DEDICACE

À ma chère maman, pour ton amour infini et tes silencieux sacrifices qui ont rendu ce travail possible.

REMERCIEMENTS

Nous tenons à exprimer notre profonde gratitude à Madame **KOUMBA**, Directrice Générale de l'Institut Facultaire d'Informatique et de Management (IFIM), ainsi qu'à l'ensemble du corps enseignant et aux membres de l'administration, pour leur encadrement, leur disponibilité et leur soutien tout au long de notre formation. Nos remerciements vont également à Monsieur **TATY**, notre encadreur pédagogique, pour son suivi attentif, ses conseils avisés et son accompagnement constant durant ce stage.

Nous adressons ensuite nos vifs remerciements à Monsieur **Freddy HANOU**, Directeur Général de **YOD Ingénierie**, pour la confiance qu'il nous a témoignée en nous accueillant au sein de son entreprise et en nous confiant des missions enrichissantes qui ont largement contribué à notre apprentissage professionnel. Nous remercions également l'ensemble de l'équipe du service d'ingénierie et de programmation pour leur disponibilité et leur collaboration.

Enfin, nous exprimons toute notre reconnaissance à notre famille, et tout particulièrement à notre mère, Madame **OBOUMEYEM OBAME Tatiana**, pour son soutien financier constant, ses encouragements et sa patience, qui ont été essentiels à la réalisation de ce travail.

SIGLES ET ABRÉVIATIONS

RDP : Remote Desktop Protocol

VPN : Virtual Private Network

ZTNA : Zero Trust Network Access

MFA : Multi-Factor Authentication

SaaS : Software as a Service

PaaS : Platform as a Service

IaaS : Infrastructure as a Service

GPO : Group Policy Object

AD : Active Directory

LDAP : Lightweight Directory Access Protocol

PRTG : PRTG Network Monitor

OU : Organizational Unit

CPU : Central Processing Unit

RAM : Random Access Memory

Apache : Apache HTTP Server

MariaDB : Maria DataBase

PHP : Hypertext Preprocessor

OwnCloud : OwnCloud

Ubuntu : Ubuntu Linux

Windows Server 2019 : Microsoft Windows Server 2012

LEXIQUE

Active Directory (AD) : Système de gestion centralisée des utilisateurs, des ordinateurs et des ressources dans un réseau Windows. Il permet de gérer les comptes utilisateurs, les permissions et les politiques de sécurité.

Apache : Serveur web open-source utilisé pour héberger des applications web, comme l'interface d'OwnCloud dans ce projet.

Cloud computing : Technologie permettant de stocker, gérer et traiter des données sur des serveurs GPO (Group Policy Object) : Objet de stratégie de groupe dans Windows Server, utilisé pour configurer et appliquer des politiques de sécurité et des restrictions aux utilisateurs et aux ordinateurs.

IaaS (Infrastructure as a Service) : Modèle de cloud computing où une infrastructure informatique (serveurs, stockage, réseaux) est fournie à la demande via Internet.

Infrastructure centralisée : Architecture informatique où les ressources (postes de travail, serveurs, données) sont gérées depuis un point central, facilitant l'administration, la sécurité et la maintenance.

LDAP (Lightweight Directory Access Protocol) : Protocole utilisé pour interroger et gérer des annuaires, ici pour connecter OwnCloud à Active Directory afin de synchroniser les comptes utilisateurs.

MariaDB : Système de gestion de base de données open-source, utilisé comme alternative à MySQL pour stocker les données d'OwnCloud (comptes, partages, historiques).

MFA (Multi-Factor Authentication) : Méthode de sécurité nécessitant plusieurs formes d'authentification (mot de passe, code, biométrie) pour accéder à un système.

NETCORE : Logiciel développé par YOD Ingénierie pour la gestion centralisée du personnel des entreprises du groupe NEDCO**.**

VPN (Virtual Private Network) : Réseau privé virtuel qui crée une connexion sécurisée et chiffrée entre des appareils distants et un réseau interne.

WireGuard : Protocole VPN moderne, utilisé par Tailscale, connu pour sa simplicité, sa rapidité et son chiffrement robuste.

AVANT-PROPOS

L'Institut Facultaire d'Informatique et de Management (IFIM) est un établissement d'enseignement supérieur gabonais fondé le **28 octobre 2018** par Monsieur **Élie NTOUMBA TCHYMANGA**. Spécialisé dans les domaines de l'informatique, du management et des nouvelles technologies, l'IFIM a pour mission de former des professionnels dotés d'une **triple compétence** : informatique, management et entrepreneuriat.

Sous la direction de **MADAME KOUMBA**, Directrice Générale, l'IFIM mise sur une pédagogie innovante et professionnalisante. Ses cursus, axés sur les réalités du marché gabonais et international, proposent des licences en développement web, génie logiciel, électronique, télécommunications, réseaux, finance, logistique, ressources humaines et économie.

L'institut articule ses formations autour d'un équilibre entre théorie et pratique, afin de doter les étudiants des compétences techniques, analytiques et humaines indispensables dans les entreprises modernes. Chaque apprenant est ainsi préparé à concevoir, piloter et mettre en œuvre des solutions informatiques et managériales concrètes, tout en développant un **esprit entrepreneurial**.

L'IFIM valorise aussi des qualités telles que la **maîtrise des architectures informatiques**, la **psychologie des affaires**, les **aptitudes relationnelles**, et la **compréhension des enjeux économiques et sociaux**. Cette approche vise à former des jeunes Gabonais talentueux, motivés et prêts à s'engager activement dans le développement de leur pays.

En s'adaptant continuellement aux mutations du monde professionnel, l'IFIM s'impose aujourd'hui comme un **acteur incontournable** de la formation supérieure au Gabon, contribuant activement à l'émergence d'une génération compétente, innovante et entreprenante.

SOMMAIRE

Chapitre 4 : Déploiement de la solution choisie

Section 1 : Mise en œuvre de l'infrastructure

1.1.1. Présentation de l'architecture cible, Étapes techniques du déploiement

1.2.2. Installation et configuration des serveurs, Configuration du service RDP

1.2.3. Mise en place du VPN pour sécuriser les connexions distantes, Intégration du cloud

1.2.4. Supervision de l'infrastructure avec PRTG Network Monitor, Sécurité du système

Section 2 : Résultats et bilan

2.1.1. Tests, validation

2.2.2. Observations post-déploiement

2.3.3. Limites rencontrées

2.4.4. Suggestions d'amélioration

Conclusion générale

Bibliographie

Annexes

INTRODUCTION GENERAL

Dans l'ère numérique actuelle où la productivité et la sécurité des données sont des enjeux majeurs, de nombreuses entreprises font face à des défis importants dans la gestion de leur parc informatique. Lors de mon stage, j'ai constaté que l'absence de système centralisé entraînait des problèmes récurrents : performances médiocres des postes de travail, désorganisation des fichiers, et vulnérabilités en matière de sécurité. Ces dysfonctionnements, directement liés à une gestion décentralisée et anarchique des ressources informatiques, impactaient significativement l'efficacité opérationnelle et la qualité du travail des collaborateurs.

Face à ces constats, une question fondamentale s'impose : Comment la mise en place d'un système de gestion centralisé peut-elle optimiser les postes de travail en résolvant les problèmes de performance, d'organisation et de sécurité identifiés ? Cette problématique découle directement des observations terrain qui ont révélé trois lacunes majeures : la gestion disparate des ressources par les utilisateurs, l'absence de standardisation dans l'organisation des fichiers, et les risques accrus pour la sécurité des données. Le projet vise ainsi à démontrer qu'une solution centralisée peut apporter des réponses concrètes à ces défis.

Notre réflexion s'articulera autour de deux axes principaux. Dans un premier temps, nous procéderons à un diagnostic approfondi des dysfonctionnements du système actuel et analyserons leurs impacts sur les opérations quotidiennes. Cette analyse nous permettra de justifier techniquement et économiquement le choix d'une solution centralisée. Dans un second temps, nous présenterons la solution concrètement mise en œuvre, en détaillant son architecture, son déploiement et les résultats obtenus en termes d'amélioration des performances, de rationalisation de l'organisation des données et de renforcement de la sécurité. Cette démarche démontrera comment la centralisation peut transformer la gestion des postes de travail en un véritable levier de performance pour l'entreprise.

PREMIÈRE PARTIE : PRÉSENTATION DU CADRE GÉNÉRAL DU STAGE

Cette partie introduit l'historique, la mission et l'organisation de **YOD Ingénierie**, l'entreprise qui m'a accueilli pour mon stage. Elle offre un aperçu du contexte d'évolution de la structure, de son rôle au sein du groupe **NEDCO**, et des services proposés aux filiales et clients externes, tout en présentant ses missions principales et quelques solutions développées.

Chapitre I : Historique, mission et organisation

Ce chapitre présente **YOD Ingénierie**, l'entreprise où j'ai réalisé mon stage, en mettant en lumière son historique, son appartenance au groupe **NEDCO** et les motifs de sa création. Il détaille ses missions principales et secondaires, ainsi que quelques outils et solutions développés, offrant une compréhension de son rôle clé dans la gestion informatique des entreprises du groupe, tout en soulignant ses services pour des clients externes.

Section 1 : Historique et missions de l'entreprise

Cette section retrace l'historique de **YOD Ingénierie** et expose ses missions principales. Elle décrit son évolution en tant que pôle technologique du groupe **NEDCO**, ainsi que les divers services qu'elle propose, tant aux filiales internes qu'aux clients extérieurs.

1.1. Historique de **YOD Ingénierie**

YOD Ingénierie est une société d'ingénierie informatique innovante et dynamique, intégrée au groupe **NEDCO,** un ensemble de sept entreprises complémentaires créé par **M. NGEUL** en 2018. Fondée initialement à Cotonou (Bénin), elle a été établie pour centraliser et fournir des services informatiques aux sociétés du groupe, jouant un rôle stratégique de pôle technologique. Depuis 2019, elle est dirigée par **M. Freddy,** renforçant son développement. Son siège social a ensuite été transféré à Libreville (Gabon), où se trouve son principal centre technique, comprenant :

- Une équipe de plus de quinze ingénieurs spécialisés,
- Un laboratoire de développement et de tests,
- Un centre de formation agréé dédié à l'amélioration des compétences numériques des collaborateurs.

Dans une démarche d'expansion régionale, **YOD Ingénierie** dispose d'un bureau à Cotonou (Bénin), servant de hub de déploiement pour l'Afrique de l'Ouest et de centre de support technique régional. Bien que sa mission première soit axée sur les besoins internes du groupe **NEDCO**, elle s'est imposée comme un acteur reconnu dans les services informatiques, s'adressant à des entreprises externes et à des particuliers. Aujourd'hui, elle accompagne des partenaires tels qu'Ogar Assurance, en concevant et déployant des solutions numériques adaptées aux réalités locales, tout en respectant les normes internationales.

1.2. Missions de **YOD Ingénierie**

La mission principale de **YOD Ingénierie** est de fournir l'ensemble des services informatiques aux sept entreprises du groupe **NEDCO**, en tant que bras technologique centralisé.

Ses principales responsabilités internes incluent :

- La conception, le développement et la maintenance des infrastructures numériques et des solutions logicielles pour toutes les filiales du groupe.
- La gestion de la sécurité informatique, des réseaux et des serveurs, y compris la configuration et le dépannage réseau pour les entreprises comme Ingenium ou Bifev.
- La mutualisation des ressources technologiques afin d'optimiser les coûts et d'améliorer la performance globale des sociétés du groupe.
- La formation et l'accompagnement des collaborateurs des différentes entreprises du groupe pour renforcer leurs compétences numériques.

Dans ce cadre, **YOD Ingénierie** a conçu et déployé plusieurs outils clés, notamment :

- **NETCORE**, un logiciel destiné à la gestion centralisée du personnel et des employés de toutes les entreprises du groupe **NEDCO**.
- **LEVILAGE**, un logiciel de réservation de salles de fêtes et de cérémonies, développé pour répondre aux besoins spécifiques de clients externes.

Au-delà de cette mission interne, **YOD Ingénierie** intervient également pour des clients externes en leur proposant :

- La création de logiciels et d'applications sur mesure, comme **LE VILAGE**.

- La conception de sites web modernes et performants, parmi lesquels le site web de **Ogar Assurance.**
- La configuration, l'hébergement et la gestion de serveurs pour des entreprises et des particuliers.
- Le développement de solutions cloud et de cybersécurité, incluant la migration, la virtualisation et la sécurisation des données.
- La maintenance informatique et le support technique pour des clients externes tels que **Ogar Assurance** et d'autres organisations.

Section 2 : Présentation et mission du service d'accueil – Déroulement du stage

Cette section décrit le service auquel j'ai été affecté durant mon stage, sa composition, son organisation et ses missions principales. Elle détaille également les tâches qui m'ont été confiées, les activités que j'ai réalisées et les compétences que j'ai pu développer tout au long de cette expérience.

2.1. Composition et organisation du service

Pendant mon stage à **YOD Ingénierie**, j'ai été affecté au service programmation. C'est dans ce service que sont réalisés à la fois le développement de logiciels et de sites web, mais aussi la gestion et la maintenance des systèmes et réseaux de l'entreprise.

Le service comptait sept membres, moi y compris. Il y avait quatre développeurs qui travaillaient sur la conception des logiciels et des sites web, deux personnes chargées de la communication et du marketing, et moi qui m'occupais principalement de l'administration système. Mon travail consistait à configurer et gérer les serveurs, assurer la maintenance réseau et superviser les différents équipements informatiques de la structure. Chacun avait son domaine précis, mais nous travaillions ensemble sur certains projets, ce qui permettait d'avancer plus rapidement et de partager les compétences.

2.2. Mission du service d'accueil

Le service où j'étais affecté s'occupait surtout de développer des solutions informatiques et d'administrer les systèmes et réseaux. Il créait des logiciels, des applications et des sites web pour les besoins internes du groupe **NEDCO**, mais aussi pour des clients externes. Il gérait également tout ce qui concernait la configuration des serveurs, la supervision et le dépannage des réseaux.

C'est dans ce service que sont développés des outils importants comme **NETCORE**, qui permet de gérer le personnel de toutes les entreprises du groupe **NEDCO**, ou encore **LEVILAGE**, un logiciel de réservation de salles de fêtes et de cérémonies. L'équipe s'occupe aussi de la configuration et de la maintenance réseau pour des entreprises comme Ingenium et Bifev.

2.3. Déroulement du stage

Mon stage s'est déroulé étape par étape. Dès mon arrivée, j'ai été bien accueilli par les membres de l'équipe et on m'a présenté les différentes activités du service. Ma première mission a été de mettre en place un serveur Linux accessible uniquement via un VPN pour sécuriser les accès.

Ensuite, j'ai commencé à superviser tout le parc informatique de l'entreprise. Je me suis occupé de la configuration des serveurs et de certains services comme Apache, mais aussi de la mise en place de solutions cloud pour faciliter le stockage et l'accès aux données.

Par la suite, on m'a confié la mise en place de certaines politiques de sécurité. J'ai notamment déployé un système qui permettait aux administrateurs de voir en temps réel ce qu'un employé fait sur son ordinateur et de pouvoir prendre la main à distance en cas de problème. Pour cela, j'ai utilisé l'outil LiteManager qui s'est avéré très pratique pour l'assistance et la gestion à distance.

Au fil du stage, j'ai acquis de l'expérience dans l'administration Linux, la gestion de réseaux et la sécurité informatique. J'ai travaillé sur des projets concrets et appris à configurer, superviser et sécuriser des systèmes tout en apportant mon aide à l'équipe. Ce stage m'a permis de mettre en pratique mes connaissances et d'élargir mes compétences techniques grâce aux différentes missions qui m'ont été confiées.

CHAPITRES II : élaboration de la problématique et définition des objectifs visés

Le deuxième chapitre est consacré à l'élaboration de la problématique et à la définition des objectifs visés. Il part de l'analyse de l'existant pour mettre en évidence les difficultés rencontrées dans la gestion du parc informatique et de l'organisation des services numériques. Ce chapitre montre comment ces constats ont conduit à la réflexion autour d'une solution adaptée : le déploiement d'une infrastructure centralisée de postes de travail, avec accès distant sécurisé et services cloud intégrés.

Section 1 : Étude des concepts et problématique

Cette section présente d'abord les concepts clés liés au projet, comme l'infrastructure centralisée, l'accès distant sécurisé et les services cloud intégrés, en s'appuyant sur des définitions issues de sources fiables. Elle expose ensuite les problèmes rencontrés dans l'entreprise et explique de quelle manière la solution proposée peut y répondre, ce qui conduit à la formulation de la problématique du stage.

2.1.1. Définitions des concepts clés

Infrastructure centralisée de postes de travail : La gestion centralisée des postes de travail englobe l'ensemble des technologies et processus permettant de centraliser le monitoring, la maintenance et l'administration des équipements informatiques d'une organisation à partir d'un serveur unique. Elle vise à optimiser la sécurité, la conformité et les performances, tout en réduisant les coûts de gestion.

Accès distant sécurisé : L'accès distant sécurisé désigne l'ensemble des mesures (VPN, ZTNA, MFA, chiffrement, authentification unique, etc.) mises en œuvre pour permettre aux utilisateurs externes d'accéder aux ressources informatiques d'une entreprise en toute sécurité, en minimisant les risques de cyberattaques, tout en assurant la confidentialité et l'intégrité des données.

Services cloud intégrés : Le cloud computing correspond à l'utilisation de serveurs distants hébergés dans des centres de données pour stocker, gérer et traiter des données via Internet

(SaaS, PaaS, IaaS…). Les services cloud intégrés impliquent la mise en place d'une infrastructure permettant à la fois l'hébergement sécurisé des données, la mutualisation des ressources, l'accessibilité depuis différents terminaux et la sauvegarde centralisée

2.1.2. Construction de la problématique

Lorsque j'ai été chargé de superviser le parc informatique, j'ai observé plusieurs difficultés majeures. L'architecture réseau était rudimentaire : un routeur central connecter à switch et un point d'accès unique auquel tous les postes étaient connectés, sans segmentation ni contrôle. Cette situation rendait le réseau vulnérable et peu performant.

Du côté des postes de travail, plusieurs problèmes se posaient :

- Les documents étaient mal organisés, souvent stockés uniquement sur les bureaux, et pouvaient disparaître à la synchronisation du cloud mal configuré.
- La lenteur des ordinateurs provenait en partie de la **RAM insuffisante** et de l'usage de modèles tout-en-un peu adaptés aux exigences actuelles.
- Les mises à jour système étaient trop irrégulières, exposant l'environnement à des failles de sécurité.
- La présence de **plusieurs antivirus simultanés** sur certains postes générait des conflits et des alertes systèmes fréquentes, réduisant la stabilité.

Pour résoudre ces problèmes nous avons proposé la mise en place d'une infrastructure centralisée de postes de travail, associée à un accès distant sécurisé et à des services cloud intégrés. Contrairement à la première idée d'investir dans plusieurs ordinateurs performants, cette solution repose sur l'acquisition de deux serveurs distincts.

Le premier serveur, fonctionnant sous Windows Server 2019, est dédié à la connexion des utilisateurs. C'est sur ce serveur que sont créés les comptes, installés les logiciels et effectuées les mises à jour. Toute l'administration des postes de travail y est centralisée, ce qui permet aux utilisateurs d'accéder à leur environnement de travail sans avoir à gérer eux-mêmes les installations ou les configurations.

Le second serveur, généralement configuré sous Linux, est réservé à l'hébergement des services critiques, notamment le cloud privé destiné au stockage, au partage et à la sauvegarde sécurisée

des fichiers. Cette séparation permet de garantir de meilleures performances, d'assurer une sécurité accrue et de réduire les risques en cas de panne d'un des serveurs.

Grâce à cette organisation, l'administrateur garde un contrôle complet : il gère les droits d'accès, définit les services disponibles pour chaque utilisateur et peut bloquer certaines actions ou sites web si nécessaire. Les utilisateurs, eux, bénéficient d'un environnement stable et performant, avec des données mieux organisées et protégées.

C'est ainsi que je me suis posé la question : Dans quelle mesure le Déploiement d'une infrastructure centralisée de postes de travail avec accès distant sécurisé et services cloud intégrés peut-elle résoudre les problèmes d'organisation, de performance et de sécurité des postes de travail ?

Section 2 : Les objectifs du projet

Cette section présente les objectifs fixés pour le projet ainsi que les différentes parties prenantes impliquées dans sa réalisation. Elle précise les résultats attendus et le rôle de chaque acteur dans la mise en œuvre de l'infrastructure centralisée avec accès distant et services cloud intégrés.

2.2.1. Définition des objectifs

L'objectif du projet est de mettre en place une infrastructure centralisée de postes de travail afin que la gestion complète du système soit assurée uniquement par les administrateurs. Avec cette solution, les employés n'ont plus à se soucier de l'installation des logiciels, des mises à jour ou de l'organisation des documents ; toutes ces tâches sont effectuées par l'équipe technique.

Ce fonctionnement permet également de renforcer la sécurité : les administrateurs ont un contrôle total sur les accès, les applications autorisées et les droits des utilisateurs. Ils peuvent créer et gérer les comptes, déterminer les services disponibles et superviser en temps réel les activités sur les postes.

Ainsi, le projet poursuit trois grands objectifs :

- Centraliser et simplifier la gestion informatique.

- Libérer les utilisateurs de toutes les tâches techniques.
- Assurer la sécurité et la fiabilité des données de l'entreprise.
- Renforcer la sécurité grâce à la gestion des droits, aux mises à jour centralisées et à la supervision des activités.
- Réduire les coûts matériels en évitant l'achat de plusieurs ordinateurs performants pour chaque utilisateur.

2.2.2. Les parties prenantes

Bien que nous ayons eu l'opportunité de concevoir et de mener à bien ce projet de manière autonome, plusieurs personnes ont joué un rôle essentiel dans son bon déroulement, contribuant à sa réussite à travers leurs expertises et leur soutien. Permettez-moi de souligner les différentes contributions qui ont permis de transformer cette initiative en une solution fonctionnelle et efficace.

Tout d'abord, nous avons assumé la responsabilité complète de la conception et du développement de l'infrastructure. Cette tâche a impliqué une planification rigoureuse, incluant la définition des besoins techniques, la sélection des outils et des logiciels appropriés, ainsi que la mise en œuvre pratique. Nous avo personnellement supervisé l'installation des serveurs, effectué la configuration détaillée des systèmes (Windows Server 2019 et Linux), et conduit une série de tests approfondis pour garantir la stabilité et la performance de l'ensemble. Cette phase solitaire a requis une gestion minutieuse des ressources et une résolution proactive des défis techniques rencontrés tout au long du processus.

Cependant, je ne saurais minimiser l'apport précieux de l'équipe technique basée au Bénin. Cette équipe a apporté une contribution significative en participant activement aux phases de test de la solution déployée. Après chaque étape de mise en production, ces collaborateurs ont procédé à des vérifications rigoureuses, évaluant la fiabilité du système dans des conditions réelles d'utilisation. Leurs retours détaillés ont permis d'identifier des ajustements nécessaires, d'améliorer la robustesse de l'infrastructure et de s'assurer que la solution répondait aux attentes des utilisateurs finaux, tant au niveau des performances que de la sécurité. Leur expertise locale et leur engagement ont été des atouts majeurs pour garantir une implémentation réussie sur le terrain.

Par ailleurs, mon encadreur de stage professionnel a été un pilier incontournable tout au long de cette aventure. Sa présence attentive et ses conseils avisés m'ont accompagné à chaque étape clé du projet. Il effectuait des suivis réguliers, prenant le temps d'examiner l'avancement de mon travail, de discuter des choix techniques opérés et de m'orienter lorsque des décisions complexes se présentaient. Il a validé les étapes critiques, telles que la configuration initiale des serveurs, la mise en place du cloud privé et les tests finaux, apportant une validation professionnelle qui a renforcé la crédibilité de l'infrastructure développée. Son expérience et son regard extérieur ont été déterminants pour maintenir le cap et assurer que le projet respectait les standards attendus.

Ainsi, bien que la réalisation technique et la conception originelle de l'infrastructure aient été entièrement de mon fait, la qualité et l'efficacité de la solution finale doivent beaucoup au soutien collectif. L'équipe technique du Bénin, par ses tests et ses validations sur le terrain, et mon encadreur de stage, par son accompagnement stratégique, ont formé un réseau de collaboration qui a permis de surmonter les obstacles et d'atteindre les objectifs fixés. Cette synergie a non seulement garanti la fiabilité de l'infrastructure centralisée avec accès distant et services cloud, mais a aussi renforcé mon apprentissage et ma confiance en tant que futur professionnel dans ce domaine.

L'élaboration du projet s'est déroulée sur une période d'un mois, suivie d'une semaine dédiée aux tests finaux et à la validation. Chaque semaine correspondait à une étape bien définie : le choix et l'installation des systèmes, la configuration des serveurs et du cloud, la création des utilisateurs et la mise en place des politiques de sécurité. La dernière semaine a permis de réaliser une série de tests approfondis afin de s'assurer de la stabilité, de la sécurité et de la performance de l'infrastructure avant sa mise en production.

Ce découpage hebdomadaire a permis de suivre une méthode de travail claire et progressive, en validant chaque étape avant de passer à la suivante. Les tests intermédiaires ont été essentiels pour identifier rapidement les erreurs de configuration et y apporter des corrections immédiates. Grâce à cette organisation, le déploiement final s'est déroulé sans difficulté majeure. Cette approche a également permis de documenter chaque étape, facilitant la maintenance et l'évolutivité future de l'infrastructure.

Semaine	Activités réalisées
Semaine 1	Choix des solutions (Windows Server 2019 et Linux Ubuntu). Installation des systèmes sur les serveurs et configuration des VPN pour les accès distants.
Semaine 2	Choix de la solution cloud. Mise en place et configuration du serveur cloud. Interconnexion des deux serveurs et premier test de communication.
Semaine 3	Création et gestion des utilisateurs via Active Directory. Mise en place des stratégies de groupe (GPO). Deuxième test pour vérifier les accès et permissions.
Semaine 4	Déploiement du cloud pour les utilisateurs finaux. Configuration des politiques de sécurité et analyse des limites de l'infrastructure. Dernier test et validation finale.
Semaine 5	Semaine supplémentaire consacrée à des tests complets pour s'assurer de la stabilité, de la sécurité et de la performance de l'infrastructure.

La première partie de ce rapport a introduit le contexte de mon stage au sein de YOD Ingénierie, filiale du groupe NEDCO, spécialisée dans la gestion des services informatiques. Elle a retracé l'historique de l'entreprise, ses missions et des solutions phares comme NETCORE et LEVILAGE, illustrant son expertise. Le service programmation et administration système, où j'ai été intégré, a été décrit, mettant en lumière son organisation et les activités réalisées, qui m'ont permis de comprendre les défis techniques et organisationnels. Les limites de l'infrastructure actuelle, telles que la lenteur des postes, la désorganisation des documents, l'absence de centralisation et les failles de sécurité, ont conduit à envisager une solution moderne : une infrastructure centralisée avec accès distant sécurisé et services cloud. Cette conclusion ouvre la voie à la deuxième partie, qui détaillera l'analyse de la problématique, les objectifs et la mise en œuvre technique de la solution proposée.

DEUXIÈME PARTIE : ÉTUDE ET MISE EN ŒUVRE DU PROJET

Cette deuxième partie du rapport est consacrée à l'étude détaillée du projet et à sa mise en œuvre technique. Elle commence par une analyse des problèmes identifiés sur le terrain, puis présente la solution retenue ainsi que les étapes de sa réalisation. Cette partie permet de comprendre les choix techniques effectués, leur justification et leur application concrète dans le cadre du stage.

Chapitre III : Analyse du problème et choix de solution

Le chapitre 3 revient sur l'idée générale du projet, en s'appuyant sur les constats faits lors de la supervision du parc informatique. Il présente les limites de l'infrastructure existante et montre comment l'étude du terrain a permis de confirmer la pertinence d'une solution basée sur une infrastructure centralisée, avec accès distant sécurisé et cloud intégré.

Section 1 : Rappel de l'idée et étude sur le terrain

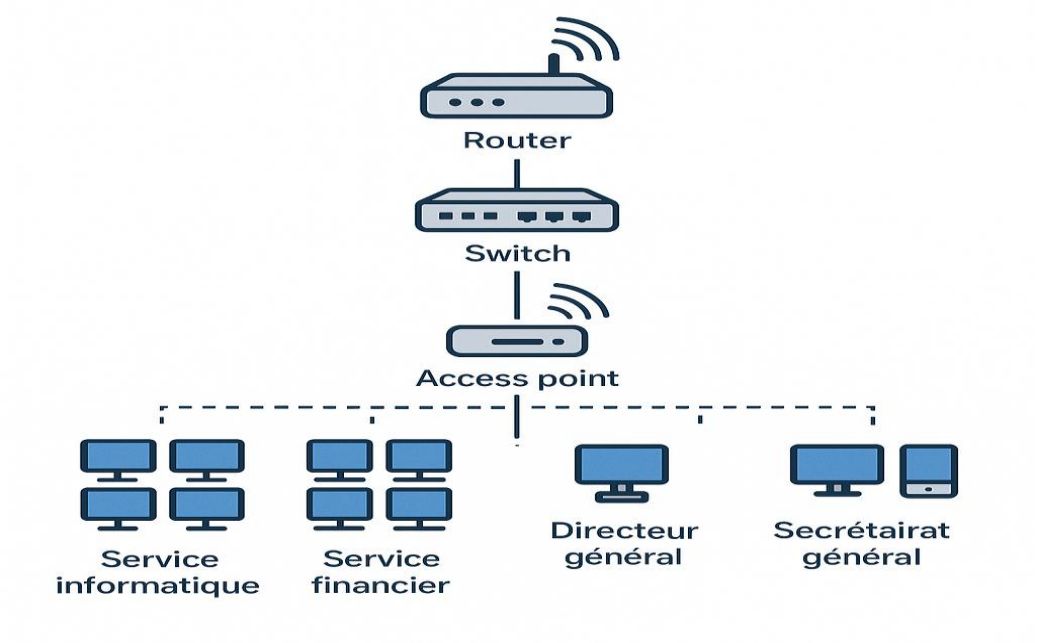
Cette section rappelle brièvement le principe de la solution envisagée, puis présente les observations faites sur le terrain. Elle met en lumière les difficultés rencontrées dans l'ancienne organisation : réseau, sécurité, performance, qui ont justifié la mise en œuvre du projet.

1.1. État de l'infrastructure existante

Lorsque j'ai commencé mon stage à YOD Ingénierie, l'infrastructure informatique en place présentait une organisation très basique. Le réseau reposait sur un seul routeur central relié à un switch et à un point d'accès Wi-Fi unique, utilisé par l'ensemble des employés pour se connecter. Cette architecture était non segmentée, ce qui signifiait que tous les postes de travail se retrouvaient sur un même plan réseau, sans politique d'isolation, de filtrage ni de priorisation du trafic.

Les postes de travail étaient majoritairement des ordinateurs tout-en-un, peu puissants, avec une mémoire vive (RAM) très limitée et des performances insuffisantes pour les tâches professionnelles courantes. De plus, il n'existait aucune gestion centralisée des utilisateurs ou des équipements. Chaque utilisateur gérait son poste indépendamment, installait ses logiciels à sa manière, et aucune politique de sécurité ni de supervision n'était réellement appliquée.

Enfin, le système de stockage de fichiers reposait sur un cloud mal configuré, utilisé de manière non sécurisée, sans réelle politique de sauvegarde ou de contrôle des accès. Il n'y avait pas non plus de système de mise à jour global.



1.2. Observations techniques relevées pendant le stage

Au fil des semaines de supervision du parc informatique, plusieurs dysfonctionnements techniques majeurs ont été relevés. Tout d'abord, il a été constaté que la plupart des ordinateurs souffraient de lenteurs importantes. Le démarrage de certains postes pouvait prendre plus de cinq minutes. Cette situation était due principalement à une RAM insuffisante et à des composants matériels inadaptés aux besoins réels des utilisateurs.

Ensuite, la gestion des documents était totalement désorganisée. Les fichiers étaient souvent enregistrés directement sur le bureau, sans structure de dossiers claire. De plus, la synchronisation avec le cloud entraînait parfois des suppressions involontaires des fichiers à la fois sur le poste et dans le cloud, faute de paramétrage correct.

La sécurité était également un point critique. Aucun système de mise à jour automatique n'était en place, ce qui exposait les postes à de potentielles failles. Certains ordinateurs avaient même

plusieurs antivirus installés simultanément, ce qui causait des conflits logiciels et une baisse de performance générale.

Enfin, l'absence totale de gestion centralisée (type Active Directory) compliquait le suivi, l'administration et la supervision. Chaque poste fonctionnait en autonomie, sans aucun contrôle global des droits d'accès, des logiciels installés ni de la configuration réseau.

Section 2 : Recherche et justification d'une solution introduit

Cette section présente les différentes solutions envisagées pour répondre aux problèmes identifiés dans l'infrastructure existante. Elle expose les raisons techniques et stratégiques qui ont conduit au choix de la solution finale, à savoir la mise en place d'une infrastructure centralisée de postes de travail, intégrant un accès distant sécurisé et des services cloud. Cette approche a été retenue comme étant la plus adaptée au contexte de l'entreprise, tant en termes de performance que de sécurité et de coûts.

2.1. Proposition des options possibles

Face aux problèmes identifiés sur le terrain : lenteur des postes, désorganisation des fichiers, absence de sécurité et de gestion centralisée, plusieurs solutions ont été envisagées.

La première option consistait à remplacer progressivement les postes de travail par du matériel plus performant. Cette solution aurait permis d'améliorer la vitesse d'exécution et la stabilité des machines, en optant pour des ordinateurs plus puissants avec davantage de RAM, un meilleur processeur et un système plus fluide. Mais, cette option représentait un investissement financier très élevé, sachant qu'un seul poste coûte entre 200 000 et 250 000 FCFA. En tenant compte du nombre d'employés dans les différents services, le coût total se chiffrerait en millions de francs CFA. De plus, cette solution ne répondait qu'au problème de performance matérielle, sans résoudre les autres difficultés liées à l'organisation, à la sécurité ou à la gestion des utilisateurs.

La deuxième option envisagée était de mettre en place une infrastructure centralisée, avec un serveur principal pour la gestion des utilisateurs et un autre pour les services critiques comme le cloud. Cette approche permettrait de centraliser la gestion de tous les postes, de sécuriser les données, de structurer l'accès aux ressources, et d'assurer une supervision efficace. Elle offrait également l'avantage d'être évolutive, c'est-à-dire facilement adaptable à l'ajout d'utilisateurs ou de services futurs. En plus, son coût global était nettement inférieur à celui d'un remplacement matériel massif.

2.2. Choix de la solution retenue et motivations techniques

Après évaluation des options, la solution retenue a été celle de l'infrastructure centralisée, car elle offrait une réponse globale à tous les problèmes rencontrés : performance, sécurité, organisation, accès distant, et réduction des coûts.

Cette solution s'appuie sur deux serveurs distincts :

- Un serveur Windows Server 2019, destiné à l'administration du réseau, la création des comptes utilisateurs, l'application des politiques de sécurité (GPO), la gestion des sessions distantes via RDP, et le contrôle total des activités.
- Un serveur Linux (Ubuntu), dédié à l'hébergement du cloud privé **owncloud**, à la sauvegarde des fichiers, à leur partage sécurisé, et à la synchronisation des documents sans risque de perte.

Cette architecture présente plusieurs avantages techniques :

- Une gestion centralisée qui permet aux administrateurs de tout contrôler : installations, mises à jour, accès utilisateurs, restrictions, supervision.
- Une réduction des coûts : plus besoin d’équiper chaque employé avec un ordinateur puissant, un poste basique suffit pour se connecter au serveur central.
- Une sécurité accrue grâce à un accès par VPN, permettant à l'équipe de Yod Ingénierie, basée au Bénin, de s'y connecter.
- Une meilleure organisation des fichiers grâce au cloud centralisé, évitant les pertes ou les doublons.
- Une solution évolutive, qui peut facilement s’adapter à la croissance de l’entreprise ou à l’ajout de nouveaux services.

Chapitre IV : Déploiement de la solution choisie

Ce chapitre est consacré au déploiement pratique de la solution retenue. Il décrit les différentes étapes techniques mises en œuvre pour installer, configurer et sécuriser l'infrastructure centralisée. L'objectif est de montrer comment la solution a été réalisée, depuis la préparation des serveurs jusqu'à la mise à disposition des services pour les utilisateurs.

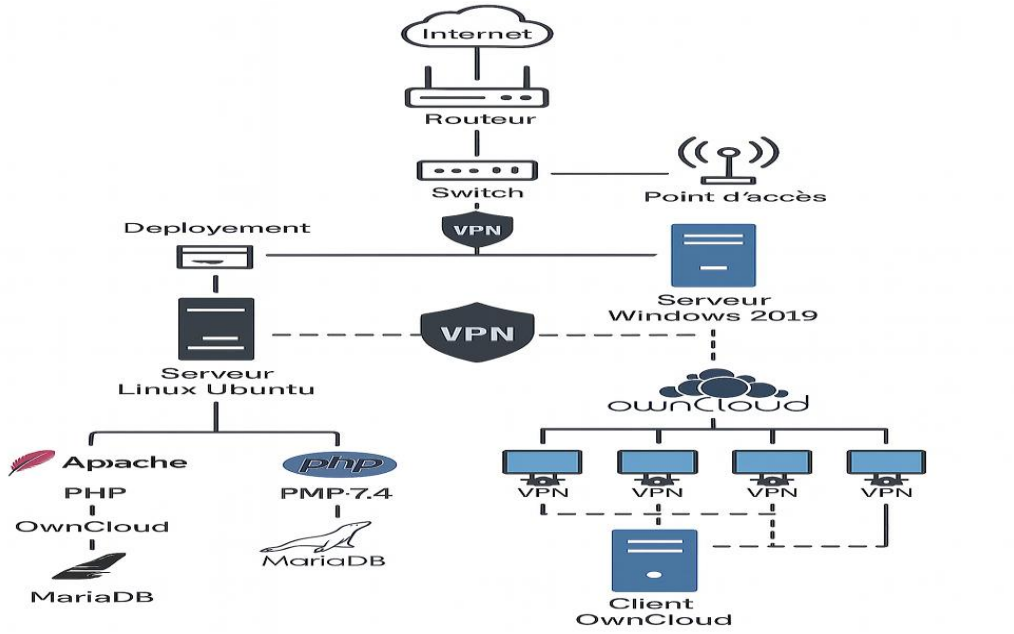
Section 1 : Mise en œuvre de l'infrastructure

Cette section présente la mise en œuvre concrète de l'infrastructure, notamment l'installation des systèmes d'exploitation sur les serveurs, la configuration des accès distants via VPN, ainsi que l'interconnexion des services. Elle détaille les outils utilisés, les choix techniques faits, et les premières vérifications permettant de valider le bon fonctionnement de l'environnement déployé.

1.1.1. Présentation de l'architecture cible, Étapes techniques du déploiement

L'architecture cible mise en place repose sur un modèle centralisé et sécurisé, basé sur deux serveurs distincts qui communiquent entre eux au sein du même réseau. Le premier serveur, sous Windows Server 2019, est chargé de la gestion des utilisateurs, de l'administration des sessions via RDP, de la définition des stratégies de sécurité (GPO), et du contrôle global du système. Le second serveur, sous Linux Ubuntu, est dédié à l'hébergement du cloud privé, au stockage sécurisé des fichiers, et à leur synchronisation.

L'ensemble est accessible via un réseau VPN, permettant aussi bien aux utilisateurs internes qu'aux membres de l'équipe situés à distance, notamment au Bénin, de se connecter et de travailler dans un environnement sécurisé. Cette infrastructure offre une meilleure performance, une meilleure gestion des accès et une séparation claire des responsabilités entre les services d'administration et ceux de stockage.



Cette sous-section présente les différentes étapes techniques qui ont été nécessaires à la réalisation concrète du projet. Chaque étape a été réalisée de manière progressive, en suivant un ordre logique permettant d'assurer la cohérence, la sécurité et la stabilité de l'infrastructure mise en place.

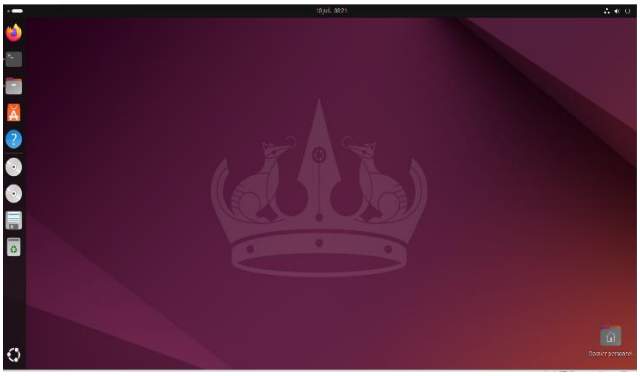
- Installation des systèmes d'exploitation : mise en place de Windows Server 2019 pour l'administration des utilisateurs et de Linux Ubuntu pour l'hébergement du cloud.
- Configuration du Bureau à distance (RDP) pour autoriser plusieurs connexions simultanées.
- Mise en place du VPN pour sécuriser les connexions distantes
- Intégration du cloud interne (OwnCloud).
- Supervision de l'infrastructure avec PRTG Network Monitor.
- Sécurité du système.

1.2.2. Installation et configuration des serveurs, Configuration du service RDP

La première étape du déploiement a consisté à installer et configurer les deux serveurs principaux de l'infrastructure. Chacun avait un rôle bien défini :

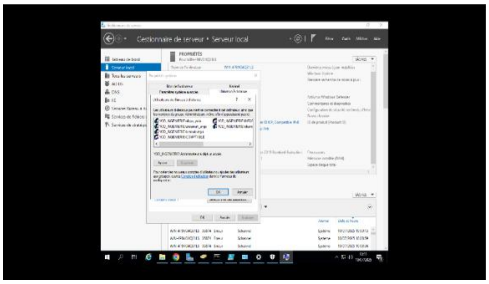
- Le serveur principal, installé sous Windows Server 2019, est destiné à gérer les utilisateurs, les sessions à distance RDP, les politiques de sécurité GPO et les services d'annuaire Active Directory.
- Le second serveur, installé sous Ubuntu Server, est dédié à l'hébergement des services critiques, notamment le cloud privé Owncloud, ainsi qu'à la gestion du stockage et des sauvegardes de fichiers.

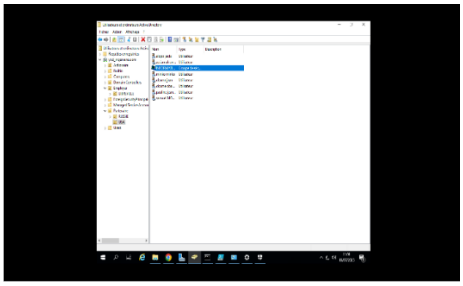
  L'installation s'est déroulée en plusieurs étapes :
- Téléchargement et gravure des images ISO officielles de Windows Server 2019 et Ubuntu.
- Installation de Windows Server 2019 sur une machine physique ou virtuelle : partitionnement du disque, configuration de l'utilisateur administrateur, définition de l'adresse IP statique.
- Installation d'Ubuntu Server et mise ajour des maquets

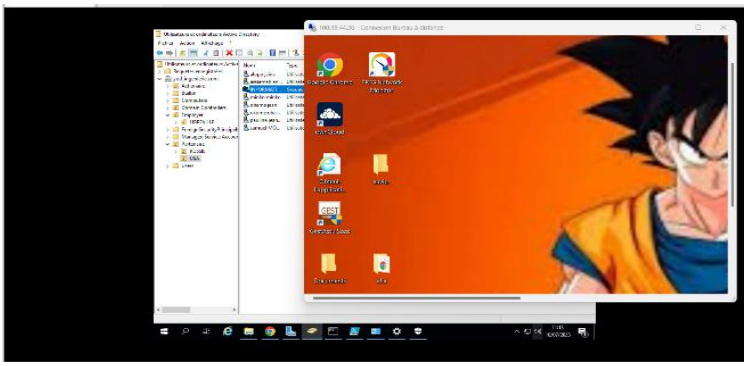


Les captures supplémentaires et les étapes détaillées relatives à l'installation sont disponibles en **Annexe 1.**

Après l'installation de Windows Server 2019, une étape clé du déploiement a consisté à configurer le service RDP (Remote Desktop Protocol) pour permettre des connexions multi-sessions. Cette configuration autorise plusieurs utilisateurs à se connecter simultanément à un environnement de travail centralisé, depuis des postes clients ou via un VPN, sans nécessiter de machines locales puissantes. Nous avons créé des unités d'organisation (OU) et des groupes dans Active Directory, ajouté les utilisateurs à ces groupes, puis attribué aux groupes les autorisations nécessaires pour la gestion à distance. Cette configuration permet à tous les membres des groupes de se connecter à distance via le protocole RDP.







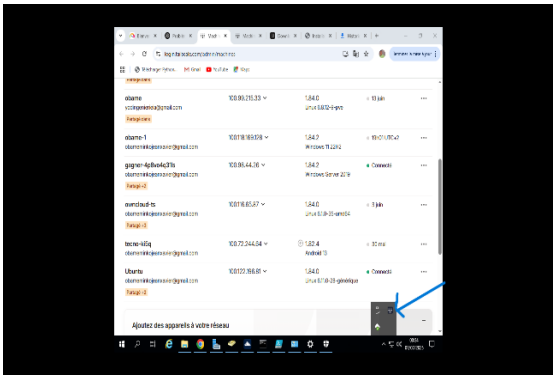
Les configurations additionnelles et les captures d'écran supplémentaires sont compilées dans **l'Annexe 2.**

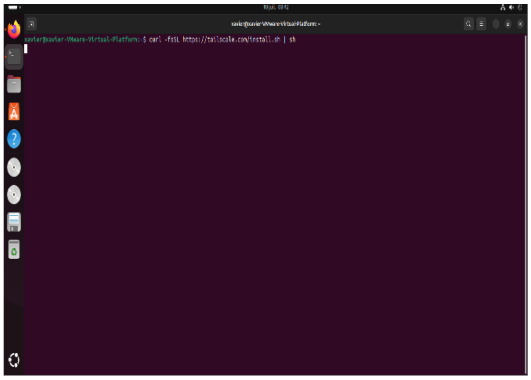
1.2.3. Mise en place du VPN Tailscale pour sécuriser les connexions, distantes Intégration du cloud

Pour garantir un accès sécurisé à l'infrastructure depuis l'extérieur, un réseau privé virtuel (VPN) a été mis en place à l'aide de Tailscale, une solution VPN moderne basée sur le protocole WireGuard. Le choix de Tailscale s'est justifié par sa simplicité de déploiement, sa compatibilité multiplateforme, et sa capacité à établir automatiquement des connexions chiffrées entre tous les appareils d'un même réseau virtuel.

- Création du compte Tailscale et configuration du domaine de gestion.
- Installation de l'agent Tailscale sur les deux serveurs (Windows Server et Ubuntu), puis sur les postes des utilisateurs ayant besoin d'un accès distant.
- Authentification et autorisation des machines via l'interface d'administration Tailscale, avec attribution automatique d'une IP privée dans le réseau Tailscale.

- Vérification de la connectivité : chaque poste connecté au VPN peut accéder aux ressources internes (serveur RDP, cloud, etc.) comme s'il était physiquement dans le réseau local.



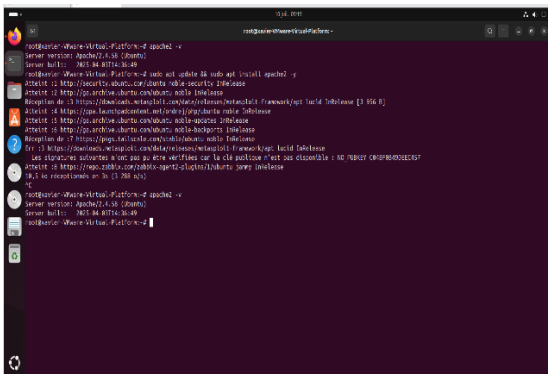


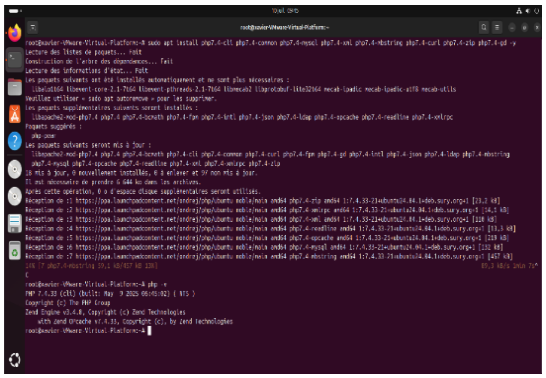
Les étapes détaillées d'installation et les scripts de configuration sont fournis en **Annexe 3**.

Pour offrir aux utilisateurs un espace de travail sécurisé, partagé et synchronisé, un cloud interne basé sur OwnCloud a été mis en place sur le serveur Ubuntu. Ce service permet à chaque utilisateur d'accéder à ses documents à distance, de les partager avec ses collègues et de les retrouver automatiquement sur tous ses appareils grâce au système de synchronisation.

- Mise à jour du server avant toute installation, le serveur Ubuntu a été mis à jour afin de garantir la stabilité du système et éviter les conflits entre paquets
- Installation d'Apache un serveur web Apache a été installé pour héberger l'interface web d'OwnCloud. C'est ce service qui permet d'accéder au cloud via un navigateur
- Installation de MariaDB base de données, OwnCloud nécessite une base de données pour stocker les comptes utilisateurs, les partages, les historiques, etc. MariaDB (alternative libre à MySQL) a été utilisée
- Installation de PHP et des extensions requises, OwnCloud étant une application web écrite en PHP, ce langage et ses modules sont indispensables à son fonctionnement. Les extensions installées permettent, par exemple, la gestion des fichiers compressés (zip), le chiffrement, l'affichage des images, etc.
- Téléchargement et extraction d'OwnCloud, Le fichier compressé contenant OwnCloud est téléchargé depuis le site officiel, puis décompressé dans le dossier des sites web Apache
- Création de la base de données OwnCloud, Une base nommée owncloud est créée, ainsi qu'un utilisateur dédié, pour sécuriser les accès.

- Attribution des droits d'accès, Les fichiers OwnCloud doivent appartenir à l'utilisateur Apache (www-data) pour fonctionner correctement

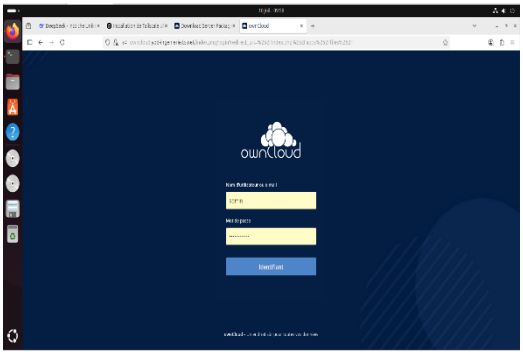


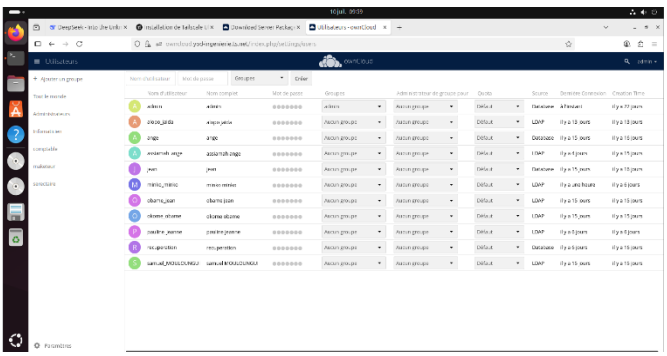


Les captures complémentaires et le guide complet d'installation sont regroupés en **Annexe 4**.

- Le client OwnCloud a été installé directement sur le serveur Windows Server 2019, depuis la session de l'administrateur. Comme tous les utilisateurs se connectent à ce même serveur pour travailler, cela permet que le client OwnCloud apparaisse automatiquement sur le bureau de chaque utilisateur, sans qu'il soit nécessaire de l'installer plusieurs fois. Grâce à cette méthode, chaque utilisateur voit un le logiciel cloud directement sur son bureau. Ce logiciel est synchronisé avec le serveur cloud (Linux) et se met à jour automatiquement dès qu'un fichier est ajouté, modifié ou supprimé

Après l'installation, l'interface cloud était accessible depuis tous les navigateurs, que ce soit sur le serveur Ubuntu, sur le serveur Windows ou sur d'autres machines du réseau.





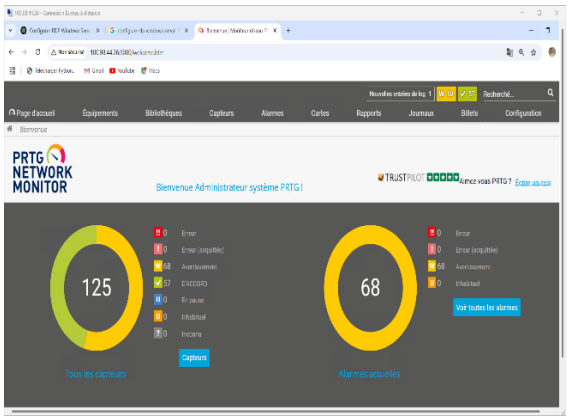
Les autres captures, notamment celles relatives à la synchronisation et au partage de fichiers, sont disponibles en **Annexe 5**.

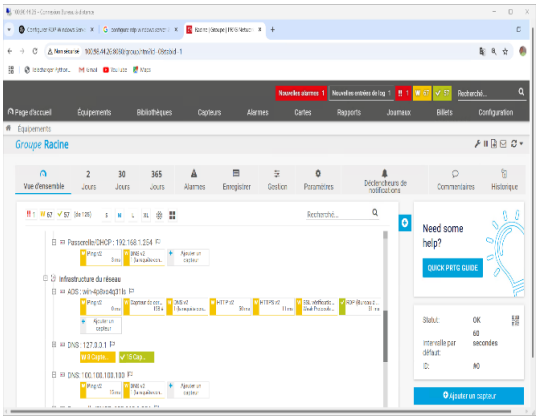
1.2.4. Supervision de l'infrastructure avec PRTG Network Monitor, Sécurité du système

Pour assurer un bon fonctionnement de l'infrastructure, un système de supervision réseau a été mis en place avec l'outil PRTG Network Monitor. Ce logiciel permet de surveiller en temps réel les deux serveurs installés (Windows Server 2019 et Ubuntu) afin de détecter rapidement tout problème technique.

Grâce à PRTG, l'administrateur peut :

- Surveiller la charge des serveurs (CPU, mémoire, disque).
- Vérifier l'état des services essentiels comme le cloud, le VPN ou les connexions RDP.
- Être alerté automatiquement en cas de surcharge, d'arrêt de service ou d'anomalie.
- Analyser les performances du réseau et des applications utilisées.

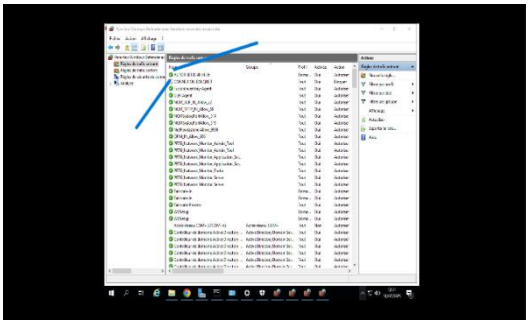


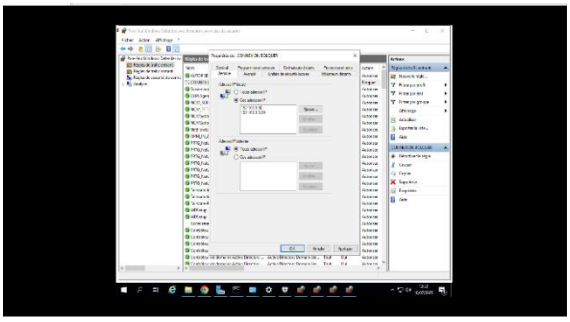


Les rapports complets et l'ensemble des graphiques détaillés sont disponibles en **Annexe 6.**

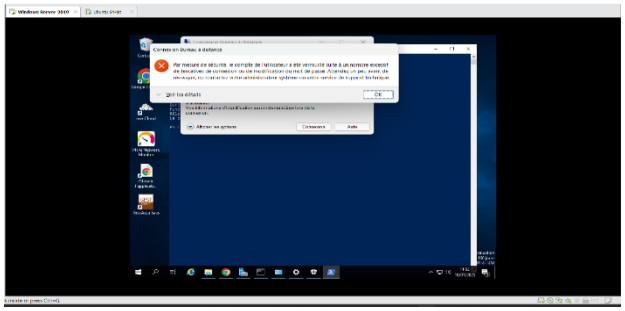
La sécurité de l'infrastructure a été renforcée à plusieurs niveaux, aussi bien sur le **serveur Windows** que sur le **serveur cloud (OwnCloud)**.

Sur le serveur Windows : Les **adresses IP locales ont été bloquées**, empêchant toute connexion directe en dehors du VPN. Les utilisateurs ne peuvent accéder à leur session que via l'adresse VPN, ce qui renforce considérablement la sécurité des connexions.

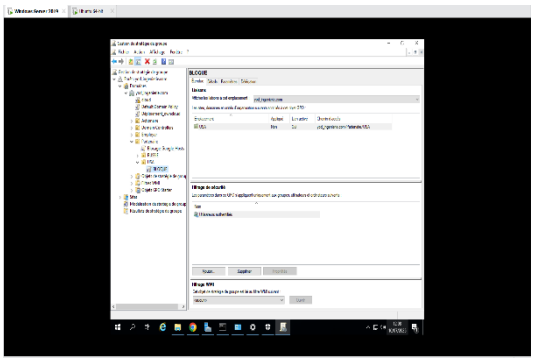


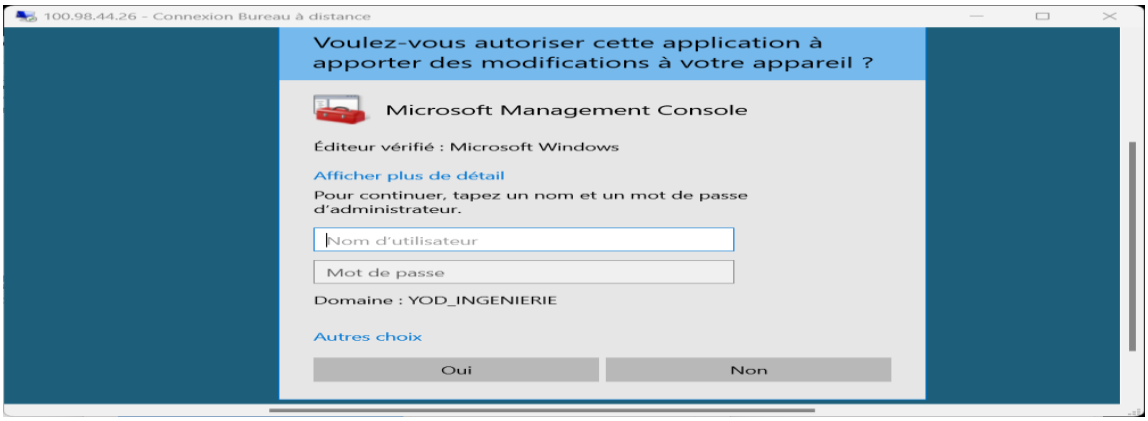


Afin de prévenir les intrusions malveillantes et les attaques par force brute, une politique de verrouillage de compte a été mise en place sur le serveur Windows. Ainsi, après **trois tentatives de connexion infructueuses**, le compte utilisateur concerné est **automatiquement bloqué pendant 15 minutes**. Cette mesure contribue à renforcer la sécurité d'accès au système.



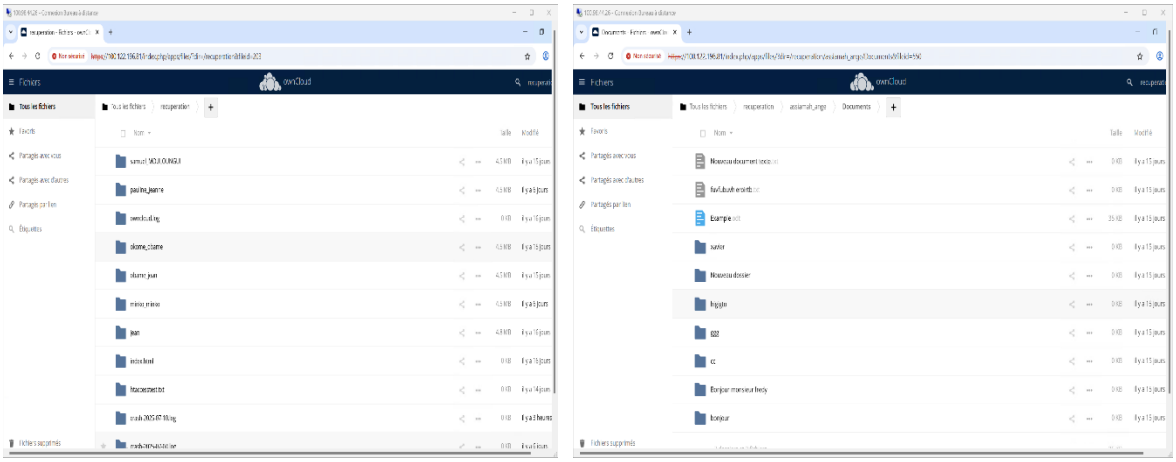
L'accès aux paramètres système et au panneau de configuration a été désactivé pour les utilisateurs via des stratégies de groupe (GPO)





Les configurations détaillées et captures complémentaires sont regroupées en **Annexe 7**.

Sur le serveur cloud : Un **système de sauvegarde miroir** a été configuré pour empêcher la suppression des données, que ce soit volontaire ou accidentelle. Cela garantit que les fichiers restent toujours récupérables, même en cas d'erreur humaine.



Les détails techniques de la configuration, ainsi que les captures complémentaires du système de sauvegarde, sont fournis en **Annexe 8**.

Le **protocole LDAP** a été mis en place pour **lier le serveur cloud OwnCloud à l'Active Directory** du serveur Windows. Grâce à cette intégration, les utilisateurs peuvent se connecter au cloud en utilisant **exactement les mêmes identifiants** que ceux utilisés pour accéder à leur session Windows.

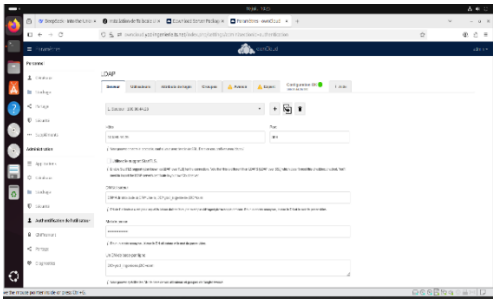
Lorsqu'un utilisateur tente de se connecter au cloud, **OwnCloud interroge automatiquement l'Active Directory** :

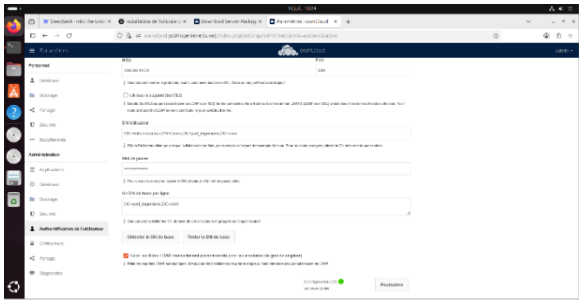
- Il **vérifie si les identifiants saisis existent** dans l'annuaire AD.

- Si c’est le cas, il **récupère les informations de l’utilisateur** (nom, identifiant, etc.).
- Puis, **il crée automatiquement un compte cloud** lié à ce profil.
- L’utilisateur est alors **connecté directement** au cloud, sans avoir à créer manuellement un compte.

Si un utilisateur saisit des identifiants qui n’existent pas dans l’Active Directory, le serveur LDAP renvoie une erreur et l’accès au cloud est refusé.

Cette configuration permet **d’automatiser la gestion des comptes OwnCloud**, d’éviter les doublons et de **centraliser l’administration des utilisateurs**, tout en facilitant l’expérience de connexion.





Les paramètres détaillés de configuration ainsi que la liste des utilisateurs synchronisés sont disponibles en **Annexe 9**.

Section 2 : Résultats et bilan

Cette section présente les résultats obtenus après le déploiement de la solution, ainsi qu’un bilan général du projet. Elle met en lumière les améliorations constatées au sein de l’infrastructure informatique, les points forts de la mise en œuvre, mais aussi les limites rencontrées et les axes possibles d’amélioration pour l’avenir.

2.1.1 Tests, validation

Une fois le déploiement terminé, plusieurs tests ont été menés afin de valider le bon fonctionnement de l'ensemble de la solution. Ces vérifications ont porté principalement sur les éléments suivants :

Connexion distante sécurisée : les utilisateurs ont pu accéder à leur environnement via VPN sans difficulté, depuis n'importe quel lieu disposant d'une connexion Internet.

Création automatique des comptes utilisateurs dans le cloud : grâce à l'intégration LDAP avec Active Directory, les comptes se généraient automatiquement à la première connexion.

Synchronisation en temps réel des fichiers : le client OwnCloud installé sur les postes permettait une mise à jour automatique des données entre le poste de l'utilisateur et le serveur cloud et **Stabilité des connexions RDP** : les sessions multi-utilisateurs sur le serveur Windows Server 2019 ont été maintenues de manière fluide, même en cas de connexions simultanées.

Répartition efficace des rôles : le serveur Windows gérait l'environnement de travail, tandis que le serveur Linux assurait l'hébergement du cloud et des sauvegardes critiques.

2.2.2. Observations post-déploiement

Après plusieurs jours d'utilisation, l'infrastructure mise en place a démontré sa stabilité et son efficacité. La centralisation des postes a permis une meilleure organisation des données, une réduction des interventions manuelles des utilisateurs, ainsi qu'un meilleur contrôle global des accès et des services.

Les utilisateurs ont apprécié la simplicité d'accès à leurs environnements et la possibilité de retrouver leurs documents synchronisés automatiquement, même en situation de mobilité.

2.3.3 Limites rencontrées

Malgré ces bons résultats, quelques limites techniques ont été relevées, La principale contrainte concerne la gestion de l'espace dans le cloud OwnCloud. Un système de sauvegarde miroir a été mis en place pour empêcher toute suppression accidentelle ou volontaire de fichiers. Si cette solution garantit une sécurité optimale, elle engendre aussi une accumulation continue des données, sans possibilité de nettoyage automatique.

Avec le temps, cela peut saturer l'espace de stockage, affecter les performances du serveur cloud, ou générer des coûts supplémentaires pour l'extension de capacité.

2.4.4 suggestions d'amélioration

Pour pallier cette limite et garantir la pérennité du système, plusieurs améliorations peuvent être envisagées :

- Mettre en place un système d'archivage pour déplacer manuellement ou automatiquement les fichiers anciens vers un espace de stockage séparé.
- Adopter un système de versionnage plus léger, limitant la duplication inutile des données.
- Prévoir une extension de capacité (ajout de disque ou volume distant) pour anticiper la croissance future de l'espace utilisé.

Cette deuxième partie a permis de détailler l'ensemble des étapes techniques mises en œuvre pour répondre aux besoins identifiés au sein de l'entreprise. À partir d'une infrastructure initialement limitée, le projet a abouti à la mise en place d'un système centralisé, moderne, sécurisé et adapté aux réalités du terrain. Chaque composant – qu'il s'agisse des serveurs, du cloud privé, du VPN ou encore de la supervision – a été soigneusement sélectionné et configuré pour améliorer la performance globale, simplifier la gestion des postes, automatiser les processus et renforcer la sécurité des données.

CONCLUSION GENRAL

Dans le cadre de notre stage à YOD Ingénierie, nous avons été confrontés à une problématique bien précise : comment améliorer l'organisation, la performance et la sécurité du parc informatique de l'entreprise, tout en limitant les coûts liés à l'achat de nouveaux équipements.

Pour y répondre, nous avons adopté une méthodologie progressive. Nous avons commencé par une observation sur le terrain afin d'identifier les principaux problèmes. Ensuite, plusieurs solutions ont été envisagées et comparées. Le choix s'est porté sur la mise en place d'une infrastructure centralisée, combinée à un accès distant sécurisé et à l'intégration d'un service cloud interne. La solution a été mise en œuvre étape par étape, avec deux serveurs dédiés, des outils de supervision, un système de sécurité renforcé et une automatisation de la gestion des utilisateurs.

Les résultats obtenus ont été positifs. L'infrastructure mise en place a permis une meilleure organisation du travail, une centralisation efficace des données, une réduction des risques liés aux erreurs humaines et une amélioration globale de la sécurité. Les utilisateurs ont désormais un environnement de travail plus stable et plus simple à utiliser, tandis que les administrateurs ont un contrôle total sur l'ensemble du système.

Cependant, certaines limites subsistent, notamment au niveau de l'espace de stockage du cloud, qui peut se remplir rapidement à cause du système de protection empêchant toute suppression. Cela ouvre la voie à des suggestions d'amélioration, comme la mise en place d'un quota par utilisateur ou d'un système d'archivage automatique pour éviter la saturation.

En résumé, ce projet nous a permis de mettre en pratique nos connaissances, de développer de nouvelles compétences et de proposer une solution concrète et fonctionnelle à une problématique réelle. Il représente un pas important dans notre parcours professionnel et une contribution utile pour l'entreprise.

BIBLIOGRAPHIE

University of Chicago Press. (2019). *The Chicago Manual of Style* (17e éd.). Chicago, IL : University of Chicago Press.

American Psychological Association. (2019). *Publication Manual of the American Psychological Association* (7e éd.). Washington, DC : APA.

ISO. (2021). ***ISO 690*** *: Information and documentation – Principes directeurs pour les références bibliographiques*. Genève : Organisation internationale de normalisation.

Scribbr. (2019). *Bibliographie aux normes APA*. Récupéré de Scribbr.fr

MyStudies. (2025, 5 mars). *Bibliographie de rapport de stage : guide complet*. Récupéré de MyStudies.com

MémoRédaction. (2025, 11 mars). *Bibliographie de rapport de stage : exemples et conseils*. Récupéré de Memoredaction.com

Paessler. (S.d.). ***PRTG Manual*** *: Active Directory Integration*. Paessler.com

Tailscale Inc. (2025, mai). *Tailscale Quickstart guide*. Tailscale.com

Ubuntu Documentation. (2013). *ActiveDirectoryHowto*. Help.ubuntu.com

OwnCloud. (S.d.). *LDAP – Active Directory integration guide*. OwnCloud.dev

ANNEXES