République algérienne démocratiqueet populaire

Université Sheikh Al-Arabi Tebessi

Faculté des sciences exactes, et sciences de la nature et de la vie

Département Informatique

Domaine : Mathémathique et informatique

Filére : Informatique

Spécialité : Réseaux et sécurité informatique

Réalisé par :

L'étudiante Ounis Takwa

Conception et la réalisation d'une plateforme de calcul au niveau du laboratoire de recherche LAMIS

Devant le jury

Pr. Hakim benjenna	president
Dr. Taher mekhaznia	Examinateur
Mr. Abdelhakim Gharbi	Encadreur

Année universitaire :2023/2024

Remerciements

Je remercie chaleureusement mon encadreur, M. Gharbi Abdelhakim, pour son soutien indéfectible, ses conseils avisés, et sa patience tout au long de ce projet. Ses encouragements et son expertise ont été essentiels à la réussite de ce travail.

Je remercie Le directeur Pr Hakim Benjanna et les membre de laboratoire pour avoir accepté notre collaboration et Acceptation du travail dans ses locaux

Nous exprimons aussi nos vifs remerciements aux membres du jury, Pr. Hakim Benjanna et Dr. Taher Mekhaznia, d'avoir accepté d'évaluer ce travail.

Je souhaite également remercier ma famille, qui a toujours été ma source d'inspiration et de motivation. À mes parents, pour leur amour inconditionnel, leur soutien moral et financier, et pour m'avoir inculqué les valeurs du travail et de la persévérance. À mes frères et sœurs, pour leur compréhension et leur encouragement constant.

Enfin, je remercie mes amis pour leur amitié sincère, leur soutien et leurs moments de détente qui m'ont permis de garder le moral durant les périodes de stress et de travail intense. Vos encouragements et votre présence ont été inestimables tout au long de cette aventure académique.

Table des matiere :

Table des tableaux :

Table des figures :

Résumé

Ce projet de fin d'études a porté sur l'analyse et la mise en œuvre d'une solution de gestion et de support à distance pour améliorer l'efficacité de notre infrastructure informatique. Nous avons exploré les concepts théoriques du partage de ressources dans les réseaux informatiques, étudié les avantages et les défis associés à une gestion centralisée des ressources, et examiné diverses solutions de support à distance comme Google Desktop, SolarWinds Dameware et TeamViewer. Après une analyse comparative, nous avons choisi Terminal Server pour sa robustesse et son efficacité, détaillant sa mise en œuvre pratique, de l'installation à la validation des tests, confirmant ainsi son adéquation pour répondre aux besoins de notre laboratoire.

Summary

This final year project focused on analyzing and implementing a remote management and support solution to improve the efficiency of our IT infrastructure. We explored theoretical concepts of resource sharing in computer networks, studied the advantages and challenges associated with centralized resource management, and reviewed various remote support solutions like Google Desktop, SolarWinds Dameware, and TeamViewer. After a comparative analysis, we chose Terminal Server for its robustness and efficiency, detailing its practical implementation from installation to validation testing, confirming its suitability to meet the needs of our laboratory.

ملخص

ركز هذا المشروع النهائي على تحليل وتنفيذ حل لإدارة ودعم عن بعد لتحسين كفاءة البنية التحتية لتكنولوجيا المعلومات لدينا. استكشفنا المفاهيم النظرية لمشاركة الموارد في شبكات الكمبيوتر، ودرسنا الفوائد والتحديات المرتبطة بإدارة الموارد المركزية، واستعرضنا حلول الدعم عن بعد المختلفة مثل Google Desktop وSolarWinds Dameware وTeamViewer. بعد تحليل مقارن، اخترنا Terminal Server نظرًا لقوته وكفاءته، وقمنا بتفصيل تنفيذه العملي من التثبيت إلى اختبار التحقق، مؤكدين على ملاءمته لتلبية احتياجات مختبرنا.

Introduction générale :

À l'heure du numérique, les entreprises et les établissements scolaires font face à un défi majeur : la gestion efficace des ressources informatiques et des données. En raison de l'augmentation des informations et des applications, il est devenu essentiel de stocker de partager et d'accéder aux données afin d'assurer le bon déroulement des activités quotidiennes.

Le partage des ressources physiques est l'une des principales difficultés auxquelles les laboratoires informatiques font face. Lorsque les utilisateurs et les applications se multiplient, il est essentiel de trouver des solutions performantes pour stocker et partager les données de manière sécurisée et accessible.

À cet égard, ce mémoire de fin d'études présente une approche innovante afin d'optimiser le partage des ressources dans un réseau informatique dans un laboratoire de recherche. Notre objectif est de résoudre le problème de gestion des ressources en intégrant un serveur dans l'infrastructure réseau, tout en garantissant un accès sécurisé et efficace aux ressources informatiques.

Dans cette introduction générale, nous exposerons brièvement le cadre de l'étude, la problématique à laquelle nous faisons face, ainsi que les objectifs que nous souhaitons atteindre à travers ce mémoire. Par la suite, nous présenterons succinctement le plan de notre travail, en soulignant les principales étapes de notre approche afin d'atteindre une solution fiable et performante.

Dans cette perspective, nous étudierons de manière approfondie les bénéfices et les difficultés liés à l'intégration d'un serveur terminal dans un réseau de laboratoire de recherche, tout en explorant les diverses technologies et solutions disponibles pour résoudre cette question. Finalement, nous terminerons en mettant en avant l'importance de cette étude dans le cadre actuel de la gestion des ressources informatiques.

Chapitre 1 : Le partage des ressources dans les réseaux informatiques.

1 Introduction

Les réseaux informatiques ont révolutionné la façon dont les individus et les organisations interagissent et partagent des informations à l'ère numérique. Ces réseaux jouent un rôle crucial dans la connectivité, la communication et le partage de ressources, contribuant ainsi à l'efficacité et à la productivité des systèmes informatiques modernes. Dans ce chapitre introductif, nous explorerons les concepts fondamentaux des réseaux informatiques et du partage de ressources, en mettant en lumière leur importance et leurs applications dans divers contextes.

2 Fundaments theories:

2.1 Définition des réseaux informatiques :

Réseau (informatique) : ensemble d'ordinateurs et de terminaux interconnectés pour échanger des informations numériques. [1]

2.2 Types de réseaux :

En différenciant les réseaux en fonction de la proximité des appareils, nous avons les classifications suivantes :

- **LAN (Local Area Network) :** Ce réseau est constitué d'ordinateurs au sein d'une même organisation, connectés dans une petite zone géographique à l'aide d'une technologie commune, typiquement Ethernet.
- **MAN (Métropolitain Area Network) :** les MAN connectent plusieurs Un réseau métropolitain (MAN) est constitué de commutateurs ou de routeurs et couvre une zone géographique relativement petite, s'étendant généralement sur quelques dizaines de kilomètres. Le réseau fonctionne à des débits élevés, allant de 1 à 100 Mbits/s.
  En règle générale, un réseau de liaisons à haut débit interconnecte les routeurs, utilisant souvent la technologie de la fibre optique (optique).
- **WAN (Wide Area Network) :** Un WAN interconnecte plusieurs LAN sur de grandes distances géographiques (plus de 1000 kilomètres).
  La plupart un réseau étendu (WAN) est Internet. Le WAN utilise un routeur pour fonctionner Permet de choisir l'itinéraire le plus adapté pour atteindre le nœud réseau. [1]

2.3 Architecture d'un réseau :

2.3.1 Conceptes fondamantaux :

- **Le client :** processus consiste à demander l'exécution d'une opération à un autre processus en envoyant un message contenant le descriptif de l'opération à exécuter et en attendant la réponse de l'opération par un message en retour.
- **Serveur :** processus d'exécution d'une opération sur demande d'un client et de transmission du résultat au client.
- **Requête :** message envoyé par un client à un serveur décrivant l'opération à effectuer au nom du client.

Réponse : message transmis par un serveur à un client suite à l'exécution d'une opération, contenant le résultat de l'opération.

2.3.2 Architecture d'un réseau client-serveur :

2.3.2.1 Definition:

Un client/serveur est un modèle informatique basé sur le traitement distribué dans lequel un utilisateur lance un logiciel client sur un ordinateur relié à un réseau, déclenchant simultanément le lancement d'un logiciel serveur sur un autre ordinateur possédant les ressources souhaitées par l'utilisateur (client). [2]

2.3.2.2 Présentation de l'architecture Client/serveur :

L'architecture client/serveur est un modèle de communication entre plusieurs ordinateurs d'un réseau qui distingue plusieurs postes clients qui communiquent avec un serveur (une machine généralement très puissante en termes d'entrée/sortie) qui leur fournit des services. Ces services comprennent des applications de données telles que l'heure, les fichiers et la connexion. Les programmes clients fonctionnent sur les machines clients et fournissent les services.[2]

2.3.2.3 Fonctionnement d'un système Client /serveur :

Le client initie la conversation en envoyant une requête au serveur en utilisant son adresse IP et son port, qui indiquent une demande spécifique de service du serveur. Ce service est fourni par le serveur, qui ensuite renvoie le résultat au client.

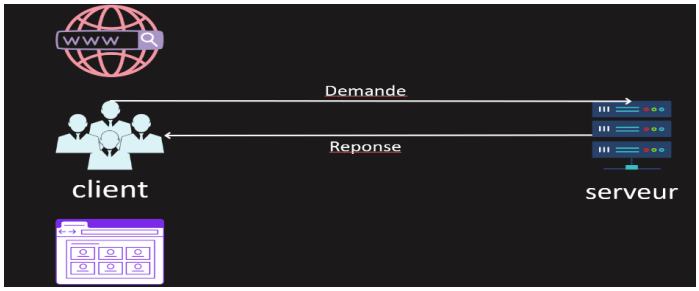

Figure 1 : Fonctionnement d'un système Client /serveur

2.3.2.4 Protocols de communication:

- **TCP/IP (Transmission Control Protocol/Internet Protocol) :**

TCP : assure la livraison des données de manière fiable et ordonnée.
IP : gère le routage des paquets de données à travers le réseau.

- **HTTP (HyperText Transfer Protocol) :**

Utilisé pour le transfert de données hypertexte sur le World Wide Web. Il est basé sur le modèle client-serveur où un navigateur Web agit en tant que client et récupère des ressources à partir de serveurs Web.

- **FTP (File Transfer Protocol) :**

Protocole utilisé pour le transfert de fichiers entre un client et un serveur sur un réseau TCP/IP.

- **SMTP (Simple Mail Transfer Protocol) :**

Protocole utilisé pour l'envoi de courrier électronique entre les serveurs de messagerie.

2.4 Plateforme de calcul :

Le terme "plateforme de calcul fait généralement référence à un environnement matériel et/ou logiciel conçu pour exécuter des tâches de calcul intensif. Ces plateformes sont utilisées dans divers domaines, tels que la recherche scientifique, l'ingénierie, la finance, et l'analyse de données. Voici quelques caractéristiques clés d'une plateforme de calcul :

- **Infrastructure Matérielle :** Comprend des serveurs, des superordinateurs, ou des clusters de calcul qui fournissent la puissance de traitement nécessaire pour exécuter des algorithmes complexes et traiter de grandes quantités de données.

- **Logiciels de Calcul :** Inclut des systèmes d'exploitation, des bibliothèques de calcul scientifique, des outils de gestion de clusters, et des applications spécifiques à des domaines qui facilitent l'exécution des tâches de calcul.
- **Capacité de Traitement :** La plateforme doit être capable de traiter de grands volumes de données à des vitesses élevées, souvent en utilisant des techniques de calcul parallèle et distribué.
- **Stockage de Données :** Comprend des systèmes de stockage haute performance capables de gérer et de stocker de grandes quantités de données nécessaires pour les calculs.
- **Réseau de Communication :** Une infrastructure de réseau rapide et fiable pour permettre la communication entre différents composants de la plateforme et pour transférer des données rapidement.
- **Accès et Sécurité :** Doit fournir des mécanismes pour l'accès sécurisé des utilisateurs, la gestion des identités, et la protection des données sensibles.

Exemples de plateformes de calcul comprennent Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, ainsi que des installations de calcul haute performance (HPC) comme les superordinateurs utilisés dans les centres de recherche.

3 Partage les ressource :

3.1 Définition :

Le partage de ressources est l'une des fonctionnalités les plus importantes des réseaux informatiques. Cette fonctionnalité permet aux utilisateurs d'un réseau d'accéder et d'utiliser des ressources, telles que des fichiers, des imprimantes ou des connexions Internet ou meme les ressources systemes, qui sont disponibles sur d'autres appareils connectés au réseau grâce à l'utilisation de cette fonctionnalité. [3]

3.2 Types de ressources partagées :

Dans les environnements réseau, le partage de ressources est largement utilisé pour optimiser l'utilisation des ressources et améliorer l'efficacité. Les ressources peuvent être partagées et

accessibles de manière centralisée au lieu d'être stockées en double sur chaque appareil du réseau, ce qui réduit les coûts et simplifie la gestion.

Un réseau peut partager diverses ressources. Voici quelques exemples typiques :

- **Les fichiers et les dossiers :** Il permet aux utilisateurs d'accéder et de modifier les fichiers et dossiers stockés sur d'autres appareils réseau.
- **Imprimante :** Les utilisateurs peuvent envoyer des documents à une imprimante connectée à un autre périphérique du réseau.
- **Connexions Internet :** Cela permet aux appareils du réseau de partager une seule connexion Internet, ce qui évite le besoin de plusieurs connexions Internet individuelles.
- **Périphériques de stockage :** Permet aux utilisateurs d'accéder et d'utiliser des périphériques de stockage tels que des disques durs externes ou des lecteurs de stockage réseau (NAS) à partir d'autres appareils du réseau.
- **Ressources systèmes** : Les ressources système sont les composants matériels et logiciels d'un système informatique qui lui permettent de fonctionner. Elles comprennent notamment :
  - La mémoire vive (RAM) qui stocke temporairement des données pour un accès rapide
  - Le stockage (mémoire principale) qui stocke les données pour de plus longues périodes
  - L'unité centrale de traitement (CPU) qui exécute les instructions et traite les données
  - Les cartes graphiques qui produisent les images
  - Les processeurs, mémoires, organes d'entrée/sortie et canaux de communication .[3]

3.3 Avantages du partage de ressources :

Le partage de ressources est une pratique fréquente dans le domaine des réseaux informatiques qui permet aux utilisateurs d'accéder et d'utiliser des fichiers, des appareils et des services sur un réseau. Les ressources communes peuvent englober des imprimantes, des scanners, des lecteurs de stockage, des fichiers et des logiciels. [4]

Les opérations de partage de données en réseau sont effectuées à l'aide de différents protocoles et technologies, tels que le Protocole de Transférante de Archives (FTP), le Protocole de Transférée de HyperText (HTTP), le Protocole de Accès a Directories Ligérot (LDAP), etc.

Les opérations les plus fréquentes qui peuvent être réalisées avec un réseau :

- **Accès distant :** donne aux utilisateurs la possibilité de se connecter à une ressource réseau à partir d'un endroit éloigné. Cela englobe l'utilisation d'une connexion sécurisée comme un VPN (Virtual Privat Network) pour accéder à un ordinateur ou à un serveur.
- **Partager des fichiers :** Il est possible de partager des fichiers sur un réseau, ce qui permet à plusieurs utilisateurs d'accéder et de modifier le contenu en même temps. Ceci simplifie la coopération sur des projets et la gestion des documents communs.
- **Impression réseau :** Il est possible de partager les imprimantes sur un réseau, permettant ainsi à plusieurs utilisateurs d'envoyer des travaux d'impression de leur propre ordinateur. Cela facilite la gestion des machines d'impression et augmente l'efficacité dans les espaces de travail communs.
- **Partage de périphériques de stockage :** Il est possible de partager des disques de stockage, comme les disques durs externes ou les lecteurs flash, sur un réseau, pour permettre aux utilisateurs d'accéder aux fichiers et aux données qui y sont stockés.
- **Services de partage :** Outre les ressources matérielles, on peut également partager des services réseau, comme des serveurs web, des serveurs de messagerie ou des bases de données. Cela donne la possibilité à différents utilisateurs d'accéder aux mêmes services et d'exploiter la puissance de traitement d'un serveur centralisé.

3.4 Challenges et contraintes :

3.4.1 Sécurité :

L'un des principaux défis du partage de ressources est la sécurité. Lorsque plusieurs utilisateurs accèdent aux mêmes ressources, il est essentiel de mettre en place des mécanismes robustes d'authentification, d'autorisation et de chiffrement pour protéger les données sensibles contre les accès non autorisés et les violations de la confidentialité.

3.4.2 Gestion des droits d'accès :

Gérer efficacement les droits d'accès aux ressources partagées peut être complexe, en particulier dans les environnements où différents utilisateurs ont des besoins d'accès différents. Il est crucial de mettre en place des politiques de gestion des accès claires et cohérentes pour garantir que seuls les utilisateurs autorisés ont accès aux ressources appropriées.

3.4.3 Conflits de ressources :

Dans les environnements où les ressources sont partagées entre de nombreux utilisateurs, des conflits peuvent survenir lorsque plusieurs utilisateurs tentent d'accéder à la même ressource simultanément. Cela peut entraîner des problèmes de performances et des temps d'attente prolongés, en particulier pour les ressources à forte demande telles que les serveurs ou les imprimantes.

3.4.4 Gestion de la bande passante :

Le partage de ressources peut entraîner une utilisation intensive de la bande passante réseau, en particulier lors du transfert de gros fichiers ou lors de l'accès à des ressources à distance. Il est important de surveiller et de gérer la bande passante pour garantir des performances optimales pour tous les utilisateurs du réseau.

3.4.5 Compatibilité des plateformes:

Assurer la compatibilité des différentes plateformes et systèmes d'exploitation peut être un défi lorsque plusieurs utilisateurs accèdent aux mêmes ressources à partir de périphériques différents. Des efforts supplémentaires peuvent être nécessaires pour garantir une expérience utilisateur transparente et cohérente quel que soit le périphérique utilisé.

3.4.6 Gestion des versions :

Dans les environnements où les fichiers et les applications sont partagés entre plusieurs utilisateurs, la gestion des versions devient importante pour éviter les conflits et assurer l'intégrité des données. Des mécanismes de contrôle de version et de sauvegarde sont nécessaires pour gérer efficacement les modifications et les mises à jour des ressources partagées.

3.4.7 Performance :

Le partage de ressources peut entraîner une dégradation des performances, en particulier lorsque les ressources sont fortement sollicitées ou lorsque le réseau est congestionné. Il est essentiel de surveiller les performances du réseau et d'identifier les goulets d'étranglement pour garantir des performances optimales pour tous les utilisateurs.

3.5 Sécurité dans le partage de ressources :

3.5.1 Risques liés au partage de ressources :

Le partage de ressources dans un réseau informatique présente certains risques potentiels, notamment en ce qui concerne la sécurité, la confidentialité et la disponibilité des données. Voici quelques-uns des principaux risques liés au partage de ressources :

a) Accès non autorisé:

L'un des risques les plus critiques est la possibilité qu'un utilisateur non autorisé puisse accéder à des ressources sensibles ou confidentielles. Cela peut se produire en raison de vulnérabilités de sécurité, de mauvaises pratiques d'authentification ou de contrôles d'accès insuffisants.

b) Fuites de données :

Le partage de ressources peut augmenter le risque de fuites de données, où des informations sensibles sont accidentellement exposées ou divulguées à des personnes non autorisées. Cela peut se produire par exemple si des fichiers sont mal configurés ou si les autorisations d'accès ne sont pas correctement définies.

c) Altération de données :

Les données partagées sont susceptibles d'être altérées ou corrompues, que ce soit intentionnellement par un utilisateur malveillant ou accidentellement en raison d'erreurs de manipulation des fichiers. Des contrôles de sécurité appropriés, tels que le chiffrement et les vérifications d'intégrité, peuvent aider à atténuer ce risque.

d) Indisponibilité des ressources :

Une utilisation intensive des ressources partagées peut entraîner une surcharge des serveurs, des périphériques ou des canaux de communication, ce qui peut entraîner une dégradation des performances voire une interruption complète du service. Les pannes matérielles ou logicielles peuvent également affecter la disponibilité des ressources partagées.

e) Attaques par déni de service (DDoS) :

Les ressources partagées sont souvent la cible d'attaques par déni de service (DDoS), où des attaquants tentent de submerger un serveur ou un réseau avec un trafic malveillant pour le rendre

indisponible. Cela peut entraîner une interruption du service pour tous les utilisateurs qui dépendent des ressources partagées.

f) Propagation de logiciels malveillants :

Le partage de fichiers, d'applications ou de périphériques peut faciliter la propagation de logiciels malveillants tels que les virus, les vers et les chevaux de Troie. Des contrôles de sécurité appropriés, tels que les logiciels antivirus et les pares-feux, sont nécessaires pour détecter et prévenir les infections.

g) Violation de conformité :

Le partage de ressources peut entraîner des violations de conformité avec les réglementations en matière de protection des données et de confidentialité, telles que le RGPD (Règlement Général sur la Protection des Données) en Europe ou la HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis. Les organisations doivent s'assurer que le partage de ressources est conforme aux exigences légales et réglementaires applicables.

3.5.2 Mécanismes de sécurité :

La sécurité dans le partage de ressources est d'une importance cruciale pour garantir la confidentialité, l'intégrité et la disponibilité des données partagées. Voici quelques considérations de sécurité à prendre en compte lors du partage de ressources dans un réseau :

a) Authentification et contrôle d'accès :

Mettez en place des mécanismes d'authentification solides pour vérifier l'identité des utilisateurs qui accèdent aux ressources partagées. Utilisez des méthodes telles que les noms d'utilisateur et les mots de passe robustes, les certificats numériques ou les systèmes de biométrie. En outre, définissez des politiques de contrôle d'accès pour limiter l'accès aux ressources uniquement aux utilisateurs autorisés.

b) Chiffrement des données :

Utilisez le chiffrement pour protéger les données sensibles pendant leur transmission sur le réseau. Utilisez des protocoles de communication sécurisés tels que SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour le transfert de fichiers et le partage de données sur Internet.

De plus, chiffrez les données stockées sur les serveurs de fichiers ou les périphériques de stockage pour empêcher tout accès non autorisé.

c) Surveillance et audit :

Mettez en place des mécanismes de surveillance et d'audit pour suivre les activités liées au partage de ressources. Cela peut inclure la journalisation des événements, la surveillance du trafic réseau et l'analyse des journaux d'audit pour détecter les comportements suspects ou les tentatives d'intrusion.

d) Mise à jour et patch management :

Assurez-vous que les systèmes et les logiciels utilisés pour le partage de ressources sont régulièrement mis à jour avec les derniers correctifs de sécurité. Les vulnérabilités de sécurité connues peuvent être exploitées par des attaquants pour compromettre la sécurité des ressources partagées, il est donc essentiel de maintenir un environnement à jour et sécurisé.

e) Sécurité physique :

Protégez les équipements réseau, les serveurs et les périphériques de stockage physiquement en restreignant l'accès aux locaux serveurs, en utilisant des serrures et des alarmes, et en surveillant l'environnement pour détecter toute activité suspecte.

f) Sécurité des communications sans fil :

Si vous utilisez des réseaux sans fil pour le partage de ressources, assurez-vous de sécuriser votre réseau Wi-Fi en utilisant des méthodes telles que le chiffrement WPA2 (Wi-Fi Protected Access 2), les mots de passe forts et la désactivation du SSID broadcast pour réduire les risques d'accès non autorisé.

g) Formation et sensibilisation des utilisateurs :

Sensibilisez les utilisateurs aux bonnes pratiques de sécurité, tels que la création de mots de passe forts, le signalement des activités suspectes et la protection des informations sensibles. Offrez une formation régulière sur les menaces de sécurité et les techniques d'attaque courantes pour aider les utilisateurs à reconnaître et à éviter les risques.

4 Conclusion:

Dans ce chapitre, nous avons examiné en détail le concept du partage de ressources dans les réseaux informatiques. Nous avons abordé divers aspects, notamment les méthodes de partage de ressources telles que le partage de fichiers, d'imprimantes et d'autres périphériques, ainsi que les protocoles associés et les configurations nécessaires. Nous avons également discuté des avantages, des défis et des contraintes du partage de ressources, ainsi que des bonnes pratiques de sécurité à mettre en œuvre pour atténuer les risques.

Le domaine du partage de ressources continue d'évoluer avec l'avancement des technologies de réseau et des besoins des utilisateurs. Les perspectives futures incluent le développement de solutions de partage de ressources plus robustes, sécurisées et évolutives, ainsi que l'intégration de nouvelles technologies telles que le cloud computing, la virtualisation et l'intelligence artificielle pour améliorer l'efficacité et la flexibilité du partage de ressources.

Dans le prochain chapitre, nous aborderons la présentation du laboratoire de recherche LAMIS (Laboratoire d'Analyse et de Modélisation des Images et des Signaux), en mettant en évidence son infrastructure, ses équipements, ses applications et ses contributions à la recherche scientifique et technologique. Nous examinerons également les défis et les opportunités liés à la gestion et au partage des ressources dans un environnement de laboratoire de recherche.

Chapitre 2 : Présentation de laboratoire LAMIS

1 Presentation de laboratories lamis

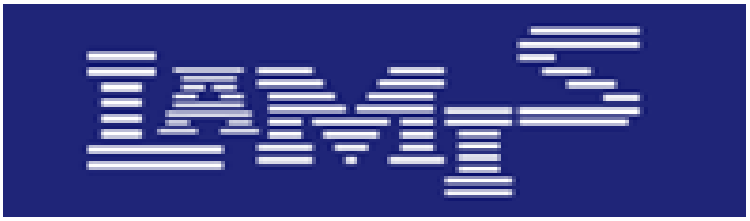

Figure 2 : LAMIS

LAMIS est un Laboratoire de Mathématiques, Informatique et Systèmes de l'Université de Larbi Tebessi. Le laboratoire a été créé en 2012 et est une entité au sein du Département de Mathématiques et d'Informatique de la Faculté des sciences exactes, de la vie et des sciences naturelles à l'Université de Larbi Tbessi, Tébessa, en Algérie.

Le laboratoire mène des recherches dans un large éventail de sujets relevant des disciplines de l'informatique, de l'ingénierie, de la technologie et des mathématiques. Les domaines de recherche actuels comprennent l'architecture informatique, la vision par ordinateur, les systèmes distribués, le traitement d'images et de signaux, la logique et la sémantique, le traitement du langage naturel, les réseaux et les communications sans fil, les systèmes d'exploitation et la virtualisation, ainsi que l'informatique durable.

Le laboratoire est divisé en quatre (4) équipes avec des thèmes de recherche clairement identifiés. Actuellement, nous comptons environ cent vingt (120) membres. Quelque 80 étudiants diplômés supplémentaires sont engagés dans des recherches en vue de l'obtention d'un doctorat.

Le LAMIS est logé dans l'ancien bâtiment de l'université de Larbi Tbessi, au niveau du bloc de recherche, au 4ème étage.

2 Architecture du réseau LAN de laboratoire LAMIS

Le reseau LAN de laboratoire se compose de switcher relié au reseau de l'université avec des cable en fibre , et un ensemble de pc et serveurs repartis sur 3 salles , comme il est illustré sur la figure suivante .

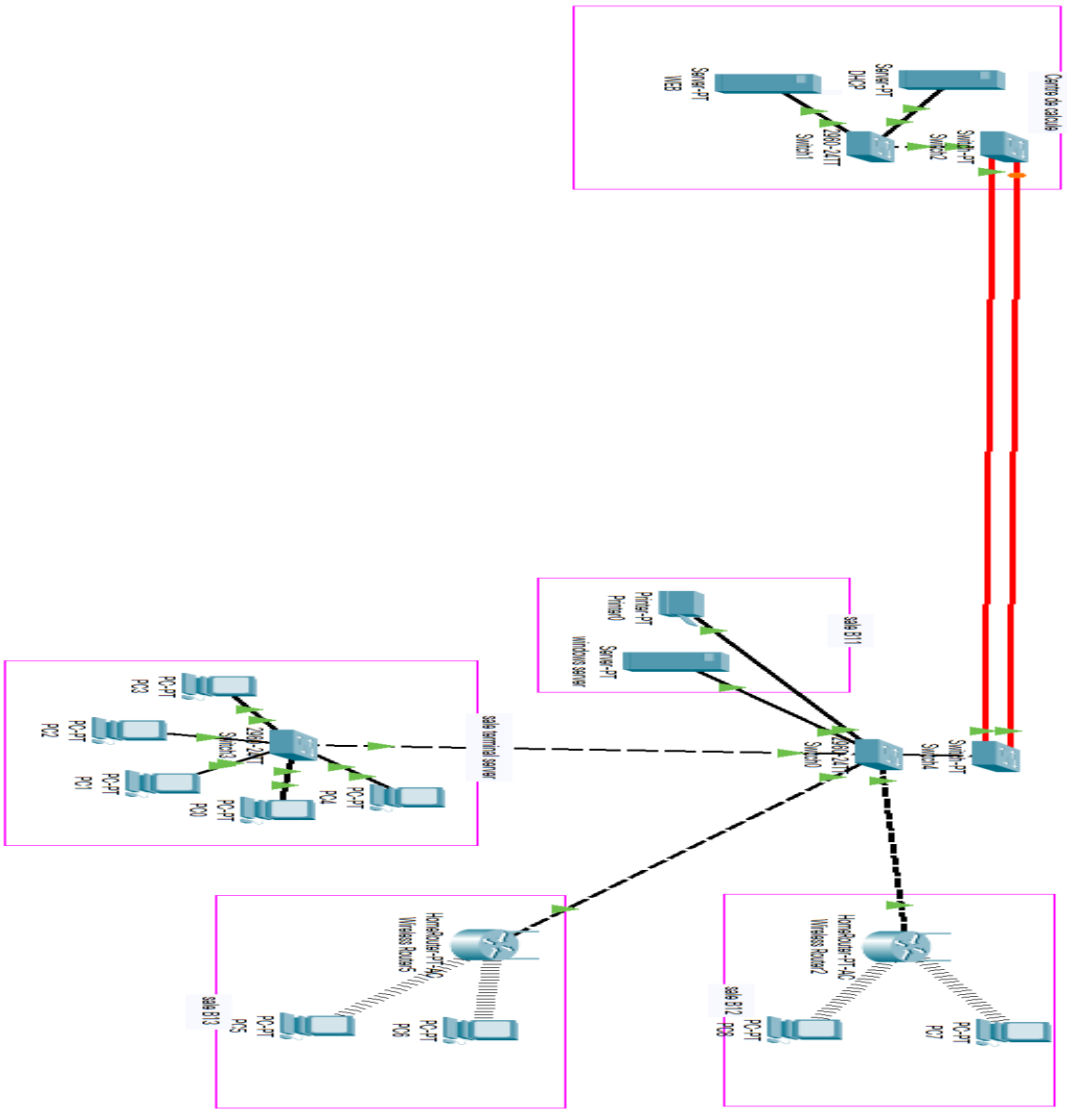

Figure 3 : Architecture du réseau LAN de laboratoire LAMIS

3 Équipes et membres:

3.1 Ingénierie des Systèmes d'Information et d'Imagerie :

3.1.1 L'équipe est responsable des principaux domaines suivants :

- Gestion continue des systèmes d'information de recherche existants ; soutien au développement de nouveaux systèmes et à leur mise en œuvre ; amélioration des systèmes existants.
- Développement de nouvelles méthodes et outils pour résoudre des problèmes complexes d'apprentissage et de prise de décision dans des conditions d'incertitude.
- Exploration des questions de gestion (gouvernance) dans les systèmes d'information.
- Développement et amélioration des processus métier pour améliorer l'efficacité de la saisie des données et garantir la cohérence, l'exhaustivité et l'exactitude de toutes les données pertinentes pour la recherche.
- Développement de nouvelles techniques de traitement d'images efficaces, de systèmes d'imagerie et de leurs applications en ingénierie de l'information, en biologie et en sciences médicales.

3.2 Systèmes distribués et intelligents :

L'équipe est engagée dans la recherche de systèmes intelligents distribués problématiques dans les domaines suivants :

- Soft-computing (réseaux de neurones, algorithmes génétiques, ensembles flous et logique floue, ensembles approximatifs).
- Modélisation et simulation de systèmes parallèles et distribués
- Systèmes d'agents et de multi-agents.
- Reseaux de capteurs sans fil
- Systèmes robotiques et systèmes intelligent
- Réseaux de capteurs sans fil

3.3 Analyse et mathématiques appliquées :

L'équipe Analyse et Mathématiques Appliquées est spécialisée dans l'étude :

- Concept de système dynamique.
- La distinction entre les systèmes linéaires et les systèmes non linéaires.
- Comportement particulier pouvant présenter certains comportements de systèmes non linéaires
- Modes de masquage de l'information à l'aide de systèmes chaotiques proposés dans la littérature
- Par rapport au cryptage conventionnel.

3.4 Systèmes dynamiques, elliptiques et chaotiques :

Le travail de cette équipe s'articule principalement autour de quatre axes :

- Mathématiques fondamentales,
- Analyse appliqué,
- Probabilities et statistiques,
- Evolution des systèmes et modélisation

4 Projets en cours :

- IA-CAD : Un nouveau système d'aide au diagnostic précoce du cancer du sein à l'aide d'une approche basée sur le Deep Learning, projet d'équipe Mix
- Un système intelligent pour le diagnostic anatomopathologique
- Détection précoce des maladies neuronales par l'analyse de manuscrits
- Application de techniques avancées d'intelligence artificielle pour aider au diagnostic des maladies pulmonaires
- Développement et déploiement d'un système intelligent de détection de la corrosion dans les équipements industriels.
- Diagnostic intelligent assisté par ordinateur des pathologies cardiovasculaires
- TrustGov/ Une nouvelle approche biométrique basée sur l'apprentissage profond pour sécuriser les applications d'administration en ligne.

- Point fixe : Théorie et applications
- Le comportement asymptotique des solutions à certains problèmes d'évolution non linéaire
- Stabilisation et explosion de solutions dans les systèmes d'évolution non linéaires

5 Ressources informatique de Laboratoire :

N°	Equipment	Caractéristiques	Nombre
1	HP Z8 G4	**Processeurs** 2,5 GHz 38,50 Mo de mémoire cache, 28 cœurs Jusqu'à 3,8 GHz avec la technologie Intel Turbo Boost Supporte des taux de transfert de mémoire DDR4 allant jusqu'à 2 666 MT/s 205 W **Carte graphique** : Nvidia Quadro P1000 avec 4 GO **Écrans**: Écran HP Z Z22n G2 **Stockage et lecteurs** : Disque dur HP 300 Go 15K SAS SFF (carte d'extension de contrôleur nécessaire) Mémoire : Mémoire RAM 8 Go DDR4-2666 ECC Reg (8 Go x 1) HP	1
2	Ryzen 9 7900X3D 5,60 GHz 12-Core	CPU - AMD Ryzen 9 7900X3D 5.60 GHz 12-Core | Corsair VENGEANCE 32GB DDR5 5600MHz RAM | 2TB M.2 SSD P41+ Carte graphique - Nvidia RTX 4090 24 GB avec architecture Ada Lovelace, la nouvelle technologie ultra efficace de Nvidia | Carte mère ASUS Prime X670-P avec RAM DDR5 et support PCIe 5.0 M.2 Windows 11 Home préinstallé avec tous les pilotes à jour,	1

		Boîtier PCS Spectrum II ARGB Mid-Tower.	
3	Lenovo i3	**Processeur :** Intel Core i3-10110U (2C / 4T, 2.1 / 4.1GHz, 4MB). **Mémoire vive (RAM) :** 4 Go de RAM solderée, avec un slot SO-DIMM pour une augmentation jusqu'à 12 Go (4 Go solderés + 8 Go SO-DIMM). Stockage : Un disque dur de 1 To à 5400 rpm. Carte graphique : Intel UHD Graphics intégrée. **Écran** : 15,6 pouces FHD (1920 x 1080)	10
4	Dell i3 8Go	**Processeur :** Intel Core i3 12100 up to 4.3 GHz, 12 Mo de cache. **Mémoire vive (RAM)** : 8 Go DDR4 (2 slots). Stockage : 1 To HDD + 256 Go SSD **Carte graphique :** Intel HD Graphics 520	4
5	Canon imageRunner 2520	**Imprimante :** UFR II/UFRII LT Printer Driver. **Pilotes :** Disponibles pour téléchargement. **Système d'exploitation** : Compatible avec plusieurs systèmes d'exploitation, notamment Windows et macOS	1

Tableau 1 : Ressources informatique de Laboratoire

6 Problematique :

Le laboratoire LAMIS est confronté à plusieurs défis en ce qui concerne le partage de l'utilisation des equipements puissants, des logiciels et le stockage des données entre leurs étudiants et chercheurs. Les étudiants et les chercheurs rencontrent des difficultés pour accéder aux logiciels et aux outils nécessaires à leurs recherches et projets, ce qui limite leur capacité à accomplir leurs tâches efficacement et entrave l'apprentissage et la recherche efficaces.

Ces défis soulignent la nécessité urgente de développer une solution global et intégré qui facilite le partage des ressources physique et logiciels ainsi que le stockage des données de manière sûre et efficace. Cette solution doit fournir un accès centralisé aux logiciels nécessaires ainsi que des espaces de stockage sécurisés et fiables pour les données, avec des mécanismes efficaces pour le partage des calculateurs et des ressources entre les étudiants et les chercheurs.

Face à ces défis, la question se pose de savoir comment atteindre cet objectif de manière efficace et efficiente. Quelles sont les mesures pratiques à prendre pour développer une plateforme de calcule, de partage et de stockage des logiciels et des données plus performant ? Comment surmonter les défis techniques et organisationnels pour atteindre cet objectif et renforcer la collaboration et la productivité au sein de l'institution ?

Chapitre 3: Etude des solutions Existante

1 Introduction

Le laboratoire de recherche LAMIS mène des travaux dans des domaines variés tels que l'intelligence artificielle, la recherche biomédicale et la physique. La plateforme de calcul est essentielle pour ces recherches car elle fournit les ressources matérielles et logicielles nécessaires à l'analyse de données massives, la simulation de systèmes complexes et l'optimisation de processus.

L'objectif de ce projet : est de permettre d'améliorer l'efficacité, la collaboration et l'innovation au sein de laboratoire, renforçant ainsi leur position en tant que leaders académiques dans la région. En intégrant des technologies de serveur terminal, nous visons à optimiser les processus administratifs et académiques, notamment les délais et les coûts opérationnels. La centralisation des ressources informatiques permettra une gestion plus efficace des infrastructures technologiques, assurant une maintenance simplifiée et une allocation optimale des ressources.

En plus de collaboration, ce projet favorisera un environnement où les termes enseignants, les chercheurs et les étudiants peuvent interagir et partager des connaissances de manière plus fluide et sécurisée. Les outils de collaboration en ligne et l'accès distant aux logiciels spécialisés permettent des échanges académiques dynamiques, tant au sein de l'institution qu'avec des partenaires externes, nationaux et internationaux. Cette synergie a renforcé l'innovation, en facilitant l'émergence de projets interdisciplinaires et en soutenant la recherche collaborative.

2 État de l'art :

Une analyse des différentes solutions de plateforme de calcul disponibles a été réalisée. La plateforme Terminal Server a été retenue en raison de ses avantages en termes de flexibilité, de sécurité et de possibilités de collaboration.

2.1 Les différentes solutions de plateforme de calcul disponibles :

2.1.1 Google desktop :

Figure 4 : Google desktop

Chrome Remote Desktop est une extension du navigateur Chrome développée par Google qui permet aux utilisateurs d'accéder à des ordinateurs à distance de manière sécurisée via Internet. Il s'intègre au navigateur et peut être lancé depuis le bureau (Windows, Mac, Linux).

L'extension fonctionne à la fois sur le navigateur Chrome ou sur un Chromebook. La connexion à distance peut fonctionner à court et à long terme. Elle permet aux utilisateurs de l'un ou l'autre ordinateur d'avoir accès aux applications et aux fichiers en toute sécurité.

Pour lancer Chrome Remote Desktop à partir du navigateur sur un ordinateur, on doit ajouter l'extension dansle navigateur et on confgure l'accès à distance.

En plus de l'extension, Chrome Remote Desktop est disponible en logiciel et application à télécharger pour Chrome OS, Mac OS X, iOS, Windows, Android et Linux. Celui-ci nécessite une version mise à jour du navigateur ou de l'application Google Chrome sur toutes les plateformes mentionnées pour fonctionner de manière interchangeable.

C'est un outil simple et gratuit à utiliser pour gérer et accéder aux ordinateurs à distance via Internet. [5]

2.1.1.1 Avantages de Google Desktop pour le partage des ressources :

Accès facile aux fichiers et aux documents : Google Desktop offre un accès rapide et pratique aux système et aux documents partagés, ce qui facilite la collaboration et la productivité au sein de l'équipe.

Recherche rapide et efficace des ressources partagées : La fonction de recherche de Google Desktop permet aux utilisateurs de trouver rapidement et efficacement les ressources partagées, même parmi de grandes quantités de données.

Collaboration en temps réel avec les membres de l'équipe : Google Desktop facilite la collaboration en temps réel en permettant aux membres de l'équipe d'accéder et de modifier les ressources partagées simultanément, ce qui favorise un travail efficace et une communication fluide.

2.1.1.2 Mise en place de Google Desktop pour le partage des ressources :

Installation et configuration de Google Desktop :

- Étape 1. Sur l'ordinateur hôte, ouvrons la page de téléchargement de Chrome Remote Desktop. Cliquons sur "Accès à distance", puis sur le bouton de téléchargement.

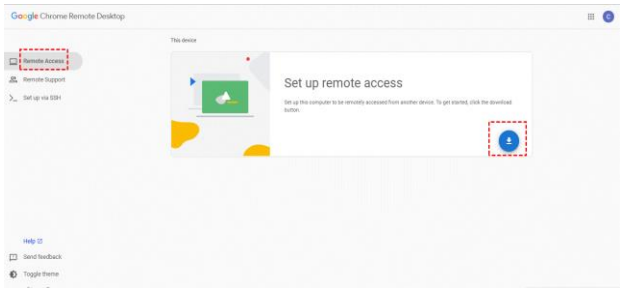

Figure 5 : Étape 1 de l'installation et configuration de Google Desktop

- Étape 2. Ensuite, la fenêtre sera redirigée vers le Chrome Web Store,

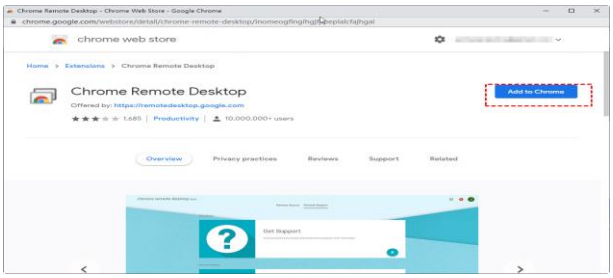

Figure 6 : Étape 2 de l'installation et configuration de Google Desktop

- Étape 3.Cliquons sur "Accepter et installer" pour lancer l'installation.
- Étape 4. Entrons un nom, puis cliquons sur "Suivant".

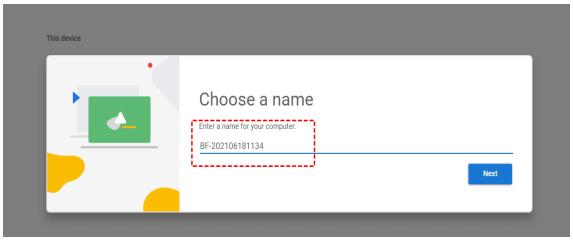

Figure 7 : Étape 4 de l'installation et configuration de Google Desktop

- Étape 5. Choisissons un PIN (Personal Identification Number) avec au moins 6 chiffres, puis saisissons-le deux fois pour démarrer le programme.

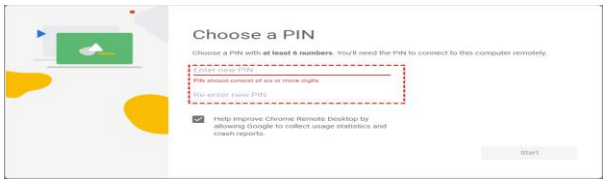

Figure 8 : Étape 5 de l'installation et configuration de Google Desktop

- Étape 6. Sur l'ordinateur local, ouvrons le navigateur Chrome et accédons ici. Ensuite, connectons-nous au même compte Google.
  Une fois connectés, nous pouvons voir les ordinateurs disponibles.

Figure 9 : Étape 6 de l'installation et configuration de Google Desktop

- Étape 7. Cliquons sur l'ordinateur configuré précédemment, et saisissons son NIP (….). Ensuite, nous pouvons commencer notre contrôle à distance.

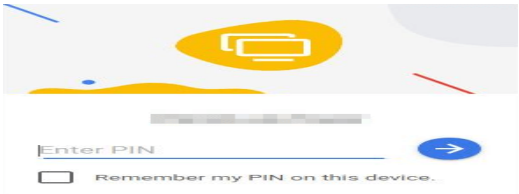

Figure 10 : Étape 7 de l'installation et configuration de Google Desktop

- Étape 8. La connexion a maintenant été établie avec succès.

2.1.1.3 Comment utiliser Chrome Remote Desktop ? :

Pour commencer, rendons-nous sur le service en ligne afin de réaliser les premiers pas de mise en place du système sur notre ordinateur. Nous aurons deux actions à réaliser : l'installation de l'extension pour navigateur Chrome et celle du logiciel de bureau. Nous pouvons aussi suivre nos liens directs si nous le désirons.

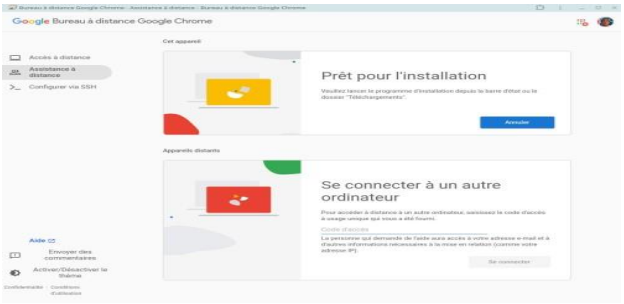

Figure 11 : Comment utiliser Chrome Remote Desktop

Une fois que nous avons configuré notre ordinateur, nous pourrons y accéder simplement depuis nos appareils mobiles. Nous pourrons aussi partager notre bureau avec un autre utilisateur, qui pourrait nous dépanner, par exemple. Veillons à ne pas ouvrir notre accès à des personnes inconnues.

Comme la plupart des applications de bureau à distance, Chrome Remote Desktop utilise un code pour authentifier la connexion du périphérique local au poste de travail distant. Il suffit de partager le code avec l'utilisateur avec lequel on souhaite communiquer pour autoriser l'accès. Une fois le code reçu, l'utilisateur peut contrôler le clavier et la souris de l'ordinateur distant et ainsi accéder à tout le système.

2.1.1.4 les inconvenient de google desktop :

- **Perte de contrôle sur les données :** Lors du partage des ressources, il existe un risque de perte de contrôle sur les données, où des personnes non autorisées peuvent accéder à des informations sensibles.

- **Gonflement des données :** La croissance du volume des ressources partagées peut entraîner un gonflement des données, rendant leur gestion et leur recherche difficiles.
- **Problèmes de sécurité :** Les ressources partagées peuvent être confrontées à des problèmes de sécurité tels que des piratages ou des attaques électroniques, en particulier si des mesures de sécurité strictes ne sont pas mises en place.
- **Conflits de versions :** Des problèmes de versions multiples ou de modifications incohérentes des fichiers peuvent survenir, entraînant des conflits de versions et des pertes de données.
- **Duplication des données :** Le partage des ressources peut entraîner la duplication des données, où les utilisateurs peuvent télécharger des copies identiques de fichiers sans coordination ni communication.
- **Définition des rôles et responsabilités :** Il peut être difficile de définir les rôles et les responsabilités entre les membres de l'équipe lors du partage des ressources, ce qui peut entraîner de la confusion et des conflits dans le travail.

En comparaison, Chrome Remote Desktop se distingue par sa simplicité, sa compatibilité multiplateforme et son intégration transparente avec d'autres services Google, tandis qu'un terminal server est plus orienté vers la fourniture d'un environnement de bureau virtuel pour l'accès à des applications et des données à distance.

En résumé, Chrome Remote Desktop est plus adapté pour un accès à distance léger et simple via un navigateur, tandis qu'un terminal server est plus approprié pour des besoins plus avancés en termes d'accès à des applications et de gestion de bureau virtuel.

2.1.2 SolarWinds Dameware :

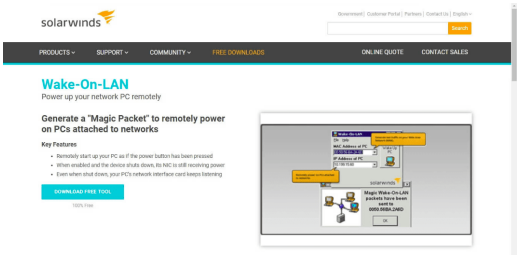

Figure 12 : SolarWinds Dameware

Les informations fournies dans les sources indiquent que *SolarWinds Dameware* est un outil de support à distance qui offre des fonctionnalités avancées telles que la gestion centralisée des

utilisateurs, des licences et des hôtes, la synchronisation avec Active Directory, la prise en charge multiplateforme, le contrôle à distance des ordinateurs Windows, macOS X et Linux, ainsi que des fonctionnalités de sécurité avancées telles que le contrôle granulaire des accès, le chiffrement AES 256 et la compatibilité avec des algorithmes de chiffrement sécurisés. Dameware permet également de créer des sessions Internet pour prendre en charge les utilisateurs distants et offre des fonctionnalités de chat en direct, de capture d'écran et de transfert de fichiers. Il propose une gestion centralisée des licences et des listes d'hôtes globales pour faciliter le déploiement et la prestation de services. [6]

En comparaison, un terminal server est une plateforme de calcul qui permet aux utilisateurs d'accéder à des applications et des données stockées sur un serveur à distance. Contrairement à Dameware qui se concentre sur le support à distance et la gestion centralisée, un terminal server est principalement utilisé pour fournir un environnement de bureau virtuel aux utilisateurs, leur permettant d'exécuter des applications et d'accéder à des données à distance.

En résumé, SolarWinds Dameware se distingue par ses fonctionnalités avancées de support à distance, de gestion centralisée et de sécurité, tandis qu'un terminal server est une plateforme plus large permettant l'accès à des applications et des données à distance.

2.1.3 TeamViewer :

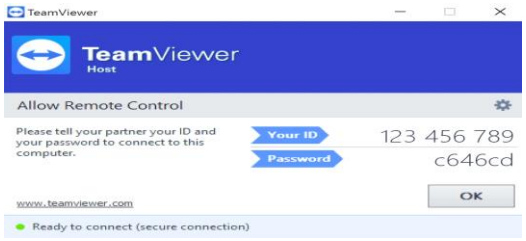

Figure 13 : TeamViewer

TeamViewer est un logiciel de contrôle à distance qui permet aux utilisateurs de se connecter à des ordinateurs et des serveurs à distance, offrant des fonctionnalités de contrôle, de gestion et de collaboration. [7]

2.1.3.1 Caractéristiques :

TeamViewer :

- Offre des fonctionnalités de contrôle à distance, de gestion et de collaboration.
- Supporte les systèmes d'exploitation Windows, macOS, Linux, iOS et Android.
- Permet de créer des sessions multi-utilisateurs sur les serveurs Terminal Server.
- Propose des options de sécurité renforcées, telles que l'authentification multifacteur et le chiffrement AES 256.
- Disponible en version gratuite pour les utilisateurs personnels, mais nécessite une licence pour les utilisations commerciales.

2.1.3.2 Avantages et inconvénients :

TeamViewer :

- Avantages : offre des fonctionnalités de contrôle à distance, de gestion et de collaboration ; supporte les systèmes d'exploitation multi-plateforme ; offre des options de sécurité renforcées.
- Inconvénients : nécessite une licence pour les utilisations commerciales ; peut être complexe à configurer pour les utilisateurs non expérimentés.

En résumé, TeamViewer est un logiciel de contrôle à distance qui offre des fonctionnalités de contrôle, de gestion et de collaboration, tandis que Terminal Server est un service de bureau virtuel qui permet aux utilisateurs de se connecter à des serveurs pour accéder à des applications et des données à distance. Les deux solutions offrent des fonctionnalités de sécurité renforcées, mais TeamViewer nécessite une licence pour les utilisations commerciales, tandis que Terminal Server est disponible dans les versions Windows et Linux.

3 La solution : Terminale server :

Definition de terminal server :

Un serveur terminal est un type de serveur informatique qui permet aux utilisateurs de se connecter à des applications et des environnements de bureau distants depuis leurs propres appareils, qu'il s'agisse d'ordinateurs, de tablettes ou de smartphones. Ce serveur centralise les applications et les données, prenant en charge les tâches de traitement et de rendu graphique, et transmet les informations ainsi que l'interface utilisateur via le réseau vers le client.

Les utilisateurs peuvent accéder à ces ressources à distance grâce à un client de bureau à distance, tel que le protocole RDP (Remote Desktop Protocol), qui permet de visualiser et de contrôler les sessions distantes. Les serveurs terminaux peuvent être configurés pour gérer plusieurs sessions simultanées, permettant ainsi à plusieurs utilisateurs de collaborer sur des ressources, des applications et des données partagées. [8]

3.1 Expression de la politique de sécurité :

Les fonctionnalités de sécurité du serveur de terminaux comprennent :

• Mot de passe de supervision et de port.

• Verrouillage de port.

• Authentification avec prise en charge de PAP.

• Attribution du niveau d'accès par utilisateur.

• Journalisation du service.

• Installation d'un dispositif de journalisation pour l'audit et la facturation.

• Réinitialisation automatique du modem.

3.2 Les équipements réseau :

Les fonctionnalités du logiciel Terminal Server comprennent :

- Prise en charge des protocoles TCP/IP, y compris telnet et rlogin.
- Prise en charge de l'accès distant, notamment PPP, SLIP et CSLIP.

- Prise en charge de l'impression via lpd, rcp et des utilitaires.
- Prise en charge des modems via PPP et des utilitaires.
- Une interface de menu orientée fenêtre avec des menus contextuels et une aide à l'écran (ligne de commande également disponible).
- ARP pour la configuration basée sur le réseau.
- Affichage dynamique des statistiques et rapports d'état de ligne pour un diagnostic rapide des problèmes.
- Écrans multiples sur les terminaux.
- Prise en charge complète des MIB SNMP, permettant une configuration à distance via SNMP ainsi que la collecte de statistiques.
- Interopérabilité avec le routage IP à travers les tables de passerelle.
- Prise en charge du serveur de noms de domaine.
- Prise en charge de WINS pour les environnements Windows®.
- Fonctions de copie et de sauvegarde de la configuration des ports.

3.3 Le protocole terminal server :

3.3.1 Historique :

Le terme « terminal server » a une longue histoire, et sa signification a évolué au fil du temps. Il est apparu en 1984 avec le développement de l'interface utilisateur graphique X Window System pour les systèmes Unix, alors très répandus. Cette interface, également connue sous le nom de « X11 », disposait de son propre protocole réseau. La révolution de ce système résidait dans sa capacité à envoyer la sortie de l'hôte vers des terminaux distants, permettant une utilisation plus flexible des ressources informatiques. Ainsi, même si le matériel du terminal restait minimal, les ordinateurs hôtes évoluaient vers le concept de serveur terminal.

Avec la croissance exponentielle des ordinateurs personnels, la nécessité d'un serveur terminal central pour répartir la puissance de calcul et gérer les applications a diminué. Les systèmes indépendants, capables d'installer leurs propres systèmes d'exploitation, ont remplacé les terminaux dépendant du serveur. Toutefois, dans le secteur commercial, la gestion centralisée a conservé son importance. Les programmes des systèmes informatiques et serveurs sont restés indispensables, faisant des serveurs terminaux la solution idéale pour permettre l'accès aux clients. De nos jours, le terme « terminal server » fait de plus en plus référence aux solutions logicielles

développées à cet effet, comme le programme et protocole réseau Telnet 3270 pour l'accès aux systèmes IBM. [8]

3.4 Presentation de protocole terminale server :

Le Terminal Server est à l'origine une technologie permettant aux utilisateurs d'accéder à des programmes et des fichiers situés sur un autre ordinateur via n'importe quel appareil disposant d'une connexion Internet. Avec Terminal Server, on accède à un bureau virtuel sur l'ordinateur distant, ce qui permet d'exécuter des applications, de parcourir des fichiers et de réaliser des tâches nécessitant une grande puissance de traitement.

L'objectif principal de Terminal Server est de permettre le partage de l'utilisation d'un serveur et de ses applications avec des PC clients légers. Cela permet une utilisation efficace des ressources informatiques centralisées tout en offrant une expérience utilisateur complète à distance. [8]

Le Terminal Server permet :

- D'utiliser le même environnement de travail, quel que soit le système d'exploitation utilisé sur le PC (Windows 3.1, 3.11, 95, 98, NT 4.0, Windows 2000, XP, 2003, etc.).
- D'éviter de renouveler un parc informatique vieillissant ou d'investir dans des machines coûteuses, en optant pour des solutions plus économiques.
- De changer de machine sans fermer sa session et ses programmes en cours.
- D'équilibrer la charge de travail entre plusieurs serveurs Terminal Server pour optimiser les performances et la disponibilité.

On peut l'utiliser :

Le Terminal Server est particulièrement utile :

- Pour des utilisateurs ayant des profils similaires en termes d'applications utilisées.
- Pour réduire les coûts de mise à jour du parc informatique.
- Pour diminuer les coûts de gestion en centralisant la configuration uniquement sur le serveur.
- Pour permettre à des utilisateurs distants, via une connexion Internet, d'accéder à des applications centralisées.
- Pour administrer des serveurs à distance de manière efficace.

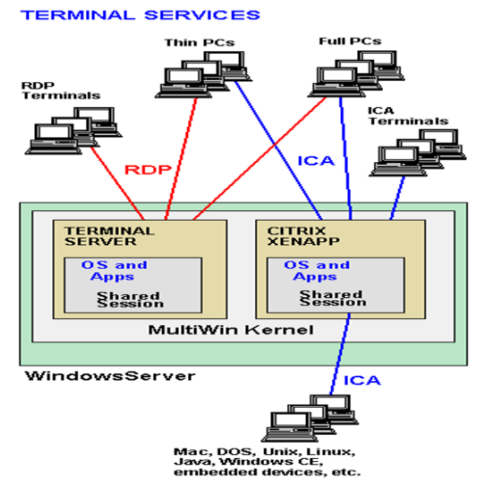

Figure 14 : Terminal Server

Les services Terminal Server utilisent les protocoles RDP et ICA

3.5 Role de protocole terminal server :

Il existe deux manières de mettre en oeuvre Terminal Server :

- **En mode administration distante :** Le mode Administration à distance ne déploie que les composants d'accès distant de Services Terminal Server, excluant les composants de partage des applications. Cela garantit une charge minimale sur les serveurs critiques. Les administrateurs peuvent ainsi gérer le serveur à distance comme s'ils étaient physiquement présents, avec une restriction de deux connexions administratives simultanées.
- **En mode serveur d'applications :** Vous pouvez déployer et gérer des applications à partir d'un emplacement central, ce qui épargne aux administrateurs le temps nécessaire au développement et au déploiement, tout en réduisant les efforts de maintenance et de mise à niveau. Une fois qu'une application est déployée dans les services Terminal Server, divers clients peuvent s'y connecter via des connexions distantes, locales ou longue distance.

  L'installation des applications se fait directement sur le serveur Terminal Server et ne peut être réalisée que par un administrateur, de serveur à serveur, sous réserve de la configuration appropriée de la stratégie de groupe.

  En plus des licences requises pour les services Terminal Server, il existe deux licences optionnelles : la licence de Connecteur Internet de services Terminal Server de Windows 2000

(qui permet l'accès anonyme à 200 utilisateurs) et la licence d'accès client Terminal Server de Windows 2000 pour le travail à domicile.

Pour améliorer les capacités du Terminal Server, l'utilisation de MetaFrame de Citrix Systems est recommandée. MetaFrame facilite la gestion des périphériques et des ressources locales des clients, offrant ainsi une expérience utilisateur enrichie et une gestion améliorée du réseau. [9]

3.6 Coûts liés à l'environnement client-terminal serveur :

Les coûts de licence représentent l'une des principales dépenses associées aux serveurs de terminaux, et ils varient en fonction du nombre d'utilisateurs simultanés et des logiciels nécessaires. Il est crucial de décider quelles applications centraliser, que ce soit des produits propriétaires tels que Windows et Microsoft Office, ou des alternatives open-source comme Linux et LibreOffice. En plus des coûts de service, les opérateurs doivent également prendre en compte :

- **Matériel informatique :** Assurer une puissance de calcul suffisante et prévoir la redondance pour remplacer rapidement les composants défectueux. Cela inclut l'achat initial de serveurs robustes et la planification pour l'expansion future si nécessaire.
- **Maintenance et exploitation :** Budgetiser les coûts de maintenance, de câblage, d'électricité, etc., nécessaires au bon fonctionnement continu des serveurs de terminaux. Il est important d'inclure ces dépenses dans le budget global pour assurer la disponibilité et la performance.
- **Maintenance des applications :** Assurer la maintenance régulière des applications installées sur les serveurs de terminaux. Cela comprend les mises à jour logicielles, les adaptations nécessaires pour assurer la compatibilité avec les nouveaux systèmes d'exploitation ou matériels, ainsi que l'installation de nouveaux services terminaux au besoin.
- **Sauvegarde et protection :** Investir dans des logiciels de sécurité et des solutions de sauvegarde robustes pour protéger les services terminaux et les bases de données contre les pannes matérielles, les pertes de données et les accès non autorisés. La sauvegarde régulière des données critiques est essentielle pour garantir une reprise rapide en cas de sinistre.
- **Gestion des droits :** Allouer des ressources budgétaires pour gérer les droits d'accès de manière sécurisée à long terme. Cela inclut l'authentification des utilisateurs, l'autorisation

appropriée pour l'accès aux applications et données sensibles, ainsi que la gestion des identités et des accès (IAM) pour maintenir la sécurité des systèmes. [10]

3.7 Terminal server : les composants élémentaires :

Trois modules sont nécessaires pour mettre en place une structure client terminal server :

1. **Ressources matérielles serveur** prenant en charge les systèmes multi-utilisateurs.
2. **Protocole réseau** pour l'accès à distance.
3. **Application client** terminal server.

Comme tout serveur, un serveur de terminal nécessite des ressources matérielles adéquates pour fonctionner efficacement. Il est crucial de s'assurer que suffisamment de puissance de calcul est disponible pour héberger chaque application ainsi que le système d'exploitation du serveur. La performance du processeur est particulièrement importante, avec une préférence pour les processeurs multi-cœurs. L'espace de travail et l'espace disque sont également critiques et dépendent des exigences spécifiques des applications gérées. De plus, le nombre de clients accédant simultanément aux services du serveur de terminal est un facteur déterminant.

Ensuite, un protocole est nécessaire pour établir la communication entre le serveur de terminal et le client. Ce protocole définit les directives pour l'échange de données, permettant ainsi un accès à distance aux utilisateurs du service terminal. Alors que les protocoles initiaux, comme le X11 mentionné précédemment, se concentraient principalement sur la configuration de la connexion, les nouveaux protocoles tels que Citrix ICA (Independent Computing Architecture) ou le protocole RDP (Remote Desktop Protocol) de Microsoft offrent également des fonctionnalités avancées telles que la compression, le chiffrement et la mise en cache des données transmises.

Enfin, un logiciel client doit être installé sur chaque appareil pour permettre aux utilisateurs de se connecter au serveur de terminal via le protocole à distance et d'utiliser les applications prévues. Souvent, l'architecture logicielle et matérielle est complétée par un serveur de gestion des licences d'accès.

3.8 Principes de protocole Terminale server :

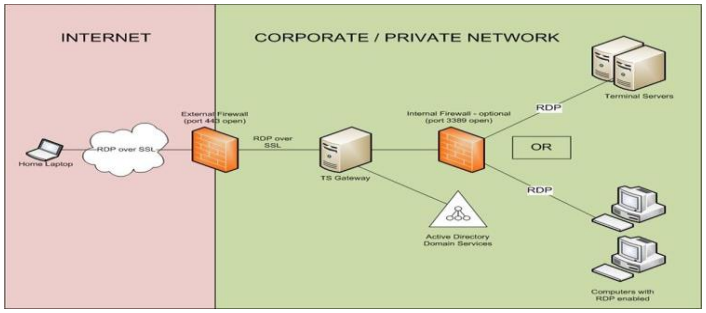

Figure 15 : Principes de protocole Terminale server

Lorsqu'on se connecte à un serveur Terminal Server, une nouvelle session est créée et personnalisée selon nos préférences. Les ressources telles que l'espace disque, le processeur et la mémoire sont allouées de manière à garantir le bon fonctionnement de toutes les sessions, sans compromettre les performances des autres.

Sur le serveur Terminal Server, c'est le serveur lui-même qui exécute les applications. Nos actions via le clavier et la souris sont transmises au serveur, qui renvoie les mises à jour d'écran à notre appareil.

Le protocole RDP (Remote Desktop Protocol) est utilisé pour établir la connexion entre le serveur et notre appareil. Ce protocole est spécifiquement optimisé pour l'accès à distance, assurant ainsi une expérience utilisateur fluide et fiable.

3.9 Le bureau à distance :

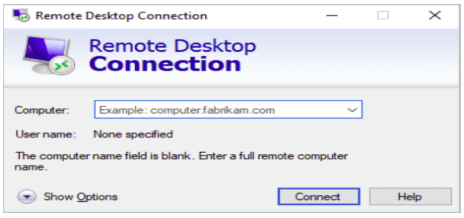

Figure 16 : Le bureau à distance

Le Remote Desktop Connection (RDC) ou Bureau à distance est une technologie qui permet à un utilisateur d'ordinateur de se connecter à un ordinateur distant ou à un serveur de terminaux situé dans un lieu différent. Le protocole de Bureau à distance (RDP), développé par Microsoft, est un protocole propriétaire sécurisé utilisé pour cette communication réseau lorsque l'utilisateur

travaille à distance. En plus du RDP, d'autres protocoles comme l'Independent Computing Architecture (ICA) et le Virtual Network Computing (VNC) sont également utilisés par les logiciels de bureau à distance.

Le RDP est largement reconnu pour sa fiabilité et sa compatibilité étendue avec divers systèmes d'exploitation tels que Windows, Mac, Linux, Unix, Android et iOS. Il permet aux utilisateurs d'accéder à distance à des ordinateurs de bureau professionnels pour effectuer des diagnostics ou résoudre des problèmes rencontrés par les utilisateurs. [11]

3.10 Avantages de l'utilisation de Terminal Server :

- **Flexibilité :** Ils permettent un accès global aux infrastructures informatiques spécifiques de l'organisation, offrant un choix varié de terminaux et de systèmes d'exploitation pour les utilisateurs.
- **Hautes performances :** Les utilisateurs bénéficient de performances supérieures par rapport aux systèmes de bureau standard. Les mises à niveau du serveur peuvent améliorer les performances sans nécessiter de mise à niveau des clients légers locaux.
- **Fiabilité :** Les clients légers sont robustes et fiables car ils ne possèdent pas de pièces mobiles ni de disques durs, nécessitent peu de configuration et ne disposent pas de système d'exploitation, réduisant ainsi les risques de panne matérielle par rapport aux ordinateurs de bureau standard.
- **Rentabilité :** Le déploiement de l'architecture à distance avec des licences permet à l'entreprise de réaliser des économies significatives. L'utilisation des serveurs de terminaux est rentable et contribue à maximiser les économies globales.
- **Sécurité informatique :** Il est possible d'intégrer des solutions de sauvegarde et des concepts de sécurité complets dans un environnement de serveur de terminaux. Les données traitées demeurent dans les infrastructures internes, renforçant ainsi la sécurité et le contrôle des informations sensibles.

3.11 les inconvénients du modèle client terminal server :

- **Compatibilité :** Certains logiciels peuvent ne pas être pleinement compatibles avec les serveurs de terminaux, ce qui peut limiter les capacités opérationnelles de l'entreprise. Cela

peut nécessiter la recherche d'alternatives pour exécuter certains processus spécifiques, ce qui peut affecter la productivité et les opérations.

- **Uniformité :** L'uniformité est souvent difficile à maintenir lorsque différents clients utilisent des solutions logicielles variées. Cela peut entraîner des disparités de performances et compliquer la gestion centralisée des applications et des processus au sein d'une instance centrale. Cette hétérogénéité peut perturber le flux de travail et nécessiter des efforts supplémentaires pour standardiser les pratiques.

L'intégration d'un serveur de terminaux est bénéfique si les entreprises opèrent dans des endroits différents.

4 Conclusion :

En conclusion, ce chapitre nous a permis de poser les bases de notre projet en établissant un cadre clair pour l'évaluation des différentes solutions de support à distance. Les prochaines étapes consisteront à effectuer des tests pratiques et à analyser les résultats afin de formuler des recommandations concrètes pour l'implémentation de la solution optimale.

Chapiter 4 : Mise en oeuvre et réalisation

1 Introduction

Ce chapitre est consacré à la mise en œuvre et à la réalisation pratique de la solution choisie, portant sur l'utilisation de Terminal Server comme solution de partage de ressources et de support à distance. Après avoir établi les bases théoriques et comparé diverses solutions potentielles, nous avons choisi Terminal Server pour ses nombreux avantages, notamment en termes de centralisation, de sécurité et de performance.

2 Description de la solution choisie:

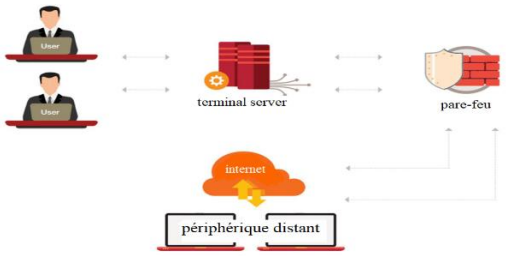

Figure 17 : Description de la solution choisie

Description de la solution

La solution que nous avons choisie consiste à installer un serveur terminal au niveau de local du laboratoire LAMIS en utilisant la machine HP Z8 G4 dont les caractéristiques ont été citées précédemment en suivant les étapes suivantes :

1. Installation de serveur
2. Configuration de service terminal server
3. Configuration de serveur
    - Les utilisateurs
    - Le stockage
    - La sécurité

3 Topologie physique de réseau

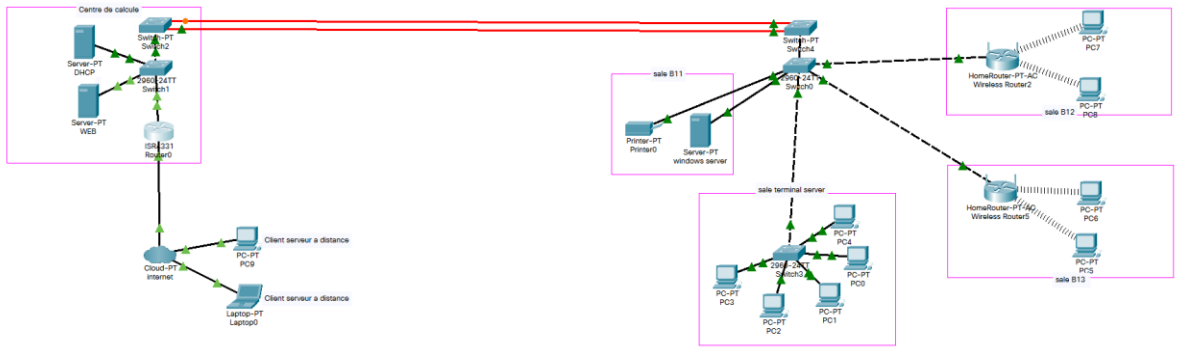

Figure 18 : Topologie physique de réseau

4 Installation de serveur :

Pour donner le rôle de serveur à une machine, nous devons installer un système serveur. Pour notre travail, nous avons choisi Windows Server, qui est un système d'exploitation serveur polyvalent et puissant, basé sur les améliorations que Microsoft a apportées aux différentes versions de Windows Server. Ce système présente un certain nombre de caractéristiques, car ils font partie du même projet de développement. Ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage. Ce système nous offre un certain nombre de fonctionnalités de gestion de réseau et des utilisateurs réseau, parmi lesquelles on trouve :

4.1 Utilisateurs et groupes :

Utilisateurs et ordinateurs d'Active directopy (AD) est un des principaux outils d'administration pour gérer l'active directory, avec cet utilitaire, on peut prendre en charge tous les utilisateurs, les groupes et les taches informatique, et gérer les unités d'organisation [12]. Les groupes ou les stratégies de groupe sert a simplifier les taches de l'administrateur en leur offrant un contrôle centralisé sur les privilèges, autorisations et capacités des utilisateurs et des ordinateurs.

4.2 DNS domain name system :

DNS est un service internet standard qui organise les groupes d'ordinateurs en domaines. Les domaine DNS sont organisés selon une structure hierarchique.la hiérarchie de domaine DNS est définie a l'échelle de l'internet, et les différent niveaux de la hiérarchie identifient les ordinateurs, les domaines organisations et domaine de premier niveau.

DNS est utilisé pour faire correspondre les noms d'hôtes a des adresses IP numérique, par le biais de DNS, une hiérarchie de domaine AD peut être définie à l'échelle de l'internet, ou bien la hiérarchie de domaine peut être séparée de l'internet et demeure privée [13].

4.3 Protocole DHCP (dynamic host configuration protocol) :

Le Protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une machine, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.

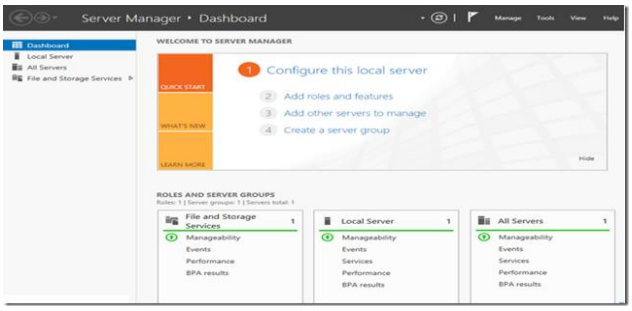

Figure 19 : Windows server

Apres l'etape de l'installation la modification de nom de la machine est necessaire n

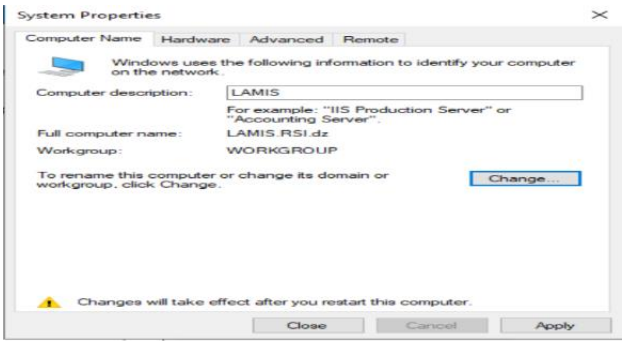

Figure 20 : Nom de serveur

Pour l'adresse IP, nous étions obligés de respecter le schéma d'adressage de réseau de l'université pour intégrer ce serveur dans le réseau. Pour cela, nous avons choisi l'adresse statique suivante :.

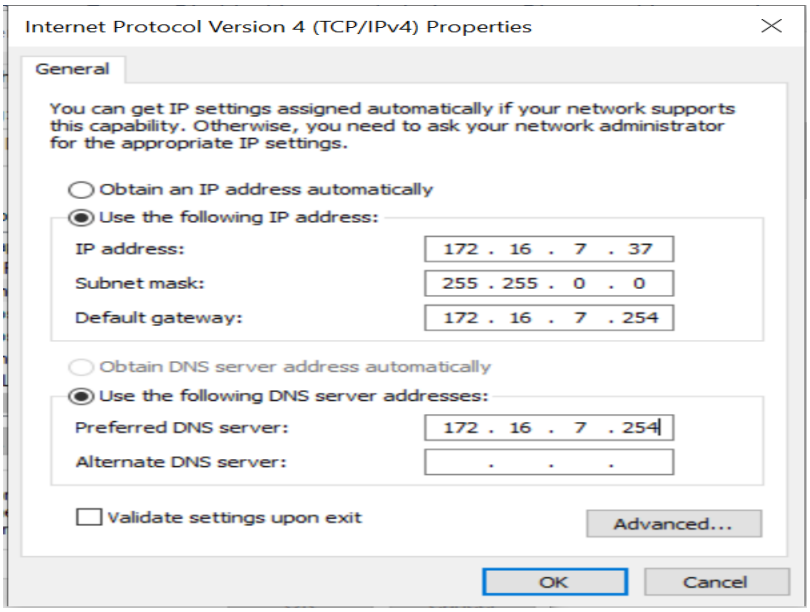

Figure 21 : L'adresse IP de serveur

Après cette étape, le serveur est prêt à recevoir un rôle dans le réseau.

5 Installation de terminal server:

- Pour démarrer l'installation, nous lançons le Gestionnaire de serveur. Cela peut être fait à l'aide de la commande **servermanager.exe** dans la fenêtre Exécuter.

5.1 Configuration des rôles et des composants :

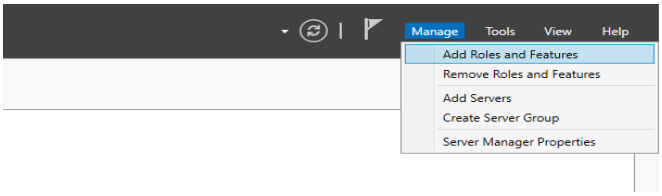

Figure 22 : Configuration des rôles et des composants

Dans l'élément Rôles du serveur, nous cochons la case Services Bureau à distance et cliquons

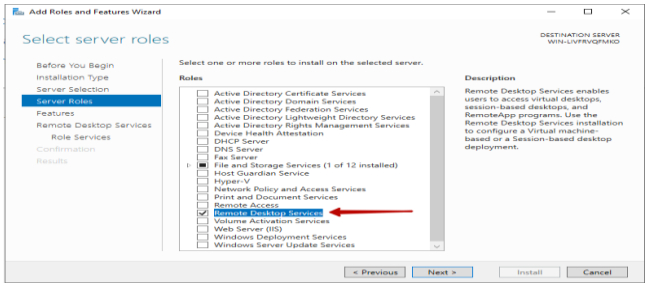

Figure 23 : Installation Services Bureau à distance

Dans la section Services de rôle, nous sélectionnons les services de rôle que nous souhaitons installer, tels que la Licence Bureau à distance, on doit aussi ajouter des fonctionnalités telque bureau adistance. Après avoir redémarré le serveur, nous pouvons observer un message concernant l'installation réussie, et Pour vérifier les licences, exécutons le diagnostic de licences Bureau à distance.

Ensuite, nous ajoutons les licences nécessaires.

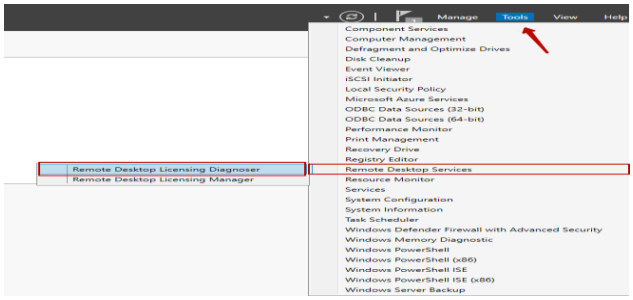

Figure 24 : ajoutons les licences nécessaires

Comme nous pouvons le constater, aucune licence n'est installée pour le moment.

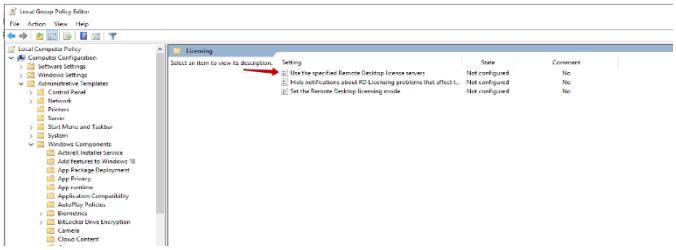

Figure 25 : modifier Utiliser les serveurs de licences

- Nous traduisons le mode en Activé.
- Ci-dessous, nous décrivons le serveur de licences. Dans cet exemple, il s'agit de localhost.
- Nous pouvons également spécifier l'IP 127.0.0.1 ou le nom d'hôte.

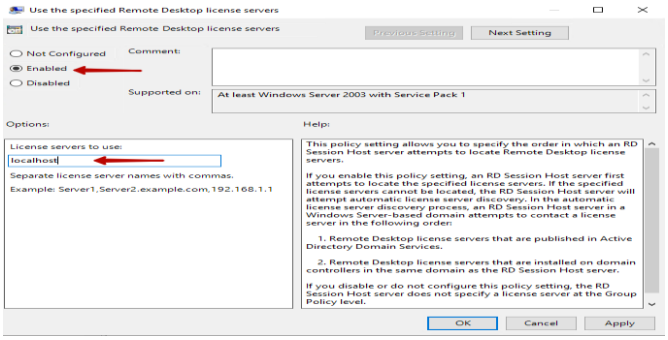

Figure 26 : S'agit de localhost

Maintenant, nous modifions Définir le mode de licence à distance.

Comme nous pouvons le voir, l'état du serveur est Non activé. Pour l'activer, nous devons acheter des licences par utilisateur ou par poste, ou utiliser le mode gratuit qui ne dure qu'un mois.

5.2 Configuration des comptes locaux

Afin de pouvoir autoriser les utilisateurs à se connecter nominativement, on utilise les comptes locaux sur le serveur pour permettre l'authentification.

Pour valider notre solution, nous avons créé des comptes avec le nom « User » qui seront affectés aux membres du labo et aux doctorants.

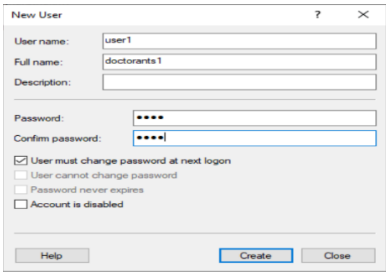

Figure 27 : Création user 1

Ces comptes utilisateurs doivent être ajoutés dans le groupe prédéfini « utilisateurs de bureau à distance » pour pouvoir utiliser ce service.

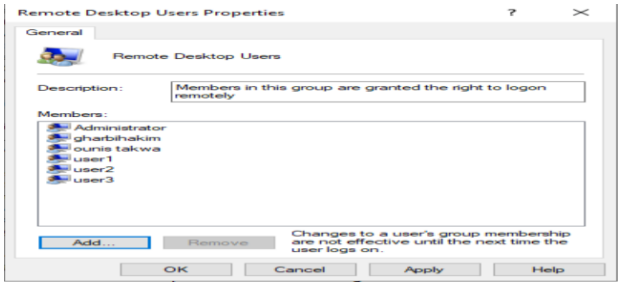

Figure 28 : Groupe utilisateurs de bureau à distance

5.3 Configuration du port Bureau à distance (port 3389) dans le pare-feu Windows.

Pour que les accès à distance ne soient pas bloqués par le pare-feu Windows, on doit ouvrir le port 3389 dans les propriétés de ce programme

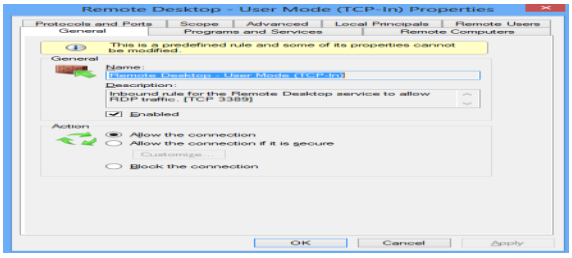

Figure 29 : Le port Bureau à distance

5.4 Configurons la redirection de port (traduction de port) dans le routeur

Connectons-nous au page de configuration du routeur et accédons à la section « Redirection de port ». Ajoutons une nouvelle règle « Redirection de port » pour le port TCP 3389 à transférer vers l'adresse IP interne du serveur.

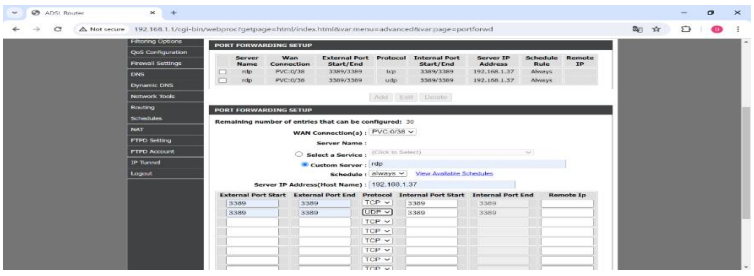

Figure 30 : Configurons la redirection de port dans le routeur

Pour voir si la redirection de port a été correctement configurée, nous pouvons utiliser notre outil réseau Port Check pour voir si le port correspondant est ouvert. Si nous obtenons une réponse «Succès » lors de la vérification du port, cela signifie que notre réseau a été correctement configuré.

5.5 Réseautage de Serveurs:

Ce serveur peut être utilisé dans trois cas possibles :

1. **Utilisation uniquement à l'intérieur de l'université :** Dans ce scénario, nous conservons l'adresse définie précédemment et le serveur sera accessible uniquement lorsque nous nous connectons depuis le réseau de l'université.

2. **Utilisation à l'extérieur de l'université avec adresse publique de l'université :** Pour ce faire, nous déplaçons le serveur vers les locaux du centre de calcul, et nous lui affectons une adresse publique, ce qui offre la possibilité d'accéder aux serveurs de n'importe quel endroit, voire de les administrer à distance.

3. **Utilisation à l'extérieur de l'université avec connexion ADSL :** Cette solution nécessite une ligne téléphonique et une connexion ADSL. Avec des modifications sur les paramètres du routeur ADSL pour utiliser le DNS dynamique (DDNS), nous procédons comme suit :

5.6 Configuration d'un nom d'hôte :

Les fournisseurs de services Internet modifient régulièrement l'adresse IP, mais avec le DNS dynamique, nous pouvons garder notre domaine pointant vers l'adresse IP actuelle de notre serveur domestique ou d'autres appareils. Nous pouvons enregistrer notre propre nom de domaine (**lamis.ddns.net**) et nous inscrire au service DNS dynamique.

- Connectons-nous à notre compte No-IP ou créons un compte.
- Sélectionnons "Ajouter un nouveau nom d'hôte".
- Saisissons le nom d'hôte et sélectionnons l'un des domaines dans le menu déroulant.
- Ce sera la nouvelle adresse Web de l'appareil.
- À côté de "Type de service", sélectionnons "DNS host A".

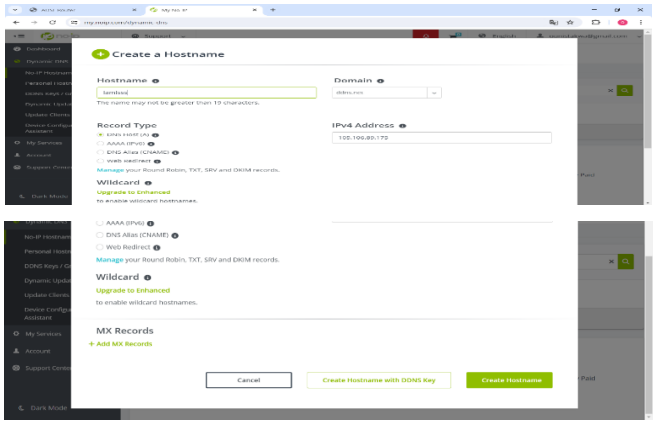

Figure 30 : Créons un compte.

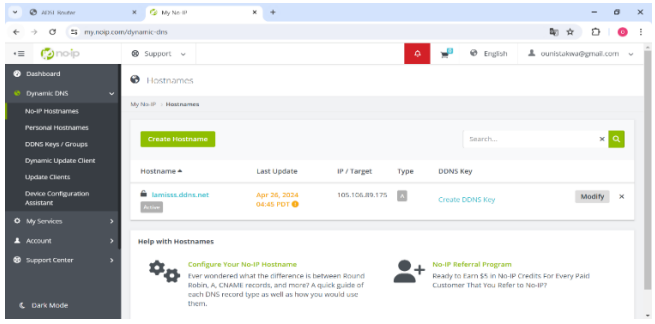

Figure 31 : Compte No-IP

Téléchargeons le logiciel client approprié et exécutons-le sur l'ordinateur pour conserver le nom d'hôte mappé sur l'adresse IP dynamique. Nous pouvons également configurer le service DDNS sur le routeur s'il le prend en charge. Nous devrions maintenant pouvoir accéder à notre ordinateur en utilisant le nom lamisss.ddns.net depuis Internet via Remote Desktop en utilisant n'importe quel client Remote Desktop compatible et notre nom de domaine.

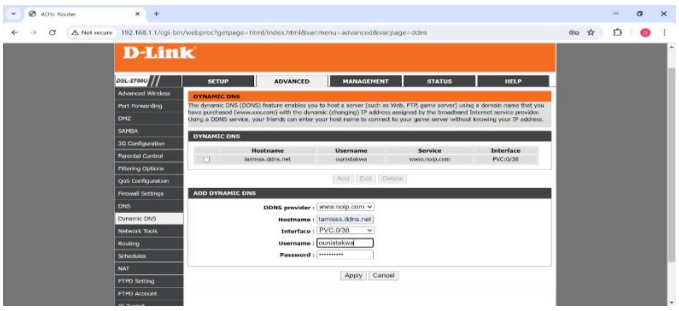

Figure 32 : Le service DDNS

6 Configuation aditionnelle de serveur

Pour assurer que le serveur terminal accomplit son rôle efficacement, on doit configurer les éléments suivants :

- Le stockage
- La gestion des utilisateurs
- La securité de serveur

6.1 Le stockage :

Pour preserver les ressources de serveur en terme de stockage on doit activer le système de quotas sur les disques et qui doivent etre convertis on disques dynamiques

6.1.1 La gestion des quotas

La gestion des quotas est une fonctionnalité précieuse qui nous permet de restreindre la capacité de stockage des ressources partagées dans Windows Server. Si nous créons des quotas, nous limiterons l'espace alloué à un volume ou à un dossier, nous permettant ainsi de pratiquer facilement la gestion de la capacité.

6.1.1.1 Gestion des quotas dans windows server

Pour définir des quotas dans Windows Server, nous devrons utiliser un outil appelé File Server Resource Manager (FSRM). Cet outil nous aide à gérer et à organiser les données conservées sur les serveurs de fichiers. L'outil File Server Resource Manager comprend les cinq fonctionnalités suivantes:

- **Infrastructure de classification de fichiers :** cette fonctionnalité nous permet d'organiser les fichiers et de mettre en œuvre des politiques.
- **Tâches de gestion de fichiers :** elles nous permettent de mettre en œuvre des politiques ou des tâches conditionnelles.
- **Gestion des quotas :** elle nous aide à restreindre l'espace disponible sur les dossiers partagés.

- **Gestion du filtrage des fichiers :** elle nous permet de limiter le type de fichiers que les utilisateurs peuvent conserver. Par exemple, nous pouvons définir un écran de fichiers pour empêcher les utilisateurs de créer des fichiers MP3 sur le serveur de fichiers.
- **Rapports de stockage :** avec cette fonctionnalité, nous pouvons générer des rapports pour comprendre les tendances d'utilisation du disque et la manière dont les données sont organisées, ce qui nous permet de repérer les activités non autorisées.

6.1.1.2 Configuration du gestionnaire de ressources du serveur de fichiers

Nous devons installer l'outil File Server Resource Manager avant de l'utiliser pour la gestion des quotas. Un moyen rapide de terminer sa configuration consiste à utiliser le gestionnaire de serveur GUI.

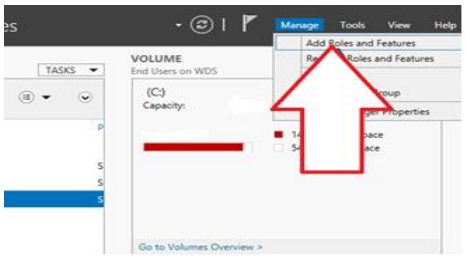

Figure 33 : Ajouter des rôles et des fonctionnalités

6.1.1.3 Création de quotas à l'aide de fsrm

Comme mentionné précédemment, la gestion des quotas nous permet de définir des restrictions et de définir l'étendue de l'espace disponible pour les utilisateurs sur le serveur. Par exemple, nous pouvons limiter tous les utilisateurs à un maximum de 5 Go sur un dossier partagé. En tant que tel, les utilisateurs ne peuvent pas ajouter de données au dossier dépassant 5 Go. Nous pouvons également configurer l'outil File Server Resource Manager pour qu'il envoie des notifications chaque fois que la limite d'utilisation spécifiée est atteinte. Par exemple, nous pouvons spécifier qu'un email doit être envoyé si 85% de l'espace a été consommé. La création de quotas à l'aide de l'outil FSRM est un processus en deux étapes :

- Créer un modèle
- Créer un quota.

a) Créer un modèle :

Avant de définir des quotas, nous devons soit créer un modèle de quota, soit choisir un modèle par défaut déjà disponible sur l'outil File Server Resource Manager. Il est recommandé de créer des quotas uniquement à partir de modèles. De cette façon, nous pouvons facilement gérer nos quotas en apportant des modifications aux modèles plutôt qu'aux quotas individuels. L'emplacement central unique pour la gestion des quotas facilite la mise en œuvre des règles de politique de stockage. **Créer un quota :**

Après avoir configuré le modèle de quota ou utilisé un modèle de quota par défaut, nous devons créer le quota.

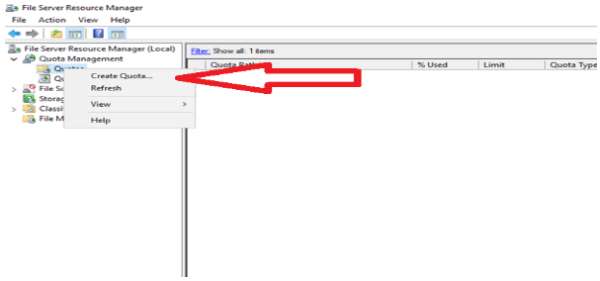

Figure 34 : Créer un quota

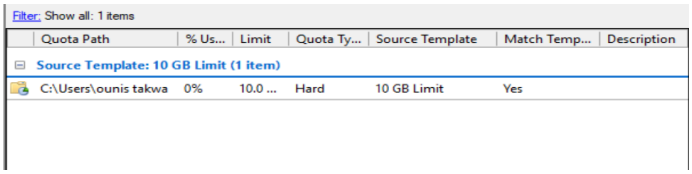

Figure 35 : Un quota pour user ounis takwa

6.1.2 Modifier les paramètres du registre

Étape 1 : Nous appuyons sur Win + R, puis nous entrez « regedit », et appuyons sur OK.

Étape 2 : Navigation :

HKEY_LOCAL_MACHINE > LOGICIEL > Microsoft > Windows NT > Version actuelle > Winlogon

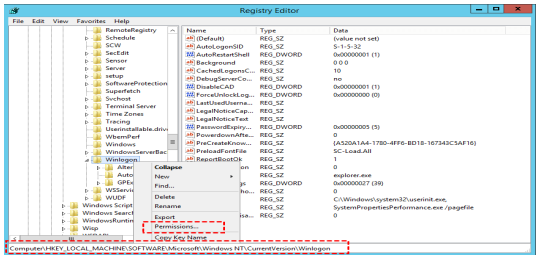

Figure 36 : Modifier les paramètres du registre

Étape 3. Choisissons l'utilisateur sous la case Sécurité et assurons-nous que l'autorisation de lecture est définie sur « Autoriser ».

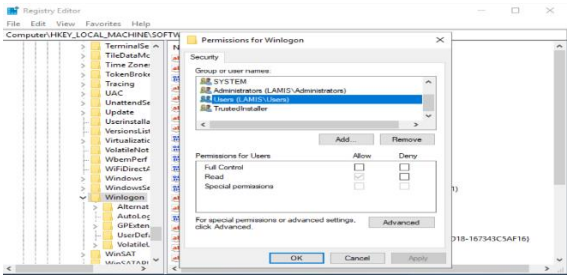

Figure 37 : L'autorisation de lecture est définie

6.1.3 Le disque dynamique

Le disque étranger dynamique, compatible avec Windows 7, Windows 8 et Windows 10, consiste à créer des volumes illimités sur le disque. Ses volumes illimités permettent de disposer d'un espace énorme pour l'exécution et le stockage. En outre, les disques dynamiques peuvent également modifier la configuration de Windows.

Ce disque dynamique d'un ordinateur Windows gère tous ses volumes via la base de données LDM. LDM est l'abréviation de **logical disk manager**. Chaque disque dynamique porte une base de données LDM cachée de 1 Mo, qui stocke toutes les informations locales présentes sur les volumes. D'autres informations telles que la lettre du lecteur, l'étiquette du volume, le secteur du volume, la taille du volume, le système de fichiers, peuvent toutes être stockées dans la base de données LDM.

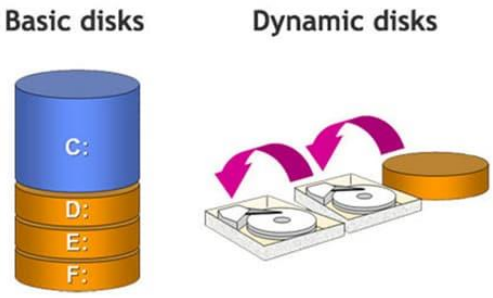

Figure 38 : Un disque de base et un disque dynamique

6.1.3.1 La différence entre un disque de base et un disque dynamique :

Pour l'instant, vous êtes familiarisé avec le disque dynamique et sa différence avec le disque de base en général, alors vérifions les différences dans leur ensemble. Cette section présente l'ensemble des différences entre le stockage sur disque de base et le stockage sur disque dynamique, ainsi que les types de volumes qui peuvent être créés.

Critères	Disque de base	Disque dynamique
Limite de découpage	Prend en charge 4 partitions : une primaire et trois étendues	Aucune limite pour les partitions Cependant, chaque lecteur doit être lié à au moins une partition principale
La résistance aux pannes	Aucune tolérance aux erreurs n'est accordée Vos données sont perdues en cas de corruption ou de suppression du disque	La redondance des données sur des volumes en miroir, en miroir à bandes et RAID-5
Systèmes d'exploitation compatibles	Tous les systèmes d'exploitation depuis MS-DOS	Windows 2000 et les versions ultérieures des systèmes d'exploitation, y compris Windows Exchange Server
Accès à l'information	Configuration simple autorisant uniquement l'accès aux données présentes sur un seul disque	Permet d'accéder aux données à partir de disques différents sans duplication

Convenience de stockage des données	Facile de stocker des données sur des partitions locales	Il est difficile de stocker des données, surtout lorsque plusieurs disques sont configurés avec différents types de volumes
Facilité de configuration	Facile à configurer, tout utilisateur moyen peut le faire	Difficile à configurer si vous ne maîtrisez pas l'informatique
Coût de l'application	Bas	Élevée
Oui, il supporte les disques virtuels.	Non	Oui

Tableau 2 : La différence entre un disque de base et un disque dynamique

6.1.3.2 Comment convertir un disque dynamique en disque de base ?

Cette section nous guidera pour convertir un disque de base en disque dynamique. Grâce à ce transfert, nous pouvons créer de l'espace de stockage et augmenter les performances du disque. Suivons les étapes suivantes pour effectuer la conversion entre un disque de base et un disque dynamique.

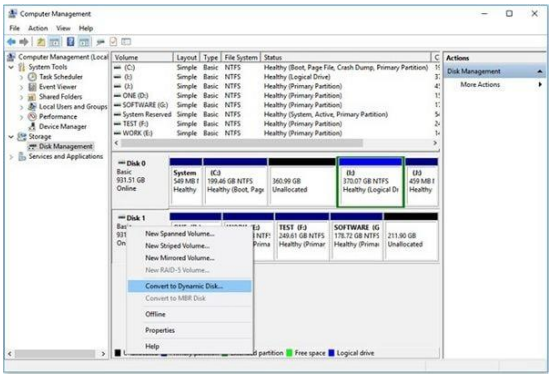

Figure 39 : Conversion en disque dynamique

Une fois le processus terminé, notre disque de base sera converti en disque dynamique. Si nous souhaitons reconvertir un disque dynamique en disque de base, cette fonction n'est pas prise en charge par la gestion des disques. Pour cela, nous aurons besoin d'un outil tiers.

6.2 Gestion des utilisateurs

our une gestion performante des utilisateurs, il est nécessaire de créer des comptes nominaux pour chaque utilisateur dans le laboratoire. L'administrateur réseau peut alors définir les jours et les horaires d'accès pour chaque utilisateur afin de préserver la puissance des ressources du serveur.

En déterminant les plages horaires pendant lesquelles les utilisateurs peuvent accéder aux ressources du serveur, l'administrateur peut réguler la charge et garantir une utilisation efficace des ressources disponibles. Cela peut contribuer à éviter les périodes de surcharge du serveur, assurant ainsi des performances optimales pour tous les utilisateurs.

En outre, la création de comptes nominaux individuels permet de mieux suivre l'utilisation des ressources par chaque utilisateur et de mettre en place des politiques de sécurité personnalisées pour protéger les données sensibles et restreindre l'accès aux informations confidentielles.

En résumé, la gestion des comptes utilisateurs et des horaires d'accès est essentielle pour optimiser l'utilisation des ressources du serveur et garantir des performances fiables et sécurisées

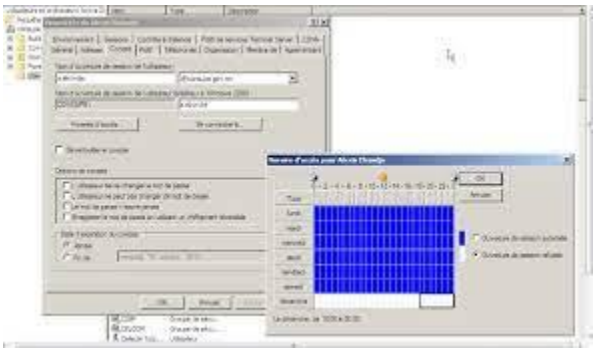

Figure 43 : parametres d’un compte utilisateur

6.3 Securité

Le protocole de bureau à distance est un excellent moyen pour les utilisateurs d’accéder et de modifier des fichiers sur des machines distantes sans avoir à être physiquement présents. Il présente cependant des failles de sécurité connues qui peuvent mettre votre entreprise en danger. Les deux principales cyberattaques qui menacent la sécurité du RDP sont les attaques par force brute et les attaques de type man-in-the-middle.

- **Attaque par force brute**

Une attaque par force brute est un type de cyberattaque qui procède par essais et erreurs pour deviner vos identifiants de connexion. Elle utilise généralement des méthodes automatisées telles que le craquage de dictionnaire, le password spraying et le credential stuffing. Les connexions RDP sont protégés par des mots de passe, mais ceux-ci ne sont pas toujours sécurisés. Les mots de passe faibles et réutilisés rendent les connexions RDP vulnérables aux attaques par force brute. Une fois qu'un cybercriminel a volé vos identifiants de connexion RDP, il peut compromettre le serveur hôte et exécuter un ransomware ou d'autres cyberattaques.

- **Attaque de type Man-in-the-middle**

Man-in-the-middle attacks – also known as on-path attacks – are a type of cyber attack in which a cybercriminal intercepts data between two devices, often a web browser and a host server. The goal of man-in-the-middle attacks is to steal, eavesdrop or modify the data for malicious purposes, such as identity theft or fraud. Since RDP connections use port 3389, cybercriminals can logically deduce that an organization is using that port and target it. Once a cybercriminal manages to hijack RDP connections flowing through port 3389, they can view the traffic and data passing through that port to compromise the host server.

6.3.1 Comment sécuriser un protocole de bureau à distance

Sécurisez les connexions au protocole de bureau à distance pour éviter que des attaques par force brute et des attaques de type man-in-the-middle ne compromettent nos connexions.

- **Limitez l'accès**

Plus le nombre d'utilisateurs auxquels nous donnons l'accès est élevé, plus le risque de violation de la sécurité est grand. Suivons le principe d'accès du moindre privilège pour réduire notre surface d'attaque et minimiser les menaces internes. Nous pourrons plus facilement contrôler l'activité de nos connexions RDP en limitant le nombre d'utilisateurs. Nous minimisons le risque de violation de la sécurité et pouvons facilement localiser les failles de sécurité en limitant le nombre d'utilisateurs qui se connectent via le RDP. Seul un nombre limité d'administrateurs devrait pouvoir modifier les paramètres de sécurité du serveur. Si nous devons permettre à quelqu'un d'accéder au RDP, donnons-lui un accès limité dans le temps.

- **Utilisez un mot de passe fort**

La faiblesse des mots de passe compromet de nombreuses connexions RDP. Les cybercriminels comptent donc sur le fait que les utilisateurs de RDP ont des mots de passe faibles qu'ils peuvent craquer. Utilisons un mot de passe fort pour protéger notre RDP contre toute violation. Un mot de passe fort comporte au moins 16 caractères et une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Un mot de passe fort exclut les mots du dictionnaire, les nombres séquentiels et les informations personnelles.

- **Activez la MFA**

L'authentification multifacteur (MFA) est une mesure de sécurité qui nécessite une forme de vérification supplémentaire pour accéder à un service ou à une application. Elle ajoute une couche de sécurité supplémentaire qui nous oblige à fournir une preuve supplémentaire de notre identité. Elle empêche les utilisateurs non autorisés d'accéder aux connexions RDP sans authentification. Même si nos identifiants de connexion RDP étaient compromis, le cybercriminel ne pourrait pas se connecter sans fournir le facteur d'authentification supplémentaire.

- **Mettez à jour vos logiciels**

Les cybercriminels recherchent constamment des failles de sécurité à exploiter, notamment en utilisant des attaques de type man-in-the-middle. Maintenons toujours nos logiciels à jour pour corriger les failles de sécurité connues et mettre à jour les fonctionnalités de sécurité qui protégeront davantage nos connexions RDP. Nous devons nous assurer que les ordinateurs client et hôte sont à jour.

- **Utilisez un serveur de passerelle de bureau à distance**

Un serveur de passerelle de bureau à distance est un service qui permet aux utilisateurs distants autorisés de se connecter à un réseau privé sur Internet. Il fournit une connexion sécurisée et chiffrée qui permet au client de se connecter au serveur hôte. Cela permet de disposer d'un point d'entrée unique et sécurisé, limité aux seuls utilisateurs autorisés.

7 Test de la solution :

7.1 Connexion en dehors de l'université

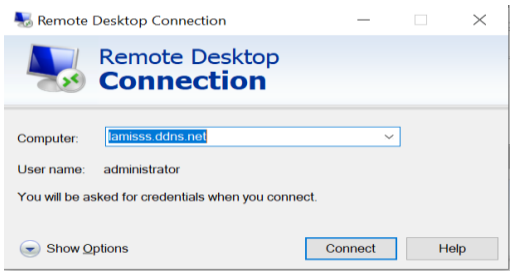

Figure 40 : Client Remote Desktop

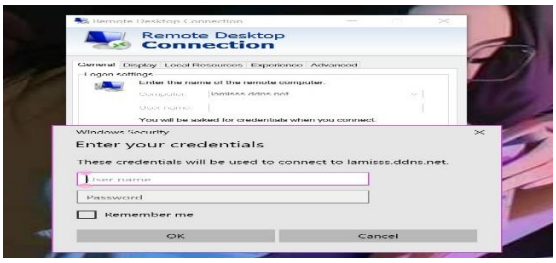

Figure 41 : Un utilisateur dans un autre LAN qui connecte le serveur

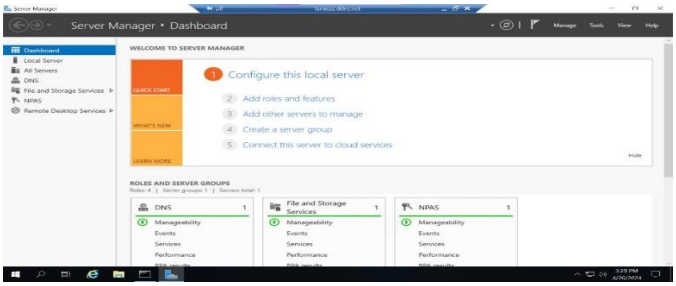

Figure 42 : Le serveur a distance

8 Conclusion

En conclusion, la mise en œuvre de Terminal Server s'est révélée être une solution performante et fiable pour la gestion et le support à distance dans notre organisation. Les résultats obtenus démontrent que Terminal Server répond efficacement aux besoins de centralisation, de sécurité et de performance.

Recruter un ingénieur de laboratoire expérimenté et compétent contribuera grandement à assurer la fiabilité, la sécurité et la performance du serveur, ce qui est essentiel pour garantir la continuité de fonctionnemnt des serveurs.

Ce projet de fin d'études a non seulement confirmé la pertinence de notre choix technologique, mais il a également fourni des bases solides pour des déploiements futurs et une gestion optimale des ressources à distance.

Conclusion Générale

En conclusion, ce projet a permis de démontrer de manière concrète et approfondie la faisabilité et l'efficacité de l'implémentation de Terminal Server pour la gestion des ressources et le support à distance dans le contexte spécifique du laboratoire de LAMIS. Les réalisations de ce projet incluent :

1. **Compréhension approfondie du partage de ressources** : Nous avons établi les bases théoriques essentielles à la compréhension des enjeux et des avantages du partage de ressources dans un environnement réseau.
2. **Analyse détaillée des besoins du laboratoire** : Une évaluation précise des besoins du laboratoire de LAMIS a été réalisée, permettant de cibler les solutions les plus adaptées.
3. **Évaluation comparative des solutions** : Nous avons analysé plusieurs solutions de gestion et de support à distance, identifiant Terminal Server comme la meilleure option en termes de performance, sécurité et coût.
4. **Mise en œuvre réussie de Terminal Server** : La mise en œuvre pratique de Terminal Server a été réalisée avec succès, incluant l'installation, la configuration et les tests de validation, démontrant ainsi sa capacité à répondre aux besoins du laboratoire.

La realisation de ce projet montrent clairement que Terminal Server est une solution viable et efficace pour améliorer la gestion des ressources et le support à distance. Une augmentation des caracteristique de serveur est souhaité surtout en terme de puisaance de calcule et puissance des GPU, on permettront de maximiser ses bénéfices pour le laboratoire de LAMIS et potentiellement pour d'autres environnements similaires.

Referance :

[1] J. F. Kurose et K. W. Ross, "Computer Networking: A Top-Down Approach," 6th ed., Pearson, 2012.

[2] Cours Master 2 professionnel informatique.

[3] https://polaridad.es/fr/Qu%E2%80%99est-ce-que-le-partage-de-ressources-en-ligne-%3F/

[4] https://tech-lib.fr/ressources-systeme/

[5] ohnson, K., & Brown, L. (2009). "Evaluating the Security of Google Desktop in Enterprise Environments."

[6] https://www.solarwinds.com/dameware/use-cases/remote-desktop-support

[7] https://dl.teamviewer.com/docs/fr/v10/TeamViewer10-Manual-Remote-Control-fr.pdf

[8] Patel, V., & Singh, R. (2015). "Analyzing the Efficiency of Resource Allocation in Multi-User Terminal Servers."

[9] Garcia, M., & Rodriguez, A. (2016). "Virtual Desktop Infrastructure for Enhanced Resource Management in Terminal Servers."

[10] Miller, R., & Davis, S. (2020). "Economic Impact of Deploying Terminal Servers for Remote Access."

[11] Miller, R., & Davis, S. (2020). "Performance Optimization of Terminal Servers Through Load Balancing."

[12] Vincent REMAZEILLES, Cisco La sécurité des réseaux,édition 2009 .

[13] M. Robert Brochu, Francis Beaudoin, Jean Laterrière,Politique de sécurité de

l’information, édition 2003.