

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira, Béjaïa
Faculté des Sciences Exactes
Département d'informatique



Mémoire de fin de cycle

*En vue de l'obtention du diplôme de master Professionnel en informatique
Option Administration et sécurité des réseaux(ASR)*

Thème

Installation et configuration des services de Windows server 2012 Cas d'étude : Candia(Tchin-Lait)

Réalisé par :

Mlle SAADELI Nouria & Mlle OUARET Kahina

Devant le Jury composé de :

Président : M^{me} TAHAKOURT Z.
Examineur : M^{me} AIT ABDELOUAHB K.
Examineur : M^{me} TASSOULT
Encadreur : M^r BOUKERRAM A.
Encadreur : M^r ELSAKAAN N.

Promotion : 2016/2017.

Remerciements

En tout premier lieu, nous remercions le bon dieu tout puissant de nous avoir donné courage, volonte et patience pour accomplir ce modeste travail.

Nous voudrions remercier particulierement notre encadreur Mr BOUKERRAM A., Mr ELSAKAAN N. pour le temps qu'il nous a accordé et pour nous avoir suivis dans nos démarches, pour nous avoir transmis les renseignements nécessaires à la réalisation de ce projet.

Nous remercions les membres de jury d'avoir accepté, consacrer une partie de leur temps pour juger ce travail.

Enfin nous remercions tous ceux qui nous ont aidés de près ou de loin pour l'élaboration de ce modeste travail.

Dédicaces

J'ai l'honneur à dédier ce modeste travail Ames très chère parents je ne peux jamais imaginer une vie sans eux, merci pour votre patience, votre soutien infini ; pour vos précieux conseils au long de ma vie, j'espère que je suis la bonne fille que vous souhaitez de l'avoir et je suis une source de fierté pour vous.

A Mes très chers frères pour qui je souhaite une vie pleine de joie, réussite et beaucoup de bonheur.

A mes très chères copines DIDA, DIHIA, LYDIA, YASSMINA avec qui j'ai passé des agréables et inoubliables moments.

Sans oublier ma binôme Melle OUARET Kahina et toute sa famille.

A toute la promotion informatique 2016/1017 à qui je souhaite une bonne continuation dans leur vie soit privé ou professionnelle.

Enfin, mes dédicaces vont à toute la famille SAADELI et NEMIR

SAADELI Nouria

Dédicaces

Je dédie ce modeste travail à :

La mémoire de ma grand mère que son âme repose en paix.

Mes très chers parents qui n'ont jamais cessé de m'aider et m'encourager durant tout mon parcours et qui m'ont permis d'être aujourd'hui ce que je suis.

Ma chère grand mère maternelle que dieu la garde.

Ma chère soeur : sonia.

Ma chère amie et binôme : noria et toute sa famille.

Mes amis :slimanou dehia, bellilli lylia, boukibba fayrouz.

Mon chéri : aziz ouaissa.

kahina ouaret

Glossaire

DHCP : Dynamic Host Configuration Protocol.

DNS : Domain Name System.

GPO : Group Policies Object.

IP : Internet Protocol.

ISCSI :Internet Small Computer System Interface.

LAN : Local Area Network.

MAC : Media Acces Control.

MAN : Metropolitan Area Network.

NAT : Network Address Translation.

NIC : Network Interface Card.

OSI : Open Systems Interconnection.

PAN : Personal Area Network.

PKI : Public Key Infrastructure.

RIP : Routing Information.

Table des matières

Glossaire

Table des matières	ii
Liste des figures	iv
Liste des tableaux	vi
Introduction générale	1
1 Les réseaux informatique	3
1.1 Introduction	3
1.2 Généralités sur les réseaux informatiques	3
1.2.1 Définition d'un réseau d'entreprise	3
1.2.2 L'objectif de réseaux informatique	3
1.2.3 Les classes de réseaux	4
1.2.4 Les équipements réseaux	5
1.2.5 Les topologies de réseau	6
1.3 Le modèle OSI	7
1.4 Le modèle TCP/IP	8
1.4.1 La comparaison entre le modèle OSI et le modèle TCP/IP	9
1.5 Deploiment d'Active Directory sous windows server 2012	10
1.5.1 Présentation de Windows server 2012	10
1.5.2 La famille Windows server 2012	10
1.5.3 La Nouveautés de Windows server 2012	12
1.5.4 Comparaisons des versions Windows server :	13
1.5.5 Active directory	14
1.6 Conclusion	18

2	Etude de l'existant	19
2.1	Introduction	19
2.2	Présentation de l'unité Tchîn-Lait / Candia	19
2.2.1	La marque Candia en Algérie	19
2.2.2	Historique et situation géographique	19
2.2.3	Les missions de l'entreprise	20
2.2.4	Les objectifs de l'entreprise	21
2.2.5	La structure de l'entreprise	22
2.3	Présentation du réseau de l'entreprise	23
2.3.1	Les différents équipements qui existent dans le réseau	24
2.3.2	Les différents logiciels de l'entreprise	25
2.4	Description du projet	26
2.4.1	Description des besoins	26
2.5	La solution proposée	27
2.5.1	Mise en œuvre des services réseaux avancées	27
2.5.2	Mise en œuvre de contrôleur de domaine Active Directory Domain Services (AD DS)	27
2.5.3	Mise en œuvre de l'autorité de certification Active Directory Certificate Services (AD CS)	28
2.5.4	Mise en œuvre des services de fichiers avancés	28
2.5.5	Mise en œuvre de la reprise en cas de panne	28
2.6	Contraintes	28
2.7	Conclusion	29
3	Réalisation	30
3.1	Introduction	30
3.2	Installation de la machine virtuelle(VMware Workstation 10)	30
3.3	Installation de Windows server 2012	31
3.4	Création du contrôleur de domaine et DNS	33
3.5	Installation et configuration du service DHCP	36
3.6	Organisation des clients AD en unités organisationnelles	37
3.7	Mise en œuvre des Group Policy Organisation (GPO)	39
3.8	Création des profils itinérants	42
3.9	Mise en œuvre de l'autorité de certification Active Directory Certificate Services (AD CS)	44
3.9.1	Exportation du certificat de l'autorité racine	45
3.9.2	Création d'un nouveau modèle de certification	46

3.9.3	Demande d'un certificat	47
3.9.4	Déploiement de serveur web (IIS)	48
3.9.5	Distribution du certificats aux clients de l'Active Directory	49
3.10	Configuration de BranchCache	50
3.11	Mise en œuvre d'une solution de sauvegarde " Backup "	53
3.12	Conclusion	55
	Conclusion générale	56
	Bibliographie	57

Table des figures

1.1	La topologie en bus.	6
1.2	La topologie en étoile	6
1.3	La topologie en anneau	7
2.1	Réseau de distribution	20
2.2	Organigramme général de Tchiv-Lait.	22
2.3	L'Architecture du réseau de Tchiv-Lait.	23
3.1	Installation de la machine virtuelle.	31
3.2	Installation de Windows server 2012.	31
3.3	Gestionnaire de serveur.	32
3.4	Configuration du serveur local.	32
3.5	Ajout du service AD DS.	33
3.6	Promouvoir du serveur en contrôleur de domaine.	34
3.7	Création du domaine Tchiv-Lait.	34
3.8	Sélection du niveau fonctionnel de la forêt et du domaine.	35
3.9	Ouverture de la session Administrateur.	35
3.10	Installation du serveur DHCP.	36
3.11	Création des étendues DHCP.	36
3.12	Ajout d'exclusion DHCP.	37
3.13	Création d'une unité d'organisation.	38
3.14	Ajout d'utilisateur.	38
3.15	Création des sessions utilisateur.	39
3.16	Modification de la stratégie de groupe par défaut.	40
3.17	Configuration d'une GPO ordinateur.	40
3.18	Configuration d'une GPO utilisateur.	41
3.19	Création d'une GPO pour une UO.	42
3.20	Création d'une nouvel GPO.	42
3.21	Configuration du partage.	43

3.22	Autorisation pour profils utilisateur.	43
3.23	Spécification du profil de l'utilisateur.	44
3.24	Configuration d'une PKI.	45
3.25	L'exportation du certificat.	45
3.26	Propriétés du nouveau modèle de certificat.	46
3.27	Mise à jour de la stratégie d'ordinateur.	46
3.28	Demande d'un nouveau certificat.	47
3.29	Le choix d'un type de certificat.	47
3.30	Installation de Serveur Web (IIS).	48
3.31	Sécuriser le serveur web avec un certificat.	49
3.32	Ajout d'une liaison de site.	49
3.33	Distribution du certificat de l'autorité aux utilisateurs d'Active Directory.	50
3.34	Ajout de fonctionnalité de BranchCache.	51
3.35	Activer la publication de hachage pour BranchCache.	51
3.36	Activer BranchCache sur un partage.	52
3.37	Configuration du client BranchCache.	53
3.38	Installation du service de sauvegarde.	53
3.39	Spécifier l'heure de la sauvegarde.	54
3.40	Résultat de la sauvegarde.	55

Liste des tableaux

1.1	La comparaison entre le modèle OSI et TCP/IP[1].	9
1.2	La Comparaison des versions Windows server [5].	13
2.1	Les Switchs et les routeurs du réseau.	24
2.2	Les Autres équipements du réseau.	25

Introduction générale

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

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

L'administrateur système gère les postes de travail et les serveurs de l'entreprise pour mettre en place les moyens et les procédures en garantissant les performances et la disponibilité des systèmes. Comme il peut recourir à un contrôleur de domaine centralisé pour simplifier les accès aux ressources et l'optimisation du trafic réseau.

Un domaine dans les services d'annuaire, regroupe un ensemble d'ordinateurs qui partagent une base de données d'annuaires centralisée. Cette base de données reprend les comptes d'utilisateurs et les informations de sécurité spécifique au domaine.

Notre stage au sein de l'entreprise Tchir-Lait Bejaia, consiste à l'installation de Windows Server 2012 et configurer l'Active Directory et ces services. Puis ajouter les ordinateurs du réseau au domaine et créer et configurer les comptes utilisateurs, a l'objectif de mettre en place un serveur contrôleur de domaine qui sera en mesure de répondre aux critères habituellement utilisés par un administrateur réseau de l'entreprise, tels que :

- L'authentification des utilisateurs.
- La gestion de droits d'accès.
- Les partages des fichiers ou répertoires.

Notre mémoire est organisé comme suit :

- Chapitre 1 " les réseaux informatique " : il décrit d'une manière générale les réseaux informatiques ainsi le déploiement d'active directory sous Windows server 2012 et ces différents services.
- Chapitre 2 " Etude de l'existant " : il montre une brève étude sur le réseau de l'entreprises Tchir-Lait, ainsi que les différents équipements et les ressources informatique qui dispose l'entreprise.
- Chapitre 3 " Réalisation " : il présente la configuration et déploiement de l'annuaire active directory et la gestion des utilisateurs, il explique encore les différents rôles à gérer par l'administrateur réseau.

Enfin, nous concluons ce travail avec des perspectives futures.

Chapitre 1

Les réseaux informatique

1.1 Introduction

Le besoin de communication et de partage a poussé les entreprises à s'orienter vers les réseaux informatiques et travailler d'avantage pour les améliorer. Dans ce chapitre, on définit le réseau informatique d'entreprise et ses différents types et outils, ensuite on présentera le déploiement d'un active directory sous Windows server 2012 et ses différents services.

1.2 Généralités sur les réseaux informatiques

1.2.1 Définition d'un réseau d'entreprise

Est un ensemble d'ordinateurs et de terminaux interconnectés pour échanger des informations numériques [1].

1.2.2 L'objectif de réseaux informatique

Le partage de ressources :

Rendre accessible à une communauté d'utilisateurs des programmes, des données et des équipements informatiques (i.e. un ensemble de ressources) indépendamment de leur localisation.

La Fiabilité :

Permettre le fonctionnement même en cas de problèmes matériels (sauvegardes, duplication ...). Penser aux applications militaires, bancaires, au contrôle des centrales nucléaires ou aérien...

La réduction des coûts :

Les petits ordinateurs (PC) ont un meilleur rapport prix/performances que les gros.

1.2.3 Les classes de réseaux

PAN (Personal Area Network) :

C'est un réseau constitué autour d'une personne (de l'ordre de quelques mètres) [1].

LAN (Local Area Network) :

Il est constitué de quelques équipements informatiques (ordinateur, imprimante et autres périphériques) limités à une entreprise, à un service d'entreprise, à un immeuble... Exemples : le laboratoire d'informatique d'un lycée, réseau dans un bâtiment[2].

MAN (Metropolitan Area Network) :

C'est une collection de réseaux locaux. Il relie des ordinateurs situés dans le même espace géographique à l'échelle d'une ville. Exemple : réseau de points de ventes dans une même ville[2].

WAN (Wide Area Network) :

C'est un réseau qui relie des réseaux locaux et métropolitains entre eux. Un réseau étendu peut être réparti sur tout un pays ou plusieurs pays du monde. Exemple : Internet [2].

BAN (Body Area Network) :

C'est une technologie de réseau sans fil basée sur radio-fréquences qui consiste à interconnecter sur, autour ou dans le corps humain de minuscules dispositifs pouvant effectuer des capteurs ou agir de façon active[2].

1.2.4 Les équipements réseaux

NIC (Network Interface Card) :

- Interface se trouvant sur un équipement terminal.
- Il est porteur d'une adresse MAC.
- On lui attribue une adresse IP relative au réseau sur lequel il se connecte.

Modem :

- Modulateur/ Démodulateur.
- Il réalise la connexion LAN.
- Il interconnecte le LAN à l'internet.
- Il implémente plusieurs serveurs de différents protocoles.

Concentrateur (hub) :

- Dispositif réseau simple.
- Interconnecte un ensemble d'ordinateurs.
- Il a deux interfaces : une de réception et l'autre de diffusion.
- Les données sont retransmises à toutes les machines.

Commutateur (switch) :

Ressemble à un hub et envoi des données est contrôlé.

Routeur :

- Assure les mêmes fonctionnalités qu'un switch.
- Permet d'interconnecter plusieurs réseaux.
- Il possède une interface connectée au réseau internet

Répétiteur :

C'est un hub avec plus de ports. Il amplifie le signal.

Passerelle (Bridge) :

C'est un moyen système qui interconnecte des réseaux hétérogènes [3].

1.2.5 Les topologies de réseau

A. La topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot " bus " désigne la ligne physique qui relie les machines du réseau [4].

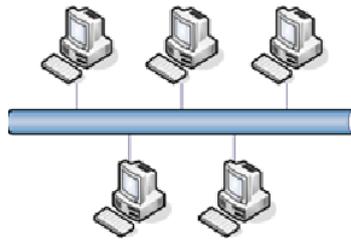


FIGURE 1.1 – La topologie en bus.

B. La topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions [4].

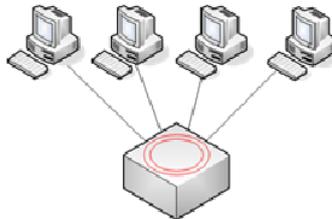


FIGURE 1.2 – La topologie en étoile .

C. La topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à son tour. Ce type de réseau résout de façon simple

et efficace les problèmes de collision que l'on rencontre dans les réseaux de type bus. Il peut également être conçu pour éviter les nœuds en panne ou hors fonctionnement. Peut couvrir des distances plus grandes qu'un réseau en bus [4].

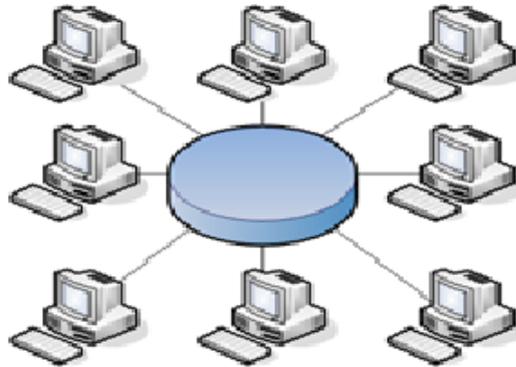


FIGURE 1.3 – La topologie en anneau .

C. La topologie en arbre

Dans un réseau possédant une topologie en arbre ,autrement dit la topologie hiérarchique, le réseau est divisées en niveaux.Le somment,le haut niveau,est connectée à plusieurs noeuds de niveau inferieur,dans la hiérarchie.Ces noeuds peuvent être eux-mêmes connectés à plusieurs noeuds de niveau inferieur.Le tout dessine alors un arbre,ou une arborescence.

1.3 Le modèle OSI

(de l'anglais Open Systems Interconnection) : est un standard de communication en réseau de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Il est décomposé en 7 parties appelées couches OSI :[3]

La couche(1) physique :

Rassemble les moyens électriques, mécaniques, optiques ou hertziens par l'equels les informations sont transmises. Les unités sont donc des bits(0 ou 1).

La couche (2) liaison de donnée :

Règles permettant d'effectuer le réassemblage et l'acheminement des données vers le matériel physique de la couche 1.

La couche (3) réseau :

Schéma général d'interconnexion (adressage) afin d'assurer le repérage physique du destinataire.

La couche (4) transport :

Regroupe les règles de fonctionnement de bout en Bout, assurant ainsi la transparence du réseau vis-à-vis des couches supérieures. Elle traite notamment l'adressage, l'établissement des connexions et la fiabilité de transport.

La couche (5) session :

Réunit les procédures de dialogue entre les applications, Etablissements et interruptions de la communication, cohérence et synchronisation des opérations.

La couche (6) présentation :

Traite les formes de représentation des données permettant la traduction entre machines différentes.

1.4 Le modèle TCP/IP

1. Définition

Le protocole TCP/IP ou "Transmission Control Protocol/Internet Protocol", développé par le ministère de la défense américaine (DoD) en 1981 est un protocole de transport fiable, en mode connecté, c'est-à-dire qu'il permet l'établissement d'une session de communication entre deux parties qui veulent échanger des données.

TCP/IP reprend l'approche modulaire (utilisation de couche ou module) mais en contient uniquement quatre.

1.4.1 La comparaison entre le modèle OSI et le modèle TCP/IP

Même si le modèle TCP/IP s'inspire fortement du modèle OSI (littéralement "Interconnexion de systèmes ouverts") en 7 couches, celui-ci n'en contient que 4. Les voici résumées et comparées avec le modèle OSI dans le tableau ci-dessous :[1]

Modèle TCP/IP	Modèle OSI
Couche Application : elle englobe les applications standard du réseau	Application : c'est à ce niveau que sont les logiciels: navigateur, logiciel d'email, FTP, chat...
	Présentation : elle est en charge de la représentation des données
	Session : elle établit et maintient des sessions de dialogue
Couche Transport (TCP) : elle assure l'acheminement des données	Transport : en charge de la liaison d'un bout à l'autre. S'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.
Couche Internet (IP) : elle est chargée de fournir le paquet de données (datagramme)	Réseau : en charge du transport, de l'adressage et du routage des paquets.
Couche Accès Réseau : elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé	Liaison Données : en charge d'encoder (ou moduler) les données pour qu'elles soient transportables par la couche physique, et fournit également la détection d'erreur de transmission et la synchronisation.
	Physique : c'est le support de transmissions lui-même: un fil de cuivre, une fibre optique, les ondes hertziennes...

TABLE 1.1 – La comparaison entre le modèle OSI et TCP/IP[1].

1.5 Déploiement d'Active Directory sous windows server 2012

1.5.1 Présentation de Windows server 2012

Windows server 2012 est un système d'exploitation serveur, polyvalent et puissant qui se base sur les améliorations que Microsoft a apportées a Windows server 2008 R2. Windows server 2012 et Windows server 2008 partagent un certain nombre de caractéristiques car ils font partie du même projet de développement. ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage [5].

Quelque avantage :

- Très simple, il comporte quatre éditions conçues pour répondre aux besoins de tous les clients.
- Plus économique, le prix par instance diminue a mesure que votre infrastructure grandit.
- Optimisé pour le Cloud, mobilité des applications dans des environnements hybrides.

1.5.2 La famille Windows server 2012

Windows server existe dans cinq versions principales :

a) Windows Server 2012 Foundation (Win12)

disponible que lors de l'achat d'un nouveau serveur et destinée aux TPE (très petites entreprises), cette édition est limitée à 15 utilisateurs,elle ne prend pas en charge la virtualisation et ne supporte qu'un seul processeur. Il n'y a, par contre, pas besoin de CAL Windows pour se connecter à un serveur Foundation. Le serveur doit être hébergé sur une machine physique.

- Idéal pour : Les clients qui recherchent un premier serveur très abordable.
- Fonctionnalités : Accès à toutes les fonctionnalités essentielles d'un premier serveur, pas de droit pour virtualiser.
- Mode de licence : Par serveur (limité à 15 utilisateurs).

b) Windows Server 2012 Essential

L'objectif de cette version est d'acheminer les PME (petites et moyennes entreprises) vers les solutions Cloud de Microsoft. elle ne prend pas en charge la virtualisation et supporte deux processeurs. Le serveur peut être hébergé sur une machine physique ou virtuelle.

- Idéal pour : Les petites et moyennes entreprises.
- Fonctionnalités : Une interface plus simple, pas de droit pour virtualiser, installation et administration simplifiées.
- Mode de licence : Par serveur (limité à 25 utilisateurs).

c) Windows Server 2012 Standard

Edition principale de Windows Server 2012 elle offre toutes les fonctionnalités, tout comme l'édition Datacenter. Elle se distingue de cette dernière par le nombre de machines virtuelles couvertes par la licence, à savoir deux. Windows Server 2012 Standard supporte jusqu'à deux processeurs par licence. Tout comme l'édition Datacenter, elle prend en charge les machines disposant d'un maximum de 64 processeurs (sockets) et de 4 To de mémoire RAM.

- Idéal pour : Des environnements à faible densité de virtualisation ou non virtualisés.
- Fonctionnalités : Accès à toutes les fonctionnalités de Windows Server et droit pour 2 machines virtuelles.
- Mode de licence : Par processeur physique (1 licence couvrant jusqu'à 2 processeurs) + CAL.

d) Windows Server 2012 Datacenter

Cette édition est destinée à ceux qui ont un recours intensif aux machines virtuelles. Chaque licence couvre en effet jusqu'à deux processeurs et un nombre de machines virtuelles illimité.

- Idéal pour : Des environnements à faible densité de virtualisation ou non virtualisés.
- Fonctionnalités : Accès à toutes les fonctionnalités de Windows Server et droit pour 2 machines virtuelles.
- Mode de licence : Par processeur physique (1 licence couvrant jusqu'à 2 processeurs) + CAL.

e) Storage Server

Cette version destinée aux partenaires Microsoft existe en deux éditions, la version Workgroup (50 utilisateurs maximum, 1 seul CPU, 6 disques maximum) et en version standard (pas de limites de ressources, déduplication, mode cluster).

1.5.3 La Nouveautés de Windows server 2012

La partie des modifications a été effectuée sur Hyper-V avec des améliorations qui réduisent encore l'écart avec VMWare :[5]

- Amélioration d'Hyper-V Replica
 1. Le choix sur les fréquences de réplication entre hyperviseur.
 2. La possibilité de répliquer une VM déjà répliqué sur un serveur différent.
 3. Hyper-V Recovery Manager, solution de réplication entre Azure et du cloud On-Premise.
- Amélioration VHDX
 1. Modification des tailles de volume VHDX à chaud (online).
 2. Ajout de la déduplication sur le format VHDX (permet d'accélérer les machines virtuelles en utilisant le cache du volume des autres VM en cours d'exécution).
 3. Partage de VHDX, permet à plusieurs machines virtuelles d'exécuter le même VHDX comme volume partagé.
- Amélioration VM Connection avec la possibilité de copier/coller et d'avoir accès au service de la même manière qu'avec RDP mais depuis la console Hyper-V.
- Activation automatique de la machine virtuelle si elle se trouve sur une version Datacenter de Windows Server 2012.
- Support complet des machines Virtuelles Linux (Dynamic Memory, 64 vCPU, redimensionnement de volume de stockage online).
- Generation 2 VM, qui permet d'utiliser UEFI et d'améliorer les démarrages de VM. Fonctionne uniquement en 64 bits avec Windows 8/Windows Server 2012.
- QoS sur Volume.

1.5.4 Comparaisons des versions Windows server :

fonctionnalités		Server 2003	Serveur 2008/2008 R2	Serveur 2012
Identité et accès	Service active directory	●	●	●
	Contrôle d'accès dynamique	○	○	●
	Virtualisation d'active directory	○	○	●
Virtualisation	Migration dynamique sans partage	○	○	●
	Règles hyper-v	○	○	●
	Conteneur hyper-v	○	●	●
Mise en réseau	Virtualisation de réseau hyper-v	○	○	●
	Gestion des adresses IP	○	○	●
Automatisation et gestion	Windows powershella	●	●	●
Stockage	Migration de stockage dynamique	○	○	●
	Qualité de service de stockage	○	○	○

○ : pas de prise en charge,

● : prise en charge complet

TABLE 1.2 – La Comparaison des versions Windows server [5].

1.5.5 Active directory

Est un annuaire au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées [6].

1. Le rôle et les avantages de l'active Directory

- **Le rôle d'Active Directory**

Un Active directory est un rôle disponible sur Windows Server qui permet la mise en place d'un service d'annuaire (d'utilisateurs, d'ordinateurs, etc.) et de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows (ex : création de session individuelles), il permet également l'attribution et l'application de stratégies de groupe (Interdiction : de changer de fond d'écran, d'installation d'applications ou de paramétrage en tout genre) [6].

- **Les avantages d'Active Directory**

- Le regroupement et la gestion de tous les utilisateurs et ordinateurs d'un réseau ainsi qu'un contrôle total de l'administrateur sur leurs sessions.
- La possibilité de l'interconnecter à un autre Active Directory d'un site distant et de gérer celui-ci avec les droits suffisants.
- Gérer la redondance dans un même système avec 2 Active Directory ou plus [6].

2. Les nouveautés d'Active Directory

- Active Directory supporte les tickets Kerberos avec des claims (prérequis pour les dynamique ACL)
- Possibilité de cloner les contrôleurs de domaine (si Hyper-V).
- Nouvelles commandes PowerShell.
- Nouvelle console Active Directory Center d'administration.
- Nouveaux objets GPO.

3. Les composants d'Active Directory

Il existe différents composants de l'active directory, chaque composant s'installe en tant que rôle de serveur dans Windows server 2012 [6].

a) Active Directory Domain Services (AD DS)

Il s'agit du composant principal, il constitue un annuaire centralisé destiné à la gestion et à l'authentification des utilisateurs et des ordinateurs.

b) Active Directory Certificate Services (AD CS)

Les services de certificats ADCS constituent l'implémentation de Microsoft de l'infrastructure à clé publique PKI. Celle-ci regroupe les composants et les processus exploités pour émettre et gérer les certificats numériques qui servent au chiffrement et à l'authentification. La mise en œuvre des services de certificats AD n'est pas obligatoire. Cependant, nombreuses sont les organisations qui déploient ce service en interne plutôt que de faire appel aux services d'un fournisseur externe.

c) Active Directory Federation Services (AD FS)

Il s'agit du composant permettant la fédération des services entre différents environnements AD. Cela permet d'établir des relations de confiance avec les partenaires externes de l'entreprise (fournisseurs, fabricants, etc.) dotés de différentes plates-formes, afin de leur donner un accès à certains services internes de manière contrôlée et sécurisée[12].

d) Active Directory Lightweight Directory Services (AD LDS)

C'est ADDS mais allège, seul annuaire est disponible. Cela est utile dans les cas où on aura besoin d'un accès à des données de l'AD sans avoir une autorisation de lecture totale dessus. ADDS contiendra une copie partielle (n'est accessible qu'en lecture) de l'AD, et ne fournit pas l'authentification réseau contrairement à ADDS.

e) Active Directory Rights Management Services (AD RMS)

Ce composant permet de renforcer la solution de sécurité existante d'une organisation en fournissant une stratégie basée sur l'objet et de protection permanente, il est capable de protéger les informations sensibles de l'entreprise, comme les documents de traitement de texte, les messages électroniques ou les données financières, même si ces informations sont déplacées ou expédiées hors de l'organisation, les restrictions de sécurité applicables à un fichier spécifique suivant le document, ou qu'il aille, et ne s'applique pas au conteneur qui accueille le document, mais sur le contenu du fichier[11].

4. La structure d'active directory

a) Utilisateurs et groupes

Utilisateurs et ordinateurs d'Ad est un des principaux outils d'administration pour gérer l'active directory, avec cet utilitaire, vous pouvez prendre en charge tous les utilisateurs, les groupes et les tache informatique, et gérer les unités d'organisation [7].

Les groupes ou les stratégies de groupe sert à simplifier les taches de l'administrateur en leur offrant un contrôle centralisé sur les privilèges, autorisations et capacités des utilisateurs et des ordinateurs.

b) Site et domaines

Un site est un groupe d'ordinateurs présents dans un ou plusieurs sous-réseaux IP .on utilise les sites pour mapper la structure physique d'un réseau.

Un domaine est une partition dans une forêt Active Directory. Le propriétaire administratif par défaut d'un domaine est le groupe Domain Admins de ce domaine. Le groupe Enterprise Admins qui dispose de permissions sur tous les objets de tous les domaines de la forêt se trouve dans le domaine racine. Un administrateur du domaine racine de la forêt peut donc disposer de tous les droits sur tous les domaines de la forêt. C'est en général pour cette raison que le domaine racine n'est pas utilisé dans les structures disposant d'une forêt avec plusieurs domaines [7].

c) forets et Arborescences

Une forêt est un ensemble de domaines partageant la même configuration, le même schéma et le même catalogue global. Dans une forêt chaque domaine approuve directement ou indirectement les autres domaines de la forêt. Ces relations d'approbations ne peuvent pas être supprimées. La forêt est la limite de sécurité d'un annuaire Active Directory. Pour garantir que les utilisateurs d'une entité ne disposent pas d'accès dans l'annuaire d'une autre entité, deux forêts distinctes doivent être créées. Lorsque les domaines ont une structure de noms contiguë, on dit qu'ils sont dans la même arborescence de domaine. Un arbre Active Directory est composé de plusieurs domaines reliés par le biais transitifs bidirectionnels, qui partagent un schéma et un catalogue global communs[7].

d) Unités d'organisation UO

Une unité organisationnelle (OU) est un conteneur dans un domaine. Une OU peut contenir des comptes utilisateurs, des groupes, des comptes ordinateurs et d'autres OU (entre autres). Les OU permettent donc d'organiser l'annuaire. Il est possible de déléguer l'administration du contenu d'une OU à un groupe et/ou utilisateur spécifique et d'appliquer des stratégies de groupes aux utilisateurs et ordinateurs dans cette OU [7].

e) Relation d'approbation

Une relation d'approbation est un lien de confiance établi entre deux domaines Active Directory (ou entre un domaine Active Directory et un domaine Windows NT4 ou entre un domaine Active Directory et un domaine Kerberos non-Windows) [7].

Une relation d'approbation se basant sur deux propriétés principales qui sont : la direction et la transitivité.

- **La direction** : d'une part si une relation est unidirectionnelle, c'est un dire dans un seul sens ce qui permet d'approuver un domaine A à partir d'un autre domaine sans que l'inverse soit appliqué, d'autre part si elle est bidirectionnelle, c'est-à-dire que les deux domaines s'approuvent mutuellement.
- **La transitivité** : C'est-à-dire que si un domaine A approuve un domaine B et que le domaine B approuve lui-même un domaine C et bien alors implicitement le domaine A approuvera le domaine C.

f) l'active directory et DNS

AD utilise le système DNS (domain name system), DNS est un service internet standard qui organise les groupes d'ordinateurs en domaines. Les domaines DNS sont organisés selon une structure hiérarchique. La hiérarchie de domaine DNS est définie à l'échelle de l'internet, et les différents niveaux de la hiérarchie identifient les ordinateurs, les domaines organisations et domaine de premier niveau.

DNS est utilisé pour faire correspondre les noms d'hôtes à des adresses IP numérique, par le biais de DNS, une hiérarchie de domaine AD peut être définie à l'échelle de l'internet, ou bien la hiérarchie de domaine peut être séparée de l'internet et demeurer privée.

DNS fait partie intégrante de la technologie Active Directory à telle enseigne que vous devez configurer DNS sur le réseau avant d'installer AD [8].

g) Protocole DHCP (Dynamic Host Configuration Protocol)

Le Protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une machine, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).

Les avantages de DHCP sont :

- Simplifier l'installation d'un grand nombre de machines.
- Grande souplesse pour les utilisateurs mobiles. Ils peuvent passer d'un réseau à un autre sans avoir à modifier leur paramètre réseau.
- Centralisation de la base effectuant la correspondance entre adresses IP et MAC.

1.6 Conclusion

Dans ce chapitre nous avons présenté les notions et les aspects élémentaires des réseaux informatiques d'entreprise, l'administration réseau et le déploiement de ad sous Windows server 2012.

Le chapitre suivant va se porter sur la présentation de l'entreprise CANDIA (TCHIN-LAIT)et sont étude du réseau ainsi ces déférent équipement de cette entreprise.

Chapitre 2

Etude de l'existant

2.1 Introduction

L'utilisation des réseaux informatiques est une condition indispensable pour la communication entre les différents secteurs de l'entreprise. Mais il est important d'assurer la sécurité du réseau informatique et cela n'est possible qu'avec un bon outil d'administration réseau et pour cela, nous présenterons l'organisme d'accueil Tchîn-lait comme première étape pour mieux connaître sa structure. Puis nous étudierons ses différents réseaux et leurs composants pour pouvoir proposer d'éventuelles solutions.

2.2 Présentation de l'unité Tchîn-Lait / Candia

2.2.1 La marque Candia en Algérie

La marque Candia est présente en Algérie depuis plusieurs années grâce à ses exportations de lait liquide, stoppées en 1998, suite à une hausse importante des taxes douanières.

Le lait en poudre Candia et surtout ses campagnes publicitaires, appréciés par la population algérienne, ont largement contribué à la notoriété de la marque sur le territoire algérien durant les années 1990. Plusieurs industriels algériens se sont spontanément adressés à Candia afin de se lancer sur le marché du lait.

Le projet de l'entreprise Tchîn-Lait a retenu l'attention de Candia qui l'a choisi. On est en 1999 et une franchise Candia est née en Algérie.

2.2.2 Historique et situation géographique

Tchîn-lait est une société privée de droit Algérien (SARL), implanté sur l'ancien site de la limonaderie Tchîn-Tchîn.

Cette dernière était à l'origine d'une entreprise familiale spécialisée dans les boissons gazeuses depuis 1954, ayant de fait une longue expérience dans le conditionnement des produits sous forme liquide.

C'est à l'arrivée des grandes firmes multinationales sur le marché des boissons gazeuses, qu'elle a révisée sa stratégie d'où l'idée de reconversion vers le lait UHT qui a donné naissance à Tchîn lait sous label " Candia ".

C'est en 1999 qu'une franchise Candia est née en Algérie, devenue fonctionnelle en 2001. Cette laiterie moderne construite sur une superficie totale de 3000 m², situé sur la route nationale n°12 à l'entrée ouest de la ville de Bejaïa (Bir-Slam).

Les installations des machines ont été effectuées par la société française Tétra pack. L'unité est dotée d'un équipement ultra moderne, de très grande capacité sous la marque Candia, 25 tests de contrôle sont effectués quotidiennement d'une manière permanente et régulière par le laboratoire Tchîn-Lait durant tout le cycle de fabrication. En plus de ces tests de qualité, le lait UHT est consigné durant 72 heures avant sa commercialisation, pour avoir la garantie d'un lait stérile.

1. Réseau de distribution

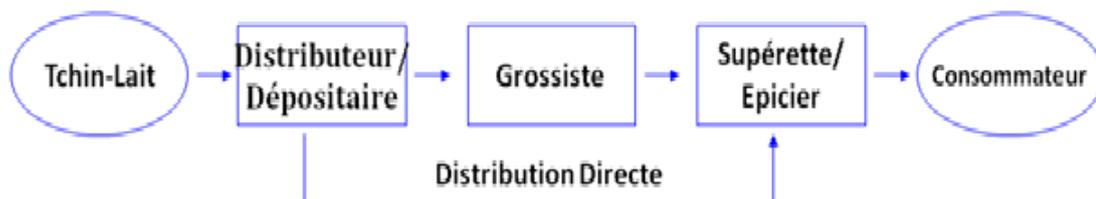


FIGURE 2.1 – Réseau de distribution

2.2.3 Les missions de l'entreprise

La mission d'entreprise est la déclaration de la raison d'être de l'entreprise et de la façon dont elle entend atteindre ses buts. Tchîn-Lait a pour mission principale de :

- Mobiliser les ressources internes en motivant les employés qui peuvent s'identifier à des valeurs fortes.
- Aligner les décisions et actions prises au quotidien par l'ensemble du personnel.
- Communiquer une image forte et claire aux clients et aux actionnaires de l'entreprise.
- Forcer les managers à se poser des questions fondamentales sur les valeurs et les comportements qu'ils doivent chercher à promouvoir.

2.2.4 Les objectifs de l'entreprise

La fonction première d'une entreprise varie selon l'entreprise ou même selon les points de vue au sein d'une même entreprise (par exemple, point de vue de l'actionnaire, de l'employé, du syndicat, de la direction, etc.). Parmi les différentes fonctions opérationnelles habituellement observées, on trouve :

- Servir le marché, en produisant et distribuant des biens et services
- Satisfaire son client.
- Assurer le revenu.
- Assurer l'épanouissement individuel à ses salariés.
- Faire gagner de l'argent à ses actionnaires.

2.2.5 La structure de l'entreprise

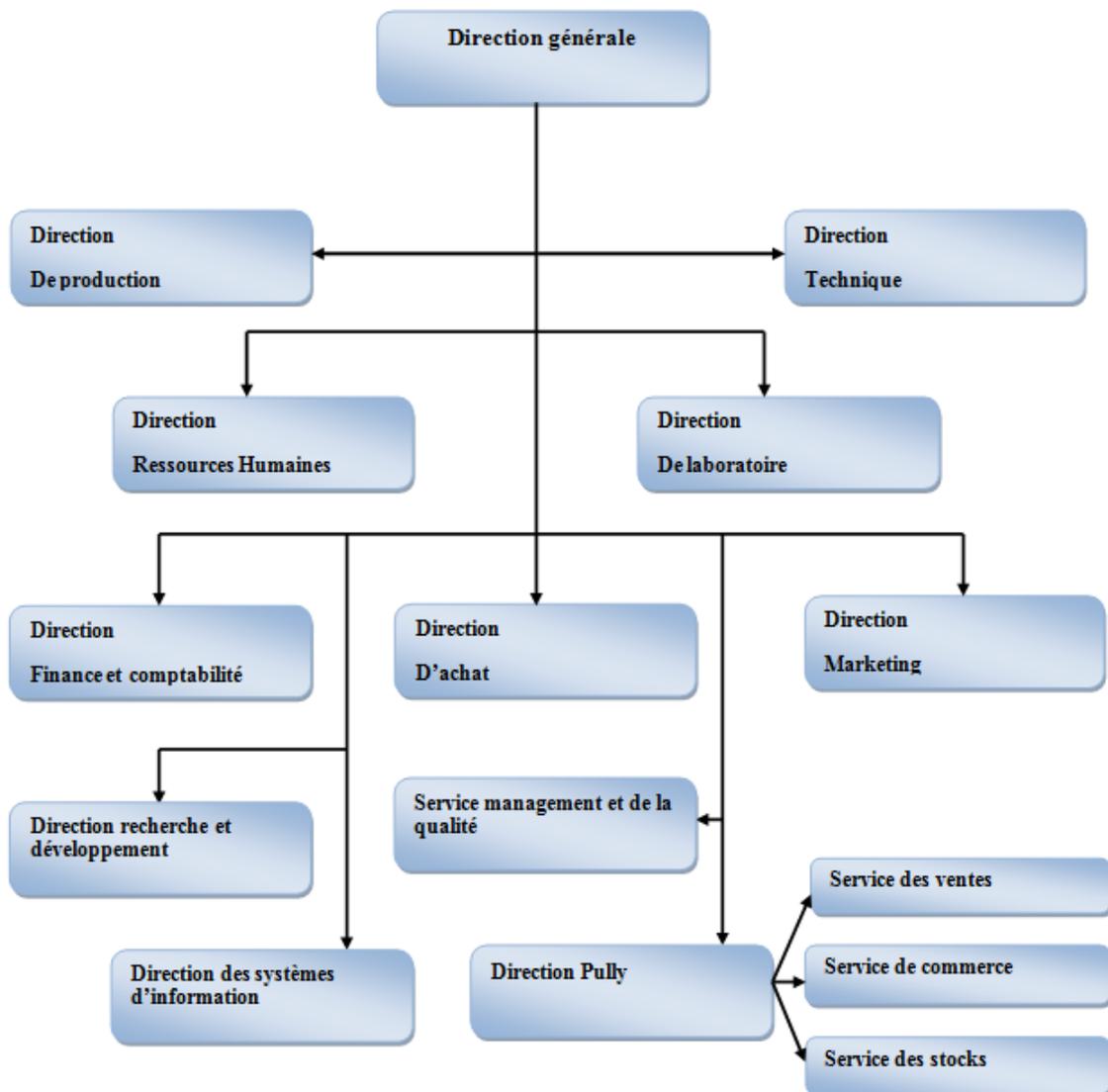


FIGURE 2.2 – Organigramme général de Tchiv-Lait.

1)Présentation de la direction d'informatique

La direction d'informatique est une structure de Tchiv-Lait rattaché directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise, et cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information. Elle est composée de :

- Un Directeur de Systèmes d'information.
- Un administrateur réseau et système.
- Un administrateur des bases de données.
- Un ingénieur support.

2.3 Présentation du réseau de l'entreprise

Le réseau d'entreprise permet de relier les ordinateurs entre eux via un serveur qui va gérer l'accès à Internet, les emails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers. Il permet aussi à l'entreprise de centraliser ses données et de travailler en équipe de manière productive.

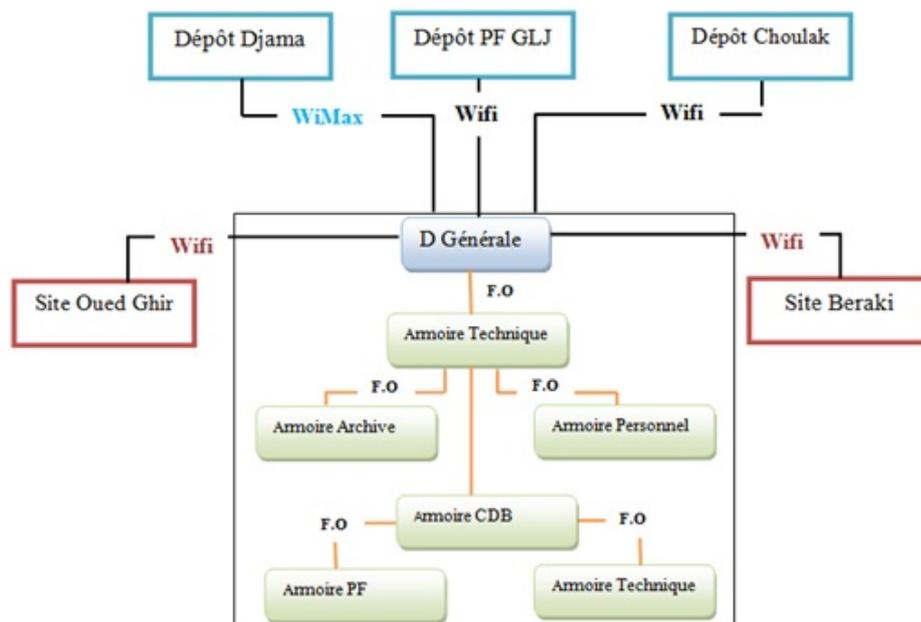


FIGURE 2.3 – L'Architecture du réseau de Tchiv-Lait.

2.3.1 Les différents équipements qui existent dans le réseau

A. Les Switchs et les routeurs du réseau

Désignation	Modèle	Caractéristiques
Quatre Switch Net Gear	GS724T	24 ports RJ45 - 2 ports SFP
Un Switch Net Gear	GS748T	48 ports RJ45 – 4 ports SFP
Trois Switch Cisco	3560	48 ports RJ45 – 4 ports SFP
Un routeur Cisco	3750	12 ports SFP
Un routeur Cisco	1900	/

TABLE 2.1 – Les Switchs et les routeurs du réseau.

B. Les différents serveurs du réseau de l'entreprise

Le réseau de Tchén Lait se base sur le mode de communication (architecture) client-serveur dont plusieurs serveurs sont disponibles pour fournir des services aux différents clients de l'entreprise. Chaque serveur s'occupe des tâches spécifiques comme suit :

- DC-server : (Domain Control Server) serveur contrôleur de domaine , il exécute les services de Active Directory .
- DB-server : (Data Base Server) est un serveur de base de données, sur lequel un système de gestion de base de données (SGBD) ici SQL Server 2008 R2 est installé .
- TERMINAL-server : est un serveur pour les applications de sauvegardes.
- WMS-server : est un serveur de gestion d'entrepôt et de traçabilité .
- EXCHANGE-server : est un serveur de messagerie Microsoft Exchange 2010. Pour cette entreprise, les comptes de messagerie sont configurés par Microsoft Office Outlook .
- PLMS-server : est un serveur pour l'application des statistiques de production.
- KSC-server : est un serveur des applications antivirus. Pour l'entreprise Tchén Lait kaspersky est installé sur tous ses ordinateurs.
- HHT-server : est un serveur des applications des ventes mobiles.
- TSE-server : est un serveur de bureau à distance .
- Serveur-DATA : est un serveur pour le partage de fichiers entre les différents services et il contient les fichiers partagés .

C. Les autres équipements

Désignation	Modèle
170 Ordinateurs	Portable & Bureau
37 Imprimantes	Epson, Canon, Canon IR25
Deux modems	ADSL
Un par feu	Sophos

TABLE 2.2 – Les Autres équipements du réseau.

D. Les supports de transmission

Pour relier les différents équipements qui sont utilisés dans le réseau de l'entreprise, TchIn-Lait opte pour deux types de media, la fibre optique et le câble à paires torsadées.

2.3.2 Les différents logiciels de l'entreprise

L'entreprise TchIn-Lait dispose plusieurs logiciels de base de données, comme :

- ERP (Entreprise Resource Planning) : est un outil informatisé qui permet le pilotage de l'entreprise. Sa particularité est d'embarquer, en un même logiciel et une seule base de données, les fonctionnalités nécessaires à la gestion de l'ensemble de l'activité d'une entreprise : gestion comptable, gestion commerciale, gestion des stocks...
- Assabil : est une solution de gestion de la force de vente mobile, elle s'adresse aux différents industriels et entreprises de distribution pour renforcer leur positionnement sur le marché et accroître leur vente.
- Logitrack : Logitrack est la dénomination du logiciel de traçabilité des produits après leur identification sur ligne de production. Logitrack, relié à l'ERP, permet de gérer :
 - les différents mouvements de stock.
 - la préparation des commandes.
 - la traçabilité dans la prise d'échantillonnage.
 - la relation avec le laboratoire qualité.
- Logiciels d'exploitation :
 - Windows serveur 2008 R2.
 - Microsoft office Word 2007, 2008, 2010.
 - Microsoft office Excel 2007, 2010, 2013, 2016.

2.4 Description du projet

La description du projet consiste à définir les besoins de l'entreprise, et de proposer des solutions qui remédieront à ces dernières.

2.4.1 Description des besoins

L'entreprise dispose à ce jour de serveurs exploitant le système Windows serveur 2008, et après l'étude que nous avons réalisée, nous avons constaté que ce système nécessite les améliorations suivantes :

- Donner aux utilisateurs une gestion efficace et simplifiée qui permettant de gérer plusieurs serveurs à partir d'un seul.
- Réduction de la consommation électrique des serveurs et réaliser des économies sur les coûts d'exploitations, fournissent aux clients une méthode simple d'accéder aux infrastructures de l'entreprise tout en préservant la sécurité et la conformité.
- Donner aux utilisateurs la possibilité d'une récupération plus rapide et temps d'arrêt minimales en cas d'une catastrophe. En effet, la gestion des utilisateurs va devenir très difficile avec l'augmentation de nombre d'utilisateur et des ressources partagées.

2.5 La solution proposée

Suite aux problèmes liés à l'administration du réseau via Windows server 2008, nous avons opté pour une solution d'administration qui est une mise à niveau des serveurs vers Windows server 2012, qui permet à l'entreprise Tchic-Lait de faire évoluer, gérer ses infrastructures plus efficacement et de répondre aux besoins des entités grâce à ces nouvelles fonctionnalités.

Windows server 2012 aide les clients à transformer les opérations du service informatique de façon à réduire les coûts et fournit un autre niveau de la valeur de l'entreprise. Il offre aux clients le Gestionnaire de serveur, une fonctionnalité permettant de gérer plusieurs serveurs à partir d'un seul et d'effectuer des tâches telles que le déploiement des rôles et des fonctionnalités à distance (pour les serveurs physiques et virtuels), créer, grouper et personnaliser des listes de serveurs. En outre, Windows PowerShell 3.0 offre une plate-forme de gestion globale pour tous les composants du datacenter.

Windows Server 2012 permet aussi aux clients de tirer parti du stockage, des réseaux et de l'infrastructure du serveur pour obtenir les meilleurs résultats de l'exploitation de n'importe quelle plateforme. Il offre également un meilleur rendement énergétique et comprend un certain nombre d'améliorations au niveau de l'hôte Hyper-V et du système d'exploitation invité qui permettent de réduire la consommation électrique des serveurs et de réaliser des économies sur les coûts d'exploitation.

Nous avons proposés différentes solutions basées sur les fonctionnalités de Windows server 2012 afin de pallier les problèmes rencontrés au sein de l'entreprise :

2.5.1 Mise en œuvre des services réseaux avancées

Configuration du serveur DHCP : a pour rôle de distribuer des adresses IP à des clients d'une manière dynamique pour une durée déterminée.

Configuration de serveur DNS : est un service dont la principale fonction est de traduire un nom de domaine en adresse IP.

2.5.2 Mise en œuvre de contrôleur de domaine Active Directory Domain Services (AD DS)

Active Directory permet de gérer les ressources réseau d'une manière simple et centralisée. Cette gestion s'appuie sur la structure physique et logique de l'annuaire Microsoft. Notre travail consistera en partie à réaliser les points suivants :

- Configuration de relation d'approbation AD DS.

- Surveiller et établir la continuité de service pour les services de domaine.
- Mettre en œuvre et gérer les GPOs.
- Gérer les paramètres utilisateurs avec les GPOs.

2.5.3 Mise en œuvre de l'autorité de certification Active Directory Certificate Services (AD CS)

Il permet de gérer l'utilisation des certificats de manière centralisée. Nous allons mettre en place quelques services proposés par AD CS tels que :

- Mise en œuvre des infrastructures à clé publique (PKI).
- Déploiement des autorités de certification AD CS.
- Déploiement et gestion des modèles de certificats.
- Mise en œuvre de la distribution de certificats.

2.5.4 Mise en œuvre des services de fichiers avancés

- Configuration du stockage iSCSI sous Windows server 2012.
- Configuration de BranchCache.
- Gestion et contrôle du partage.
- Ajout des clichés instantanés.

2.5.5 Mise en œuvre de la reprise en cas de panne

- Mise en œuvre d'une solution de sauvegarde (Backup).

2.6 Contraintes

Tout en respectant les objectifs, il est bien sur nécessaire d'assurer la continuité du service réseau et que les besoins des clients soient assurés, pendant et après la mise en œuvre du projet. Les performances du réseau ne doivent pas non plus être altérées. En outre, les utilisateurs ne doivent pas s'apercevoir qu'un changement a été opéré sur leur réseau local.

2.7 Conclusion

L'étude de l'existant nous a permis de ce familiariser avec le réseau actuel de Tchil-Lait et de l'étudier assez profondément et c'est se qui nous a permis de voire ses faiblesses, et conduit à proposé la solution pour palier à ces derniers.

Le chapitre suivant va être basée sur la description et la réalisation des différentes étapes, à savoir l'installation du matériel et de logiciel Active directory et la configuration des différents services.

Chapitre 3

Réalisation

3.1 Introduction

Ce chapitre sera consacré à la mise en œuvre et déploiement d'active directory au sein de l'entreprise Tchiv-Lait. Nous allons décrire les différentes étapes suivies lors de l'installation et configuration des services proposées par Windows server 2012.

3.2 Installation de la machine virtuelle(VMware Workstation 10)

Le sens originel de machine virtuelle est la création de plusieurs environnements d'exécution sur un seul ordinateur, dont chacun émule l'ordinateur hôte. Cela fournit à chaque utilisateur l'illusion de disposer d'un ordinateur complet alors que chaque machine virtuelle est isolée des autres. Le logiciel hôte qui fournit cette fonctionnalité est souvent dénommé superviseur ou hyper viseur. Ce concept va plus loin que celui des simples temps partagés où chaque utilisateur dispose seulement d'un espace de développement personnel, et non d'une machine simulée entière.

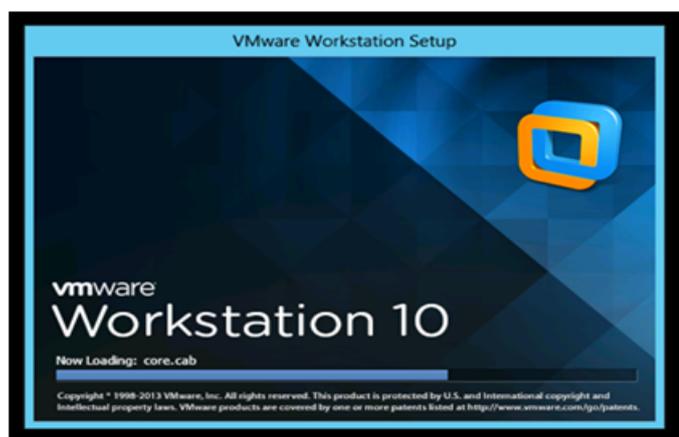


FIGURE 3.1 – Installation de la machine virtuelle.

3.3 Installation de Windows server 2012

L'installation de Windows server 2012 est très classique et ressemble à celle de Windows 8. Les différents écrans sont aussi très proches de Windows server 2008/R2.

Ce système peut être installé en démarrant depuis le DVD, ou depuis une image ISO.



FIGURE 3.2 – Installation de Windows server 2012.

Le premier démarrage se fait sur l'écran Gestionnaire de serveur, son design est très différent des anciennes versions de Windows server mais les fonctions sont conservées,

voire améliorées. Celui-ci nous donne la possibilité d'ajouter des rôles, surveiller l'état de notre serveur ou encore gérer ses fonctionnalités.

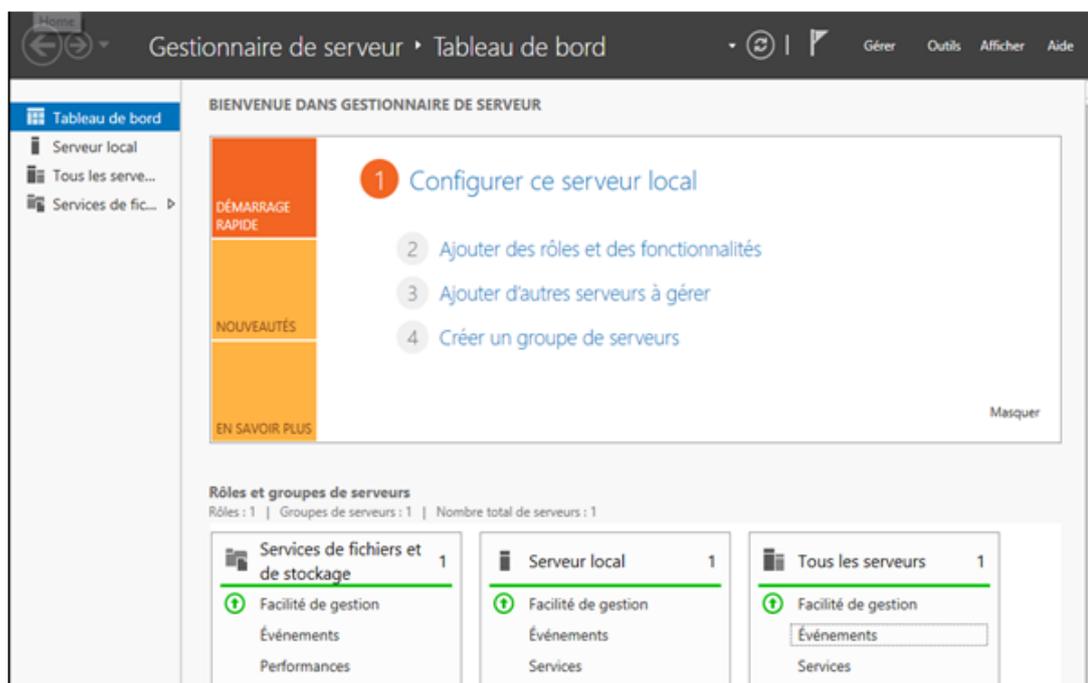


FIGURE 3.3 – Gestionnaire de serveur.

Pour commencer, il faudra configurer notre serveur local, pour cela nous cliquons sur configurer ce serveur locale, cette étape nous permet de définir les propriétés du serveur.

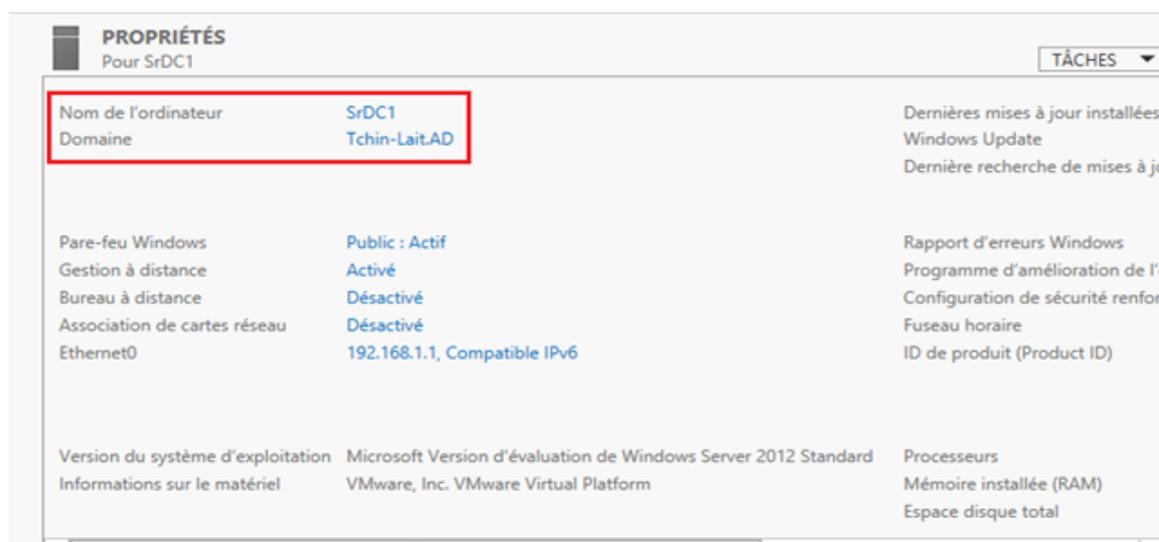


FIGURE 3.4 – Configuration du serveur local.

3.4 Création du contrôleur de domaine et DNS

Avant de promouvoir le serveur en tant que contrôleur de domaine dans notre domaine, il faut installer (le rôle Service de domaine Active Directory).

- Dans le Gestionnaire de serveur, nous avons sélectionné (Ajout des rôles et des fonctionnalités).
- Au niveau des rôles, choisir (Service AD DS) qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour indiquer que d'autres éléments requis AD DS doivent être installés, cliquer sur "Ajouter des fonctionnalités".

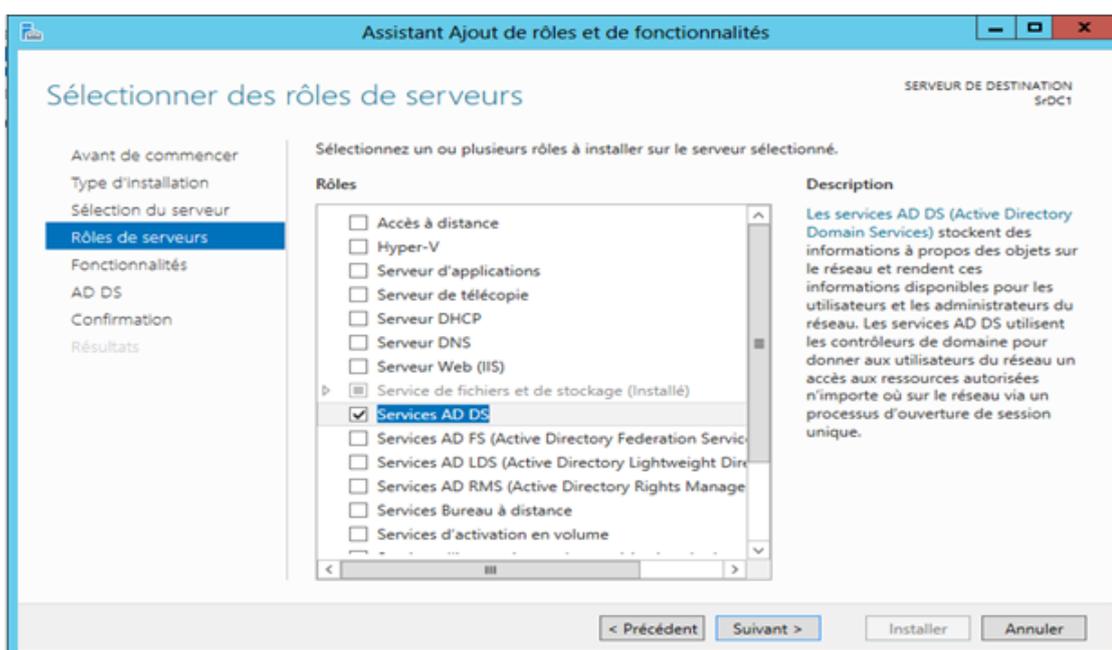


FIGURE 3.5 – Ajout du service AD DS.

Une fois les fonctionnalités d'AD DS installées, le serveur va redémarrer automatiquement. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé.



FIGURE 3.6 – Promouvoir du serveur en contrôleur de domaine.

Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en couchant sur Ajouter une nouvelle forêt et en spécifiant le nom de notre domaine appelé TchIn-Lait.AD .

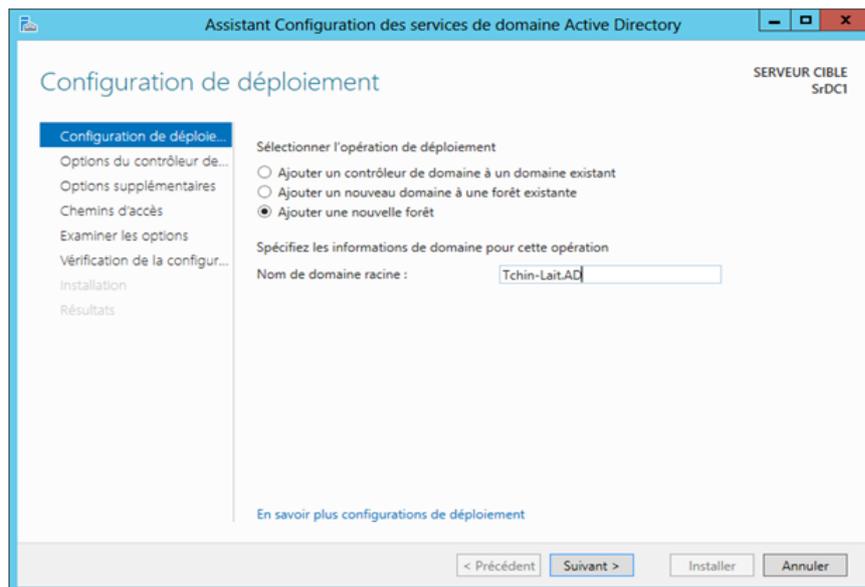


FIGURE 3.7 – Création du domaine TchIn-Lait.

L'étape suivante consiste à choisir le niveau fonctionnel de la forêt ou du domaine.

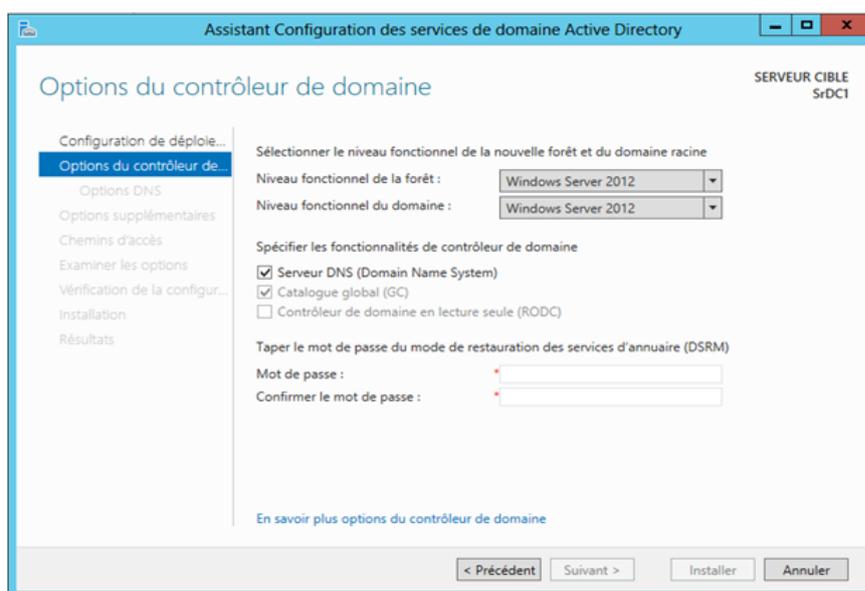


FIGURE 3.8 – Sélection du niveau fonctionnel de la forêt et du domaine.

Lorsque nous installons les services de domaine Active Directory (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS. La zone DNS résultante est intégrée à AD DS contrôlé par le serveur SrDC1. Après configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu outils, notre domaine est créé et l'ouverture d'une session s'effectue avec le compte d'administrateur du domaine TchIn-Lait.Administrateur.

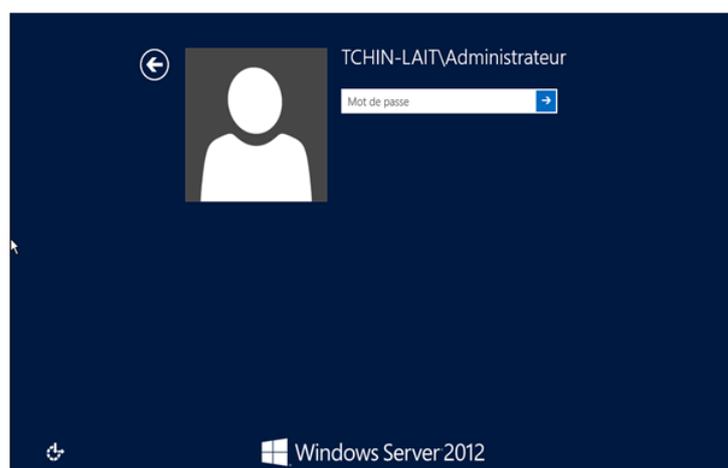


FIGURE 3.9 – Ouverture de la session Administrateur.

3.5 Installation et configuration du service DHCP

Pour que les PC et les serveurs communiquent nous devons leur donner une adresse IP, un masque de sous réseau, une passerelle et un serveur DNS qui est obligatoirement un DNS d'Active Directory.

- Dans l'assistant de gestion des rôles, ajouter le rôle DHCP.

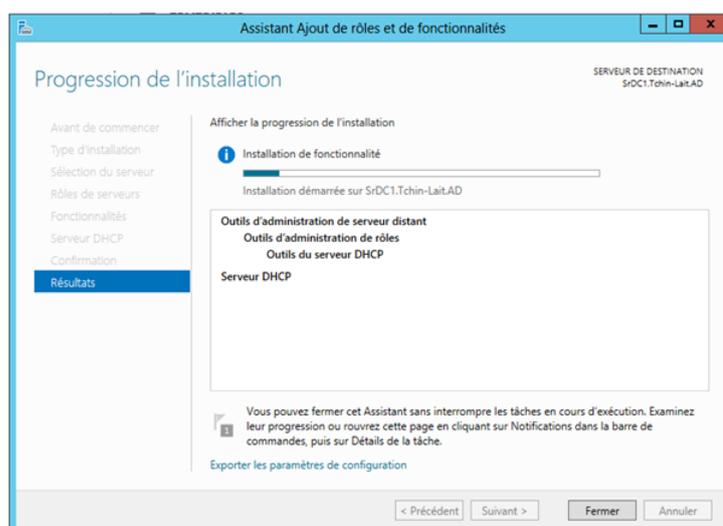


FIGURE 3.10 – Installation du serveur DHCP.

Après quelques minutes le rôle est installé, l'écran final nous invite à commencer la configuration de DHCP.

- création de nos étendues DHCP à l'aide de la console d'administration DHCP qui à été lancée depuis le menu Outils du gestionnaire de serveur.

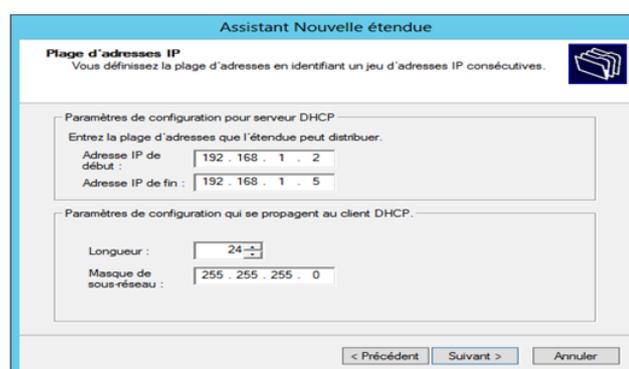


FIGURE 3.11 – Création des étendues DHCP.

- Ajouter d'éventuelles exclusion afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP , PC en adresse fixe, serveur...).

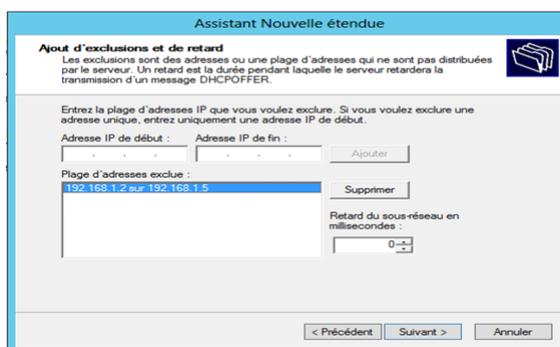


FIGURE 3.12 – Ajout d'exclusion DHCP.

3.6 Organisation des clients AD en unités organisationnelles

Nous allons commencer à peupler notre Active Directory. Pour ce faire nous devons lancer la console Utilisateur et ordinateur Active Directory. On peut la lancer depuis le Gestionnaire de serveur puis sous la rubrique AD DS.

Nous allons créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes, pour cela on se place dans l'arbre à la hauteur de notre domaine Tchiv-Lait.AD et sur le menu, nous choisissons l'option Unité d'organisation .

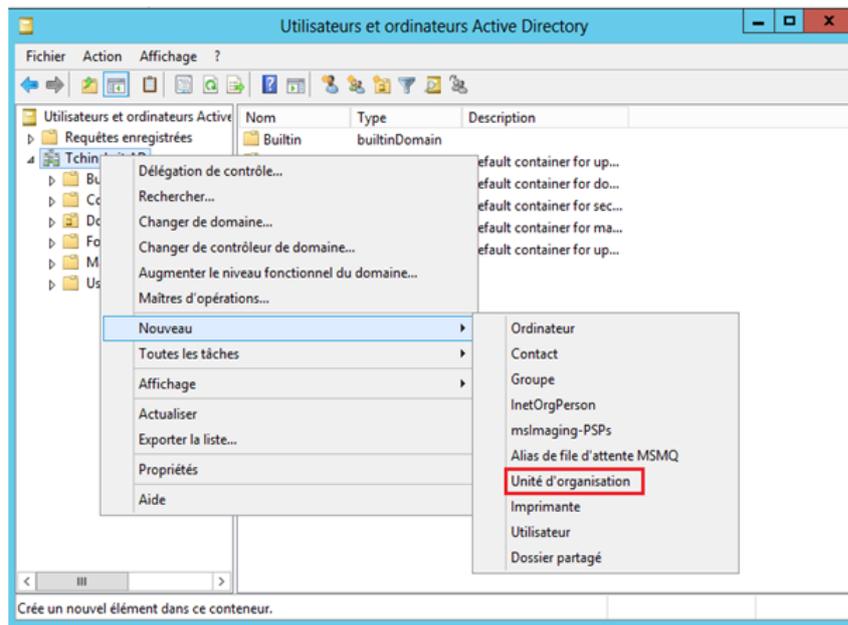


FIGURE 3.13 – Création d'une unité d'organisation.

Cette procédure nous permet de regrouper des ordinateurs ou des utilisateurs dans une seule unité afin de pouvoir leurs appliquer des procédures et des stratégies des groupes.

Après avoir créé les unités organisationnelles relatives à notre entreprise, nous pouvons créer les premiers utilisateurs et commencer à peupler nos unités. Nous répétons la même procédure pour tous les nouveaux utilisateurs.

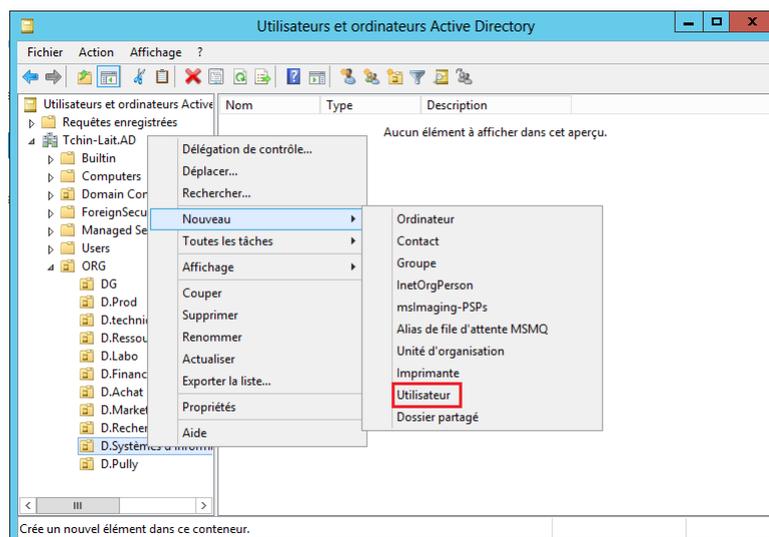


FIGURE 3.14 – Ajout d'utilisateur.

Pour chaque UO, nous avons créé des comptes utilisateurs avec un identifiant unique de la forme P.NOM@TCHIN-LAIT.AD

The screenshot shows a Windows Active Directory 'Nouvel objet - Utilisateur' dialog box. At the top, it says 'Créer dans : Tchin-Lait.AD/ORG/D.Systèmes d'information'. Below this, there are several input fields: 'Prénom' with 'Nouria', 'Initiales' (empty), 'Nom' with 'SAADELI', and 'Nom complet' with 'Nouria SAADELI'. There are also fields for 'Nom d'ouverture de session de l'utilisateur' (N.SAADELI) and a dropdown menu showing '@Tchin-Lait.AD'. Below that, there are fields for 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' with 'TCHIN-LAIT\' and 'N.SAADELI'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

FIGURE 3.15 – Création des sessions utilisateur.

3.7 Mise en œuvre des Group Policy Organisation (GPO)

Les stratégies de groupe sont des outils de configuration permettant de modifier un ensemble de paramètres s'appliquant à des configurations utilisateur ou à des configurations ordinateur membres d'un domaine Active Directory (AD DS), ils présentent plusieurs avantages dont : la réduction des couts, le contrôle des configurations, la conservation des utilisateurs productifs, le renforcement de la sécurité et la gestion des droits d'accès aux ressources.

Après avoir installé Active Directory, mis en place notre domaine dans une nouvelle forêt et créé nos unités d'organisation, nous allons mettre en place nos GPO.

La première étape consiste à modifier le ” default domaine Policy ” dans le menu ” Gestion de stratégie de groupe ” celle-ci représente la GPO par défaut de notre domaine, il suffit de faire un clic droit et de modifier comme la figure ci-dessous l’indique :

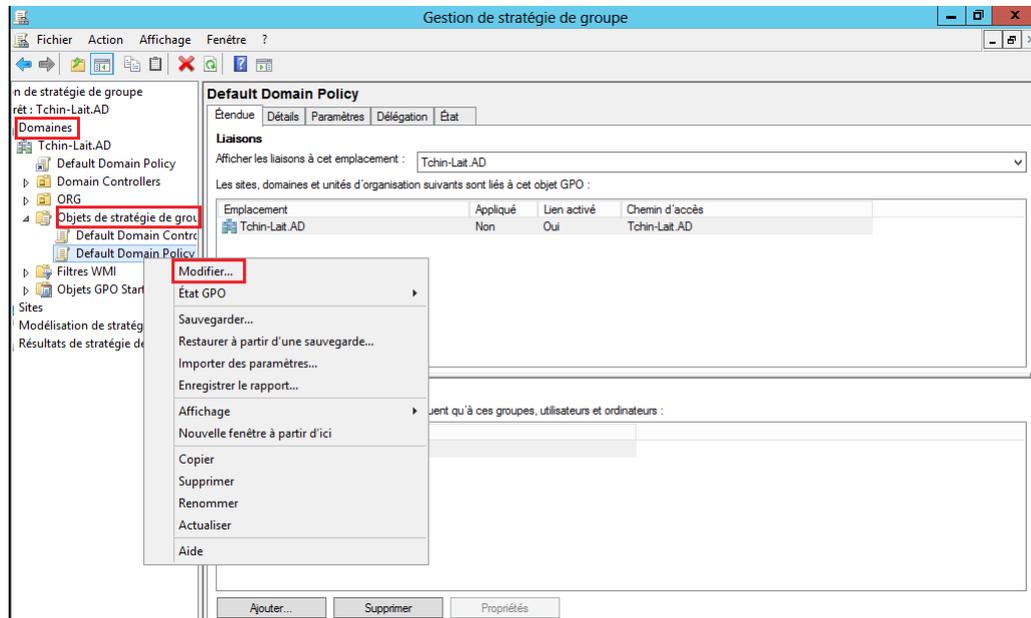


FIGURE 3.16 – Modification de la stratégie de groupe par défaut.

a) Configuration ordinateur

Arrivé à la fenêtre ” Editeur de gestion des stratégies de groupes ” nous remarquons qu’il y’a deux types de configuration : ordinateur et utilisateurs, nous commencerons par les configurations ordinateurs :

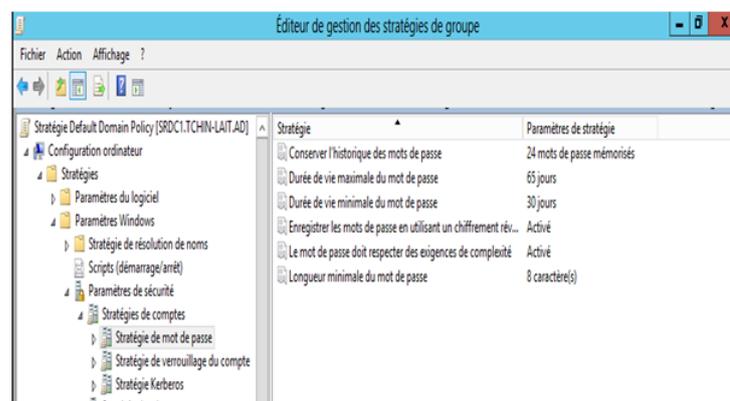


FIGURE 3.17 – Configuration d’une GPO ordinateur.

La configuration ordinateur s'applique au démarrage et est valable pour tous les utilisateurs qui ouvrent une session. Elle s'applique seulement si le site Active Directory, le domaine, ou l'OU auquel est liée la GPO contient des objets ordinateurs.

b) Configuration utilisateur

La configuration utilisateur s'applique à l'ouverture de session et " suit " l'utilisateur quelque soit l'ordinateur sur lequel il se connecte. Elle s'applique seulement si le site Active Directory, le domaine, ou l'OU auquel est liée la GPO contient des objets utilisateurs.

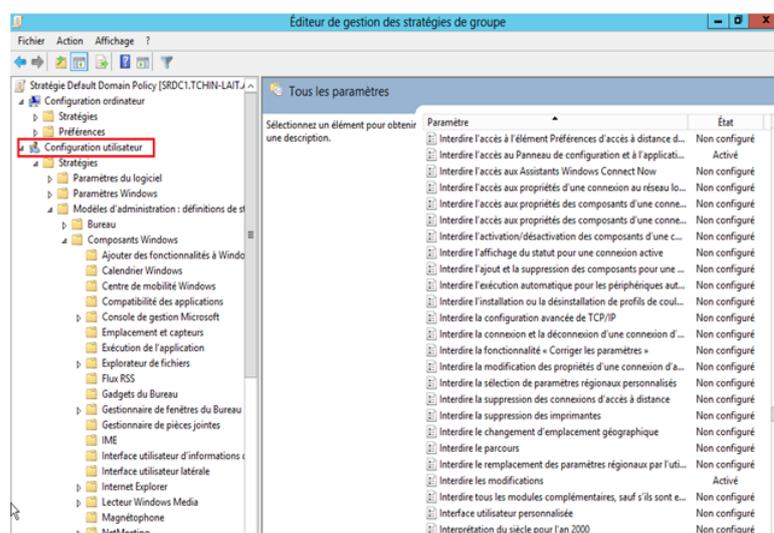


FIGURE 3.18 – Configuration d'une GPO utilisateur.

Nous pouvons faire différents paramétrages liées aux utilisateurs, comme interdire l'accès au panneau de configuration, interdire la suppression des imprimantes et bien d'autres.

c) Configuration d'une GPO pour une OU

Pour créer une GPO propre à une unité d'organisation, dans le menu " Gestion de stratégie de groupe " choisir l'unité organisationnelle puis nous n'avons plus qu'à faire une clique droite ' " "Créer un objet GPO dans ce domaine et lier ici.. " .

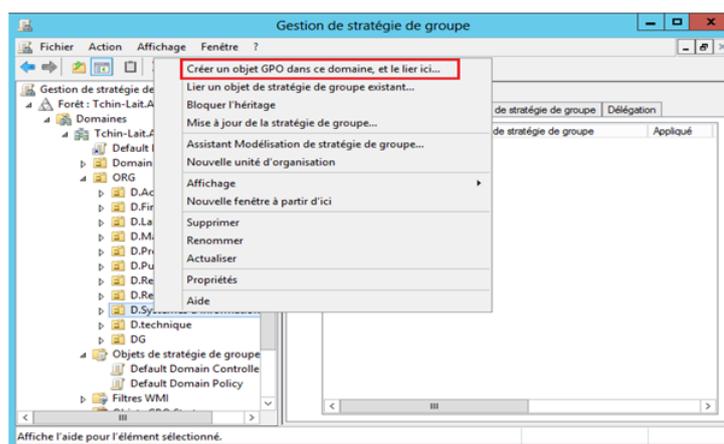


FIGURE 3.19 – Création d’une GPO pour une UO.

Une fenêtre s’ouvre nous permettant de nommer notre GPO. Dans cet exemple, nous avons choisi le nom GPO-Système d’information pour l’unité organisationnelle D.Système d’information.

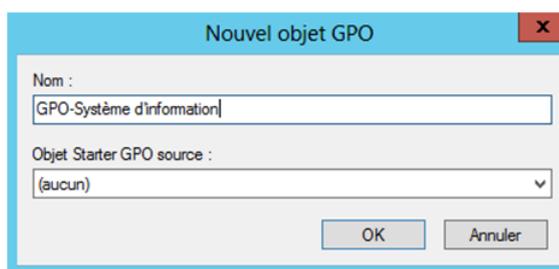


FIGURE 3.20 – Création d’une nouvel GPO.

Le GPO est maintenant visible dans l’unité d’organisation ” D.Système d’information ”. Nous n’avons plus qu’à la modifier comme nous l’avons fait précédemment pour la ” Policy default objet ”.

3.8 Création des profils itinérants

En entreprise, ce n’est pas rare que les utilisateurs changent de bureaux, utilisent l’ordinateur du collègue, changent de service, les utilisateurs sont amenés à utiliser différentes machines. De ce fait, la disposition sur une machine à l’autre ne sera pas la même (personnalisation de l’espace de travail) et les données ne seront pas les mêmes si l’utilisateur stocke du contenu sur sa machine.

La première étape consiste à créer un répertoire que nous allons partager et qui servira à stocker les données des profils, qui est nommé " Profils itinérants " .

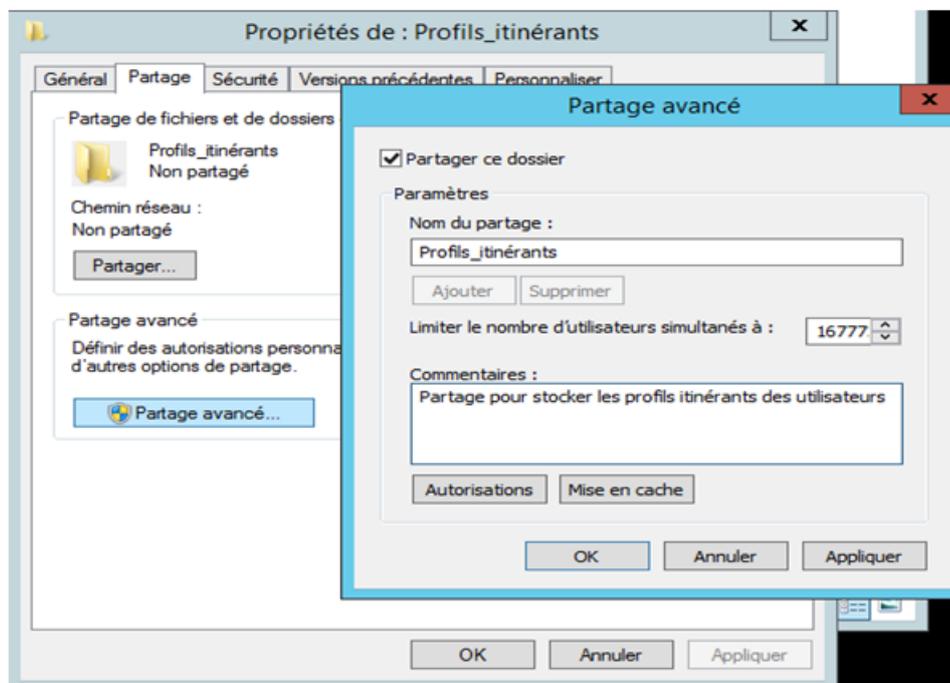


FIGURE 3.21 – Configuration du partage.

Dans la configuration du partage, cliquez sur "Autorisations" pour vérifier que le " nom de groupes ou d'utilisateurs " est bien positionné sur Tout le monde, puis indiquer autorisé sur la valeur Contrôle totale. Ensuite, dans la console Utilisateurs et ordinateurs

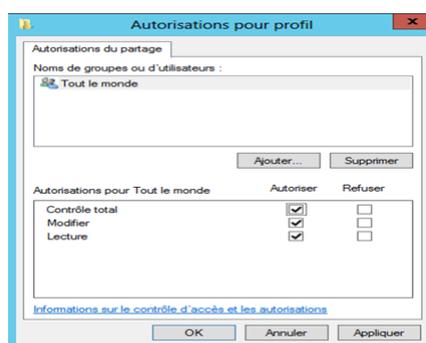


FIGURE 3.22 – Autorisation pour profils utilisateur.

Active Directory et dans les propriétés d'un utilisateur, choisir l'onglet Profil puis Chemin du profil. Nous devons renseigner l'adresse du dossier partagé sous la forme :

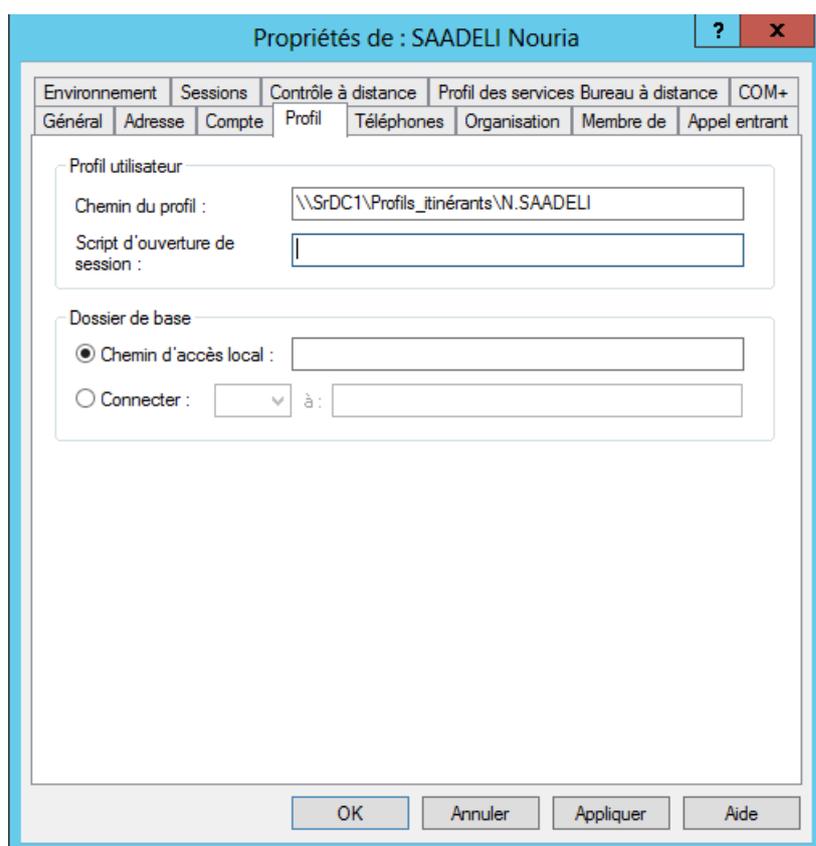


FIGURE 3.23 – Spécification du profil de l'utilisateur.

L'opération est à faire sur chaque compte utilisateur. Le dossier utilisateur sera situé sur le serveur, et sera synchronisé à chaque ouverture et fermeture de session.

3.9 Mise en œuvre de l'autorité de certification Active Directory Certificat Services (AD CS)

Dans cette partie, nous allons créer une autorité de certification racine d'entreprise et nous modifierons les stratégies de groupe pour que les clients de l'Active Directory reçoivent automatiquement le certificat de notre autorité de certification racine.

A. Installation et configuration de l'autorité de certification racine d'entreprise

Après l'installation du " Service de certificats Active Directory " sur le gestionnaire de serveur, et avoir cocher la case " Autorité de certification " pour configurer ce rôle. La figure suivante présente un résumé des configurations post installation.

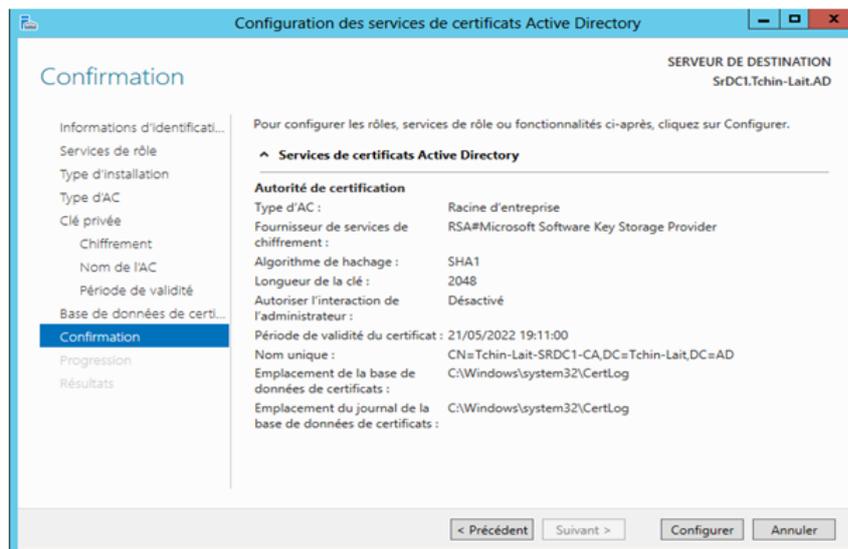


FIGURE 3.24 – Configuration d'une PKI.

3.9.1 Exportation du certificat de l'autorité racine

Notre certificat étant généré par une autorité de certification autonome, nous devons partager le certificat racine avec toutes les machines du domaine. Ainsi chaque ordinateur devra avoir le certificat racine dans le conteneur "Autorité de certification racines de confiance". Pour pouvoir partager le certificat racine, il faut commencer par l'exporter.

- Ouvrez la console mmc pour accéder aux certificats.
- Sélectionnez le premier certificat racine. Puis Faites un clic droit, "Toute les tâches" et enfin cliquez sur "Exporter".

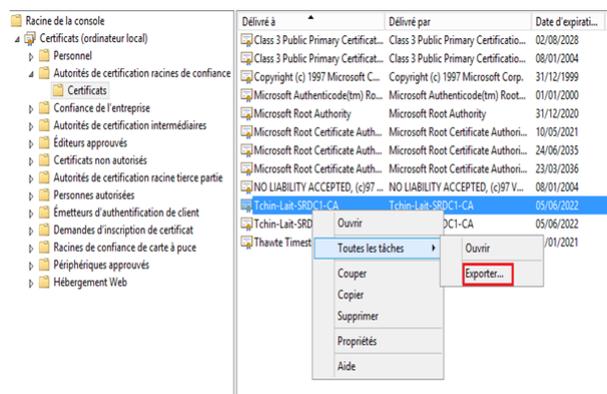


FIGURE 3.25 – L'exportation du certificat.

3.9.2 Création d'un nouveau modèle de certification

Un modèle de certificat que l'on peut appeler aussi "Template" de certificat permet de définir des paramètres comme la durée de validité, le domaine, les droits, etc. Ces paramètres seront appliqués à chaque certificat généré à partir du modèle.

- Ouvrez le "Gestionnaire de serveur"
- Dans le menu en haut à droite, cliquez sur "Outils" puis "Autorité de certification".
- Développez l'autorité de certification, puis cliquez sur "Modèles de certificats".
- Faites un clic droit sur le répertoire "Modèle de certificats", puis cliquez sur "Gérer" ensuite dupliquer le modèle " Serveur web ".

L'étape qui suit consiste à renommer le nouveau modèle de certification et modifier la période de validité.

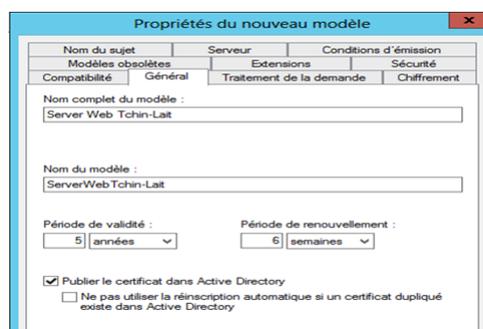


FIGURE 3.26 – Propriétés du nouveau modèle de certificat.

Dans l'onglet "Sécurité", pour le groupe d'utilisateur "Utilisateurs authentifiés" cochez les deux options suivantes : "Inscrire" et "Inscription automatique".

Pour que le nouveau modèle soit correctement pris en compte, il est conseillé de faire une mise à jour des GPO.

- Ouvrez une invite de commande (CMD), puis tapez la commande "gpupdate /force".



FIGURE 3.27 – Mise à jour de la stratégie d'ordinateur.

3.9.3 Demande d'un certificat

Sur la console aller à "Personnel", puis cliquez sur "Toutes les tâches" et enfin "Demander un nouveau certificat". Ensuite sur le menu qui apparaît sélectionner " Toutes les taches " puis " demander un nouveau certificat " .

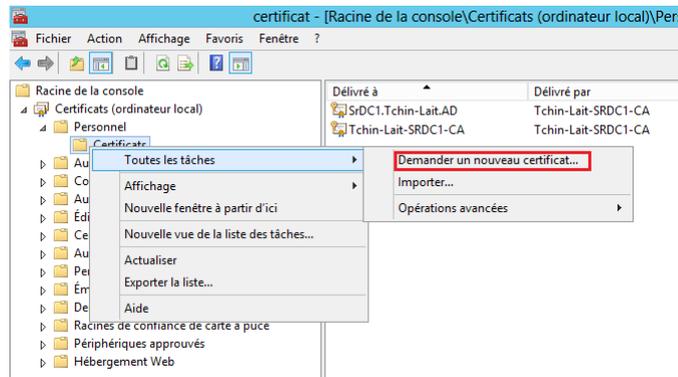


FIGURE 3.28 – Demande d'un nouveau certificat.

Suite à ca, nous choisissons notre nouveau de certificat crée auparavant qui est " serveur web tchin-lait " .

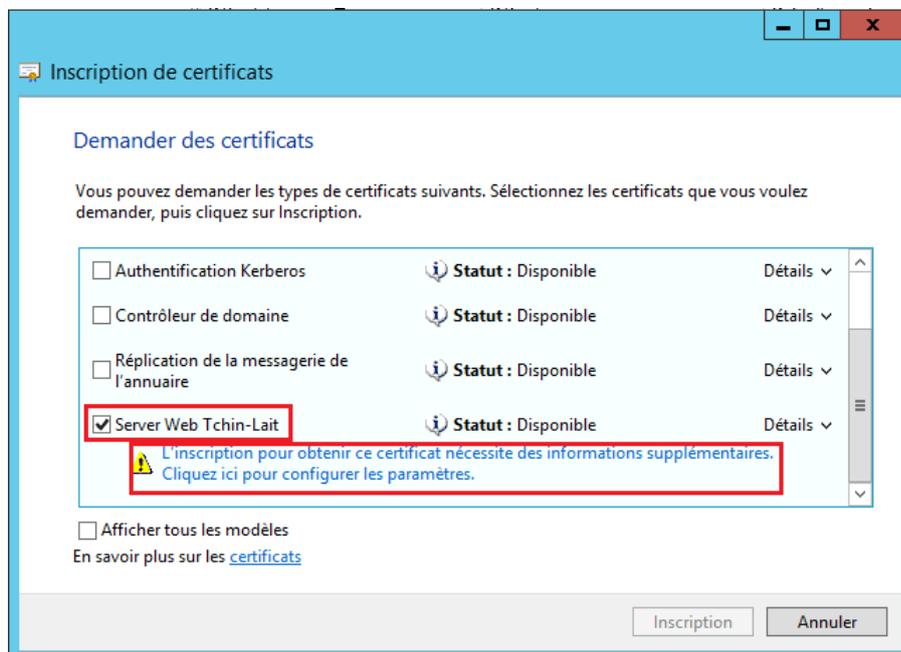


FIGURE 3.29 – Le choix d'un type de certificat.

Etant donné que ce certificat sert à vérifier l'adresse d'un site internet, et que son inscription nécessite des informations supplémentaires, ou doit indiquer le nom de domaine de l'ordinateur qui est " TchIn-Lait.AD " comme " nom commun ".

3.9.4 Déploiement de serveur web (IIS)

Nous installons d'abord le serveur web sur notre machine virtuelle, pour cela il suffit d'installer le rôle " Serveur Web (IIS) ".

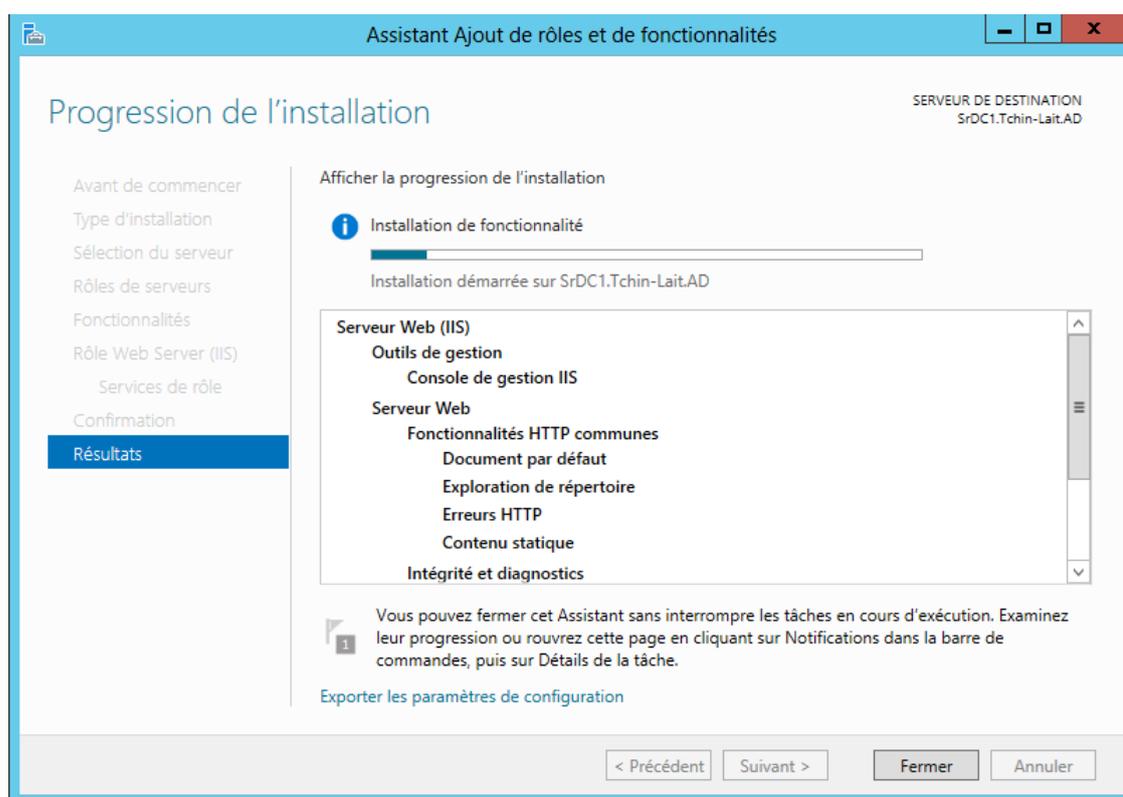


FIGURE 3.30 – Installation de Serveur Web (IIS).

En suite dans l'interface " gestionnaire de serveur ", où les développeurs peuvent faire des développements, des créations des pages web. . .etc. On peut sélectionner le site qu'on souhaite utiliser. Dans notre cas, ce sera celui par défaut.

Puis dans la colonne de droite sélectionner " Liaison " pour ajouter une liaison de site.

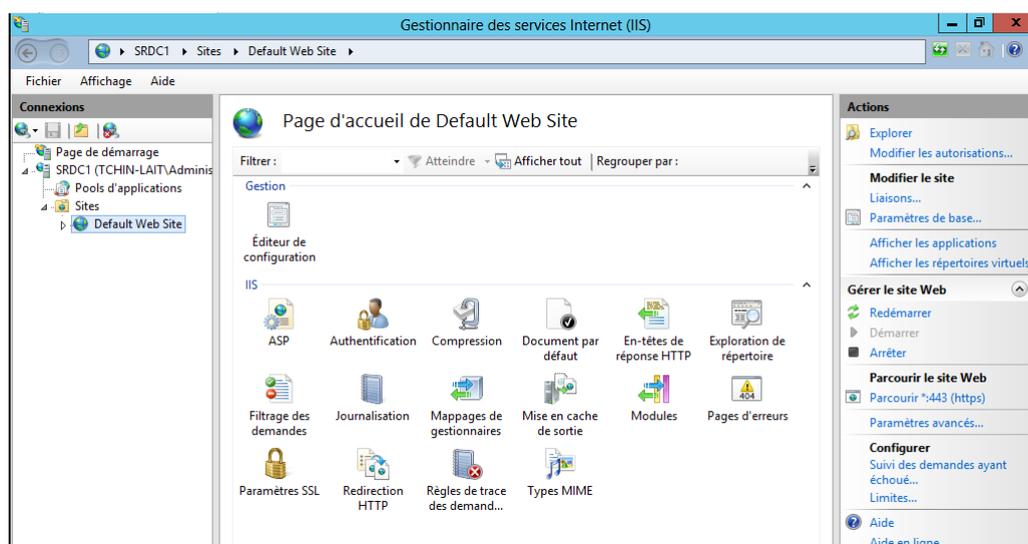


FIGURE 3.31 – Sécuriser le serveur web avec un certificat.

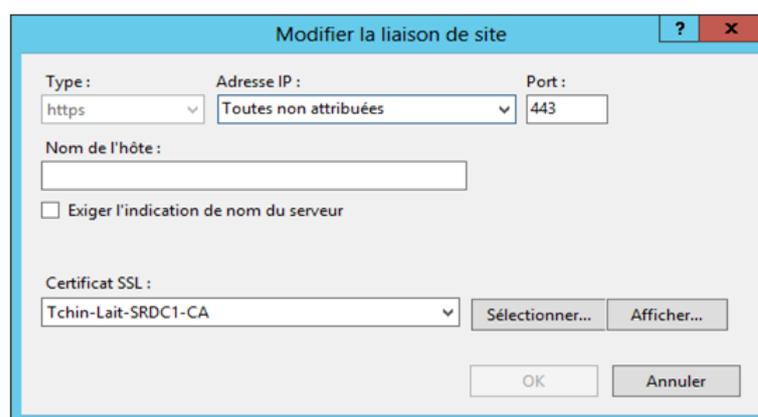


FIGURE 3.32 – Ajout d'une liaison de site.

3.9.5 Distribution du certificats aux clients de l'Active Directory

Etant donné que nous avons créé un Active Directory sur notre serveur, nous pouvons modifier les stratégies de groupe pour que nos clients reçoivent le certificat de notre autorité de certification. Ainsi, nos clients peuvent accéder à notre intranet (site Web accessible uniquement sur un réseau interne) de façon sécurisée et sans avoir d'avertissement concernant le certificat.

Dans la fenêtre "Gestion de stratégie de groupe", aller à Autorité de certification racines de confiance, effectuer un clic droit et choisir "importer".

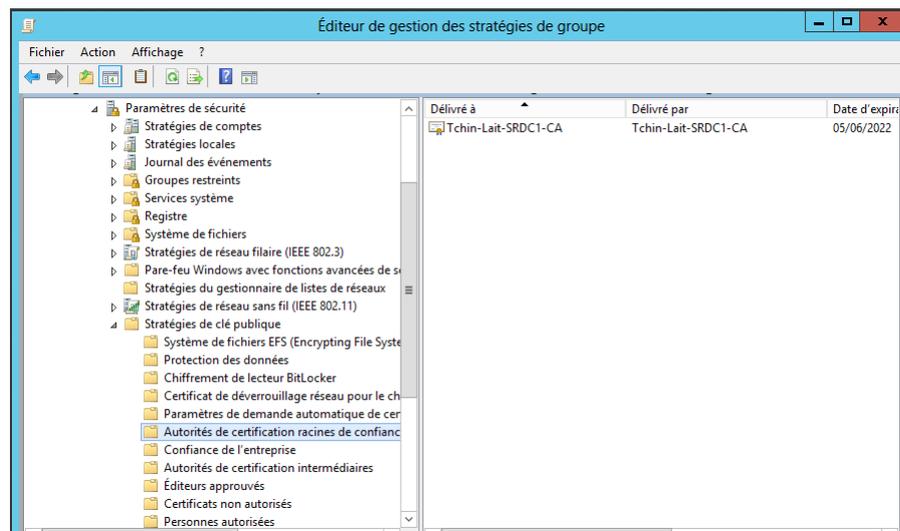


FIGURE 3.33 – Distribution du certificat de l'autorité aux utilisateurs d'Active Directory.

3.10 Configuration de BranchCache

La fonctionnalité de mise en cache des fichiers dans les succursales (BranchCache) favorise la vitesse d'exécution des applications locales en optimisant les besoins en bande passante des bureaux distants.

Les fichiers téléchargés par les utilisateurs distants depuis un serveur de fichier ou depuis un serveur Web intranet situés à l'office central sont mis en cache localement. Ainsi lorsqu'un autre utilisateur tente d'accéder au même fichier, celui-ci n'a pas à attendre le temps de téléchargement pour pouvoir travailler sur le fichier, il récupère automatiquement la copie locale.

En premier lieu, la fonctionnalité BranchCache doit être installée sur les serveurs partageant des ressources. Dans l'assistant Ajout de rôles et de fonctionnalités, on sélectionne le rôle BranchCache pour fichiers réseau dans Services de fichiers et de stockages, Services de fichiers et iSCSI.

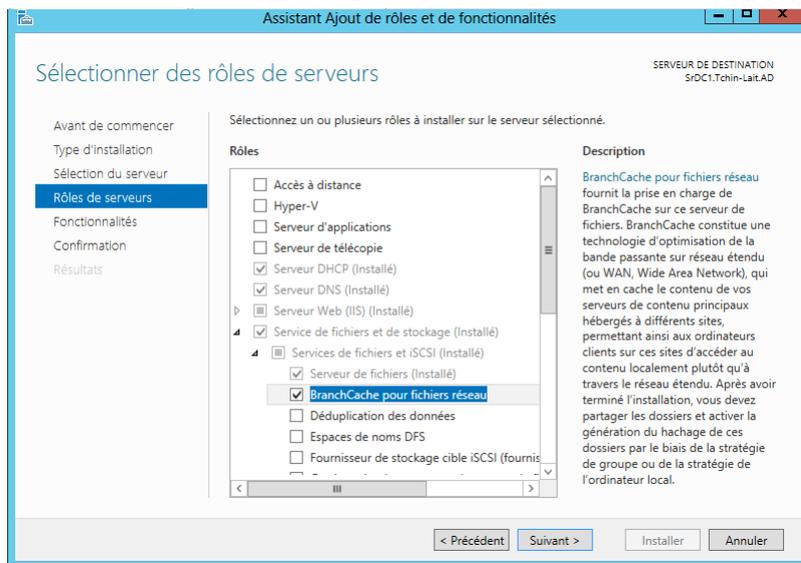


FIGURE 3.34 – Ajout de fonctionnalité de BranchCache.

L'opération suivante consiste à permettre au serveur d'utiliser les fonctions de type Hash Coding, ce qui a pour but de permettre l'identification de chaque fichier de manière unique et de détecter les modifications. Pour cela : On ouvre L'éditeur de stratégies de groupe local, et l'on se rend dans Configuration ordinateur ,Modèles d'administration ,Réseau.

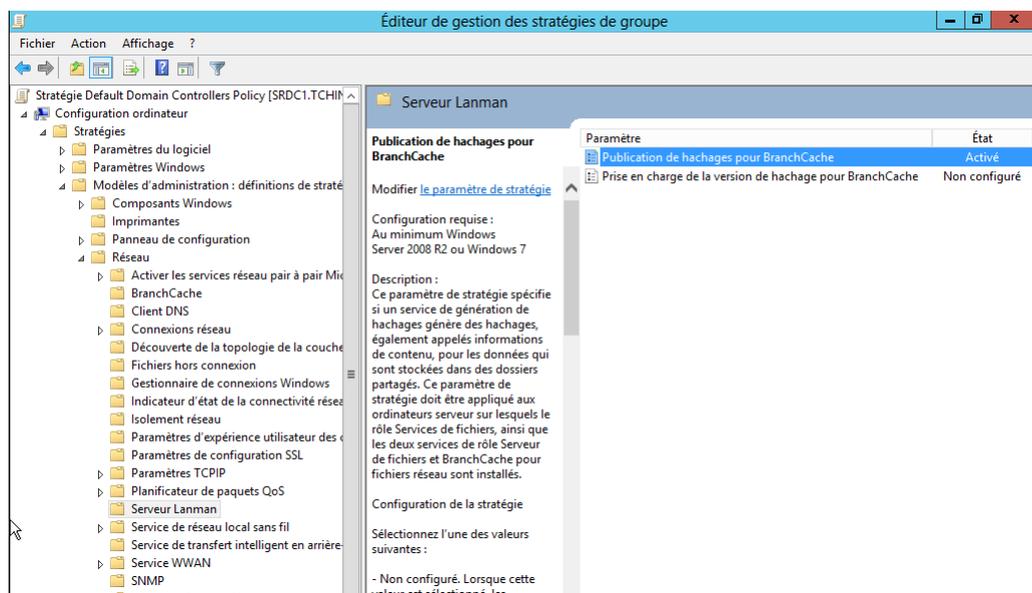


FIGURE 3.35 – Activer la publication de hachage pour BranchCache.

Il suffit de valider la configuration du paramètre. Ensuite, actualiser la stratégie de groupe sur le serveur en forçant son activation avec la commande GPUpdate / Force sur PowerShell.

Par la suite, on configure les partages sur lesquels BranchCache sera actif. On se rend pour cela dans l'onglet Partage des propriétés du dossier partagé

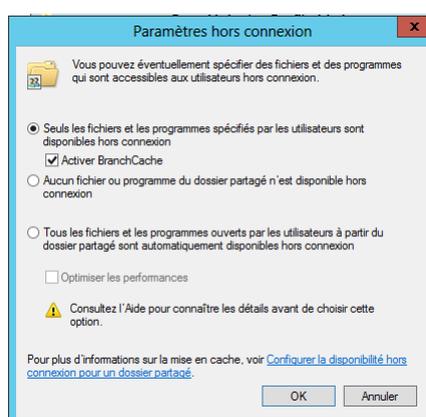


FIGURE 3.36 – Activer BranchCache sur un partage.

Enfin, il est nécessaire de configurer les postes clients pour qu'ils puissent tirer parti de BranchCache. Pour cela, nous allons configurer les postes clients grâce aux GPO :

- Tout d'abord, on ouvre la Console de gestion des stratégies de groupe.
- On crée une nouvelle stratégie nommée ici Windows BranchCache.
- On clique droit sur la stratégie créée, puis l'on choisit Modifier.
- On déroule Configuration ordinateur puis Stratégies ensuite Modèles d'administration après Réseau, puis l'on sélectionne le paramètre BranchCache.

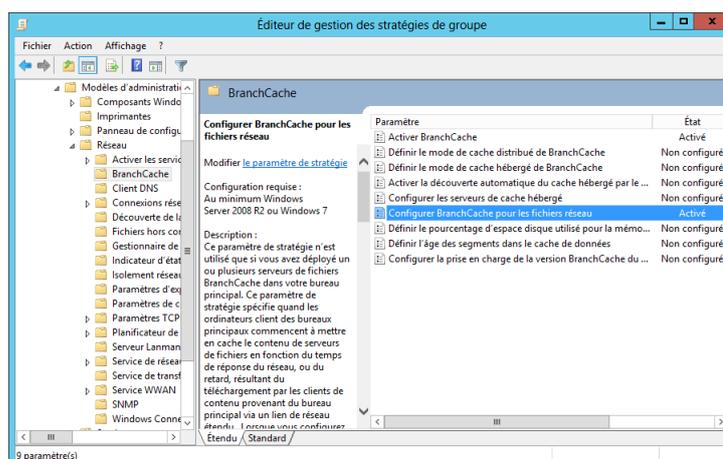


FIGURE 3.37 – Configuration du client BranchCache.

Nous ouvrons le paramètre Activer BranchCache puis l'on sélectionne " Activer ".

Enfin, pour que le client soit capable d'utiliser BranchCache afin de récupérer des fichiers provenant le serveur de fichier, nous sélectionnons le paramètre Configurer BranchCache pour les fichiers réseau, que l'on active.

3.11 Mise en œuvre d'une solution de sauvegarde " Backup "

Pour installer le service de sauvegarde il faut passer par le gestionnaire de serveur et choisir l'option " Sauvegarde de Windows Server " dans la rubrique fonctionnalités.

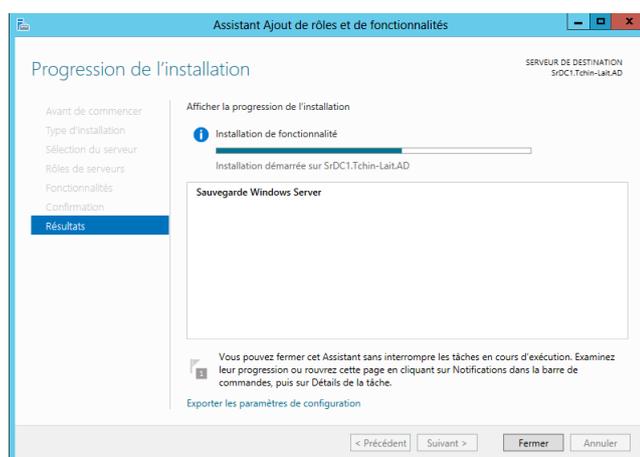


FIGURE 3.38 – Installation du service de sauvegarde.

Une fois installée, nous allons démarrer la mmc " Sauvegarde de Windows Server " depuis " outils d'administration " puis désigner " Planification de sauvegarde " .

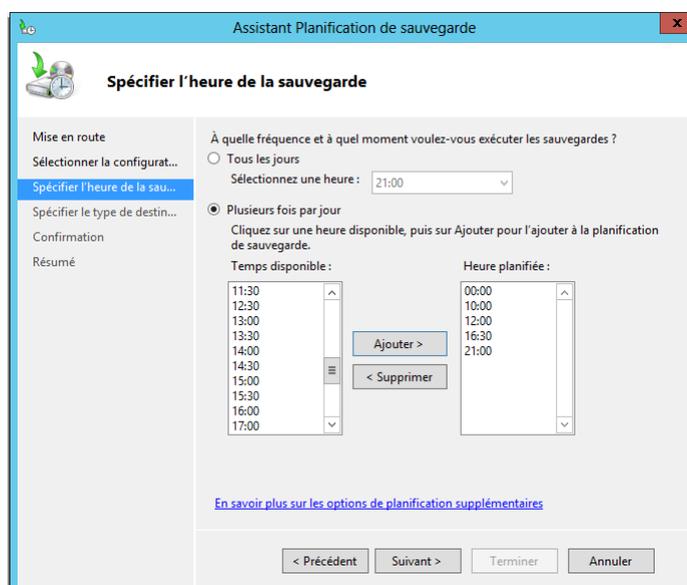


FIGURE 3.39 – Spécifier l'heure de la sauvegarde.

Nous devons spécifier le type de support à disposition. Nous choisissons de sauvegarder les données du serveur principal sur un autre disque.

Nous remarquons qu'une fois la tâche terminée le serveur lance une première sauvegarde qui a été réussite.

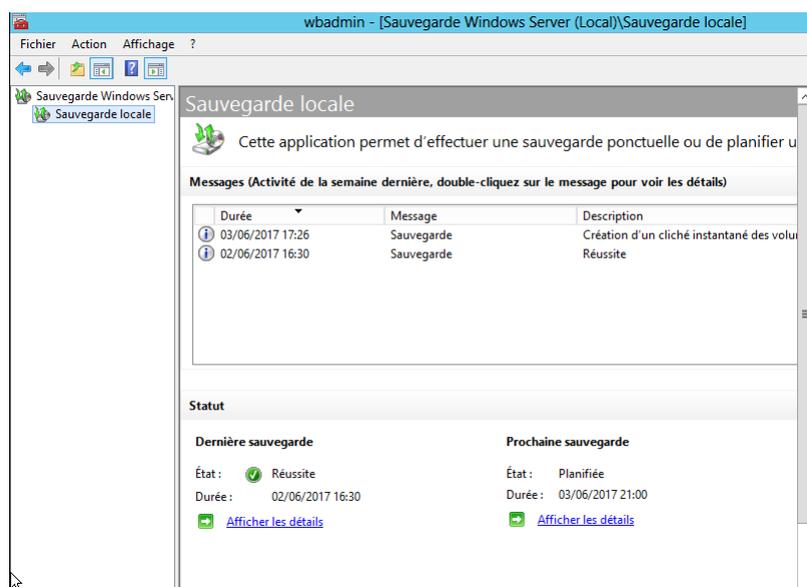


FIGURE 3.40 – Résultat de la sauvegarde.

3.12 Conclusion

La réalisation de ce chapitre nous a permis de découvrir l'environnement de Windows Server 2012 et de se familiariser avec ses différents composants et services. Premièrement en termes de fonctionnalités à savoir l'organisation des ressources de l'entreprise que ce soit humaines ou matérielles en utilisant l'AD. Deuxièmement, en termes de sécurité, que ce soit par la définition des stratégies de groupe ou par l'infrastructure PKI qui offre aux utilisateurs du domaine la possibilité de chiffrement et de signature à l'aide des certificats. Troisièmement, en termes de gestion d'adressage dynamique qui se fait grâce au serveur DHCP.

Conclusion générale

La réalisation de ce travail de fin du cycle, nous a permis d'améliorer nos connaissances et nos compétences dans le monde des réseaux sur le plan administration, qui a pour objectifs la mise en place d'une infrastructure réseau sous Windows server 2012.

Ainsi dans le cadre de ce travail, nous sommes amenés à appliquer les notions et les différents concepts retenus en réseaux et en Windows server 2012.

En effet, le réseau informatique permet aux entreprises de centraliser ses données, de travailler en équipe de manière productive et limiter les impressions papiers pour le transfert d'informations. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données. Le travail présenté nous a permis :

- Décrire d'une manière générale les réseaux informatiques.
- Le déploiement d'un contrôleur de domaine AD DS qui permet de gérer les utilisateurs et les ressources.
- Les services de fichiers avancés à savoir le BranchCache.

Nous avons proposé également, la solution de sauvegarde de reprise après sinistre (BackUp).

perspective

Implémentation d'une solution VPN et VLAN afin d'améliorer la sécurité du réseau de l'entreprise.

Bibliographie

- [1] VAIRA T. "Cours Réseaux - Adressage IP", Frères des écoles chrétienne, Avignon, 2012
- [2] Claude Servin "Réseaux et télécoms", Chargé de cours au CNAM de Paris et en écoles d'ingénieur Ancien responsable télécom au ministère de la Défense, 2003
- [3] G.PUJOLLE " les réseaux ", livre, paris, 8 eme édition 2014.
- [4] DOUKOE D. "Mise en place d'un réseau local avec connexion internet", BTS télécommunication, Centre d'enseignement supérieure des technologies internationales d'Abijan, 2007.
- [5] wiliam R .stanek guide de l'administrateur windows server 2012
- [6] Guillaume Mathieu "Tester la sécurité de son annuaire Active Directory V2 ", version du 30/01/2016.
- [7] B. DESMOND "Designing, deploying and running Active Directory", 5 eme edition O'reilly, 2013.

Webographie

- [8] <https://www.supinfo.com/articles/single/2039-active-directory>
- [9] <http://protocole-tcpip.over-blog.com/article-le-protocole-tcp-ip-definition-69189059.html>
- [10] <https://www.manzainfo.fr/index.php/microsoft/windows-serveur-2012/36-creer-un-controleur-de-domaine-sous-windows-serveur-2012>
- [11] <http://www.commentcamarche.net/contents/1-active-directory>
- [12] <https://www.it-connect.fr/chapitres/un-annuaire-active-directory-pourquoi/>

Résumé

De nos jours et avec l'usage des réseaux locaux et d'internet, les entreprises ont toutes adopté un mode de présence sur la toile.

Le meilleur moyen d'être présent ne serait pas d'avoir uniquement une communication interne sur le réseau ou de disposer d'une connexion internet, mais d'avoir une bonne plateforme informatique répondant aux nouveaux besoins.

Ce projet concerne l'étude du réseau informatique de l'entreprise Candia(Tchin-Lait) ou nous avons pu installer et configurer des différents services de windows serveur 2012 relatifs au bon fonctionnement de la plateforme de l'entreprise candia à savoir DNS,DHCP,PKI et les services de fichiers.

Mots clés :Windows Serveur 2012,Active Directory,Domaine,Infrastructure PKI, Partage,Sauvegarde.

Abstract

Nowadays and with the use of local networks and internet, companies have all adopted a mode of presence on the web.

The perfect way to be present would not only have an internal communication over the network or have an internet connection, but to have a good IT platform responding to new needs.

This project concerns the study of computer network Candia(Tchin-Lait) company where we were able to install and configure of various services related in windows server 2012 to the proper functioning Candia platform namely DNS, DHCP, PKI and file services.

Keys words :Windows Server 2012,Active Directory,Domaine,PKI, Sharing, Backup.