République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences exactes
Département d'Informatique

Mémoire de Fin de cycle

En vue de l'obtention du diplôme de

Master en Informatique

Option

Administration et sécurité des réseaux

Thème :

Tolérance aux pannes des serveurs cas THCIN-LAIT

Réalisé par :
HADDAD Jugourta
TOUATI Badreddine

Devant le jury composé de :

Président :	M. ACHEROUFENE Achour
Encadreur :	M.SIDER Abderrahmane
Examinatrice :	Mlle. HAMZA Lamia

Année universitaire 2013-2014

Table des matières

Table des figures

Liste des tableaux

Abréviation

ARPANET : Advanced Research Projects Agency Network

BLR : Boucle locale radio

CIDR : Classless Inter Domain Routing

D.G : Direction Générale

DMZ : DeMililtarized Zone

DNAT : Destination Network Adress Translation

ERP : Enterprise Resource Planning

F.O : fibre optique

FTP : File Transfer Protocol

GPRS : General Packet Radio Service

GSM : Global System Mobile

HA : High Availability

Http : Hyper Text Transfer Protocol

IDS : Intrusion Detection System

IEEE : Institute of Electrical and Electronics Engineers

IETF : Internet Engineering Task Force

IIS : Internet Information Services

Internet : international network

IP : Internet Protocol

IPSec : Internet Protocol Security

ISO : International Standardization Organisation

LAN : Local Area Network

L2TP : Layer 2 Tunneling Protocol

MAC : Media Access Control

MAN : Metropolitan Area Network

NAT : Network Adress Translation

OSI : Open Systems Interconnection

PDA : Personal digital assistant

PME : Petite ou Moyenne Entreprise

POE : Power over Ethernet

PPTP : Point-to-Point Tunneling Protocol

RAID : Redundant Array of Inexpensive Disks

RJ45 : Registered Jack 45

SLC : Smart Link Communication

SMTP : Simple Mail Transfer Protocol

SNAT : Source Network Adress Translation

TCP : Transport Control Protocol

TS : Terminal Server

UHT : Ultra Haute Température

UMTS : Universal Mobile Telecommunication System

VLAN : Virtual Local Area Network

VPN : Virtual Private Network

WAN : Wide Area Network

WDS : Wireless Distribution System

WiMax : Worldwide Interoperability for Microwave Access

WI-FI : Wireless Fidelity

WLAN : Wireless Local Area Network

WMAN : Wireless Metropolitan Area Network

WPAN : Wireless Personal Area Network

Introduction générale

l'univers des systèmes informatiques composé de réseaux, de données et d'applications prend un rôle et une place chaque jour plus important dans les entreprises. Ces systemes doivent répondre aux niveau de continuité operationellé fixé par les besoins de chaque entreprise, en utilisant differentes solutions entre autre celles qui permettent une plus grande tolerence aux pannes.

Le domaine des télécommunications et des réseaux est en plein effervescence. En effet, chaque laps de temps qui s'écoule apporte sa moisson ; de nouvelles offres technologiques et des méthodes de plus en plus adéquates. Confronté à ce flux incessant de nouveautés, le praticien doit faire des choix qui s'avéreront décisifs pour l'entreprise, structurant ainsi de manière stratégiques l'avenir de son système d'information. Ces choix conforteront l'entreprise en termes de compétitivité, de gain de temps et d'argent.

Il est important que nous disposions de bases solides et récentes dans le domaine de la sécurité des systèmes d'information. Cela nous permettra d'évaluer judicieusement la pertinence des solutions proposées par les constructeurs de matériels et les éditeurs de logiciels.

C'est pour cela que nous avons opté pour la mise en place d'une solution avec tolérance aux pannes pour l'entreprise TCHIN-LAIT " CANDIA " qui se trouve être l'un des leaders incontournable dans la production de lait UHT en Algérie.

Le premier chapitre sera consacré à une partie fondamentale qui n'est autre que la sécurité informatique dans les réseaux d'entreprise, en termes de menace ainsi que les multiples technologies et outils avec les quels nous pouvons y remédier, et plus précisément au critère de disponibilité dans le réseau et le système d'information.

Par la suite, nous nous intéresserons dans le deuxième chapitre, à la description de l'environnement de notre travail, en outre, notre organisme d'accueil qui est TCHIN LAIT " CANDIA " et nous nous étalerons sur l'étude de son réseau informatique, D'où nous tirerons une problématique .

Enfin, dans le dernier chapitre nous dresserons une solution afin de répondre aux exigences de continuité opérationnelle fixée par l'entreprise. Notre principal objectif portera sur la mise en œuvre d'une simulation de la solution d'équilibrage de charge basée sur deux Terminal Server avec basculement que nous avons recommandé. L'exécution de la solution se fera dans un environnement virtuel sur VmWare sous Windows Serveur 2008.

Chapitre 1

Sécurité des réseaux

1.1 Introduction

L'univers des systèmes d'information composé de réseaux et des systèmes informatiques prend un rôle et une place chaque jour plus important dans l'univers des entreprises.

Cependant, la réalité du terrain nous démontre que le système d'information est vulnérable et qu'il peut subir des piratages, des attaques, des pertes de données, des dysfonctionnements, voir des sinistres. Il est donc indispensable pour les entreprises de savoir définir et de garantir la sécurité et la disponibilité de ses ressources informatiques.

1.2 Réseau informatique

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons et dont le but est d'échanger des informations ou des biens matériels, par contre, le réseau informatique, c'est l'ensemble des ressources de communication (matérielles et logicielles), d'ordinateurs et des clients cherchant à exploiter ces ressources afin de répondre à un besoin d'échange d'information [**B2**].

Types de réseaux

1. **Réseau local (LAN)** Le réseau local (LAN, Local Area Network) désigne un réseau habituellement privé dont la taille est limitée à quelques kilomètres. Le débit est généralement compris entre 1 Mbit/s et 100 Gbit/s. ce sont par exemple réseaux

Ethernet ou Wifi[**B2**].

2. **Réseau métropolitain (MAN)** Le réseau métropolitain (MAN, Metropolitan Area Network) est un réseau privé ou publique, de la taille d'une ville ou d'un campus, utilisé pour interconnecter des LAN. Les débits sur ces réseaux sont en général inferieur à 10 Gbit/s [**B2**].

3. **Réseau étendu (WAN)** Le réseau étendu (WAN,Wide Area Network), encore appelé réseau longue distance, peut s'étendre a l'échelle d'un pays ou d'un continent. Son débit peut atteindre 40 Gbit/s [**B2**].

1.3 Les réseaux informatique sans fil

Un réseau sans fil (en anglais wireless network) est comme son nom l'indique, un réseau dans lequel au moins deux périphériques (ordinateur, PDA, imprimante, routeur, etc.) peuvent communiquer sans liaison filaire [**B2**].

Les réseaux sans fil ont recours à des ondes radioélectriques (radio et infrarouge) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions, comme nous le verrons ci-dessous.

Types de réseaux sans fil

Les réseaux sans fil appartiennent à plusieurs catégories, régies par des normes spécifiques :

1. **Les réseaux WLAN (Wireless Local Area Network) ou Wifi**

   Obéissent aux normes de la famille IEEE 802.11, dont la première édition date de1997 ; ils sont destinés à faire communiquer des équipements séparés par une distance de l'ordre de quelques dizaines de mètres, par exemple dans un immeuble ; les dispositifs d'émission et de réception de ces appareils ont une puissance maximale de 100 mW (à comparer

avec celle d'un téléphone portable GSM, qui est de 1 W) [**B2**].

2. **Les réseaux WPAN (Wireless Personal Area Network) ou Bluetooth**

   Obéissent à la norme IEEE 802.15.1 ; ils permettent des communications entre des appareils distants de quelques mètres, par exemple un téléphone et son oreillette sans fil ; les promoteurs de cette norme l'ont déjà déployée pour les assistants personnels (PDA) et ils envisagent des débouchés sur le marché du jouet et des consoles de jeu ; la puissance des émetteurs est plus faible que pour les appareils 802.11, en général 1 mW (il existe bien une option de la norme qui permet une puissance de 100 mW, mais elle n'est pratiquement pas utilisée), et de ce fait la consommation électrique est moindre ; la norme IEEE 802.15.3 (Bluetooth2) est une évolution de la norme Bluetooth avec des débits plus rapides et des mécanismes de sécurité améliorés par rapport à 802.15.1 [**B2**].

3. **Les réseaux WMAN (Wireless Metropolitan Area Network)**

   Obéissent à la norme 802.16, plus connue sous le nom de WiMax, ou de Boucle locale radio (BLR) ; ils sont capables de relier des équipements distants de quelques kilomètres, par exemple pour se substituer aux liaisons ADSL dans les zones rurales à faible densité [**B2**].

4. **Les réseaux WWAN (Wireless Wide Area Network)**

   Utilisent les systèmes de téléphonie sans fil tels que GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service) ou UMTS (UniversalMobile Telecommunication System) comme couche de liaison de données pour constituer une infrastructure d'accès à l'Internet [**B2**].

1.4 Sécurité informatique

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques [**B3**].

1.5 Les normes associées à la sécurité

1.5.1 La norme ISO 20000

Cette norme décomposé en ISO 2000-1, ISO 2000-2, s'appuie sur les bonnes pratiques ITIL (Information Technology Infrastructure Library) et comprend un ensemble de bonnes pratiques en matière de gestion des services informatiques. Elle prend comme principe la roue de Deming ou PDCA (Plan-Do-Check-Act) et s'inscrit dans un processus de formalisation de normes de qualité (ISO9000) ou de sécurité des systèmes d'information (ISO 27001).

Il s'agit d'un système de gestion complémentaire avec une architecture identique composé d'un guide de bonnes pratiques (ISO 20000-2). Ce système complète la norme ISO 20000-1 [**B6**].

1.5.2 Les normes ISO 2700x

La norme ISO 27001

Elle s'est imposée comme référence en matière de sécurité des systèmes d'information, principalement pour la mise en œuvre d'un Système de Gestion de la Sécurité de l'information (ISO 27005). Elle peut être considérée comme la transposition en sécurité informatique de la démarche qualité ISO 9001.
La série des normes ISO 27 00x est actuellement et sera composée des éléments suivants [**B6**] :

1. **ISO/IEC 27000 :2009** : Fournit une présentation et une introduction aux normes ISO 27000 et définit le vocabulaire spécifique utilisé sur tous l'ensemble des normes.

2. **ISO/IEC 27001 :2005** : Norme principale de définition des besoins pour le SMSI (Système de Management de la Sécurité de l'information). Elle correspond au principe de certification des organisations.

3. **ISO/IEC 27002 :2005** : Il s'agit de la description des bonnes pratiques décrivant un ensemble compréhensible d'objectifs de contrôle de sécurité et un ensemble de bonnes pratiques de contrôles de sécurité généralement acceptés.

4. **ISO/IEC 27003 :2010** : Comprend le guide d'implémentation détaillé relatif à l'adoption de la série complète de la norme ISO27001.

5. **ISO/IEC 27004 :2009** : Contient la norme qui définit les principes d'évaluation et de mesure de ce qui a été implémenté dans le cadre du système de mangement de la sécurité de l'information pour mesurer l'efficacité du système de gestion de la sécurité mis en place.

6. **ISO/IEC 27005 :2011** : Contient la norme de gestion du risque de sécurité de l'information comprenant des conseils sur la sélection des analyses de risque appropriées, les méthodes et outils de gestion.

7. **ISO/IEC 27006 :2011** : Guide décrivant les exigences pour les organismes procédant à l'audit et à la certification des systèmes de mangement de la sécurité de l'information qui ont réussi la certification ISO/IEC 27001.

8. **ISO/IEC 27007 :2011** : Cette norme proposera des instructions pour les audits accrédités en cas d'audit ISO/IEC 27001 d'un SMSI. Statut : non publié.

9. **ISO/IEC TR 27008 :2011** : Cette norme propose un guide sur le contrôle de sécurité d'audit de l'information. Il est prévu qu'elle se focalise sur ces contrôles.

10. **ISO/IEC 27010 :2012** : Cette norme multipartie propose un guide sur le mangement de sécurité de l'information pour le secteur des communications.

11. **ISO/IEC 27011 :2008** : Guide pour la gestion de la sécurité de l'information dans le secteur des télécommunications (aussi connu comme ITU X.1051).

12. **ISO/IEC 27013 :2012** : Guide pour l'intégration de l'implémentation entre ISO/IEC 20000 :1 (IT Service Management) et ISO/IEC 27001 (SMSI), pour le secteur de l'industrie.

13. **ISO/IEC 27014** : Cette norme va couvrir la gouvernance de sécurité de l'information. Statut : non publié.

14. **ISO/IEC 27015** : Cette norme sera un guide système de management de la sécurité de l'information pour l'accréditation des services financiers dans les organisations. Statut : proposé.

15. **ISO/IEC 27031 :2011** : Cette norme se focalise sur la continuité d'activité dans les systèmes d'informations.

16. **ISO/IEC 27032 :2012** : Cette norme propose un guide sur la cyber-sécurité [**B6**].

1.6 Les menaces et leurs impacts

Les systèmes d'information sont vulnérables par rapport à plusieurs menaces susceptibles de leur infliger différents types de dommages et des pertes significatives.
L'importance des dégâts peut s'échelonner de la simple altération de données à la destruction complète du centre de données informatiques.
Les impacts des différentes menaces varient considérablement suivant les conséquences affectant l'entreprise, certaines affectent la confidentialité ou l'intégrité des données, d'autres agissent sur la disponibilité des systèmes.
La valeur réelle des pertes relatives au manque de sécurité n'est pas toujours possible à estimer car beaucoup d'entre elles ne sont jamais découvertes, d'autres peuvent être délibérément ignorées pour éviter de montrer une mauvaise image de l'entreprise.

1.7 Technologies ou dispositifs de sécurité utilisées dans les réseaux

1.7.1 Les pare-feu

Il consiste à protéger le réseau de l'entreprise des intrusions extérieures [**B3**]. Ces dispositifs filtrent les trames (contenant des données) des différents couches du modèle TCP/IP afin de contrôler leur flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes.

Le filtrage réalisé par le pare-feu constitue le premier rempart de la protection du système d'information. Il peut être composé de périphériques comportant des filtres intégrés dont la fonction principale est de limiter et de contrôler le flux de trafic entre les parties de réseaux.

Ils permettent l'accès de l'entreprise aux ressources externes en contrôlant la sécurité des transferts .

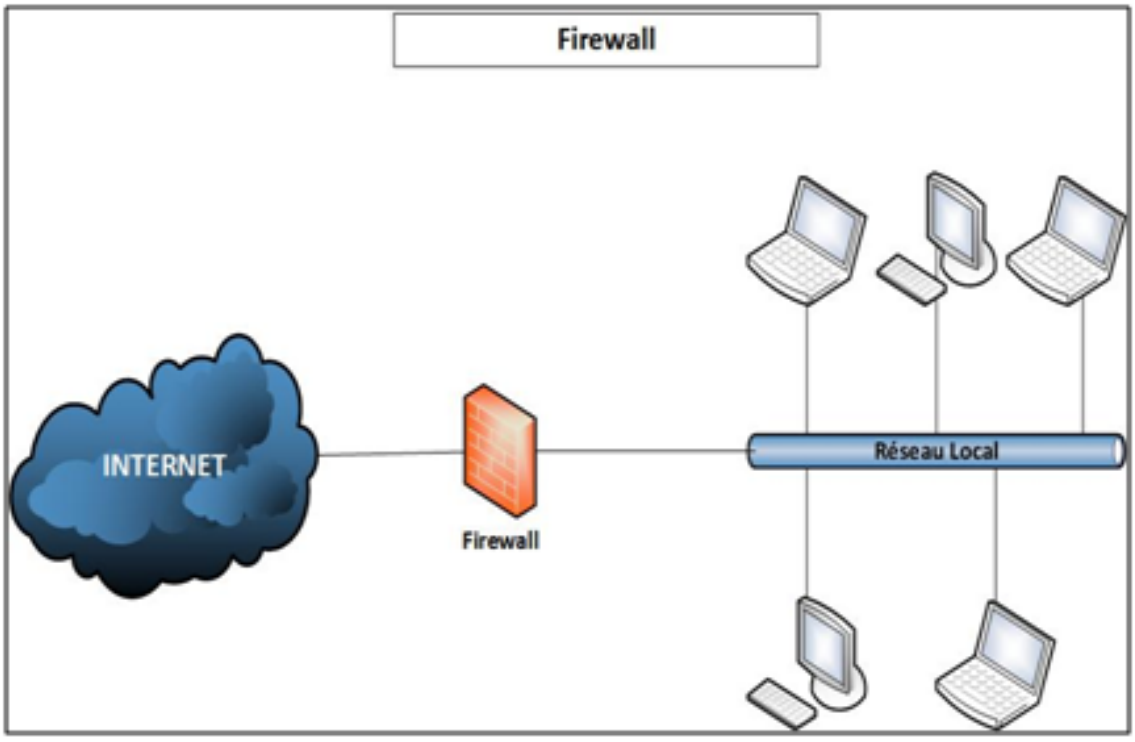

FIGURE 1.1 – Firewall

1.7.2 Le NAT (Network Adress Translation)

La translation d'adresse ou NAT est aussi un dispositif de sécurité complémentaire au filtrage dans la mesure où elle masque les adresses privées qui ne sont par conséquent plus visibles de l'extérieur[**B3**].

Les firewalls étant généralement intégrés aux routeurs qui possèdent de plus des fonctionnalités de translation, il est nécessaire pour la compréhension des règles de routage et de filtrage de savoir dans quel ordre sont effectuées ces différentes opérations.

Pour un paquet entrant, la translation concerne l'adresse destination (celle qui est masquée) ; cette opération est nommée DNAT (Destination NAT). Il est nécessaire que la translation soit réalisée avant le processus de routage puisque le routeur doit connaître l'adresse interne pour prendre sa décision.

Pour un paquet sortant, la translation concerne l'adresse source (celle qui doit être masquée) ; cette opération est nommée SNAT (Source NAT). Dans ce cas, le filtrage est d'abord effectué pour savoir si le paquet est autorisé à sortir. La translation est ensuite réalisée après le processus de routage, en sortie du routeur .

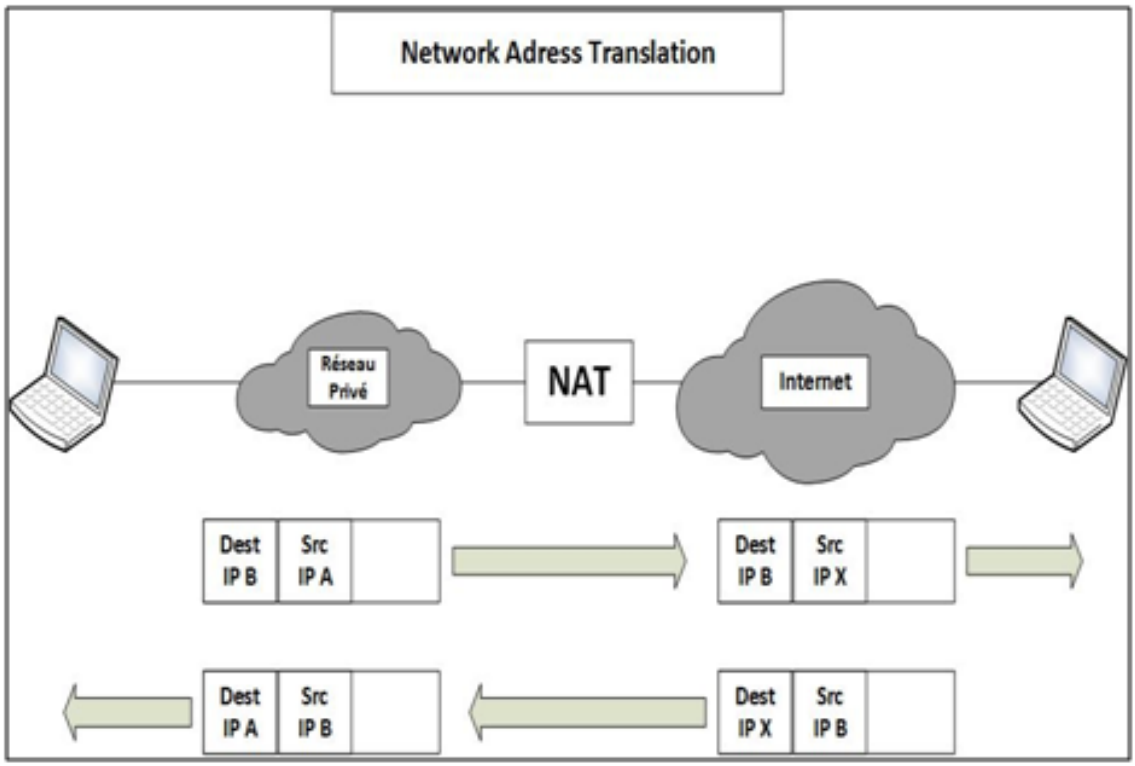

FIGURE 1.2 – Network Adress Translation

1.7.3 Les VPN (Virtual Private Network)

La connexion à distance sur un réseau interne d'une PME impose d'utiliser un réseau privé virtuel d'entreprise (VPN). Cette fonctionnalité chiffre le trafic réseau sensible et requiert une authentification forte, fournissant un accès à distance sécurisé [**B3**].

Le trafic VPN est chiffré pour garantir la confidentialité des transferts de données pendant la durée de la connexion. Le principe du VPN consiste à établir un chemin virtuel unique avec l'identification de l'émetteur et du récepteur. Ce chemin est aussi appelé tunnel.

Le VPN établit une connexion sécurisé vers un réseau à distance en utilisant la technique de tunnelling à travers Internet. Cette technique consiste en l'encapsulation, la transmission, la désencapsulation d'un paquet de données sous forme de message à l'intérieur d'un paquet IP. Le transfert de ces données est réalisé à travers Internet.

Il existe différents protocoles pour le tunneling à travers internet :

- Internet Protocol Security (IPSec).
- Layer 2 Tunneling Protocol (L2TP).
- Point-to-Point Tunneling Protocol (PPTP).
- Secure Socket Layer/Transport Security Layer (SSL/TSL).

Le protocole IPSec vise à sécuriser l'échange de données au niveau de la couche réseau. D'autres protocoles associés comprennent les protocoles PPTP et L2TP.

Le protocole SSL est utilisé depuis peu dans la fonctionnalité des VPN, il est incorporé entre les couches Application et Transport. Il permet l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant le transfert .

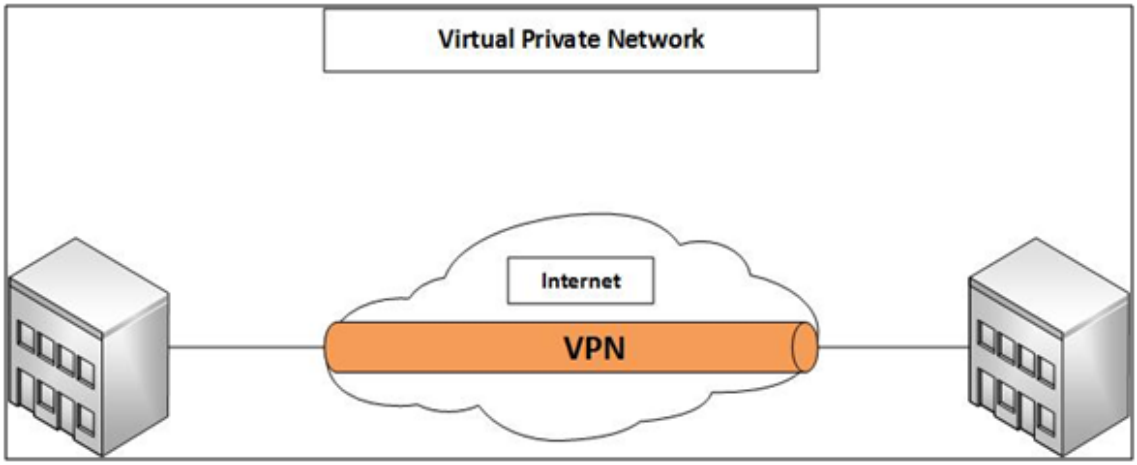

FIGURE 1.3 – Virtual Private Network

1.7.4 Les VLAN (Virtual Local Area Network)

Beaucoup d'utilisateurs sont aujourd'hui mobiles et la situation géographique d'un utilisateur n'a pas forcement de lien avec son appartenance logique : deux collaborateurs situés aux deux extrémités de l'entreprise peuvent souhaiter appartenir au même domaine de diffusion, donc au même LAN qui devient ainsi virtuel car il n'a plus de réalité géographique [**B3**].
Un VLAN redéfinit les domaines de diffusion de manière à regrouper les utilisateurs de manière logique ou à économiser la bande passante, améliorer la confidentialité des données et faciliter la gestion de la mobilité. Il est implémenté sur un commutateur ou Switch et réalise un domaine " logique " de diffusion.
Les VLAN peuvent être construits à l'image de l'organisation de l'entreprise.
Il existe trois types de VLAN :

1. **VLAN de niveau 1** Dans un vlan de niveau 1, aussi appelé VLAN par port, l'appartenance d'une machine à un VLAN est définis par le port auquel elle est connectée.

2. **VLAN de niveau 2** Les VLAN de niveau 2 sont aussi nommés VLAN par adresse MAC. Dans cette méthode, l'adresse MAC d'une machine est affecté à un VLAN. En pratique, c'est encore le port qui est affecté à un VLAN, mais de manière dynamique.

3. **VLAN de niveau 3** Dans ce VLAN, aussi nommé VLAN par sous-réseau, l'adresse IP est affectée à un VLAN .

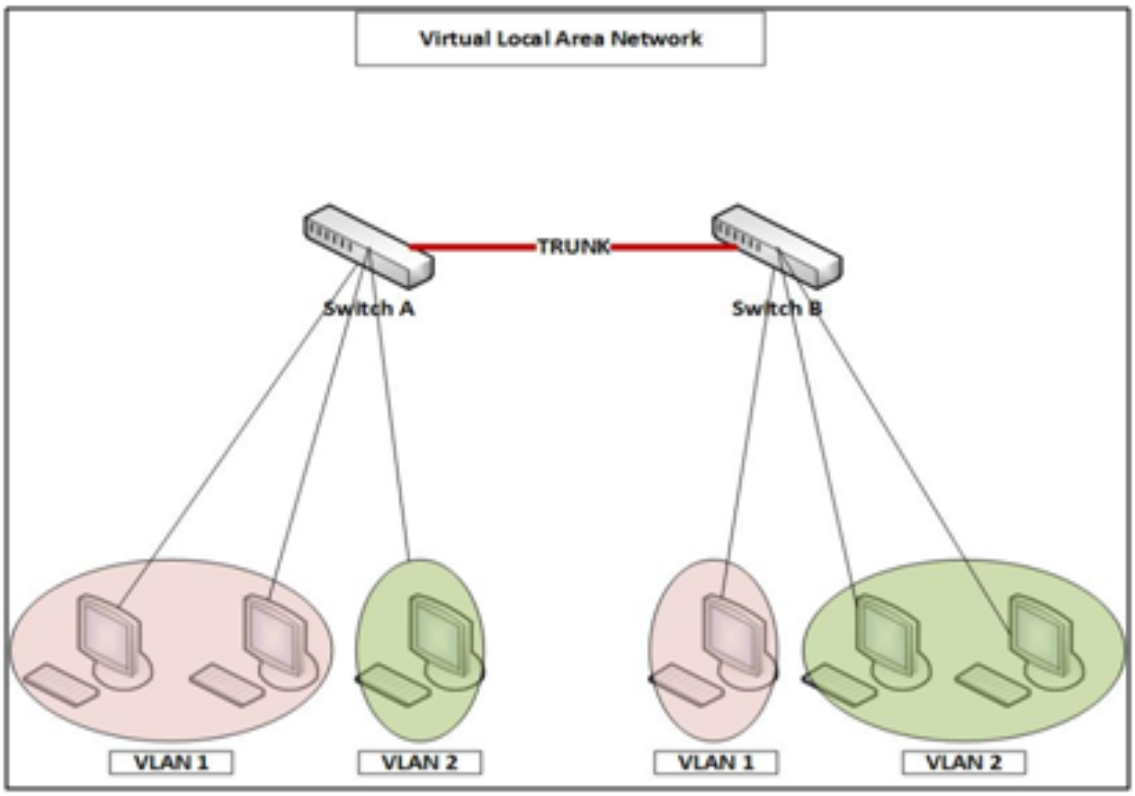

FIGURE 1.4 – Virtual Local Area Network

1.7.5 Les proxys

Un système mandataire (Proxy) repose sur un accès à l'internet par une machine dédié : le serveur mandataire ou Proxy server, qui joue le rôle de mandataire pour les autres machines locales et exécute les requêtes pour le compte de ces dernières [**B3**].

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP ...) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients ...).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés (proxy cache) .

1.7.6 DMZ (DeMilitarized Zone)

Une zone démilitarisée (ou DMZ, DeMililtarized Zone) est une zone de réseau privée ne faisant partie ni du réseau local privé ni de l'Internet [**B3**]. A la manière d'une zone franche au-delà de la frontière, la DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes.
Un niveau supplémentaire de sécurité peut être introduit avec un deuxième firewall. Les règles d'accès sur le firewall du réseau local privé sont plus restrictives. La DMZ est située entre les deux firewalls (DMZ " en sandwich ") avec des règles moins restrictives introduites par le premier firewall .

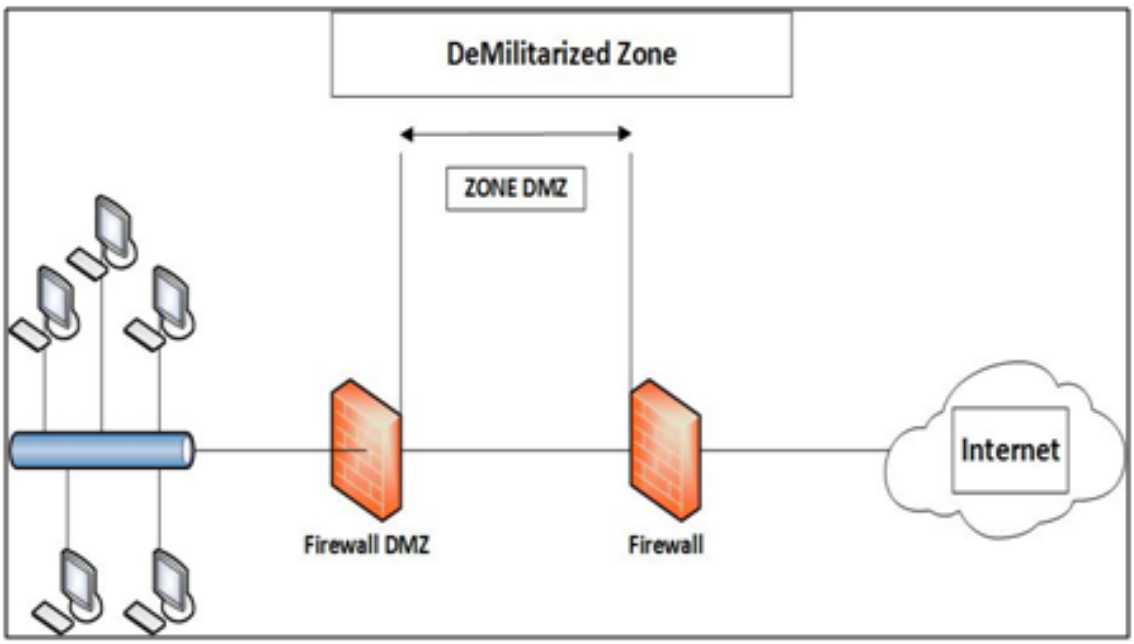

FIGURE 1.5 – DeMilitarized Zone

1.7.7 Les IDS

Les systèmes de détection sont conçus pour informer des accès non autorisés ou des intrusions dans les réseaux. Les pare-feu qui opèrent avec les systèmes de détection d'intrusion sont capables de détecter automatiquement les menaces venant de l'extérieur, plus rapidement qu'une vérification par un opérateur [**B3**].

Il existe deux types de détection d'intrusion :

- Le premier système, basé sur l'hôte, doit être installé sur chaque machine à protéger. Il est, en général, intégré au système d'exploitation qu'il protège. Ces types d'IDS sont prévus pour la détection des menaces à un haut niveau de sécurité.

- Le second système, basé sur le réseau, est implémenté en tant qu'analyseur intelligent de protocole. Ses composants surveillent le trafic réseau au niveau physique. Ce second type de système de détection est théoriquement plus efficace que le premier dans le sens où un seul système peut surveiller plusieurs ressources .

1.7.8 POE (Power over Ethernet)

Littéralement puissance par-dessus ethernet abrégé PoE, permet de faire passer une tension électrique en plus des données. POE permet d'alimenter certains appareils d'un réseau ethernet tels que des téléphones IP, des disques durs réseaux, des imprimantes, des caméras IP ou des points d'accès Wi-Fi [**B4**].

Cette technologie permet d'installer des appareils tels une imprimante ou une camera IP dans les endroits qui sont dépourvus de prise électrique. Comme les données et l'alimentation électrique passent dans le même câble Ethernet, il n'y a plus qu'un unique câble à tirer par périphérique connecté.
De ce fait, comparativement à une alimentation externe, la quantité de connectique et d'adaptateurs est réduite. La redondance électrique généralement présente en salle machine avec des commutateurs double alimentation et des onduleurs, se trouve aussi simplifiée. Le tout offre ainsi une facilité de gestion .

1.8 Critères de sécurité

Les critères de sécurité de base sont la disponibilité, l'authentification, l'intégrité et enfin la confidentialité. Dans nôtre thème, nous allons nous concentrer sur la disponibilité qui est un critère important. La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, déterminer la capacité d'une ressource à être utilisée.

1.9 Continuité opérationnelle

La continuité opérationnelle désigne la capacité d'une entreprise à résister aux temps d'indisponibilité (arrêts planifiés ou non, pannes, sinistres) et à faire fonctionner normalement et sans interruption des services importants, en respectant les contrats de niveau de service qu'elle s'est fixés [**w2**].

Pour obtenir le niveau de continuité opérationnelle recherché, l'entreprise devra sélectionner un ensemble de services, de logiciels, de matériels et de procédures, les décrire dans un plan documenté, les implémenter et les mettre en pratique régulièrement.

La solution de continuité opérationnelle doit englober les données, l'environnement d'exploitation, les applications, l'environnement hébergeant les applications et l'interface utilisateur. Pour qu'elle soit considérée comme performante et complète, elle doit faire en sorte que tous ces éléments soient disponibles.

La continuité opérationnelle inclut la reprise après incident et la haute disponibilité. Elle peut être définie comme la capacité à résister à tous les types d'indisponibilité (arrêts planifiés ou non et sinistres), et à assurer le traitement ininterrompu de toutes les applications importantes.

L'objectif final est d'atteindre un temps d'indisponibilité inférieur à 0,001 % de la durée du service totale. Un environnement à haute disponibilité se caractérise par des objectifs qui sont plus exigeants en matière de temps de reprise (quelques secondes à quelques minutes) et de point de reprise.

1.10 Haute disponibilité

On appelle " haute disponibilité " (en anglais " High Avaibility ") toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement d'un service 24H/24 [**B7**].

Ces solutions doivent être capables de fournir au mieux un temps de reprise, très inferieur à celui d'une topologie de solution sans haute disponibilité .

1.10.1 Critères de la haute disponibilité

La haute disponibilité propose plusieurs technologies différentes de résilience des données et de disponibilité des applications.
Chacune de ces technologies a des caractéristiques différentes. Ces caractéristiques doivent être choisies en fonction des besoins uniques de chaque application métier [**W2**].

Budget

Chaque solution à haute disponibilité implique un coût. Son coût doit être comparé aux avantages qu'elle apporte à l'entreprise. Une disponibilité continue avec un temps d'indisponibilité nul est possible sur le plan technique, mais le coût de la protection assurée par une telle solution risque d'être trop élevé .

Besoins en temps de disponibilité

Les besoins en temps de disponibilité désignent la durée totale de disponibilité du système pour les applications d'utilisateurs finaux. La valeur est exprimée en pourcentage du total des heures de travail planifiées [**W2**].

Vue d'ensemble des types d'indisponibilité

Contre quel type d'indisponibilité (arrêt ou panne) l'entreprise tente-t-elle de se prémunir ? La réduction de la fenêtre de sauvegarde, la maintenance planifiée, les arrêts non prévus, ou

les sinistres frappant un site sont des événements que nous devons prendre en compte lorsque vous choisissez une solution à haute disponibilité.

Objectif de temps de reprise

L'objectif de temps de reprise est le délai nécessaire pour effectuer la reprise après un arrêt (planifié, non planifié ou sinistre) et relancer le fonctionnement normal d'une application ou d'un ensemble d'applications [**W2**].

Objectif de point de reprise

L'objectif de point de reprise est le point de cohérence jusqu'où vous devez préserver les données en cas de panne. Les modifications des données précédant la panne ou le sinistre et qui interviennent au moins dans cette plage de temps sont préservées grâce au processus de reprise. La valeur zéro est admise et équivaut à une exigence de "perte de données zéro" [**W2**].

Besoins en résilience

L'entreprise doit identifier ce dont elle a besoin pour se protéger en cas de panne du système hébergeant l'application. Les besoins en résilience englobent l'ensemble des applications, des données et des environnements système qui doivent être protégés pendant tout le temps d'indisponibilité du système de production. Ces entités restent disponibles pendant toute la reprise en ligne, même lorsque le système qui les héberge tombe en panne.

Reprise en ligne et commutation automatiques

L'entreprise doit définir le degré de contrôle qu'elle concède aux fonctions d'automatisation en cas des arrêts non planifiés. Les solutions à haute disponibilité permettent de personnaliser le degré d'interaction lors du traitement d'une reprise en ligne.

En cas de panne, l'application peut effectuer automatiquement une reprise en ligne sur un système de secours, y compris la totalité du démarrage de l'environnement d'application.

Critères de distance

La distance entre les systèmes (dispersion géographique) a ses avantages mais reste soumise à des limitations physiques et pratiques. Dans le cas d'une solution de reprise après incident, la possibilité d'une dispersion géographique des systèmes est toujours avantageuse. En général, plus la distance est grande entre les systèmes, plus la protection contre les sinistres à grande ampleur est élevée. Toutefois, cette distance a une incidence sur l'environnement d'application.

Nombre de systèmes de secours

Les différentes technologies de résilience des données sont proposées avec des nombres variables de systèmes de secours et de données d'application.

Accès a une copie secondaire des données

Les différentes technologies de résilience des données sont soumises à des restrictions différentes concernant l'ensemble des données de sauvegarde. Les besoins liés à l'accès à l'ensemble des données de sauvegarde doivent définir le niveau d'accès requis aux copies secondaires des données, dans le cas des autres activités déchargées à partir des copies principales, par exemple les sauvegardes et les requêtes/rapports. Nous devons prendre en compte la fréquence, la durée et le type d'accès requis à la copie de sauvegarde des données.

Performances du système

L'implémentation de la haute disponibilité a souvent des implications sur les performances. L'entreprise doit déterminer la technologie de résilience des données qu'elle va choisir en fonction de ses besoins.

1.10.2 Les composants de la haute disponibilité

La haute disponibilité permet de continuer à pouvoir accéder aux applications et aux données métier critiques en cas d'une interruption de service.

Les solutions à haute disponibilité atténuent et parfois éliminent totalement l'impact des arrêts planifiés ou non et des sinistres frappant tout un site. Ces solutions se basent sur la technologie de grappe (cluster).

Une grappe (cluster) se compose d'un ou de plusieurs systèmes qui partagent des ressources et des opérations de traitement et assurent une sauvegarde en cas de temps d'indisponibilité. Avec la mise en grappe (cluster), la haute disponibilité n'est pas considérée seulement comme un ensemble de copies identiques de la même ressource dans ces systèmes, mais comme un ensemble de ressources partagées qui fournissent en permanence des services essentiels aux utilisateurs et aux applications.

La mise en grappe (cluster) ne constitue pas une solution de haute disponibilité à elle seule, mais c'est la technologie principale sur laquelle reposent toutes les solutions de haute disponibilité.

L'infrastructure de grappe (cluster), appelée service-ressource de mise en grappe (clustering), fournit les mécanismes sous-jacents permettant de créer et de gérer plusieurs systèmes et leurs ressources comme s'il s'agissait d'une seule entité informatique homogénéisée.

La mise en grappe surveille également les systèmes et les ressources définis dans l'environnement à haute disponibilité afin de rechercher les pannes et prend les mesures appropriées en fonction du type d'indisponibilité.
La mise en grappe associe matériels et logiciels afin de réduire le coût et d'atténuer l'impact des arrêts planifiés ou non, en restaurant rapidement les services lorsque ces arrêts se produisent. Bien que la reprise ne soit pas instantanée avec une mise en grappe (cluster), elle est néanmoins rapide.

La section suivante définit les principaux composants d'une solution à haute disponibilité.

Résilience des applications

La résilience des applications peut être évaluée en fonction de son impact sur les utilisateurs. La totalité de l'environnement d'application, y compris la réplication des données et les unités commutées, peut être contrôlée via l'infrastructure de grappe comme une seule et unique entité.

La résilience des applications est classifiée selon les catégories suivantes :

► **Pas de reprise de l'application :** Suite à une panne ou un arrêt, les utilisateurs doivent redémarrer manuellement leurs applications. En fonction de l'état des données, les utilisateurs déterminent à quel moment redémarrer le traitement au sein de l'application.

► **Redémarrage automatique des applications et repositionnement manuel dans les applications :** Les applications qui étaient actives au moment de la panne ou de l'arrêt sont redémarrées automatiquement. L'utilisateur doit cependant déterminer à quel endroit reprendre dans l'application, en fonction de l'état des données.

► **Redémarrage automatique des applications et reprise semi-automatique :** En plus du redémarrage automatique des applications, les utilisateurs reviennent à un "point de redémarrage" prédéfini dans l'application. Ce point de redémarrage peut être par exemple un menu principal.

Cette technique est normalement cohérente avec l'état des données de l'application résiliente, mais l'utilisateur devra éventuellement avancer au sein de l'application pour revenir effectivement à l'état des données souhaité. Les modifications de l'application sont obligatoires pour sauvegarder les données d'état utilisateur. Lors de l'ouverture de session, l'application détecte l'état de chaque utilisateur et détermine s'il est nécessaire de récupérer le dernier état sauvegardé de l'application.

► **Redémarrage automatique des applications et reprise automatique jusqu'à la dernière frontière de transaction :**L'utilisateur est repositionné dans l'application au point de traitement cohérent avec la dernière transaction validée.

Les données d'application et le point de redémarrage de l'application coïncident exactement. Cette catégorie nécessite de modifier le code de l'application afin de sauvegarder les états

utilisateur à la fin de chaque cycle de validation, afin que l'application sache à quel endroit se trouve chaque utilisateur en cas de défaillance.

▶ **Résilience totale de l'application avec redémarrage automatique et reprise en ligne transparente :**L'utilisateur est repositionné sur la dernière transaction validée, et il voit s'afficher exactement la même fenêtre et les mêmes données que celles qu'il consultait lors de la panne ou de l'arrêt. Aucune perte de données ne se produit, une ouverture d'une session n'est pas requise, et aucune perte des ressources serveur n'est perçue.

L'utilisateur perçoit uniquement un retard dans les temps de réponse. Cette catégorie ne peut être mise en œuvre que dans une application ayant une relation client-serveur .

Résilience des données

Plusieurs technologies permettent de satisfaire les besoins en résilience des données.

1. **Réplication logique des données** La réplication logique est une topologie multi-systèmes de résilience des données destinée à la haute disponibilité. Elle est en général déployée via un produit spécialisé en haute disponibilité. La réplication est exécutée sur des objets via des méthodes logicielles [**W2**].
   Les modifications apportées aux objets (par exemple les fichiers, les membres, les zones de données ou les programmes) sont répliquées sur une copie de sauvegarde.
   La réplication s'effectue en temps ou quasi-temps réel (journalisation distante synchrone) sur tous les objets journalisés. En règle général, si l'objet, tel qu'un fichier, est journalisé, la réplication est gérée au niveau de l'enregistrement .

2. **Unité commutée** Une unité commutée est un ensemble de ressources matérielles telles que des disques, des cartes de communication ou des unités de bande qui peuvent être commutées d'un système à un autre. Pour favoriser la résilience des données.
   Il faut garder à l'esprit le fait que plusieurs technologies peuvent être combinées pour renforcer la résilience des données et comme exemple, nous avons :[**W2**].

•**La technologie RAID (Redundant Array of Inexpensive Disks)** Elle est constituée d'un ensemble de disques indépendants qui permet de réaliser une unité de stockage à partir de plusieurs disques durs. Selon le type de RAID (à partir de RAID1), l'unité ainsi créée possède une grande tolérance de panne avec un risque minimal de perte de données. La répartition sur plusieurs disques durs permet donc d'augmenter la sécurité et la disponibilité de ces données [**B3**].

Les disques assemblés en unité de stockage peuvent être utilisés de différentes façons, appelées niveaux RAID. Les formes les plus courantes sont listées ci-dessous :

-**Niveau 0 :** appelé striping ou agrégat de bandes.

-**Niveau 1 :** appelé mirroring, shadowing ou disque disposé en miroir.

-**Niveau 3 :** appelés grappes de disques identiques, une unité de stockage est réservé à la gestion de la parité.

-**Niveau 4 :** type amélioré du niveau 3 avec une gestion synchrone des unités de disques.

-**Niveau 5 :** agrégat de bandes avec parité alternée (parité répartie sur tous les disques).

-**Niveau 6 :** extension du niveau 5, utilisation d'une double parité répartie sur tous disques.

-**Niveau 10 :** assemblage de Niveau 0 et de Niveau 1.

Actuellement, les plus utilisés sont les formes RAID-1, RAID-5, RAID-10. Il existe des assemblages de type RAID matériels et logiciels .

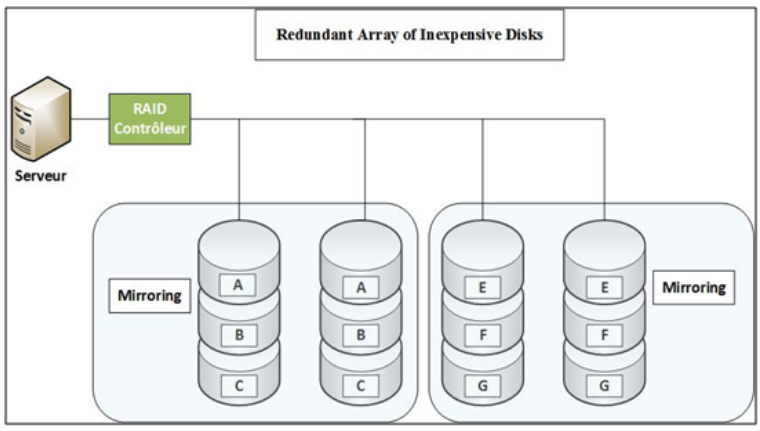

FIGURE 1.6 – Redundant Array of Inexpensive Disks

Résilience de l'environnement

La résilience de l'environnement peut être divisée en deux parties : l'environnement physique et l'environnement logique.
L'environnement physique, qui relève en fait de la disponibilité pour un système unique, privilégie les aspects tels que la redondance matérielle, la topologie de réseau (redondance des chemins d'accès), l'infrastructure de l'alimentation et la capacité de refroidissement.
L'environnement logique est l'environnement qui héberge et exécute les applications. Il comprend les paramètres systèmes, les profils utilisateur et les attributs système qui permettent à l'utilisateur d'exécuter l'application sur plusieurs serveurs [**W2**].

1. **Environnement physique**

   Un composant à protéger est le réseau. Le concept de réseau englobe les cartes réseau redondantes sur le système, et les chemins réseau de communication utilisant les matériels réseaux redondants, à l'usage des utilisateurs comme des systèmes[**W2**].

2. **Environnement logique**

   L'environnement logique est l'environnement d'exécution des applications. Il comprend les attributs système, les valeurs système, les attributs de configuration de réseau, la configuration de la gestion des travaux et les profils utilisateur [**W2**].

   Ces éléments doivent être identiques sur le système de secours et sur le système principal de production pour assurer un fonctionnement correct de l'environnement d'application. Pour garantir la cohérence de ces valeurs d'environnement logique sur plusieurs systèmes, nous pouvons utiliser un domaine administratif de grappe (cluster), la réplication logique ou un processus manuel répondant à des spécifications rigoureuses .

   Cluster

   La plupart des solutions de clusters existantes actuellement sont basées sur les systèmes d'exploitation Windows, Linux et Unix.

   Un cluster comprend un groupe de serveurs, appelés nœuds utilisant le service cluster. Cette technologie garantit un environnement de haute disponibilité, une tolérance de panne pour des ressources et des applications en cas de défaut (basculement manuel ou automatique sur le (les) autre(s) nœud(s)).

Il existe deux modes de fonctionnement :

- Equilibrage de charge (Actif/actif)
- Cluster avec basculement (Actif/passif) [**B3**].

(a) **Equilibrage de charge** Le service équilibrage de la charge réseau répartit dynamiquement des applications TCP/IP sur plusieurs serveurs.

Si l'un des serveurs tombe en panne, la charge et les connexions gérées par ce serveur se répartissent dynamiquement sur les autres serveurs, ce qui permet de créer un environnement à haut niveau de tolérance de pannes, sans qu'il faille investir dans du matériel spécialisé partagé.

Les différents serveurs du cluster peuvent avoir des équipements et des capacités différentes et la gestion générale de l'équilibrage et des reprises se produit de manière automatique [**B3**].

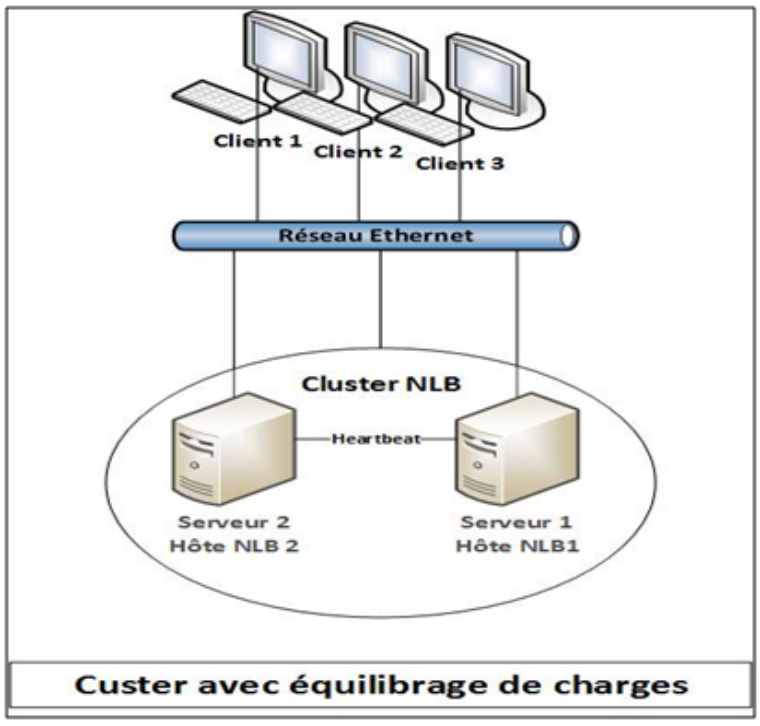

FIGURE 1.7 – Cluster avec équilibrage de charges

(b) **Cluster avec basculement** Le cluster avec basculement s'appuie sur une ressource partagée entre les nœuds du cluster.

Cette ressource consiste généralement en une baie de disque SAS ou fibre Channel partagée ou un réseau SAN SCSI.

Chaque serveur du cluster est connecté à la source partagée qui héberge la base de données commune, chargée de gérer le clustering. En principe, les nœuds du cluster ont des équipements matériels et des capacités identiques, bien qu'il soit techniquement possible de créer un cluster composé de serveurs dissemblables, ce qui n'est pas conseillé.

Les clusters avec basculement offrent un environnement à haut niveau de tolérance de pannes et de configurabilité, idéal pour les services et les applications critiques.

Il n'est pas obligatoire de programmer spécifiquement les applications pour qu'elles puissent tirer parti de la tolérance de pannes apporté par le cluster avec basculement. Toutefois, si l'application est adaptée aux clusters, elle pourra bénéficier de fonctionnalités complémentaires dans un scénario de basculement et de reprise [**B3**].

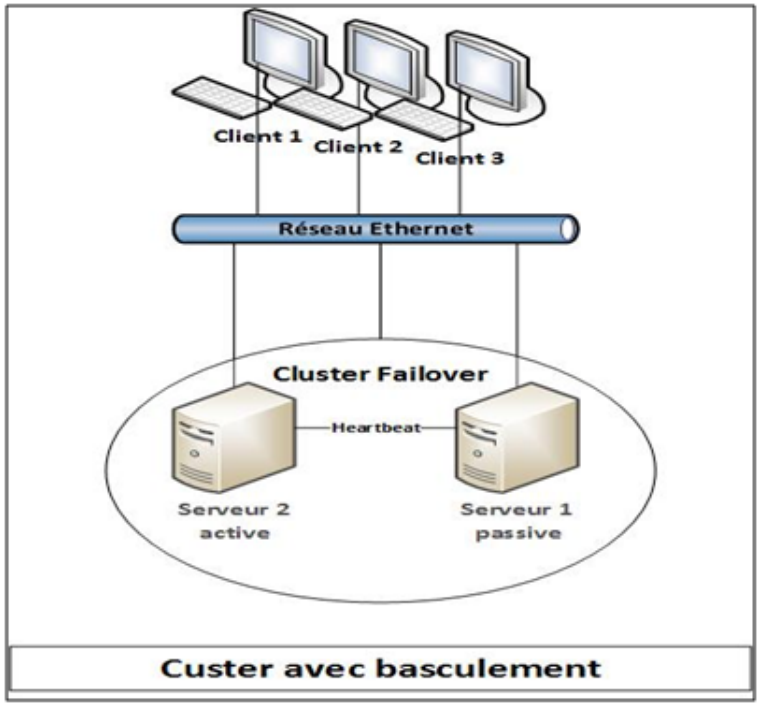

FIGURE 1.8 – Cluster avec basculement

1.10.3 Avantages de la haute disponibilité

Les avantages de la haute disponibilité sont :

√ protéger les entreprises contre les pertes de chiffre d'affaires en cas d'interruption de l'accès à leurs données et leurs applications critiques.

√ Temps d'indisponibilité planifiés : La haute disponibilité peut réduire l'impact sur les clients et les utilisateurs chaque fois qu'il faudra mettre hors ligne des systèmes ou des données pour exécuter des tâches de maintenance indispensables telles que les sauvegardes nocturnes ou l'installation de nouveaux matériels ou logiciels.

√ Arrêts non planifiés : Les solutions à haute disponibilité assurent une protection contre les arrêts non planifiés dus aux erreurs humaines, aux problèmes logiciels, aux pannes matérielles et aux problèmes environnementaux.

√ Reprise après incident : La reprise après incident comprend l'ensemble des ressources, les plans, les services et les procédures qui permettent d'effectuer la reprise des applications métier critiques sur un site distant en cas de sinistre.

√ Réduction de la fenêtre de sauvegarde : Les solutions à haute disponibilité permettent de réduire le temps d'indisponibilité du système ou des services pendant les sauvegardes.
Le temps nécessaire à l'exécution d'une sauvegarde, de A jusqu'à Z, est appelé une fenêtre de sauvegarde. La difficulté consiste à sauvegarder la totalité des données dans cette fenêtre de temps.

√ Equilibrage de charge : les solutions à haute disponibilité peuvent être utilisées pour l'équilibrage de charge.
Les technologies les plus courantes d'équilibrage de charge consistent à déplacer le travail vers les ressources disponibles et répartit dynamiquement la charge de travail.

1.11 Conclusion

La sécurité est une préoccupation primordiale dans le domaine des réseaux. Pendant de longues années la sécurité des équipements ou/et des données demandait une isolation complète de l'environnement extérieur, et une panne ou même des travaux de maintenance provoquaient une indisponibilité du réseau ou de l'un de ses composants, mais des mécanismes fondamentaux de sécurité et de disponibilité ont été mise en œuvre afin de rendre le réseau plus fiable.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

Nous allons aborder dans ce chapitre la présentation de l'organisme qui nous a accueillis dans le cadre de notre stage de fin d'étude, afin de mettre en œuvre une étude et la proposition d'une solution de tolérance aux pannes.

L'étude de l'existant, point clé de notre démarche est une étape essentielle qui vise à représenter l'état actuel du réseau de l'entreprise TCHIN-LAIT afin de découvrir les insuffisances et créer des solutions qui résolvent les anomalies trouvées.

2.2 Présentation de TCHIN-LAIT

Implantée sur l'ancien site de la limonaderie TCHIN-TCHIN, à l'entrée de la ville de Béjaïa, TCHIN-LAIT produit et commercialise le lait longue conservation UHT (Ultra Haute Température) sous le label CANDIA.

TCHIN-LAIT est une société privée de droit Algérien, constituée juridiquement en SARL. Elle est dotée d'un capital de 497.000.000 DA, détenu majoritairement par Mr Fawzi BERKATI, gérant de la société.

A son lancement, en 2001, TCHIN-LAIT commercialisait près de 4 millions de litres de produits/an. En 2013, elle en a produit et commercialisé 200 millions, avec un chiffre d'affaires de 6,3 milliards de dinars pour cette même année [**B1**].

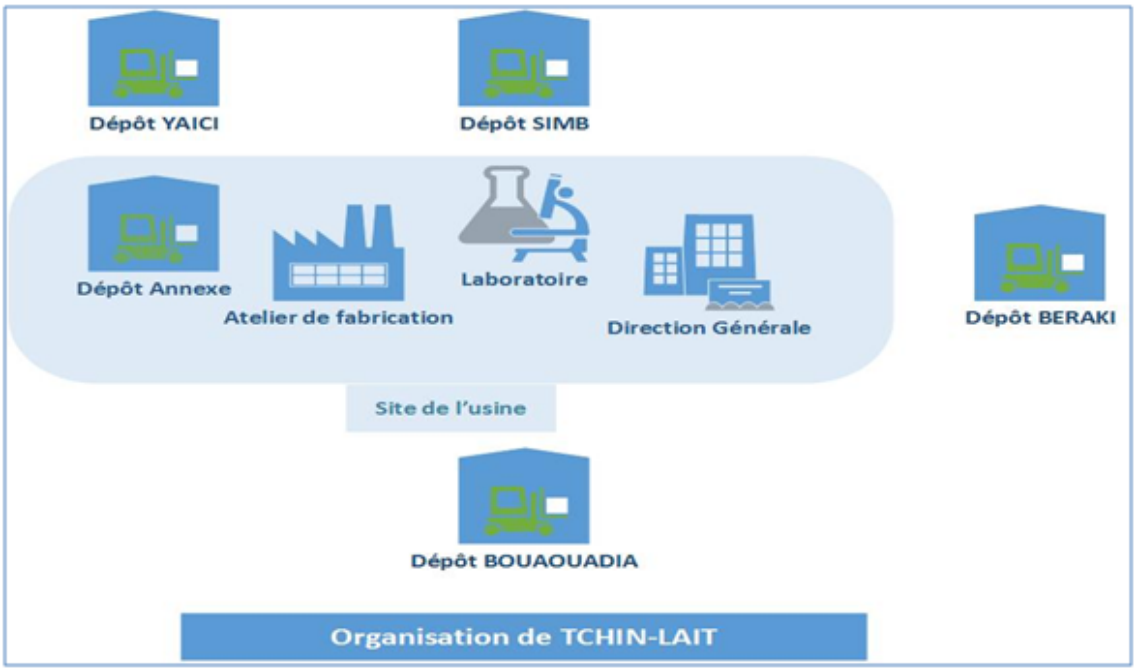

FIGURE 2.1 – Organisation de TCHIN-LAIT

2.3 Historique de TCHIN-LAIT

TCHIN-TCHIN était à l'origine une entreprise familiale, spécialisée dans les boissons gazeuses depuis 1952. Elle a de ce fait capitalisé une longue expérience dans le conditionnement des produits sous forme liquide.

L'arrivée de grandes firmes multinationales sur le marché des boissons gazeuses et la multiplication du nombre de limonadiers locaux l'a contraint à réviser sa stratégie ; d'où l'idée d'une reconversion vers le lait UHT, qui a donné naissance à TCHIN-LAIT[**B1**]. La figure suivante illustre la direction générale de TCHIN-LAIT [**W1**].

FIGURE 2.2 – Direction générale TCHIN-LAIT

2.4 Organisation de TCHIN-LAIT

TCHIN-LAIT est une laiterie moderne, construite sur une superficie totale de 6000m2, comprenant une direction et des services (la direction générale, le service commerciale, le service finances et comptabilité, le service marketing, le service de production, le service Direction maintenance, le laboratoire et le département informatique) et des sites de stockage (annexe, BOUAOUADIA, SIMB,YAICI, BERAKI).

Elle fonctionne avec un effectif total de plus de 300 personnes entre cadres, agents de maîtrise et ouvriers de production, 24/24 heures avec trois équipes de production :[**B1**].

• première équipe, 5 heures du matin à 13 heures.

• deuxième équipe, 13 heures à 21 heures.

• troisième équipe, 21 heures à 5 heures du matin.

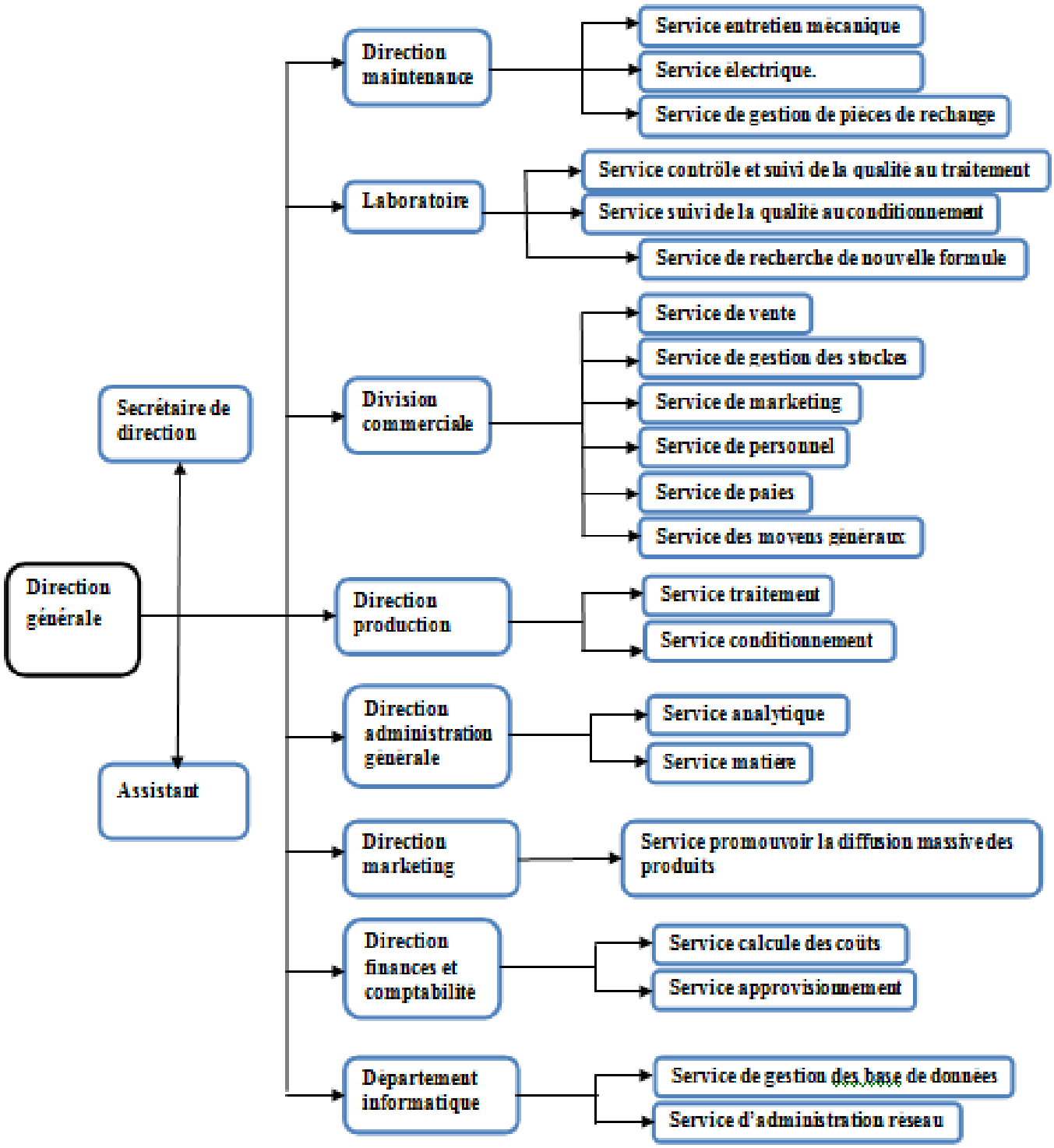

FIGURE 2.3 – Organigramme de l'organisation de TCHIN-LAIT

2.4.1 Administration générale

L'administration générale est partagée en trois étages :

-**rez-dechaussée :** il contient le service d'accueil, le service des stages et le secrétariat.

-**1ere étage :** il contient le service comptabilité et le service technique.

-**2eme étage :** il contient le bureau du directeur M.BERKATI et le département informatique .

2.4.2 Un atelier de production

Elle dispose d'un outil de production moderne, avec 4 lignes de conditionnement qui peuvent produire près de 200 millions de litres de lait/an. La figure suivante illustre l'atelier de production de TCHIN-LAIT [**W1**].

FIGURE 2.4 – Atelier de production TCHIN-LAIT

2.4.3 Un laboratoire

Elle dispose aussi d'un laboratoire équipé des dernières technologies de recherche dans le but de créer de nouvelles formules et aussi pour tester les produits finis qui arrive de la production pour vérifier leurs conformités aux normes exigé.

Les résultats des analyses sur les produits sont directement envoyés à la direction de Candia France qui pourra valider ensuite cette production.

2.4.4 Dépôts de stockages (ANNEXE)

Il se compose de plusieurs compartiment ou sont stockés les produits finis qui sorte de la production et aussi les matières premières qui vont être utilisées. Ainsi que d'autres sites (dépôts) de stockages en dehors du site de l'usine :

• **Site de BOUAOUADIA :** C'est un site de stockage de matières premières, il contient un bureau pour la gestion du site et les mises à jour du code à barre des lots d'arrivages. Il contient aussi des compartiments pour stocker les produits.

• **Site de SIMB :** C'est un site de stockage pour les emballages et quelques matières premières. Il contient des compartiments de stockage et un bureau de gestion.

• **Site de YAICI :** C'est un site de stockage pour les emballages et quelques matières premières. Il contient des compartiments de stockage et un bureau de gestion.

• **Site de BERAKI :** C'est un site de stockage qui contient les produits finis destinés à la région d'Alger et de ses alentours.

2.5 Politique de développement

TCHIN-LAIT/Candia a toujours été attentive à la satisfaction des besoins de ses consommateurs.

La preuve en est, toutes les innovations apportées au produit (bouchon à vis, nouveaux produits lancés, mise en place d'une distribution directe pour assurer la disponibilité du produit...) sont des preuves que TCHIN-LAIT est attentive à une meilleure satisfaction de ses clients, avant que le concurrent ne le fasse à sa place.

TCHIN-LAIT dispose d'un service consommateurs et traite toutes les demandes d'information et réclamations qui parviennent au service qualité. Le tableau suivant présente les chiffres de l'année écoulé de TCHIN-LAIT [**B1**].

Employés	45O
Distributeurs	30
Points de vente	21.000
Véhicules de Distribution	75
Emplois indirects	300
Millions de litres de laits produits par an	200

TABLE 2.1 – TCHIN-LAIT en chiffre

2.6 Présentation du département informatique

Le département informatique de TCHIN-LAIT est situé au deuxième étage de la direction générale. Il contient la salle machine ou sont entreposé les armoires des serveurs et de brassage ainsi que les bureaux des quatre responsables informatique :

- Deux responsables du système d'information et des bases de données.
- Deux responsables de l'administration du réseau informatique.

2.7 Etude de l'existant

Pour mener à bien l'étude de l'existant nous avons procédé à une étude par site.
La première tâche a été de rencontrer différentes personnes qui entretiennent directement ou indirectement une relation avec le département informatique de TCHIN-LAIT. Il s'agit principalement de M. Raid BAROUTDJI responsable informatique.

Après quoi, nous avons réellement débuté le travail en menant différentes recherches. Cette méthodologie de travail nous a permis d'avoir une connaissance large de l'existant.

2.7.1 Schéma générale du réseau TCHIN-LAIT

Le réseau TCHIN-LAIT est partagé en cinq sites (Usine, Site BOUAOUADIA, Site SIMB, Site YAICI, Site BERAKI) comme le montre la figure suivante.

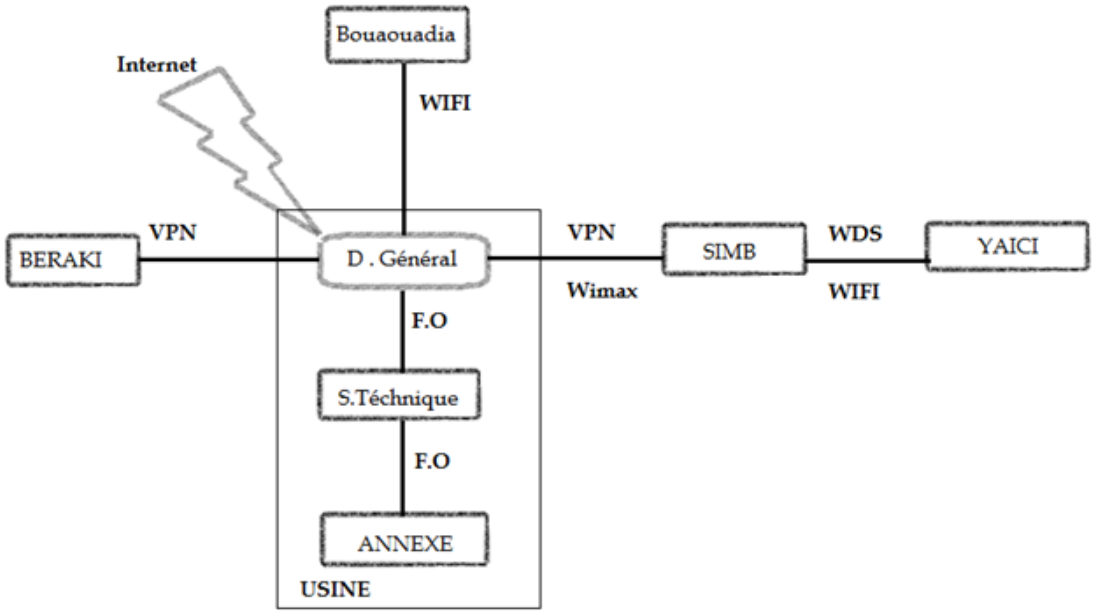

FIGURE 2.5 – Schéma général du réseau de Tchin-Lait

2.7.2 Le parc informatique TCHIN-LAIT

Le réseau TCHIN-LAIT contient un parc informatique composé d'une centaine d'ordinateurs portable et de bureaux leurs configurations est illustré dans le tableau suivant.

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

TABLE 2.2 – Configuration des ordinateurs de TCHIN-LAIT

2.7.3 Les applications de TCHIN-LAIT

Les applications de TCHIN-LAIT sont diverses installées sur les serveurs contenu en salle machine, d'autres sur les machines des employées. Quelques unes sont listées dans le tableau suivant :

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

TABLE 2.3 – Les logiciels de TCHIN-LAIT

2.7.4 Les serveurs de TCHIN-LAIT

Un serveur est un dispositif informatique matériel et logiciel qui offre des services à différents clients.

Les serveurs dont nous disposons dans le réseau de TCHIN-LAIT, sont tous dans une salle machine et présentent différentes caractéristiques énumérées comme suit :

Nom du serveur	Rôles des serveurs	Type de serveur
Serveur FP	Serveur de base de données et de fichiers partagé	Serveur HP ProLiant ML350p Gen8
Serveur VID	Serveur de vidéo surveillance	Serveur HP ProLiant ML350p Gen8
Serveur DOM	Contrôleur de domaines	Serveur HP ProLiant ML350p Gen8
Serveur DON	Serveur de base de données (ERP)	Serveur HP ProLiant ML350p Gen8
Serveur ENT	Serveur du système de gestion d'entrepôts	Serveur HP ProLiant ML350p Gen8
Serveur KAS	Serveur kaspersky	Serveur HP ProLiant ML350p Gen8
Serveur MES	Serveur messagerie	Serveur HP ProLiant ML350p Gen8
Serveur APP	Serveur qui contient quelques applications	Serveur HP ProLiant ML350p Gen8

TABLE 2.4 – Les serveurs du réseau TCHIN-LAIT

2.7.5 Le site de l'Usine

Il est considéré comme la partie centrale du réseau, il se compose lui aussi de trois sites qui sont reliés entre eux par la fibre optique.

• direction générale

• service technique

• annexe

La direction générale

Elle contient le bureau du directeur et en même temps la salle informatique ou sont mises deux armoire l'une de serveurs et l'autre de brassage, qui relie l'ensemble de la direction au réseau. Dans chaque bureau il ya une prise réseau RJ45 ou on peut brancher les équipements terminaux au réseau.

Liste des équipements de la direction générale

1. **Les équipements d'interconnexion de la direction générale**

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

TABLE 2.5 – Les équipements d'interconnexion de la direction générale

2. **Les équipements terminaux fixes de la direction générale**

Nom d'équipements	Type d'équipements	Modèles
CLP 620	DG Imprimante IP	SAMSUNG CLP 620
ZEBRA S	Imprimante IP	ZEBRA

TABLE 2.6 – Les équipements terminaux fixes de la direction générale

Le service Technique

Il est décomposé en bureau et chaque bureau possède une prise réseau Rj45. Il contient aussi une armoire de brassage centrale qui relie tous les sites de l'usine entre eux.

Liste des équipements du Service Technique

1. **Les équipements d'interconnexion du Service Technique**

Nom d'équipements	Type d'équipements	Modèles
Cisco fédérateur	Switch	Switch Cisco
Cisco Technique	Switch	Switch Cisco
Cisco DAG	Switch	Switch Cisco
NetGear Archives	Switch	Switch Cisco
WMS Usine1	Point d'accès	AP-Motorola
WMS Usine2	Point d'accès	AP-Motorola
WMS Usine3	Point d'accès	AP-Motorola
WMS Usine4	Point d'accès	AP-Motorola
WMS Usine5	Point d'accès	AP-Motorola

TABLE 2.7 – Les équipements d'interconnexion du Service Technique

2. **Les équipements terminaux fixes du Service Technique**

Nom d'équipements	Type d'équipements	Modèles
Prod 1	Imprimante IP	ZEBRA
Prod 2	Imprimante IP	ZEBRA
ML2850 Technique	Imprimante IP	SAMSUNG 2850
CLP620 Personnel	Imprimante IP	SAMSUNG CLP 620
MFC7460 DAG	Imprimante IP	BROTHER 7460
ML3470 Chefs	Imprimante IP	SAMSUNG 3470
Zebra 3 (Chefs)	Imprimante IP	ZEBRA
ML3470 Labo	Imprimante IP	SAMSUNG 3470
Pointeuse 1	Pointeuse	ZKSOFTWARE
Pointeuse 2	Pointeuse	ZKSOFTWARE

TABLE 2.8 – Les équipements terminaux fixes du Service Technique

ANNEXE

Elle se compose principalement d'équipements dédiés à la récolte des données des produits sortie de la chaine de fabrication en produits finis et c'est données sont transmis directement à la direction générale pour enrichir la base de données de l'entreprise.

Liste des équipements de ANNEXE

1. **Les équipements d'interconnexion de ANNEXE**

Nom d'équipements	Type d'équipements	Modèles
Cisco CDB	Switch	Switch Cisco
Switch PF	Switch	Switch Cisco
Switch NetGear	Switch	Switch Cisco
ProCurve Switch	Switch	Switch Cisco
AP DMV	Point d'accès	AP-Motorola
WMS CDB1	Point d'accès	AP-Motorola
WMS CDB2	Point d'accès	AP-Motorola
WMS CDB3	Point d'accès	AP-Motorola
WMS CDB4	Point d'accès	AP-Motorola
WMS CDB5	Point d'accès	AP-Motorola
WMS CDB6	Point d'accès	AP-Motorola
WMS CDB7	Point d'accès	AP-Motorola

TABLE 2.9 – Les équipements d'interconnexion annexe

2. **Les équipements terminaux fixes de ANNEXE**

Nom d'équipements	Type d'équipements	Modèles
ML3710 CDB	Imprimante IP	SAMSUNG 3710
Zebra CDB	Imprimante IP	ZEBRA
HL2270 DMV	Imprimante IP	BROTHER 2270
CLP660 DMV	Imprimante IP	SAMSUNG 660
CLP660 Appros	Imprimante IP	SAMSUNG 660
ML3710 GDS	Imprimante IP	SAMSUNG 3710
ML2850 DFC	Imprimante IP	SAMSUNG 2850
HL2270 Idjraoui	Imprimante IP	BROTHER 2270
ML3470 Bounia	Imprimante IP	SAMSUNG 3470
Pointeuse Annexe	Pointeuse	ZKSOFTWARE

TABLE 2.10 – Les équipements terminaux fixes annexe

2.7.6 Site BOUAOUADIA

Le site BOUAOUADIA est un dépôt de stockage donc l'ensemble des équipements de ce site servent à maitre à jour la base de données de l'entreprise quand le produit sort du dépôt de fabrication et entre en stock.

Il est relié à la direction générale par wifi (WDS) avec des assiettes placées l'une en face de l'autre de chaque coté des deux sites.

Liste des équipements de BOUAOUADIA

1. **Les équipements d'interconnexion de BOUAOUADIA**

Nom d'équipements	Type d'équipements	Modèles
Switch	Switch	Switch Cisco
WDS Depot	Assiette wifi	Bridge wifi
WMS Boua1	Point d'accès	AP-Motorola
WMS Boua2	Point d'accès	AP-Motorola
WMS Boua3	Point d'accès	AP-Motorola
WMS Boua4	Point d'accès	AP-Motorola

TABLE 2.11 – Les équipements d'interconnexion de BOUAOUADIA

2. **Les équipements terminaux fixes de BOUAOUADIA**

Nom d'équipements	Type d'équipements	Modèles
ML3470 Bouaoudia	Imprimante IP	SAMSUNG 3470
ZEBRA-BOUAOUDIA	Imprimante IP	ZEBRA
Appro Rabehi	Micro ordinateur	HP3330
TP BOUAOUADIA	Pistolet à barre	TP-Motorola

TABLE 2.12 – Les équipements terminaux fixes de BOUAOUADIA

2.7.7 Site BERAKI (ALGER)

Le site BERAKI qui se situe à ALGER est aussi un dépôt de stockage. Il a les mêmes équipements que BOUAOUADIA et ils servent dans le même but.

Il est relié à la direction générale par une technologie de connexion à distance qui se nome VPN (réseau privé virtuel), Cette fonctionnalité chiffre le trafic réseau sensible et requiert une authentification forte, fournissant un accès sécurisé.

Liste des équipements de BERAKI

1. **Les équipements d'interconnexion de BERAKI**

Nom d'équipements	Type d'équipements	Modèles
Routeur Beraki	Routeur	Routeur Cisco
Switches GLJ	Switch	Switch Cisco

TABLE 2.13 – Les équipements d'interconnexion de BERAKI

2. **Les équipements terminaux fixes de BERAKI**

Nom d'équipements	Type d'équipements	Modèles
ML2850 BARAKI	Imprimante IP	SAMSUNG 2850
Zebra Baraki	Imprimante IP	ZEBRA

TABLE 2.14 – Les équipements terminaux fixes de BERAKI

2.7.8 Site SIMB

Le site SIMB est aussi un dépôt de stockage. Il a les mêmes équipements que BOUAOUADIA et ils servent dans le même but.

Il est rattaché à la direction générale avec du WiMax qui est pris en charge par le fournisseur d'accès à internet.

Liste des équipements de SIMB

1. **Les équipements d'interconnexion de SIMB**

Nom d'équipements	Type d'équipements	Modèles
Routeur SIMB	Routeur	Routeur Cisco
Switch NetGear	Switch	Switch Cisco
WDS Simb	Assiette wifi	Bridge wifi
WMS SIMB1	Point d'accès	AP-Motorola
WMS SIMB2	Point d'accès	AP-Motorola
WMS SIMB3	Point d'accès	AP-Motorola
WMS SIMB4	Point d'accès	AP-Motorola

TABLE 2.15 – Les équipements d'interconnexion de SIMB

2. **Les équipements terminaux fixes de SIMB**

Nom d'équipements	Type d'équipements	Modèles
ML2850 SIMB	Imprimante IP	SAMSUNG 2850
Zebra SIMB	Imprimante IP	ZEBRA
PC Kheloufi SIMB	Micro ordinateur	Hp3330
TP SIMB 1	Pistolet à barre	TP-Motorola
TP SIMB 2	Pistolet à barre	TP-Motorola

TABLE 2.16 – Les équipements terminaux fixes de SIMB

2.7.9 Site YAICI

Le site YAICI est aussi un dépôt de stockage. Il a les mêmes équipements que BOUAOUADIA et ils servent dans le même but.

Il est relié au site SIMB par la même technique (wifi) avec la quelle a été reliée le site de BOUAOUADIA à la direction générale.

Liste des équipements de YAICI

1. **Les équipements d'interconnexion de YAICI**

Nom d'équipements	Type d'équipements	Modèles
Switch D-Link	Switch	Switch D-Link
WDS Yaici	Assiette wifi	Bridge wifi
AP YAICI1	Point d'accès	AP-Motorola
AP YAICI2	Point d'accès	AP-Motorola

TABLE 2.17 – Les équipements d'interconnexion de YAICI

2. **Les équipements terminaux fixes de YAICI**

Nom d'équipements	Type d'équipements	Modèles
Yaici ML2850	Imprimante IP	SAMSUNG 2850
Zebra 1 (Yaici)	Imprimante IP	ZEBRA
TP YAICI	Pistolet à barre	TP-Motorola

TABLE 2.18 – Les équipements terminaux fixes de YAICI

2.8 Problématique

TCHIN-LAIT dispose d'un réseau de taille importante composé de cinq sites reliés par VPN et WDS. Il est constitué de plusieurs équipements, des Switch, des routeurs, des Firewall, pour la plupart de marque Cisco.

La gestion du réseau est à la charge du département informatique qui veille à son bon fonctionnement, cependant l'augmentation continuelle de sa taille, le rend de plus en plus difficile à maintenir dans un état de marche tout en le préservant des aléas externes qui peuvent nuire à sa sécurité.

La gestion et la maintenance du réseau est assuré par un groupe de quatre ingénieurs, qui en cas de panne, seront obligés de faire par eux-mêmes l'audit et le diagnostic sur tout le réseau tout en se déplaçant de site en site. Ce qui peut rendre la tâche à la fois compliquée, ardue et quelques fois trop gourmande en termes de temps et de cout.

Le système d'information est dépourvu de plateforme de partage de données et de logiciels, qui handicape considérablement le travail du département informatique quand il s'agit d'installation ou de maintenance. En cas de panne d'un des ordinateurs de l'un des services de l'entreprise son utilisateur sera dans l'incapacité de travailler et ce qui pourra produire un retard ou un arrêt de ce service si l'ordinateur en lui-même contient un logiciel critique.

Le système se base uniquement sur les seuls équipements qui le composent, pour son bon fonctionnement c'est-à-dire qui ne dispose pas d'équipements de secours qui prennent le relais en cas de panne d'un de ses équipements. Cette non-duplication de certains composants sensibles peut provoquer l'arrêt total du système au moindre problème qui survient.

2.9 Conclusion

L'étude de l'existant nous a permis de constater que le réseau existant utilise une technologie avancée, mais présente des insuffisances au niveau de la disponibilité (manque de redondance suffisante pour quelques ressources critiques).

Chapitre 3

Cas pratique TCHIN-LAIT

3.1 Introduction

L'étude de l'existant nous a permis de mieux cerner les besoins informatiques du réseau de TCHIN LAIT et d'en tirer certaines conclusions concernant des carences en termes de tolérance aux pannes , nous proposerons des recommandations qui peuvent palier à ces carences.

3.2 Les recommandations

Ce sont les recommandations que nous avons proposé à l'entreprise TCHIN-LAIT pour mener à bien ce projet de manière globale.

-Déployer deux terminal server qui permettrons des accès à distance, réduire la tache de mise à jour des logiciels partagés sur ces serveurs et faciliter le travail de groupe.

-Proposition d'une solution de haute disponibilité qui va résoudre la contrainte de continuité opérationnel de l'entreprise.

Pour notre thème nous avons opté pour la mise en place d'une solution de haute disponibilité basée sur l'installation de deux terminal server qui permettrons en plus des accès à distance, de réduire le temps d'inactivités des employés en cas de pannes de la machine de l'utilisateur, de l'application ou carrément de l'un des deux serveurs, mais aussi de faciliter leurs mobilité au sein de l'entreprise, Dans le but de répondre à la continuité opérationnelle

que s'est fixé TCHIN LAIT.

3.3 Serveur Terminal Server

Un serveur TS sert à héberger des programmes pour les clients. Les utilisateurs peuvent se connecter à un serveur TS pour exécuter des programmes, enregistrer des fichiers et utiliser des ressources réseau sur ce serveur.

Ils peuvent accéder à un serveur Terminal Server par le biais d'une connexion Bureau à distance ou à l'aide de programmes RemoteApp.

3.4 Les services Terminal Server

Le rôle de serveur Services TS dans Windows Server 2008 est de fournir des technologies qui permettent aux utilisateurs de pouvoir accéder à des applications de l'entreprise à travers leur réseau local ou Internet.

Les services Terminal Server nous permettent de déployer et gérer efficacement des logiciels dans un environnement d'entreprise. Nous pouvons facilement déployer des programmes à partir d'un emplacement centralisé. Du fait qu'ils sont installés sur le serveur Terminal Server et non sur l'ordinateur client, les programmes sont plus faciles à mettre à niveau et à gérer.

Lorsqu'un utilisateur accède à un programme sur un serveur Terminal Server, l'exécution du programme s'effectue sur le serveur. Seules les informations du clavier, de la souris et de l'affichage sont transmises sur le réseau. Chaque utilisateur ne voit que sa propre session. La session est gérée de manière transparente par le système d'exploitation du serveur, indépendamment des sessions des autres clients.

3.5 Avantages de l'utilisation des services Terminal Server

Le fait de déployer un programme sur un serveur Terminal Server au lieu de le déployer sur chaque périphérique offre de nombreux avantages, notamment :

-Pouvoir déployer rapidement des programmes sur les périphériques informatiques d'une entreprise. Les services Terminal Server sont très utiles lorsque des programmes sont mis à jour régulièrement, peu utilisés ou difficiles à gérer.

-Ils peuvent considérablement réduire la bande passante réseau requise pour accéder à des applications distantes.

-Les services Terminal Server contribuent à améliorer la productivité des utilisateurs. Les utilisateurs peuvent accéder à des programmes exécutés sur un serveur Terminal Server à partir de périphériques, tels que des ordinateurs personnels, des bornes, du matériel de faible puissance et des systèmes d'exploitation autres que Windows.

-Les services Terminal Server améliorent les performances des programmes pour les employés de succursales qui ont besoin d'accéder à des magasins de données centralisés. Les programmes utilisant énormément de données n'ont parfois pas de protocoles client-serveur optimisés pour les connexions à basse vitesse. Les programmes de ce type fonctionnent généralement mieux sur une connexion des services Terminal Server que sur un réseau étendu (WAN) classique.

3.6 Programme RemoteApp

Les programmes RemoteApp sont des programmes auxquels nous pouvons accéder à distance par le biais des services Terminal Server et qui apparaissent comme s'ils étaient exécutés sur l'ordinateur local de l'utilisateur final.

Au lieu d'être présenté à l'utilisateur sur le Bureau du serveur Terminal Server distant,

le programme RemoteApp est intégré au Bureau du client, exécutant sa propre fenêtre redimensionnable avec sa propre entrée dans la barre des tâches. Les utilisateurs peuvent exécuter côte à côte des programmes de RemoteApp et leurs programmes locaux.
Si un utilisateur exécute plusieurs programmes RemoteApp sur le même serveur Terminal Server, les programmes RemoteApp partagent la même session des services Terminal Server.

3.7 L'objectif de la solution de haute disponibilité proposé

l'objectif principal de notre solution est de répondre aux critères de continuité opperationnel de l'entreprise et cela avec la configuration d'une solution à haute disponibilité qui va réduire le temps d'inactivité en cas de panne de l'un des serveurs que nous allons installer.

3.8 La mise en place de la solution de haute disponibilité

Avant de commencer la mise en place de la solution de haute disponibilité avec équilbrage de charge et l'installation et la configuration des deux Terminal Server, nous avons installé en premier lieux un environnement virtuel qui simule l'environnement logique de l'entreprise TCHIN-LAIT, c'est-à-dire un contrôleur de domaine (DC-Virtal) auquel nous avons affecté aussi les rôles de serveur DNS et DHCP.Le nom du domaine est V-Tchinlait.

Nous avons installé ensuite une machine cliente sous Windows 7 pour les testes de basculement entre les TSE .

Enfin nous avons introduit toutes ces machines dans le domaine y compris les machines qui vont contenir nos Terminal Server pour qu'elles puissent communiquer entre elles.

Pour la mise en place de cette solution nous allons montrer les étapes dans les figures suivantes et décrire la procédure suivie.

3.9 Installation du Terminal Server V-TSC

-Ouvrir le Gestionnaire de serveur (**Server Manager**).

Pour ouvrir le Gestionnaire de serveur, il faut cliquer sur **Start** et pointer ensuite sur **Administration tools**, puis sur **Server Manager**.

La fenêtre suivante s'ouvre. Sous la partie **Roles Summary**, cliquez sur **Add Roles**.

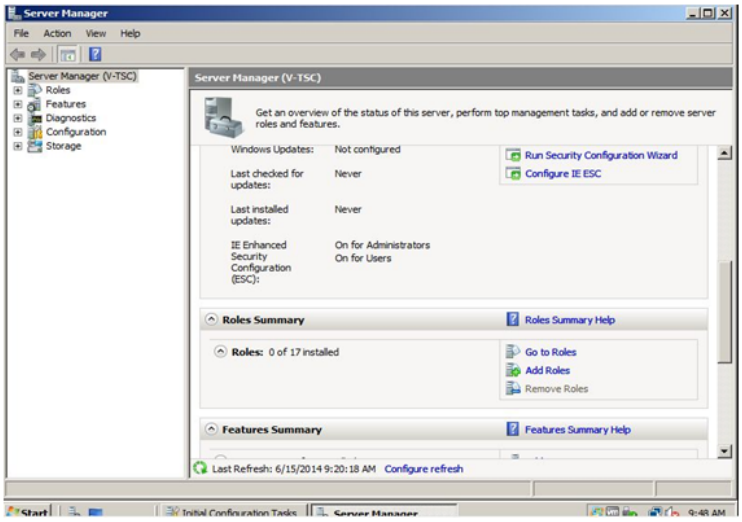

FIGURE 3.1 – Gestionnaire de serveur

-Dans la page **Select Server Roles**, activez la case à cocher **Terminal Services**, puis cliquez sur **Next**.

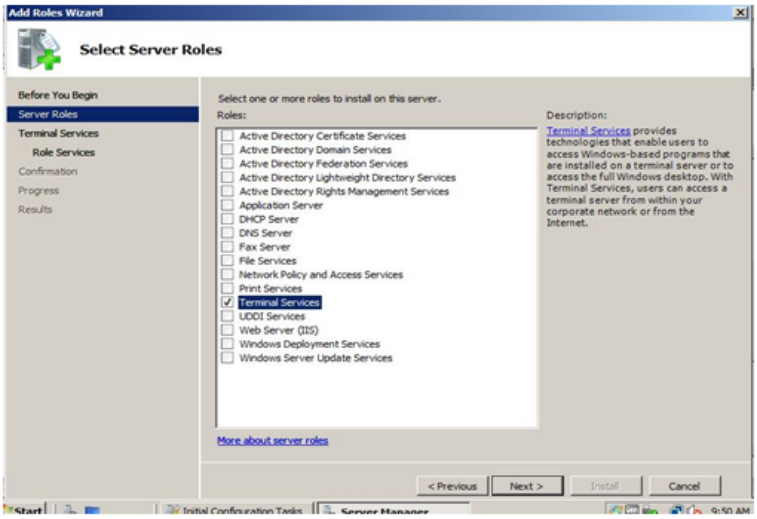

FIGURE 3.2 – Sélectionner les services de rôle

-Dans la page **Confirm Installation Selections** vérifiez les informations puis cliquer sur **Install**.

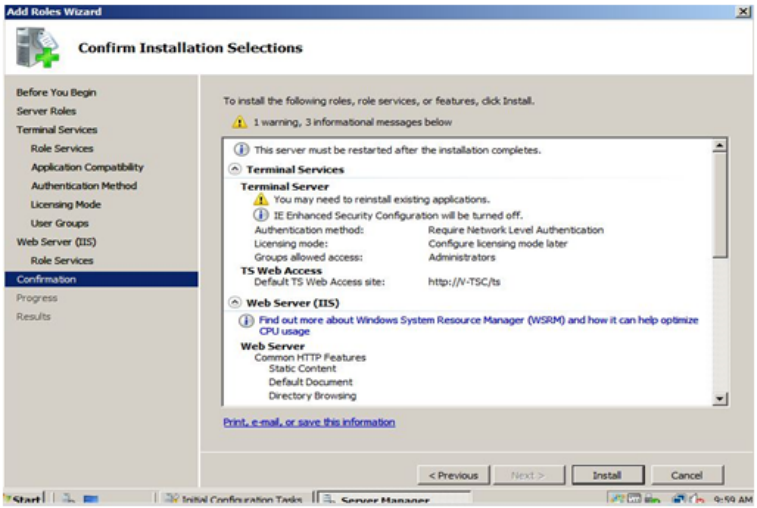

FIGURE 3.3 – Installation

-Dans la page Installation Resuls vérifiez es que tous est bien installer puis cliquer sur close puis sur Yes pour redémarrer le serveur.

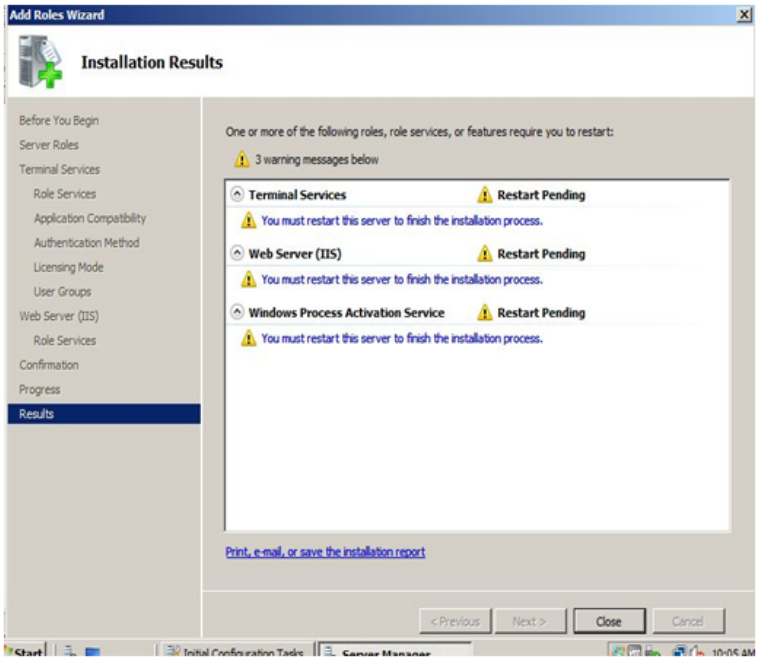

FIGURE 3.4 – Résultats de l'installation

3.9.1 Configuration du Remote App de V-TSC

Les programmes RemoteApp sont des programmes aux quels nous pouvons accéder à distance par le biais des services Terminal Server et qui apparaissent comme s'ils étaient exécutés sur l'ordinateur local de l'utilisateur final.
Les utilisateurs peuvent exécuter côte à côte des programmes RemoteApp et leurs programmes locaux.

La configuration minimale doit être Windows XP SP2 sur lesquels le nouveau client Connexion bureau à distance a été installé. Dans notre cas,nous allons configurer une application en Remote App et nous prendrons comme exemple une calculatrice.

-Pour aller à la page **TS RemoteApp Manager** cliquez sur **Start** puis **Administration tools** ensuite **Terminal Services** et enfin sur cliquez **TS RemoteApp Manager**.

-La fenêtre suivante s'ouvre. cliquez sur **Add Remote Apps** pour ajouter des programmes RemoteApp.

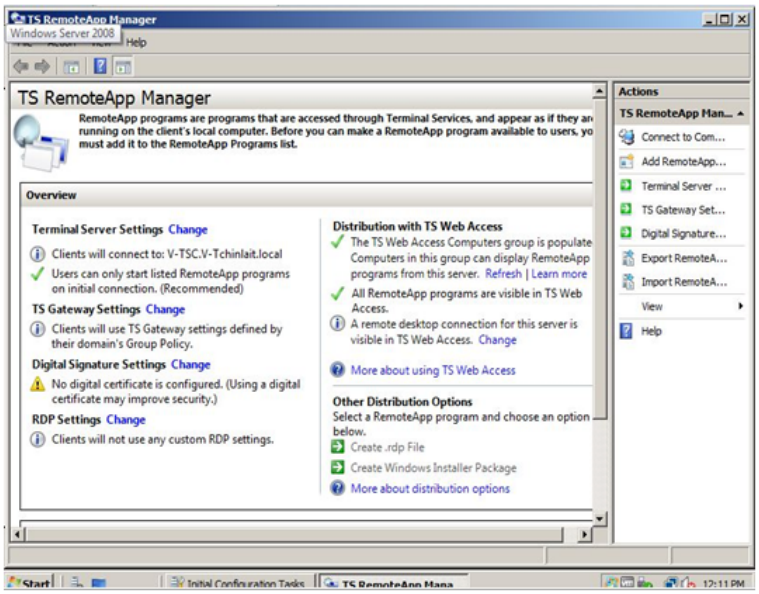

FIGURE 3.5 – Administration Remote App

-Dans la page Welcome to the **RemoteApp Wizard** lisez les informations puis cliquez sur **Next**.

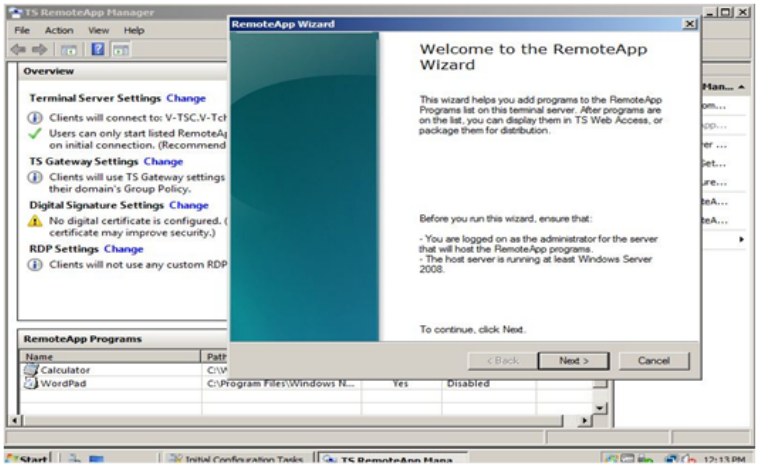

FIGURE 3.6 – Bienvenu dans l'assistant de RemoteApp

-Dans la page **Choose programs to add to the RemoteApp Programs list** activez la case à cocher correspondant à chaque programme à ajouter à la liste Programmes RemoteApp. Vous pouvez sélectionner plusieurs programmes, dans notre cas nous avons choisie la Calculatrice. Puis cliquez sur **Next**.

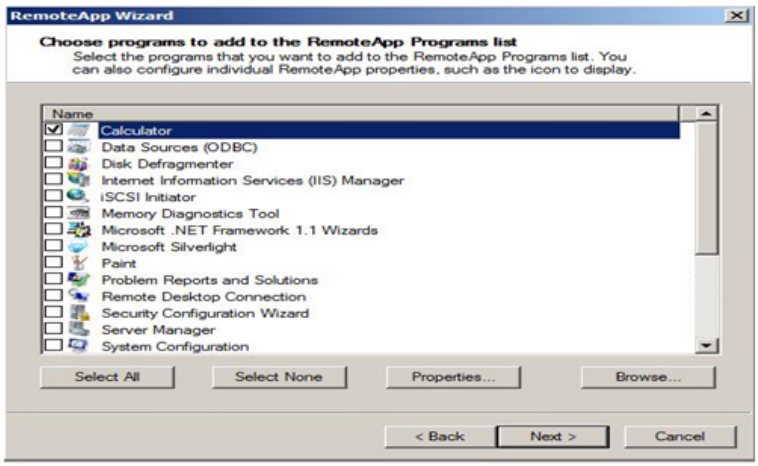

FIGURE 3.7 – Liste des programmes RemoteApp

-Dans la page **Review Settings** revoyez les paramètres puis cliquez sur **Finish**.

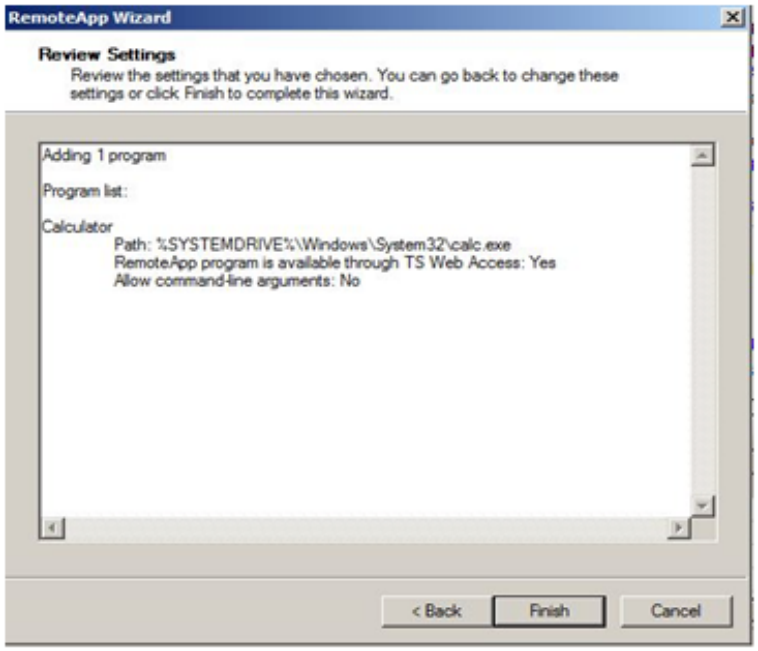

FIGURE 3.8 – Revoir les paramètres

-On peut maintenant voir la calculatrice apparaitre dans la liste des programmes RemoteApp. cliquez sur **Create.rdp File**

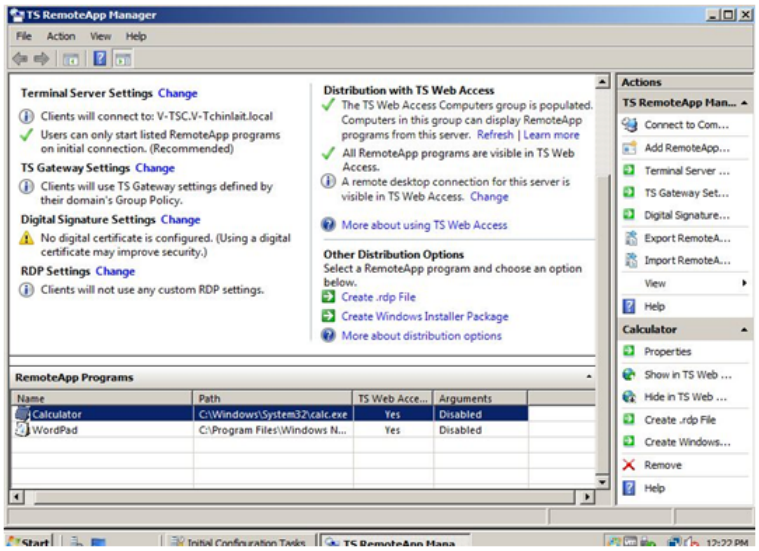

FIGURE 3.9 – Création de fichier rdp

-Dans la page **Welcome to the RemoteApp Wizard** cliquez sur **Next**

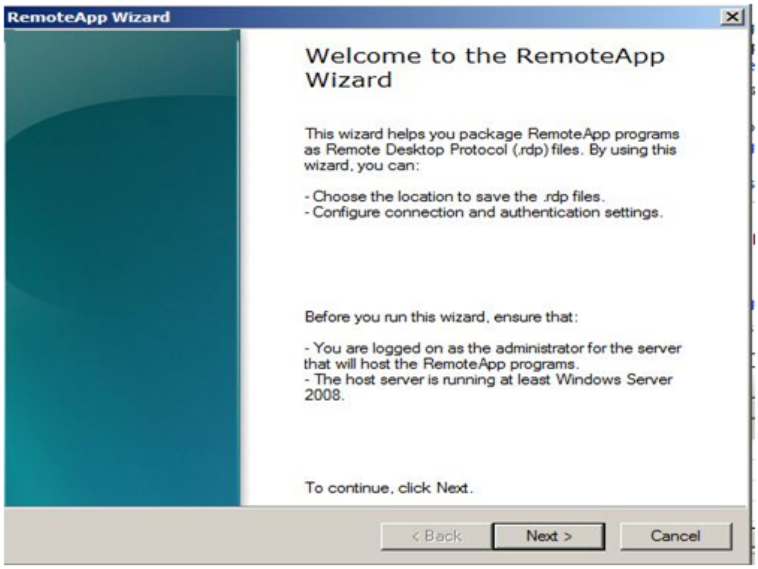

FIGURE 3.10 – Assistant RemoteApp

-Dans la page **Specify Packages Setings** cliquez sur **Next**.

-Le fichier "**.rdp**" va se placer dans le répértoire **Program Files** dans le dossier **packaged Program**.

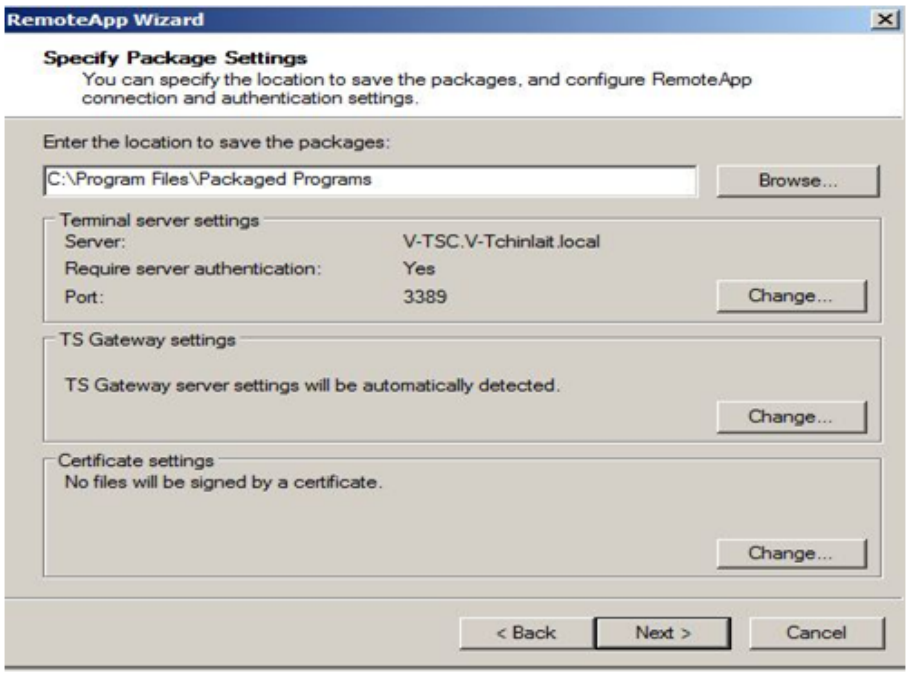

FIGURE 3.11 – Spécifications des paramètres des packages

-Dans la page **Review Setings** cliquez sur **Finish**.

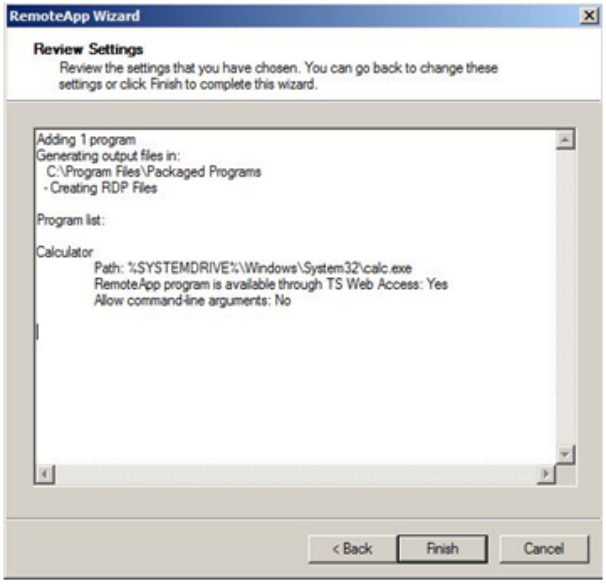

FIGURE 3.12 – Fin de la configuration RDP

-Le fichier **.rdp** est créé. Il suffit simplement de le mettre sur un poste client, pour que celui-ci ait accès à la calculatrice en Remote.

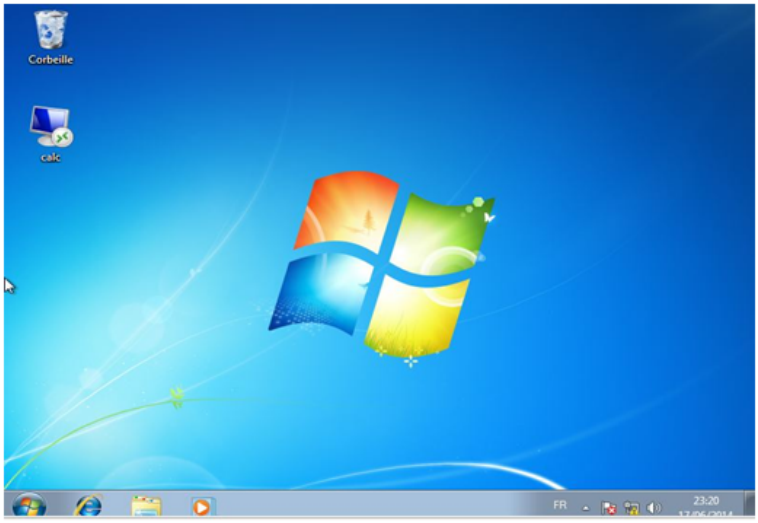

FIGURE 3.13 – Calc Remote App

-Pour lancer la calculatrice en Remote il suffit de faire un double clique sur le raccourci **calc** qui se trouve dans le bureau.

-Cette fenêtre va apparaitre puis cliquez sur **Connexion**.

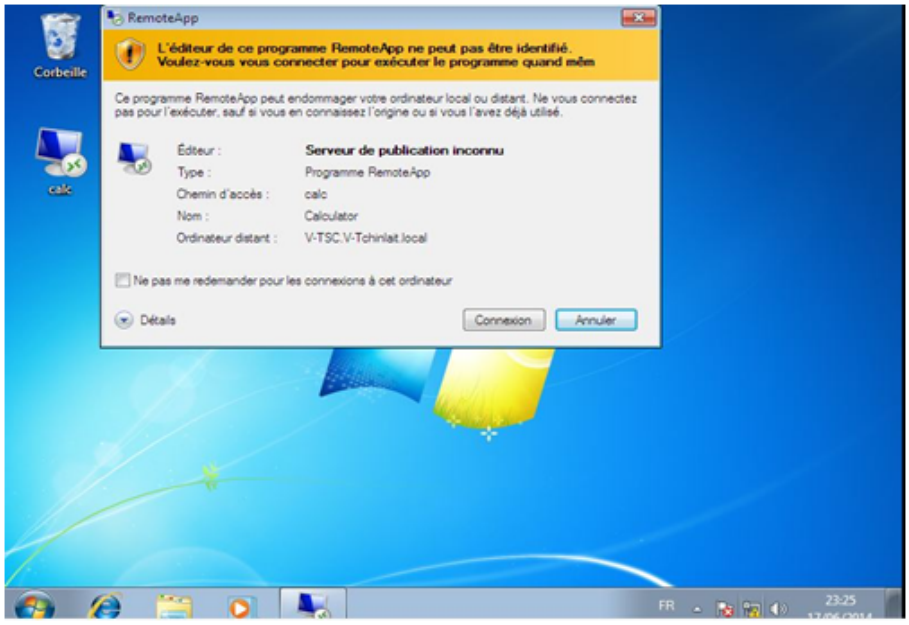

FIGURE 3.14 – Connexion Calc Remote App

-Pour se connecter a ce programme vous devez vos identifier avec votre nom d'utilisateur et mot de passe en suite vous cliquez sur **OK**.

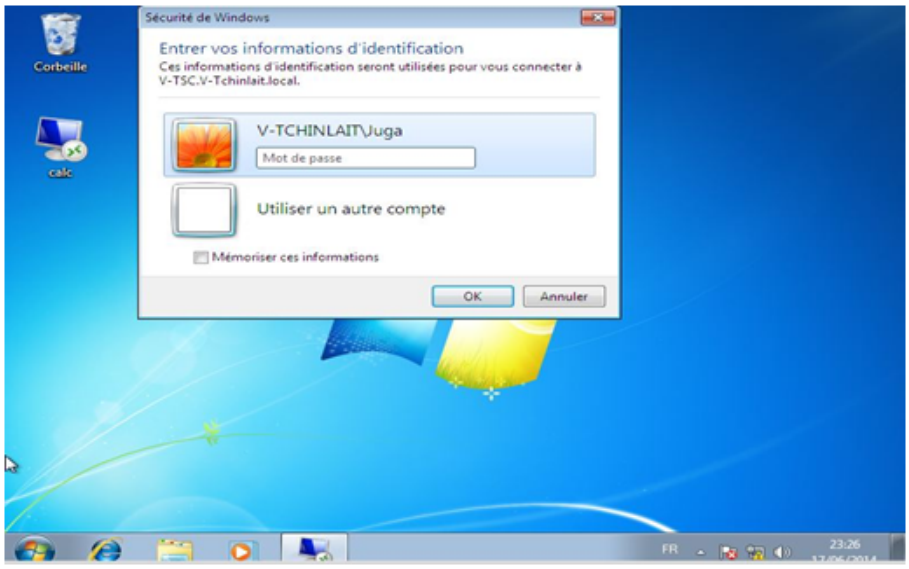

FIGURE 3.15 – Identification

-Il suffit d'attendre un moment pour le que la connexion s'établisse

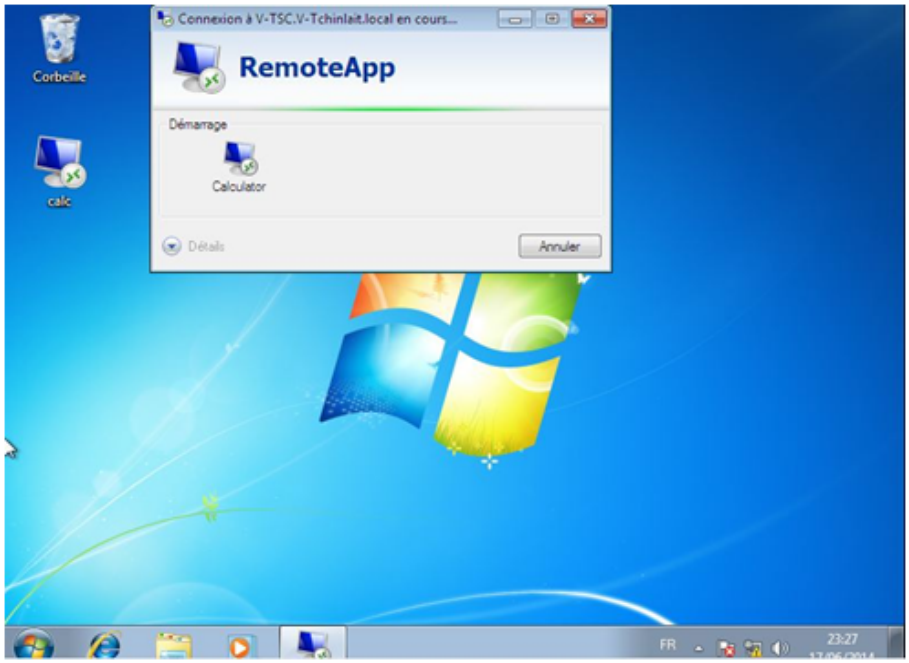

FIGURE 3.16 – Connexion Remote App

-La calculatrice est lancer .

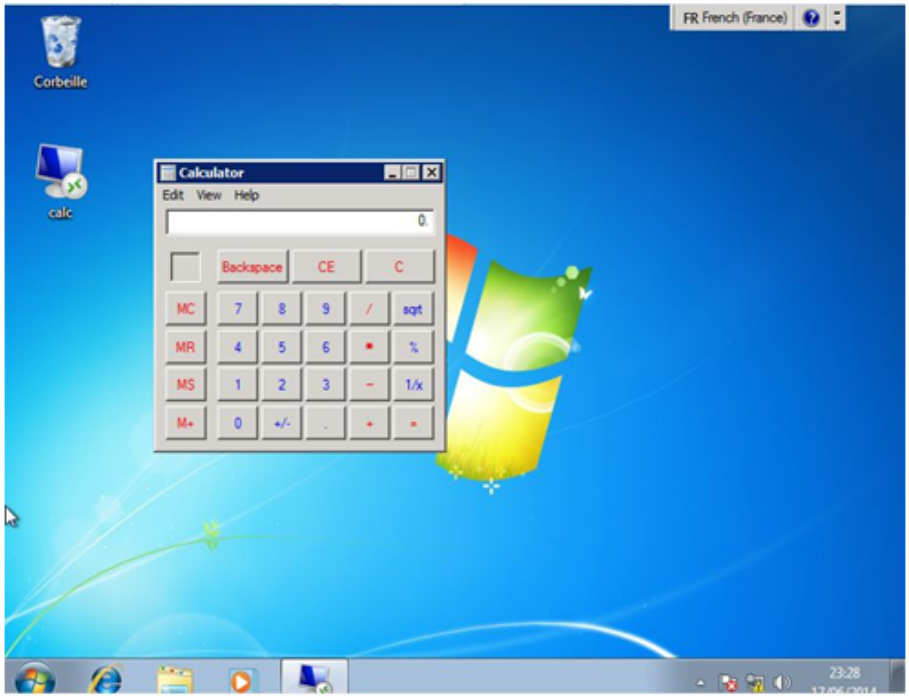

FIGURE 3.17 – Lancement de la calculatrice

3.9.2 Differents accès au serveur

Accès via le Web

Dans un navigateur internet (De préférence Internet Explorer) saisir l'adresse suivante **https ://NomDeVotreServeur/RDWeb/**. La fenêtre suivante s'ouvre, saisir un nom d'utilisateur et un mot de passe autorisés à se connecter aux services Bureau à distance, puis cliquer sur s'**inscrire**.

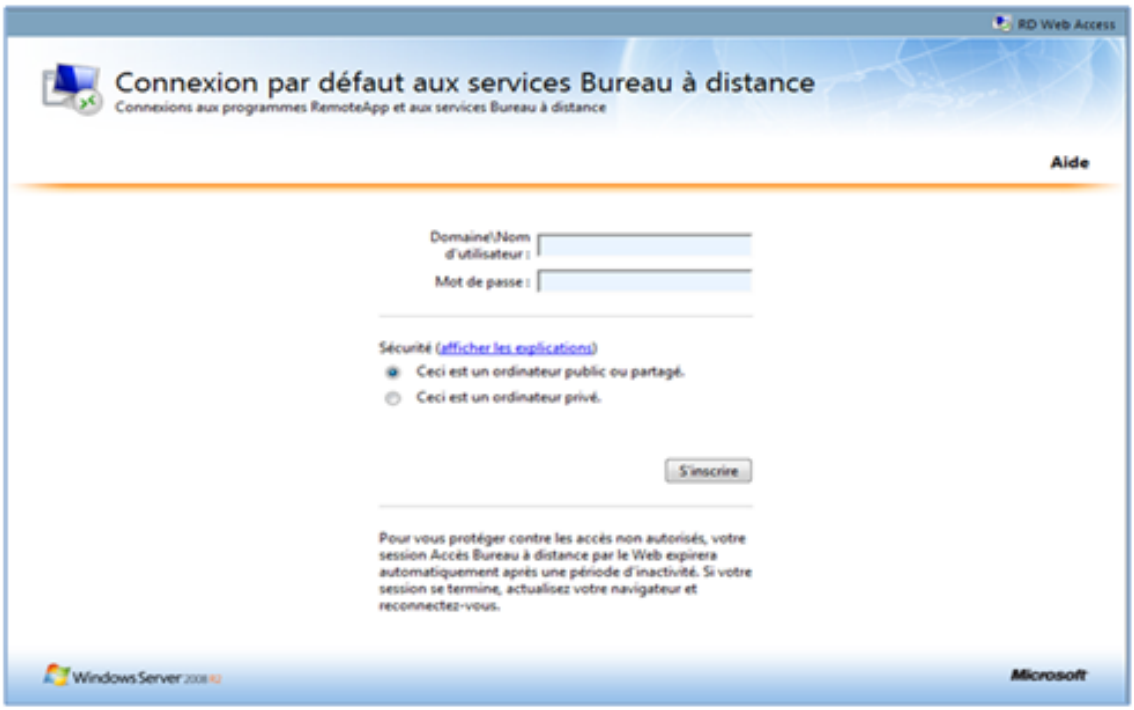

FIGURE 3.18 – Accès via Web

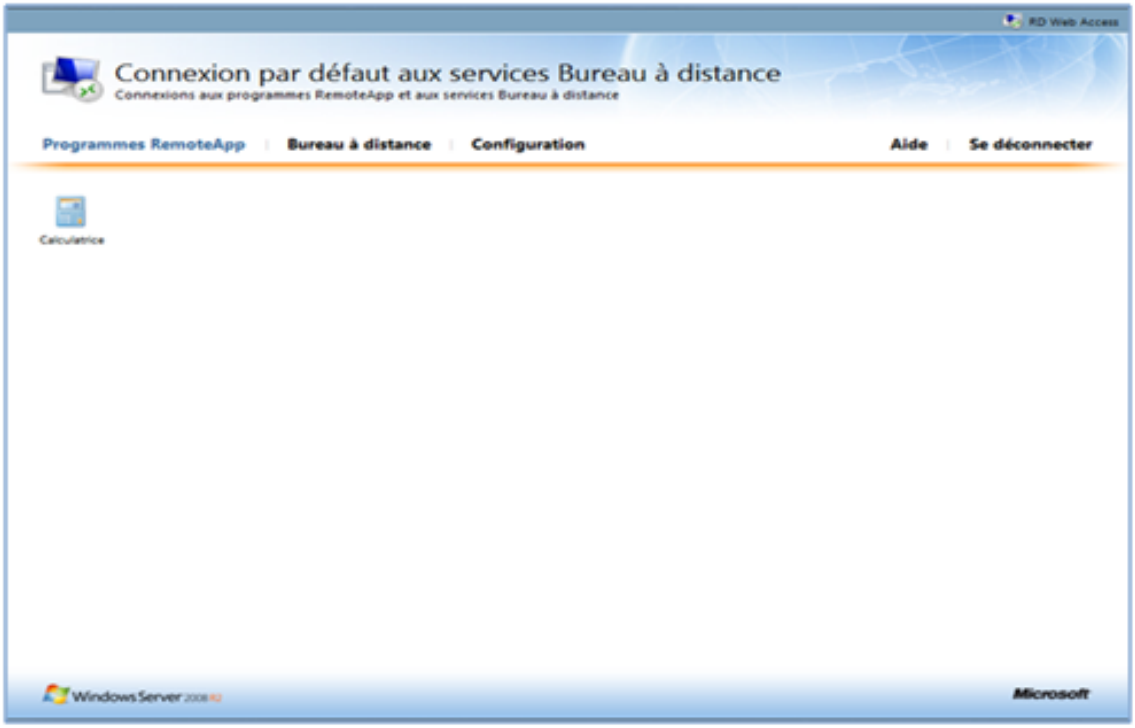

FIGURE 3.19 – Accès via Web 2

Accès via le bureau à distance

Pour accéder au programme RemoteApp via un accès a distance il suffit d'aller sur le bureau du système Window et cliquer sur le bouton **démarrer** puis **Tous les programmes** ensuite **Accessoires** et enfin sur **Connexion Bureau à Distance** et cliquez sur **Connexion**.

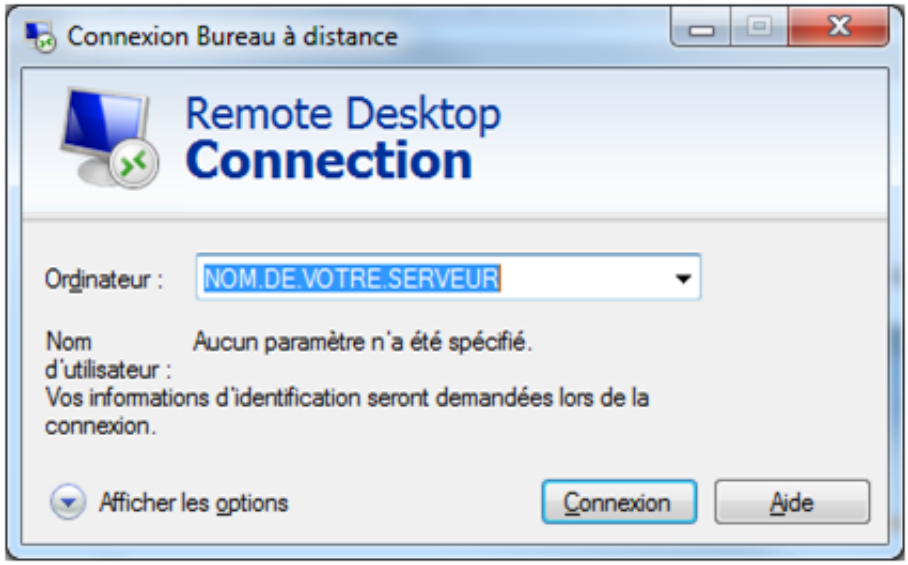

FIGURE 3.20 – Connexion au bureau à distance

Dans notre cas nous avons choisis cette dernière méthode, car plus simple à configurer.

3.9.3 Installation du Terminal Server V-TSA

Pour l'installation du Terminal Server V-TSA et la configuration de son RemoteApp nous avons suivie les même étapes que celles faites précédemment pour V-TSC.

3.10 Mise en place de la solution d'équilibrage de charge

NLB répartit le trafic sur plusieurs serveurs à l'aide du protocole réseau TCP/IP. nous pouvons utiliser NLB avec une batterie de serveurs Terminal Server pour équilibrer les performances d'un seul serveur Terminal Server en répartissant les sessions sur plusieurs serveurs.

Session Broker TS effectue un suivi des sessions déconnectées sur la batterie de serveurs Terminal Server et veille à ce que les utilisateurs soient reconnectés sur ces sessions. De plus,

Session Broker TS nous permet d'équilibrer la charge des sessions entre les serveurs Terminal Server d'une batterie de serveurs. Cette fonction est assurée par la fonctionnalité d'équilibrage de charge de Session Broker TS.
Toutefois, cette fonctionnalité d'équilibrage de charge basé sur les sessions requiert un mécanisme d'équilibrage de charge frontal pour distribuer les demandes de connexion initiales sur la batterie de serveurs Terminal Server. Nous pouvons utiliser un mécanisme d'équilibrage de charge tel que la répétition alternée DNS, NLB ou un équilibreur de charge matériel pour distribuer les demandes de connexion initiales.
En déployant NLB avec l'équilibrage de charge de Session Broker TS, nous pouvons tirer profit de l'équilibrage de charge basé sur le réseau et de la détection des serveurs ayant échoué de NLB, ainsi que de l'équilibrage de charge basé sur les sessions et de la limite du nombre de demandes d'ouverture de session en attente par serveur qui est disponible avec l'équilibrage de charge de Session Broker TS.

3.10.1 Configurer une batterie de serveurs Terminal Server avec Session Broker TS

Ce composant logiciel enfichable est inclus sur chaque serveur Terminal Server. Les serveurs Terminal Serveur qui constituent la batterie de serveurs Terminal Server communiquent avec le service Session Broker TS pour s'assurer que les utilisateurs soient reconnectés de façon transparente au serveur d'origine qui hébergeait les sessions dont ils ont été déconnectés. Le processus est le suivant :

1. Lorsque l'utilisateur ouvre une session sur la batterie de serveurs Terminal Server, le serveur Terminal serveur qui reçoit la demande d'ouverture de session client initiale adresse une requête au serveur Session Broker TS.
2. Le serveur Broker Session TS compare le nom d'utilisateur avec le contenu de sa base de données et envoie le résultat de l'opération au serveur qui a fait la requête. Deux cas de figure sont alors possibles :
   (a) S'il n'existe pas de sessions déconnectées pour cet utilisateur, l'ouverture de session se poursuit sur le serveur qui héberge la connexion initiale.
   (b) S'il existe une session déconnectée sur un autre serveur, la session cliente est transférée sur ce serveur et l'ouverture de session se poursuit.

Installer le service de rôle Session Broker TS sur V-TSA

1. Pour ouvrir le Server Manager cliquez sur **Start**, pointez sur **Administration tools**, puis cliquez sur **Server Manager**.
2. Dans notre cas le rôle des services Terminal Server est installé :
   (a) Sous **Roles Summary**, cliquez sur **Terminal Services**.
   (b) Sous **Role Services**,cliquez sur **Add Role Services**.
   (c) Dans la page **Select Role Services**, activez la case à cocher **TS Session Broker** puis cliquez sur **Next**.
3. Dans la page **Confirm Installation Selections**,cliquez sur **Install**.
4. Dans la page **Installation Results**, vérifiez que l'installation s'est correctement déroulée, puis cliquez sur **Close**.

-Pour ajouter un serveur Terminal Server au groupe local Ordinateurs annuaire de sessions

1. Sur le serveur TS Session Broker, cliquez sur **Start**, pointez sur **Administrative Tools** et cliquez sur **Computer Management** .
2. Dans le volet gauche, développez **Local Users and Groups**, puis cliquez sur **Groups**.
3. Dans le volet droit, cliquez avec le bouton droit sur le groupe **Session Directory Computers** , puis cliquez sur **Properties** .
4. Cliquez sur **Add**.
5. Dans la boîte de dialogue **Select Users, Computers or Groups** , cliquez sur **Object Types**.
6. Activez la case à cocher **Computers** et cliquez sur **OK**.
7. Recherchez le compte d'ordinateur et ajoutez-le pour chaque serveur Terminal Server que vous souhaitez ajouter.
8. Lorsque vous avez terminé, cliquez sur OK.

-Pour configurer les paramètres de Session Broker TS

1. Démarrez le composant logiciel enfichable Configuration des services Terminal Server. Pour cela, cliquez sur **Start**, pointez sur **Administrative Tools**,pointez sur **Terminal Services**, puis cliquez sur **Terminal Services Configuration**.
2. Dans la zone **Edit settings**, sous **TS Session Broker**, double-cliquez **Member of farm in TS Session Broker**.

3. Sous l'onglet **TS Session Broker**, activez la case à cocher **Join a farm in TS Session Broker**.
4. Dans la zone **TS Session Broker server IP address or name**, tapez le nom du serveur Session Broker TS : V-TSA.
5. Dans la zone de texte **Farm name in TS Session Broker**, tapez le nom de la batterie que vous voulez joindre dans Session Broker TS. : FARM1
6. Pour participer à l'équilibrage de charge de Session Broker TS, procédez comme suit :
   (a) Activez la case à cocher Participer à l'équilibrage de charge Session Broker. L'activation de cette case à cocher tirera profit de l'équilibrage de charge basé sur les sessions de Session Broker TS, ainsi que de la limite du nombre de demandes d'ouverture de session en attente par serveur.
   (b) Nous pouvons également modifier le poids du serveur dans la zone Poids relatif du serveur dans la batterie. En affectant une valeur de poids relatif, nous pouvons aider à répartir la charge entre les serveurs plus ou moins puissants de la batterie. La valeur par défaut est 100. Le poids du serveur est relatif. Par conséquent, si nous affectons la valeur 100 à un serveur et la valeur 200 à un autre, le serveur de poids relatif 200 recevra deux fois plus de sessions. Nous donnerons la même valeur.
7. Cliquez sur OK.

3.10.2 Installer Network Load Balancing

-Pour ouvrir l'Assistant Ajout de fonctionnalités et installer NLB

1. Cliquez sur **Start**, pointez sur **Administrative Tools**, puis cliquez sur **Server Manager**. Dans la zone **Features Summary** de la fenêtre principale du **Server Manager**, cliquez sur **Add Features**. – ou – Dans la zone **Customize this server** de la fenêtre Initial Configuration Tasks, cliquez sur Add Features.
2. Dans l'Assistant **Add Features**, activez la case à cocher en regard de l'option **Network Load Balancing**.

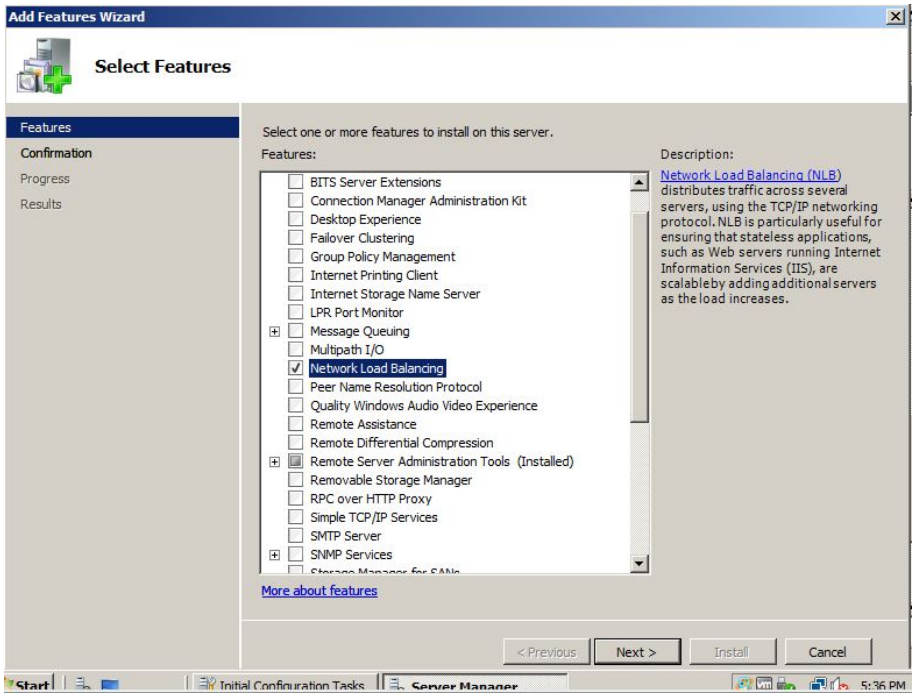

FIGURE 3.21 – Installation de la fonction NLB

3. Cliquez sur **Install**.

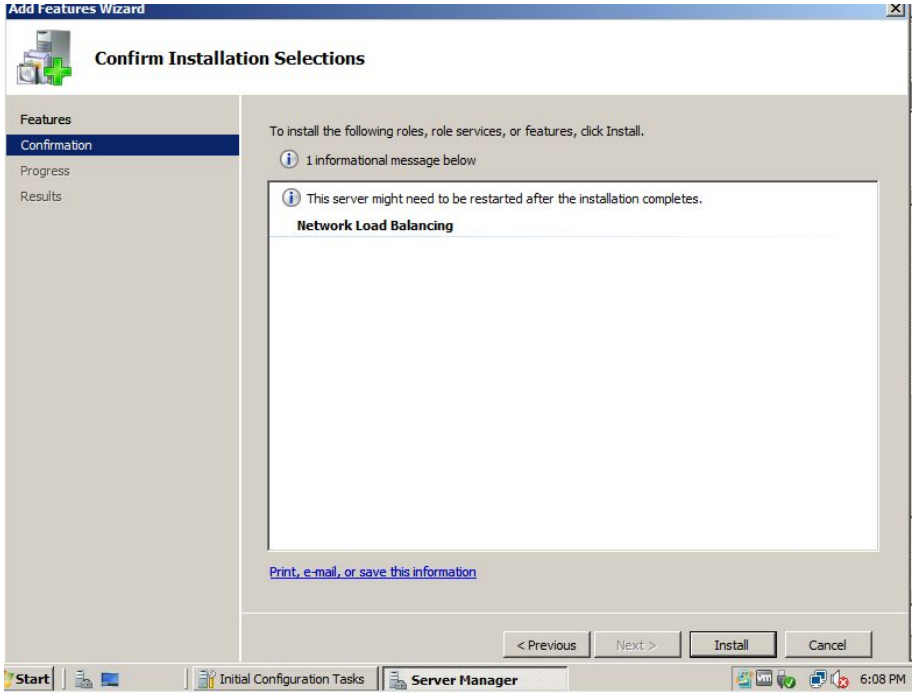

FIGURE 3.22 – Lancement de l'installation

4. Cliquez sur **Close**.

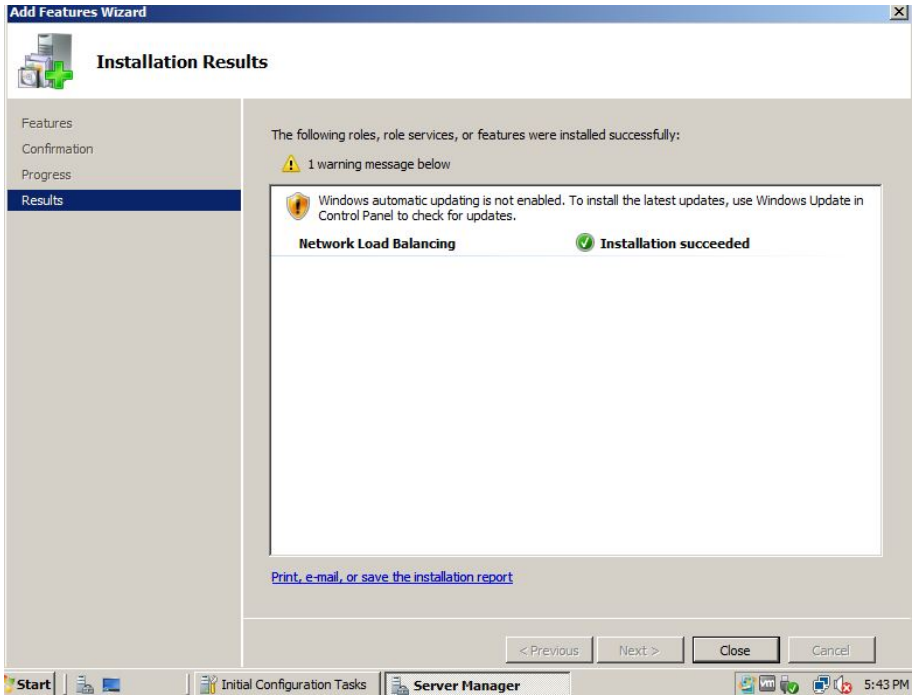

FIGURE 3.23 – Fin de l'installation

3.10.3 Creation et configuration du Cluster

1. Pour ouvrir le Gestionnaire d'équilibrage de la charge réseau, cliquez sur **Start**, puis sur **Administrative Tools** et sur **Network Load Balancing Manager**. Nous pouvons également ouvrir le Gestionnaire d'équilibrage de la charge réseau en tapant **Nlbmgr** à partir d'une invite de commandes.
2. Cliquez avec le bouton droit sur **Network Load Balancing Clusters**, puis cliquez sur **New Cluster**.

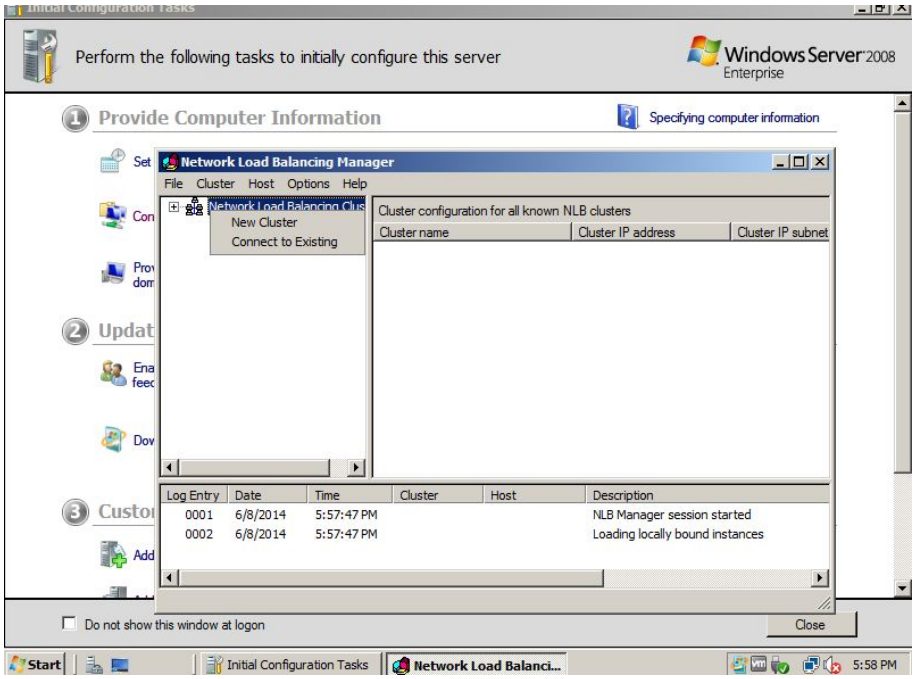

FIGURE 3.24 – Ajout du cluster

3. Établir une connexion avec l'hôte qui doit faire partie du nouveau cluster. Dans **Host**, entrez le nom de l'hôte V-TSA, puis cliquez sur **Connect**.

4. Sélectionnez l'interface que nous souhaitons utiliser avec le cluster, puis cliquez sur **Next**. (L'interface héberge l'adresse IP virtuelle et reçoit le trafic client pour équilibrer la charge.)

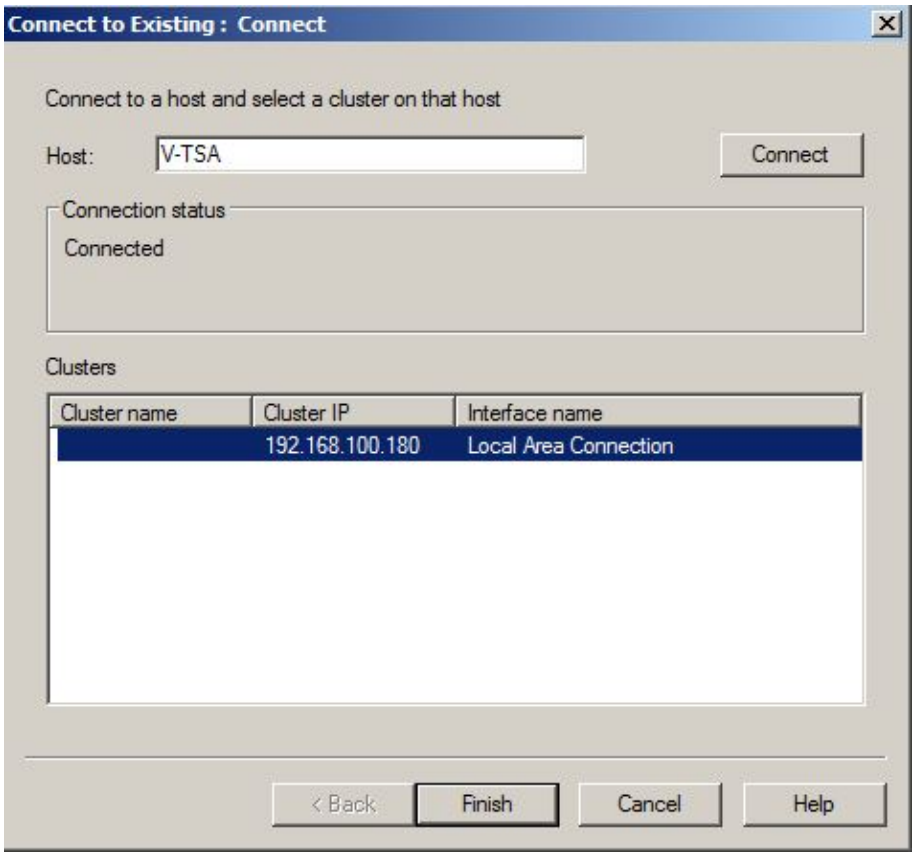

FIGURE 3.25 – Ajout du l'hote

5. Dans **Host Parameters** de l'hôte, sélectionnez une valeur dans **Priority (Unique host identifier)**. Ce paramètre spécifie un identificateur unique pour chaque hôte. L'hôte dont la priorité numérique est la plus basse parmi les membres actuels du cluster traite tout le trafic réseau du cluster qui n'est pas couvert par une règle de port. Nous pouvez remplacer ces priorités ou équilibrer la charge pour des étendues de ports spécifiques en définissant des règles sous **Port rules** de la boîte de dialogue **Network Load Balancing Properties**. Cliquez sur **Next** pour continuer.

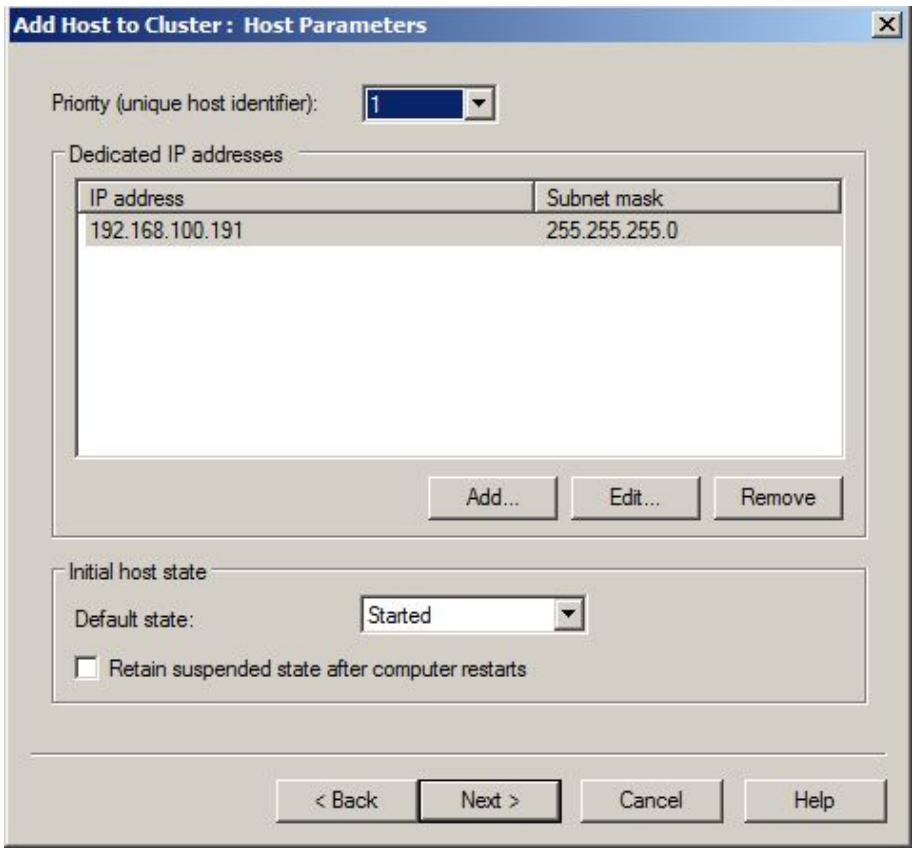

FIGURE 3.26 – Ajout du l'hote

6. Dans Adresses IP de cluster, cliquez sur **Add** et tapez l'adresse IP de cluster que partagent tous les hôtes du cluster 192.168.100.180. NLB ajoute cette adresse IP à la pile TCP/IP sur l'interface sélectionnée de tous les hôtes choisis pour faire partie du cluster. NLB ne prend pas en charge le protocole DHCP (Dynamic Host Configuration Protocol). Il désactive le protocole DHCP sur chaque interface qu'il configure, donc les adresses IP doivent être statiques. Cliquez sur **Next** pour continuer.

7. Dans Paramètres de cluster, tapez des valeurs dans Adresse IP et Masque de sous-réseau (pour les adresses IPv6, la valeur du masque de sous-réseau n'est pas requise). Un nom Internet complet n'est pas nécessaire lorsque NLB est utilisé avec les services Terminal Server.

8. Dans Mode d'opération du cluster, cliquez sur **Unicast** pour spécifier qu'une adresse de contrôle d'accès au média (MAC, Media Access Control) de monodiffusion doit être utilisée pour les opérations du cluster. En mode de monodiffusion, l'adresse MAC du cluster est attribuée à la carte réseau de l'ordinateur et l'adresse MAC intégrée de la carte réseau n'est pas utilisée. Il est recommandé d'accepter les paramètres de monodiffusion par défaut. Cliquez sur **Next** pour continuer.

9. Dans Règles du port, cliquer sur **Edit** pour modifier les règles de port par défaut. Configurez les règles de la manière suivante : Dans Étendue du port, spécifier une étendue compris entre 3389 et 3389 de façon à ce que la nouvelle règle s'applique uniquement au trafic RDP.

   Dans Protocoles, sélectionner TCP comme protocole TCP/IP spécifique devant être couvert par une règle de port. Seul le trafic réseau du protocole spécifié est concerné par la règle. Le trafic non concerné par la règle de port est traité par l'hôte par défaut.

   Dans Mode de filtrage, sélectionner **Multiple host**, ce qui spécifie que plusieurs hôtes traitent le trafic réseau pour cette règle de port. Dans Affinité (qui s'applique uniquement au mode de filtrage Hôte multiple), sélectionner **None** si nous envisageons d'utiliser Session Broker TS. Dans le cas contraire, sélectionnez Single.

10. Cliquez sur **Finish** pour créer le cluster.

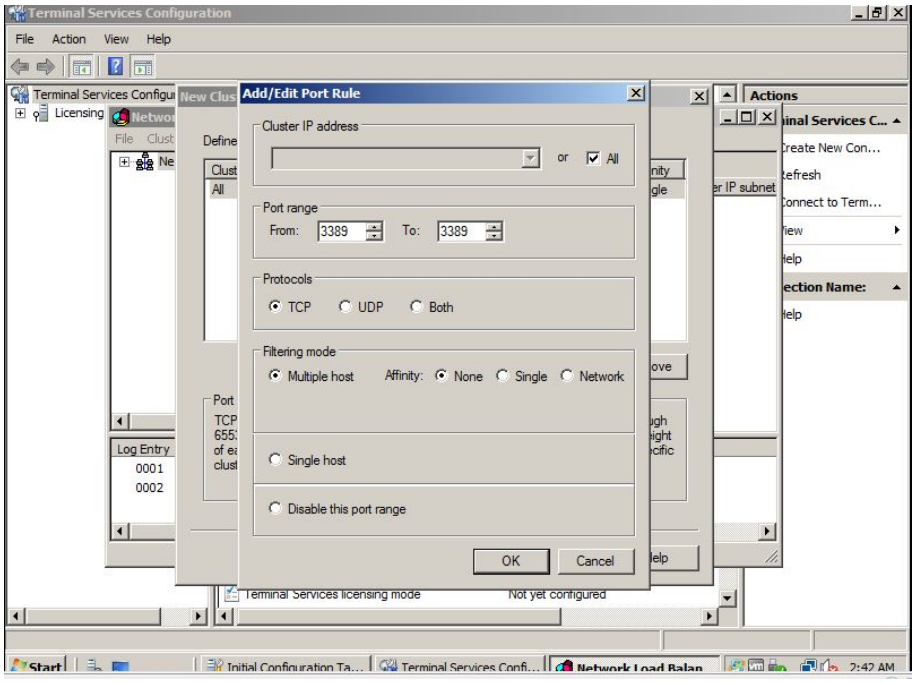

FIGURE 3.27 – Règles du port

11. Pour ajouter d'autres hôtes au cluster, cliquer avec le bouton droit sur le **new cluster**, puis cliquer sur **Add Host to Cluster**. Configurer les paramètres de l'hôte (notamment la priorité de l'hôte et les adresses IP dédiées) pour les hôtes supplémentaires en suivant les mêmes instructions que celles que nous avons utilisées pour configurer l'hôte initial. Étant donné que nous ajoutons des hôtes à un cluster déjà configuré, tout les paramètres à l'échelle du cluster restent les mêmes.

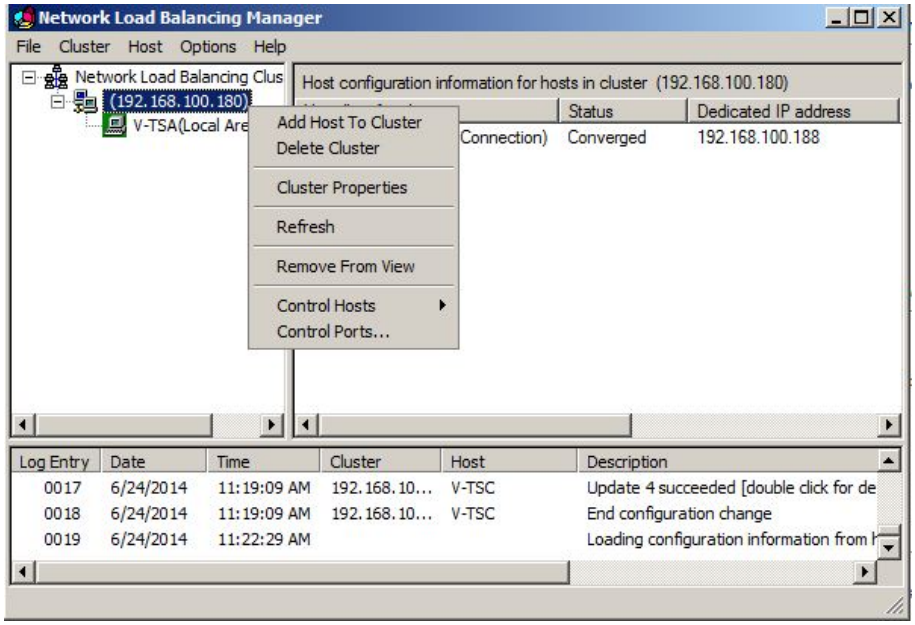

FIGURE 3.28 – Ajout de noeud

12. le résultat de l'installation sera comme montrer dans la figure suivante.

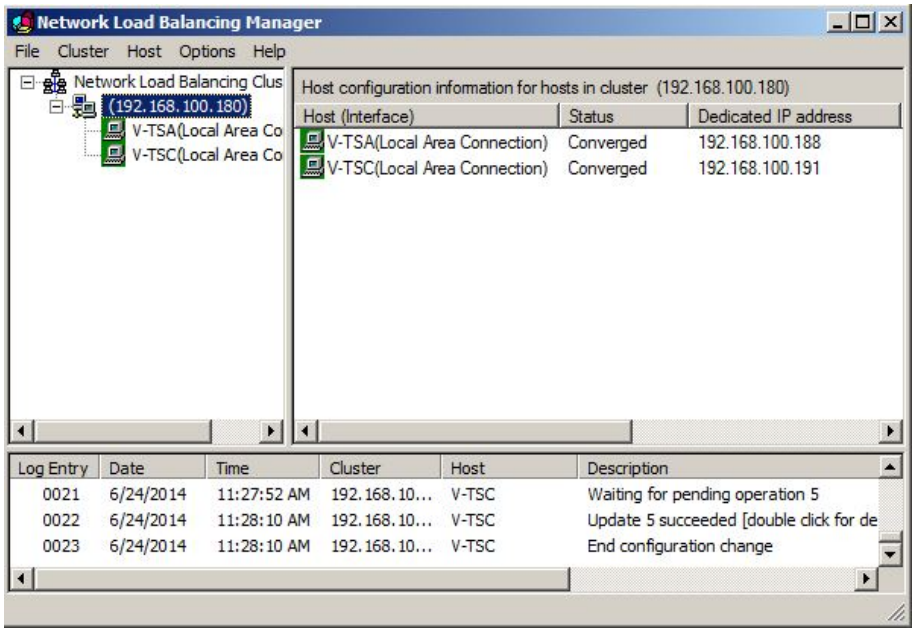

FIGURE 3.29 – Resultat de l'installation

3.11 Test

3.11.1 Test de fonctionnement du NLB

Taper à l'invite de commande **nlb dispaly all** sur tous les nœuds du cluster. Nous y trouvons le statut de chaque nœud.

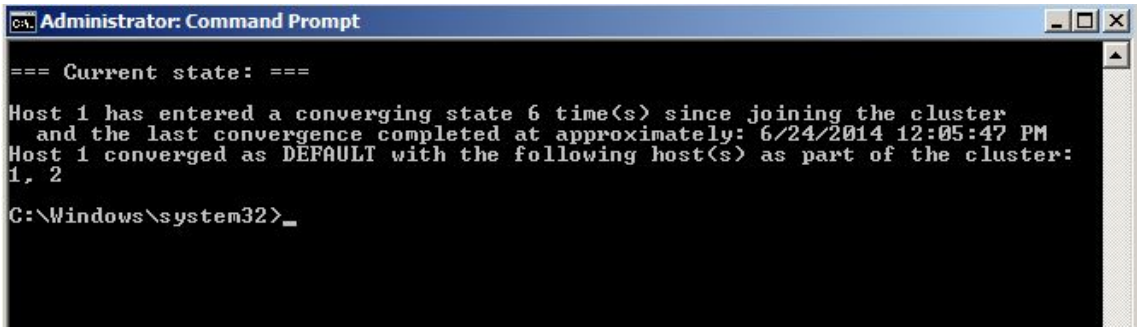

FIGURE 3.30 – Statut du noeud V-TSC

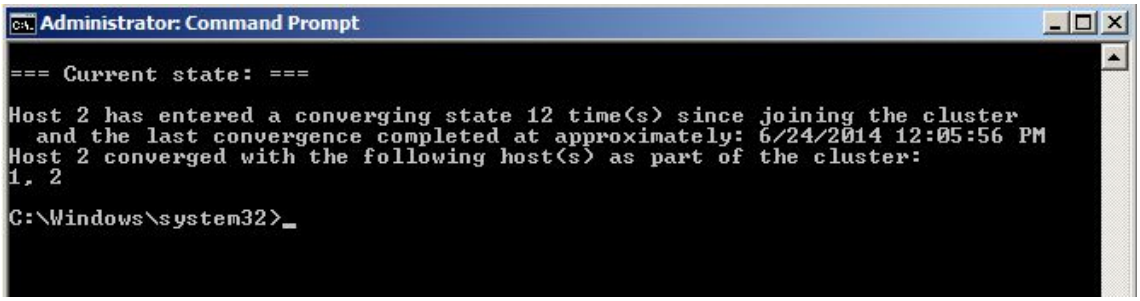

FIGURE 3.31 – Statut du noeud V-TSA

Ici le nœud 1 a convergé en tant que hôte par défaut du cluster alors que le nœud 2 est un simple membre du cluster. Si les deux nœuds avaient convergé comme hôte par défaut, cela aurait indiqué un problème de communication entre les nœuds.

3.11.2 Test de basculement du NLB

Pour commencer le test nous allons lancer le programme Remot App depuis la machine cliente.

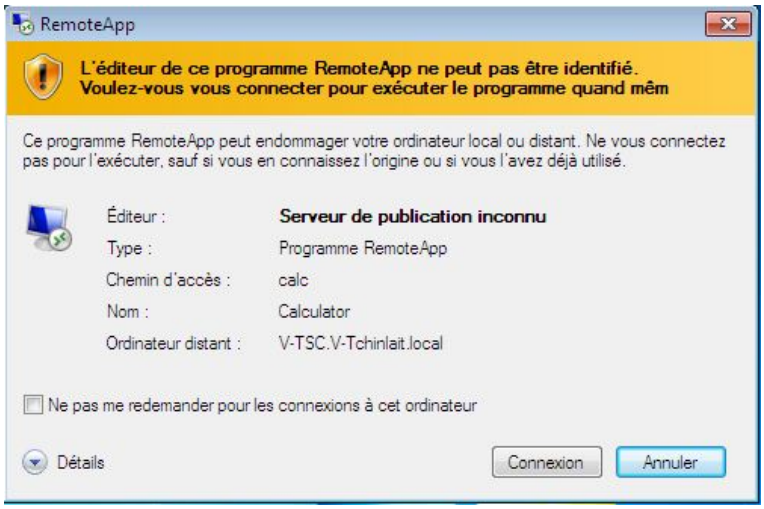

FIGURE 3.32 – Connexion

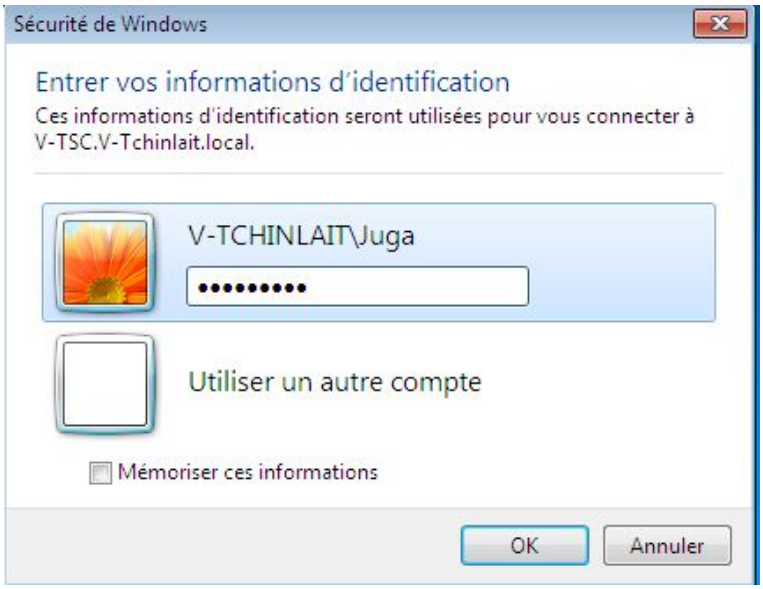

FIGURE 3.33 – Athentification

FIGURE 3.34 – Lancement du programme Remote App

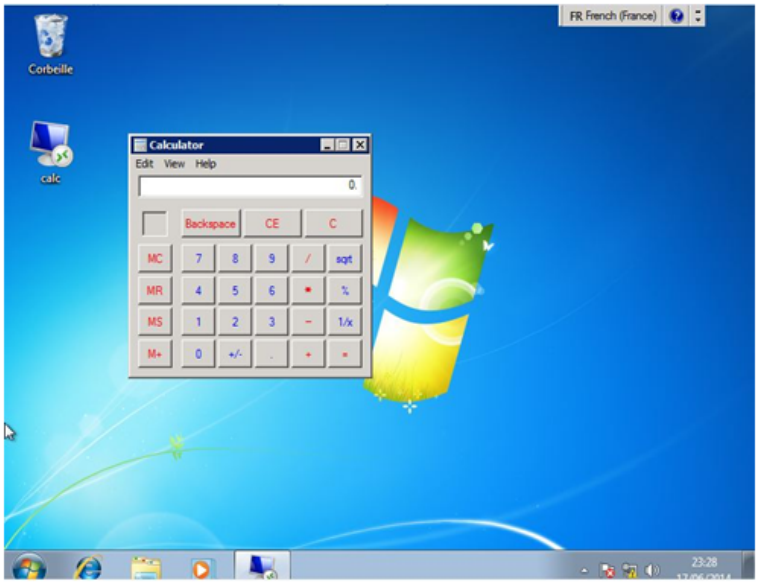

FIGURE 3.35 – Calculatrice Remote App

Taper à l'invite de commande **netstat** sur la machine cliente. Nous y trouvons les connexion TCP en cours qui démontre que le client est connecté sur V-TSC.

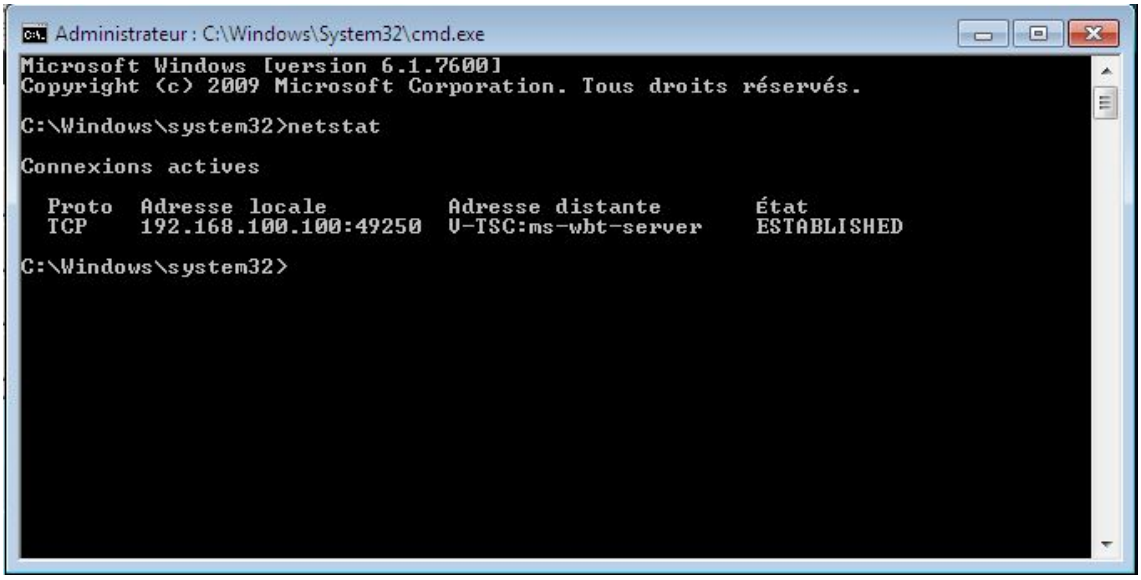

FIGURE 3.36 – Connexion TCP

A ce moment la, nous arretons la serveur V-TSC.

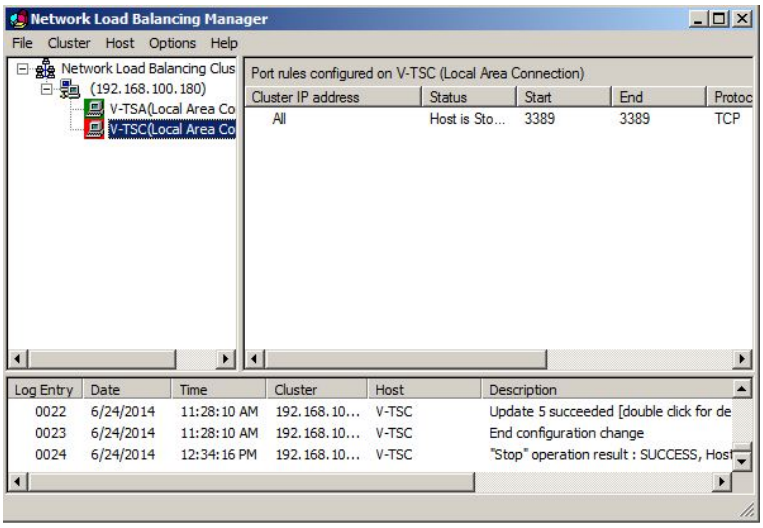

FIGURE 3.37 – Arrêt du Serveur V-TSC

Taper à l'invite de commande **netstat** sur la machine cliente. Nous y trouvons les connexion TCP en cours qui démontre que le client est connecté sur V-TSA.

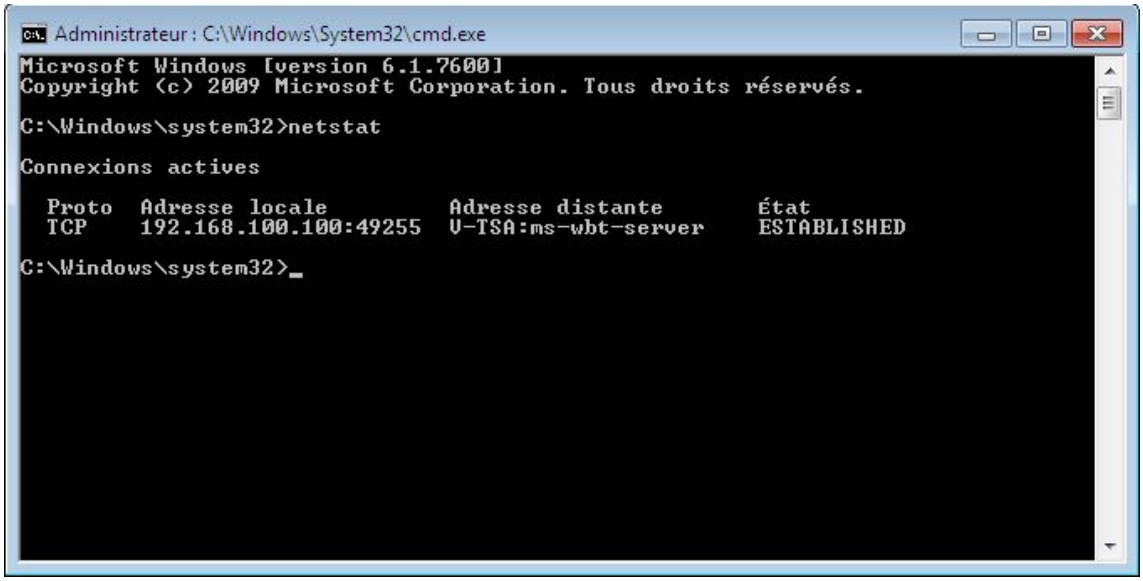

FIGURE 3.38 – Nouvelle connexion TCP

3.12 Conclusion

La solution apportée n'est certes pas optimale, mais c'est une étape que nous considérons importantes, voir inévitable que l'entreprise devra mettre en place dans les plus bref délais afin d'optimiser son réseau informatique.

Conclusion générale

Le travail que nous avons accompli a pour principal objectif la mise en œuvre d'une solution de tolérance aux pannes au sein de l'entreprise TCHIN LAIT " CANDIA ". Ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde et plus pratique sur l'importance de la haute disponibilité dans une entreprise.

Pour mettre en œuvre ce projet, nous avons été amenées dans un premier lieu à élargir nos connaissances dans le domaine systèmes informatiques dans une entreprise, ainsi que la sécurité puis étudier l'existant au niveau de l'organisme d'accueil.

Afin d'accomplir notre travail et d'aboutir au résultat escompté, nous avons choisi d'utiliser Windows server 2008 du fait de son utilisation au niveau des serveurs de TCHIN LAIT que nous installerons sur VmWare pour les différents avantages qu'il présente.

La réalisation de ce projet a été bénéfique et fructueuse pour nous dans le sens où il nous a permis d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles pour nous à l'avenir.

Bibliographie

[B1] : TCHIN-LAIT, "Document d'entreprise " ,2013.

[B2] : S.LOHIER et A.QUIDELLEUR, " Le réseau Internet des services aux infrastructures " DUNOD 2010.

[B3] : J-F. CARPENTIER, " La sécurité informatique dans la petite entreprise " 2eme édition, ENI 2012.

[B4] : S. GHERNOUATI-HELIE, " Sécurité informatique et réseaux " 3eme édition, DUNOD 2011.

[B5] : C.RUSSEL et S.CRAWFORD, " WINDOWS SERVER 2008 Volume 2" DUNOD 2008.

[B6] : J-F. PILLOU et J-P. BAY " Tout sur la sécurité informatique " 2eme édition, DUNOD 2010.

[B7] : R. SEBASTIEN, " LINUX solution de haute disponibilité " 1ere édition, ENI 2010.

[B8] : C.ORTEGA, Y.BOUVIER, T.DEMAN, M.CHATEAU, F.ELMALEH S.NEILD " Windows server 2008 R2 administration avancé " 1ere édition, ENI janvier 2011.

[B9] : D.COLOMBANI " Déployer un cluster haute disponibilité Windows avec VMware" 1ere édition, Focus avril 2009.

[B10] : E.MAILLÉ ” VMware vSphere 4” 1ere édition, ENI janvier 2010.

[B11] : P.GILLET ” Virtualisation des systèmes d’information avec VMware” 1ere édition, ENI janvier 2010.

Webographie

[W1] : http ://facebook.com/tchinlait consulté en Février 2014.

[W2] : http ://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzarj/ consulté en Mars 2014.

[W3] : http ://doc.ubuntu-fr.org/ consulté en Avril 2014.

[W4] : http ://www.vmware.com/fr/products/workstation consulté en Mars 2014.

[W5] : http ://www.microsoft.com/fr-fr/download/details.aspx ?id=5023 consulté en Mars 2014

Annexe A

VMware Workstation ?

Pourquoi choisir VMware Workstation ?

Primé plus de 50 fois, VMware Workstation est reconnu pour sa large prise en charge de systèmes d'exploitation, son environnement utilisateur riche, son ensemble complet de fonctionnalités et ses hautes performances.
VMware Workstation est conçu pour les professionnels qui utilisent des machines virtuelles dans le cadre de leur travail [**B10**].

Repousser les Limites de la Productivité

La figure ci-dessous représente l'interface de Vmware [**W4**].

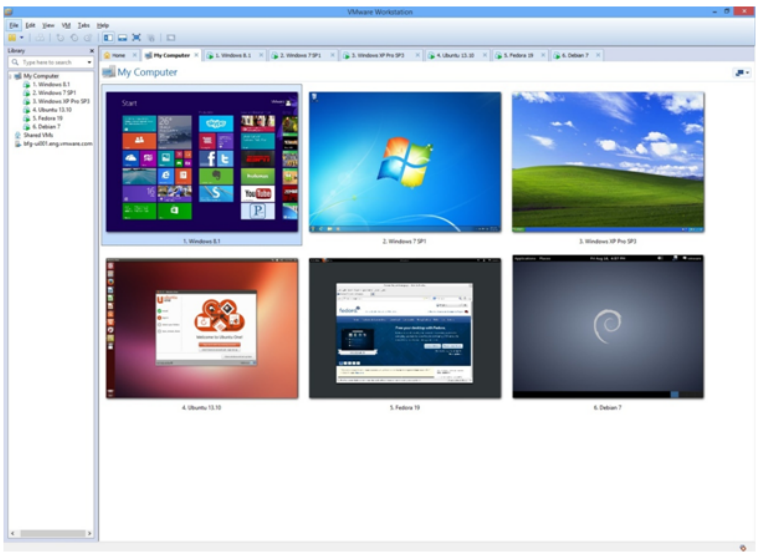

Figure 3.39 – Vmware workstation, My Computer

• Exécutez vos applications sur plusieurs systèmes d'exploitation en même temps, notamment Linux et Windows, et sur le même PC, sans redémarrer.

• Évaluez et testez de nouveaux systèmes d'exploitation, applications et correctifs dans un environnement isolé.

• Effectuez des démonstrations d'applications logicielles complexes sur un même ordinateur portable, de manière fiable et reproductible.

• Effectuez des démonstrations d'applications logicielles complexes sur un même ordinateur portable, de manière fiable et reproductible.

• Concevez des architectures de référence aux fins d'évaluation avant un déploiement en production.

• Déplacez vos machines virtuelles de votre PC vers vSphere ou le Cloud par simple glisser-déposer [**B10**].

Accessible partout et à tout moment

la figure suivante représente l'accébilité aux machines virtuels [**W4**].

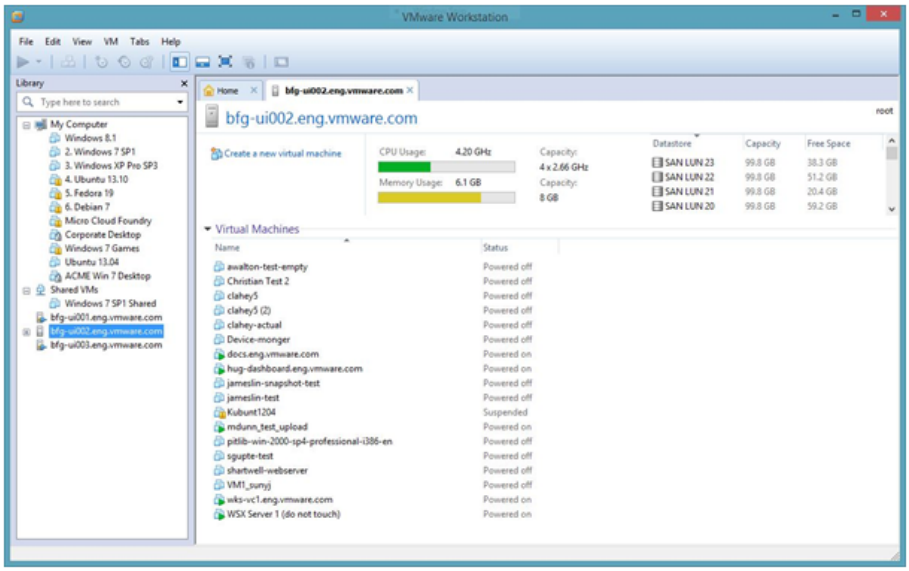

FIGURE 3.40 – Vmware workstation, connectivity

Accédez en toute transparence aux machines virtuelles dont vous avez besoin, quel que soit l'endroit où elles résident.

• Connectez-vous à distance aux machines virtuelles qui s'exécutent sur une autre instance de VMware Workstation ou sur VMware vSphere.

• L'interface Web de Workstation vous permet d'accéder aux machines virtuelles locales et hébergées sur un serveur depuis un PC, un smartphone, une tablette ou tout autre périphérique doté d'un navigateur récent.
Aucun plug-in n'est nécessaire [**B11**].

Exécuter les applications les plus gourmandes

La figure suivante représente l'exécution du logiciel google earth sur Vmware [**W4**].

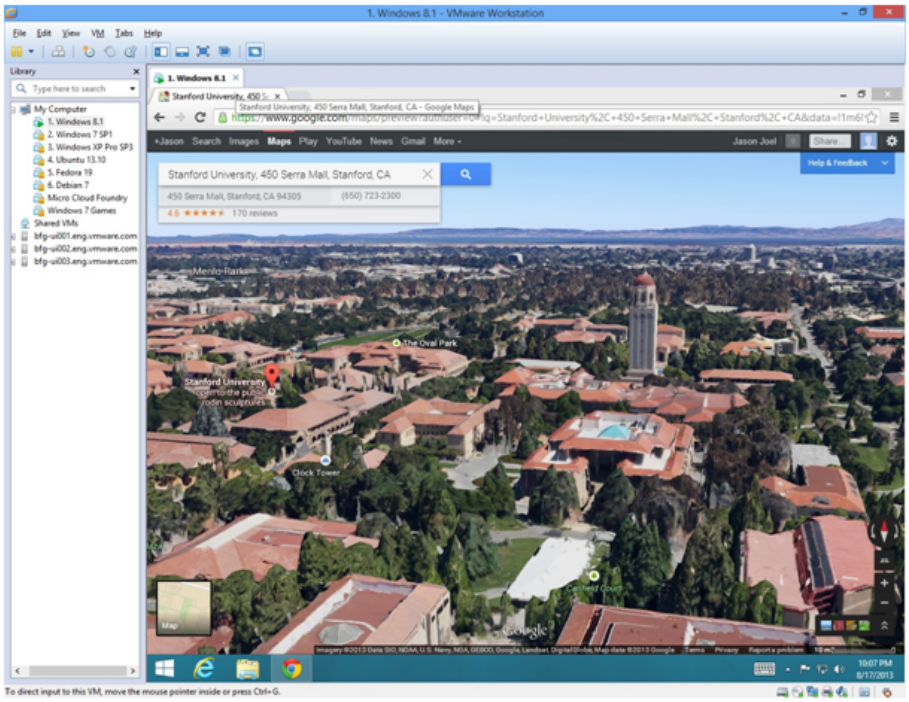

FIGURE 3.41 – Vmware workstation, applications

VMware Workstation exploite le matériel le plus récent pour répliquer les environnements de serveurs, postes de travail et tablettes.

• Créez des machines virtuelles avec un maximum de 16 processeurs virtuels ou 16 cœurs de processeur virtuels, des disques virtuels de 8 To et 64 Go de mémoire par machine virtuelle.

• Prise en charge du son HD avec effet Surround 7.1, USB 3.0 et Bluetooth.

• Processeurs virtuels incluant les extensions de virtualisation.

• Contrôleurs de disques virtuels SCSI, SATA et IDE.

• Premier logiciel à fournir un magnétomètre, un accéléromètre et un gyroscope virtuels dans une machine virtuelle[**B11**].

Machines virtuelles restreintes

La figure suivante représente la sécurité des machines virtuels sur Vmware [**W4**].

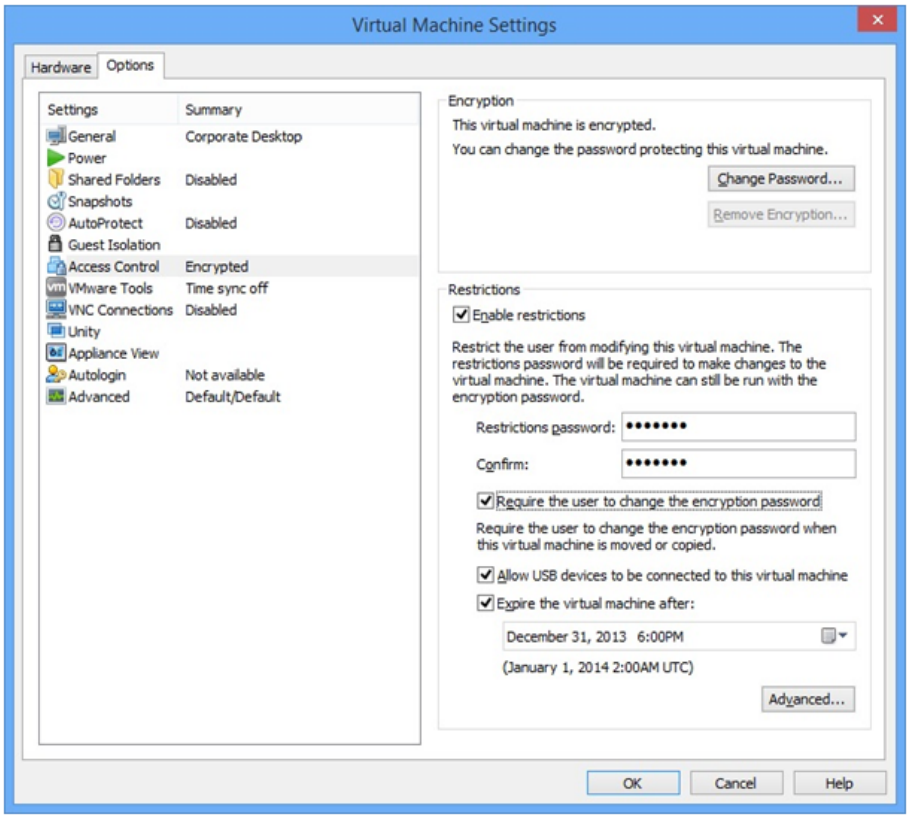

FIGURE 3.42 – Vmware workstation, restriction de machine

Créez des machines virtuelles cryptées qui demandent un mot de passe d'administration pour toute modification et expirent à la date que vous définissez.

• Solution idéale pour fournir des applications aux employés, sous-traitants ou étudiants.

• Des évaluations de logiciels peuvent être fournies aux clients potentiels sous forme d'appliances virtuelles avec date d'expiration.

• Les machines virtuelles restreintes peuvent être exécutées par toute personne utilisant Workstation, Fusion Professional ou Player Plus[**W4**].

Démultiplier les avantages en partageant les machines virtuelles

La figure ci-dessous représente les machines partagés sur Vmware [**W4**].

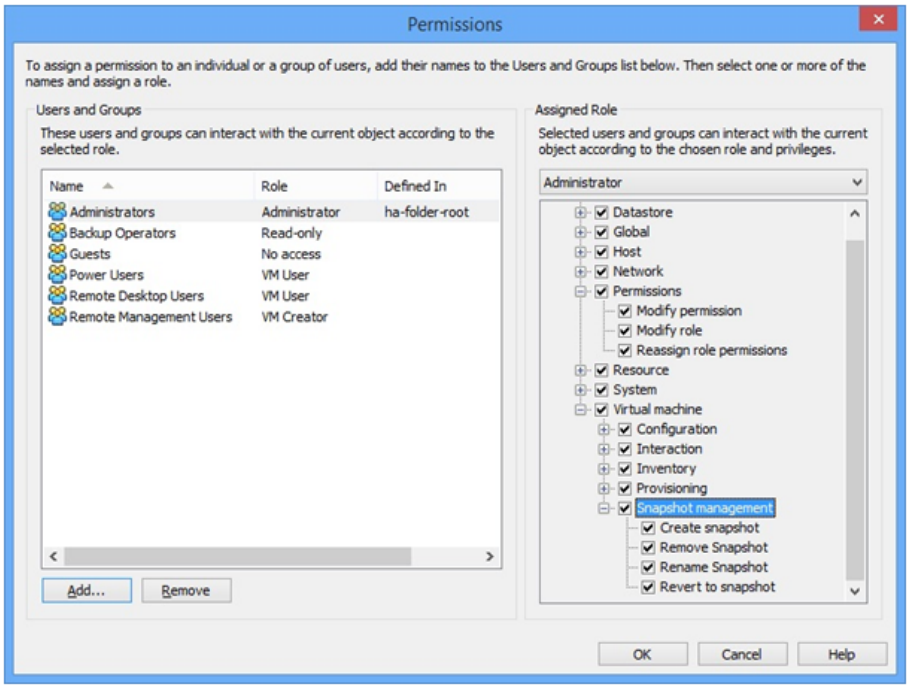

FIGURE 3.43 – Vmware workstation, partage de machine

Exécutez VMware Workstation en tant que serveur pour partager les machines virtuelles avec votre équipe, votre service ou n'importe quel autre utilisateur de l'organisation.

• Contrôle des accès utilisateur à l'échelle de l'entreprise.

• Moyen le plus rapide de partager et de tester des applications avec votre équipe dans des conditions proches de l'environnement de production [**W4**].

Annexe B

Windows Server 2008

Présentation

Microsoft Windows Server 2008 est un système d'exploitation de Microsoft orienté serveur. Il est le successeur de Windows Server 2003 sorti 5 ans plus tôt et le prédécesseur de Windows Server 2008 R2

Hyper-V

Hyper-V est un hyperviseur de système virtuel, formant la partie centrale de la stratégie de virtualisation de Microsoft. Il permet de virtualiser des serveurs au niveau de la couche Kernel du système d'exploitation. Il peut être vu comme le partitionnement d'un unique serveur physique en plusieurs petits ensembles d'ordinateurs [**B5**].

Editions de Windows Server 2008

La plupart des éditions de Windows Server 2008 sont disponibles en version x86-64 (64-bit) et x86 (32-bit).Les versions listées ci-dessous :

-Windows Server 2008 Édition Standard (x86 et x64)

-Windows Server 2008 Édition Enterprise (x86 et x64)

-Windows Server 2008 Édition Datacenter (x86 et x64)

-Windows HPC Server 2008

-Windows Web Server 2008 (x86 et x64)

-Windows Storage Server 2008 (x86 et x64)

-Windows Small Business Server 2008 (x64) pour les PME

-Windows Essential Business Server 2008 (x64) pour les PME

-Windows Server 2008 pour systèmes Itanium

-Windows Server 2008 Foundation [**B5**]

Fonctionnalités

Une machine Windows Server 2008 peut être configurée pour assurer plusieurs rôles de base :

-Services de domaine Active Directory (AD DS)

-Services AD LDS (Active Directory Lightweight Directory Services)

-Serveur DHCP

-Serveur DNS

-Serveur de fichiers

-Serveur d'impression

-Services de diffusion multimédia en continu [**W5**]

Ainsi que les fonctionnalités facultatives suivantes :

-Sauvegarde

-Chiffrement de lecteur BitLocker

-Clustering avec basculement

-Équilibrage de la charge réseau

-Stockage amovible

-Sous-système pour les applications UNIX

-Client TelnetService

-WINS (Windows Internet Name Service)[**W5**]

Installation d'un serveur windows 2008 :

1. insérer le cd d'installation dans le lecteur DVD.

2. rebooter le serveur [**W5**].

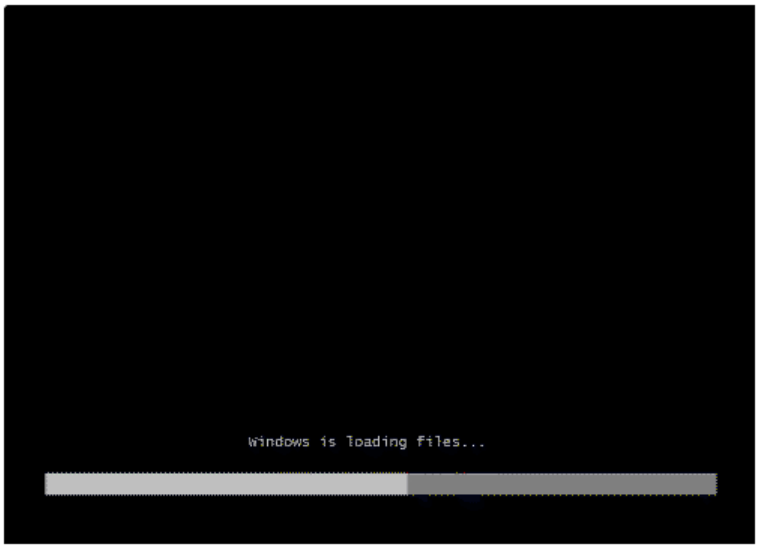

FIGURE 3.44 – Reboutement du serveur

choisir la langue et l'horaire puis appuyer sur next [**W5**].

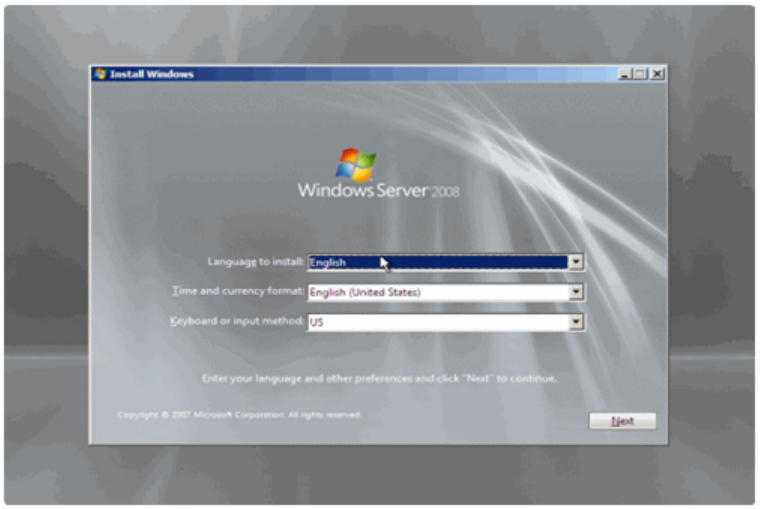

FIGURE 3.45 – Le choix de la langue

cliquer sur install now pour commencer l'installation [**W5**].

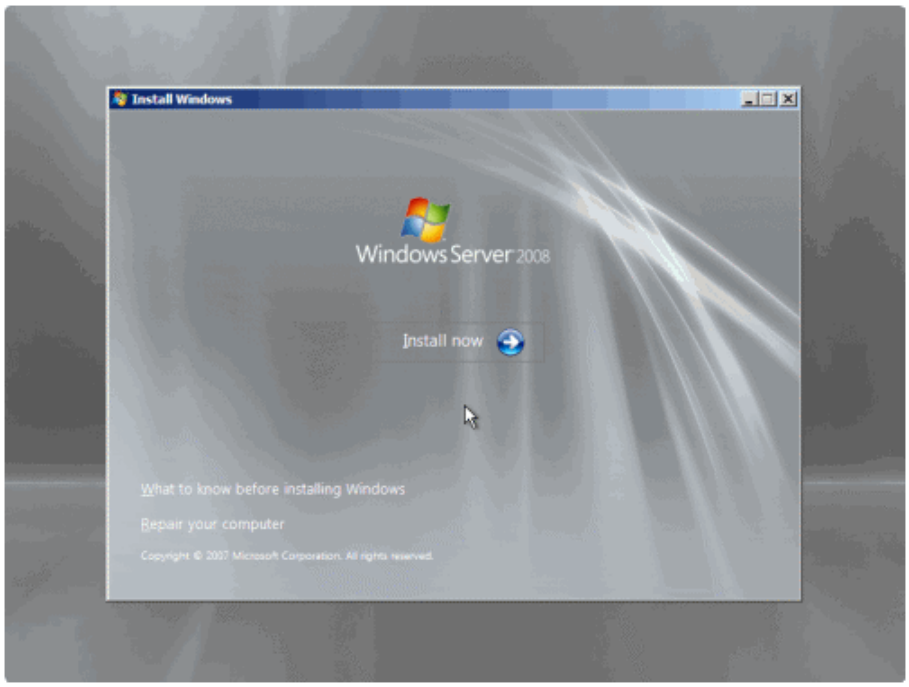

FIGURE 3.46 – L'installation

activer la licence du produit et taper sur next [**W5**].

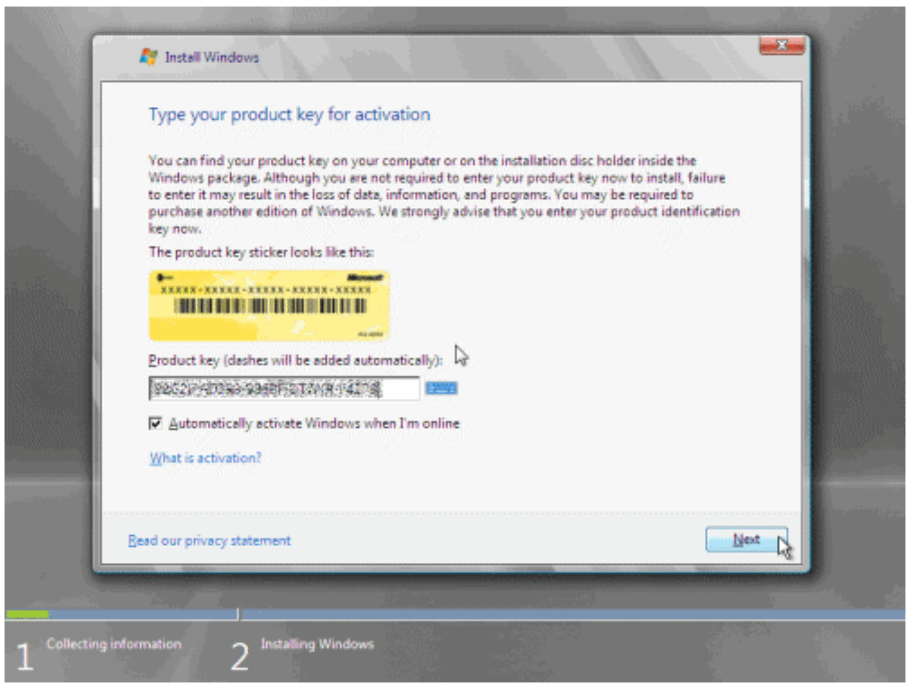

FIGURE 3.47 – Activation licence

choisir la version que nous voulons installer , et taper sur next[**W5**].

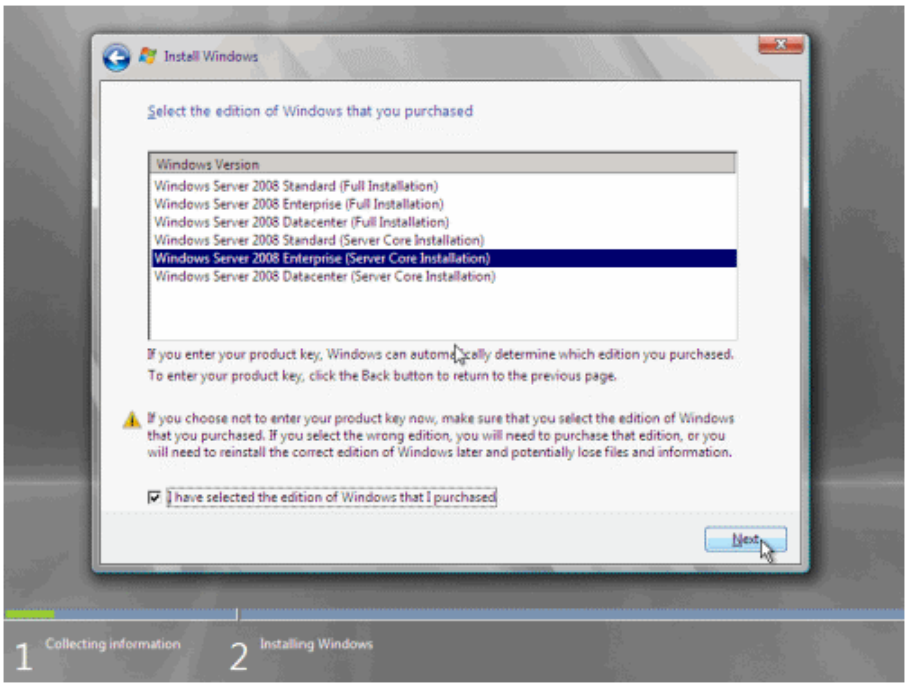

FIGURE 3.48 – Choisir la version

choisir entre la version 32 bit ou 64 bit, et taper sur next [**W5**].

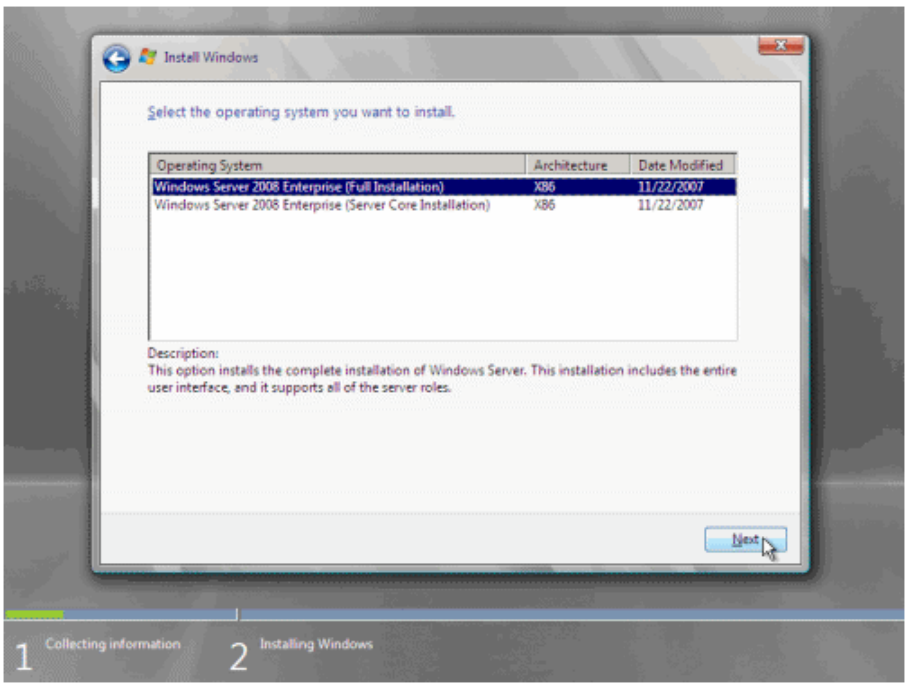

FIGURE 3.49 – Le choix de version utilisé

lire et accepter les termes de la licence, taper sur next [**W5**].

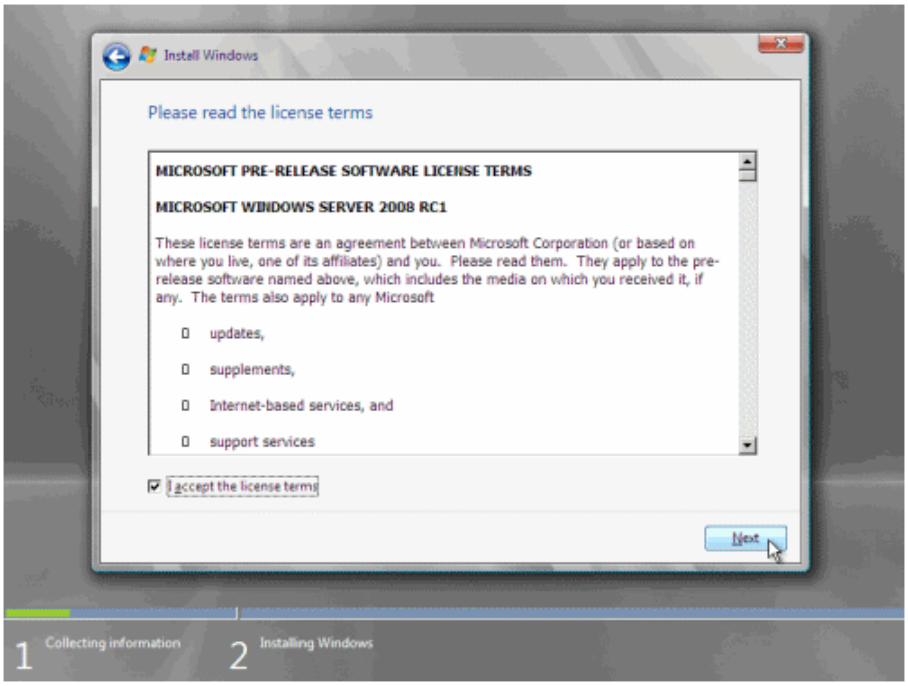

FIGURE 3.50 – L'accéptation des termes de la licence

choisir le type d'installation [**W5**].

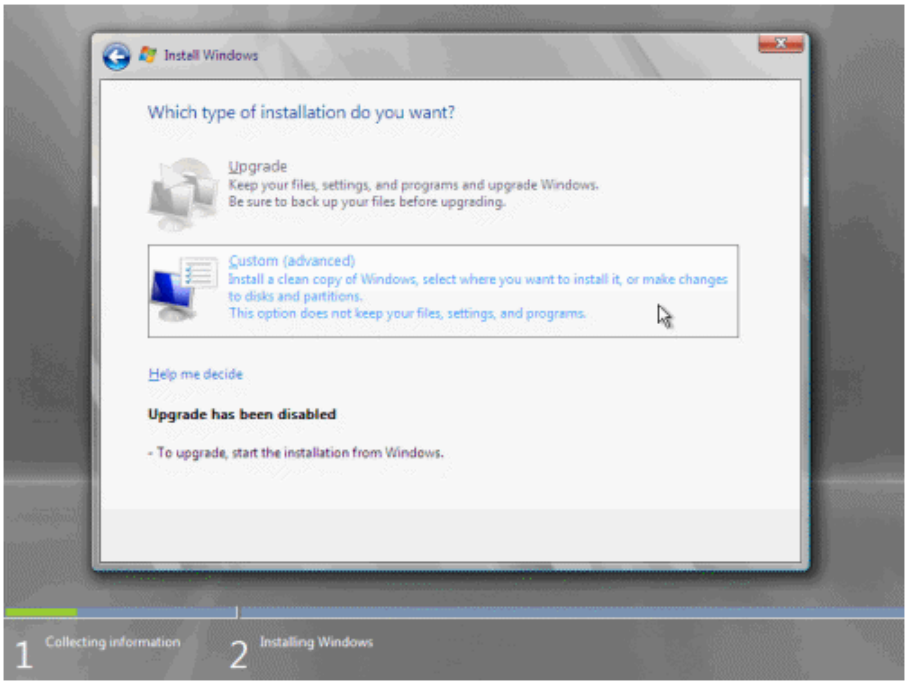

FIGURE 3.51 – Le choix du type de l'installation

choisir le disque ou nous souhaitons installer [**W5**].

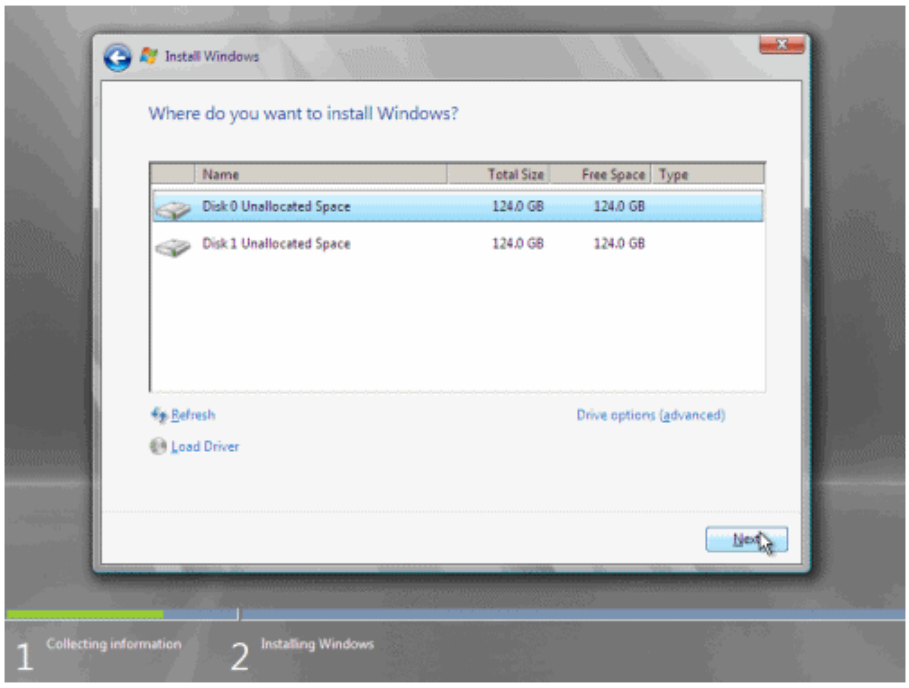

FIGURE 3.52 – Le choix du disque

attendre la fin de l'installation [**W5**].

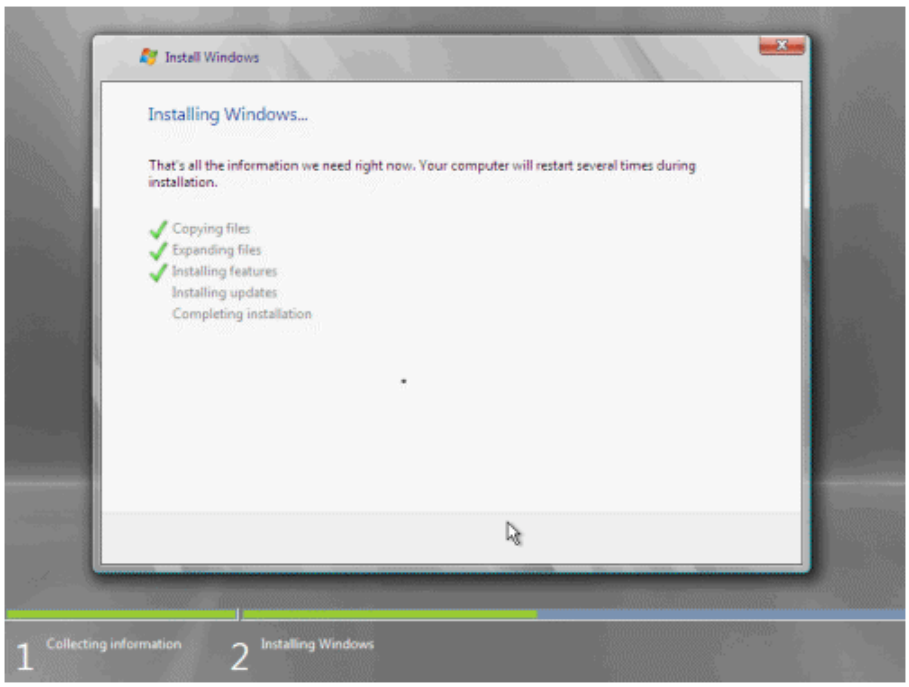

FIGURE 3.53 – L'installation en cours

une fois l'installation terminé, taper CTRL+ALT+DEL [**W5**].

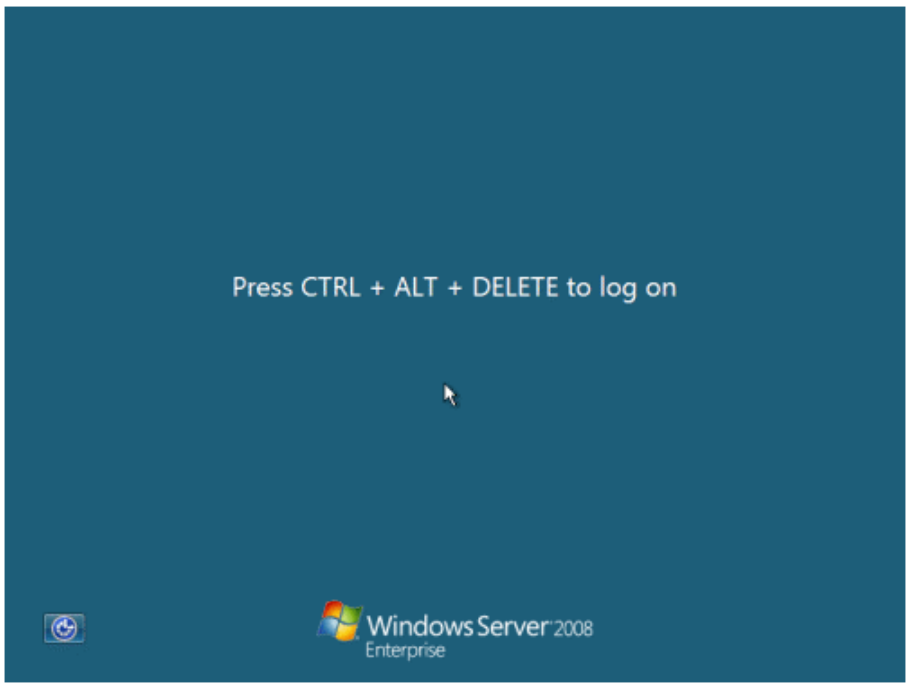

FIGURE 3.54 – L'installation terminé

A cette étape nous pouvons choisir d'installer l'un des rôles voulu, c'est-à-dire en faire : un serveur contrôleur de domaine, DNS ou DHCP ou bien tous puisque Windows permet de virtualiser les serveurs.

Résumé

Aujourd'hui, l'informatique a atteint une prodigieuse évolution technologique dans différents domaines (réseaux informatiques, bases de données, le Web, etc.). Cette évolution est nécessaire pour remédier aux problèmes rencontrés dans les entreprises. La disponibilité est l'une des caractéristiques les plus essentielles de l'informatique. C'est ceci qui nous a poussés à mettre en place une solution avec tolérance aux pannes grâce à l'équilibrage de charge. Plateforme où nous installerons et partagerons des logiciels grâce au Remoteapp, d'une part accessible par des utilisateurs dans un réseau informatique, l'exécution des applications se fera au niveau du serveur. D'une autre part, cela permettra de faciliter pour l'administrateur du réseau, d'administrer, de gérer voir de dépanner le parc informatique de son entreprise, dans un plus bref délai et cela depuis son poste de travail ou bien tout poste qui est configuré pour l'accès distant (Remote desktop). Notre travail consiste à installer et configurer deux Serveur Terminal server avec équilibrage de charge, pour la gestion des applications des employées de l'entreprise TCHIN LAIT " CANDIA ". Le déploiement de cette solution a été mise en œuvre en utilisant différents logiciels informatiques tel que Windows serveur 2008, VMWare.

Mots clés :réseau, windows server 2008, terminal server, équilibrage de charge, tolérance aux pannes, vmware.

Abstract

Today, the computer has reached a prodigious technological developments in different fields (computer networks, databases, the web...). This is necessary to address the problems encountered in business. Availability is one of the most essential features of the computer. It is this that has led us to implement a fault tolerance through load balancing. Platform where we will install the software and share with the RemoteApp, first accessed by users in a computer network, running applications will be at the server level. On the other hand, this will make it easier for the network administrator, administer, manage, view troubleshoot computer equipment from his business in a shorter period and that since his job or any job that is configured for remote access (Remote Desktop). Our job is to install and configure two server with Terminal Server load balancing for the management applications used by the company TCHIN LAIT "CANDIA." The deployment of this solution has been implemented using different software such as Windows Server 2008, VMWare.

Keywords :network, windows server 2008, terminal server, load balancing, fault tolerance, vmware.