Sujet :

Audit et Sécurité Informatique d'un Réseau Local D'entreprise

Elaboré par

Riadh Abdelli

MEMOIRE

Présenté pour l'obtention du

Diplôme de License appliqué en

Technologie de l'information et communication

UNIVERSITE VIRTUELLE DE TUNIS

Encadré par :

Mr. Kamel Khdiri (UVT Tunis)

Mr. Nizar Hakim (Ste Palma/Aremgroup)

Année Universitaire: 2010/2011

Dédicace

J’ai le grand plaisir de dédier ce travail en témoignage d’affectation et de reconnaissance à tous ceux qui m’ont aidé à le réaliser.

A tous les membres de la famille, pour leurs encouragements, soutiens, affectation et confiance.

A tous mes collègues de travail qui m’ont donné du courage pour continuer les études et pour préparer ce diplôme.

Aux Enseignant et Encadreurs de L’UVT qui nous ont donné confiance et espoir et qui nous ont soutenus durant tout le cursus universitaire de cette année.

Toutes ces valeurs m’ont donné confiance et espoir pour continuer les études et pour préparer ce travail.

Remerciement

Mes sincères remerciements s'adresse à tous le personnel de l'UVT, Administration et Enseignant qui nous donné un soutien précieux.

Mes Encadreur Mr Kamel Khdhiri mon encadreur à l'UVT pour son effort qu'il a déployé dans ce projet, ces conseils, son encouragement, son encadrement sérieux et son soutien moral. L'attention dont il a fait preuve à l'égard de mes travaux et les conseils qu'il m'a prodigué m'ont été très utiles.

Mes vifs remerciements à Mr Maher Affess : directeur Général Ste Palma, Mr Nizar Hakim : Directeur Informatique de ARemGroup, pour leurs soutiens incontestables, leurs conseils, leurs grandes expériences en management.

Je suis honoré par la présence de membres du jury d'avoir accepté ce travail en espérant qu'ils trouveront dans ce projet de quoi être satisfait et auront la gratitude de l'enrichir avec leurs critiques et corrections.

Sommaire

Introduction Générale……...1

Chapitre 1 : Présentation de la Société Palma…….…….……....2

1. **Présentation de la Société**…..……..…….…….……2
2. **Activité de la Société**…..…….……..……....2

Chapitre II : Audit t sécurité réseau informatique ……..…4

1. **Apparition du thème audit informatique en Tunisie**…….……5
2. **Introduction**……..……...…….……6
3. **Audit de sécurité**……..……6

3.1 Définition……6

3.2 Contenu de l'audit……..……6

4. La norme internationale ISO 17799……...7

4.1 Introduction……...7

4.2 Couverture thématique……..…7

4.3 Les contraintes de sécurité……...9

5. la qualité des services de sécurité……...9

5.1 Définition……...9

5.1.1 L'efficacité des services de sécurité……...……9

5.1.2 Leur robustesse……9

5.1.3 Leur mise sous contrôle……9

6. Les risques de sécurité informatique…….……10

6.1. Les types de risques……...10

6.2 Classification des risques……...10

6.2.1. Les risques Humains……...10

6.2.2. Les risques Techniques……...11

7. Méthodologie d'Audit…….……..12

7.1 Définition……..12

7.2. Les phases d'audit……12

7.2.1. Phase préparatoire……..12

7.2.2. Evaluation de la qualité des services……...13

7.2.3. Audit de l'existant……..13

7.2.4. Expression des besoins de sécurité……13

Chapitre III : Audit du réseau informatique de Palma……..…15

I. Phase préparatoire……...15

1. Définition du périmètre de l'étude……...…….15

2 .Les équipements et matériels réseau……...……..15

2.1 Description……..15

2.2 Appréciation……..……..15

II. Audit de l'existant……17
1. Les services de sécurité……17
2. Fonction Informatique de sécurité……17
2.1 Rôle des directions dans le système informatique……17
2.2 Existence de politiques, de normes et de procédures……18
2.3Responsabilité de la direction informatique……19
2.4 Existence de dispositif de contrôle interne……20
3. Décentralisation des traitements……20
3.1 Gestion des configurations……20
3.2 Analyse des demandes arrivant au help-desk……21
3.3 Procédures d'achat……21
4. Equipement Informatique……22
4.1 Inventaires des équipements informatiques……22
4.1.1 Les Unités Centrales……22
4.1.2 Les Switch et les Hubs……22
4.1.3 Les câblage Informatique……22
4.1.4 Les Imprimantes……23
4.2 Environnement du matériel……23
4.2.1Les défauts de climatisation……23
4.2.2 Détection des dégâts d'eau……23
4.2.3 Détection des dégâts du feu……24
4.2.4 Les dégâts d'électricité……24
4.3 Environnement des logiciels de base……24
4.3.1 Les Patchs……24
4.3.2 Les systèmes de fichier……25
4.3.3 Les services inutilisables……25
5. Réseaux et communications……26
5.1 Configuration du réseau……26
5.1.1 Réseau Local……26
5.1.1.1Segmentation……26
5.1.1.2 L'affectation des adresses IP……26
5.1.1.3 Les postes utilisateurs……26
a- Séquence de démarrage……26
b- Session……27
c- Active directory……27
5.2 Identification des risques……27
5.2.1 Les risques humains……27
5.2.2 Les risques techniques……28
5.2.2.1 Les Virus……28
5.2.2.2 Attaque sur le réseau……28
5.2.2.3 Attaque sur le mot de passe……29
6. Sécurité informatique……29
6.1 Repérage des actifs informationnels……29
6.2 Gestion des impacts……30

6.2.1 Intégrité des données……30

III. Solutions de Sécurité……30
1. Déploiement complet d'AD……30
2. Solution Antivirale……31
3. Le serveur de mise à jour……31
4. Système de détection d'intrusion……31
4.1 Système de détection d'intrusion d'hôte……31
4.2 Système de détection d'intrusion réseau……32
5. Solution Firewall……32
5.1 Firewall à filtrage de paquets……32
5.3 Firewall Applicatif……32
6. Annuaire……33
Chapitre IV : Installation et déploiement de Active directory……34

I. Introduction……35
II. Présentation……35

III. Structure d'active directory……36
1. Domaines……36
2. Arbres de domaines……36
3. Forêt……36
IV. Installation Active directory……36
1. Serveur……36
2. Poste client……46
3. Fonctionnement……50
Conclusion ……52

Bibliographie……53

Riadh Abdelli / Lastic3

Introduction

Vu l'importance et l'obligation de l'élaboration d'un audit de sécurité, d'après la loi n°2004-5 du 3 Février 2004. Chaque organisme doit établir un audit de sécurité informatique périodiquement afin d'identifier ses sources de menace et ces dégâts informationnels.

Partant de cette idée, nous avons décidé d'établir un rapport d'audit de sécurité informatique.

Ainsi ce rapport est scindé sur trois parties primordiales :

La première partie comporte une étude théorique qui définie le thème d'audit de la sécurité informatique.

La deuxième partie est axée sur les différentes phases d'audit réparti sur l'analyse.

La troisième partie présente une étude pratique qui définie la mise en œuvre d'une solution SSH.

Chapitre 1 : Présentation de la Société

1/ Présentation :

La société Profilé Aluminium Maghrébin, PALMA, est une société de référence dans le domaine de l'extrusion et du laquage de profilés dédié au secteur de la construction et plus précisément à la menuiserie aluminium.

Forme juridique : SARL

Capital Social : 3.300.000 dinars

Date de création : 2005

Palma est le nouveau né du groupe AREM sur la scène industrielle, qui a été créée en 2005.

PALMA, s'est donné pour objectif de contribuer au développement de cette industrie en Tunisie et dans la rive du Sud de méditerranée. Depuis son entrée en production en 2007. Elle a positionné son offre autour de deux axes d'une part fournir la branche menuiserie en aluminium en profilés d'aluminium extrudé et d'autres part produire, selon un cahier des charges ou des plans détaillés. Ainsi, PALMA est le preneur d'ordres de nombreux métiers tels que l'éclairage public, le sport. Etc. A cela s'ajoutent les profilés standard : cornières, tubes carrées, tubes ronds… dédiés à des usages usuels.

2/ Activité :

Ses performances industrielles par lesquelles se distingue son entrée sur le marché lui ont permis non seulement de réussir son positionnement, mais aussi d'exporter vers l'Algérie et la Libye.

Gamme de produits :

Les profilés standard (cornières, tubes carrées, tubes ronds...), Portes coulissantes, accessoires et produits usuels, les murs rideaux pour les façades et portes d'intérieur…

PALMA préfère des nouveautés qui se démarquent des produits déjà existants par leur caractère innovateur. Plutôt que de recourir à la casse des prix.

La Qualité de leurs produits de point de vue design, esthétique saillie, styles, teintes bien étudiées…, l'a fait démarquer de la concurrence.

Réseaux de distribution :

La société palma a crée un réseau de distribution dans toute les zones de la Tunisie. Ainsi que l'exportation de leurs produits vers l'Algérie, la Libye et l'Italie.

Certification :

Aujourd'hui, toute l'organisation est mobilisée pour la mise en place d'un système de management intégré avec plusieurs composantes : qualité, santé, sécurité et environnement se basant sur les référentiels ISO 9001 version 2000, ISO 14001 et OHAS 18001.

Pour la certification produit, PALMA a entamé les démarches avec l'ADAL (l'association de développement de l'aluminium) afin d'avoir les labels Qualicoat et Qualimarine.

Chapitre II : Audit et sécurité réseau informatique

Chapitre II : Audit et sécurité réseau informatique

1. Apparition du thème audit informatique en Tunisie

L'agence nationale de la sécurité informatique (ANSI) a été crée selon la loi N°2004-5 du 3 Février 2004 et est chargée des missions suivantes :

- Veiller à l'exécution des orientations nationales et de la stratégie générale en matière de sécurité des systèmes informatiques et des réseaux.
- Suivre l'exécution des plans et des programmes relatifs à la sécurité informatique dans le secteur public et assurer la coordination entre les intervenants dans ce domaine.
- Assurer la veille technologique dans le domaine de la sécurité informatique.
- Participer à la consolidation de la formation et du recyclage dans le domaine de la sécurité informatique.
- Etablir les normes spécifiques à la sécurité informatique et élaborer les guides techniques en l'objet et procéder à leur publication.
- Veiller à l'exécution des réglementations relatives à l'obligation de l'audit périodique de la sécurité des systèmes informatiques et des réseaux.

❖ L'apport juridique

La loi N° 2004-5 du 3 Février 2004 a promulgué l'obligation d'un audit périodique de la sécurité des systèmes d'information et des réseaux relevant à diverses structures publiques et privées et qui sera assuré par des experts en audit du secteur privé certifiés par l'agence nationale de la sécurité informatique.

Les organismes soumis à l'obligation d'audit doivent effectuer l'audit périodique de leur système d'information au moins une fois par an. L'opération d'audit se déroule par le biais d'une enquête sur le terrain basé sur les principaux éléments suivants :

- Audit des aspects organisationnels et de la structuration de la fonction sécurité, ainsi que du mode de gestion des procédures de sécurité et la disponibilité des outils de sécurisation du système informatique et de leur mode d'utilisation.

- Analyse technique de la sécurité de toutes les composantes du système informatique, avec la réalisation du test de leur résistance à tous les types de dangers.
- Analyse et évaluation es dangers qui pourraient résulter de l'exploitation des failles découvertes suite à l'opération d'audit.

2. Introduction

En Informatique le terme « Audit » apparu dans les années 70 a été utilisé de manière relativement aléatoire. Nous considérons par la suite un « audit de sécurité informatique » comme une mission d'évaluation de conformité sécurité par rapport à un ensemble de règles de sécurité.
Une mission d'audit ne peut ainsi être réalisée que si l'on a définit auparavant un référentiel, un ensemble de règles organisationnelles, procédurales ou technique de référence. Ce référentiel permet au cours de l'audit d'évaluer le niveau de sécurité réel de terrain par rapport à une cible.

3. Audit de sécurité

3.1 Définition

Un audit de sécurité consiste à s'appuyer sur un tiers de confiance afin de valider les moyens de protection mis en œuvre

Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sures.

3.2 Contenu de l'audit

L'opération d'audit prend notamment en compte des éléments suivants :

- Descriptif des matériels, logiciels et documentations.
- Appréciation globale de l'adéquation entre les besoins et le système d'information existant.
- Examen des méthodes d'organisation, de contrôle et de planification des services informatiques.
- Appréciation de la formation, de la qualification et de l'aptitude du personnel.
- Appréciation de la qualité, de l'accès, de la disponibilité et de la facilité de compréhension de la documentation.

4. La Norme Internationale ISO 17799

4.1 Introduction

Les relations entre entreprises ou administrations rendent nécessaire la définition de référentiels communs .Dans ce contexte, plusieurs normes se présentent pour assurer les relations de la sécurité des systèmes d'information :

- ISO 14000 : traitant de l'environnement.
- FIPS140 : traitant de la cryptographie
- BS7799: Specifications for security management.
- A la différence de ces normes, la norme internationale ISO (International Organisation) 17799 « publiée en juin 2005 » qui est la dernière version de la norme BS7799, peut être utilisée principalement comme base de construction du référentiel d'audit sécurité de l'entité.
- Cette norme est souvent perçue par les spécialistes de la sécurité de l'information comme une réponse à cette attente.

4.2 Couverture thématique :

La norme identifie ces objectifs selon trois critères :

- La confidentialité.
- L'intégrité.
- La disponibilité.

Ces objectifs sont regroupés au travers des dix grandes thématiques suivantes :

*la politique de sécurité : pour exprimer l'orientation de la direction à la sécurité de l'information.

*l'organisation de la sécurité : pour définir les responsabilités du management de la sécurité de l'information au sein de l'entité.

*la sécurité et les ressources humaines : pour réduire les risques d'origine humaine, de vol ou d'utilisation abusive des infrastructures, notamment par la formation des utilisateurs.

*la sécurité physique : pour prévenir les accès non autorisés aux locaux.

*la gestion des opérations et des communications : pour assurer le fonctionnement correct des infrastructures de traitement de l'information, et minimiser les risques portant sur les communications.

*les contrôles d'accès : pour maitriser les accès au patrimoine informationnel.

*l'acquisition, le développement et la maintenance des systèmes :

Pour que la sécurité soit une part intégrante du développement et de la maintenance des systèmes d'information.

*la gestion des incidents : pour s'assurer d'une bonne gestion des événements liés à la sécurité de l'information.

*la gestion de la continuité d'activité : pour parer aux interruptions des activités de l'entité et permettre aux processus cruciaux de l'entité de continuer malgré des défaillances majeures.

*la conformité à la réglementation interne et externe : pour éviter les infractions de nature légale, réglementaire ou contractuelle « pour vérifier la bonne application de la politique de sécurité ».

L'application de cette norme peut donc être le résultat d'une série d'étapes qui peuvent être schématisées ainsi :

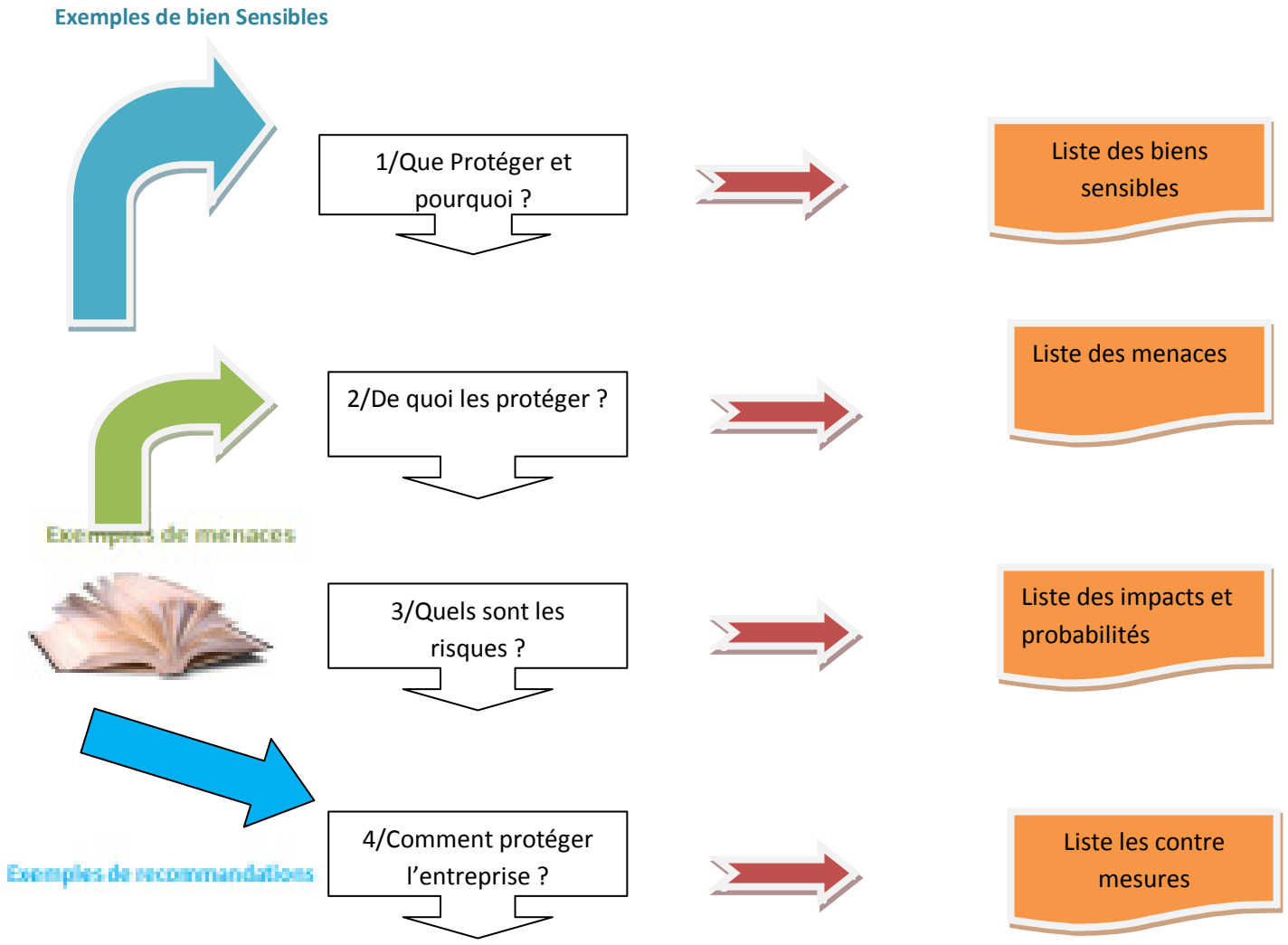


Figure1 : principe de fonctionnement de la norme ISO1779

4.3 Les contraintes de sécurité

*intégrité : garantir que l'information et les processus de l'information demeurent justes et complets.

*accessibilité : garantir que les personnes autorisées ont accès aux informations et aux avoirs associés en temps voulu.

*disponibilité : c'est la possibilité de pouvoir obtenir l'information recherchée au moment ou elle est nécessaire .garantie de continuité de service et de performances des applications ,du matériel et de l'environnement organisationnel.

*confidentialité : assurer que des informations demeurent accessibles qu'aux personnes autorisées.

5. la qualité des services de sécurité :

5.1 Définition :

La qualité de service désigne l'ensemble de paramètre échangé pendant une communication avec connexion pour que les informations passent correctement.

Appliquée aux réseaux à commutation de paquets « réseau basé sur l'utilisation de routeurs », la qualité de service « Qos » désigne l'aptitude à pouvoir garantir un niveau acceptable de perte de paquets, défini contractuellement, pour un usage donné.

Les services de sécurité peuvent avoir des niveaux de performance très différents selon les mécanismes employés .ces niveaux couvrent :

*l'efficacité des services de sécurité.

*leur robustesse (puissance)

*leur mise sous contrôle.

5.1.1 L'efficacité des services de sécurité :

De même que certaines serrures (fermetures) sont plus faciles à violer que d'autre, les services de sécurité sont conçus pour résister à des niveaux d'attaque variables, selon les mécanismes mis en œuvre, ce qui les rend plus ou moins efficaces.

5.1.2 Leur robustesse :

De même que certaines protections actives devenir défaillantes sans que cela provoque une réaction, les services de sécurité peuvent être étudiés pour détecter toute anomalie par des mécanismes complémentaires, ce qui les rend plus ou moins robustes.

5.1.3 Leur mise sous contrôle :

De même qu'un responsable ne sera véritablement sur de la protection apportée par la serrure de sécurité que s'il s'assure que les occupants ferment effectivement à clé l'issue concernée ;, les services de sécurité peuvent être accompagnés de mesure de contrôle destinés à garantir la pérennité des mesures pratiques mises en place, ce qui les rend plus ou moins (sous contrôle).

6. Les risques de sécurité informatique :

6.1. Les types de risques :

En ce qui concerne l'analyse de risque, on a défini 12 types de menaces.

.Accidents physiques.

.Malveillance physique

.Panne du SI

.Carence de personnel.

.Interruption de fonctionnement du réseau.

.Erreur de saisie.

.Erreur de transmission.

.Erreur d'exploitation.

.Erreur de conception/ développement.

.Copie illicite de logiciels.

.Indiscrétion/ détournement d'information

.Attaque logique du réseau.

6.2 Classification des risques :

6.2.1. Les risques Humains :

Les risques humains sont les plus importants, ils concernent les utilisateurs mais également les informaticiens.

.Malveillances : Certains utilisateurs peuvent volontairement mettre en danger le système d'information en y introduisant en connaissance de causes des virus, ou en introduisant

Volontairement de mauvaises informations dans une base de données.

.**Maladresse** : Comme en toute activité les humains commettent des erreurs, ils leur arrivent donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes.

Inconscience : De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sana le savoir.

6.2.2. Les risques Techniques :

.Programmes malveillants : C'est un logiciel développé dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :

.Le virus : Programme se dupliquant sur d'autres ordinateurs.

.Le ver : Exploite les ressources d'un ordinateur afin d'assurer sa reproduction.

.Le Cheval de Troie : Programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur.

.Accidents : il s'agit là d'un évènement perturbant les flux de données en l'absence de dommages aux équipements (panne, incendie, dégâts des eaux d'un serveur ou centre informatique,..).

.Erreurs : que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation de données ou de leurs supports, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données.

.**Technique d'attaques par messagerie** : en dehors de nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques tels que :

.Le Pourriel (Spam) : Un courrier électronique non sollicité, la plus part du temps de la publicité. Ils encombrent le réseau.

.l'Hameçonnage : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles.

.Attaques sur le réseau : les principales techniques d'attaques sur le réseau sont :

. Le Sniffing : technique permettant de récupérer toutes informations transitant sur le réseau. Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications.

.La Mystification (Spoofing) : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles.

.Attaques sur les mots de passe : les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Dans ce cadre, notons les deux méthodes suivantes :

.L'attaque par dictionnaire : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants.

.L'attaque par force brute : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution (par exemple de "aaaaaa "jusqu'à "zzzzzz" pour un mot de passe composé strictement de six caractères alphabétiques).

7. Méthodologie d'Audit

Le but de la méthode utilisée est de mettre à disposition des règles, modes de présentation et schémas de décision.

7.1 Définition :

Une méthodologie est une démarche rigoureuse et standardisée s'appuyant sur des outils tels que des questionnaires, des logiciels spécialisés et permettant de faire l'analyse de sécurité du système d'information dans ce contexte, plusieurs méthodes globales se présentent, citons comme exemples :

.La méthode COBIT (control objectives for information and technology).

.La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).

.La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux).

.La méthode MEHARIE (Méthode Harmonisée d'Analyse Risques).

7.2. Les phases d'audit :

La méthodologie à suivre se décompose en quatre phases :

.phase préparatoire.

.Evaluation de la qualité des services.

.Audit de l'existant.

.Expression des besoins de sécurité " solutions."

7.2.1. Phase préparatoire :

.La définition du domaine couvert qui consiste à délimiter le périmètre de l'étude et à préciser les cellules qui le composent.

.La définition du réseau en précisant les points de forts et de faiblesses.

7.2.2. Evaluation de la qualité des services :

.Le questionnaire d'audit : c'est un questionnaire prenant en compte les services à satisfaire. A chaque service correspond un lot de questions auxquelles il est demandé de répondre par oui ou par non. "annexe 1."

.La mesure globale de la qualité des services : une mesure globale de la qualité ou la performance d'ensemble d'un service de sécurité est élaborée automatiquement par la méthode à partir des réponses au questionnaire d'audit correspondant. Les résultats de l'audit de l'existant sont également utilisés pour établir une image consolidée de l'audit des mesures de sécurité.

7.2.3. Audit de l'existant :

L'audit de l'existant est déterminé en suivant la démarche d'un plan bien organisé et détaillé élaboré par une autre société "SONAIDE"

7.2.4. Expression des besoins de sécurité :

.L'expression des besoins de mesures spécifiques de sécurité : proposer des solutions de sécurité, opérer une sélection des mesures, répondre aux risques majeures découlant de l'étude des menaces les plus graves.

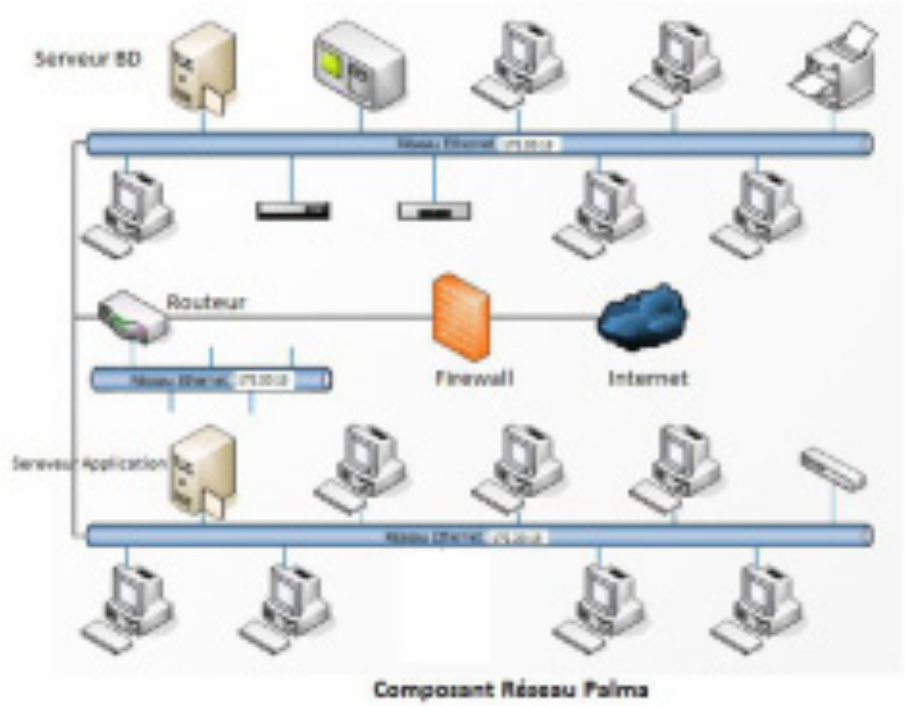
.l'expression des besoins de mesures générales de sécurité : réduire les conséquences des risques majeur (graves.)

Chapitre III : Audit du réseau informatique de Palma

Chapitre III : Audit du réseau informatique de Palma

I. Phase préparatoire

1. Définition du périmètre de l'étude



Composant Réseau Palma

2. Les équipements et matériels réseau

2.1 Description

Le réseau actuel de la société Palma est constitué de 32 postes interconnectées entre eux par une cascade de 2 Switch et 2 Hubs

Le Local de la Société Palma comporte un câblage réseau normalisé. Des câbles paires torsadées en utilisant le protocole de liaison de données Fast Ethernet.

- Plage d'adresse IP
  La Ste Palma dispose de plage d'adresse IP routables alloués au routeur et aux postes de travail connectés au réseau.
- Topologie du réseau
  Tous les postes de travail connectés au réseau sont placés sur le même segment. Des Switchers en cascade sont utilisés dont les différents postes de travail leurs sont connectés.
- Equipements existants
  - Des PC de bureau et portables : Pentium IV, Dual Core
  - Un serveur HP proliant pour de base de données

- Un serveur Dell qui gère différents applications
- Un modem pour l'accès Internet et pour la connexion VPN
- Un Firewall pour contrer les intrusions de l'extérieur
- 2 Switch de 24 Ports et é Hubs de 5 ports
- Des Imprimantes monoposte et réseau

2.2 Appréciation

- Faiblesse du réseau actuel

La situation actuelle souffre de défaillances du fait que le réseau n'obéit pas en effet aux normes d'exploitation. Nous citons si après à titre d'exemple certains problèmes du réseau :

- Absence de stratégie claire de protection des attaques virales (Anti spam par exemple) venant des messageries électroniques depuis les ordinateurs qui ont un accès internet.
- Absence d'un détecteur d'intrusion contre tout accès non autorisé de l'extérieur vers le réseau local.
- Absence d'une politique pour la mise à jour de l'antivirus et des correctifs de Windows.
- Absence d'un mécanisme de filtrage des paquets entrant/sortant.
- Absence d'une stratégie centralisée comme Active directory pour gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité, ...).

- Point Fort du réseau
  - Même avec les faiblesses citées plus haut, le réseau de la Ste Palma présente un ensemble de points forts qu'il faut préserver, voire renforcé Citons à titre d'exemple :
  - L'existence d'un responsable informatique améliore la qualité du travail et offre aux employés l'opportunité d travailler dans les meilleures conditions.
  - La construction du local doté d'un câblage obéissant aux normes en matière de câblage informatique.
  - Prise en compte la sécurité contre les risques physiques (les dégâts d'eau, de feu ou d'électricité).
  - La connexion à internet et aux ressources du réseau local est rapide offrant un confort d'accès
  - Existence d'un Firewall qui permet la protection des réseaux informatiques internes de l'entreprise contre les intrusions du monde extérieur, en particulier les piratages informatiques.

II. Audit de l'existant

1. Les services de sécurité

Un service de sécurité est une réponse à un besoin de sécurité, exprimé en terme fonctionnel décrivant la finalité du service, généralement en référence à certains types de menaces

En Plus, un service de sécurité peut ainsi lui-même être constitué de plusieurs autres sous-services de sécurité pour répondre à un besoin.

Nous avons définit des domaines de responsabilité, numérotés de 1 à 16, qui abordent dans la société, du point de vue de la sécurité :

- Sécurité des locaux
- Sécurité réseau étendu
- Sécurité du réseau local
- La sensibilisation et la formation à la sécurité
- Contrôle d'accès applicatif
- Contrôle de l'intégrité des données
- Confidentialité des données
- Disponibilité des données
- La sécurité logique des équipements
- Les plans de secours
- Les plans de sauvegarde
- Authentification
- Contrôle d'accès
- Configuration des logiciels
- La maintenance
- La gestion des incidents

2. Fonction Informatique de sécurité

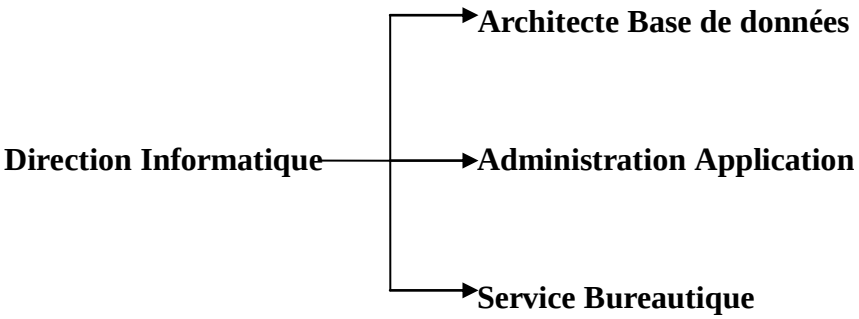
La qualité de l'organisation générale de la fonction informatique dépend essentiellement de principaux facteurs : le positionnement de la fonction informatique, la séparation des fonctions et la gestion du personnel informatique.

2.1 Rôle des directions dans le système informatique :

Le système d'information est considérée comme un sous-système de l'entreprise lié au système opérant qui réalise les activités, et au système de décision qui fixe les objectifs et effectue les choix.

La Ste Palma est une filiale d'Aremgroup, ainsi la direction Informatique est centralisée au siège.

L'organigramme du système d'information est comme suit



Organigramme du système Informatique

- Selon un Budget, les nouveaux projets informatiques qui sont proposés suite à un besoin exprimé par la direction informatique, sont transmis directement vers la direction générale pour acceptation ou refus.
  - **Appréciation**
- L'existence de procédures de suivi fournit un avantage très important pour le bien de l'entreprise car ces procédures permettent :
  - L'évaluation du patrimoine existant
  - Le suivi de la situation actuelle
  - Le développement bien structuré des projets
  - Présence de planification pour l'application informatique

2.2 Existence de politiques, de normes et de procédures :

L'existence de poétique, méthode, normes et procédures informatiques permettent de justifier que la fonction informatique est bien organisée et qu'elle respecte les règles de travail, et ce afin d'avoir un service de qualité et bien développé.

Actuellement, le service informatique fonctionne selon une poétique informatique de sécurité claire et formalisée mais ne suit pas :

- Une méthode clairement définie
- Une norme de sécurité informatique standard
- Une procédure informatique formalisée

- **Appréciation**

- L'inexistence de méthode de d'évaluation des risques et de la gestion de la sécurité informatique a pour conséquence :
  - Le non garanti de l'harmonisation et de la qualité des applications.
  - Le non maitrise de la gestion des projets informatiques
  - Difficulté d'évaluation du personnel informatique

- L'inexistence de procédure informatique formalisée relative à la sécurité peut engendrer :
  - Difficultés de la mise à jour des applications informatiques
  - Absence de formation et de sensibilisation des utilisateurs
  - Absence d'un guide de sécurité aux utilisateurs
  - **Recommandation**
    Chaque direction peut suivre des fiches techniques ou des manuels de politique, de norme et de procédures servant à la planification, à l'organisation, au contrôle et à l'évaluation de la direction informatique concernant :
  - Les normes de management de la sécurité du système informatique
  - Les procédures par la mise à jour des applications informatiques et l'élaboration d'un guide de sécurité aux utilisateurs.
  - Existence de toute documentation relative aux politiques, normes et procédures informatiques.

2.3 Responsabilité de la direction informatique

Les responsabilités de la direction informatique doivent être justifiées par les éléments suivants :

- Définition claire des responsabilités de la direction informatique
- Equilibre entre les pouvoirs et les responsabilités de la direction informatique

- Le service informatique a un rôle moteur dans la circulation de l'information dans la société, il est suivi par des responsables spécialistes :
  - Administrateur Réseau
  - Maintenance équipement informatique

  - **Appréciation**

    La séparation des fonctions des responsables informatiques diminue les risques d'accumulation des fonctions

    La présence d'une structure dédiée à la planification et le suivit des travaux informatiques offre une souplesse lors de :

    - L'exploitation
    - La gestion du parc informatique
    - La gestion du réseau LAN et WAN

  - **Recommandation**
    La direction Informatique doit instaurer une structure qui sera chargé à la planification et au suivit des travaux afin de :
  - Suivre la productivité du personnel informatique

- Satisfaire les besoins des décideurs et des utilisateurs
- Assurer l'existence de la veille technologique dans le secteur informatique.

2.4 Existence de dispositif de contrôle interne

La réalisation des objectifs du contrôle interne nécessite la mise en œuvre par l'entreprise, des dispositifs suivants :

- Un système adéquat de définition des pouvoirs et des responsabilités.
- Une documentation satisfaisante décrivant les procédures de la société
- Des procédures efficaces permettant de respecter une structure d'audit interne efficace.
-

3. Décentralisation des traitements

3.1 Gestion des configurations

Actuellement, l'architecture appliquée par la plupart des postes à Palma, est une architecture client/serveur à deux niveaux « appelé aussi 2-tiers ». Cela signifie que les machines clientes contactent un serveur de base de données, qui leur fournit des services de données. Ces services sont exploités par des programmes, appelés programme client, s'exécutant sur les machines clientes.
En plus, on constate seulement quelques postes appliquent une architecture à trois niveaux (appelé architecture 3-tiers). Cela signifie qu'il y'a un niveau intermédiaire, c'est-à-dire il existe une architecture partagée entre trois ressources :

- Premièrement, un client « l'ordinateur demandeur de ressources » équipé d'une interface utilisateur chargée de la présentation.
- Deuxièmement, un serveur d'application est chargé de fournir la ressource mais faisant appel à un autre serveur.
- Troisièmement, un serveur de base de données, fournissant au serveur d'application les données dont il a besoin.

- **Appréciation**

  On constate qu'une architecture client/serveur 2 tiers est évolutive, car il est facile d'ajouter ou d'enlever des clients sans perturbation et modification du fonctionnement du réseau

  En plus l'architecture 2 tiers interroge un seul serveur pour évaluer un service demandé. Mais, en cas de panne, seul ce serveur fait l'objet d'une réparation, et non le PC client, cela signifie que ce serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui.

- **Recommandation**

L'implémentation d'une architecture multi tiers est plus efficace pour la société. Cette architecture qui se base sur la technologie du Web met en évidence au moins 3 niveaux

3.2 Analyse des demandes arrivant au helpdesk :

Il n'existe aucun guide d'aide aux utilisateurs pour les applications utilisées.

- **Recommandation**

  Afin d'établir une méthode de sécurité, il est important de développer un guide d'aide utilisateur pour les services de la sécurité appliquée dans la société et bien analyser les demandes arrivant à ce guide.

3.3 Procédures d'achat

Les achats Informatiques sont initiés généralement par le responsable du service informatique et réalisé par le chef du service financier.

- Le rôle du responsable informatique

  L'utilisateur final informe sur un problème qui s'est produit lors de son utilisation d'un tel équipement.

  Une consultation décrit si cet équipement a besoin d'un entretien ou il est inutilisable, d'où une demande d'achat doit être élaborée par le responsable informatique.
- Le rôle du chef du de service financier

  Ce dernier reçoit la demande d'achat émanant du responsable

  Elabore les consultations

  Procède au choix du fournisseur en concertation avec les acteurs concernés

  Elabore un bon de commande selon le budget accordé

  Reçoit le bon de livraison et la facture après leur prise en charge par le responsable concerné
- **Appréciation**

  L'informatisation du système de gestion et d'organisation relatif à la gestion de l'approvisionnement constitue un point fort envers l'amélioration du fonctionnement de ce domaine. Cela a pour conséquence de bien contrôler :
- La gestion des commandes et des fournisseurs
- Le tenu et le suivi du stock
- Prise en charge automatiquement des entrées et sorties
- Contrôle du stock
- Gestion des inventaires

4. Equipement Informatique

4.1 Inventaires des équipements informatiques

4.1.1 Les Unités Centrales

De références, Dell, HP, la configuration est généralement comme suit :

- Processeur : Dual Core
- Mémoire Minimale de 512 MO
- Espace disque minimal de 160 GO

- **Appréciation**
  On constate que la configuration matérielle répond aux exigences minimales pour la configuration des applications et pour une exploitation facile et assurer une rapidité des traitements

4.1.2 Les Switch et les Hubs

Les différents postes de travail sont interconnectés via des Switch et des hubs en cascade.

- **Appréciation**
  Les Switch envoient directement le trafic seulement à la destination, contrairement aux hubs qui envoient le trafic à tous les ports et non seulement à la destination
  L'utilisation des hubs augmente le risque d'intrus obtenant l'accès au réseau et menant une attaque d'écoute.
- **Recommandation**
  Il est conseillé de remplacer tous équipements passifs par des équipements actifs

4.1.3 Le câblage Informatique

Le système de câblage informatique installé au bâtiment Palma est conçu pour fonctionner de façon optimale pour permettre des évolutions futures.
Tous équipements informatiques existent dans la société sont interconnectés via le câblage de type paire torsadé catégorie 5
Les boitiers des prises muraux sont repérés par des étiquettes portant un numéro unique sur le réseau et qui est repéré facilement dans le panneau de brassage pour l'interconnexion avec les commutateurs « prise Rj45 ».

- **Appréciation**
  Le système de câblage installé fonctionne selon les besoins en termes de bande passante et de débit disponible
  Le Schéma de conception de câblage pour l'interconnexion des différents équipements n'est pas bien géré : les extrémités des câblages interconnectés aux commutateurs ne sont pas bien organisées.

L'absence d'un suivi d'entretien de câblage peut être un point faible pour la sécurité du câblage.

4.1.4 Les Imprimantes

Chaque service possède une imprimante configurée et partagée sur un poste utilisateur

- **Appréciation**

La présence de ce type d'imprimante est un avantage pour la société de point de vue cout d'une part, mais aussi c'est une vulnérabilité vu que toute panne du PC ou est configuré l'imprimante engendre une panne générale pour tous les connectés

- **Recommandation**

Prévoir l'utilisation des imprimantes réseaux, ou la configuration est gérée par l'administrateur réseau, et ou l'attribution d'accès est selon le paramètre IP de l'imprimante et non d'un PC.

4.2 Environnement du matériel

4.2.1 Les défauts de climatisation

Il n'a pas une salle informatique pour héberger le matériel informatique. Les serveurs, modem sont placés dans un bureau bien climatisé, l'accès à ce bureau n'est pas restreint.
L'armoire informatique se situe dans un emplacement qui n'est pas climatisé.

- **Appréciation**

Les équipements informatiques sont conçus pour travailler dans un environnement spécifique pour respecter les conditions normales de fonctionnement. Alors que ces conditions sont partiellement respectées.

- **Recommandation**

Il est recommandé de

- Spécifier un local protégé et bien aménagé comme salle informatique.
- Placer un climatiseur dans le local ou se trouve l'armoire informatique.

4.2.2 Détection des dégâts d'eau

LA société ne possède pas un détecteur contre l'humidité et les dégâts d'eau.

- **Appréciation**

Il y'a risque de propagation de l'eau dans la salle connectique ce qui peut causer des incidents à citer :

- Divers cours-circuits entrainant la rupture de service des équipements
- Détérioration des équipements
- Corrosion des câbles et connecteurs

- **Recommandation**

Il est conseillé d'utiliser des tubes isolés pour le câblage d'alimentation, ainsi que pour le câblage réseaux.

4.2.3 Détection des dégâts du feu

Il y'a une présence physique contre les dégâts de feu.

- **Appréciation**

Ce type d'incident peut mener à la destruction partielle de la société et particulièrement des équipements informatiques.

- **Recommandation**

Il est recommandé de

- Eviter le stockage de produits inflammables dans le bureau ou se trouve le matériel informatique
- Vérifier régulièrement les circuits électriques

4.2.4 Les dégâts d'électricité

Les deux serveurs, les Switch, ainsi que quelques postes utilisateurs sont protégés par des onduleurs contre les coupures électriques

- **Appréciation.**

L'utilisation d'un onduleur est un point fondamental pour protéger le matériel informatique contre :

- Coupure électrique
- Surtension, c'est-à-dire une valeur nominale supérieure à la valeur maximale prévue pour le fonctionnement normal.
- Sous-tension, c'est-à-dire une valeur nominale inférieure à la valeur maximale prévue pour le fonctionnement normal.

- **Recommandation**

Il est recommandé de brancher les onduleurs avec tous les équipements informatiques, afin de commander proprement l'extinction de données en cas de coupure de courant.

4.3 Environnement des logiciels de base :

Les systèmes d'exploitation installés au niveau des différents postes de travail sont :

- Windows XP
- Windows Vista
- Windows 7
- Windows 2003 Server

4.3.1 Les Patchs

Les patchs de sécurité « service Pack » ne sont pas installés au niveau des postes de travail.

- La majorité des patchs de sécurité relatifs au système d'exploitation ne sont pas appliqués. Cette faille offre aux intrus la possibilité d'exploiter les vulnérabilités non corrigées.
- **Recommandation**
  Il est conseillé d'installer un serveur de mise à jour Windows afin de distribuer les patchs sur le réseau vers les postes de travail.

4.3.2 Les systèmes de fichier

Le système de fichier détecté au niveau des postes utilisateurs est le FAT et le NTFS.

- **Appréciation**
  Le système de fichier FAT n'offre pas de mécanisme de sécurité qui peuvent être appliqués aux fichiers stockés sur le disque tel que :

- La sécurité des fichiers : les droits d'accès peuvent être assignés aux fichiers et répertoires.
- Le cryptage : les fichiers peuvent être stockés sur le disque sous forme crypté.
  - **Recommandation**
    Il vaut mieux réinstaller les postes utilisateurs en FAT par le système de fichier en NTFS, ceux ci peut offrir
- Une sécurité au niveau des fichiers et des dossiers
- Une compression des fichiers
- Un quota des disques
- Un cryptage de fichiers
-

4.3.3 Les services inutilisables

Des services non nécessaires sont en exécution sur les postes travail.

- **Appréciation**
  Le démarrage de certains services non nécessaire augmente le risque d'une intrusion au système, si jamais une vulnérabilité liée à ce service apparait. Le service d'accès à distance au registre est activé, ce service permet de manipuler à distance la base de registre
- **Recommandation**
  Il faut arrêter et désactiver le démarrage automatique des services non nécessaires pour les postes utilisateurs, exemple vous pouvez désactiver le Netmeeting « le partage de bureau à distance Netmeeting ».

5. Réseaux et communications

5.1 Configuration du réseau

5.1.1 Réseau Local

5.1.1.1 Segmentation

Absence de séparation logique au niveau du réseau. Tous les postes connectés sont placés sur le même segment.

- **Appréciation**
  Les données échangées par le personnel (administratif, technique etc...) dispose du même niveau de confidentialité ce qui augmente le risque de perdre la confidence dans des données échangées.
- **Recommandation**
  Il faut appliquer une séparation physique du réseau local en utilisant les commutateurs entre les équipements interconnectés selon le degré de confidentialité.

5.1.1.2 L'affectation des adresses IP

Les adresses IP des équipements du réseau sont attribuées de façon statique

- **Appréciation**
  Un attaquant, à l'aide d'outils spécifique, peut facilement identifier l'adresse IP de l'équipement désigné, pour accéder à ces ressources.
- **Recommandation**
  Il est conseillé d'intégrer un serveur DHCP qui permet d'attribuer automatiquement des adresses IP à la station de travail.

5.1.1.3 Les postes utilisateurs

a- Séquence de démarrage

La séquence de démarrage actuellement défini pour plusieurs postes de travail est le suivant

- Disquette/CDROM
- Disque Dur

- **Appréciation**
  L'utilisation de cette séquence de démarrage offre à l'intrus, obtenant l'accès physique au poste de travail, le lancement d'un système d'exploitation pour mener ces attaques.
- **Recommandation**
  La séquence de démarrage qui doit être appliquée est la suivante :

- Disque Dur
- CD ROM/Disquette

b- Session

La plus part des postes utilisateurs ne possède pas de session, mais il y'a d'autres qui possèdent la configuration de deux sessions :
Une pour l'administrateur informatique, et l'autre pour l'utilisateur.

- **Appréciation**

  L'absence de session offre à l'intrus la possibilité de collecter un ensemble d'information sur la cible (nom d'utilisateur, partage).
  L'audit des postes de travail connectés au réseau a relevé la présence de cette vulnérabilité pour plusieurs postes.
- **Recommandation**

  L'exigence d'avoir au moins deux sessions pour chaque poste, une pour l'utilisateur avec privilège restreint de préférence pour ne pas modifier la configuration initiale et la deuxième pour l'administrateur qui est le seul à pouvoir modifier les paramètres de base.
  Une authentification par Login et Mot de passe est obligatoire.

C- Active directory

Les postes client sont intégrés dans le WORKGROUP, ou le compte d'accès par défaut est administrateur sur les postes client ce qui provoque Requêtes nombreuses provenant des postes clients qui veulent devenir le "maitre de Workgroup"

- **Appréciation**

  Active directory fournit des services centralisés de Gestion des ressources et de la sécurité, il permet également l'attribution et l'application de stratégies.
- **Recommandation**

  Une Intégration des postes de travail au domaine spécifié est nécessaire. Cette étape donne à l'administrateur un droit de contrôle des utilisateurs en leur attribuant les droits biens spécifiés et de gérer les différents ressources, aussi il y'a un gain de temps pour l'administrateur et pour l'utilisateur.

5.2 Identification des risques

5.2.1 Les risques humains

La société n'a pas pu parfaitement lutter contre les risques humains :

- Les risques de malveillance

- Les risques de maladresse et d'inconscience des utilisateurs :
  - Effacer involontairement les données ou des programmes
  - Exécuter un traitement non souhaité
  - Introduire des programmes malveillants sans le savoir
    - **Appréciation**
      La majorité des failles et incidents de sécurité sont dus à des erreurs humains, des utilisateurs sont encore inconscient ou ignorant des risques qu'ils encourent l'ors de l'utilisation d'un programme mal veillant.
    - **Recommandation**
      Une formation des utilisateurs est nécessaire à la sécurité informatique. Il faut s'assurer également que les utilisateurs sont sensibilisés aux risques informatiques et adhérant aux exigences de sécurité des systèmes d'information.

5.2.2 Les risques techniques

5.2.2.1 Les Virus

La majorité des postes de travail disposent d'un antivirus installé (Kaspersky) qui vérifie en permanence les fichiers de l'ordinateur, mais il y'a quelques un qui sont mal configurés et qui ont une mise à jour ancienne.

- **Appréciation**
  La mise à jour des antivirus est paramétré et se fait automatiquement chaque 2 heures et un scan se fait automatiquement à chaque démarrage.
- **Recommandation**
  Il faut reconfigurer le programme antivirus convenablement pour quelques postes afin d'avoir une protection fiable, une mise à jour automatique et un scan régulier.

5.2.2.2 Attaque sur le réseau

Absence d'un système de détection d'intrusion contre tous accès non autorisé depuis l'extérieur

- **Appréciation**

Le système de détection d'intrusion sera un composant primordial pour les mécanismes de sécurité des réseaux. Grace à lui on peut détecter les tentatives d'attaques de l'extérieur

- **Recommandation**
  Il est conseillé d'implanter un système de détection d'intrusion sécurisé :

- **NIDS :** (Network Intrusion Détection System): est un détecteur d'intrusion réseau qui détecte les attaques réseau en se basant sur une base de signatures très à jour.
- **HIDS :** (Host Intrusion Détection System) : Ces ondes s'incèrent entre les applications et le cœur du système d'exploitation pour protéger des applications ou des serveurs critiques.
  Les solutions **IDS** (Intrusion Détection System) pour réseau garantie une surveillance permanente du réseau.

5.2.2.3 Attaque sur le mot de passe

Aucun mécanisme n'est pris en considération pour lutter contre les attaques sur les mots de passe.

- **Appréciation**
  Un intrus peut mener une attaque pour collecter les mots de passe afin d'accéder aux ressources matériels mises en question.
- **Recommandation**
  L'administrateur doit respecter les exigences de la stratégie de mot de passe

- Durée limitée de la conservation de l'historique
- Durée de vie maximale
- Durée de vie minimale
- Exigence de complexité
- Longueur min
- Cryptage

6. Sécurité informatique

6.1 Repérage des actifs informationnels

Les systèmes d'information comme ensemble de processus à valeurs ajoutées tiennent compte des données entrantes et sortantes

- **L'intranet**
  Les services fournis par l'intranet
- Une base de données qui héberge tous données informationnelles « Financier, Personnel, scientifique…..) dont les utilisateurs ont besoin.
- Le partage : la plupart des utilisateurs utilise le partage de fichiers comme étant une source d'échange de données.
- Messagerie Interne entre Utilisateur
- **Extranet**
- Les services fournis par l'extranet sont
- Les courriers électroniques
- L'utilisation de l'internet
- **Appréciation**

L'intranet constitue un moyen essentiel pour moderniser la communication entre les utilisateurs, partager l'information

- **Recommandation**

  Il faut bien administrer le partage et l'accès aux fichiers en utilisant l'annuaire Active directory pour bien préserver les droits d'accès et centraliser la gestion des ressources.

6.2. Gestion des impacts

6.2.1 Intégrité des données

Faible intégrité pour les données traitées par les logiciels bureautique « Excel, Word, Excel »

Moyenne intégrité pour les données traitées par le logiciel « OCTAL » et une intégrité totale sur le logiciel « SAGE » et « DECEMPRO ».

- **Appréciation**

  L'intégrité des données peut être potentiellement en danger car aucun test formalisé n'a été réalisé contre l'effacement accidentel des données et les pannes matérielles sur les divers supports d'information.

- **Recommandation**

  Pour protéger les données contre les erreurs de manipulations des utilisateurs ou contre les catastrophes naturelles, il faut prendre compte :

- RAID « Redondant Array of Independant Disq » désigne une technologie permettant de stocker les données sur de multiples disques durs
- Contrôle de la saisie des données : les données sensibles doivent être autocontrôlées par une personne assurant la vérification des données saisies
- Intégration d'un outil de vérification d'intégrité

III. Solutions de Sécurité

1. déploiement complet d'AD

Grace à Active directory sécurité est entièrement intégrée dans Active Directory. Le contrôle d'accès peut être défini non seulement sur chaque objet de l'annuaire, mais aussi sur chaque propriété de chacun des objets.
Active Directory fournit à la fois le magasin et l'étendue de l'application pour les stratégies de sécurité.
Une stratégie de sécurité peut inclure des informations de compte, telles que des restrictions de mot de passe applicables sur l'ensemble du domaine ou des droits pour des ressources de domaine spécifiques.
Les stratégies de sécurité sont mises en place par le biais des paramètres de Stratégie de groupe. Ainsi les avantages de Active directory est :

- Amélioration de la productivité des utilisateurs
- Réduction des tâches d'administration informatique
- Amélioration de la tolérance de pannes pour réduire les périodes d'indisponibilité
- Amélioration de la sécurité

2. Solution Antivirale

La protection antivirale consiste à appliquer une solution antivirus client/serveur Cette solution consiste à installer un serveur antivirus sur le réseau, et de déployer sur chaque machine le client associé. Une telle solution permet de centraliser la tache d'administration : mise à jour des fichiers de signature et déploiement automatiquement sur les postes clients.

L'antivirus proposé implémente aux moins les fonctionnalités suivantes : exécution en tache de fond, détection automatique, récupération des fichiers importants après une suppression accidentelle, filtrage du courrier électronique indésirable et mise à jour automatique.

3. Le serveur de mise à jour

Microsoft software update services (SUS) est un maillon essentiel dans la nouvelle politique de sécurité de Microsoft

3.1.Principe de fonctionnement

Le fonctionnement de SUS est relativement simple. Pour déployer, deux modules doivent être mis en place, un client et un serveur.

- Le module serveur télécharge les informations à partir du cite Windows update de Microsoft et vous laisse choisir les mises à jour à installer sur les postes clients.
- Le module client quand à lui communique périodiquement avec le serveur pour savoir si des mises à jour sont disponibles, si oui il les installe.

Cette solution offre un avantage de réduction de la bande passante internet et une simplification d'administration et de déploiement.

4. Système de détection d'intrusion

Les IDS (Intrusion Détection System) sont des équipements logiciels ou matériels Qui permettent de mettre en place des mécanismes de détection d'intrusion.

On distingue principalement deux catégories de détection d'intrusion :

- Host-based IDS (HIDS : Host intrusion Detection System)
- Network-based IDS (NIDS : Network Intrusion Detection System)

4.1 Système de détection d'intrusion d'hôte

Cette catégorie (HIDS) a pour objectif la surveillance de l'activité d'une machine en utilisant les fichiers de log du système et en contrôlant l'intégrité de celui-

ci avec des outils comme AIDE (Advanced Intrusion Détection Environment) qui est un logiciel qui permet de contrôler l'intégrité du système de fichier sur un serveur.

4.2 Système de détection d'intrusion réseau

Un NIDS travaille sur les données transitant sur le réseau. Il peut détecter en temps réel une attaque s'effectuant sur l'une des machines. Il contient une base de données avec tous les codes malicieux et peut détecter leurs envois sur une des machines.

On peut citer par exemple un NIDS appelé Snort.

5. Solution Firewall

La solution de filtrage consiste à déployer trois niveaux consiste à déployer trois niveaux de filtrage sur les ressources du réseau, comme écrit ci-dessous :

5.1 Firewall à filtrage de paquets

La majorité des équipements de routage actuels disposent d'une fonctionnalité de firewalling basé sur le filtrage de paquets. Cette technique permet de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC.

5.2 Firewall Statefull Inspection

Cette solution sera implémentée par un équipement firewall matériel qui agit en tant que passerelle, afin de garantir la sécurité entre le trafic du réseau interne, public et démilitarisé.

La technologie « stateful Inspection » permet de contrôler les couches applicatives, sans nécessité de proxy applicatif pour chaque service, en cherchant une session correspondante pour les paquets analysés. La solution Firewall proposée supportera de plus les fonctionnalités suivantes :

- Module d'interconnexion des réseaux virtuels
- Authentification, autorisation d'adresse NAT
- Journalisation et support du service SYSLOG

Au niveau architecture du réseau, le firewall proposé définira trois domaines de sécurité :

- Zone interne : Représente le réseau local de l'organisme. Cette zone contient le plus haut niveau de sécurité
- Zone externe : représente la zone publique par laquelle passe tout le trafic de destination internet.
- Zone démilitarisée : représente la zone contenant les serveurs visibles de l'extérieur dont l'accès est public.
-

5.3 Firewall Applicatif

Un Firewall applicatif sera installé sur tous les postes client et les serveurs afin de protéger en premier lieu des tentatives d'intrusion interne.

En deuxième lieu, l'utilisation d'un firewall applicatif permet de contrôler les connexions depuis et vers ces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants.
On peut citer par exemple un Firewall : Mod_security et Mod_Proxy.

6. Annuaire

Un annuaire permet de stocker des données légèrement typées, organisées selon des classes particulières et présentées dans un arbre.

On peut trouver des solutions d'annuaire comme LDAP, c'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leur valeur : la racine O »organisation », le sous ensemble d'une organisation ou « organizationlUnit », le nom de domaine Dc »domainComponent » et la personne Person « schéma standard pour une personne »

Chapitre IV : Installation et déploiement d'Active directory

I. Introduction

Vu les vulnérabilités qu'on a rencontré pendant l'étude de l'audit de la sécurité informatique du réseau de la Société Palma et vu l'augmentation des services (messagerie, serveur fichiers…), je propose le passage du Workgroup au domaine et l'installation de l'annuaire Active directory afin de centraliser la gestion des ressources et la mise en place des règles de sécurité.

Le facteur temps et sécurité sont des facteurs importants pour les sociétés, ceci pousse les décideurs à avoir des solutions centralisées de gestion des ressources informatiques.

II. Présentation

Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire *Active Directory* est basé sur les standards TCP/IP , DNS, LDAP, Kerberos, etc.

Le service d'annuaire Active Directory doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc.

Active Directory permet de recenser toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. Active Directory constitue ainsi le moyeu central de toute l'architecture réseau et a vocation à permettre à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

Fig. 1 :

Active Directory est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits

associés il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise.

III. Structure d'active directory

1. Domaines

Un domaine Active Directory (AD) est la principale frontière logique dans un annuaire. Pris séparément, un domaine AD ressemble beaucoup à un domaine NT. Les utilisateurs et les ordinateurs sont tous stockés et gérés dans les limites qu'il définit. Les domaines AD servent de limites de sécurité pour les objets et contiennent leurs propres stratégies de sécurité. Par exemple, chaque domaine peut appliquer aux utilisateurs des stratégies de mots de passe différentes. Un domaine étant une organisation logique d'objets, il peut aisément s'étendre sur plusieurs emplacements physiques.

Un domaine regroupe des ordinateurs, des périphériques, des utilisateurs. C'est une sorte de zone sécurisée, sur laquelle on ne peut pénétrer que quand on a été authentifié par le Contrôleur de Domaine.

2. Arbres de domaines

Un arbre Active Directory est composé de plusieurs domaines reliés par le biais d'approbations transitives bidirectionnelles, qui partagent un schéma et un catalogue global communs.

3. Forêts

Une forêt est un groupe d'arbres de domaines interconnectés. Des approbations implicites existent entre les racines des arbres d'une forêt. Si tous les domaines et arbres de domaines ont en commun un même schéma et un même catalogue global, ils ne partagent en revanche pas le même espace de noms.
La structure d'Active Directory lui permet de gérer de façon centralisée des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites.

IV. Installation Active directory

Ord il faut bien spécifier les plages d'adressage IP pour les différents matériels

J'ai pris comme exemple :

- Pour les postes de travail : de 172.20.13.100 à 172.20.13.200
- Pour les serveurs : de 172.20.13.1 à 172.20.13.10
- Pour les routeur/éléments actifs : de 172.20.13.11 à 172.20.13.20
- Pour les Imprimantes : de 172.20.13.21 à 172.20.13.30

1. Serveur

Procédure

- menu « Démarrer. Tous les Programmes. Outils d'administration. Gérer votre serveur ». Cliquez sur le lien « Ajouter ou supprimer un rôle ».

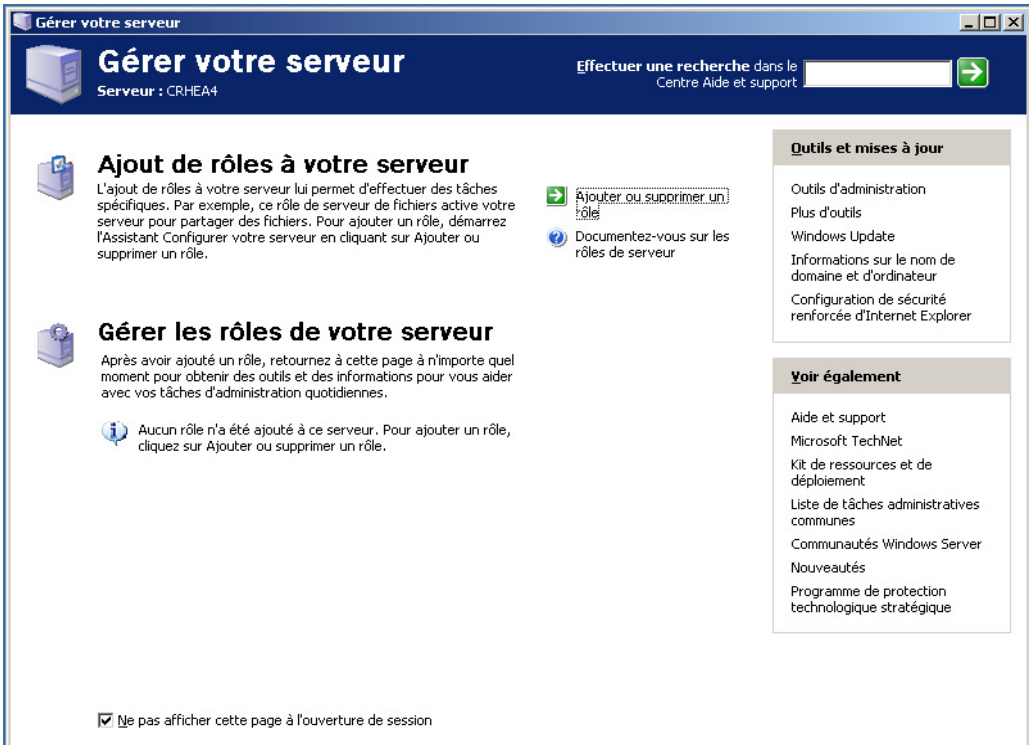


Figure 1 : l'assistant « Gérer votre serveur »

L'étape préliminaire (figure 2) vous invite à effectuer les dernières vérifications avant le début de la procédure d'installation d'Active Directory. Quand tous les éléments nécessaires sont en place, cliquez sur le bouton « Suivant > » pour continuer.

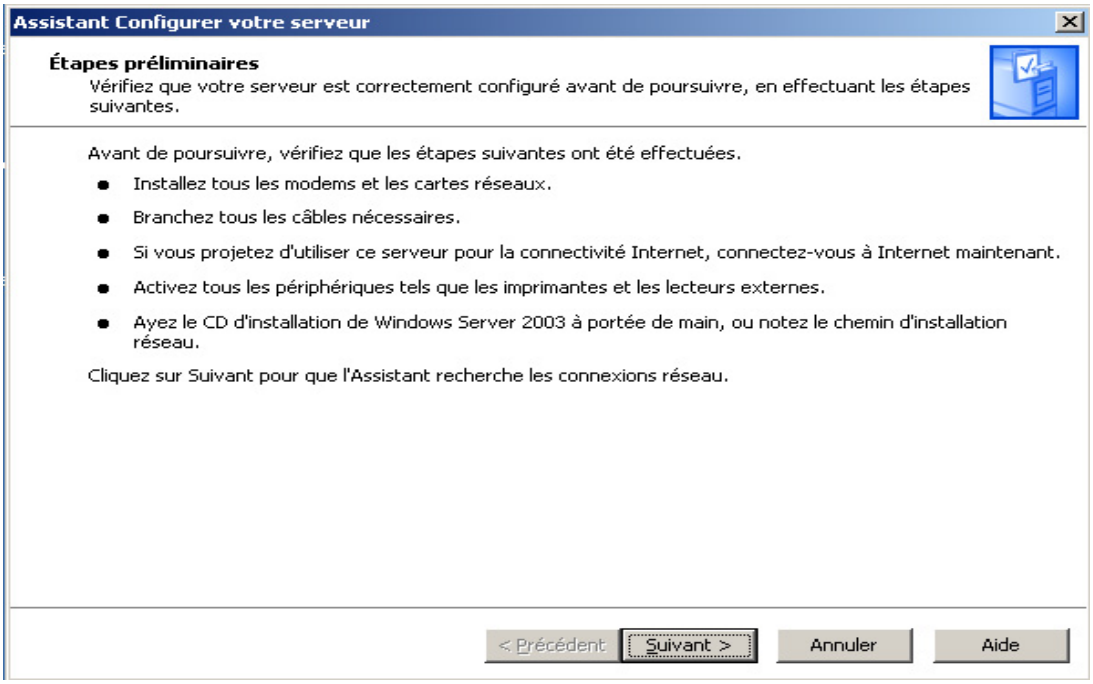


Figure 2 : Etapes préliminaires, instant des ultimes vérifications

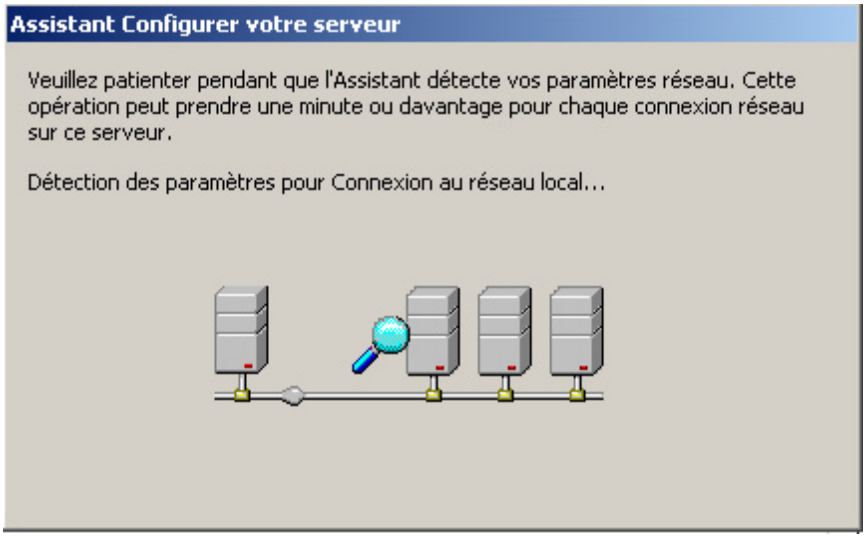


Figure 3 : Détection des paramètres réseau

Ensuite on spécifier le nouveau rôle « contrôleur du domaine » dans la liste de l'assistant « Configurer votre serveur » de la (Figure 4)

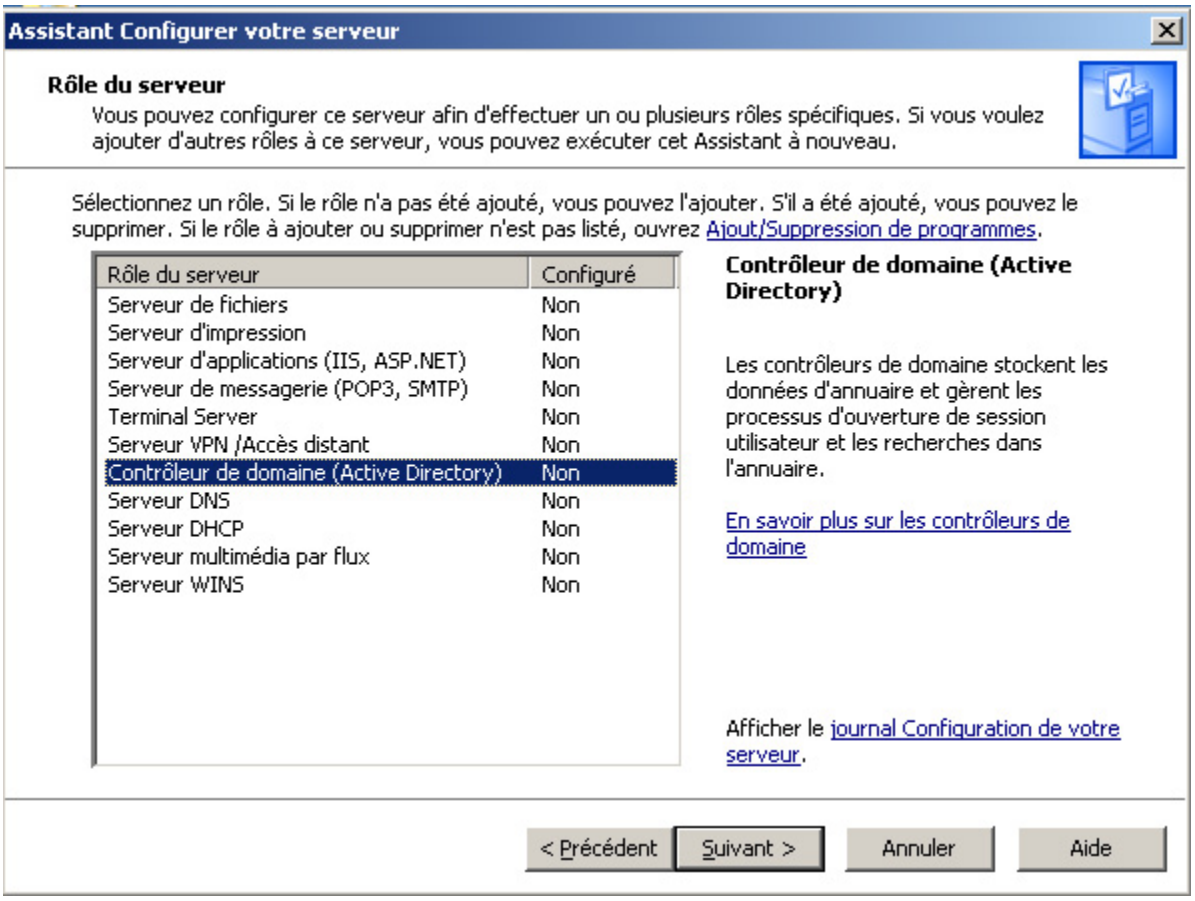


Figure 4 : Sélection du rôle Contrôleur de domaine

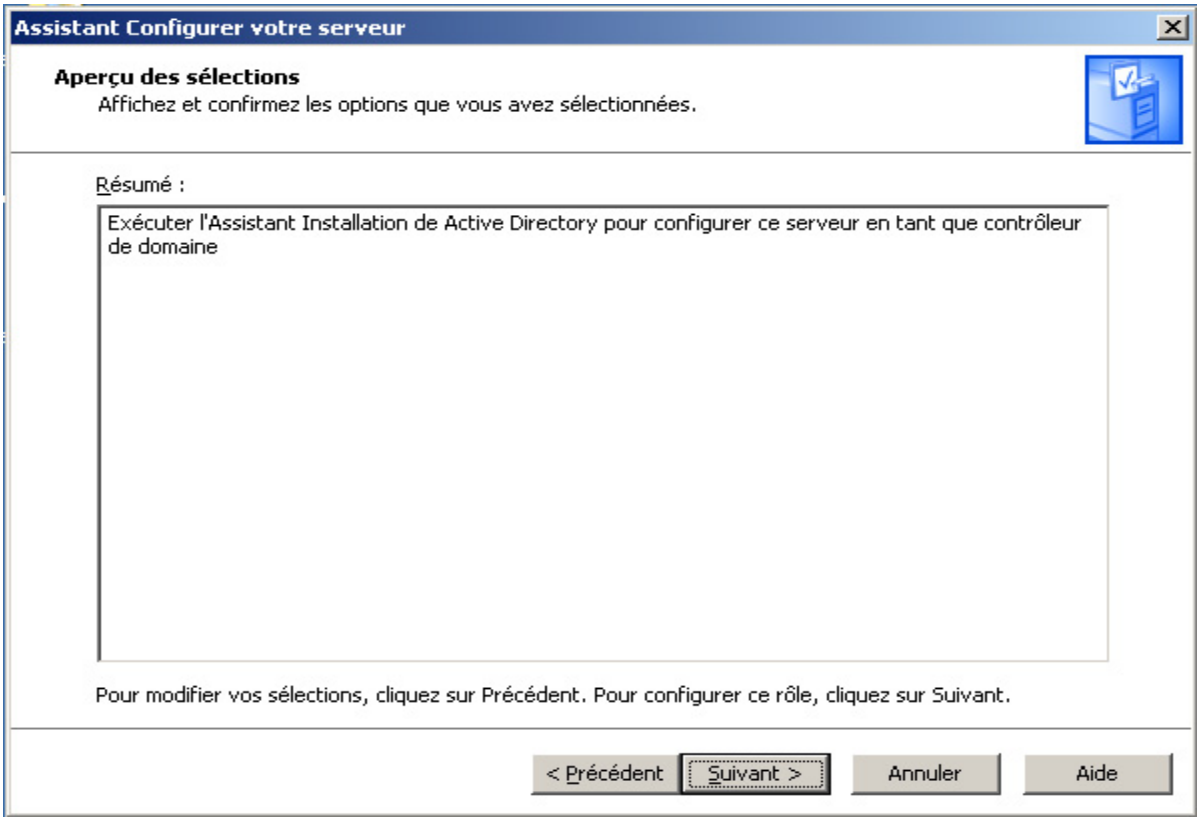


Figure 5 : Résumé de l'installation à effectuer

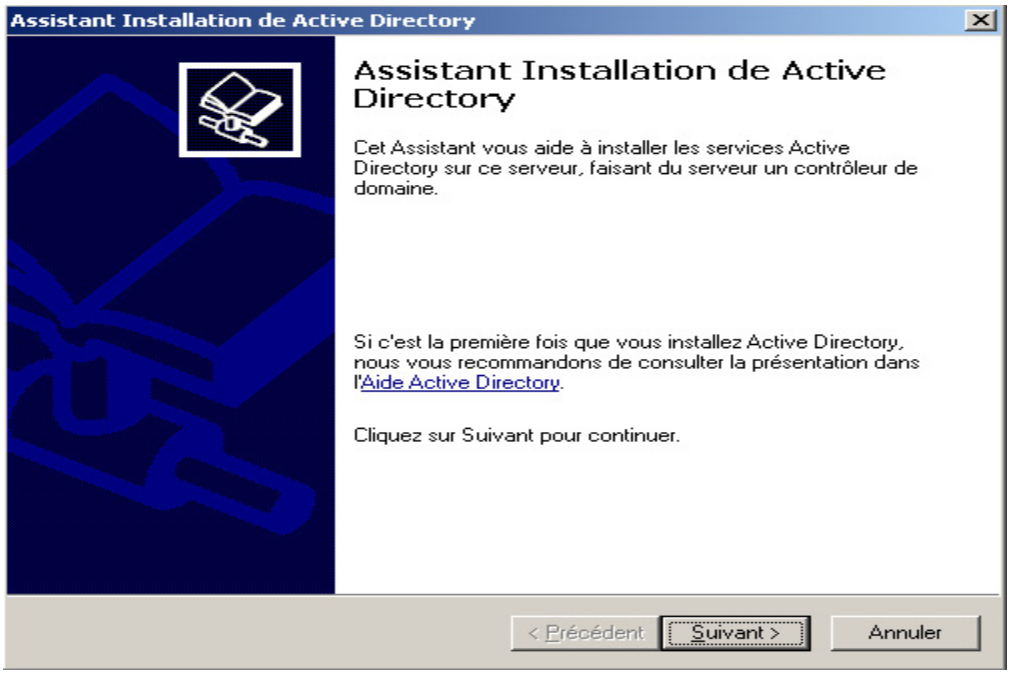


Figure 6 : Lancement de l'.assistant d'installation d'Active Directory

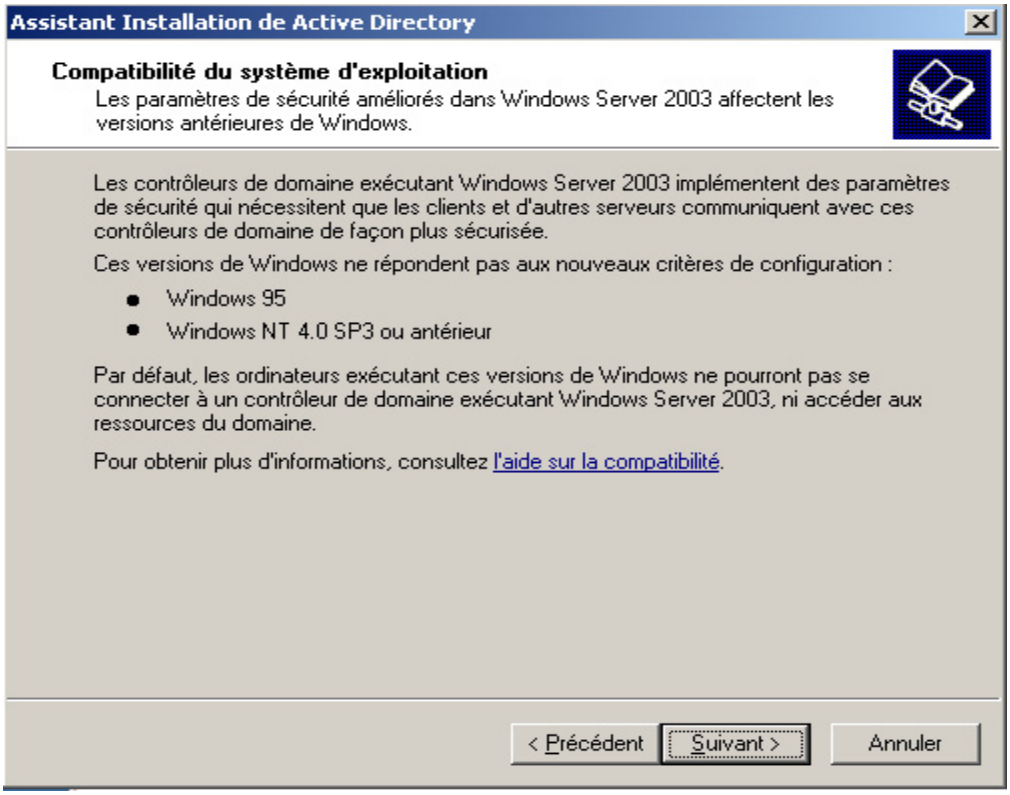


Figure 7 : Compatibilité des systèmes d'exploitation clients

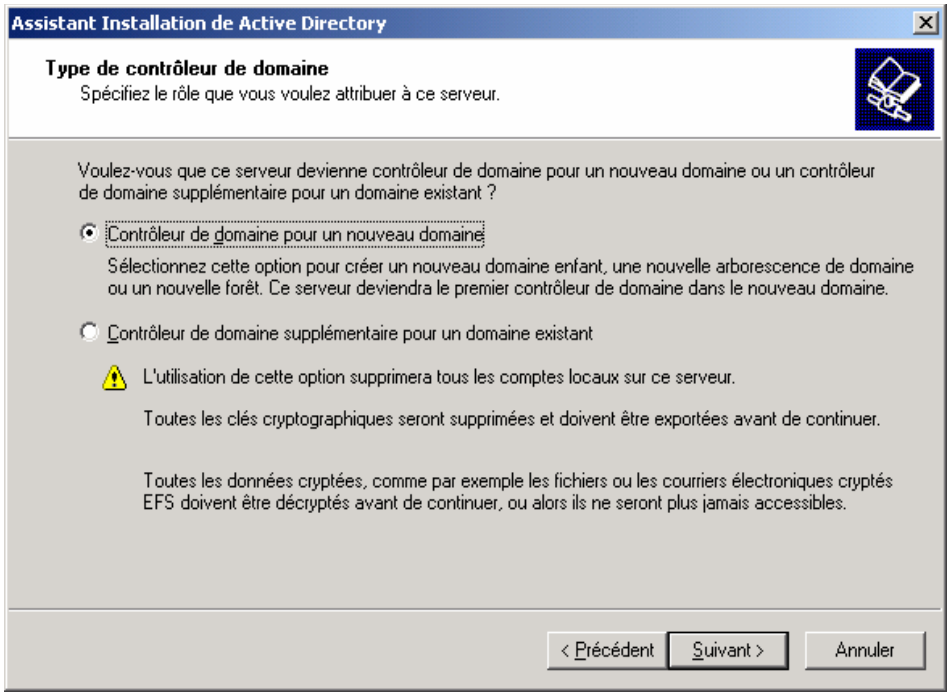


Figure 8 : Installation du contrôleur principal du domaine

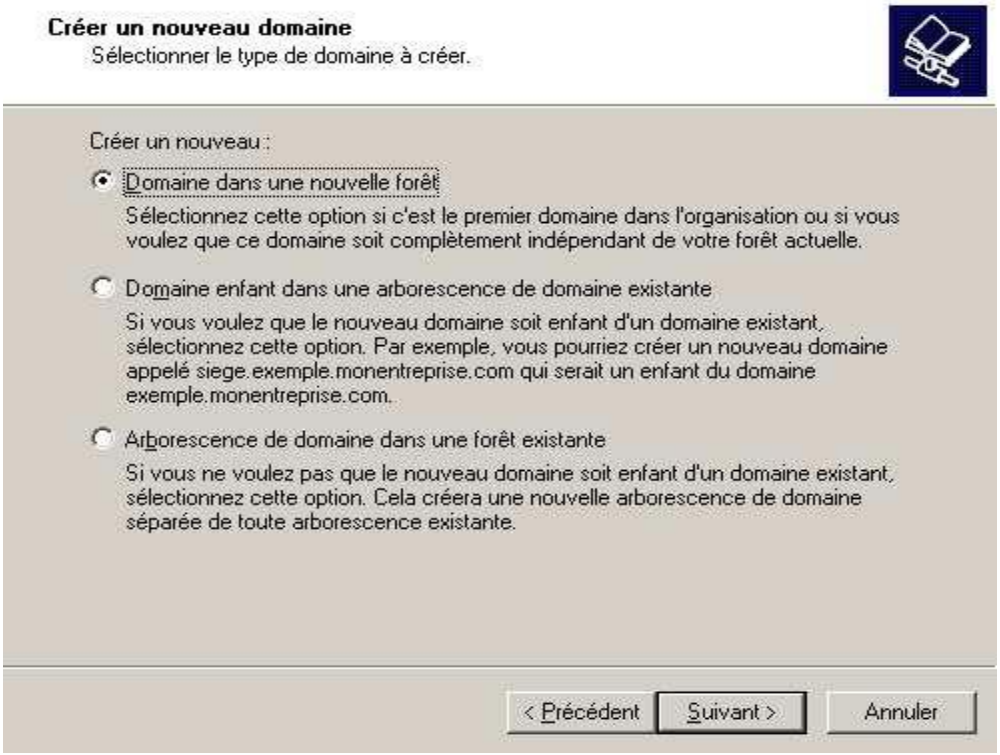


Figure 9 : Nouveau nom dans nouvelle forêt

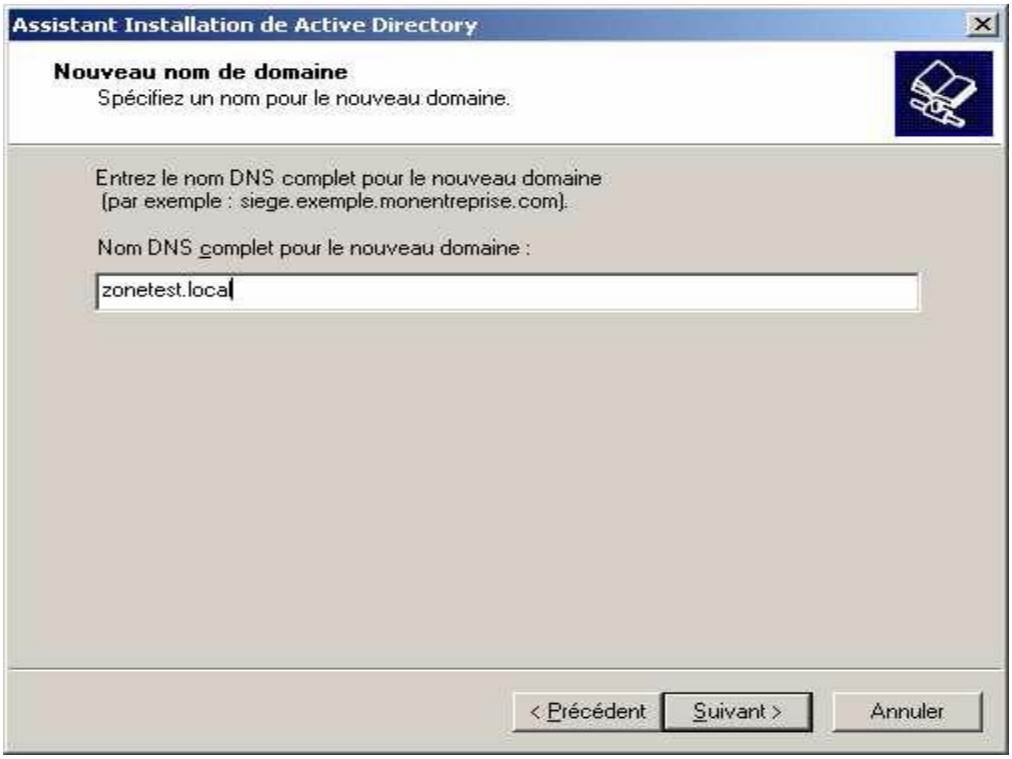


Figure 10 : Nom DNS du domaine

Ensuite on va donner le chemin de la base de données et du journal Active Directory. Microsoft préconise des disques durs différents pour des raisons de performances et de meilleure récupération (cf. figure 11).

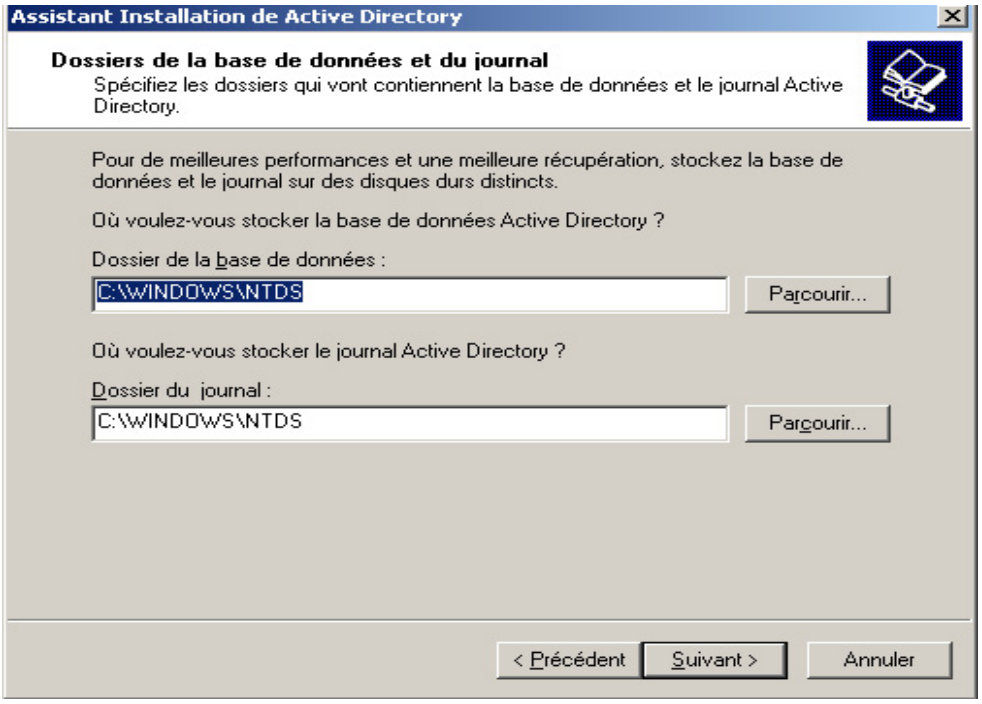


Figure 11 : Emplacement des données et du journal AD

On Indique ensuite 'emplacement du dossier Sysvol selon Figure 12

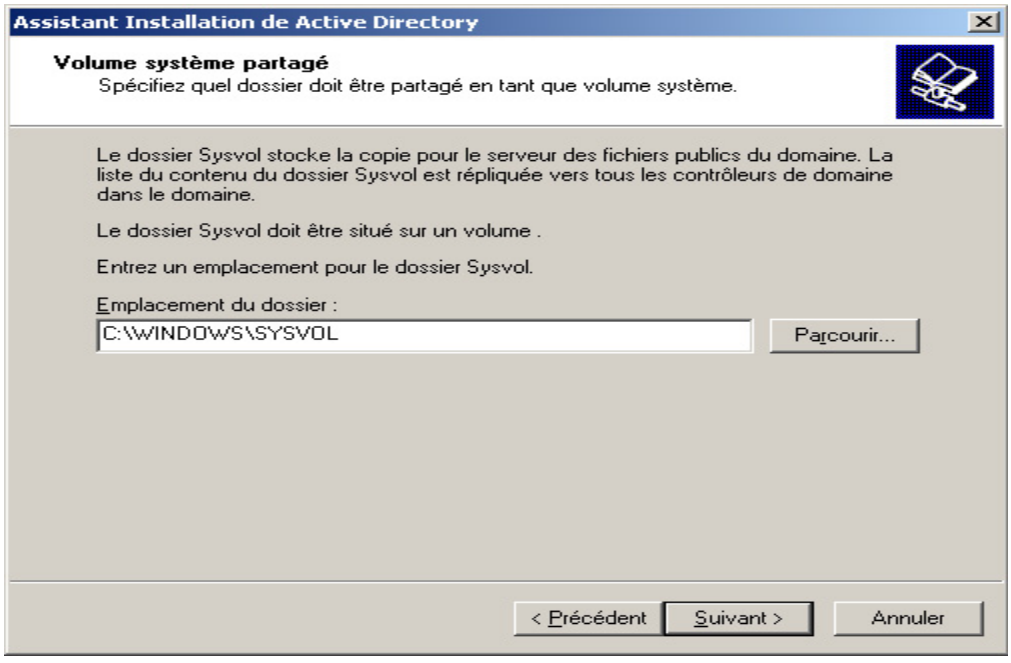


Figure 12 : Emplacement du dossier Sysvol

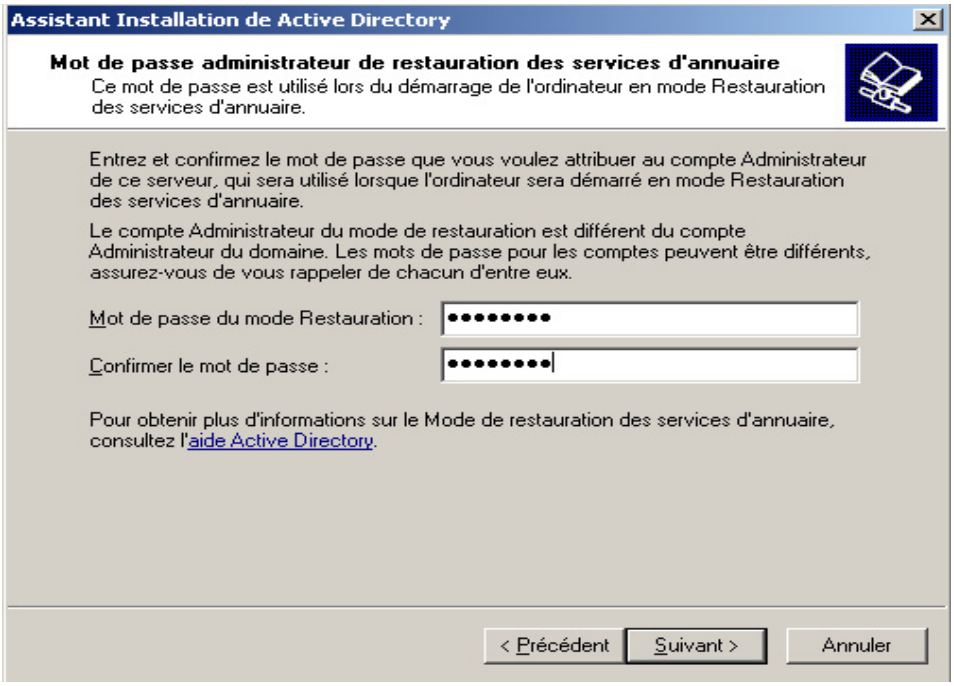


Figure 13 : Saisie du mot de passe administrateur

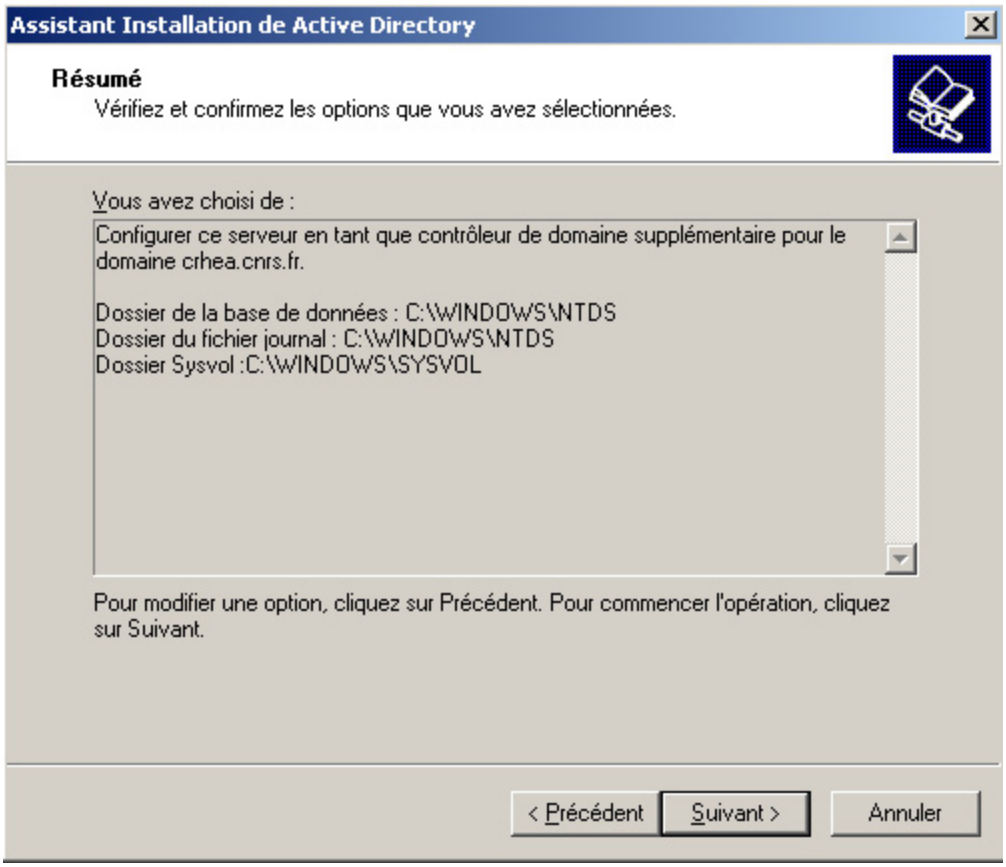


Figure 14 : Affichage du résumé

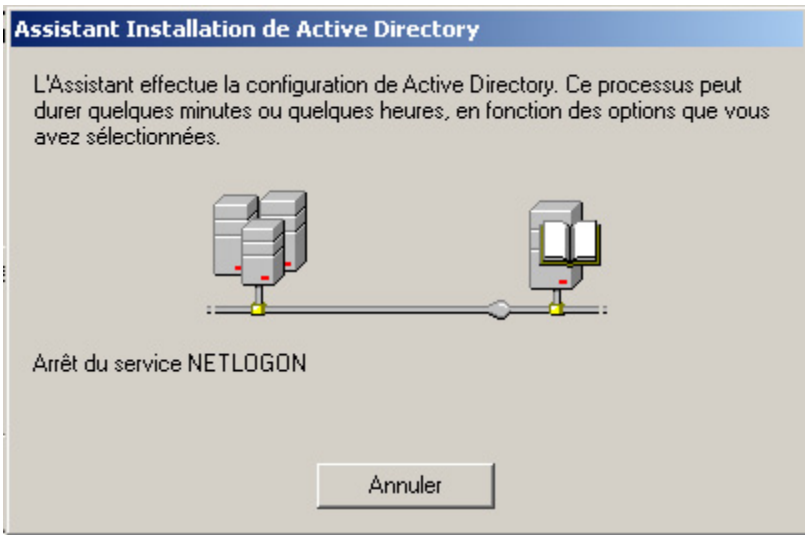


Figure 15 : Configuration d'Active Directory

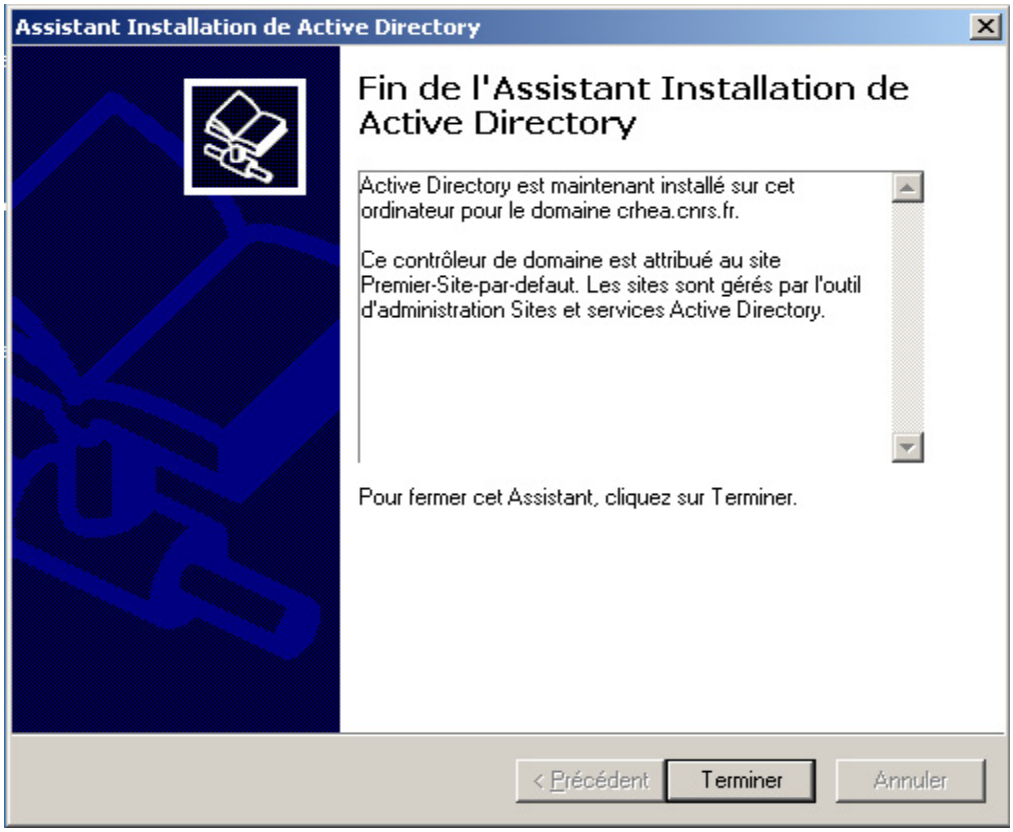
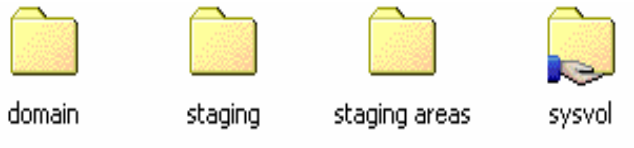


Figure 16 : Fin de l'installation d'Active Directory

- Un redémarrage du Le serveur est nécessaire à cette étape.
- On doit vérifier que **le dossier \WINDOWS\SYSVOL** contient bien ceci :



Vérifier les partages :
Par « Gestion de l'ordinateur » les partages **NETLOGON** et **SYSVOL** doivent y apparaître.

- ✓ **Configuration et optimisation DHCP**

Dans la console DHCP, on ajoute le serveur à l'aide d'un clic-droit, puis on active et on démarre le service propriétés du service DHCP. Puis on autorise le serveur DHCP à agir sur le domaine

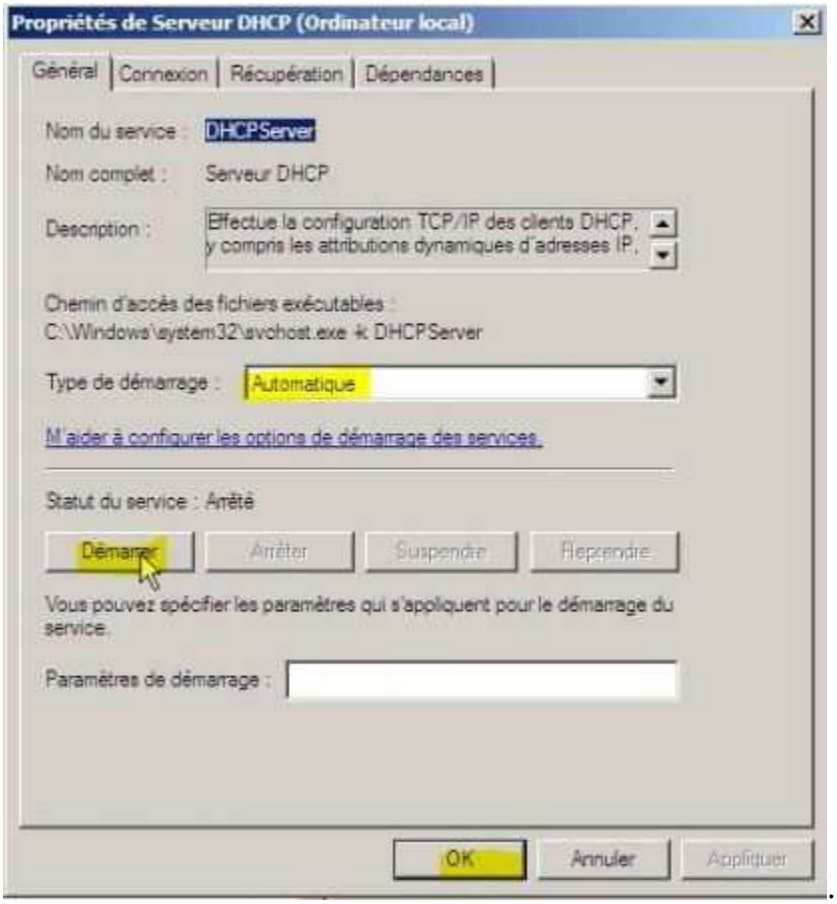


Figure 17 : Activation DHCP

Nous allons maintenant créer une étendue qui distribuera les adresses IP aux postes clients. Pour cela, au niveau du serveur, clic-droit => nouvelle étendue.

On crée l'étendu selon le plan d'adressage qu'on a définit au début, ensuite on peut spécifier le routeur ou la passerelle par défaut qui doit être distribué par cette étendu en lui attribuant son adresse IP dans « option de l'étendu »

2. **Poste Client**
   De préférence il faut donner une notation significative pour les postes clients et pour les sessions utilisateurs, on peut utiliser pour les postes la racine PC suivi du Nom et pour les sessions on peut choisir le Nom et le prénom séparé par un tiré.

   - Une Intégration des postes clients dans le domaine avec un compte Administrateur local.
   - Les comptes utilisateurs sont configurés au niveau active directory selon la figure 17.

- **Création des comptes utilisateurs**

Pour créer un nouveau compte utilisateur utilisez la console **Utilisateurs et ordinateurs Active Directory**.

1 Cliquez avec le bouton droit sur **Nouveau**, puis sur **Utilisateur**, ou utilisez le bouton **Nouvel utilisateur** dans la barre d'outils.

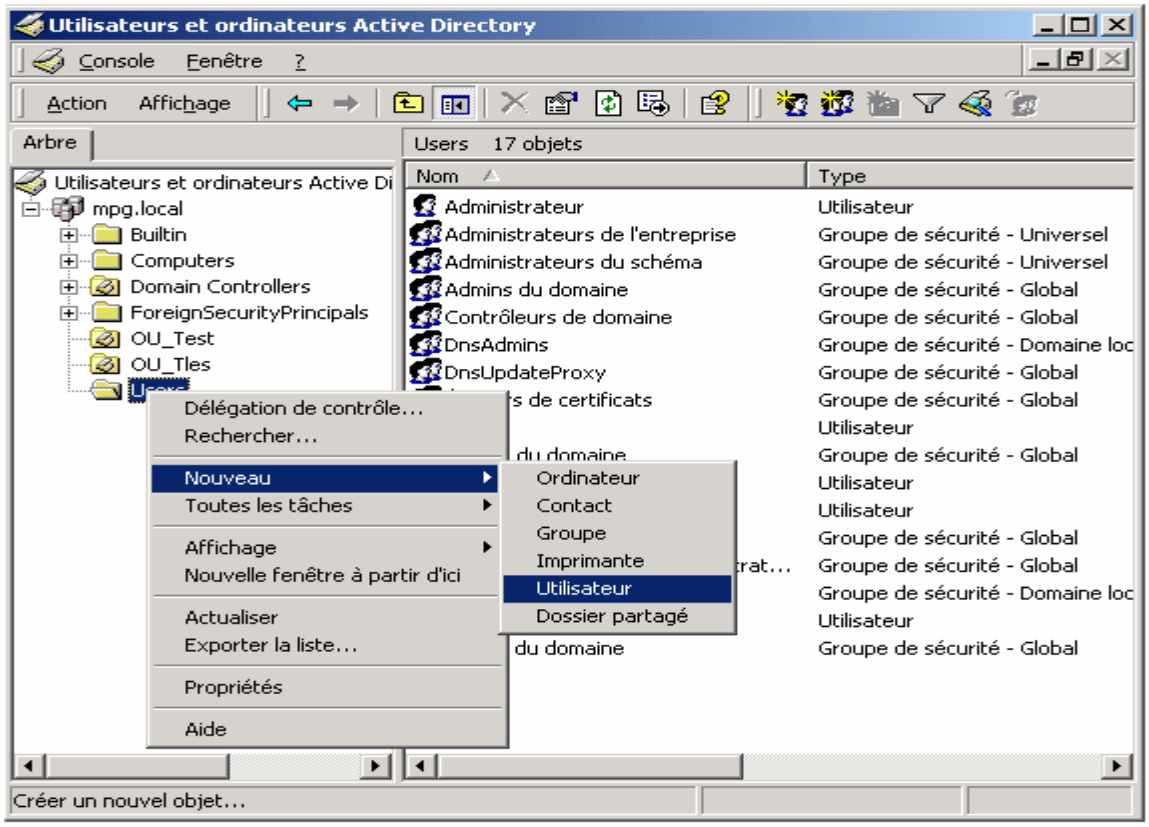


Figure 18 : Création des comptes utilisateur

2. Tapez les informations utilisateur :
Prénom :
Nom :
Nom d'utilisateur : Comme on l'a définit Ex : **riadh_abdelli**

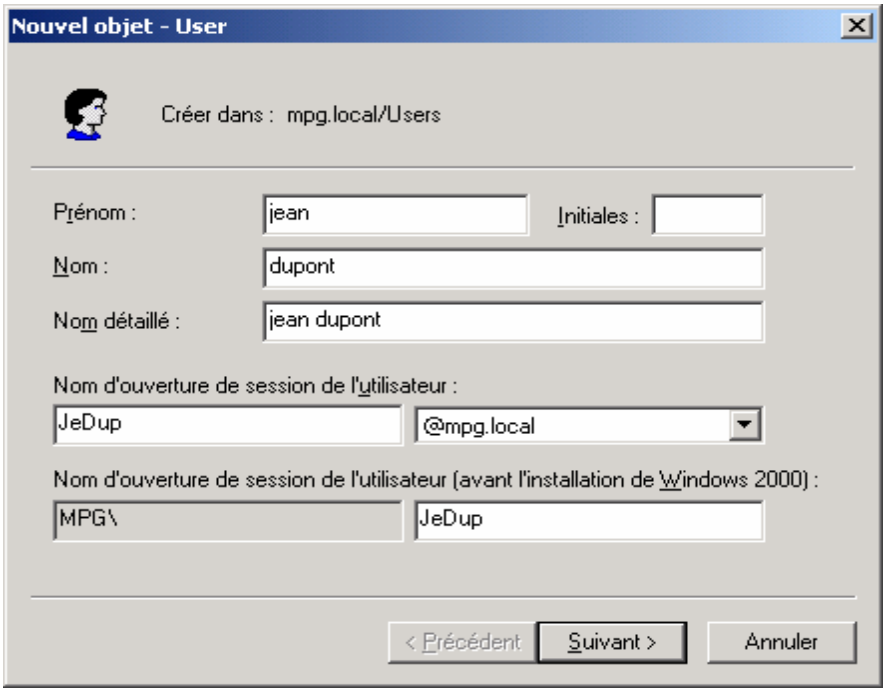


Figure 19 : Création des comptes utilisateur

3. Cliquez sur **Suivant**
4. L'assistant vous demande ensuite de saisir le mot de passe et ses propriétés.

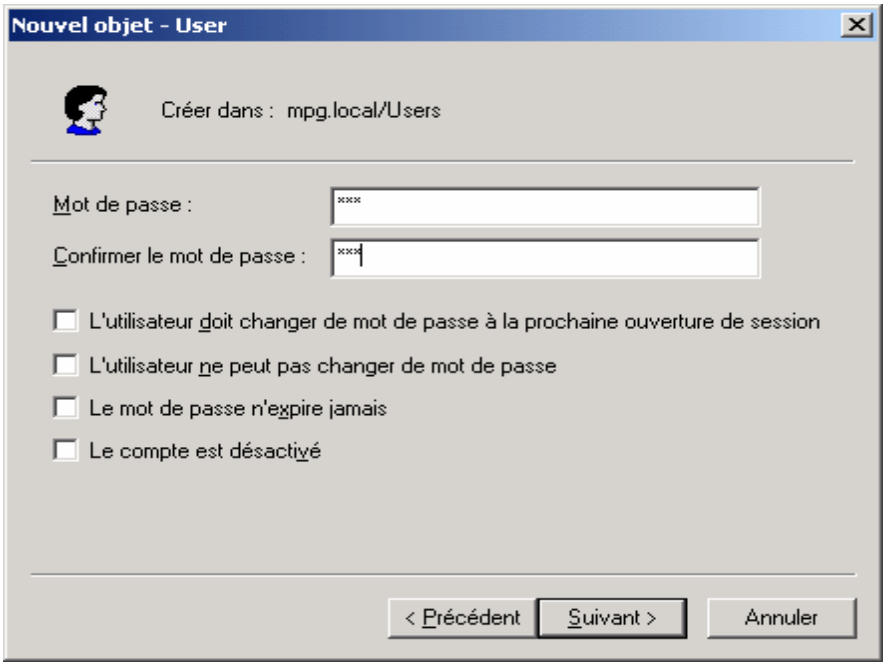


Figure 20 : Attribution mot de passe

- **L'utilisateur doit changer de mot de passe à la prochaine session.** Cela lui donne la responsabilité du mot de passe, une fois son compte créé.
- **L'utilisateur ne peut pas changer de mot de passe.**
- **Le mot de passe n'expire jamais.** Le délai d'expiration du mot de passe peut être paramétré, pour forcer les utilisateurs à en changer régulièrement.
- **Le compte est désactivé.** En cas d'absence durable d'un utilisateur ou changement d'année scolaire. Évite de recréer des comptes (les permissions devraient aussi être recréées !). Ou compte servant de modèle à la création d'autres comptes

Entrez un mot de passe dans les zones **Mot de passe** et **Confirmer le mot de passe** et sélectionnez les options de compte appropriées.

5. En acceptant la boîte de dialogue de confirmation, le compte est crée.

- **Un utilisateur est obligatoirement membre d'un groupe d'utilisateurs**.
  Par défaut, il est membre du groupe Utilisateurs du Domaine. Pour le vérifier, clic droit sur son nom / Propriétés / Membre De
  Un utilisateur peut être membre de plusieurs groupes.

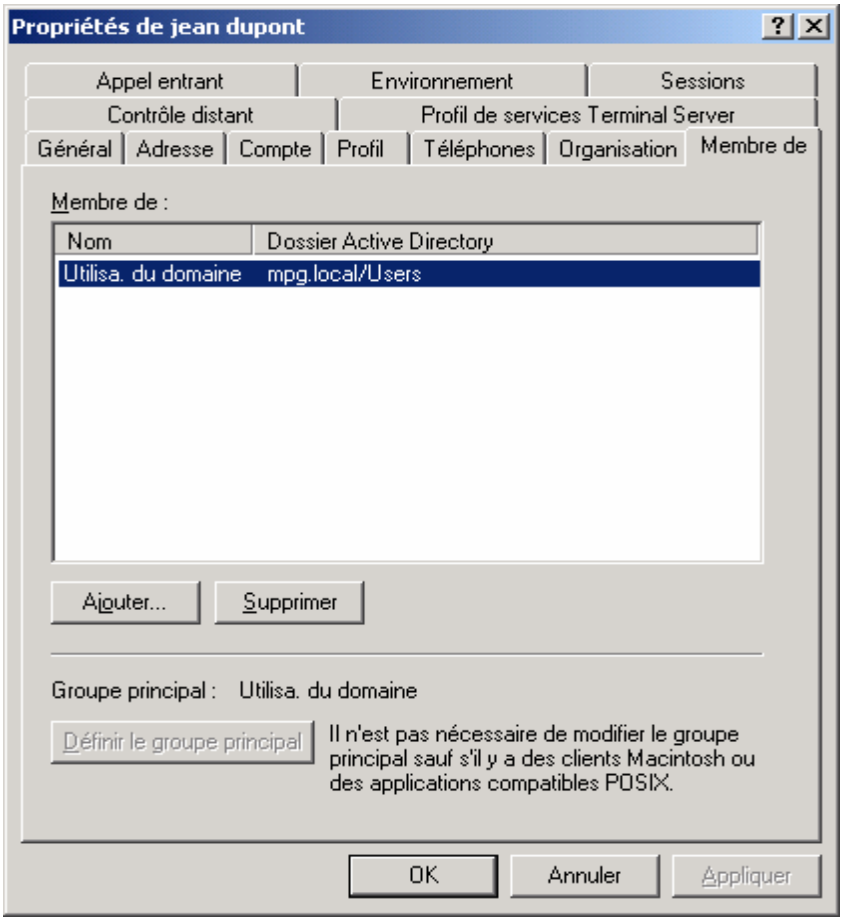


Figure 21 : Groupe utilisateur du domaine

- **Gestion des groupes dans un domaine**
  Les groupes de Windows 2003 sont utilisés pour gérer les comptes d'utilisateurs dans le but d'accéder à des ressources. Tout ceci dans un souci de simplifier l'administration. Il est en effet plus aisé d'utiliser un groupe en fonction du besoin, plutôt que de sélectionner plusieurs utilisateurs éparpillés dans une liste de comptes

  - Les groupes simplifient l'affectation d'autorisations à des ressources :
  - Les utilisateurs peuvent être membres de plusieurs groupes

✓ **Type de groupe**
Deux types de groupes sont disponibles :
- les **groupes de sécurité** utilisés pour gérer la sécurité des ressources du ou des domaines.
- les **groupes de distribution** utilisés par exemple pour envoyer des messages électroniques à l'ensemble des utilisateurs de ces groupes. Ces groupes ne peuvent pas être utilisés pour la sécurité. Des applications comme Exchange 2003 s'appuient sur la base d'annuaire Windows 2003 et peuvent ainsi utiliser les groupes de distribution.

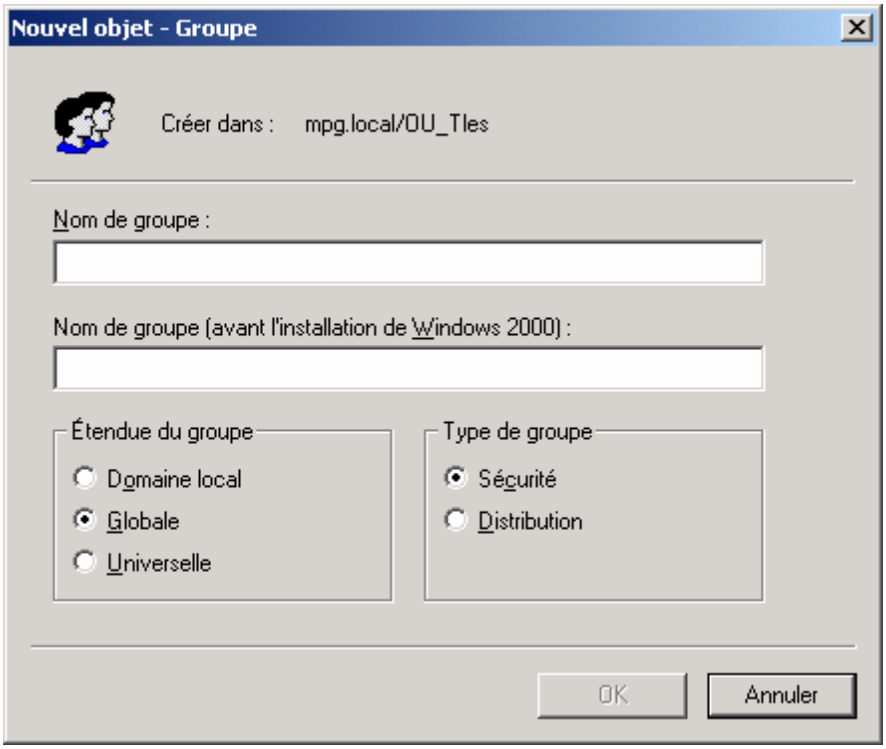


Figure 22 : Type de Groupe

Par défaut, les différents groupes opérateurs ne disposent pas de membres. On procède à l'ajout des comptes d'utilisateurs dans ceux-ci pour attribuer des droits spécifiques. II est préférable de limiter les droits des utilisateurs à leurs fonctions pour une question de maîtrise de la sécurité.
Le conteneur ***Users*** liste les groupes prédéfinis du domaine avec une étendue globale ainsi que quelques groupes prédéfinis du domaine avec une étendue de domaine local, selon la figure. 23

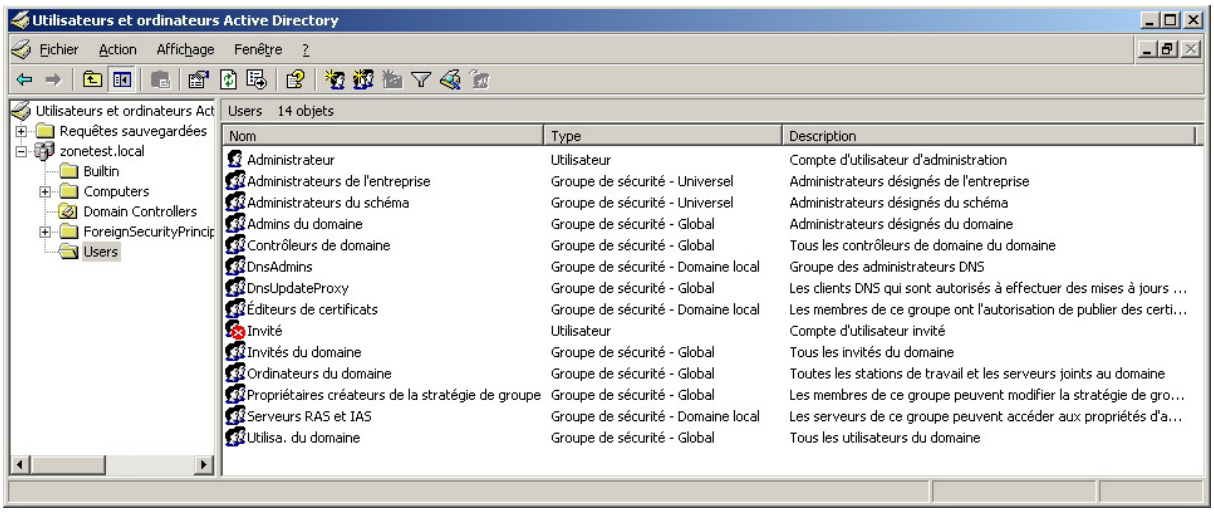


Figure 23 : Liste de Groupe

3. Fonctionnement

Après l'installation d'active directory nous aurons le schéma du réseau Palma selon la figure 24.

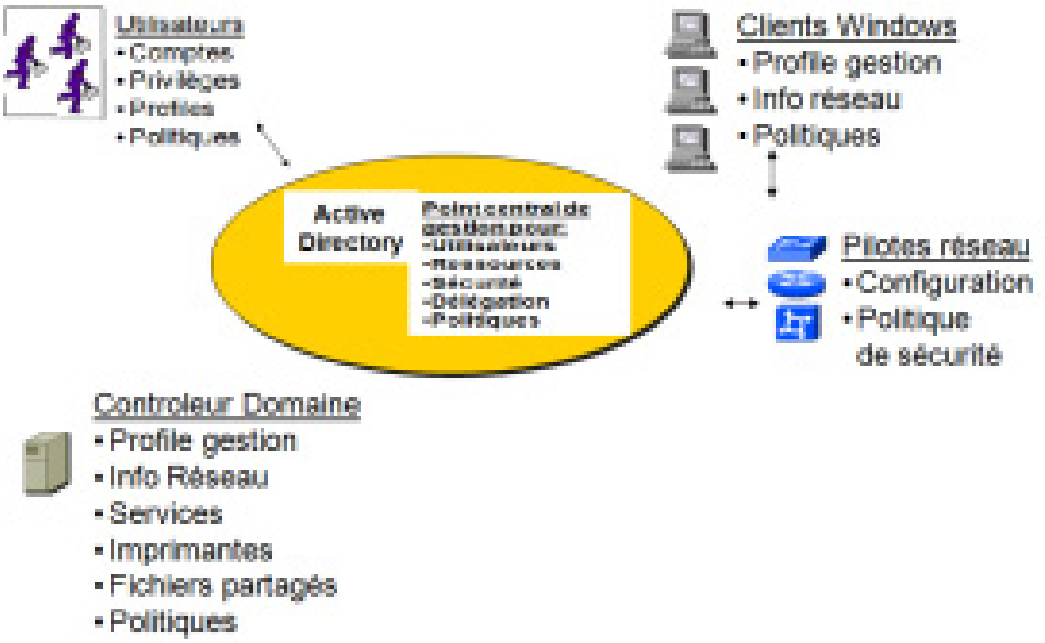


Fig. 24 : Schéma réseau avec Active directory

La composition du réseau de palma après l'installation d'active directory est comme suit :

- **Domaine** :

  Pour définir la frontière de **sécurité**

- **Un contrôleur de domaines :**

  Le serveur qui gère les composantes d'Active Directory

- **Des "clients" : stations, imprimantes, etc.**
- **Des utilisateurs**

  Chaque utilisateur a un certain nombre d'attributs et son propre UID (**U**ser **I**dentity : Un numéro de code qui lui permet d'être identifié sur le domaine
- **Des groupes**

  Qui contiennent les utilisateurs, des ordinateurs et d'autres groupes. Les groupes simplifient la gestion d'un grand nombre d'objets.

Toute personne faisant partie du domaine se connecte avec un compte utilisateur crée au niveau active directory. Le compte utilisateur contient les informations sur l'utilisateur, ses appartenances aux groupes et les informations concernant la politique de sécurité.

Les services ajoutés grâce à Active directory sont :

- ➢ Centralisation de la gestion des comptes Windows
- Absence de comptes locaux sur les postes clients à gérer
- Une base unique de comptes, délais validité.

- ➢ Centralisation de la gestion des PC Windows
- Prise en main à distance : accès aux disques, base de registre, services

- ➢ Mise en place de règles de sécurité
- Les modalités d'accès aux ordinateurs et l'utilisation des logiciels

- ➢ Authentification unique
- ➢ Partages des ressources simplifiés

Conclusion

A la fin de ce travail, je peux dire que j'ai bien pu avoir une visibilité concrète sur un domaine bien spécifique qui est la sécurité informatique.

En plus, ce travail m'a été profitable en terme d'acquérir une bonne expérience professionnelle, à travers laquelle j'ai eu l'occasion d'appliquer mes connaissances scientifiques et de confronter la notion théorique à la pratique.

Et pour conclure, je peux dire que l'objectif global n'est pas atteint par un seul projet, mais par une succession de projets afin d'établir un audit de sécurité selon une méthode et norme standard.

Bibliographie

www.ansi.tn

www.clusif.fr

www.clusif.fr

www.microsoft.com/technet/prodtechnol/w2kadsi.asp.

www.cygwin.com

www.commencamarche.com

www.isc.cnrs.fr

www.parisscyber.com

www.Reso-Net.com/es.htm

www.microsoft.com/france/window