature électronique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- Authentique : L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Infalsifiable : La signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
- Non réutilisable: La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- Inaltérable : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- Irrévocable : La personne qui a signé ne peut le nier.

La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres.

Le principe de la signature électronique repose sur deux familles d'algorithmes, qui seront utilisés de manière complémentaire des algorithmes de chiffrement dit « asymétriques » ou à « clé publique » et des fonctions de hachages.

Elle dispose elle même d'un certificat, soit auto-signé, soit signé par une autorité de niveau supérieur.

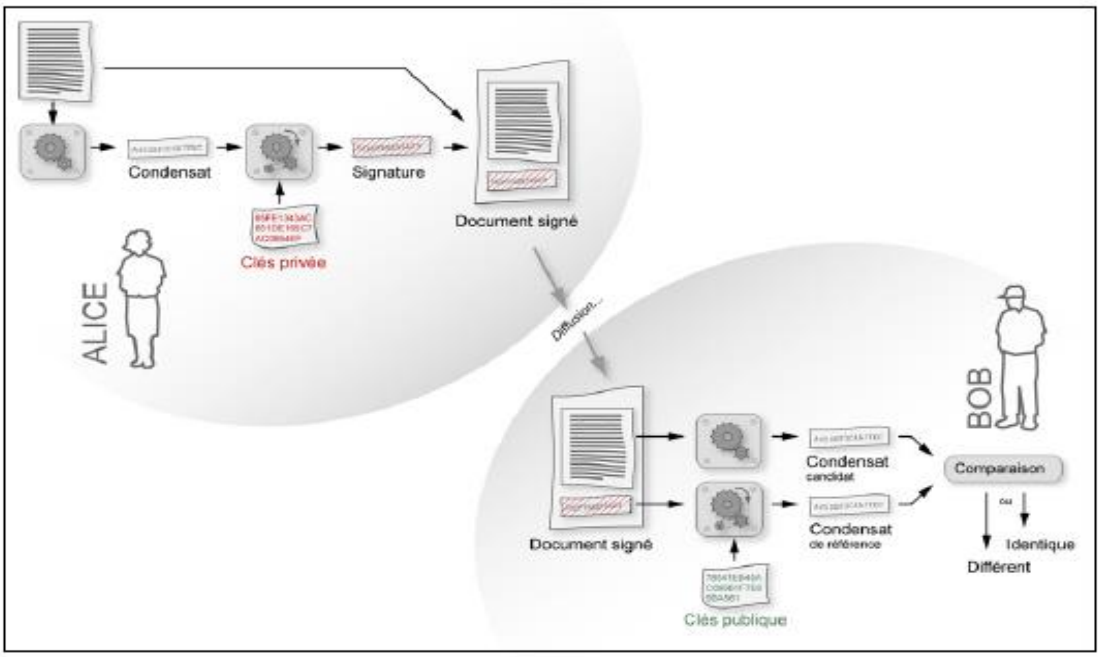

Figure 14:Principe algorithmique de la signature électronique

Dans la signature nous avons une bi-clé : une clé (privé) pour la création de signature et une clé (publique) pour la vérification de signature, pour signer un message voici comment se passe:

- A l'aide de la clé privée de signature de l'expéditeur, une empreinte connue sous le nom "message digest" est générée par hachage en utilisant l'algorithme SHA-1) ou MD5 (Message Digest 5), le plus utilisé étant SHA-1. Cette empreinte est ensuite cryptée avec cette clé privée de signature.
- On joint au message l'empreinte et le certificat contenant la clé publique de signature.
- Le destinataire vérifie la validité du certificat et son non révocation dans l'annuaire.
- Le destinataire transforme l'empreinte avec la clé publique de signature ainsi validée. Cette opération permet de s'assurer de l'identité de l'expéditeur.
- Ensuite le destinataire génère une empreinte à partir de message reçu en utilisant le même algorithme de hachage. Si les deux empreintes sont identiques, cela signifie que le message n'a pas été modifié.

1.2 Organisation d'une PKI

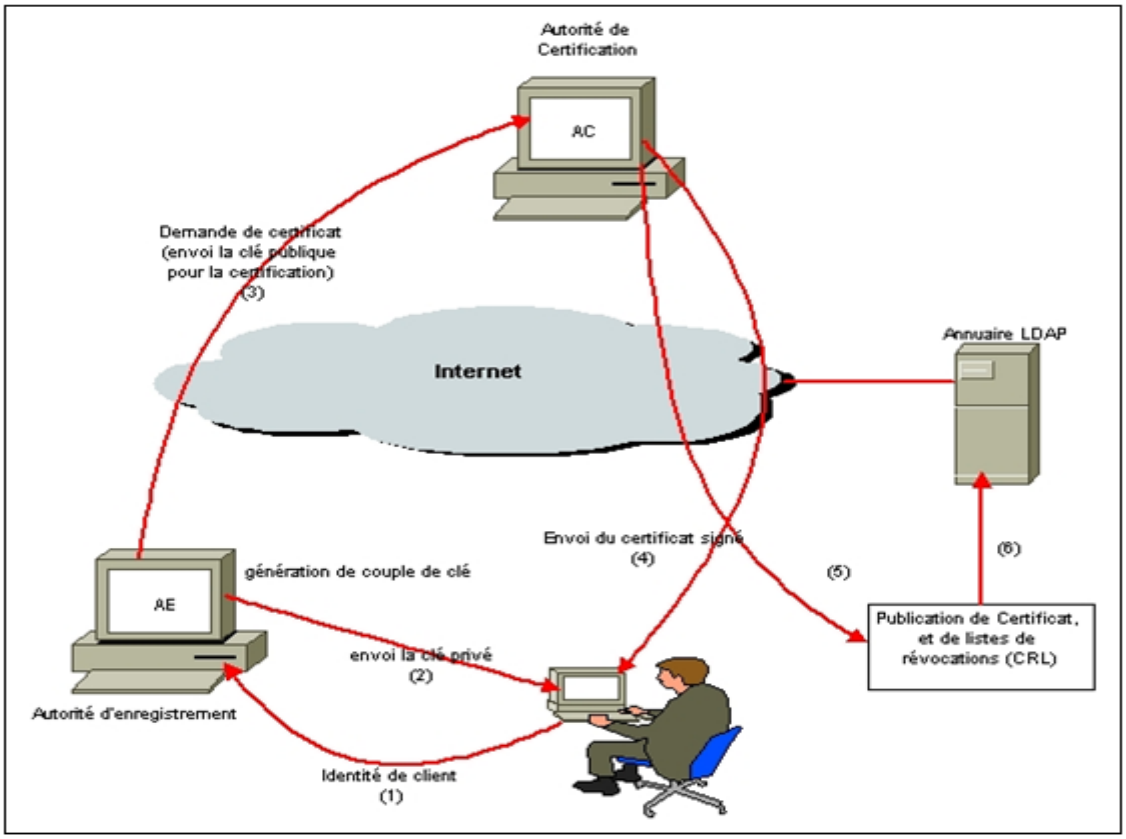

Figure 15:Organisation d'une PKI

Dans une infrastructure à clé publique ; pour obtenir un certificat numérique, l'utilisateur fait une demande auprès de l'autorité d'enregistrement. Celle-ci génère un couple de clé (clé publique, clé privée), envoie la clé privée au client, applique une procédure et des critères définis par l'autorité de certification qui certifie la clé publique et appose sa signature sur le certificat, parfois fabriqué par un opérateur de certification.

- Composants d'une infrastructure de clé publique

Une infrastructure de clé publique représente la somme des composants implémentés sur un réseau pour offrir des services de certificats. Les services de certificats comprennent l'émission, l'utilisation et la maintenance des certificats. Ils définissent les composants d'une infrastructure de clé publique nécessaire pour mettre en œuvre de manière sure ces services de certificats sur votre réseau.

Cette infrastructure se compose de quatre éléments essentiels :

- Une Autorité d'Enregistrement (Registration Autorités) : c'est cette autorité qui aura pour mission de **traiter les demandes de certificat** émanant des utilisateurs et de générer les couples de clés nécessaires (clé publique et clé privée). Son rôle peut s'apparenter à la préfecture lors d'une demande de carte d'identité.
- Une Autorité de Certification (Certification Autorités) : elle reçoit de l'Autorité d'Enregistrement les demandes de certificats accompagnées de la clé publique à certifier. Elle va **signer à l'aide de sa clé privée** les certificats, un peu à la manière de la signature de l'autorité sur une carte d'identité. Il s'agit du composant le plus critique de cette infrastructure en raison du degré de sécurité requis par sa clé privée.
- Une Autorité de Dépôt (PKI Repositories) : il s'agit de l'élément chargé de **diffuser les certificats numériques** signés par la CA sur le réseau (privé, Internet, etc.).
- Les utilisateurs de la PKI : ce sont les **personnes effectuant des demandes** de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu [18][19]

3. Conclusion

Dans ce chapitre, nous avons précisé que l'infrastructure de clé publique est un ensemble de technologies, procédures et pratiques qui supportent l'implémentation et l'exploitation des certificats basés sur la cryptographie à clé publique.

Chapitre 4 : Réalisation

Dans ce chapitre, nous proposons tout d'abord de présenter l'environnement logiciel et matériel de l'implémentation ADS. Par la suite, nous exposons les principaux choix d'implémentation que nous avons retenus. Puis, nous passons en revue les tâches réalisées. Enfin, nous présentons les étapes de la mise en place de notre réseau. Dans ce contexte, nous précisons l'administration d'une ou plusieurs tâches dans Active Directory peut aller de tâches simples comme la gestion des comptes utilisateurs du domaine, à des actions plus complexes comme la gestion du contrôleur de domaine.

1. Environnement d'exploitation (Virtual PC 2007)

Le déploiement de Windows Server 2008 et Windows XP Professional peut être implémenté dans un environnement d'entreprise ou comme dans notre cas de configuration, peut s'appliquer dans un environnement virtuel à l'aide de technologies de virtualisation telles que Microsoft Virtual PC 2007.

On va créer alors 2 machines Virtual sur Microsoft Virtual PC 2007 :

- Un serveur (contrôleur de domaine) nommé « **MyServer** ».
- Une station de travail nommé « **MyStation** ».

On a de même déterminé la mémoire physique recommandée et d'espace disque pour un échantillon de systèmes d'exploitation invités selon la taille de disque dur de notre machine 3Go comme suit :

- Windows XP Professional
- Windows Server 2008 Enterprise.

1.1. Installation Windows Server 2008

Pour mettre en évidence notre infrastructure PKI, nous allons commencer par établir une infrastructure réseau commune via l'installation de Windows Server 2008, la configuration d'Active Directory, l'installation d'une station de travail Windows XP Professionnel et l'ajout de cette station de travail à un domaine.

1.1.1. Processus d'installation

Nous allons commencer l'installation du serveur sous Microsoft virtuel PC 2007 afin de remplir les conditions nécessaires et de préparer celui-ci à l'installation d'Active Directory, et du serveur DNS.

Pour installer Windows 2008 Server, on suit les étapes de configuration d'un système d'exploitation dans un environnement virtuel :

Pour la partie réseau, la tâche la plus importante consiste à mettre en place la configuration du protocole TCP/IP.

La configuration de protocole TCP/IP peut être faite manuellement comme indique ou automatique à travers un serveur DHCP (Dynamic Host Configuration Protocol) qui est implanté dans un équipement réseau (généralement un routeur, mais ca peut être un point d'accès sans fils par exemple) ou dans un PC (généralement un serveur réseau) qui attribue automatiquement une adresse IP unique à tous les PC connectés au réseau local dans une plage donnée. Ceux-ci doivent obligatoirement configuré en IP dynamique. Cette fonctionnalité simplifiée la configuration IP d'un réseau interne.

Le serveur DNS exige une adresse IP statique.

Pour les ordinateurs clients par contre ils peuvent être configuré avec en serveur DHCP

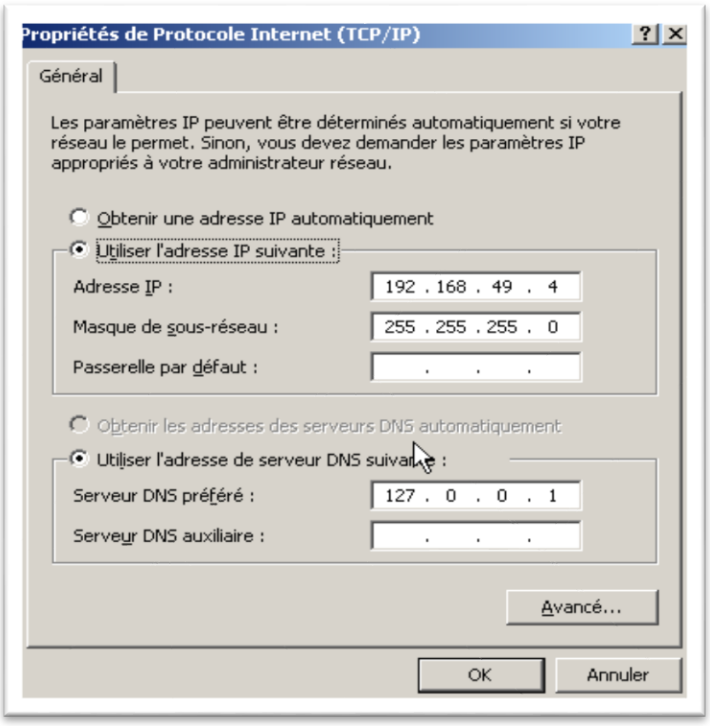

Figure 16:Mise en place de protocole TCP/IP

Dans la liste, il est réputé d'indiquer au début l'appartenance de cet ordinateur à un « WORKGROUP ».

Et comme notre machine sera un Contrôleur de Domaine alors il ne sera pas membre d'un domaine donc gardez par défaut **« Non cet ord…… »** Et **WORKGROUP**

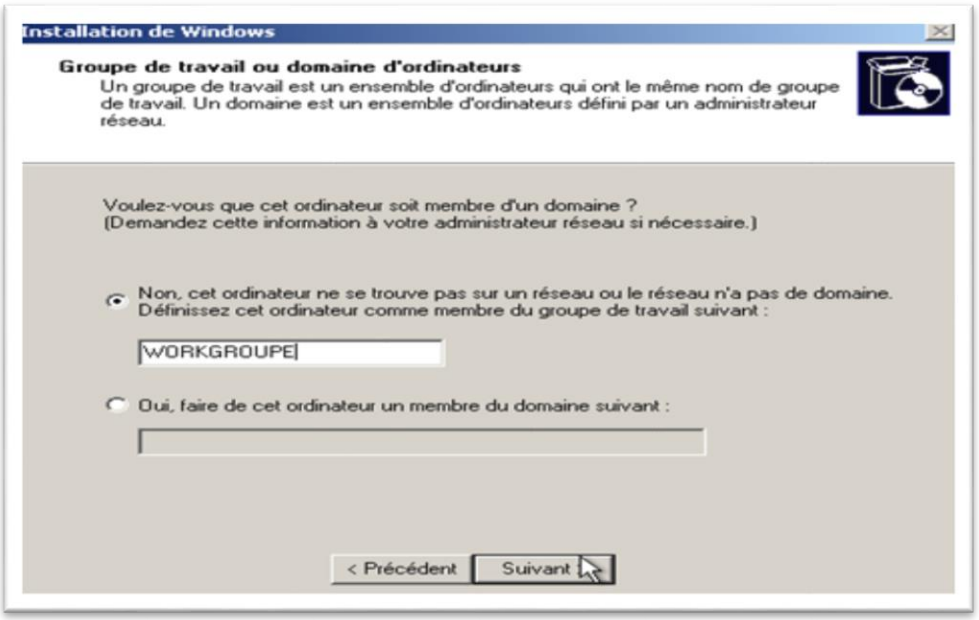

Figure 17:Configuration l'appartenance d'ordinateur

L’installation se poursuit par la copie des fichiers et se finalise.

1.1.2. Déploiement d’Active Directory

Les composants critiques définis dans une PKI nécessitent un stockage organisé et une facilement accessibilité. Le service d’annuaire peut participer à cette tâche en assurant une organisation adéquate des données de la PKI est permettre son accès de façon simple.
Le service d’annuaire est utile dans le cas d’une PKI pour différentes raisons :

- Les certificats générés par une PKI peuvent être stockés dans l’annuaire et récupérés facilement par les utilisateurs et les applications.
- Elle peut stocker également la liste de révocation (CRL, Certificate Revocation List) permettant ainsi aux utilisateurs de vérifier la validité d’un certificat de façon simple.
- Les organisations PKI qui permettent de gérer le recouvrement de clé, peuvent utiliser l’annuaire pour stocker les clés privées, cryptées bien évidemment.

Active Directory permet aux contrôleurs de domaine de fonctionner comme des homologues. Les clients peuvent donc mettre à jour Active Directory sur n'importe quel contrôleur de domaine Windows Server 2008 du domaine.

C'est ensuite que vient le début de la configuration du contrôleur de domaine. Cela nous donne donc le choix entre le fait de créer :

- Un nouveau contrôleur de domaine: Pour un nouveau domaine enfant, une nouvelle arborescence de domaine ou une nouvelle forêt.

L'option qui nous intéresse est donc la première qui consiste à créer un nouveau domaine: « **Contrôleur de domaine pour un nouveau domaine ».**

Figure 18:Type de contrôleur de domaine

Il faut connaitre d'abord le rôle de domine avant de choisir le type de domaine à configurer : Les domaines alors permettent de réaliser certains objectifs de gestion de réseau, tels que la structuration d'un réseau, la délimitation de la sécurité, l'application d'une stratégie de groupe et la réplication d'informations.

C'est ensuite qu'il va falloir choisir entre les trois différents types de configurations que nous avons à choisir :

- Domaine dans une nouvelle forêt : Cette option permet donc de créer un nouveau contrôleur de domaine pour une nouvelle forêt.
- Domaine enfant dans une arborescence déjà existante : Cette option permet de créer un domaine enfant pour un domaine déjà existant dans une forêt, et bien il se configure automatiquement une relation d'approbation transitive bidirectionnelle entre les deux domaines.
- Arborescence de domaine dans une forêt existante : Cette option permet de créer un contrôleur de domaine racine dans une forêt déjà existante.

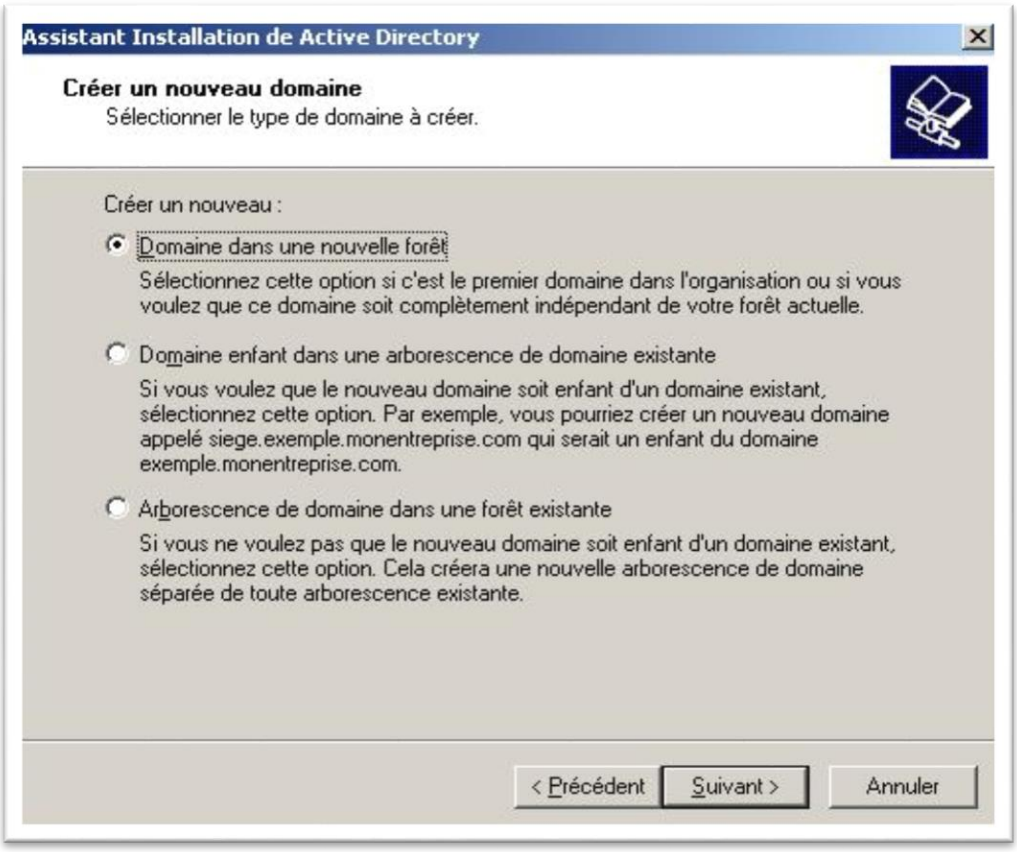

Figure 19:Création d'un nouveau de domaine

C'est ensuite qu'il va falloir rentrer le nom complet du domaine. Il faut dire qu'Active Directory utilise des noms de domaine FQDN (Fully Qualified Domain Name). C'est ainsi que l'infrastructure Active Directory nécessite un serveur DNS pour la résolution de ces types de noms.

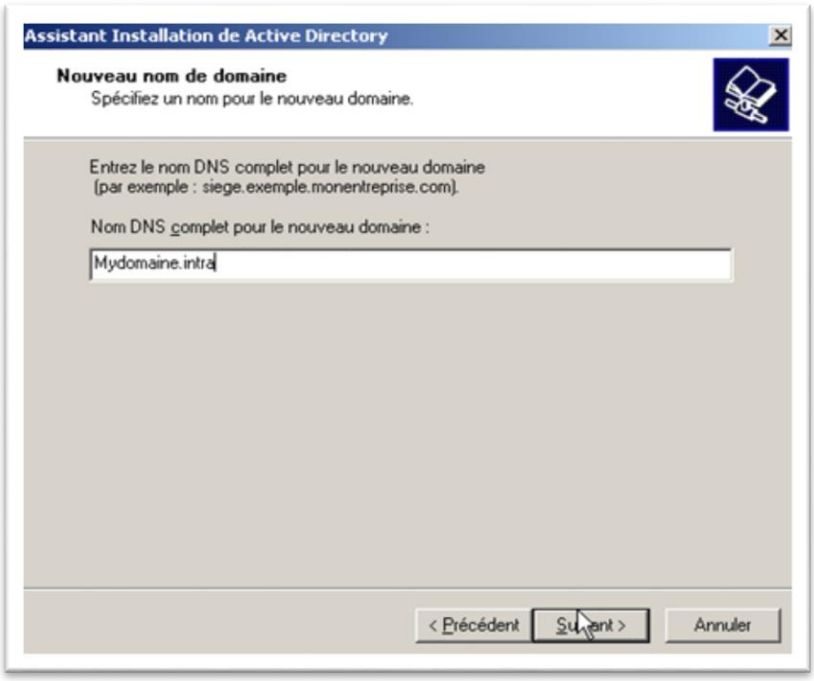

Figure 20:Nom de domaine du nouveau domaine

Notre domaine s'appelle donc « **MyDomain.intra** ». Puis il va falloir renseigner le nom NetBIOS de notre domaine pour la compatibilité avec les versions antérieurs de Windows : alors dans la page Nom de domaine NetBIOS, vérifiez que « **Mydomain** »apparaît.

Cela devient nécessaire ainsi serveur mécanisme de résolution de nom NetBIOS.

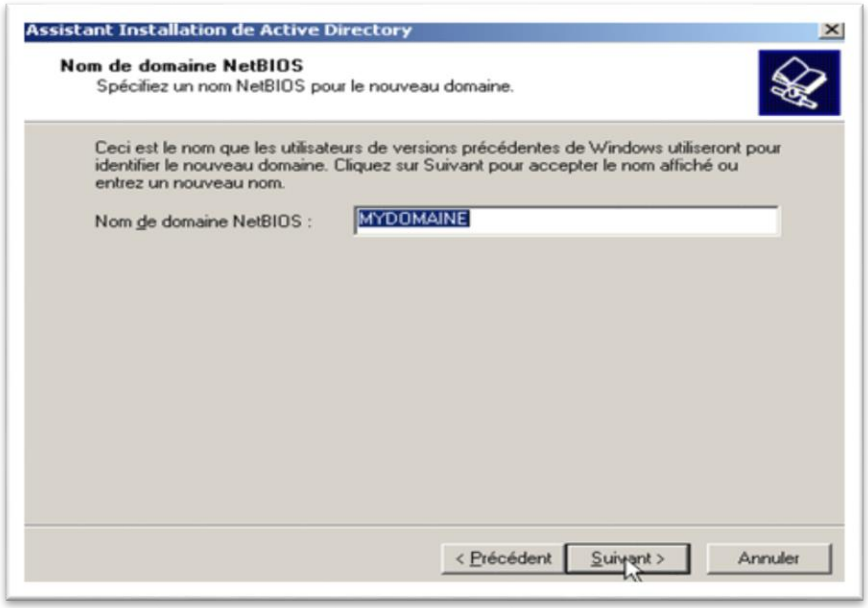

Figure 21:Nom NetBIOS du nouveau domaine

Pour bien fonctionner un contrôleur de domaine Windows server 2008 cela exige la nécessité de DNS, donc on a besoin d'un serveur de DNS. C'est pour cela que l'option qui suit est la création ou la configuration d'un serveur DNS.

N'ayant pas installé de serveur DNS nous avons donc choisi la deuxième option qui nous permet d'installer et de configurer le serveur DNS sur cet ordinateur.

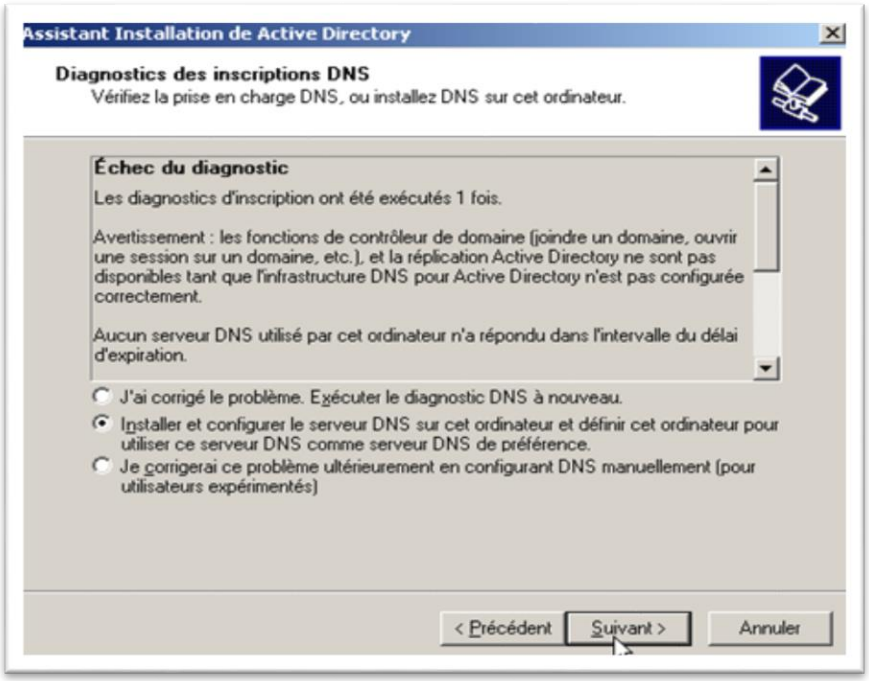

Figure 22:installation de Dns

Une sauvegarde de serveur complète est généralement plus volumineuse qu'une sauvegarde des volumes critiques. Le fait de restaurer une sauvegarde de serveur complète ne restaure pas uniquement les données des services ADS à l'heure de la sauvegarde mais également toutes les données que contiennent les autres volumes.

La restauration de ces données supplémentaires n'est pas nécessaire pour accomplir la restauration ne faisant pas autorité des services de domaine Active Directory.

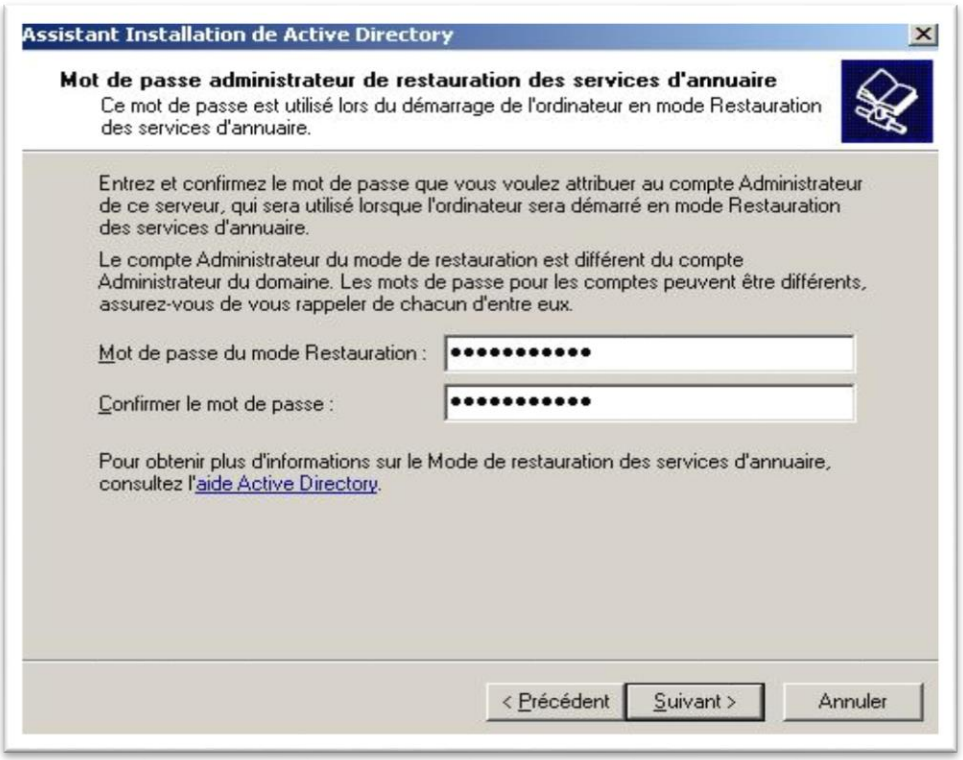

Figure 23:Mot de passe de restauration des services d'annuaires

Mot de passe de restauration des services d'annuaires

Une fois l'installation d'Active Directory **terminé**, nous redémarrons alors notre ordinateur.

2. Gestion de compte d'utilisateurs

Les comptes utilisateurs permettent, sauf restrictions, d'ouvrir une session sur tous les ordinateurs clients du domaine.

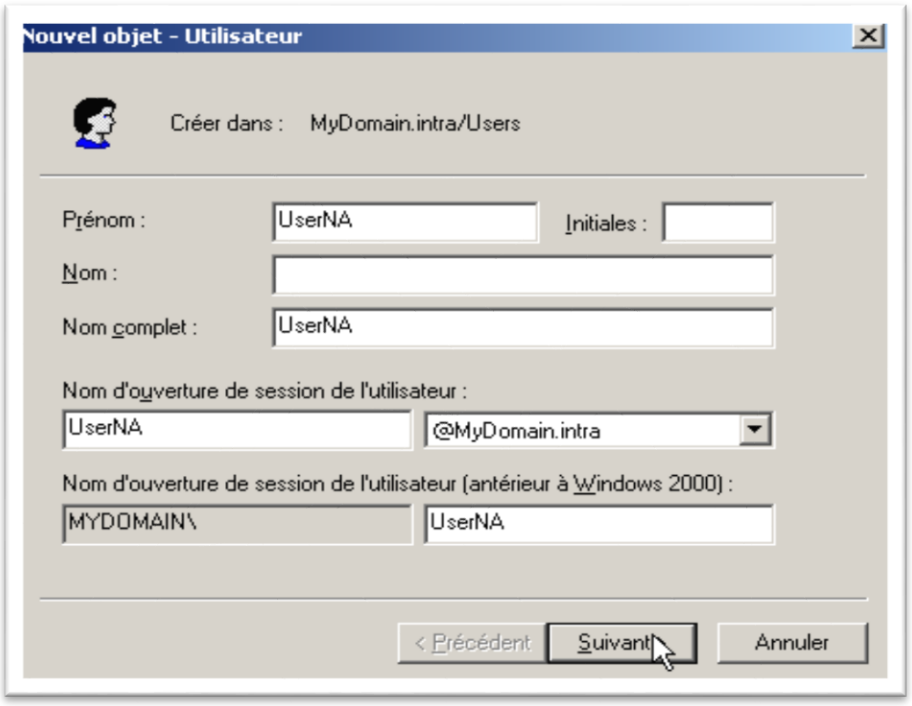

Figure 24:Création d'un compte utilisateur

Le compte utilisateur créé fait maintenant partie du domaine.

De même on a aussi créé d'autres comptes utilisateurs pour l'exploitant lors des tests à effectuer prochainement.

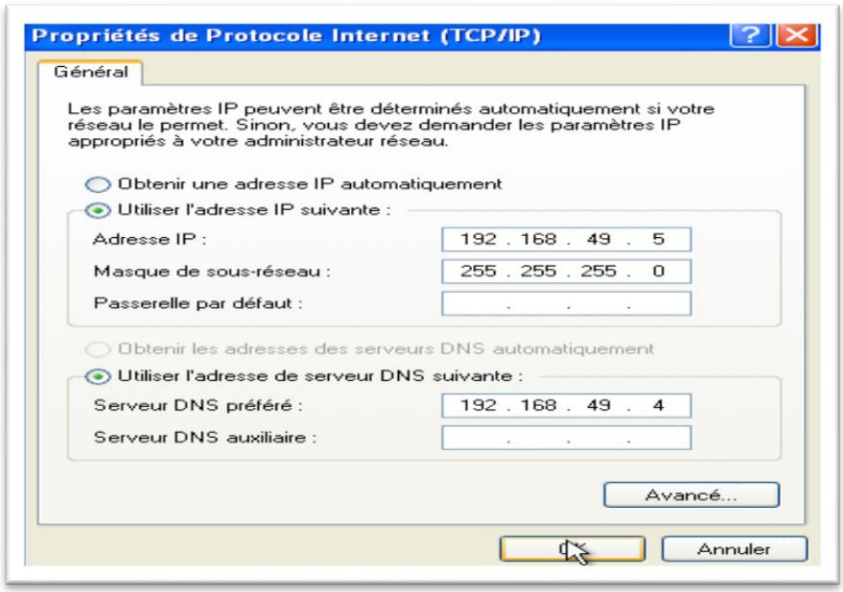

Figure 25:Mise en place de protocole TCP/IP

- Après avoir vérifié la connectivité IP (Internet Protocol) entre le membre et un contrôleur de domaine, modifiez l'adresse DNS dans les propriétés IP de la station de travail, on à choisir l'adresse IP de Windows Server 2008 comme une adresse de serveur DNS préféré. Pour permettre l'accès à notre ordinateur aux ressources d'un réseau Microsoft.

Vérifions que le **Nom de l'ordinateur** est **Mysation,** et **de l'appartenance de notre ordinateur au domaine « Mydomain ».**

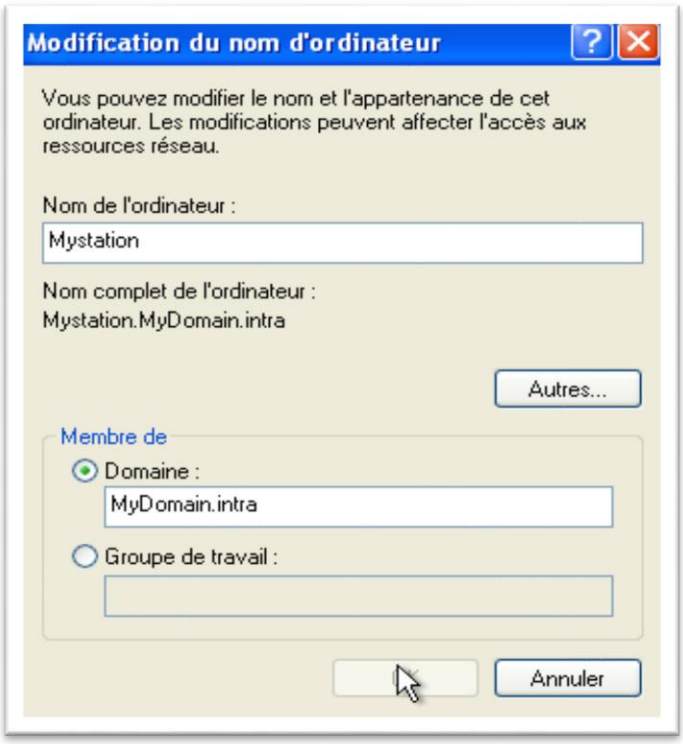

Figure 26:Modification de l'appartenance d'un ordinateur à un domaine

Sous **Membre de**, on écrit le nom de notre domaine « **MYDOMAIN »** dans la zone **Domaine**.

Par la suit la boîte de dialogue **Nom d'utilisateur de domaine et mot de passe** s'affiche. Nous devons alors fournir un compte qui bénéficie de privilèges permettant d'entrer dans le domaine.

:

Figure 27: Modification de nom d'ordinateur

L'affichage du message **Bienvenue dans le domaine MYDOMAIN** indique que la station de travail a été ajoutée au domaine.

Redémarrerons alors la station de travail.

Figure 28:ouverture d'une session windows

Pour pouvoir réaliser notre travail on a eu recoure à créer 2 groupes globaux

« GGAuthorizedUsers » et « **GGNotAuthorizedUsers ».**

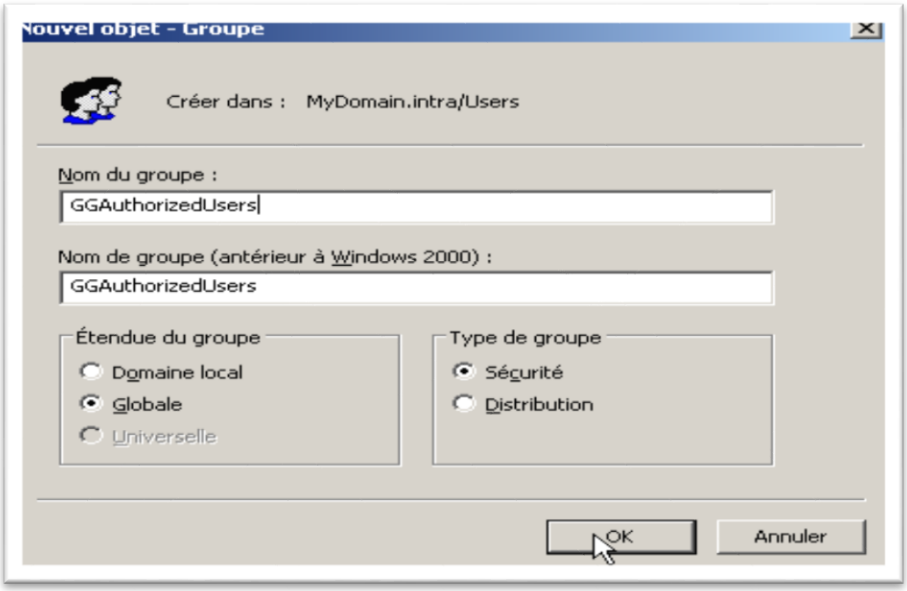

Figure 29:Création des groupes globaux

Après avoir créer les groupes globaux, nous allons maintenant ajouter des membres a ces goupes :

- Pour **GGAuthorizedUsers** : Administrateur et UserMMC.
- Pour **GGNotAuthorizedUsers** : UserNA.

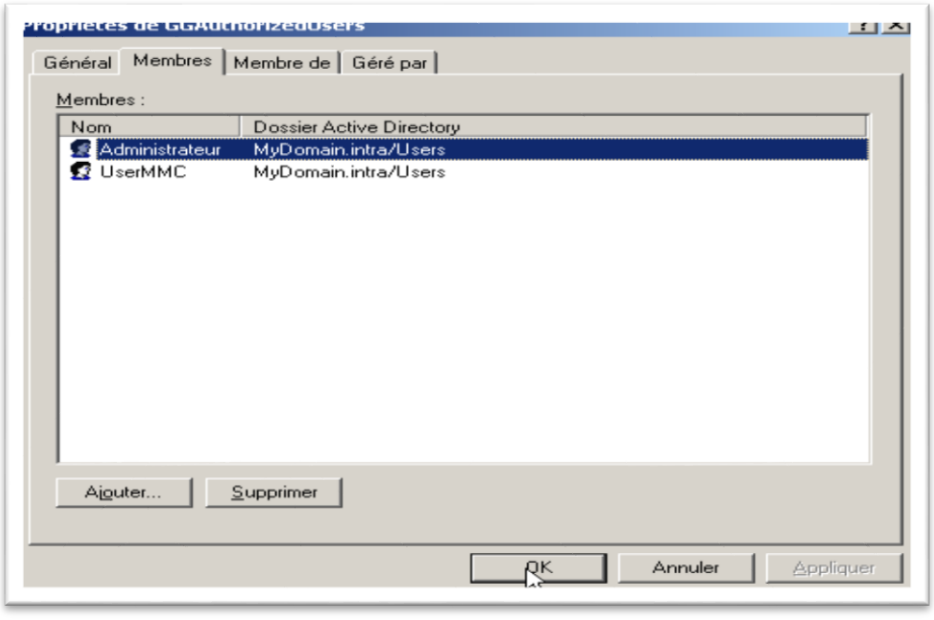

Figure 30:Ajouter des membres à des groupes globaux

- **Les groupes de domaine locaux**

Nous avons créer 2 groupes de domine locaux « **GDLAuthorized »** et « **GDLNotAuthorized ».**

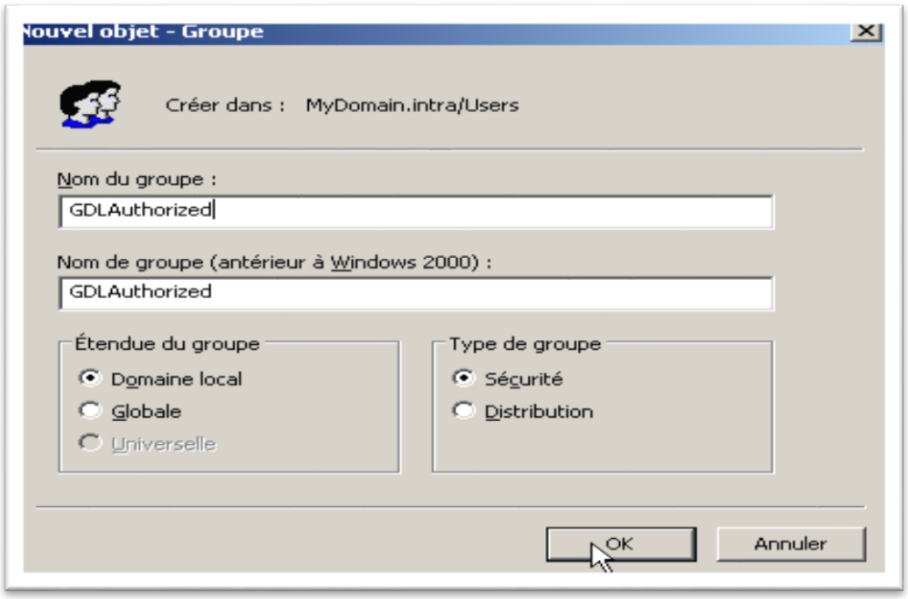

Figure 31:Création de groupes de domaine locaux

Enfin, nous allons ajouter des membrest a ces goupes :

- Pour **GDLAuthorized:** GGAuthorizedUsers.
- Pour **GDLNotAuthorized**: GGNAuthorizedUsers.

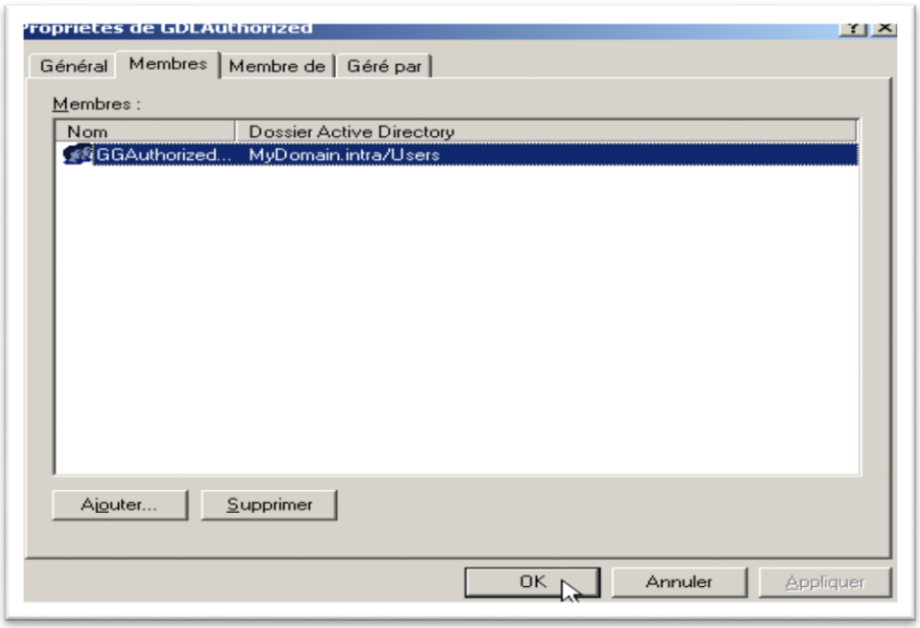

Figure 32:Ajouter des membres à de groupes de domaine locaux

3 .Installation et configuration des différents services

3.1 Configuration d'un serveur Dns

a. Configuration

Tout d'abord on vérifie sur quelle interface écoute notre serveur DNS. Par défaut, il écoute toutes les adresses IP associées à l'ordinateur local. S'il est important pour modifier : Démarrer -> Tous les Programmes -> Outils d'administration -> DNS -> Clique droit sur votre serveur DNS -> Propriété -> Onglet interface**.**

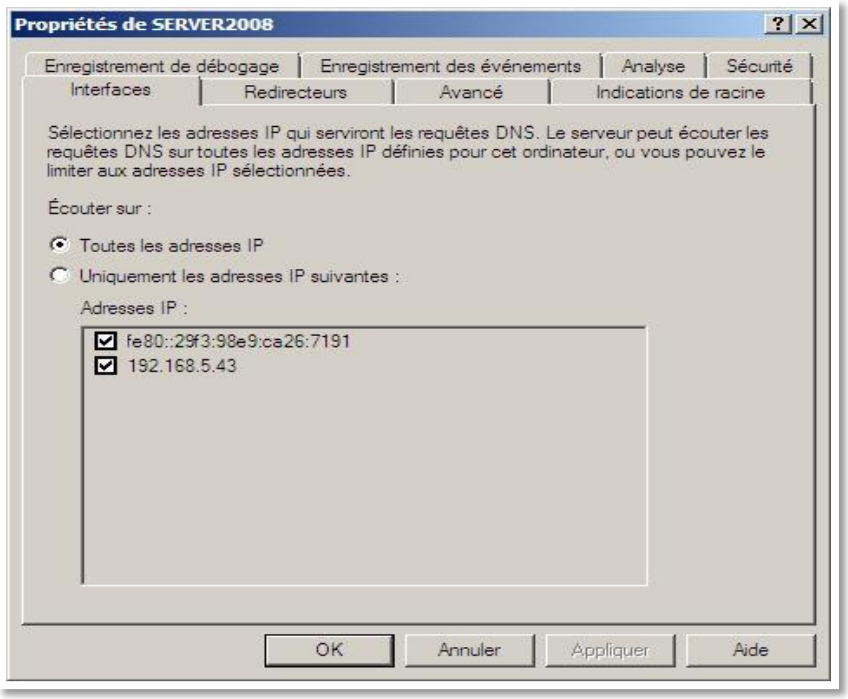

Figure 33:Propriétés de server 2008

Ensuite on regarde s'il ya des serveurs racines, car si notre serveur DNS n'a pas de serveur racine recensé, il ne peut que résoudre les adresses de son réseau ou sous réseau. Pour cela onglet « indicateur de racine ».

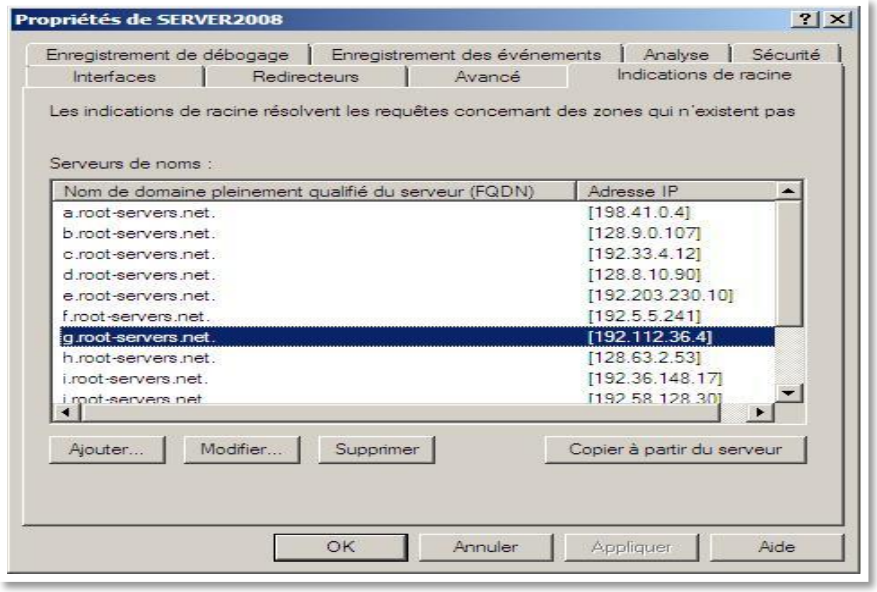

Figure 34:Propriétés

Puis il faut configurer une redirection, c'est à dire si notre serveur DNS ne peut répondre à la requête il redirige la requête vers un autre serveur DNS. Donc il faut renseigner l'adresse IP du serveur redirecteur DNS.

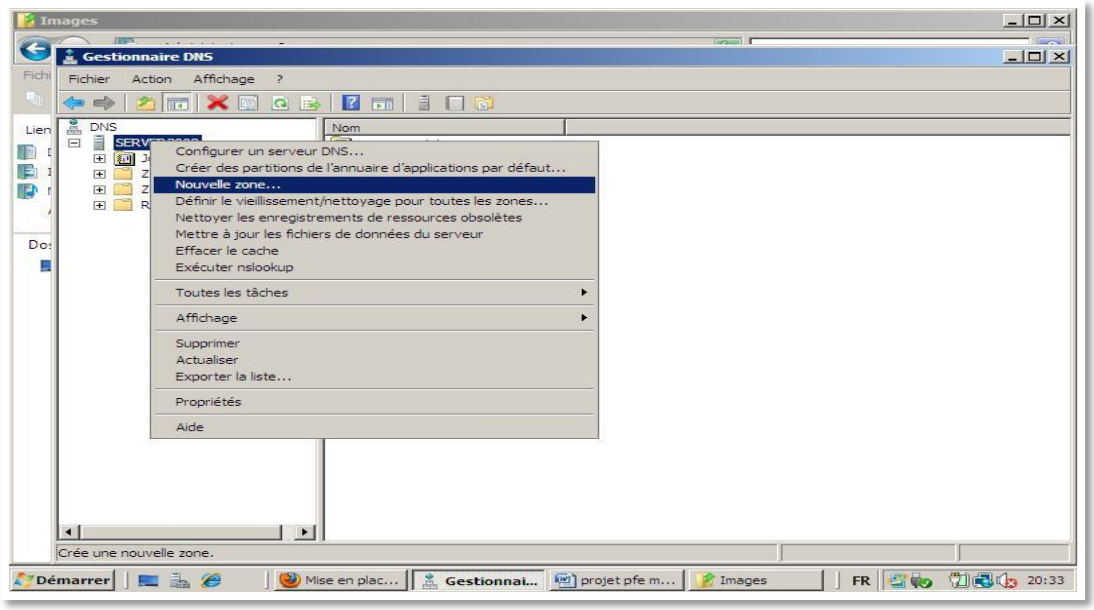

Figure 35:Gestionnaire Dns

Une fois le type de zone choisie, il nous est demandé de choisir si l'on veut une « zone de recherche directe » ou une « zone de recherche inversée ».

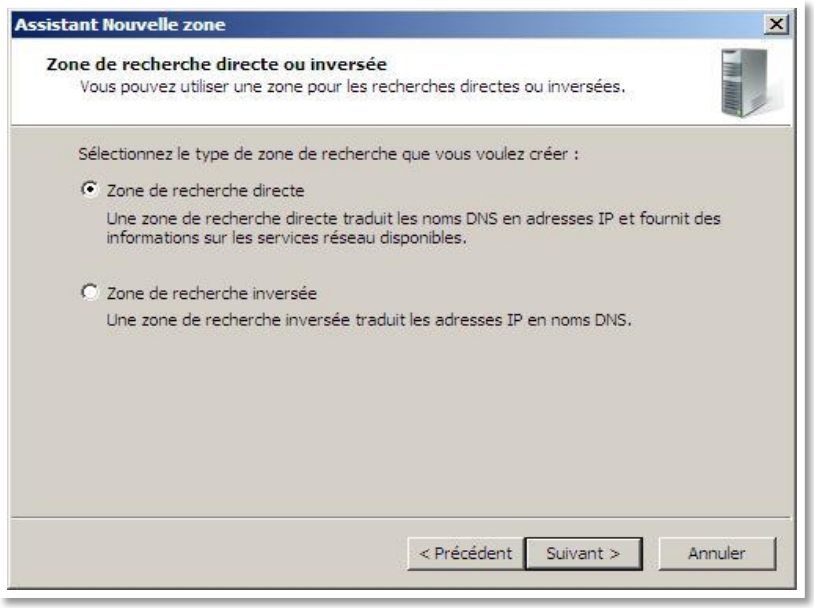

Figure 36:Assistant nouvelle zone

Puis il est demandé de choisir le nom de la zone, que le nom du domaine succède notre nom de zone. Dans ma machine exemple on est intégré à aucun domaine donc il est succéder de Maintenant notre zone est créée, mais il est indispensable dans une zone d'avoir deux types d'enregistrement le SOA et le NS (Name Server).

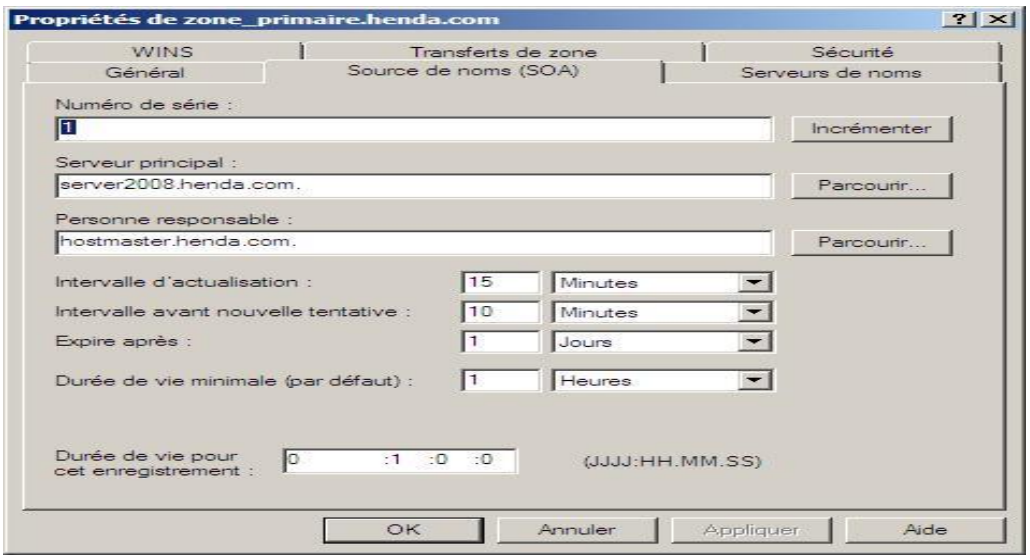

Figure 37:propriétés de zone primaire

3.2. Installation de serveur web IIS

Démarrer, Outils d'administration puis Gestionnaire de serveur. Dans Résumé des rôles**,** Ajouter des rôles**.** L'Assistant Ajout de rôles pour ajouter le rôle de serveur Web.

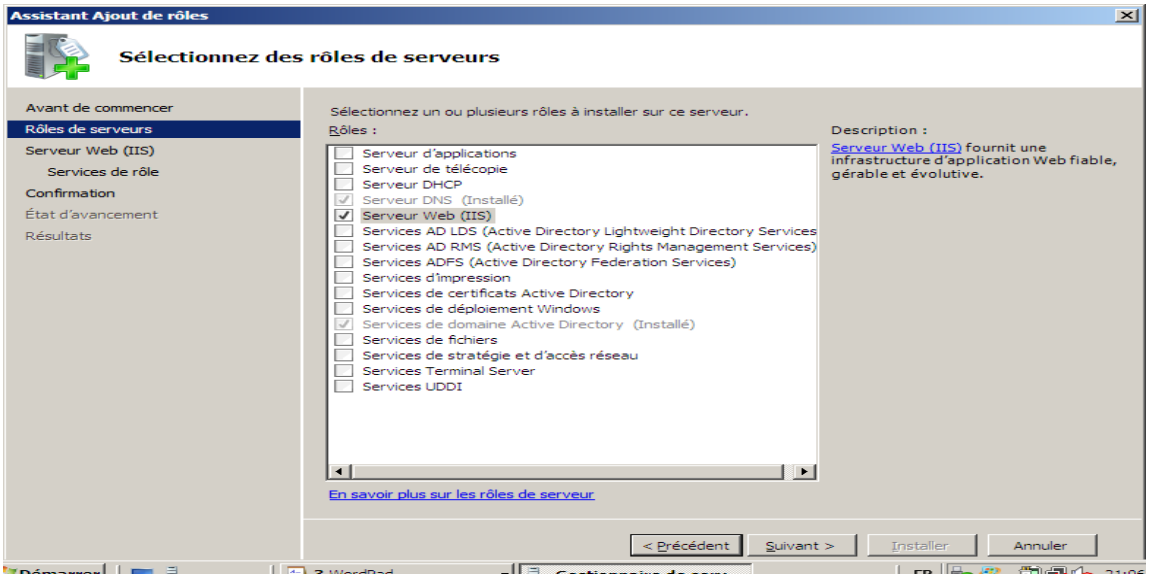

Figure 38:Assistant ajout de rôles

-Conception d'une page Web index.html placée à la racine du répertoire de base

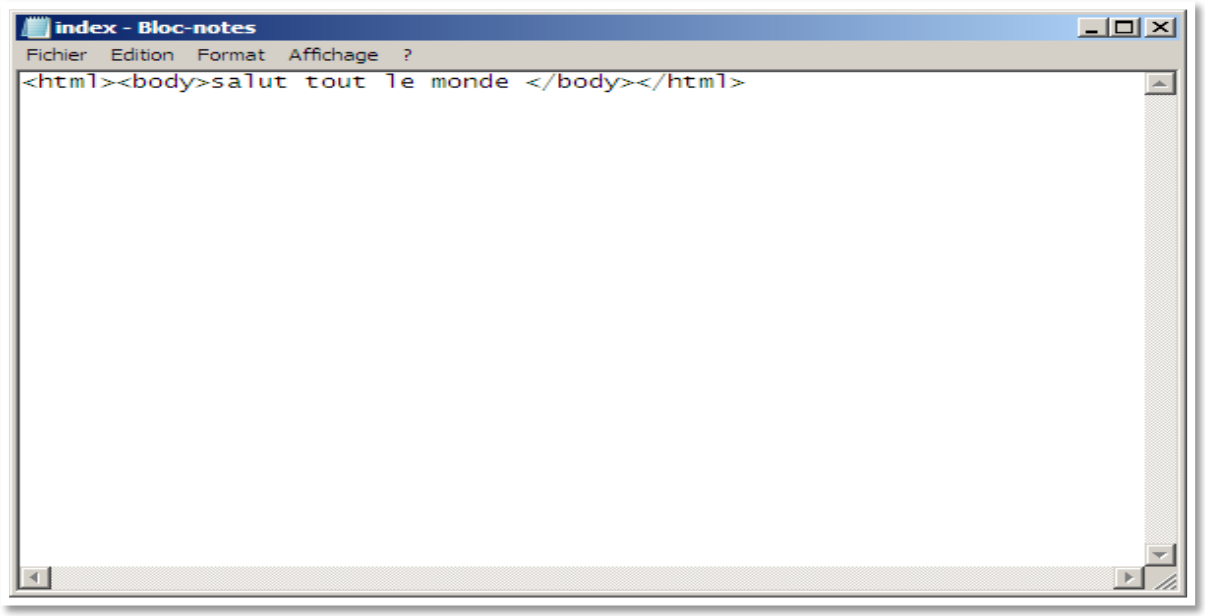

Figure 39:index

Résultat dans Internet Explorer Accès via l'URL http://192.168.5.43

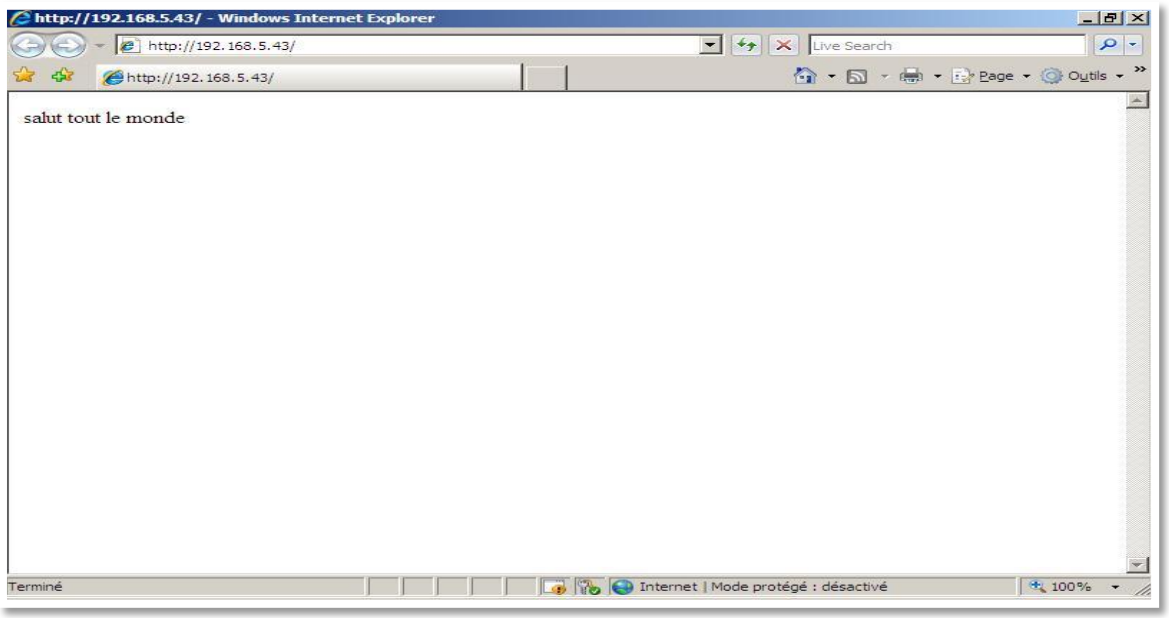

Figure 40:URL

Création d'un dossier placée à la racine du répertoire de base

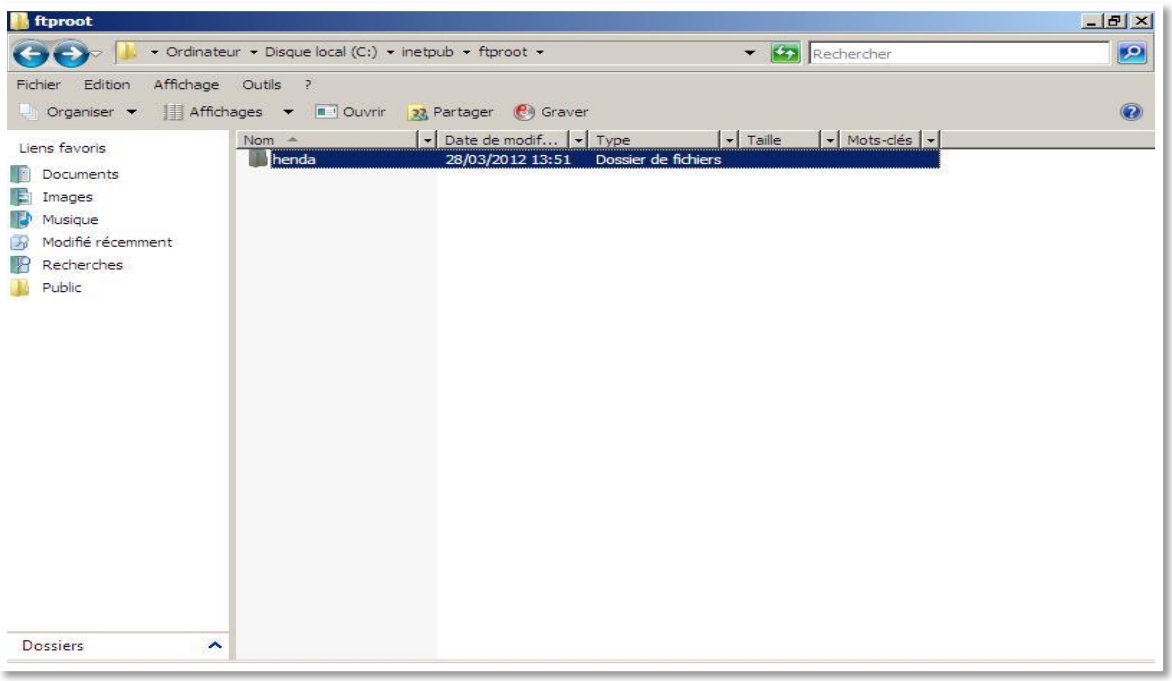

Figure 41:ftp root

Accès via l'URL Ftp:// 192.168.5.43

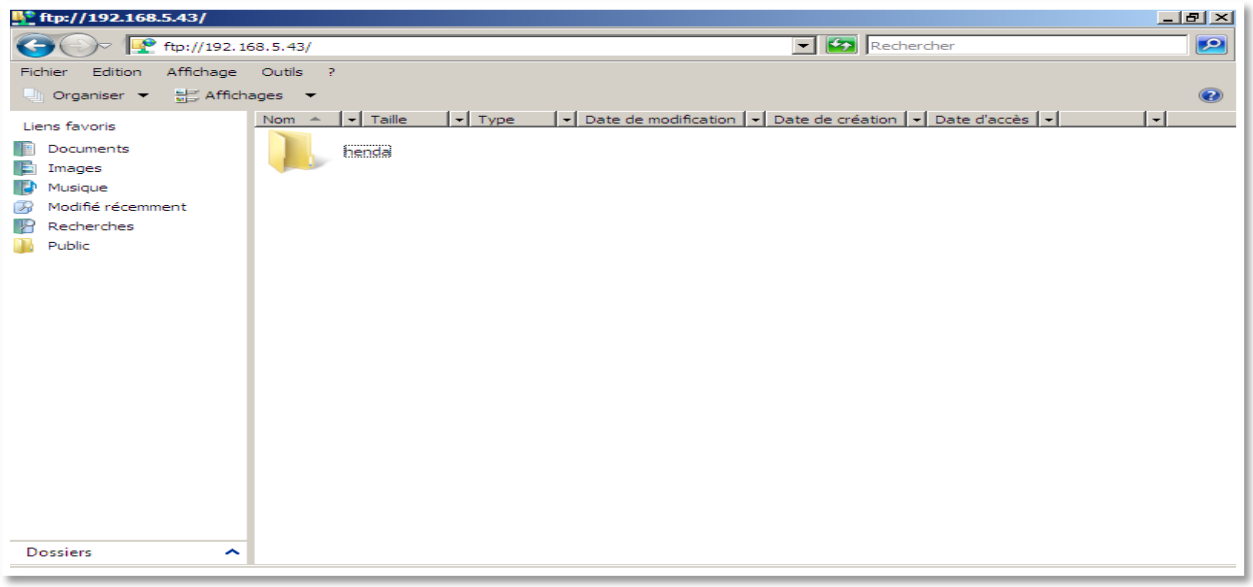

Figure 42:Accès via URL

3.3. Installation de service FTP

3.3.1 Fonctionnalité de sécurité FTP

a-Ajout d'un site FTP

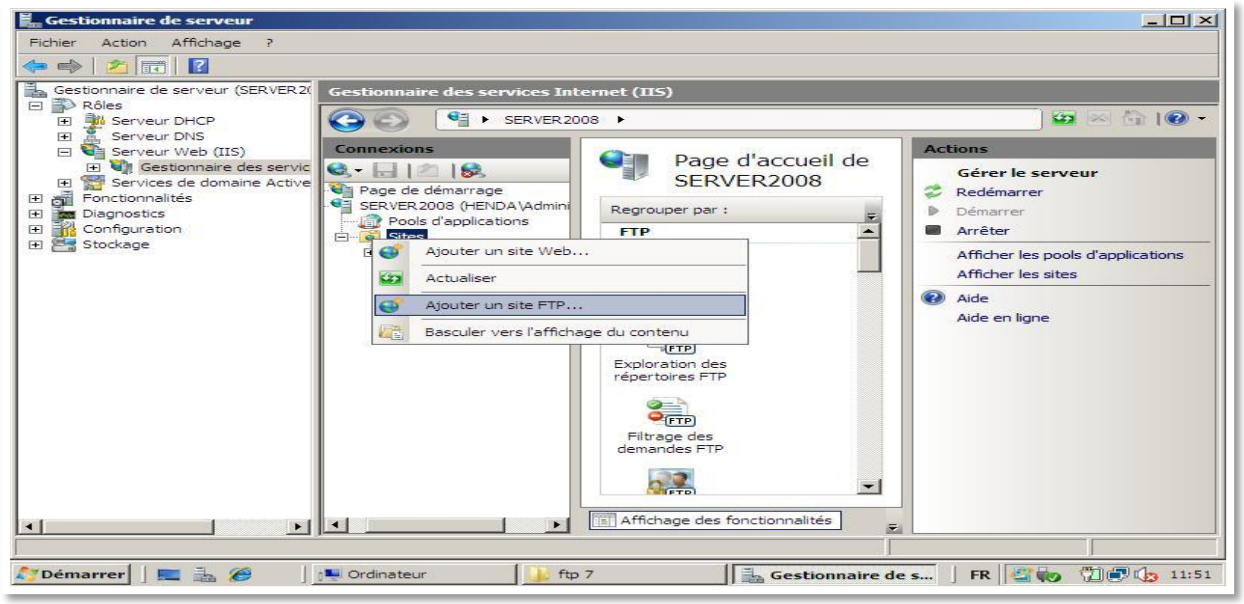

Figure 43:Ajout d'un site ftp

Site nommé Henda, et emplacement root c:\inetpub\ftproot

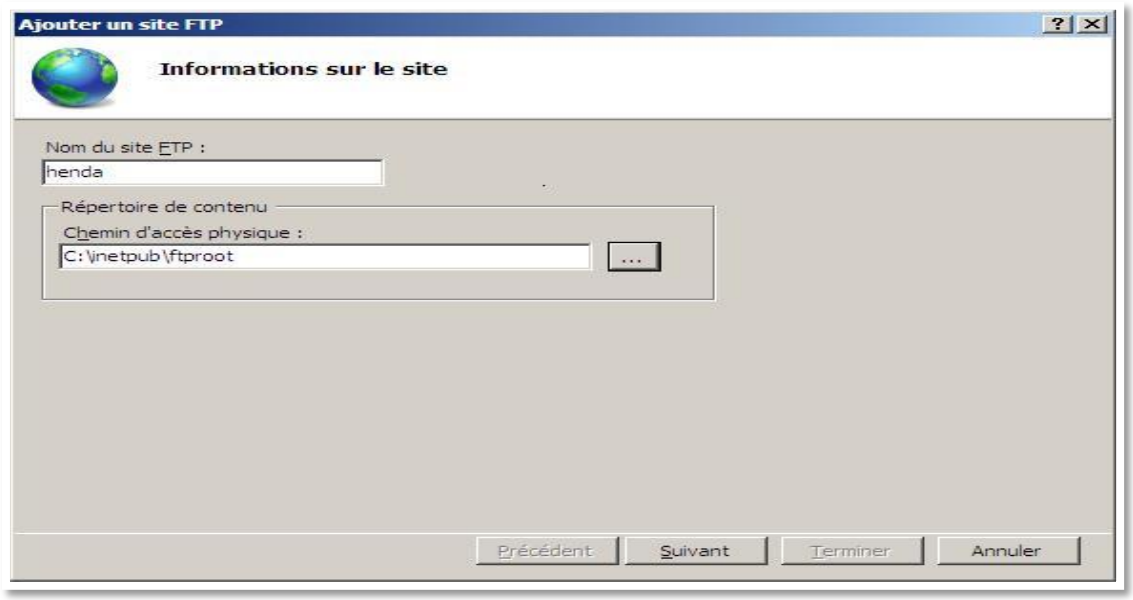

Figure 44:nom du site ftp

Il s'agit de définir les droits d'accès et construire des accès anonymes, ou des accès spécifiques pour des comptes utilisateur Windows.

Il s'agit uniquement d'un accès public, donc je choisis «tous les utilisateurs»

Avec autorisations lecture seul

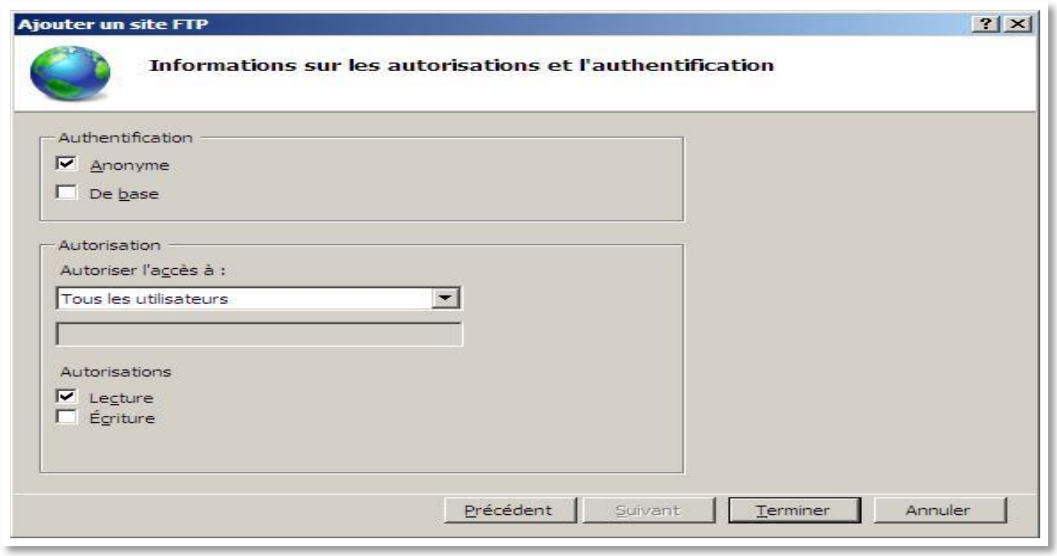

Figure 45:Authentification anonyme

Résultat dans le gestionnaire des services Internet

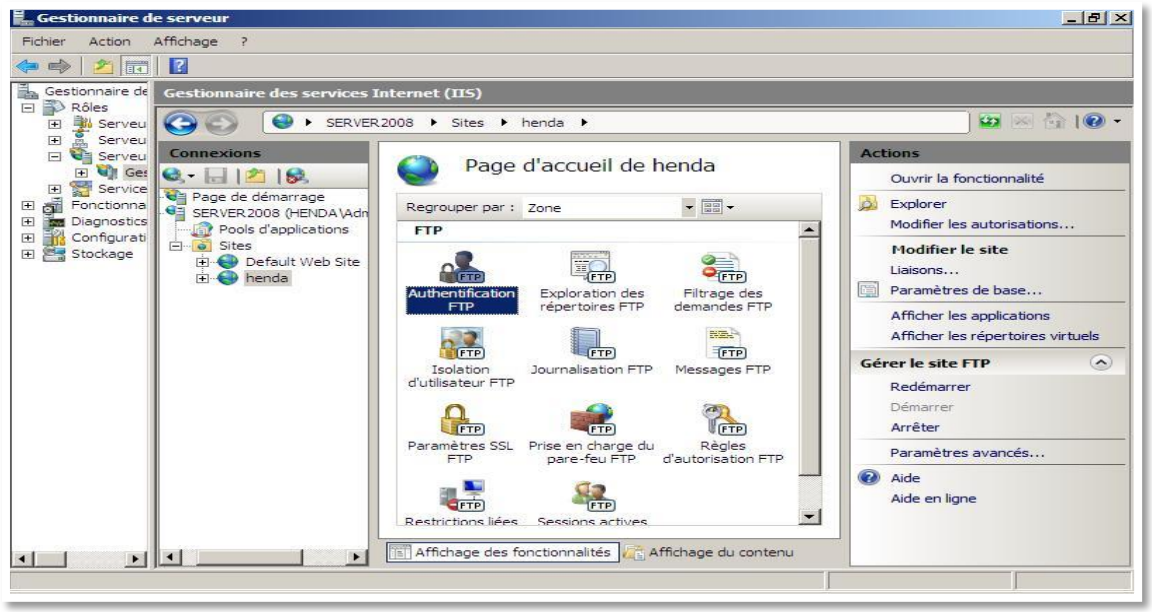

Figure 46: gestionnaire des services internet IIS

b-Authentification FTP

L'authentification permet de déterminer qui peut accéder aux ressources sur un serveur Web.

Assistant "Authentification"

Activer Authentification anonymes

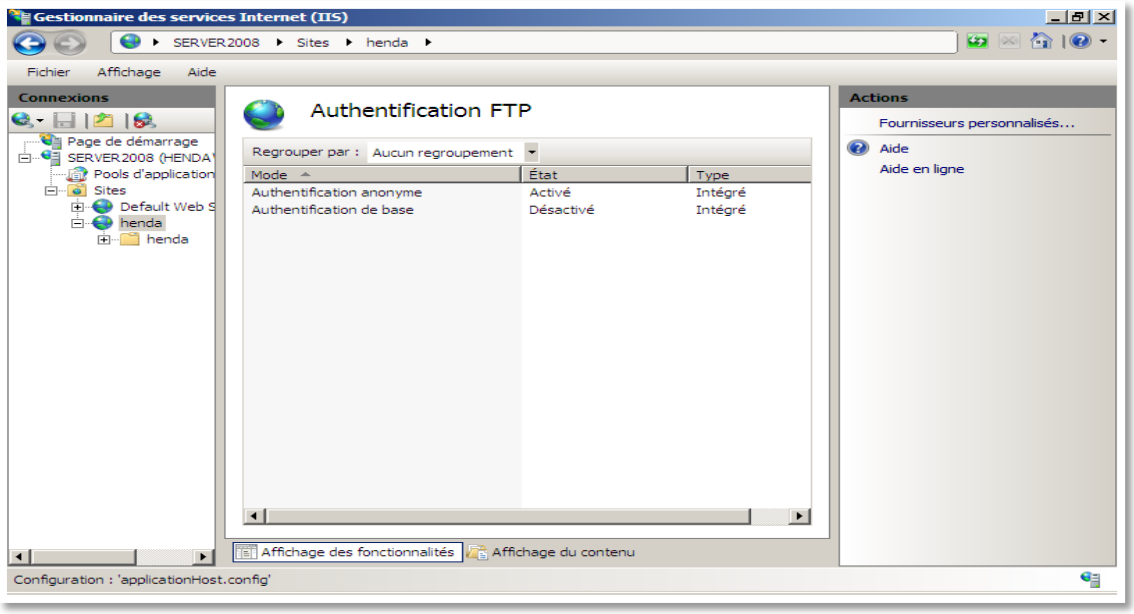

Figure 47:Authentification de base

C-Règle d'autorisation

Règle d'autorisation : Autoriser l'accès à ce contenu : tous les utilisateurs

Autorisations : lecture et écriture

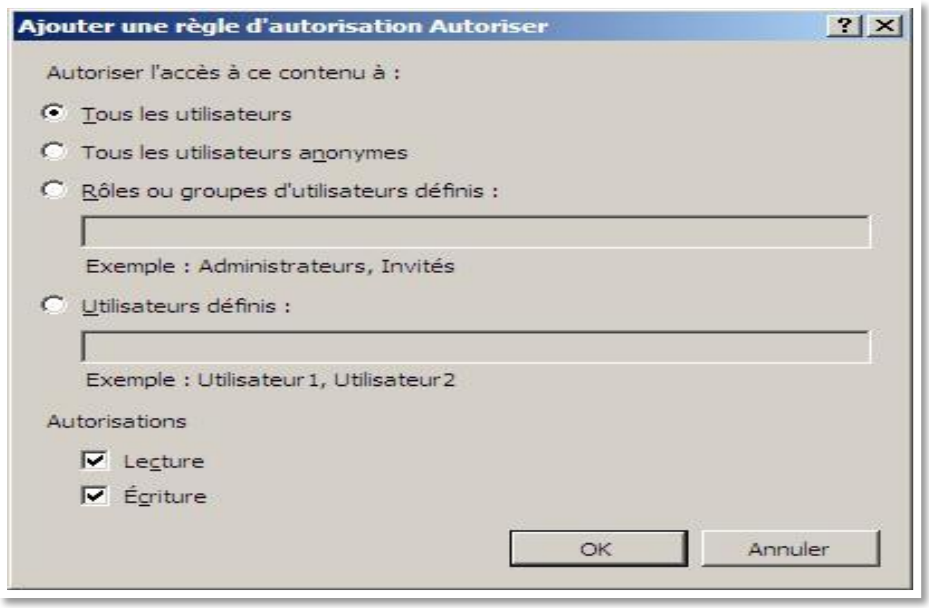

Figure 48:règle d'autorisation

Résultat dans le gestionnaire des services Internet

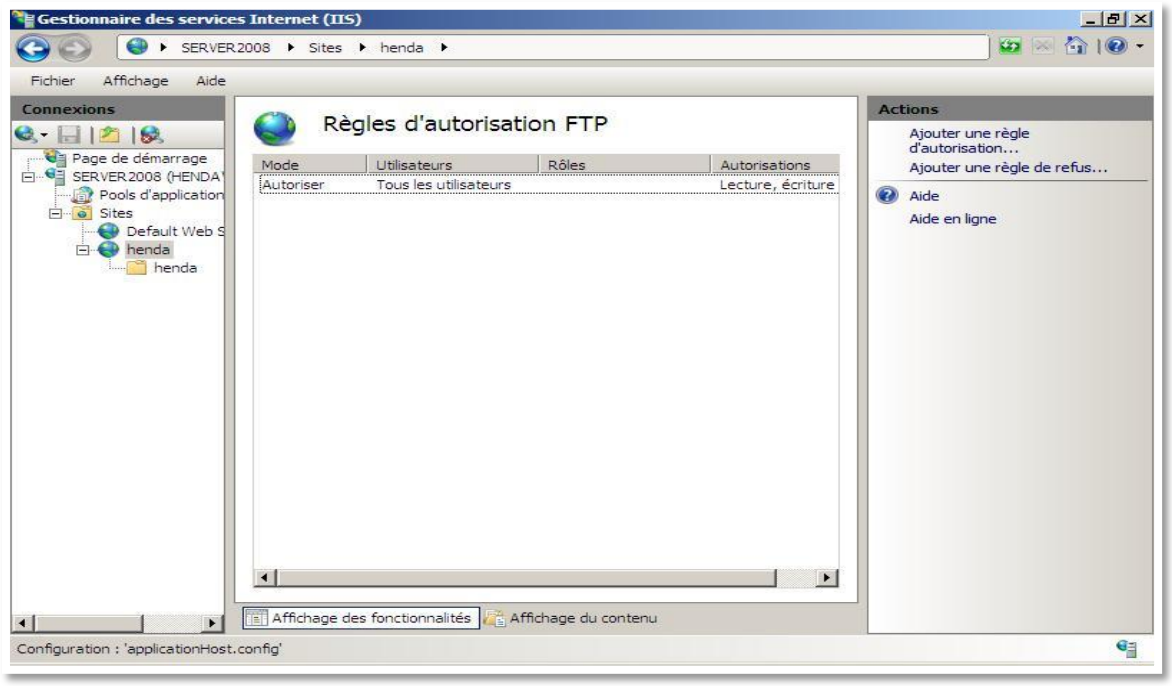

Figure 49:règle d'autorisation

d-Session active FTP

Pour Voir tous les pc connecté aux réseaux

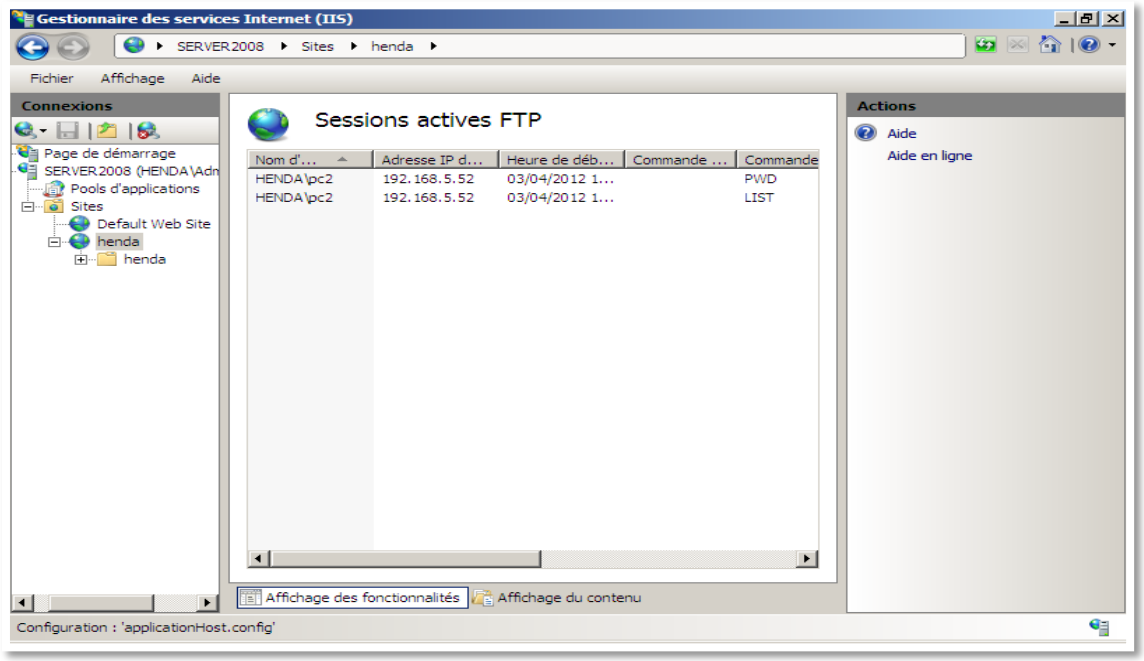

Figure 50:sessions active Ftp

3.3.2. Coté client FTP :

Résultat via l'URL ftp://server2008.henda.com

Tous les utilisateurs peuvent autoriser l'accès au donnés

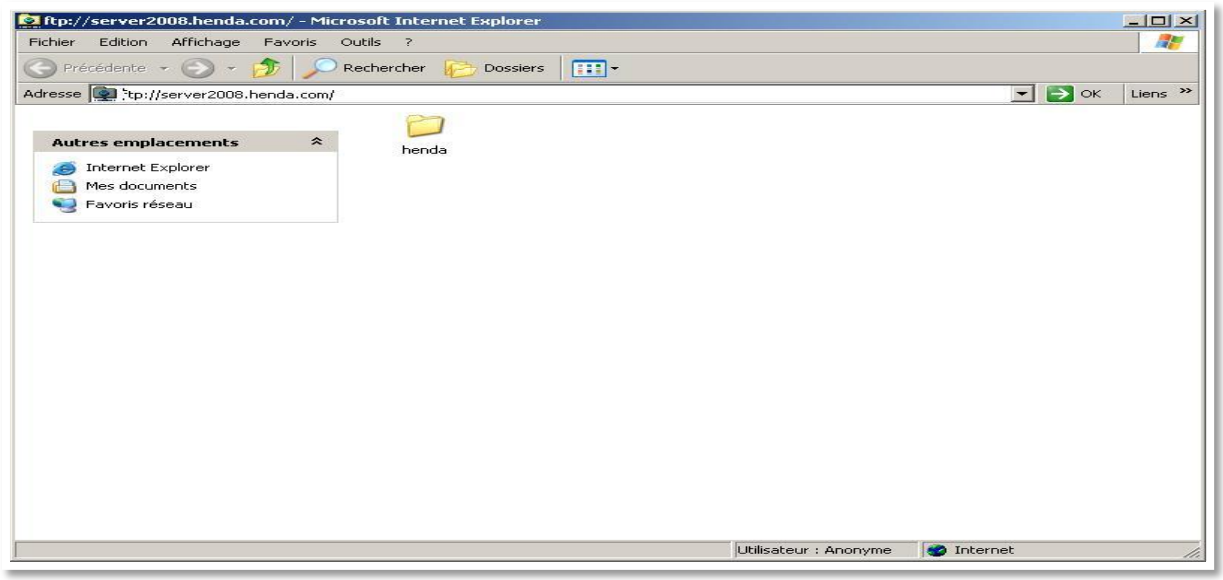

Figure 51:client Ftp

Authentification de base et activé pour donner l'accès a un certains client

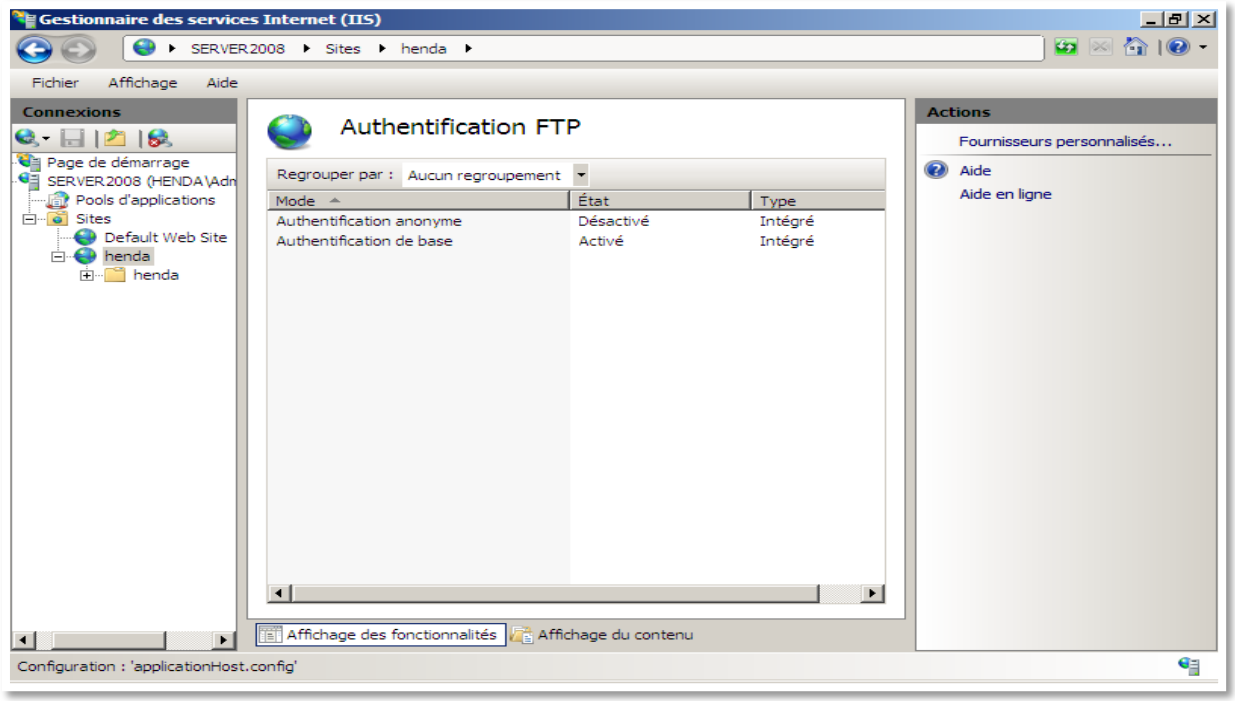

Figure 52:Authentification Ftp

3.4. Installation et configuration d'un serveur DHCP

a. Configuration de carte réseau

Il faut donner une adresse IP statique à la machine.

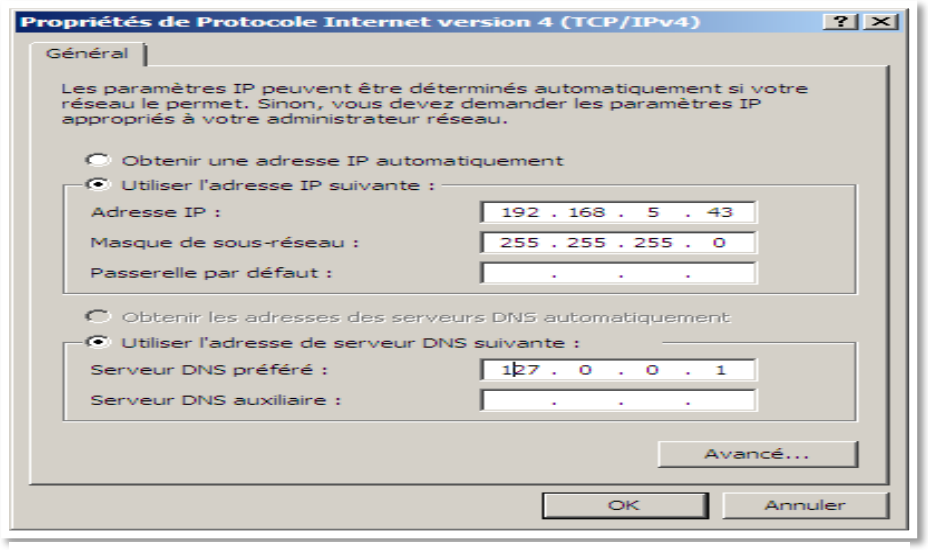

Figure 53:Propriétés de protocole internet

b.Installation

Quand le serveur DHCP assigne une adresse IP à un poste client, il garde l'adresse IP et le nom du poste client référant en mémoire ce poste

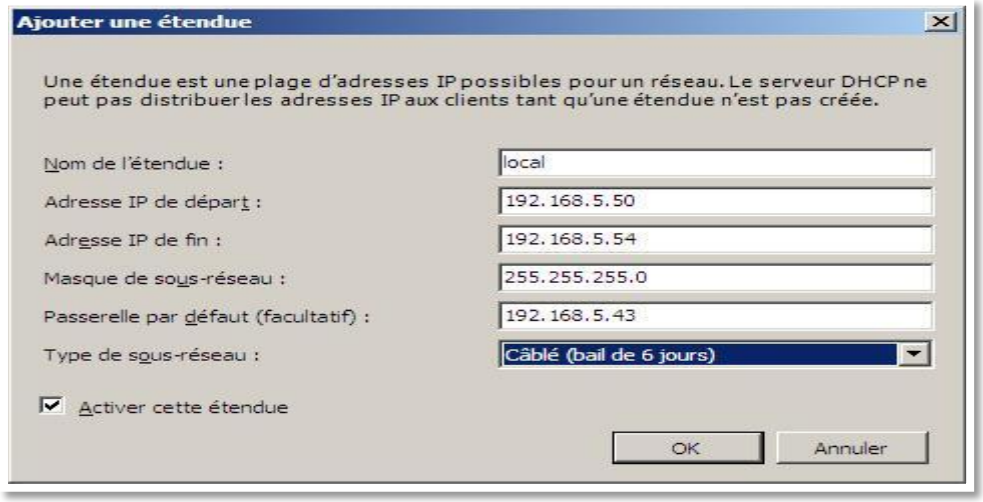

Figure 54:Ajout d'une étendue

Concernant l'IPv6 Les postes clients recevront automatiquement une adresse IPv6 sans aucune configuration

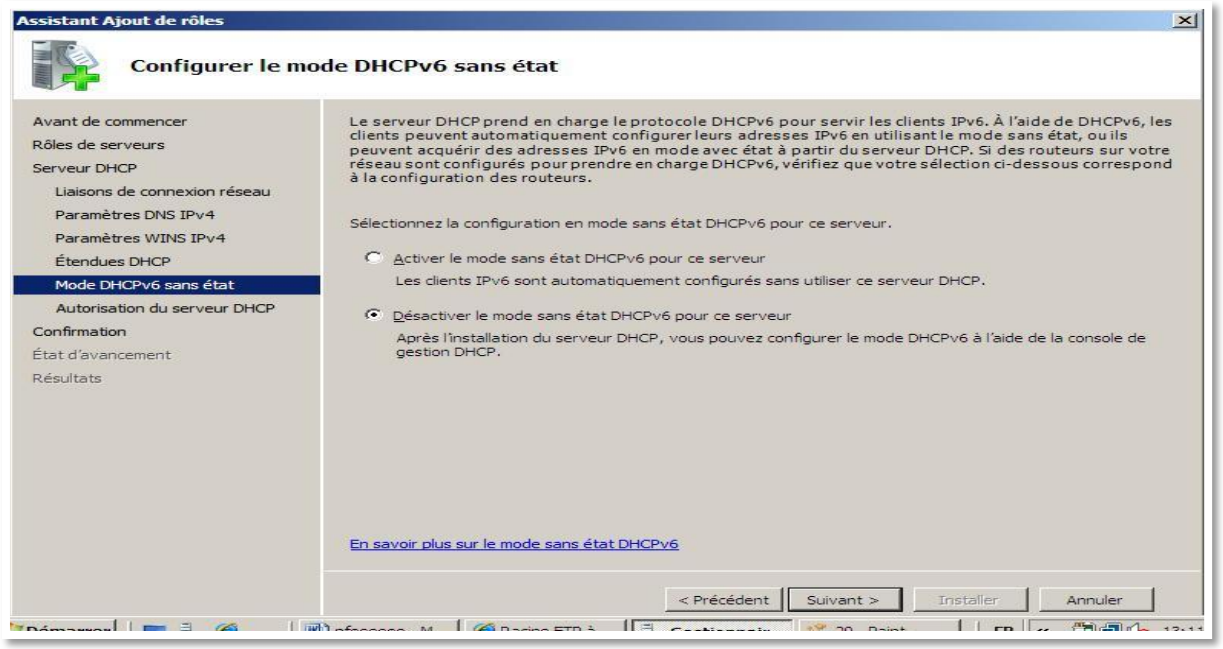

Figure 55:configuration de mode DHPCP6

Sur cette page, comme pour l'IPv4, nom de domaine et les adresses IPv6 de serveur DNS un clic sur valider à chaque fois pour vérifier que les adresses saisies sont bien correctes.

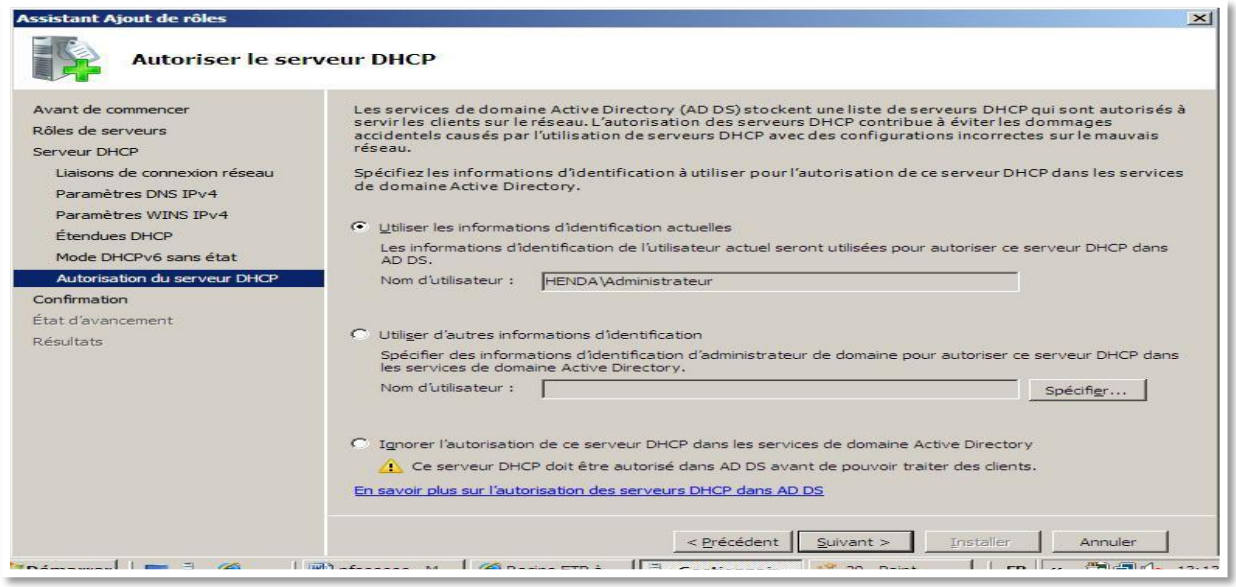

Figure 56:Assistant Ajout de rôle

c. Configuration

Un clic droit sur **IPv4,** puis **Nouvelle étendue**

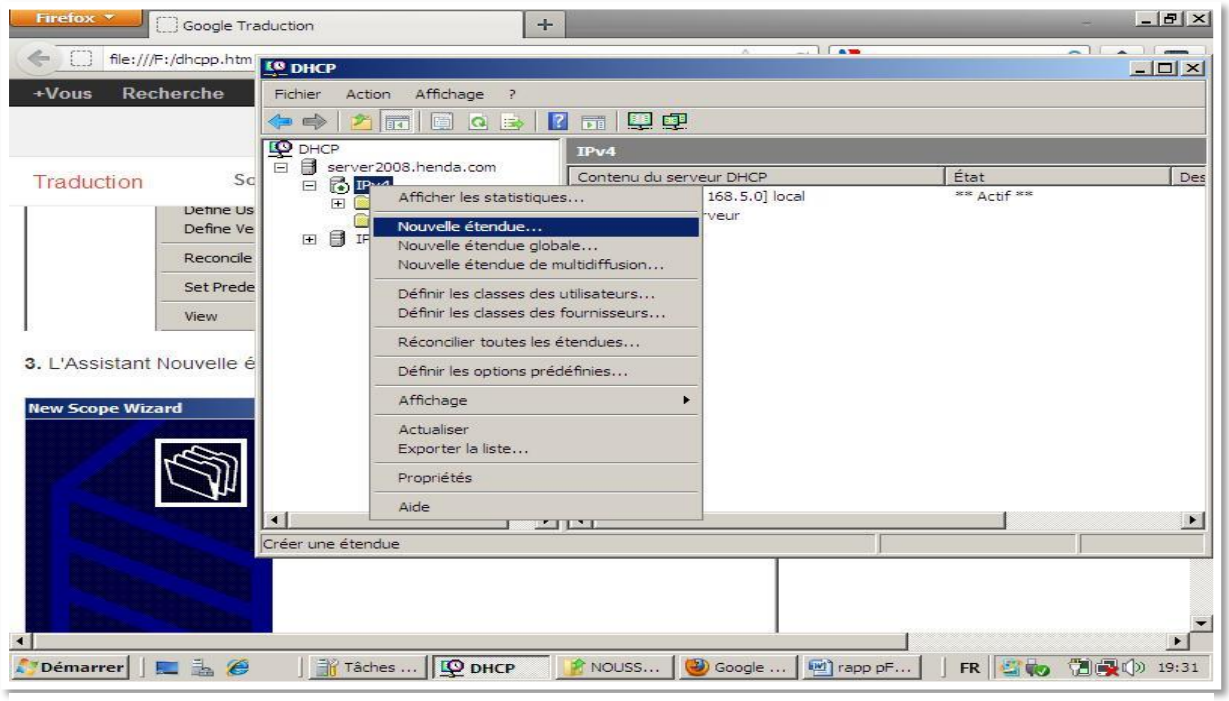

Figure 57:Nouvelle étendue

Maintenant, nous allons choisir la plage d'adresses IP. Dans l'adresse IP de début 192.168.5.43 **et** l'adresse IP de fin 192.168.5.230**.** Pour le masque de sous-réseau, nous allons utiliser 255.255.255.0.

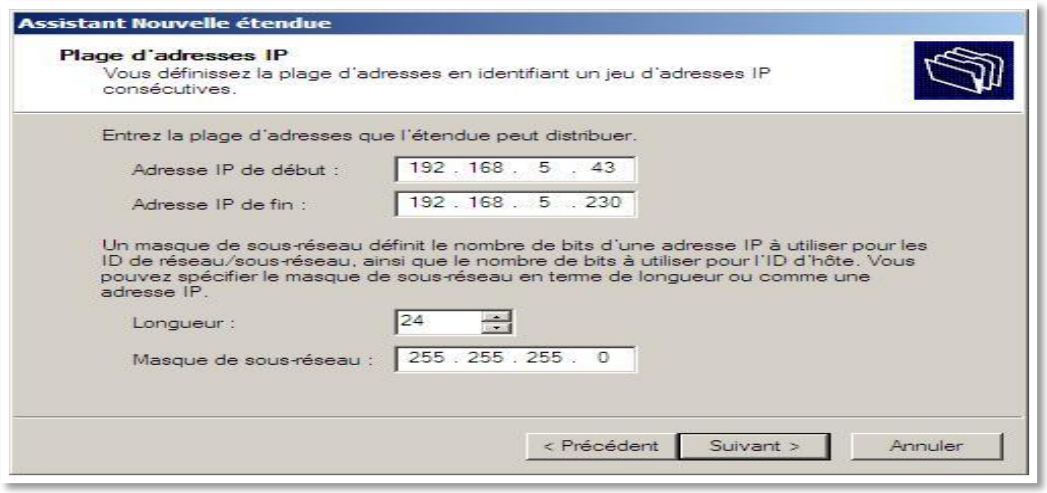

Figure 58:plage d'adresse

Maintenant nous allons configurer une plage d'exclusion en entrant **l'adresse IP de début:** Comme **192.168.5.200** puis **l'adresse IP de fin: 192.168.5.230** lieu.

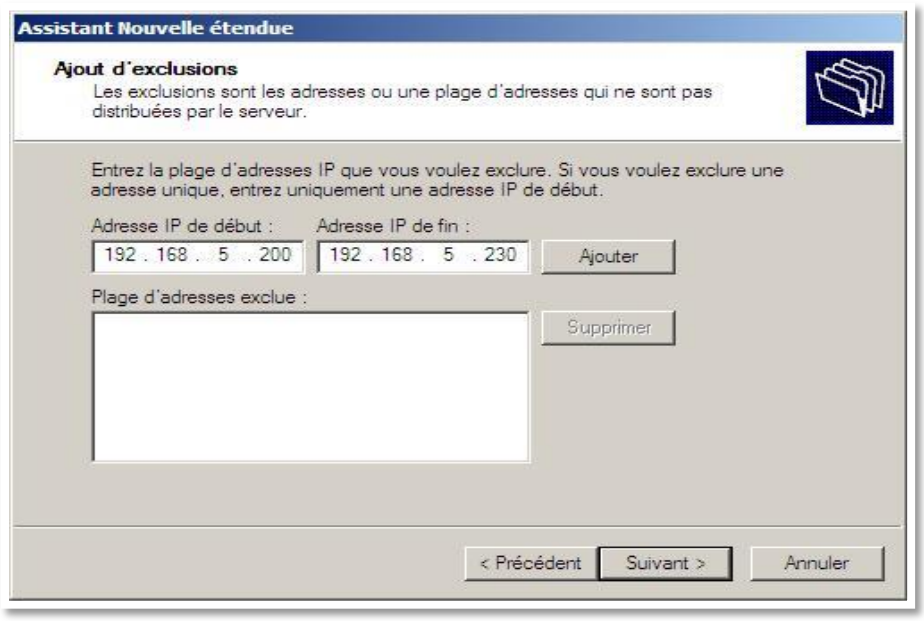

Figure 59:Ajout d'exclusions

Après avoir défini la durée de bail un clic sur **Suivant.**

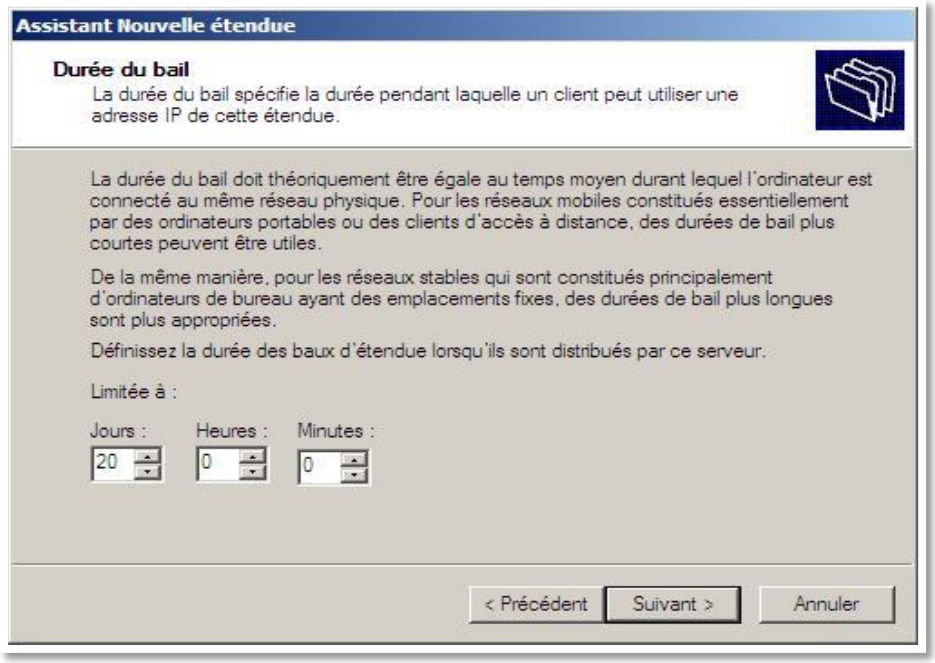

Figure 60:durée du ball

L'assistant va maintenant demander si souhaite configurer les options DHCP

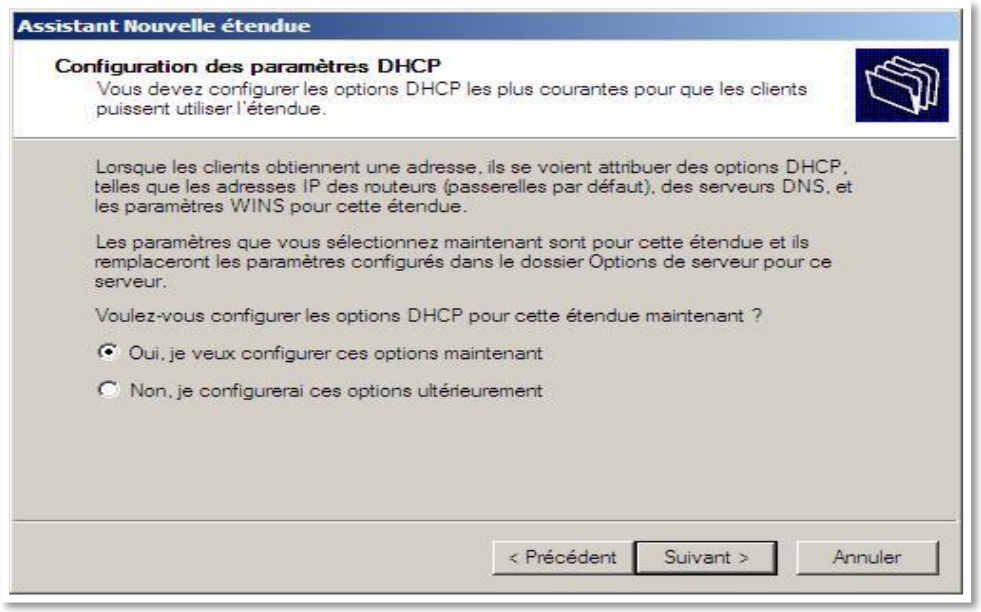

Figure 61:configuration des paramètres DHCP

L'écran suivant demande on active l'étendue. Choisir ce qui fonctionne ensuite clic sur **Suivant**

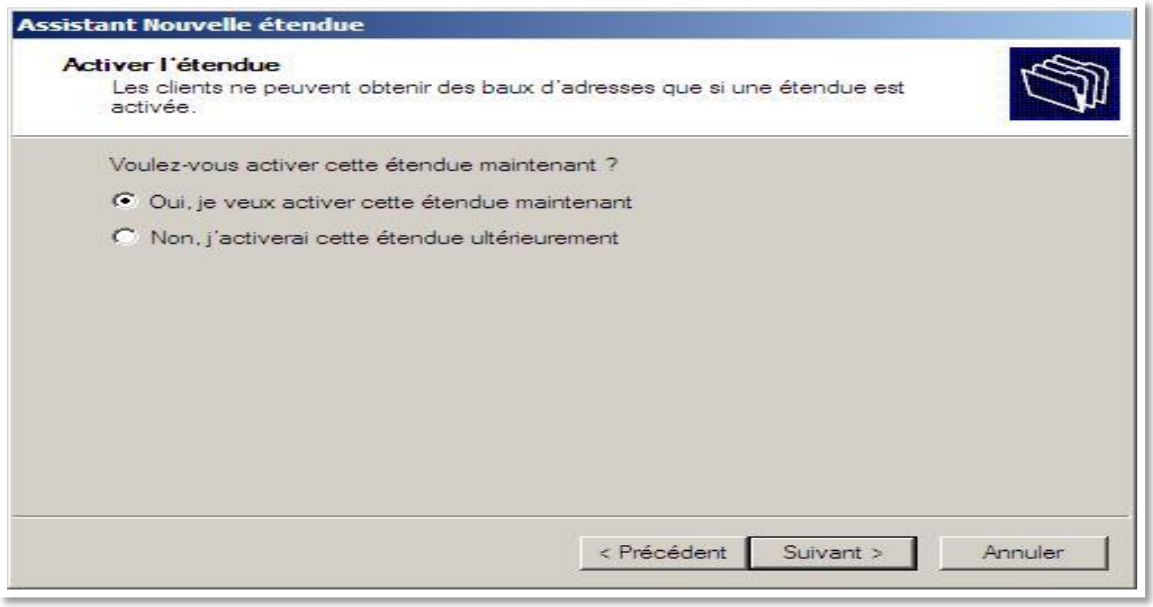

Figure 62:Activer étendue

Dans la fenêtre d'entrée Nouvelle réservation on introduit les informations suivantes

Nom**: priver**

Adresse IP: **192.168.5.52**,

Adresse MAC: **00-13-f7-cc-38-83**

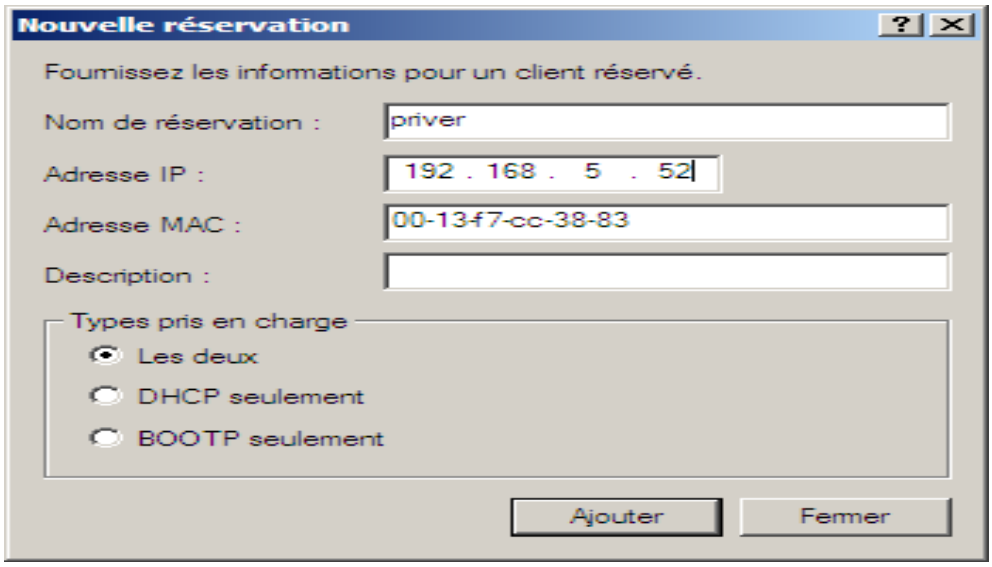

Figure 63:nouvelle réservation

3 .4.1.Configuration d'un client DHCP :

Au coté client le serveur et accepter l'adresse attribué par le serveur DHCP

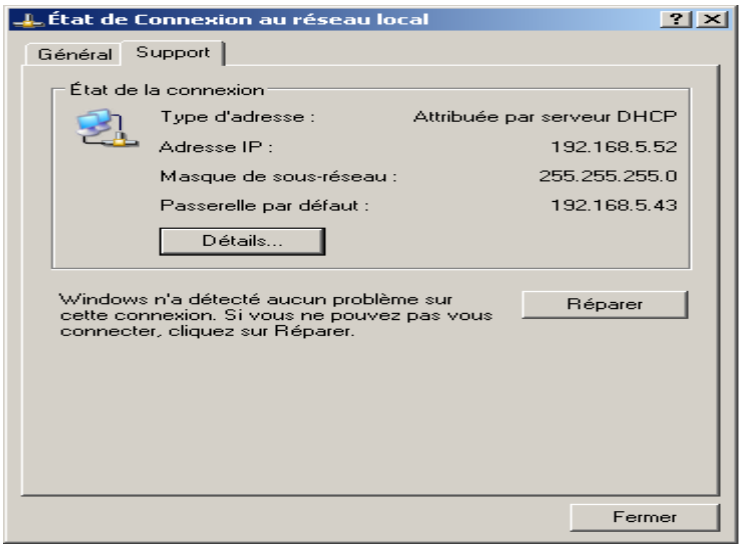

Figure 64:Etat de connexion au réseau local

4. Installation de services de certificats

Dans de nombreuses entreprises, plusieurs collaborateurs peuvent partager la même station de travail et d'autres se déplacent hors de l'enceinte de protection physique de l'entreprise avec leurs portables.

On va alors configurer le service de certificats pour effectuer la demande de certificat EFS par MMC (Microsoft Management Consol), par l'interface Web, et enfin par une GPO (Group Policy Object).

Pour installer le service de certificats, il faut ouvrir une session en tant que Administrateur du domaine « **Mydomain.intra** », et suivre les étapes en s'assurant que l'icone « **services de certificats** » est cochée.

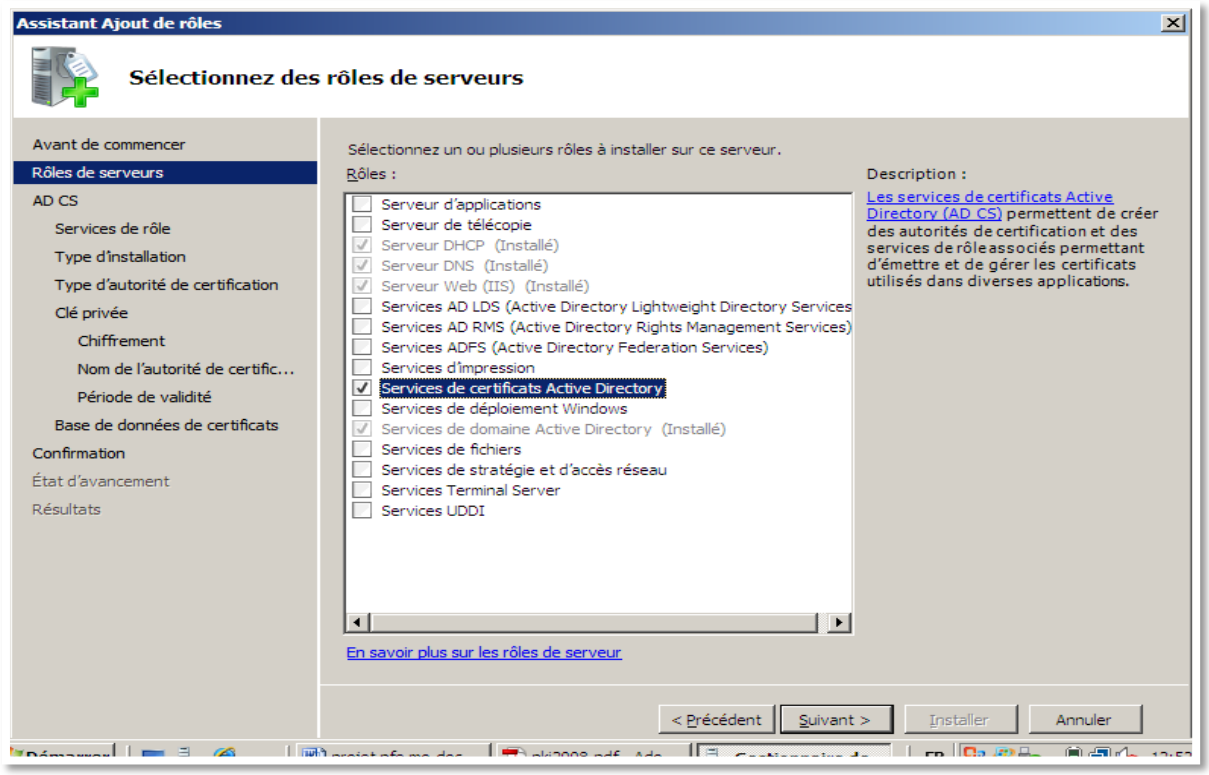

Figure 65:Ajout de services de certificats

En suite, il ya 4 types d'autorités de certification

- Autorités de certification racines d'entreprise : est censée être le type d'autorité de certification le plus approuvé dans l'infrastructure à clé publique d'une organisation, Les services Actives directory doivent être disponibles dans le réseau pour implémenter ce type de CA **(**Autorité de Certificat).

- Autorités de certification secondaire d'entreprise : C'est une CA subordonnée à la CA racine d'entreprise auprès duquel elle obtiendra des certificats. Elle requiert aussi les services Active Directory.
- Autorités de certification racine autonome : Elle est semblable au CA racine d'entreprise mais ne nécessite pas de services Active Directory. Elle peut délivrer des certificats pour effectuer par exemple l'authentification auprès des serveurs Web sécurisés.
- Autorité de certification secondaire autonome : Elle est semblable au CA racine autonome, elle obtient les certificats de cette dernière et ne nécessite pas de services Active Directory.

Dans notre condition de travail nous allons configurer notre autorité de certification en tant que autorités de certification racines d'entreprise : nous Cochons la case « **Autorités racines d'entreprise ».**

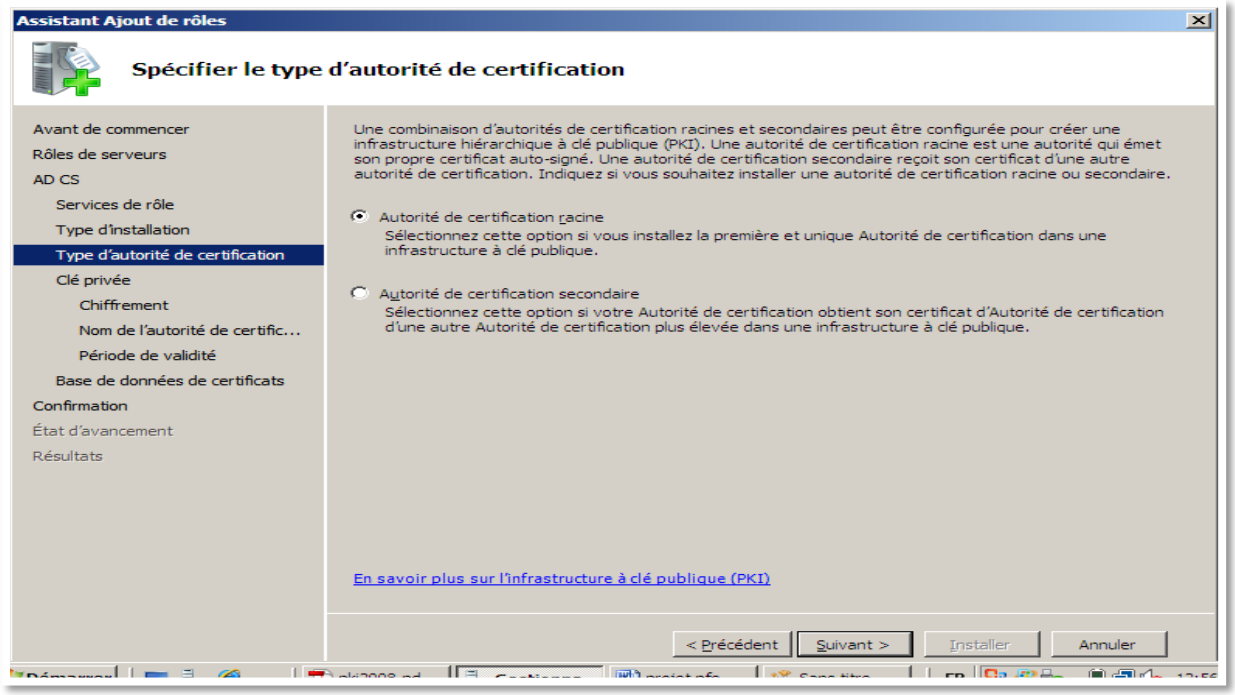

Figure 66:Type d'autorité de certification

Type d'autorité de certification

C'est en suite qu'il va falloir donner le nom à notre autorité de certification « **MyCertificateAuthority »,** en précisant si besoin, le chemin de la base de données de certificats et des fichiers journaux de certificats.

4.1. Déploiement de Certificats Encrypting File System

Pour mettre en évidence notre infrastructure PKI, on va présenter un exemple de déploiement à savoir le déploiement de Certificats EFS : cependant on peut aussi faire d'autre (certificat web, carte à puce…).

Cette section alors présente les processus de création et de déploiement des certificats EFS pour l'infrastructure à clé publique (PKI).

4.1.1. Modèle de certificat Encrypting File System

Les modèles de certificats permettent de personnaliser des certificats émis par les services de certificat, comme leur émission et leur contenu.

L'outil « **Autorité de certification** », présent dans les outils d'administration de Windows Server 2008, vous permet de gérer votre autorité de certification

- La liste des **certificats révoqués** contient tous les certificats révoqués dans cette infrastructure. Il est possible de publier la liste des certificats révoqués manuellement, en effectuant une clique droite sur « **Liste des certificats révoqués** » puis en choisissant « **Publier** » dans **Toutes les tâches**. Vous pouvez publier une liste de base ou seulement une liste delta.
- La liste des **certificats délivrés** vous permet de consulter mais aussi de révoquer les certificats émis par cette autorité de certification. Pour révoquer un certificat, sélectionnez-le puis effectuez une clique droite afin de choisir « **Révoquer un certificat** » dans le menu **Toutes les tâches**. Il est possible de choisir une raison pour cette révocation. Le certificat apparait alors dans la liste évoquée précédemment.
- **Les demandes en attente**, dans le cas d'une autorité de certification autonome, apparaissent ici. Il vous est alors possible de délivrer ou non le certificat à l'utilisateur. Pour cela, sélectionnez le certificat puis effectuez une clique droite dessus. Choisissez « **Délivrer** » ou « **Refuser** » dans le menu **Toutes les tâches**. Dès lors, l'utilisateur peut aller consulter le nouvel état de sa demande.
- **Les demandes ayant échoué** représentent les certificats n'ayant soit pas été autorisés, soit n'ayant pas pu être émis (demande de certificat avancé incorrecte, erreur de création du certificat, etc).

- **Les modèles de certificats** : Vous pouvez administrer ces modèles depuis cet outil.

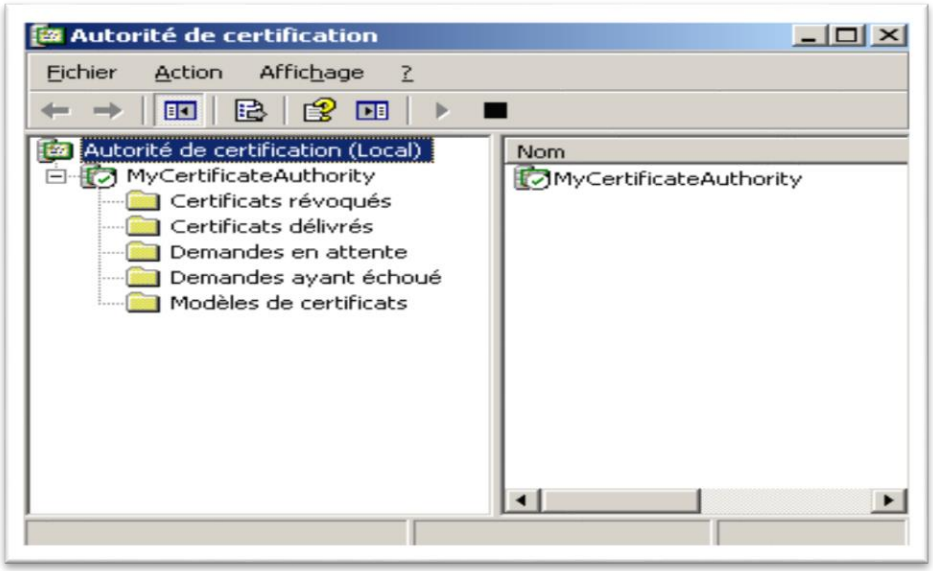

Figure 67:Composants de l'autorité de certification

4 .1 .1.1.Création de modèle de certificat

Pour créer un modèle de certificat, nous allons sur le contrôleur de domaine exécutant la console Windows Server 2008 : créons notre modèle **« MyEFS »** copie du modèle **EFS Basique.**

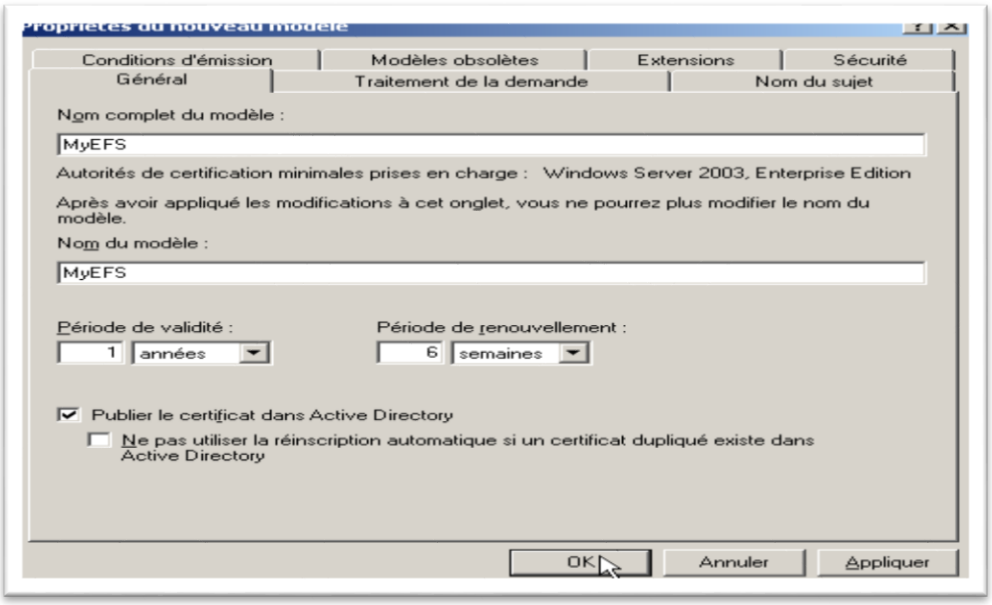

Figure 68:Création du modèle de certificat « MyEFS »

4.2. Gestion des Access Control List des modèle de certificat

Pour autoriser ce modèle de certificat : on doit ajouter l'utilisateur en question (UserMMC) puis lui activons les cases « Lecture » et « Inscrire ».

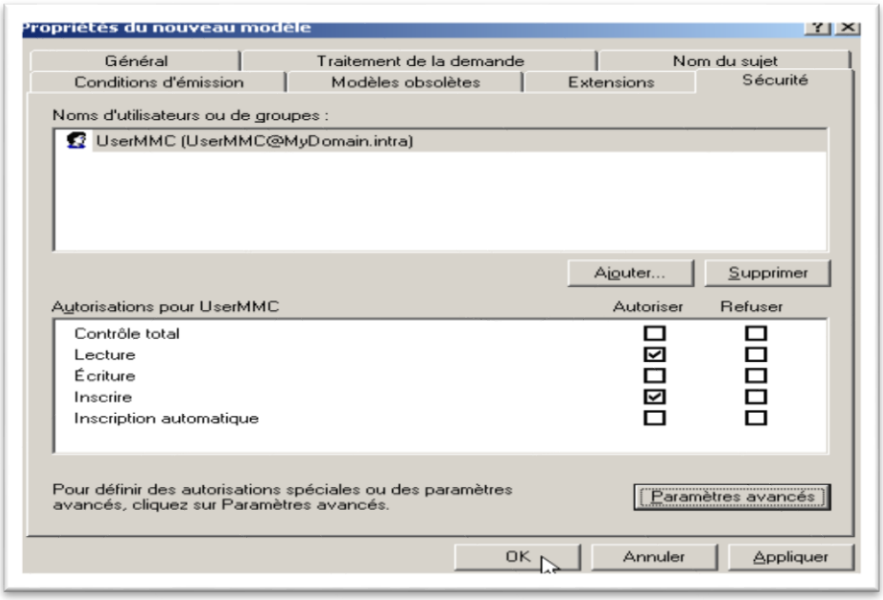

Figure 69:Autoriser le modèle de certificat « MyEFS »

4.2.1. Activation d'un modèle de certificat

Pour ajouter un modèle de certificat a une autorité de certification : il suffit de choisir le modèle déjà crée depuis « **Modèle de certificat à délivrer »**.

4.2.2. Demander un certificat via la console Microsoft Management Consol

Cette Procédure de demande d'un certificat de la console MMC, **nous devons** tout d'abord ouvrir une session en tant que UserMMC sous « MYDOMAIN » par la suit réalisons ceci **:**

- Nous configurons la console **MMC** en ajoutant **composant logiciel enfichable « Certificat »**.
- Par la suite, nous effectuons la demande de certificat.

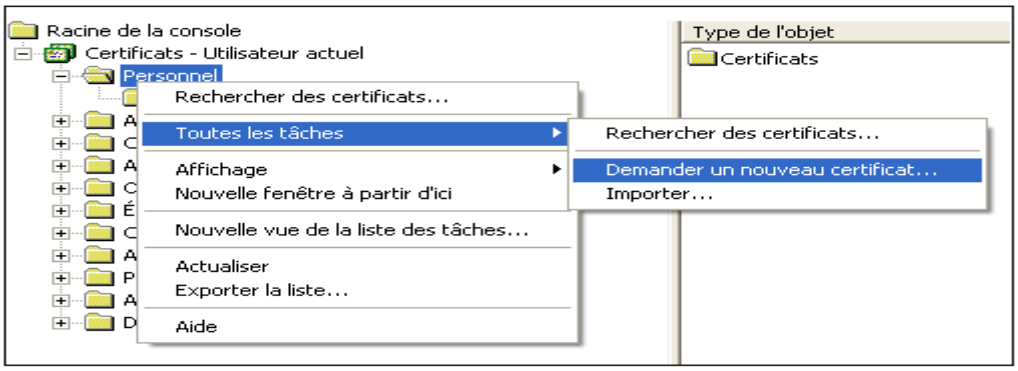

Figure 70:Demande de certificat

C'est ensuite qu'on a défini un **Nom convivial pour notre certificat « MyCertificate ».**

Figure 71:Nom Conviviale de certificat

⇨ Enfin, une boîte de dialogue comportant la mention **La demande de certificat a réussi** apparaît.

4.2.3. Crypter un fichier ou dossier avec Encrypting File System

Après avoir créé configurer l'autorité de certification et le modèle de certificat ainsi que la procédure de demande de certificat, nous pouvons commencer à utiliser EFS pour protéger notre dossier « MyFolder » contre des accès non autorisés.

Pour cela nous devons disposer d'un certificat EFS et d'une autorisation NTFS pour modifier le dossier.

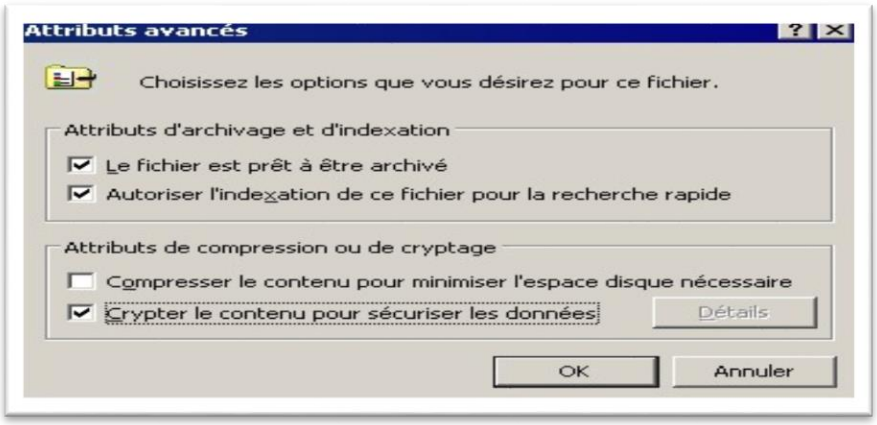

Figure 72:Cryptage de « MyFolder »

4.3. Connexion à un dossier partagé après cryptage

Pour que client « UserMMC » peut accéder à ce dossier partagé (MyFolder), on ouvre une session sous Windows XP en tant que UserMMC :

- Pour atteindre notre partage depuis l'ordinateur client, nous devons utiliser l'UNC « \\myserver.mydomain.intra ».

⇨ Comportement anormal : Accès Refusé à « MyFolder », ceci est contre la nature c-à-d que cet utilisateur puisqu'il dispose de contrôle total sur ce dossier mais il n'a pas pu ouvrir son contenu.

4.3.1. Liaison d'un certificat à un fichier

Nous vêlons protéger les données sensibles par cryptage et permettre des accès multiples. Avec EFS, l'administrateur peut crypter un fichier et donner à d'autres la possibilité d'y accéder. Pour cela, il doit indiquer que le fichier crypté est partagé et activer l'accès partagé en ajoutant les certificats de cryptage EFS de tous les utilisateurs autorisés à y accéder.

Cependant, le partage de données cryptées selon notre cas est soumis à une contrainte : c'est que l'utilisateur ajouté à un fichier crypté doit disposer d'un certificat de cryptage EFS sur l'ordinateur où se trouve le fichier. Et pour pouvoir effectuer cette tâche, nous devrons ajouter l'utilisateur à ce fichier.

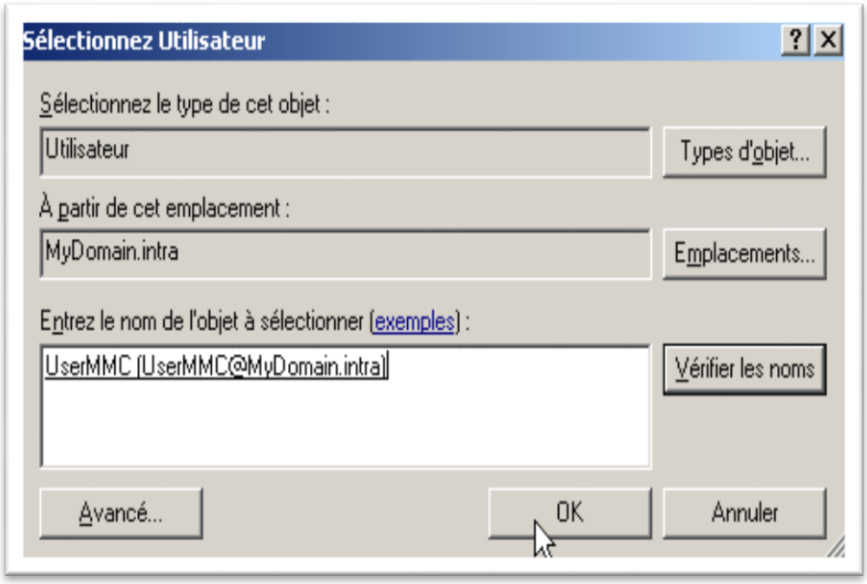

Figure 73:Ajouter l'utilisateur à ce fichier

4.3 .2.L'interface Web «Certsrv »

Pour effectuer une nouvelle demande de certificat, les utilisateurs peuvent se connecter à l'aide d'Internet Explorer sur le site Web : « http://Myserver.Mydomain.intra/certsrv».

- **Demander un certificat** : permet de demander des certificats standards ou avancés.
- **Afficher le statut d'une requête de certificat en attente** : permet dans le cas d'une autorité de certification autonome, de récupérer un certificat après ayant été validé par l'administrateur.
- **Télécharger un certificat d'autorité de certification**: permet de télécharger le certificat de l'autorité de certification ainsi que la liste de révocations des certificats de cette infrastructure.

Pour soumettre une demande de certificat avancée via le Web à une Autorité de certification Windows Server 2008 : on a accédé à « **Créer et soumettre une demande de certificat auprès de cette Autorité de certification »**, en renseignant les informations d'identification et toute autre option requises.

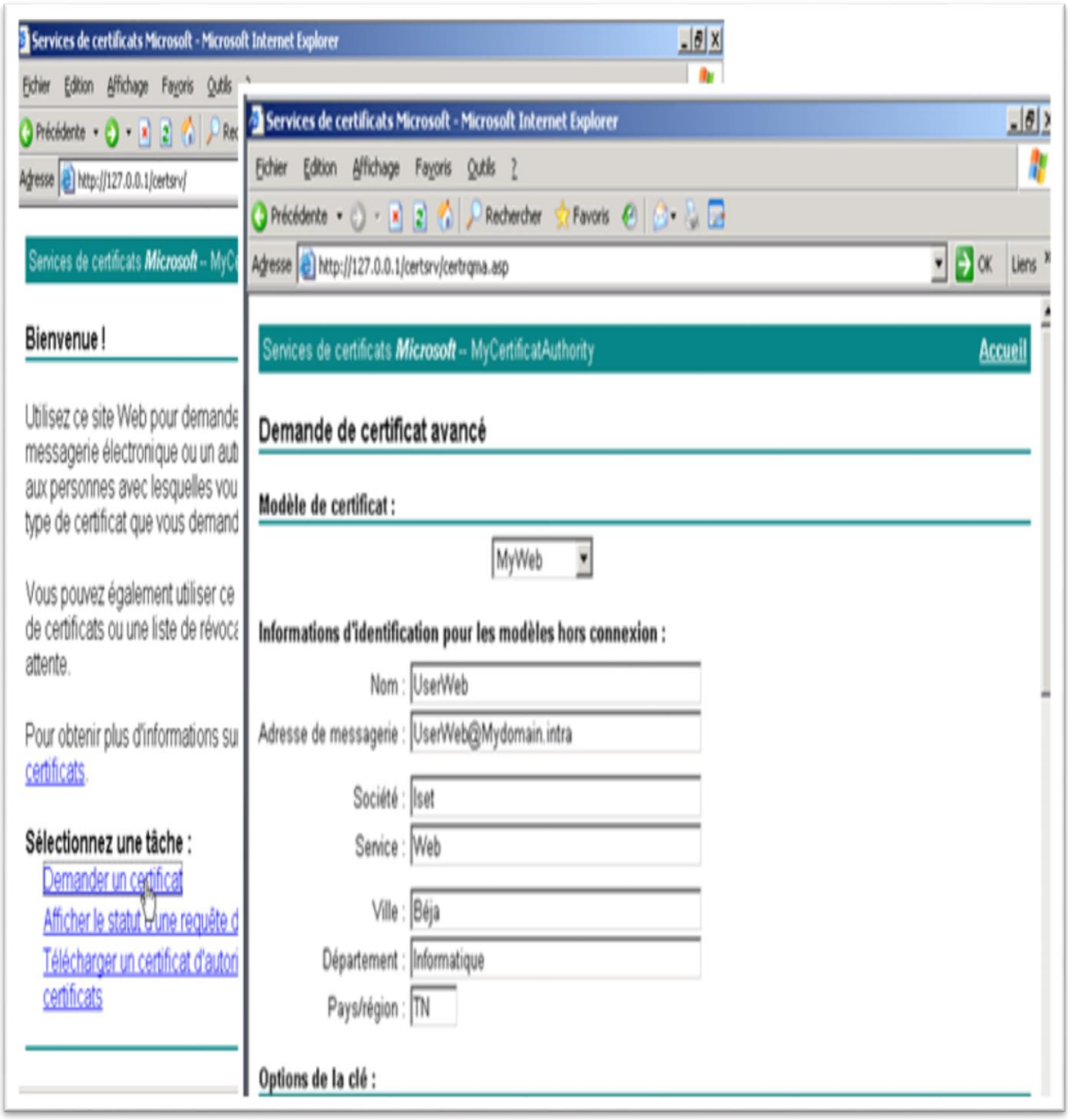

Figure 74:L'interface Web

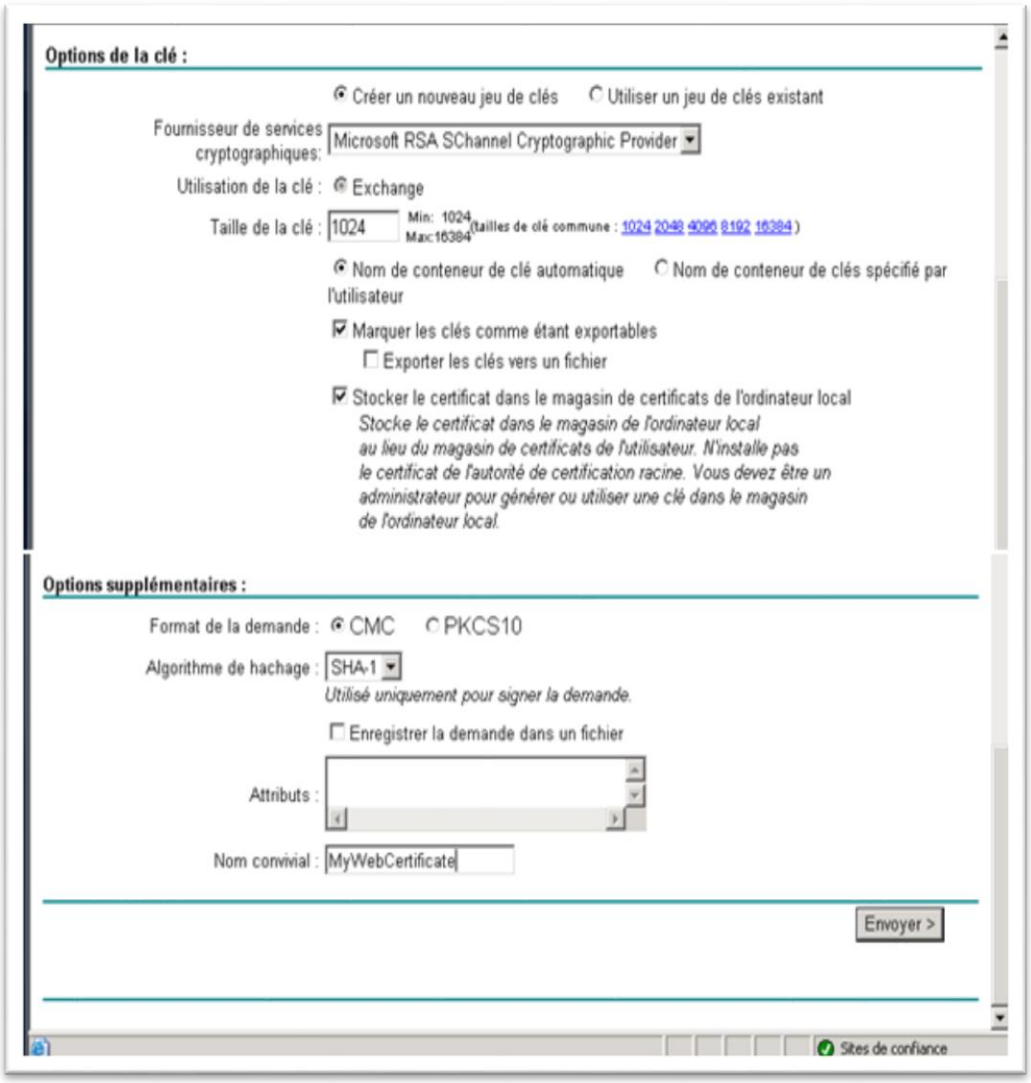

Figure 75:L'interface Web

C’est ensuite qu’on effectue l’une des actions suivantes :

- Si la page Web **Certificat en attente** s'affiche, voir la procédure de vérification d'un certificat en attente dans les Rubriques connexes.
- Si la page Web **Certificat émis** s'affiche, Installons alors ce certificat.

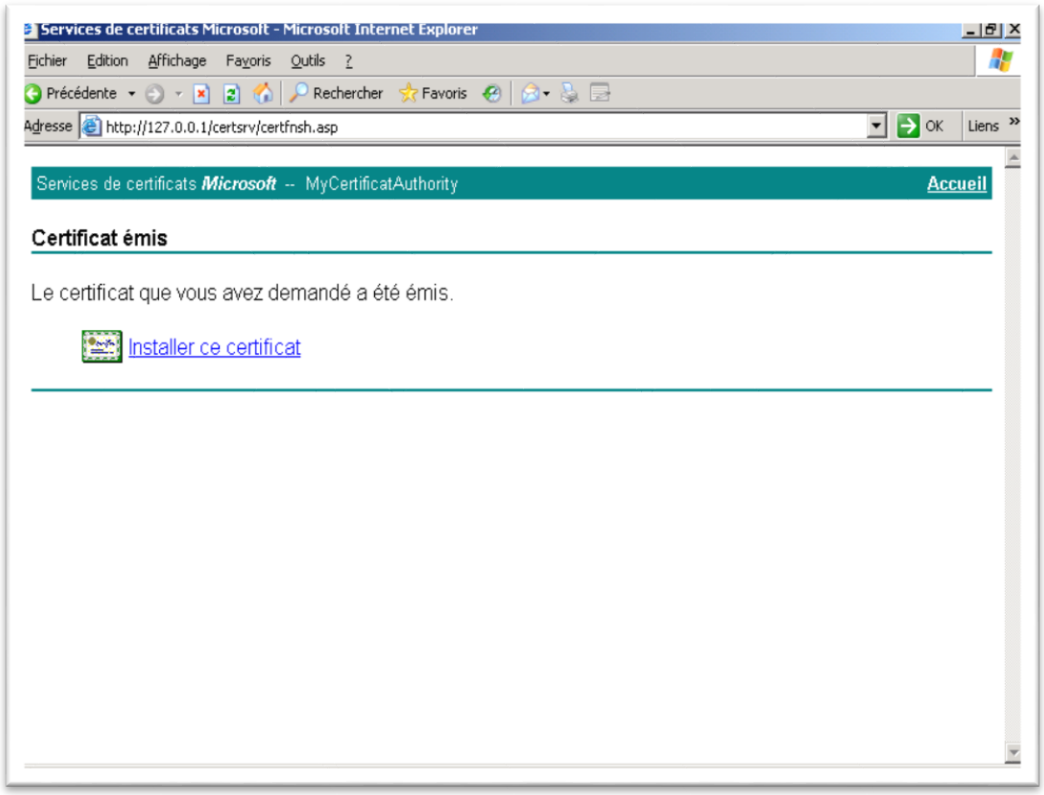

Figure 76:Installation de certificat

Pour afficher cette certificat avec Internet Explorer, On y accède depuis l'onglet **Contenu** de menu **Outils / Options Internet**.

Dès le chiffrement d'un fichier, le **certificat** personnel apparaît :

Dans l'exemple ci-contre, l'utilisateur **UserWeb**, membre du **MyCertificateAuthorit**y, a chiffré un fichier, si bien qu'un certificat lui a été automatiquement attribué.

On sélectionne alors ce certificat, puis on appuie sur le bouton **Affichage** afin d'obtenir ses caractéristiques.

L'onglet **Général** nous montre les **rôles du certificat.**

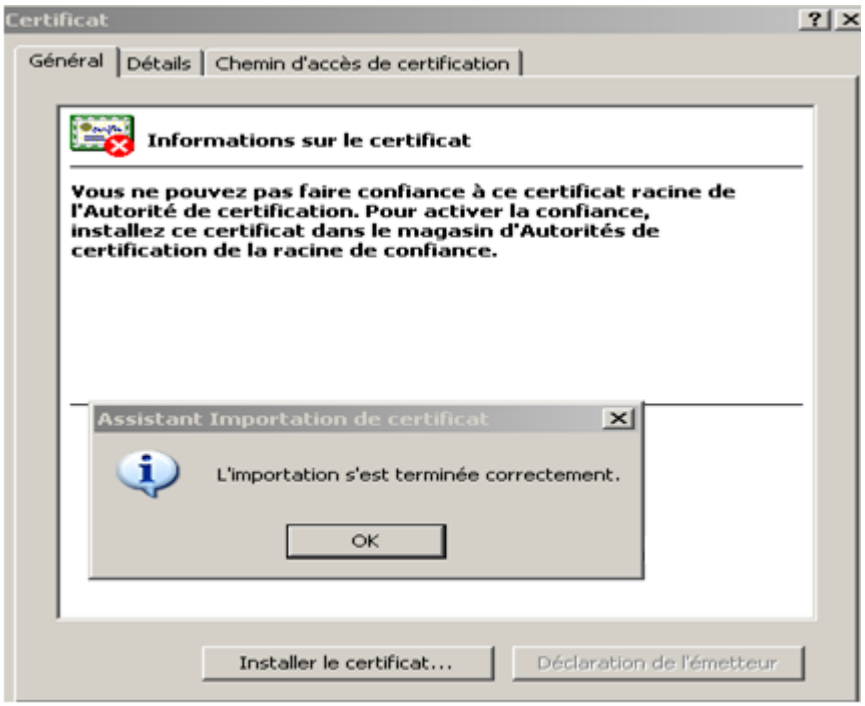

Figure 77: Le certificat MyWeb

5. Conclusion

Nous avons présenté, dans ce chapitre les possibilités de sécuriser les échanges sur un réseau informatique, de garantir l'identité d'un utilisateur ou encore de sécuriser le stockage de ses données à l'aide des différents services sous server 2008 et d'une infrastructure à clés publiques qui se base sur les certificats numériques

Conclusion Générale

Ce travail indique le chemin à suivre pour pouvoir mettre en place une infrastructure active directory et gestion des certificats dans un environnement Microsoft Windows Server 2008, et ce a travers une série d'étapes et de procédures nécessaire afin de réaliser cet objectif. Il s'agit donc d'un travail qui explique à la fois le pourquoi mais aussi montre le comment.

On peut alors parler d'un véritable projet de l'exploitation de déférents service et mise en place d'une infrastructure de clé publique sous Microsoft Windows server 2008 que nous proposons et conseillons aux Tunisie télecom

Pour réaliser ce travail, on a tout d'abord commencé par une étude théorique qui englobe l'infrastructure de clé publique et ces principaux composants, et l'infrastructure Active Directory. Ensuite on a réalisé une partie pratique qui présente en premier temps la préparation d'un environnement ADS et dans un deuxième temps la configuration de services de certificat.

Cette période de stage effectué au sain de Tunisie télecom a été très en matière enrichissante d'informations surtout qu'elle a constitué pour nous une transformation de connaissances de l'état théorique vers l'état pratique de telle façon à les rendre en harmonie parfaite avec les besoins du milieu professionnel : le sens de la responsabilité, les relations humaines, la discipline et l'initiative …

Il ne nous a pas été simple de nous familiariser avec la vigueur et la méthodologie de domaine de travail au niveau de Tunisie télecom, sans l'assistance de ses personnels qui ont eu l'amabilité de nous faire part de leurs suggestions et leurs critiques dans le but de nous envoler toute l'ambigüité.

Nous désirons saisir cette occasion pour dire que ce stage nous a été d'une très grande utilité aussi bien sur le plan pédagogique que sur le plan professionnelle travailler pendant quatre mois consécutifs afin de préparer un projet d'ensemble et le formaliser dans le cadre d'un rapport écrit nécessite beaucoup de réflexion, d'effort et surtout de l'engagement.

Neto-graphie :

[1] : http://fr.wikipedia.org/wiki/Active_Directory ; Le 04/09/2016

[2] :http://webman.developpez.com/articles/dotnet/activedirectory/vbnet/?page=gestion_ad #L5.1.1 ; Le 04/09/2016

[3] :http://technet.microsoft.com/fr-fr/library/cc785263(v=ws.10).aspx ; Le 06/09/2016

[4] : http://www.artduweb.com/windows/dns ; Le 06/09/2016

[5] : http://fr.wikipedia.org/wiki/Domain_Name_System ; Le 06/09/2016

[6] : http://www.labo-microsoft.org/articles/win/delegation_dns/3/#st3 Le 07/09 /2016

[7] : http://fr.wikipedia.org/wiki/Kerberos ; Le 08/10/2016

[8] : http://www.scribd.com/doc/85641687/Rapport-Pfa-Kerberos ; Le 09/09/2016

[9] : http://www.scribd.com/doc/61814154/kerberos ; Le 09/09/2016

[10] http://fr.wikipedia.org/wiki/Domain_Name_System Le 09/09/2016

[11] https://fr.wikipedia.org/wiki/File_Transfer_Protocoll Le 09/09/2016

[12] http://www.linux-france.org/prj/edu/archinet/systeme/ch27s02.html Le 01/10/2016

[13]http://msdn.microsoft.com/fr-fr/library/cc730981(v=ws.10).aspx Le 01/10/2016

[14] : http://www.securiteinfo.com/cryptographie/pki.shtml ; Le 01/10/2016

[15] : http://www.fullsecurity.ch/fileadmin/documents/vpn/Tutorial_PKI_PG.pdf ;

Le 01/10/2016

[16] : http://www.labo-microsoft.org ; Le 01/10/2016

[17] : http://cayrel.net/IMG/pdf/PKI_PGP_OpenSSL.pdf ; Le 10/10/2016

[18] : Sécurisez ses échanges éléctroniques aves une PKI ; Eyralles ; Thierry Autret ;Laurent Belfin Marie-Laure Oble –Laffaire ; Le 1/10/2016