République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**ouloud **M**AMMERI DE **T**IZI- **O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Présenté par :

DJOUDI Mariem

TOUBAL Sarah

Thème

Implémentation d'un serveur de partage sécurisé au niveau de l'entreprise 2INT Partners

M^r M. LAZRI, Maitre de conférences, UMMTO,	Président
M^r F. OUALLOUCHE, Maitre de conférences, UMMTO,	Encadreur
M^r W. KHADIR, Directeur d'études, 2INT Partners,	Co-encadreur
M^r Dj. ALLOUACHE, Maitre de conférences, UMMTO,	Examinateur

Soutenu le : 08/07/2018

Dédicace

« Louange à Dieu ; seul et unique »

Je dédie ce modeste travail à ***mes très chèrs parents****, pour leurs sacrifices, leurs encouragements et soutiens durant mes études, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure une bonne santé et une longue vie.*

A mes très chères sœurs : ***Sihem****,* ***Laeticia*** *et* ***Karima*** *pour leurs soutient et leurs amour.*

A toute la famille ***TOUBAL.***

A mon très cher binôme ***Mariem***

A tous mes ami(e)s

Et à tous ceux qui ont contribué de prés ou de loin pour que ce travail soit possible, je vous dis merci.

Sarah

Dédicace

« Louange à Dieu ; seul et unique »

Je dédie ce modeste travail à ***mes très chers parents****, pour leurs sacrifices, leurs encouragements et soutiens durant mes études, Que dieu leur procure une bonne santé et une longue vie ; surtout mon cher frère* ***Farid*** *qui ma vraiment soutenue tout au long de mon parcoure, je le dédié aussi à ma chère belle sœur* ***Fatima Zahra*** *; ma sœur* ***Safia*** *et* ***ma grand mère.***

Je remercie infiniment la personne la plus proche de moi ***Toufik*** *et la plus chère amie et sœur* ***Sonia.***

A mon très cher binôme ***Sarah***

A tous mes ami(e)s

Mariem

Table des figures

Liste des tableaux

SOMMAIRE

Chapitre 2 : Solution proposée

Chapitre 3 : Sécurisation des serveurs implémentés

Introduction

Les réseaux et les systèmes informatiques sont devenus des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les entreprises de communication, les banques, les assurances, le domaine médicale ou encore le domaine militaire. Un réseau informatique est l'interconnexion de différents équipements informatiques tels que les postes clients, les switchs, les routeurs et les serveurs.

La présence d'un serveur dans un réseau est primordiale car il permet de fournir des services ou des opérations sur demande d'un ou plusieurs clients. Il existe différents types de serveurs tels que les serveurs d'impression, les serveurs web, les serveurs de partage de fichiers ainsi les serveurs de stockages de fichiers.

Le partage de données est l'une des premières raisons d'un déploiement de serveur de fichiers. Chaque poste de travail autorisé, quelque soit son système d'exploitation, peut se connecter au serveur qui peut être considérer comme une unité de disque de stockage.

Dans le cadre de notre projet de fin d'études, nous avons effectué un stage au sein de l'entreprise 2INT Partners afin d'implémenter un serveur de partage de fichiers indispensable au bon fonctionnement de l'entreprise. En effet, ce serveur permettra de résoudre le problème de partage d'une quantité importante de fichiers. De plus, le serveur backup permettra d'avoir une copie des différents fichiers échangés sur le réseau de 2INT Partners.
Notre travail est structuré comme suit :

- Dans le premier chapitre, nous présenterons quelques quelques généralités sur les réseaux informatiques et l'étude de l'architecture du réseau existant au sein de l'entreprise 2INT Partners.

- Le second chapitre, nous proposons les solutions les plus optimales afin de répondre aux besoins de l'entreprise.

- Dans le troisième chapitre nous présenterons la méthodologie suivie pour sécuriser le serveur de partage implémenté dans l'entreprise 2INT Partners.

Enfin, nous terminerons notre mémoire par une conclusion générale et quelques perspectives sur notre travail.

CAHIER DES CHARGES

Le présent projet sera établi au sein de l'entreprise 2INT Partners qui consiste à améliorer l'infrastructure du réseau déjà existant. Le travail demandé a pour objectif de simplifier la gestion des fichiers et l'échange de données entre les différents ordinateurs (opérateurs) de l'entreprise.

Une étude préalable est demandée afin de vérifier la nécessité de l'utilisation d'un serveur de partage de fichiers. En effet, une quantité importante de fichiers est manipulée par les employés de 2INT Partners et ces fichiers ne sont pas enregistrés sur une seule machine dédiée mais dispersés sur plusieurs supports. Donc, rechercher et traiter ces fichiers devient très difficile.

Ce serveur doit offrir une sécurité et une centralisation de fichiers en permettant à tout utilisateur connecté au réseau (fait parti ou non à l'entreprise) ayant l'autorisation de télécharger ou d'envoyer un ou plusieurs fichiers. De plus, différents niveaux d'accès soit lecture seule ou la possibilité de modifier les documents seront définis.

La deuxième phase du travail demandé consiste à sécuriser le serveur de partage de fichiers.

Chapitre 1 Généralités sur les réseaux et étude de l'existant

1.1. *Préambule*

Le système informatique est généralement défini par l'ensemble de données et de ressources matériels et logiciels de l'entreprise. Il permet de les stocker ou les faire circuler sur le réseau. Il est considéré comme le cœur de l'entreprise, il est donc recommandé d'améliorer l'architecture du réseau existant afin de rajouter de nouvelles fonctionnalités qui nous permet d'avoir une bonne gestion du système, une souplesse d'utilisation et d'administration qui répond à nos besoins. Pour cela il faut passer par une étude du réseau pour connaitre les différents équipements matériels et logiciels utilisés ainsi les caractéristiques de l'existant etc. Cette étude est donc obligatoire.

1.2. Quelques généralités sur les réseaux informatiques

Un réseau informatique est un ensemble d'entités interconnectées les unes avec les autres. Il est un ensemble de machines reliées entre eux grâce à des lignes physiques comme les câbles on dit c'est un réseau filaire ou bien un réseau non filaire relié par des ondes éléctromagnitiques.

- ✓ On peut classer les réseaux selon : la taille, la topologie ou l'architecture réseau : **[1]**

1.2.1. Classification selon la taille

- ***LAN :*** réseaux locaux pour de courtes distances avec des débits de quelques dizaines de Mbits/seconde jusqu'à quelques centaines.
- ***MAN :*** destinés à parcourir de très grands périmètres qui sont fédérateurs de réseaux locaux.
- ***WAN :*** il signifie un réseau étendu permettant de connecter plusieurs LAN éloignées entre elles. Le débit devient de plus en plus faible de la distance. Internet est un regroupement de WAN.

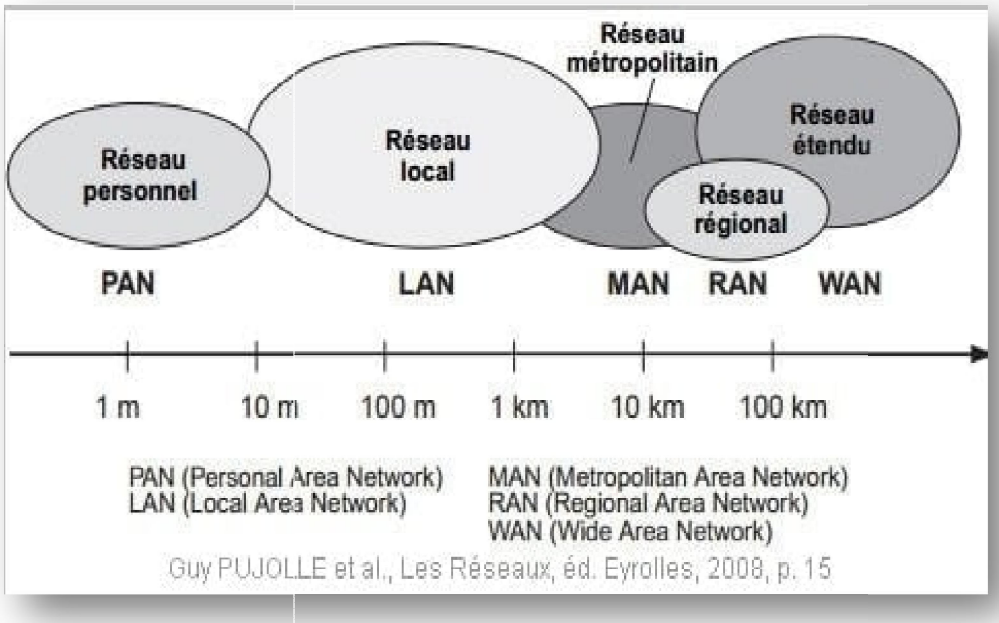

Figure 1.1: *Classification des réseaux informatique selon la taille*

1.2.2. Classification selon l'architecture réseau

- **Architecture Peer to Peer**

Parfois appelée poste à poste dans cette architecture un ordinateur central jouant le rôle d'un serveur dédié. Ainsi chaque ordinateur dans tel réseau est parfois serveur, parfois client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

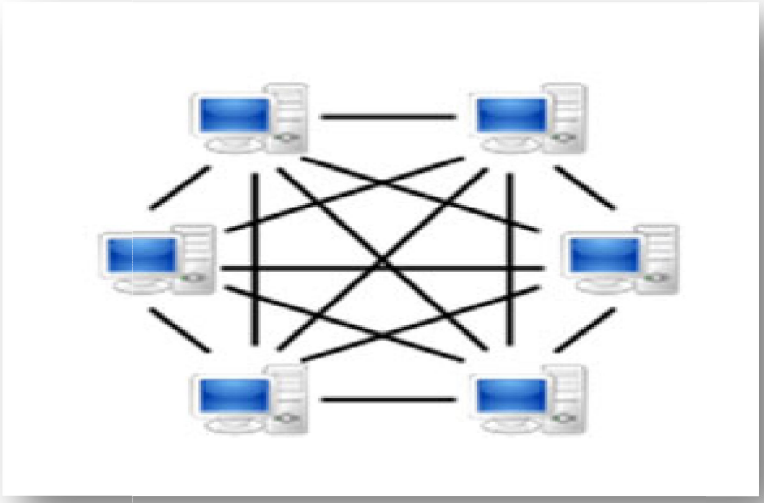

Figure 1.2 : *Architecture poste à poste*

➢ Architecture de type client/ serveur

Un réseau d'architecture client/serveur est celui où les ordinateurs (clients) sont reliés à un serveur dédié qu'est un ordinateur central fournit des services réseaux aux clients.

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur qui est une machine généralement très puissante en terme de capacité d'entrée-sortie, qui leurs fournit des services. Ces services sont des programmes fournissant les données telles que les fichiers, une connexion…**[7]**

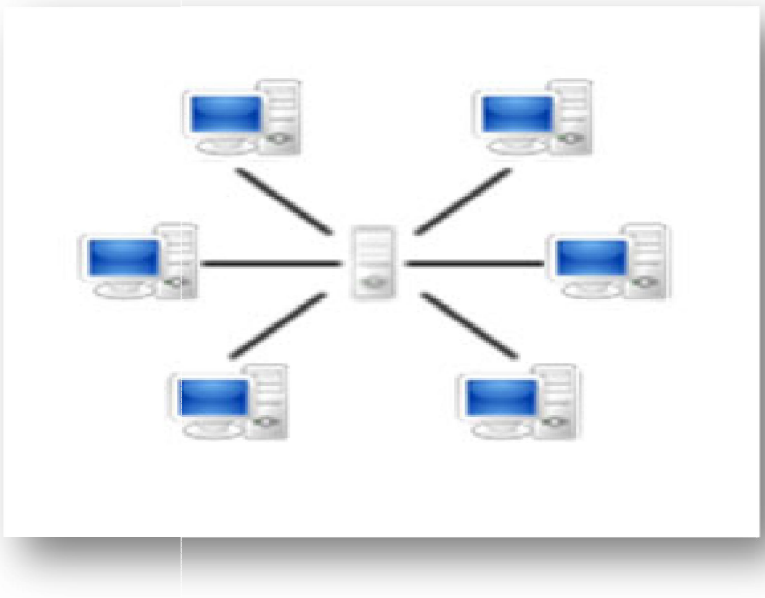

Figure 1.3 *: Architecture client serveur*

1.2.3. Classification selon la topologie

C'est le classement selon l'arrangement physique, c'est-à-dire la configuration spatiale du réseau et les machines qui le composent, on distingue généralement les topologies suivantes :

➢ *Topologie en bus*

Tous les équipements sont branchés en série sur le serveur. Chaque poste reçoit l'information mais seul le poste pour lequel le message est adressé traite l'information.

On utilise un câble coaxial pour ce type de topologie.

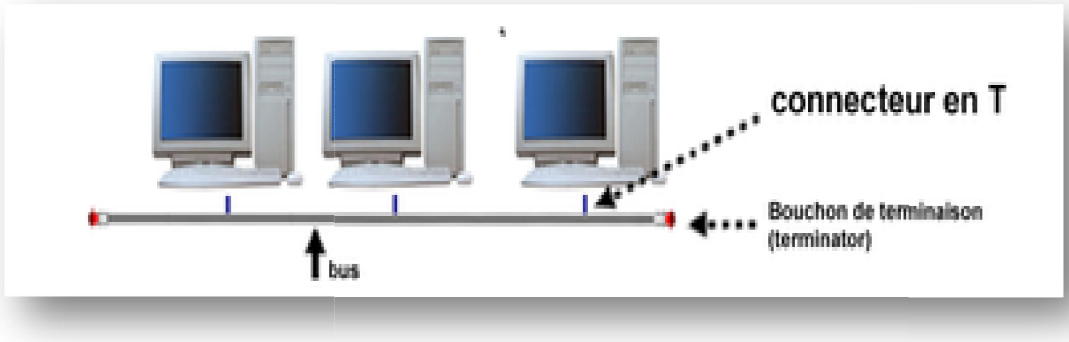

Figure 1.4 : *Topologie en bus*

➢ *Topologie en anneau*

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

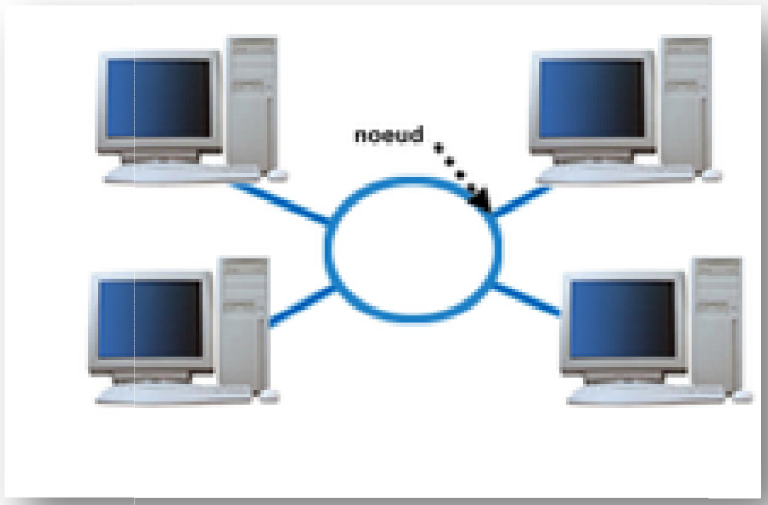

Figure 1.5: *Topologie en anneau*

➢ *Topologie en étoile*

La topologie réseau la plus courante, notamment avec les réseaux Ethernet, les ordinateurs du réseau sont relies à un système matériel central appelé concentrateur.

Il comprend un certain nombre de jonction auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Donc il assure la communication entre les différentes jonctions. C'est

Ce type de réseaux est facile à maintenir mais la défectuosité du nœud central provoque un arrêt de tout le réseau.

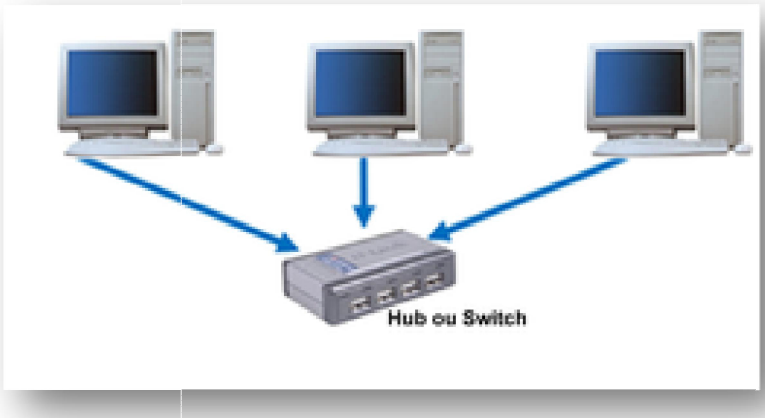

Figure 1.6: *Topologie en étoile*

1.3. Les supports de transmission

Les supports de transmission sont nombreux. Parmi ceux-ci, on distingue : les supports métalliques, non métalliques et immatériels. Lors de la conception d'un réseau, le choix du support de transmission dépendra d'un certain nombre de critères parmi lesquels on distingue :

- Bande passante : la bande passante d'une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important.
- Vitesse de transmission.
- Distance du câble.
- Insensibilité au bruit.
- Type du signal véhiculé (analogique ou numérique).
- Le cout

1.4. Description du modèle OSI

Le modèle OSI (Open Systems Interconnexions), créé en 1978 par l'organisation internationale ISO a pour objectif de constituer un modèle de référence d'un réseau informatique et ceci dans le but de permettre la connexion entre les architecture propriétaires, hystérogène qui existaient. Ce modèle est constitué de sept couches dont chacune correspond à une fonctionnalité particulière d'un réseau et chaque couche est immédiatement adjacente même si le model OSI est très peu implémenté aux couches. Il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant du réseau. Ainsi contrairement aujourd'hui, TCP/IP est mis en œuvre partout même lorsque l'on parle de ce protocole on l'associe aux couches de modèle OSI.

Les quartes premières couches dites basse assurent l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les trois autres couches dites hautes, sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques.

Voici les septes couches du model OSI :

Couche1 « Physique » : elle s'occupe de la transmission de bits sur un canal de communication, et d'adapter le signal électrique au support physique.

Couche2 « Liaison » : elle assure l'acheminement point à point des données.

Couche3 « Réseau » : c'est la couche qui permet le routage des paquets dans les sous-réseaux.

Couche4 « Transport » : elle assure un acheminement des messages complets au destinataire.

Couche5 « Session » : cette couche s'intéresse à établir et maintenir des sessions c'est-à-dire débuter le dialogue entre deux machines.

Couche6 « Présentation » : elle est responsable de la présentation des données de telle sorte qu'elle soit indépendante du type de microprocesseur ou du système d'exploitation.

Couche7 « Application » : cette couche est le point de contacte entre l'utilisateur et le réseau, c'est donc elle qui va apporter à l'utilisateur des services de base offerts par le réseau comme par exemple le transfert de fichiers et la messagerie.

1.5. Architecture TCP/IP

C'est une architecture développée en quatre couches sur une base de protocoles existants :

Couche 1 « Accès au réseau » : c'est la couche de plus bas niveau sur le réseau. Cette couche contient des protocoles qui gèrent l'acheminement des informations entre émetteur et récepteur.

Couche 2 « Réseau **» :** dans cette couche on trouve principalement deux protocoles

Couche3 « Transport » **:** dans cette couche on retrouve les protocoles de transport des données, les plus utilisées sont le protocole TCP et UDP.

Couche4 « Application » : c'est la couche qui contient les protocoles de communication entre les clients et les serveurs (serveur http, FTP).

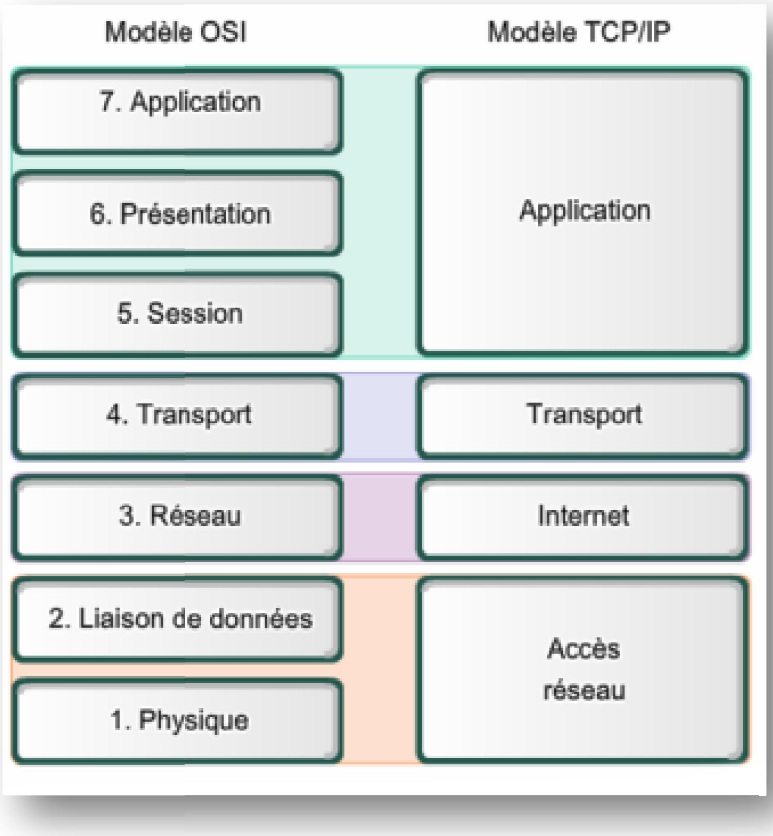

Figure 1.7 : *Analogie de model OSI avec le modèle TCP/IP*

1.6. Les protocoles des données

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau, Certains protocoles seront par exemple spécialisés dans l'échange de fichiers FTP, d'autres pourrons servir à gérer simplement l'état de la transmission

Sur internet par exemple, les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble relié entre eux. Cette suite de protocoles s'appelle TCP/IP.

1.6.1. Protocole TCP

Est un protocole fiable, ce protocole de sécurité d'échange de données : créé dans le but d'établir une communication de haute fiabilité entre deux exécutées sur deux ordinateurs autonomes et raccordés à un réseau.

1.6.2. Protocole IP

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâces à la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les notes sous la forme xxx.xxx.xxx.xxx ou chaque xxx présente un entier de 0 à 255.

Par exemple 194.153.205.26 est une adresse IP, on peut distinguer deux parties dans une adresse IP :

- ✓ Les nombres de gauche désignent le réseau.
- ✓ Les nombres de droite désignent les ordinateurs de ce réseau.

1.6.3. Protocole UDP

Le protocole UDP est l'un des deux principaux protocoles utilisé sur les réseaux TCP/IP, que le réseau soit Ethernet ou sans fils. Contrairement au TCP, il ne permet pas à l'émetteur de vérifier si les données sont effectivement reçues en recevant un accusé de réception. De fait, il est sa structure est plus simple et les transferts plus rapides. Par contre, il utilise aussi 65535 ports différents pour communiquer de (de 0 à 255), chaque réseaux utilise un ou plusieurs numéros pour communiquer.

- ✓ Apres avoir vu quelques généralités sur les réseaux informatiques, nous allons faire maintenant une étude du réseau de l'organisme d'accueil.

1.7. Présentation de l'entreprise 2INT

2INT Partners est un prestataire de service informatique spécialisé dans le déploiement et l'installation de solutions réseau, qui est toujours à la recherche de la solution économique et robuste pour satisfaire la clientèle, l'entreprise essaye toujours de répondre aux mieux aux besoins et aux exigences de ses clients. Cette entreprise se situe à la Nouvelle ville, wilaya de Tizi-Ouzou.**[7]**

1.7.1. Historique de l'entreprise

Créée en 2012, 2INT Partners débute comme une entreprise d'installation de solutions réseaux et serveurs. Avec le progrès technologique, l'entreprise tente de suivre l'évolution des besoins des utilisateurs afin d'innover en matière de solutions IT

L'entreprise compte actuellement 24 salariés, dont 10 responsables des différents services. **[7]**

1.7.2. Les valeurs de l'entreprise

Les principales valeurs de l'entreprise sont :

- ✓ Innover afin de suivre l'évolution des besoins.
- ✓ Satisfaire la clientèle en privilégiant les besoins des clients.

Fournir une assistance aux clients après qu'ils aient acquit un produit ou un service. **[7]**

1.8 .Présentation de l'existant

Une étude de l'architecture réseau de l'entreprise est très importante pour déterminer les besoins de cette infrastructure afin de l'optimiser et de l'améliorer.

Il est nécessaire de connaitre le matériel physique et logique dont dispose cette infrastructure car ces informations vont nous aider à prendre des décisions par rapport à les améliorations que nous allons apporter à ce réseau. **[7]**

Après des visites au niveau des salles contenant les différents équipements intervenant dans le réseau de l'entreprise 2Int Partners, nous sommes arrivés à représenter l'architecture du réseau global en utilisant le site web creately.com, tel que schématisé par la figure suivante **[2]** :

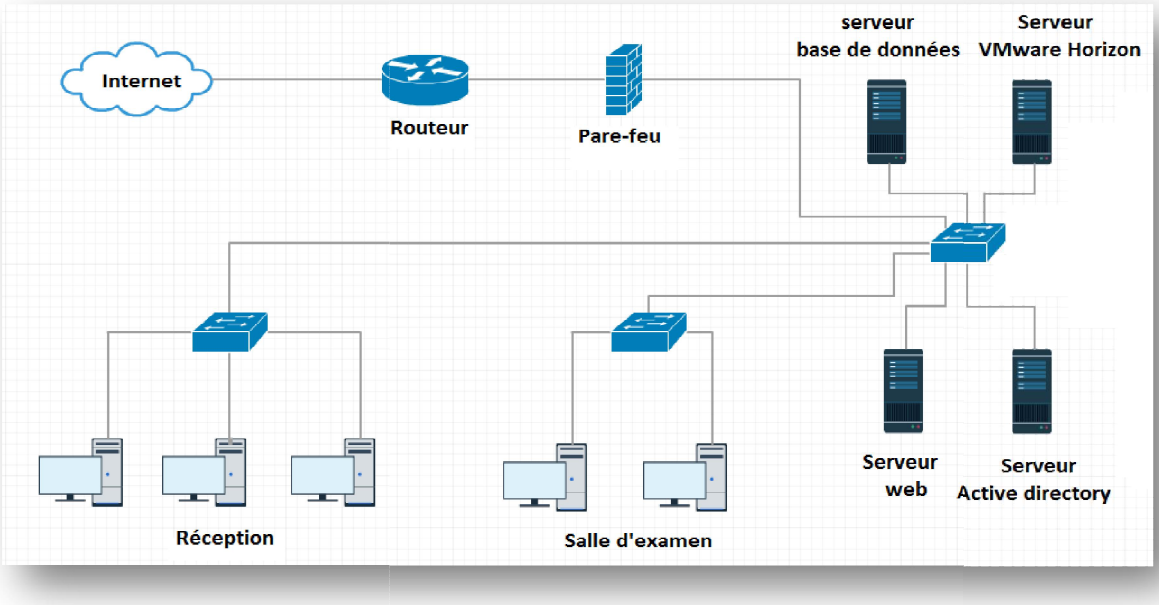

Figure 1.8 : *L'architecture existante*

Dans la suite de ce chapitre, nous présentons les différents équipements utilisés.

1.9. Les équipements utilisés

1.9. 1. Les serveurs

Un serveur est un dispositif informatique matériel et logiciel qui offre des services, à un ou plusieurs ordinateurs appelés clients. Un serveur informatique répondant en permanence des requêtes provenant des clients. Il est utilisé par les entreprises, les institutions et les opérateurs de télécommunication, les centres de traitement de données, ...etc. **[8]**

Un serveur est caractérisé par :

- Utiliser les ressources de machines dédiées à des tâches bien particulières
- Permettre à plusieurs machines d'utiliser ces ressources distantes
- Structurer et centraliser les ressources
- Gagner en souplesse

- **Serveur d'impression**

Le serveur d'impression permet de partager une ou plusieurs imprimantes entre une dizaine voire même une centaine d'ordinateurs situés sur un même réseau informatiques, cette imprimante ne peut pas satisfaire toutes les requêtes en temps réel donc elle fait la mémorisation des travaux à réaliser, cela se fait par la gestion des ressources de la file d'attente. **[8]**

- **Serveur de messagerie**

Un serveur de messagerie électronique est un logiciel qui est connecté à Internet, il permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques. **[8]**

- **Serveur de partage de fichiers**

Il permet de partager des données à travers un réseau et possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichiers. **[9]**

- **Serveur de stockage de fichiers**

C'est un serveur de sauvegarde pour une protection des données en continu, il permet une sauvegarde incrémentale des données et assure une copie intégrale du serveur initial, tout en réduisant le risque de pertes de données à quelques secondes ou quelques minutes au maximum. Tous les fichiers sont copiés même ceux qui restent ouverts lors de la sauvegarde. **[9]**

1.9.2. Les serveurs existants

- **Serveur de base de données**

C'est un outil qui possède toutes les caractéristiques pour pouvoir accompagner l'utilisateur dans la manipulation, le contrôle, le tri, la mise à jour, et bien d'autres actions encore, de bases de données grâce au langage SQL.

- **Serveur VMware Horizon**

Un administrateur Horizon doit effectuer des taches spécifiques pour permettre aux utilisateurs de se connecter à des applications et des postes de travail distants.

- **Serveur web**

Un serveur Web est un programme qui utilise le protocole HTTP pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandées via des requêtes transmises par les clients HTPP de leurs ordinateurs. Des ordinateurs et des appliances dédiés peuvent également jouer le rôle de serveurs Web.

- **Serveur Active Directory**

Active Directory est un outil destiné aux utilisateurs, il permet une représentation globale de l'ensemble des ressources et des droits associés, il représente aussi un outil d'administration et de gestion du réseau. Il fournit des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise. La structure d'Active Directory lui permet de gérer de façon centralisée des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites.

1.10. Le routeur DLink 2750U

Il est un élément intermédiaire dans un réseau informatique assurant le routage des paquets son rôle est de faire transiter les paquets d'une interface réseau vers une autre, et acheminer le différent segment des paquets en fonction de la couche trois, les routeurs prennent des discision logique d'optimisation pour choisir la meilleur voie des données d'un réseau à un autre et de diriger ensuite les paquets vers le pont de sortie qui correspond au ont de sortie suivant.

1.11. Switch

Il désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Contrairement au concentrateur ou hub, le Switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau.

Le Switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

1.12. Firewall pfsense

C'est un logiciel et /ou un matériel permettant de faire respecter la politique de sécurité du réseau.

PfSense est un routeur/pare-feu open source , il utilise des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise. PfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy, serveur VoIP.

1.13. Poste clients

C'est des ordinateurs qui sont connectés au réseau avec un accès à internet ce qui les rend vulnérables aux intrusions externes.

Selon l'architecture du réseau de cette école ;il existe 5 PC de ce type de matériels ,deux se trouvent au niveau de la salle d'examen, et les trois autres PC sont implémentés au niveau de la réception.

1.14. Les Logiciels existants

Tableau 1.1 : *Liste des applications existantes dans notre infrastructure* **[7]**

Les applications	***Description***
Team Viewer	Team Viewer est un utilitaire qui offre plusieurs fonctions parmi elles les fonctions de bureau à distance, de conférence en ligne et de transfère de fichiers.
FileZilla	FileZilla est un client FTP utilisé afin de transférer des fichiers vers ou à partir d'un serveur FTP distant.
Kaspersky	Kaspersky est un anti virus qui protège les utilisateurs contre les virus avec une protection en temps réel.

1.15. La sécurité existante

➢ La sécurité informatique

C'est l'ensemble des moyens techniques organisationnels juridiques et humains nécessaire à la mise en place de moyens visant à empêché l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.

➢ La sécurité physique

La sécurité physique vise à favoriser l'exploitation des équipements informatiques dans des conditions fonctionnelles optimales, de manière à bénéficier d'un maximum de performances durant un maximum de temps.

Dans cette entreprise la sécurité physique existante est :

- Le routeur et les Switchs ont été placés dans une armoire fermée.
- L'accès à la salle où se trouvent les serveurs est strictement interdit sauf aux personnels.
- L'entreprise dispose d'un par feu dans son réseau.

➢ La sécurité logique

La sécurité logique est la sécurité fournit par le système d'exploitation, les logiciels de base, et les administrateurs du système.

Les postes de travail sont équipés par un système d'exploitation Windows 7 avec une suite Microsoft office 2010 professionnel.

Les serveurs sont équipés d'un système d'exploitation Linux Ubunto 16.04 et Windows serveur 2012, nous avons aussi recensé d'autres applications, qui sont comme suit :
La présence d'un antivirus « Kaspersky » qu'il permet de protèger les utilisateurs contre les virus avec une protection en temps réel.

1.16. Critique de l'existant

Les données utilisées au sein de l'entreprise 2INT Partenrs sont très importantes. En effet, les différentes notes des étudiants, les cours partagés, le suivi des carrières des employés ajoutant à

cela le manque de gestion des fichiers et les difficultés d'échanges des données entre les différents postes du réseau.

Toutefois, dans l'architecture du réseau existant, on ne trouve pas de serveur de fichiers. De plus, en cas d'une intrusion les pertes seront très lourdes pour l'entreprise et l'image de cette dernière va se détériorer.

1.17. *Discussion*

Dans ce chapitre nous nous sommes intéressé à découvrir et connaitre quelques généralités sur les réseaux informatiques, ainsi à se familiariser avec le réseau existant au sein de l'école 2INT Parteners.

En faisant une étude qui nous a permis de détecter quelques anomalies telle que le manque d'un serveur de partage dans cette infrastructure, donc nous allons opter pour les résoudre dans le chapitre suivant.

2.1. Préambule

Afin de trouver une meilleure solution, nous allons faire une recherche d'applications qui répondent à nos besoins ; une application pour le partage de fichiers et une autre pour le stockage. Ces deux applications sont très importantes pour le bon fonctionnement du notre réseau car elles permettent de partager des fichiers entre les différents utilisateurs, l'accès à distance aux fichiers et la sauvegarde.

2.2. Solution proposée

Après l'étude faite sur l'architecture de ce réseau, nous proposons deux solutions qui sont comme suit :

- Implémentation d'un serveur de partage dans le réseau pour simplifier la gestion des fichiers et l'échange de données entre les différents postes.
- Installation d'un serveur de sauvegarde de données (Backup), pour l'enregistrement automatique et régulier des données de l'entreprise. Cela nous permet de récupérer les données en cas d'une perte.

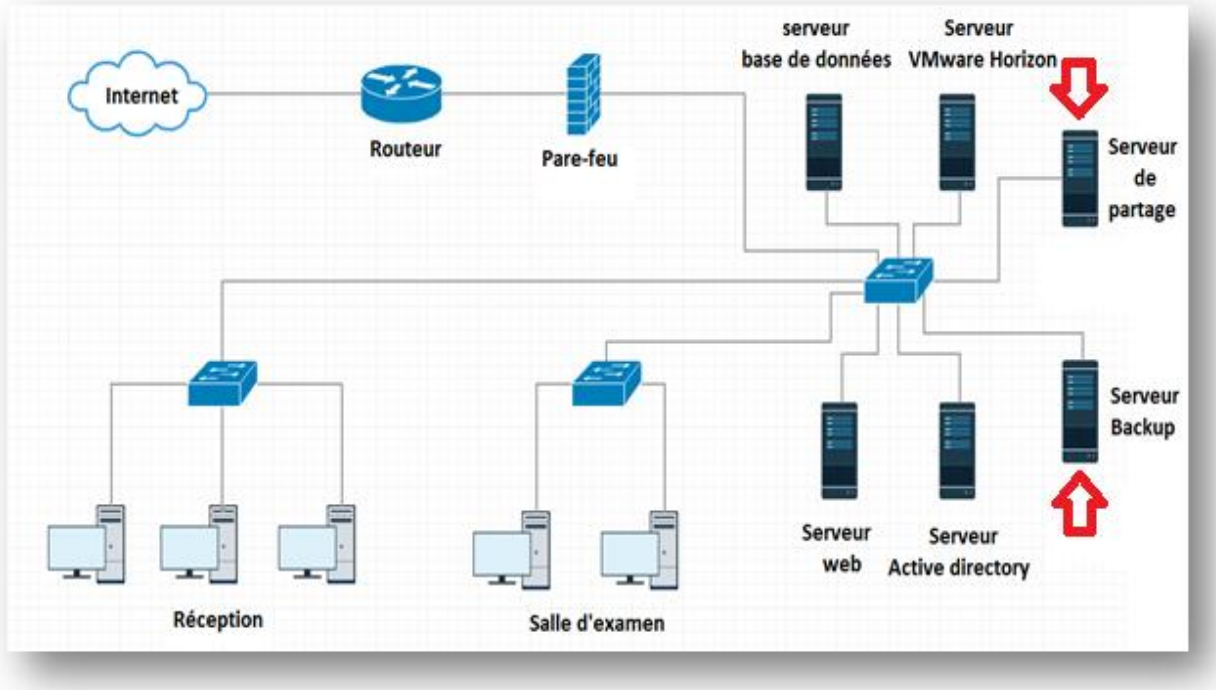

Figure 2.1 : *Architecture proposée*

2.2.1. Choix d'une solution de partage de fichiers

Plusieurs applications peuvent être utilisées comme serveur de partage de fichiers. Afin de faire un choix, nous avons fait une étude comparative entre les serveurs de partage les plus utilisés. Cette étude est représentée par le tableau suivant :

Tableau 2.1 : *Comparaison entre les applications de partage de fichiers.*

Applications	***Avantages***	***Inconvénients***
OwnCloud 	• Application open source. • Simple à utiliser. • Stockage des fichiers, synchronisation avec différents appareils (Android,…) • Partage des données. • Chiffrement et sécurisation des données envoyées. • Accès aux fichiers via un navigateur qui ne nécessite pas l'installation du client OwnCloud. • Permet de retrouver plusieurs anciennes versions d'un document modifié. • Gestion des tâches. • Personnalisation de l'environnement graphique. • Migration, back up des données. • Calendrier.	• Certains types de données peuvent être exclus de chiffrement. • Galerie photos, appel vidéo et audio player non disponible.

WebSharingLite 	• Interface claire et intuitive. • Zoom accessible. • Permet de transférer sans fil des fichiers vers et depuis notre téléphone ou tablette à l'aide d'un navigateur web. Nous pouvons lire et gérer de la musique, regarder nos photos, dispose en outre la possibilité de partager.	• Mauvaise expérience audio. • Limitations d'utilisation dans la version gratuite par d'envois multiples. • Logiciel payant 2.99$.
Xender 	• Connu plus tôt pour le transfert par Flash. • Application de transmission libre qui utilise la puissance réelle de la connexion Wifi Direct. • Nous pouvons envoyer toutes sortes de fichiers, y compris des applications, des jeux, des films, des chansons, des dossiers, des documents, etc ; • Vitesse fulgurante en secouant simplement notre appareil streaming de bonne qualité. • Accès rapide aux vidéos.	• Installation un peu longue. • Exige que l'expéditeur et le récepteur aient Xender installé en eux. • Quelques soucis de fonctionnement. • Problème de sécurité des données.

Parmi ces différentes applications étudiées, nous avons constaté que OwnCloud est une application libre (open source) contrairement à WebSharingLite dont le logiciel est payant. De plus, OwnCloud est basée sur une interface graphique ce qui la rend conviviale, simple à utiliser et à installer en la comparant à Xender qui prend beaucoup de temps lors de son installation et pour qu'elle soit fonctionnelle, elle doit être installé sur les deux périphériques qui veulent s'échanger des fichiers. Le deuxième inconvénient de l'application Xender est qu'elle est moins sécurisée par rapport à OwnCloud.

En utilisant OwnCloud, nous pouvons mettre en place une plate-forme de partage de fichiers sécurisée. L'administrateur réseau peut créer et supprimer des comptes et définir pour chaque compte les droits d'accès.

2.2.2. L'application OwnCloud

OwnCloud est une application open source, elle permet de mettre en service un Cloud local sécurisé pour le partage et le stockage des données, elle est aussi une application PHP utilisant Apache et MySQL qui donne la possibilité d'uploder les fichiers par son interface web qui sont disponible avec des options de partage, les fichiers textes peuvent être consultés directement depuis le navigateur. Avoir une application de partage de fichiers dans l'entreprise 2INT Parteners est très important car cette application permet de partager les notes des étudiants entre les enseignants et le secrétariat. Cet application permet aussi aux enseignants de partager des cours avec les étudiants, les étudiants à leurs tour peuvent accéder à ces informations partagées à distance, il se fait juste d'avoir un compte, un nom d'utilisateur et un mot de passe et bien sur avoir des droits de télécharger, partager, licture donnés par l'administrateur de ce réseau. **[10]**

2.3. Les étapes suivies pour la mise en place de notre application

Dans cette solution nous allons installer l'application choisie auparavant (Owncloud), qui est un logiciel libre offrant une plateforme de services de stockages et de partage de fichiers. Elle est présentée comme une alternative à Dropbox, lequel est basé sur un cloud public, le stockage des données se fait au sein de l'infrastructure de l'entreprise et les accès sont soumis à la politique de sécurité informatique de celle-ci.

OwnCloud peut être installée sur n'importe quel serveur, ce serveur supportant une version récente de PHP et supportant MySQL (base de données par défaut). Pour de meilleures performances, stabilités, intégrité des fonctionnalités, nous optons pour les différentes plateformes représentées par le tableau 2.2.

Tableau 2.2 : *Les différentes plateformes utilisées et leurs options*

Plateforme	Types
Système d'exploitation	Debian9.2.0
Base de données	MySQL
Serveur web	Apache2
Runtime PHP	PHP 4.6.6

- ✓ La première étape consiste à installer le système d'exploitation Debian9 (voir annexe) ensuite on passe a l'installation de la base de donnée MySQL.

2.3.1. MySQL

C'est un système open source (logiciel libre) de gestion de bases de données(SGBD) relationnelles, il est distribué sous une double licence GPL et propriétaire et il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public applications web principalement que par des professionnels, en concurrence avec Oracle, Informix et Microsoft SQL Server.

Le couple PHP/MySQL est très utilisé par les sites web et proposé par la majorité des hébergeurs Web. Plus de la moitié des sites Web fonctionnent sous Apache, qui est le plus souvent utilisé conjointement avec PHP et MySQL.

- ✓ Pour installer MySQL nous allons utiliser les commandes suivantes :
  - ➢ Echo –e deb http://repo.msql.com/apt/debian/stretch mysql-5.7\ndeb-scr http://repo.mysql.com/apt/debian/strechmysql-5.7"> /etc/apt/sources.hist.d/dmysql.list
  - ➢ Wget –O/tmp/RPM-GPG-KEY-mysql http://repo .mysql.com/RPM-GPG-KEY-mysql
  - ➢ apt-key add /tmp/RPM-GPG-KEY-mysql
  - ➢ Apt update
  - ➢ Apt install mysql-server
- ✓ L'installation de MySQL est bien terminée donc nous allons entamer l'étape suivante qui consiste à installer le service apache2.

2.3.2. Le service Apache

Apache HTTP Server (logiciel libre) est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire sur le réseau Internet. Ce protocole permet de faire le transfert de données et il définie la communication entre un client et un serveur sur le (WWW). Ce protocole fonctionne sur le principe « requête-réponse ».

- ✓ Sur le terminal nous allons écrire la commande suivante qui remet d'installer le service Apache2 :

```
root@debian:/home/sarah/Téléchargements# apt-get install apache2
```

Figure 2.2 : *Installation du service Apache*

- ✓ Pour prendre en compte son activation, il faut redémarrer ce service on saisissant la commande suivante dans un terminal :

```
root@debian:/home/sarah# service apache2 restart
```

Figure 2.3 : *Redémarrage de service Apache*

- ✓ Après avoir installé le service Apache2, nous allons passer à l'installation de phpMyAdmin.

2.3.3. PhpMyAdmin

phpMyAdmin est une application Web pour les systèmes de gestion de base de données MySQL réalisée principalement en PHP et distribuée sous licence GNU GPL.

C'est l'une des plus célèbres interfaces pour gérer une base de données MySQL sur un serveur PHP, cette interface permet d'exécuter facilement des requêtes comme les créations de table de données, insertions, mises à jour, suppressions et modifications de structure de la base de données, ainsi que l'attribution et la révocation de droits et l'import/export.

✓ On passe maintenant à l'installation de PhpMyAdmin, en utilisant toujours la même commande « apt-get » suivie du nom du paquet qu'on désire installer:

```
root@debian:/home/sarah/Téléchargements# apt-get install phpmyadmin
```

Figure 2.4 : Installation de PhpMyAdmin

✓ Une fois les paquets sont téléchargés , nous allons passer à l'étape de configuration :

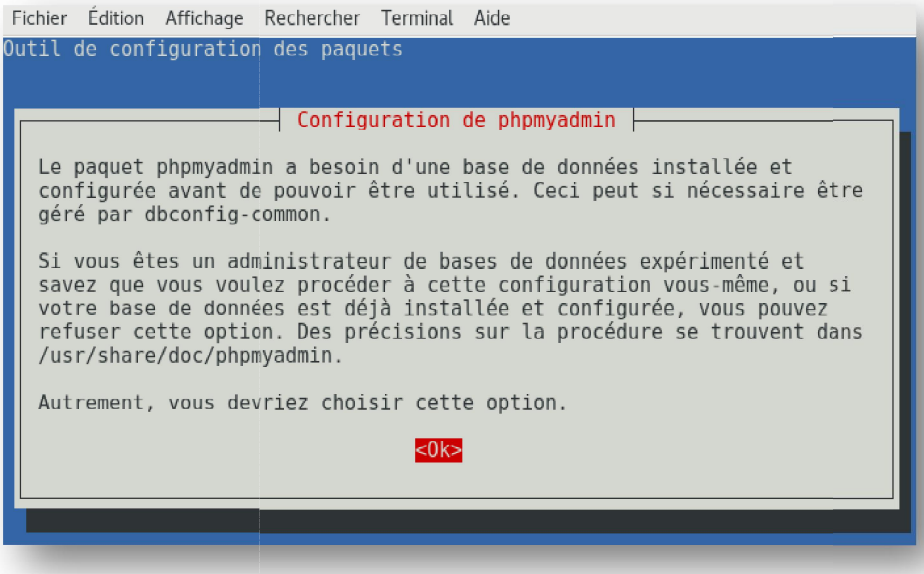

Figure 2.5 : *Configuration de phpMyAdmin*

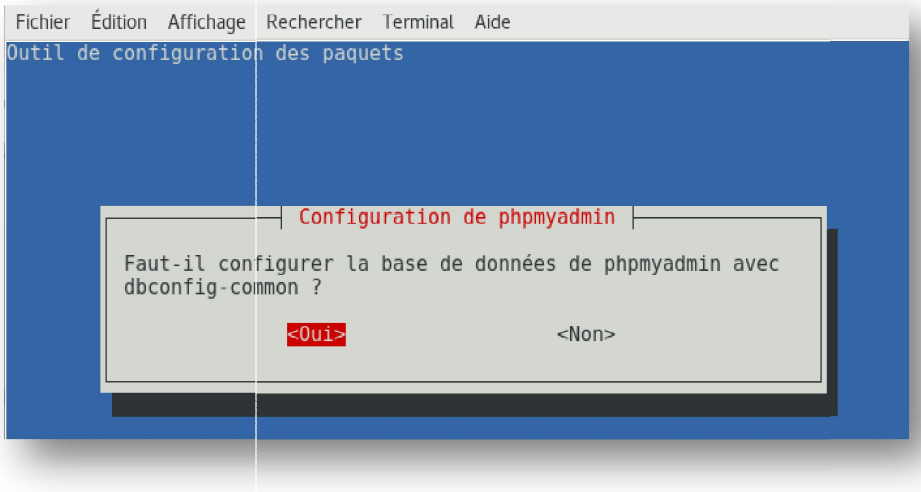

Figure 2.6: *Configuration de base de données de phpMyAdmin*

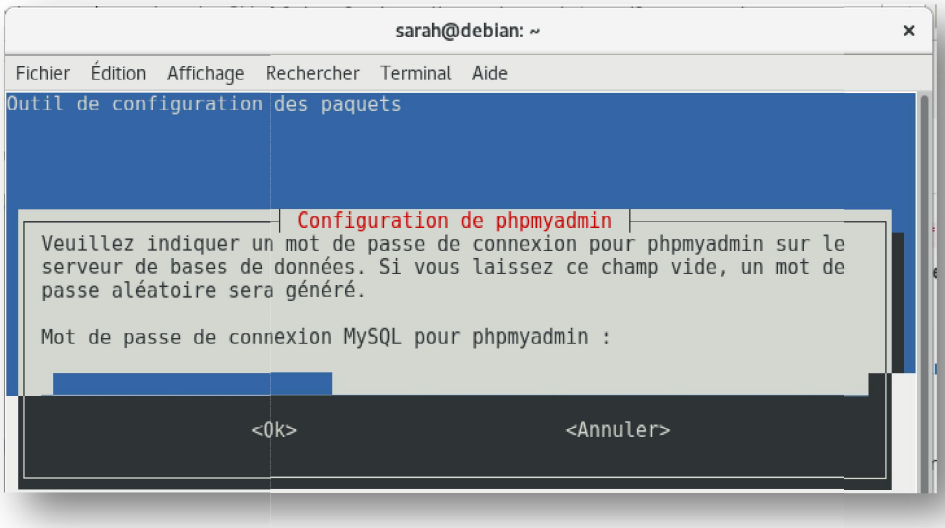

Figure 2.7: *Insertion du mot de passe*

✓ Enfin, une page d'accueil apparait ce qui veut dire que phpMyAdmin est installé.

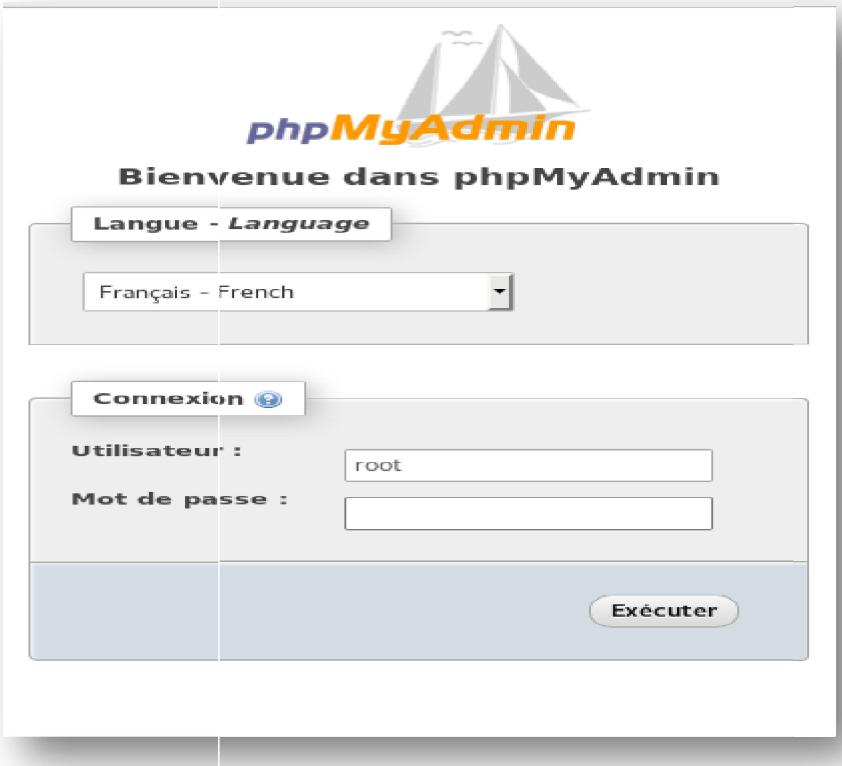

Figure 2.8 : *Page d'accueil*

✓ Les dépendances d'OwnCloud ; MySQL, apache2 et phpMyAdmin sont installés, on passe donc à l'installation d'OwnCloud elle-même.

2.3.4. Installation de OwnCloud

D'abord nous devons télécharger l'application OwnCloud depuis le site officiel et pour se connecter à ce serveur , il suffit d'avoir un navigateur Web et se rendre sur l'adresse du serveur , dans notre cas l'adresse est localhost /owncloud et saisir notre nom d'utilisateur et le mot de passe.

OwnCloud peut être utilisé avec n'importe quel navigateur Web moderne.

- Mozilla Firefox > version 14
- Chrome > version 18
- Safari > version 5
- Internet Explorer > version 11

Pour installer OwnCloud à partir des lignes de commandes, nous devons en premier lieu télécharger la dernière version ensuite décompresser l'archive dans le répertoire approprié par la commande « tar jxf owncloud-10.0.8.tar.bz2 », le contenu sera décompresser dans un unique répertoire :

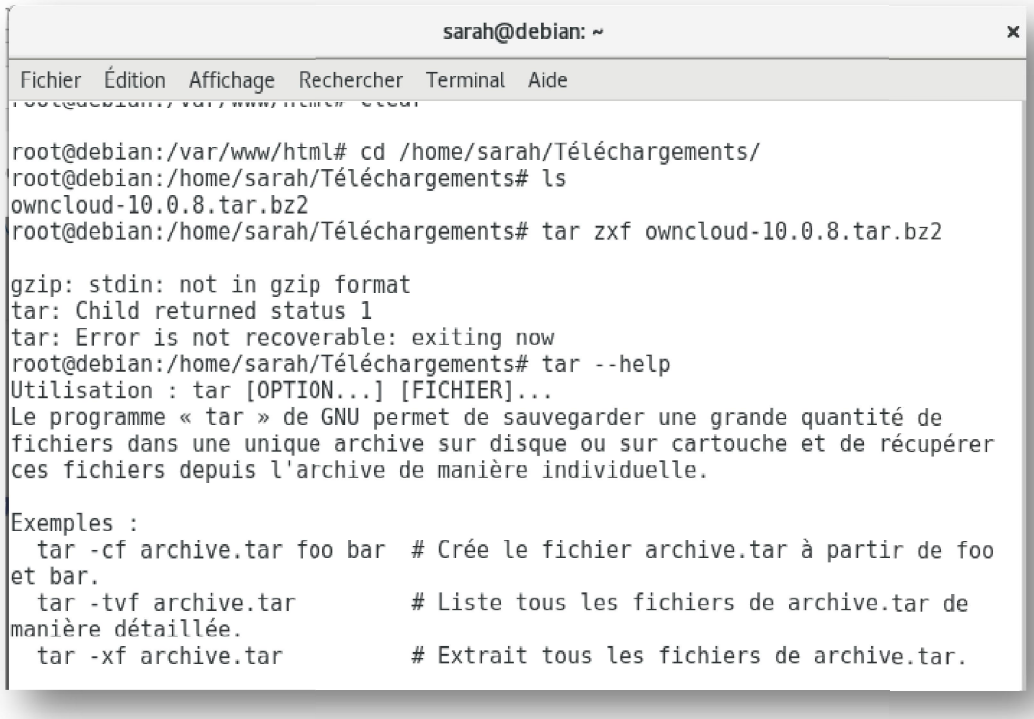

Figure 2.9 : *Téléchargements et décompressions*

Nous avons supprimé le fichier OwnCloud déjà existant et nous l'avons copié vers sa destination finale « var/www/html » ; car sur certain serveurs http, il est recommandé d'installer Owncloud en dehors de la racine document :

```
root@debian:/var/www/html# cp -R /home/sarah/Téléchargements/owncloud /var/www/html/
```

Figure 2.10 :*Les commande nécessaire pour effectuer l'opération*

Nous avons changer les droits d'accés :

```
root@debian:/home/sarah# chown -R www-data:www-data /var/www/html/owncloud/
```

Figure 2.11 : *Installation de OwnCloud*

L'installation du serveur est maintenant terminée. Nous pouvons nous rendre sur l'interface web de Owncloud pour terminer sa configuration.

Pour cela, nous utilisons un navigateur internet et nous allons sur l'URL de notre serveur. L'URL est localhost/owncloud.

✓ Une fois nous sommes sur cette page de configuration, nous aurons quelques champs à remplir.

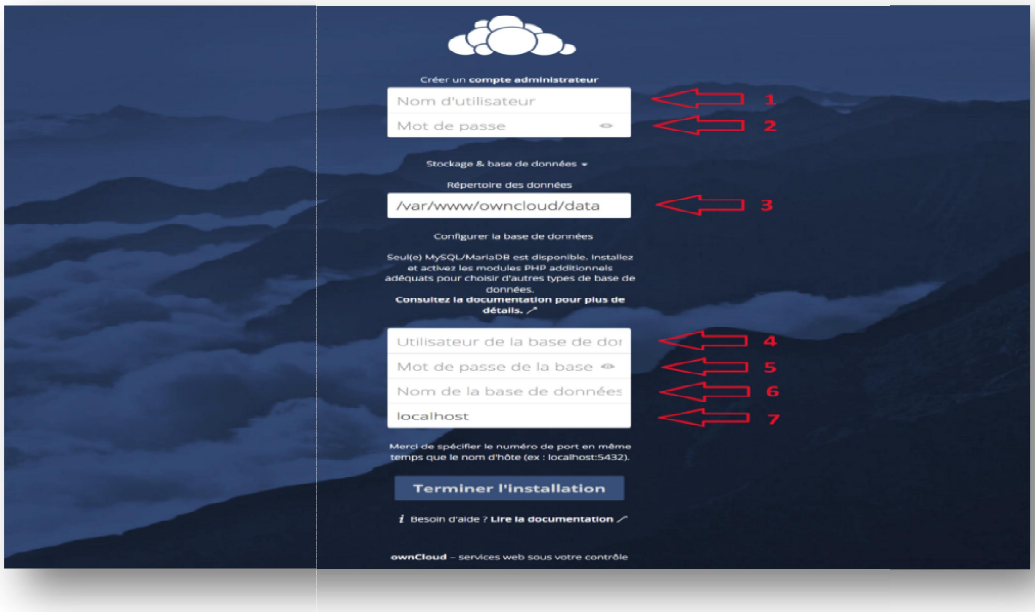

Figure 2.12 : *Les champs à remplir*

Les champs numérotés dans la figure 2.12 sont données comme suit :

1 : Ce champ correspond au nom de l'utilisateur administrateur de OwnCloud.

2 : Mot de passe de l'administrateur.

3 : Répertoire où seront stockés les fichiers partagés sur OwnCloud. Ce répertoire devra disposer des droits adéquats en lecture et écriture pour permettre à notre serveur de fonctionner.

4 : Nom d'utilisateur que le serveur Owncloud utilisera pour accéder à la base de données. Cet utilisateur doit disposer de droits avancés.

5 : Mot de passe de l'utilisateur de la base de données.

6 : Nom de la base de données destiné à ownCloud.

7 : Adresse IP ou localhost de notre serveur de base de données. Comme notre base de données est installée sur la même machine que notre serveur OwnCloud, localhost est parfaitement adapté.

Nous avons créé un compte administrateur en saisissant notre identifiant ainsi que son mot de passe. Le répertoire des données (déjà renseigné) est : « var/www/html /ownCloud/data ».

- ✓ Ensuite, nous avons choisi MySQL comme base de données, nous avons rempli les champs comme suit :

  A : Nom de la base de données : « OwnCloud » et son mot de passe.

  B : Serveur : localhost.

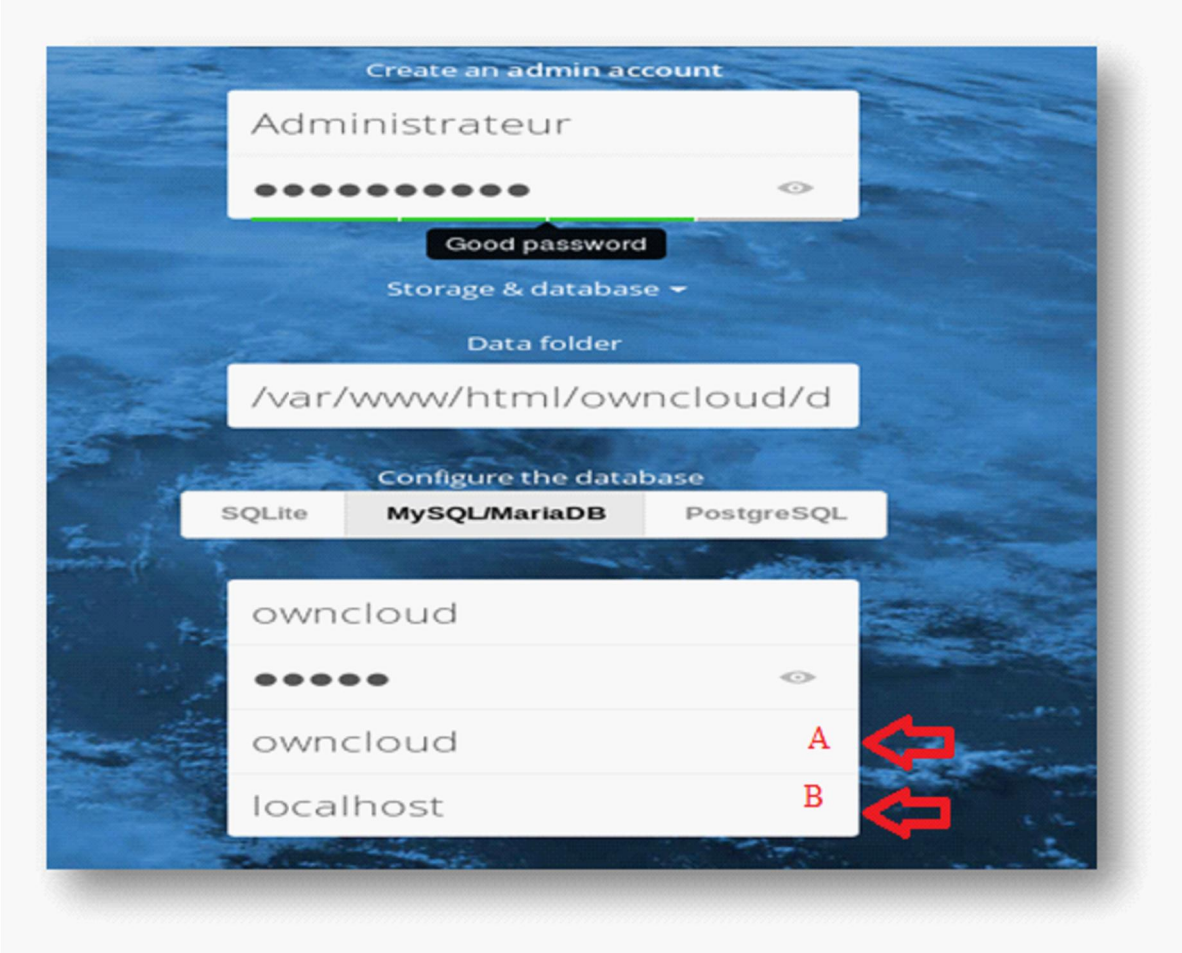

Figure 2.13 : *Création d'un administrateur*

✓ Par la suite, nous remarquons qu'il faut modifier les droits d'accès pour l'administrateur :

Figure 2.14 : *Apparition d'un problème d'accès*

✓ La commande suivante permet au service apache d'avoir le droit d'écriture et de lecture dans le dossier data :

```
root@debian:/home/sarah/Téléchargements# Chmod 770 /var/www/html/owncloud
```

Figure 2.15 *: Modification des droits d'accès*

✓ Nous pouvons maintenant cliquer sur « Terminer l'installation ».

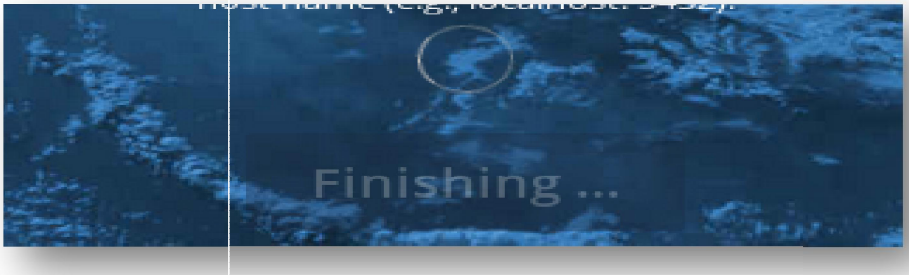

Figure 2.16 *: Fin d'installation*

✓ La page suivante finit par s'ouvrir, donc nous avons terminé l'installation de notre serveur OwnCloud :

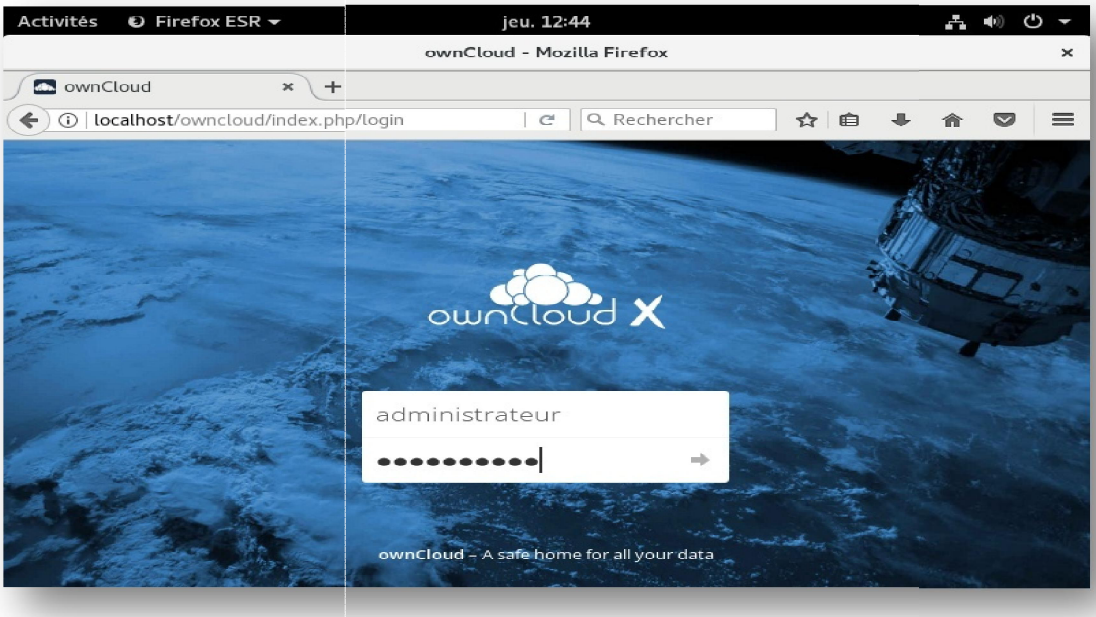

Figure 2.17: *Accès de l'administrateur*

✓ A l'aide des figures suivantes, nous allons expliquer les fonctionnalités que contient cette application.

2.4. Fonctionnalités de OwnCloud

✓ Cette fenêtre nous permet de naviguer sur l'interface Web de OwnCloud, elle s'ouvre par défaut sur la page'' *fichiers'',* sur cette page nous pouvons ajouter, supprimer et partager des fichiers, et plus généralement opérer des changements en fonction des privilèges que l'administrateur du serveur nous a attribués.

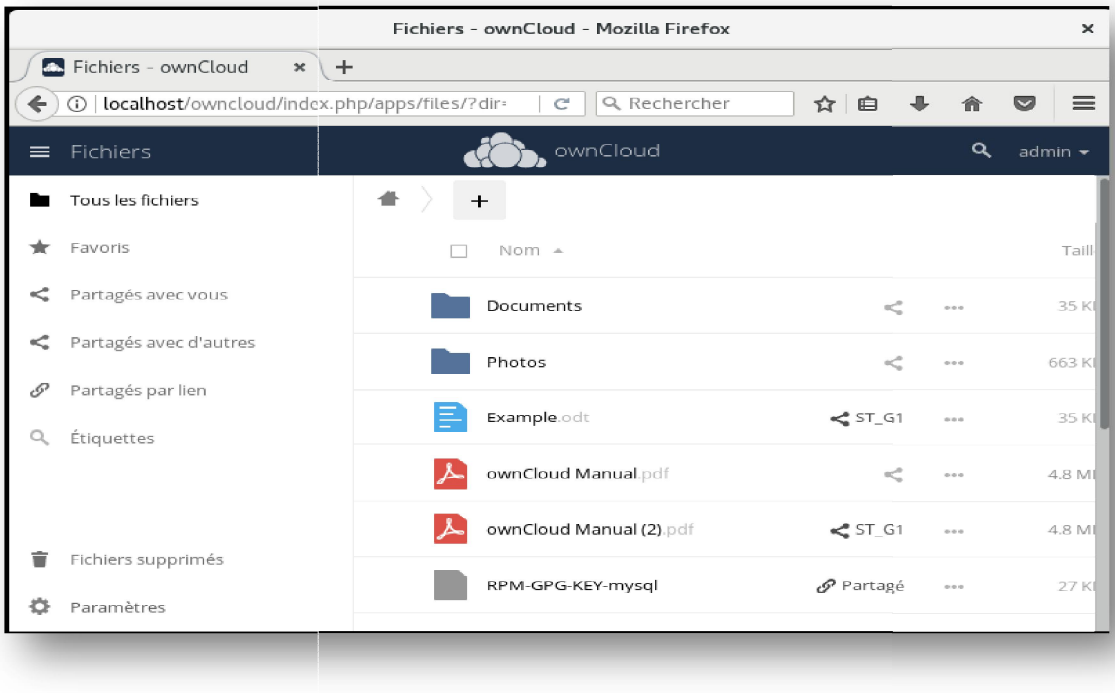

Figure 2.18 : *Fonctionnalités de OwnCloud*

✓ Existence de quelques options importantes pour un ficher comme : détail, renommer, télécharger et supprimer.

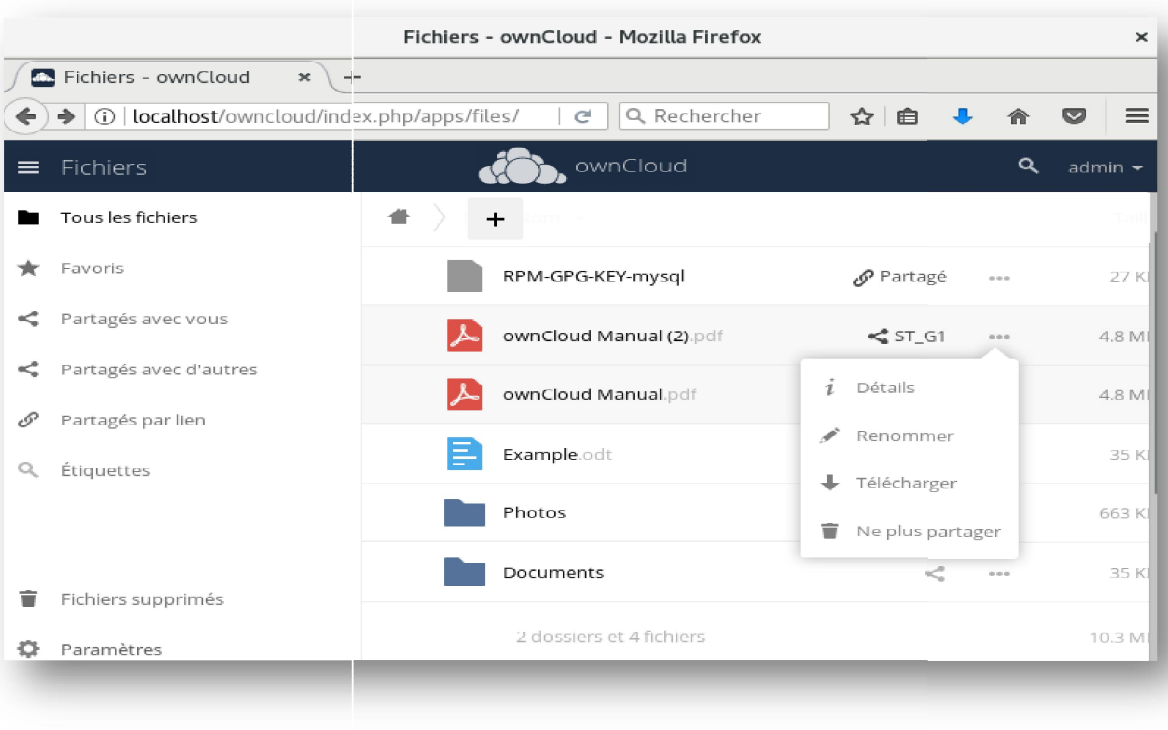

Figure 2.19 : *Options sur les fichiers*

✓ Une autre fenêtre en haut à droite pour plus de paramètres, ajout d'utilisateurs, obtenir de l'aide et en fin une case pour se déconnecter.

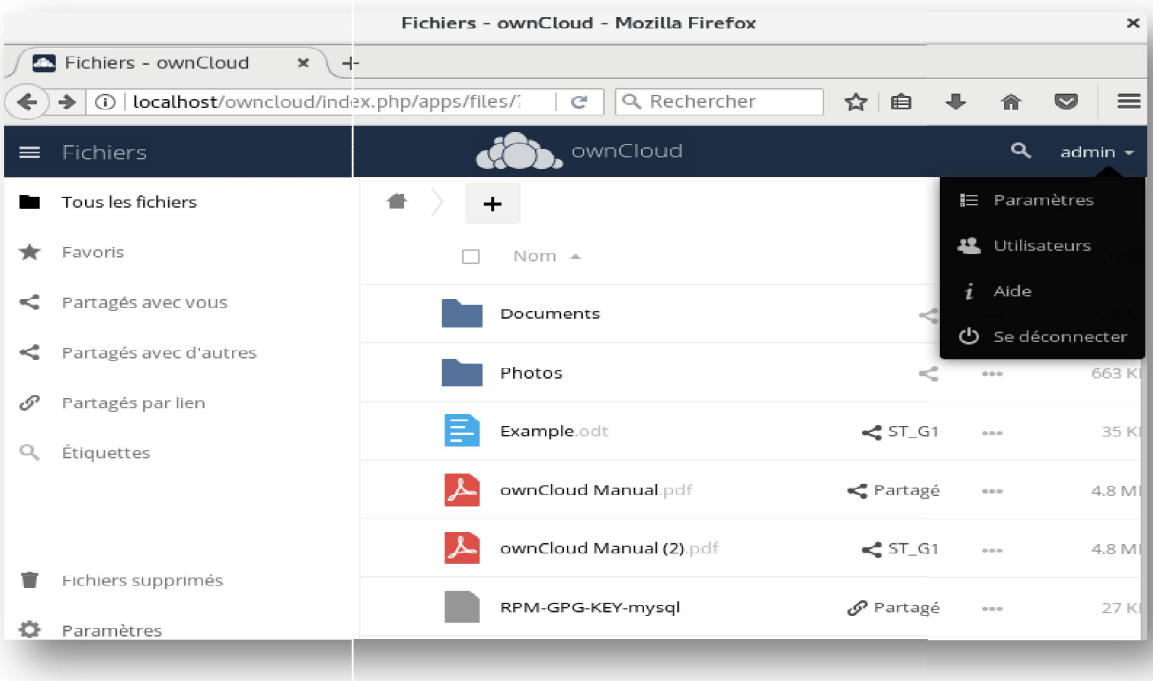

Figure 2.20 : *Fenêtre des paramètres*

✓ Création des utilisateurs et des groupes avec leurs mots de passe en cliquant sur « créer » :

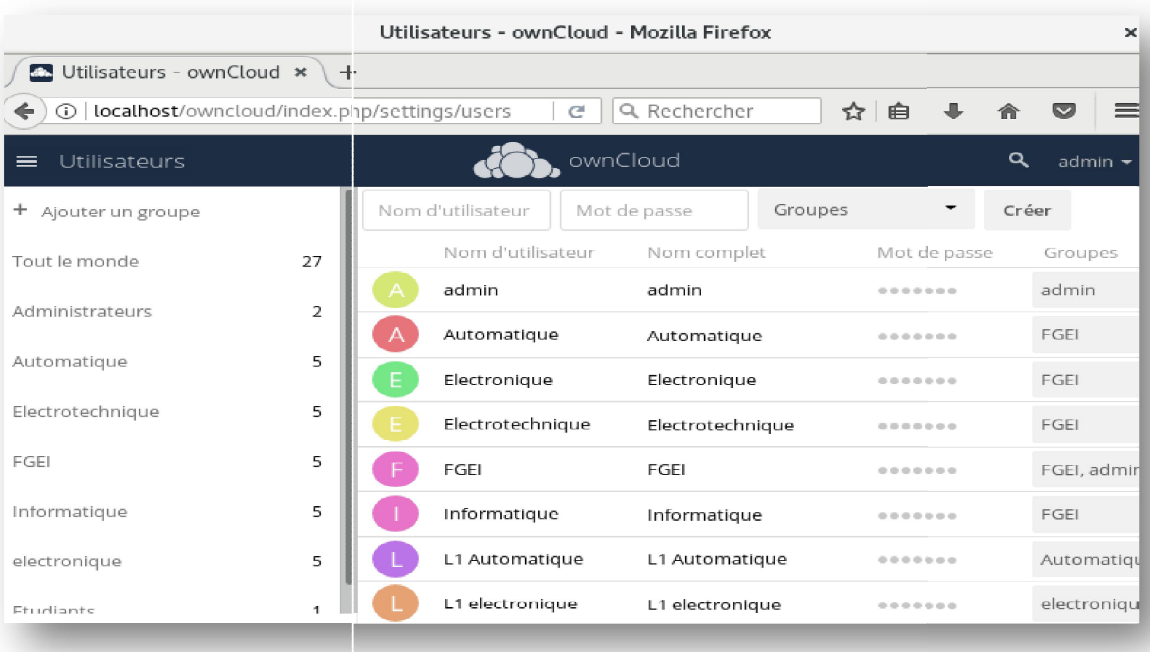

Figure 2.21 : *Création des utilisateurs et des groupes*

➢ Voici un exemple de partage d'un fichier entre l'administrateur et un utilisateur « L2 Automatique », cet utilisateur pourra accéder à distance à ce fichier via son compte. Il pourra le lire, le partager, le modifier …etc, selon les droits qui lui sont attribués par l'administrateur :

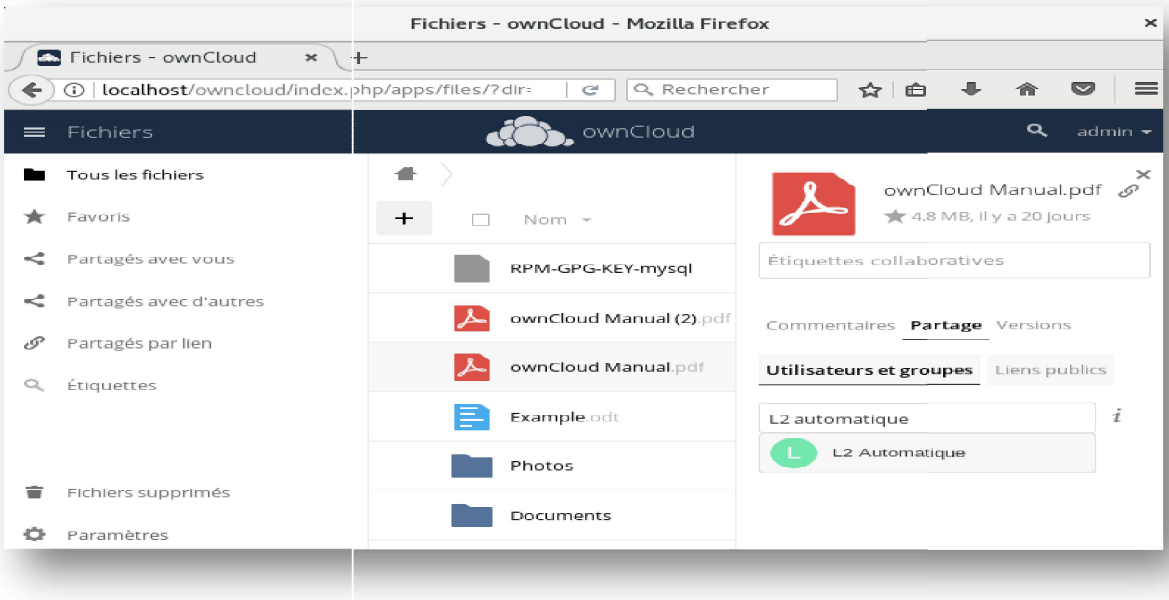

Figure 2.22 : *Partage d'un fichier*

✓ Toutes fois un utilisateur qui ne possède pas un compte peut accéder à des fichiers à partir des liens qu'on appel des « liens publiques »

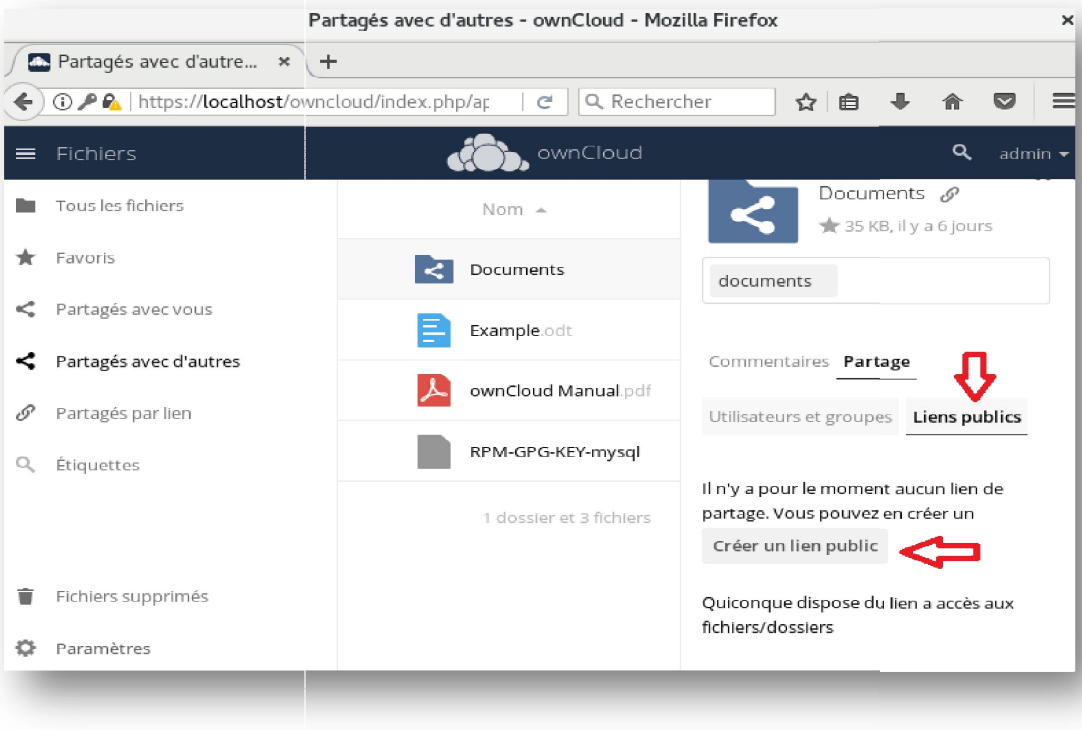

Figure 2.23: *Partage d'un lien publique*

✓ Aussi l'administrateur réseau peut attribuer aux fichiers un mot de passe, ainsi une date d'expiration, une fois on a dépassé la date le fichier va disparaitre.

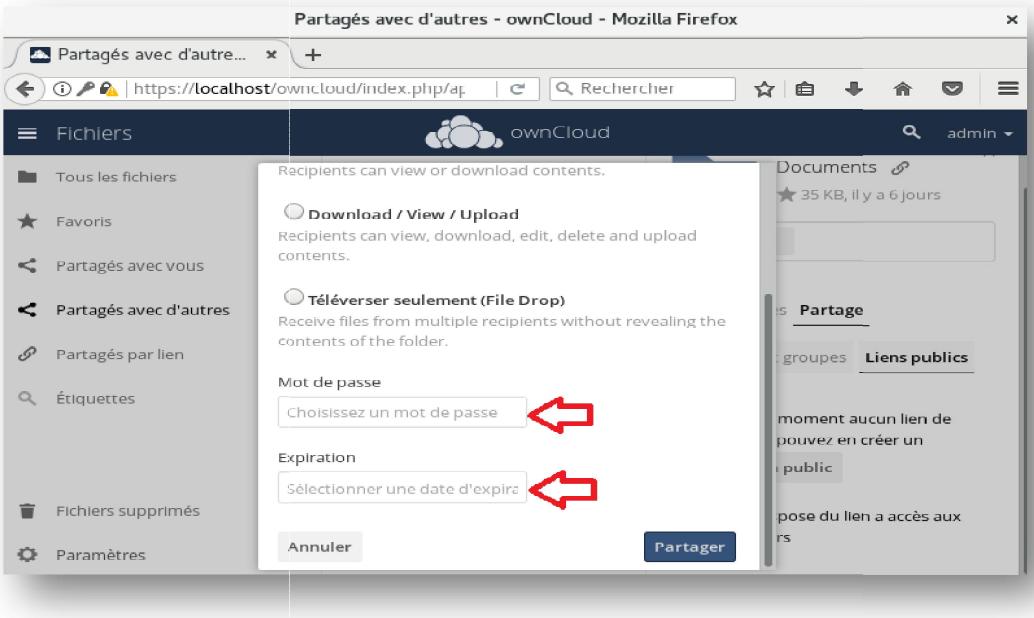

Figure 2.24 : *Mot de passe et date d'expiration du fichier à partager*

✓ L'administrateur du réseau peut donner à l'utilisateur différent droit d'accès comme le téléchargement, la lecture, … etc

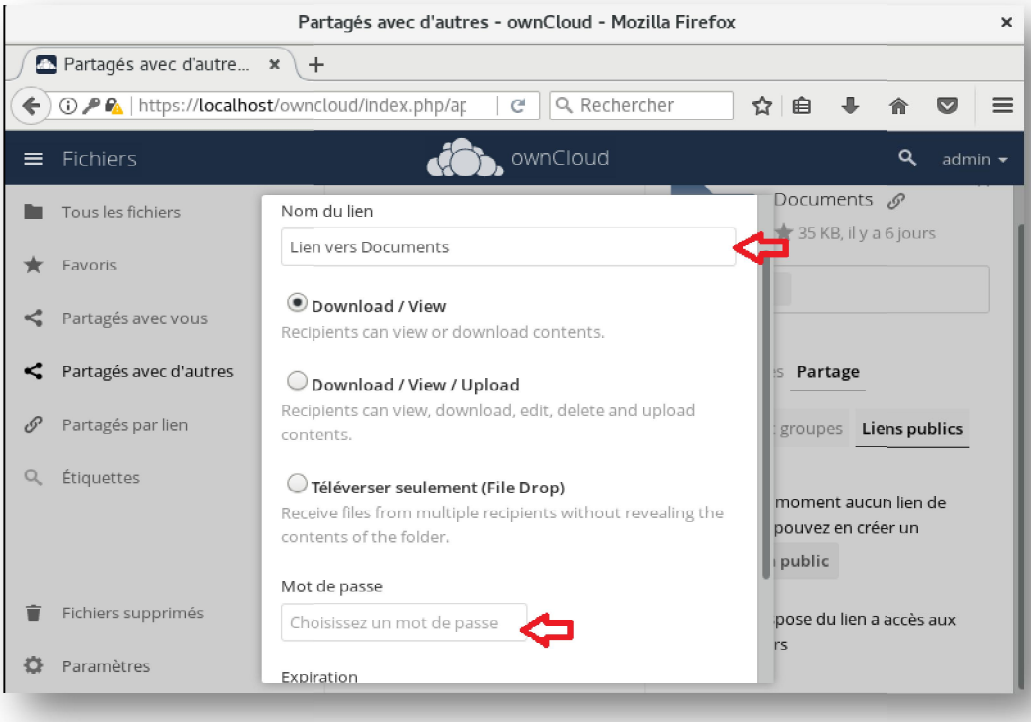

Figure 2.25 : *Attribution de droits d'accès à l'utilisateur*

✓ Sur OwnCloud l'administrateur peut décider d'installer des applications supplémentaires comme l'antivirus, la gestion des contacts et des agendas, etc. a partir de l'icône « Market » :

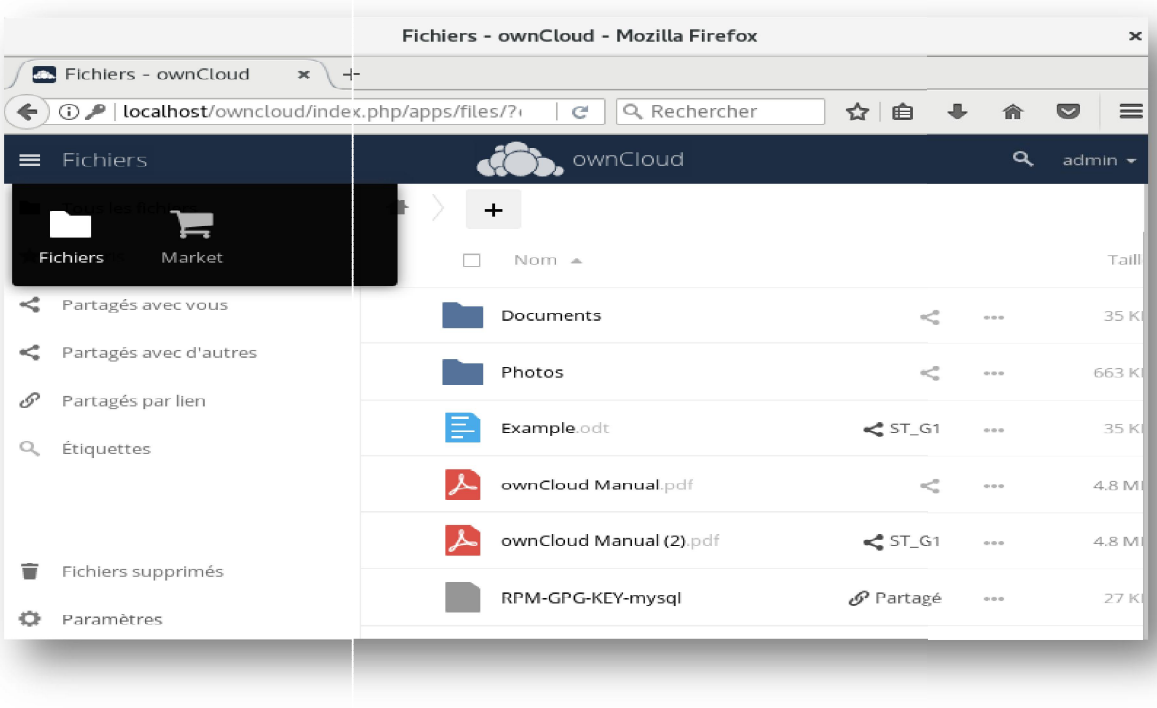

Figure 2.26 : *Existence de l'icone market*

✓ En cliquant sur l'icône marché on peut choisir la catégorie des applications qu'on désir télécharger

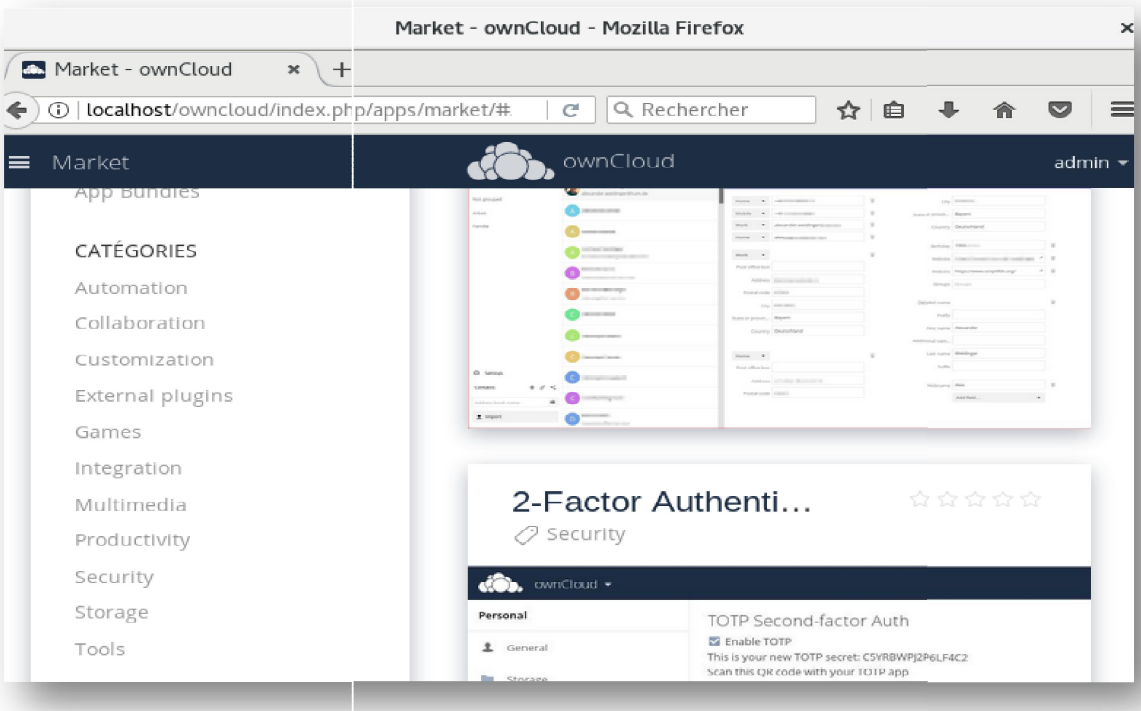

Figure 2.27 : *Catégories des applications*

2.5. Sauvegarde de données

La sauvegarde informatique ou backup consiste à réaliser une copie de données, les cloner, les compresser, les chiffrer et les conserver en toute sécurité dans un espace de stockage. Il est important d'adapter les solutions de sauvegarde qui répondent aux besoins de notre entreprise, le choix est lié au volume d'informations à stocker et aussi à la taille de l'entreprise.

Généralement, une copie de sauvegarde est hébergée sur un serveur distant de backup, un disque de sauvegarde, un périphérique de stockage comme des disques durs externes, des solutions comme Dropbox, Google Drive ou directement dans le cloud.

La sauvegarde s'applique aux données actives comme les fichiers sur lesquels nous travaillons au quotidien, et non pas aux données inactives comme des données figées :

- Bases de données, fichiers clients, documents de travail
- Historiques et écritures comptables
- Données stratégiques liées au développement de l'entreprise
- Communications importantes (e-mail, mémos, etc.)
- Données sensibles protégées par chiffrement et cryptage

La sauvegarde des données préserve l'activité de l'entreprise, notamment en cas de défaillance du système informatique.

L'entreprise peut faire face à plusieurs types de risques qui mettent en danger ses données, nous citons :

- ***Risques humains :*** la perte ou le vol d'un appareil dont les données sont liées à celles de l'entreprise, une mauvaise manipulation entraînant l'effacement de données sensibles, piratage des données...
- ***Risques liés à l'environnement :*** perte de données suite à des catastrophes naturelles (incendies, inondations...) dans les locaux de l'entreprise.
- ***Risques liés aux dysfonctionnements matériels :*** une panne d'un serveur par exemple. En cas de pertes de données, l'impact financier peut être notable pour l'entreprise en raison de la disparition de fichiers ou d'applications sensibles (base de données clients, rapports financiers, etc.), ou de la perte de temps engendrée par la remise en ligne de ces données.

C'est pourquoi on met en place une stratégie de sauvegarde au sein du réseau de l'entreprise 2INT Partners.

✓ Le stockage de données peut s'effectuer sur différents supports locaux ou externes :

2.5.1. Supports locaux de sauvegarde

Cette solution de backup est efficace en cas de panne du disque dur source ou de suppression accidentelle. La sauvegarde en local peut se faire sur des supports tel que :

- ***Disque interne :*** dossier local, un autre disque dur du même ordinateur ;
- ***Périphériques de stockages :*** clé USB, disque dur externe, CD, DVD ;
- ***Serveur dédié :*** sauvegarde sur un serveur dédié, connecté sur le réseau de l'entreprise ;
- ***NAS :*** disque dur ou ensemble de disques durs accessible via le réseau de l'entreprise ;

2.5.2. Supports de sauvegarde externes

L'utilisation de cette solution de sauvegarde, permet d'éviter une destruction totale de nos données et les sauvegarder en cas d'un risque lié à l'environnement, alors la reprise de notre activité peut se faire plus facilement grâce aux supports suivants :

- ***Service de backup distant ou dans le Cloud :*** le Cloud désigne l'ensemble des solutions de stockage distant par l'intermédiaire d'un réseau, généralement Internet ; et le service de backup distant désigne une solution de sauvegarde automatique et garantie une restauration rapide et complète de nos données.
- ***Export FTP*** *:* envoi manuel de la sauvegarde sur un serveur distant
- ***NAS hébergé :*** dans un Datacenter répondant à des normes de sécurité élevées.

Voici les types de sauvegardes existants :

➢ ***La sauvegarde totale automatique :*** c'est la solution de sauvegarde la plus simple à mettre en place. Nous pouvons pour cela nous tourner vers un logiciel de sauvegarde gratuit.

- ***La sauvegarde différentielle :*** il permet de ne sauvegarder que les fichiers qui ont été modifiés ou ajoutés depuis la dernière sauvegarde complète en date.

- ***La sauvegarde incrémentale :*** la sauvegarde incrémentale permet de ne sauvegarder que les fichiers modifiés depuis la dernière sauvegarde, mais elle a la particularité de conserver les différentes versions d'un fichier.

2.5.3. Quelques critères de sauvegarde

Vitesse de sauvegarde : plus le volume de données et le nombre d'utilisateurs est important, plus la vitesse de sauvegarde est cruciale, ceci afin de minimiser les pertes d'information au de-là de dix utilisateurs, il est préférable d'opter pour un système de sauvegarde automatique par exemple les serveurs.

Fiabilité du support et facilité d'utilisation : la durée de vie du matériel doit être à la hauteur de l'investissement, un matériel couteux doit être pérenne.Il est important de vérifier le mode de classement des données sur le support de sauvegarde pour une restauration rapide.

Enfin, la gestion et l'administration de notre support de sauvegarde doivent être simples.

Sécurité : les données sauvegardées doivent être cryptées afin d'empêcher une tierce personne à accéder à des données confidentielles.

Compatibilité à l'environnement : certain système physiques (disque dur externe, lecture sur bande) sont particulièrement fragile (chaleur, poussière, choque…)

Compatibilité : on doit vérifier si la solution de sauvegarde supporte Windows, Apple et Linux car notre parc informatique peut évoluer.

2.6. Choix d'une solution de sauvegarde

Tableau 2.3: *Avantages et inconvénients des applications proposées*

Applications	Avantages	Inconvénients
Duplicati	• Cette application est disponible pour	• Stockage des données sous

	Windows et Linux et elle est gratuite elle comporte : • Chiffrement fort : Duplicati utilise un fort cryptage AES 256 pour protéger nos sauvegardes. • Sauvegarde incrémentales : elle effectue une sauvegarde complète au départ ; Par la suite, Duplicati met à jour la sauvegarde initiale en ajoutant uniquement les données modifiées. • Compression : toutes les données de sauvegarde sont compressées avant d'être cryptées et téléchargées. • Planificateur : il est intégré pour exécuter nos sauvegardes automatiquement aux heurs et aux intervalles que nous définissons. • Mise à jour automatique : Duplicati est livré	format zip : c'est-à-dire ils ne sont pas directement exploitables.

	avec un programme de mise à jour intégré qui télécharge et installe la dernière version disponible pour nous. De cette façon, nous pouvons facilement garder Duplicati à jour.	
Sbackup 	• Crée des sauvegardes compressées et non compressées. • Prend en charge plusieurs profils de sauvegarde. • Permet la journalisation, les notifications par email. • Sauvegarde planifiées et sauvegarde manuelles. • Nous divisons les sauvegardes non compressées en plusieurs blocs. • Prend en charge la sauvegarde locale et distante.	• Sauvegardes manuelles : donc cette application nécessite toujours une intervention humaine.
Online Backup	• Sauvegarde automatique, incrémentale et restauration des	• Manque de sécurité : il s'agit d'une application en

	données.	ligne ce qui signifie que les pirates peuvent détecter des failles quelque part dans le site pour intercepter nos données. • Logiciel payant : 15euro/ mois / utilisateur.

Duplicati est un logiciel libre (open source), livré avec un programme de mise à jour automatique ainsi qu'un haut niveau de sécurité des données qui sont cryptées à l'aide d'un logiciel de chiffrement « AES » très performant, contrairement au logiciel payant « online backup » celui-ci est moins sécurisé car il permet d'effectuer des sauvegardes en ligne, pour cette raison il est plus au moins vulnérable, donc nos données personnelles peuvent être intercepter par un hacker.

De plus, l'application Duplicati permet d'effectuer des sauvegardes des données de type incrémentales, bien qu'elle se dispose d'un planificateur qui exécute automatiquement les sauvegardes selon des intervalles que nous lui définissons, par contre le logiciel sbackup nécessite toujours une intervention humaine pour effectuer une sauvegarde manuelle.

L'infrastructure de l'école nécessite une mise en place d'une véritable stratégie de sauvegarde, pour cela nous avons opté à une solution de sauvegarde automatique, gratuite et fiable qui est l'implémentation du logiciel de sauvegarde « Duplicati ».

2.7. Installation du l'application Duplicati

✓ Nous avons téléchargé l'application Duplicati, à partir du site officiel en choisissant la dernière version (Duplicati 2.0.3.6)

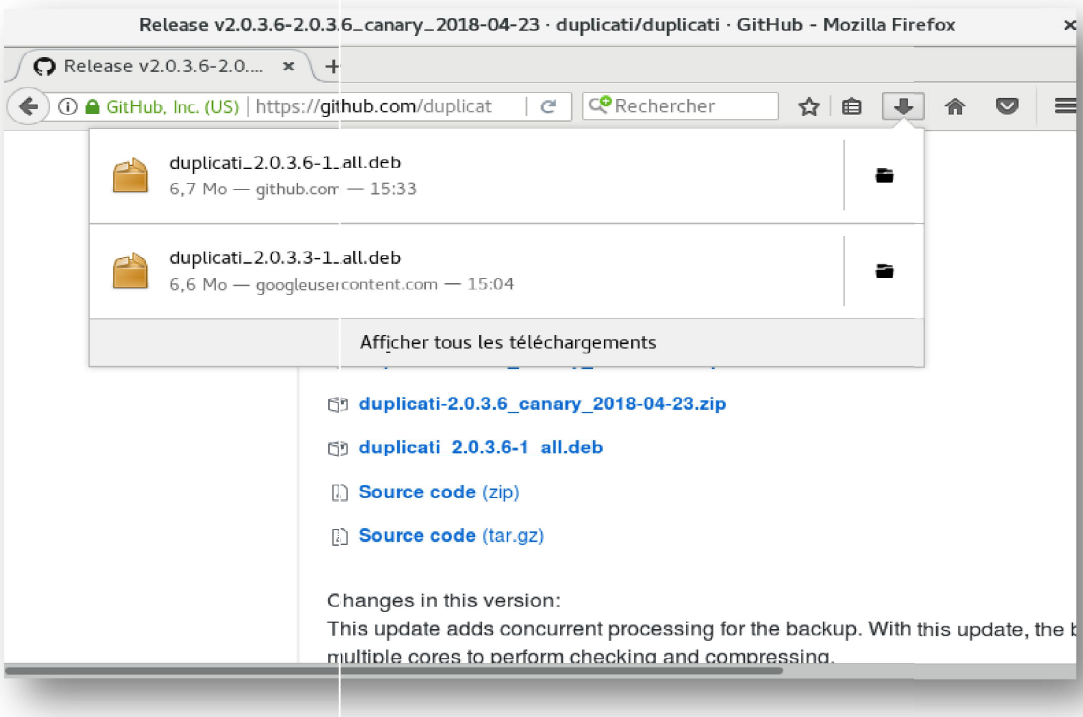

Figure 2.28 : *Téléchargement de Duplicati2.0.3.6*

✓ Nous avons accédé au répertoire « Téléchargement », puis nous allons installer notre application à l'aide de la commande « dpkg » :

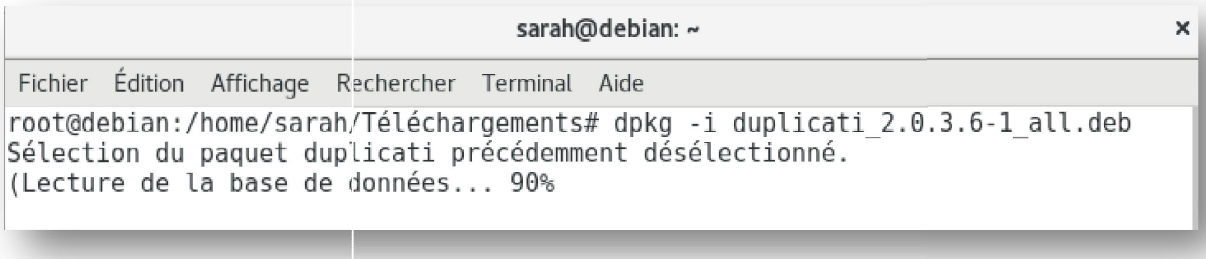

Figure 2.29 : *Installation de Duplicati*

✓ Installation des dépendances manquantes en utilisant la commande apt-get :

Figure 2.30 : *Installation des dépendances manquantes*

✓ Cette étape consiste à démarrer, puis activer le démon au démarrage du système:

```
root@debian:/home/sarah/Téléchargements# systemctl start duplicati.service
root@debian:/home/sarah/Téléchargements# systemctl enable duplicati.service
Created symlink /etc/systemd/system/multi-user.target.wants/duplicati.service →
/lib/systemd/system/duplicati.service.
root@debian:/home/sarah/Téléchargements#
```

Figure 2.31 : *Démarrage et activation de Duplicati*

✓ Nous allons accéder maintenant à Duplicati à partir de l'adresse localhost:8200 de notre machine.

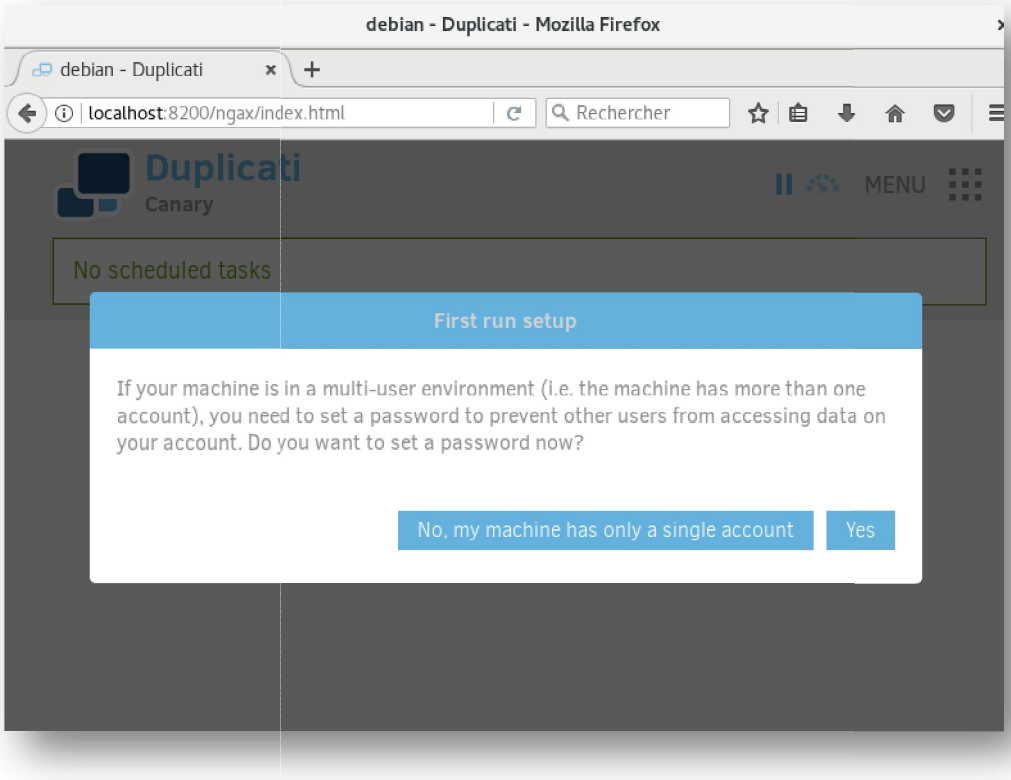

Figure 2.32 : *Configuration de l'application*

✓ Sécurisation de l'application avec un mot de passe :

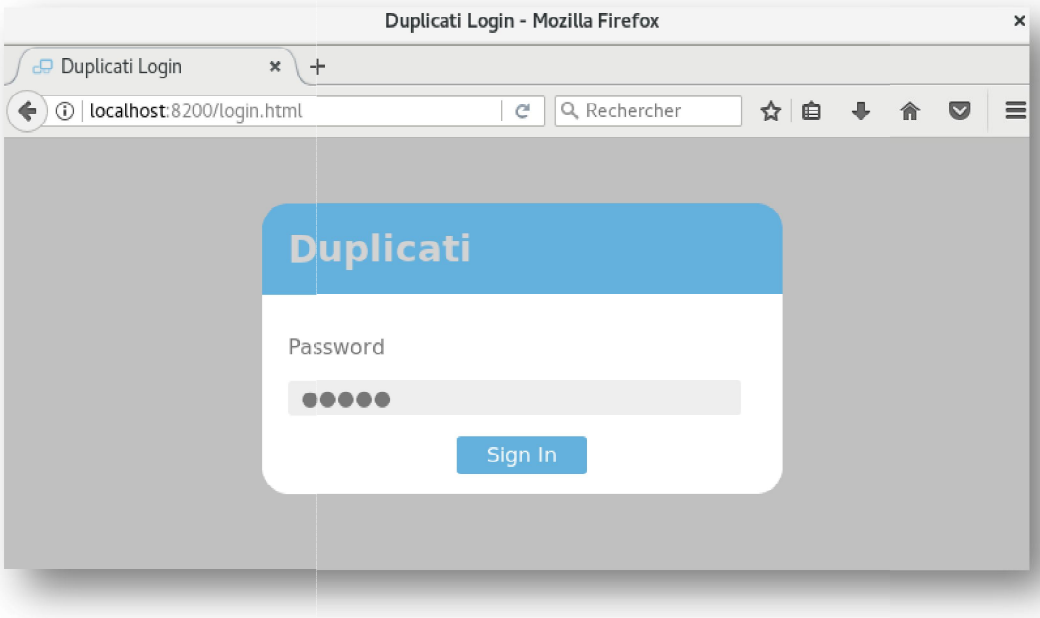

Figure 2.33 : *Création d'un mot de passe*

✓ Le menu à droite nous permet d'ajouter : des sauvegardes, restaurations ou bien déconnecter de l'application. En accédant aux paramètres nous aurons d'autres fonctionnalités comme le changement de la langue de l'interface utilisateur.

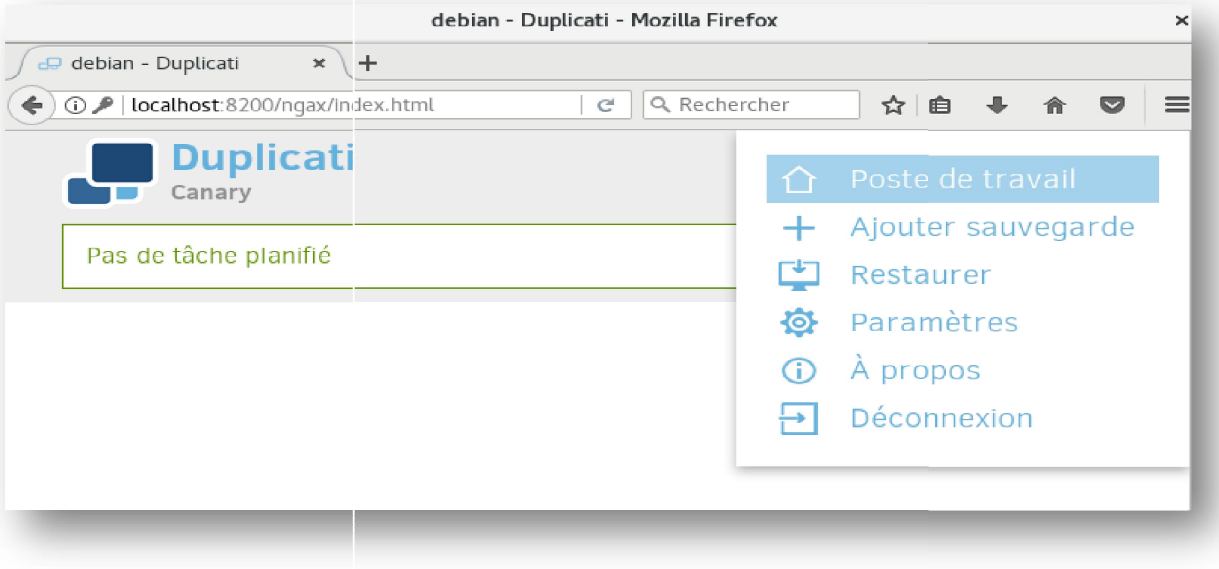

Figure 2.34 : *Fonctionnalités sur Duplicati*

✓ Pour créer un backup avec Duplicati, nous choisissons le menu Ajouter une sauvegarde, puis Configurer une nouvelle sauvegarde.

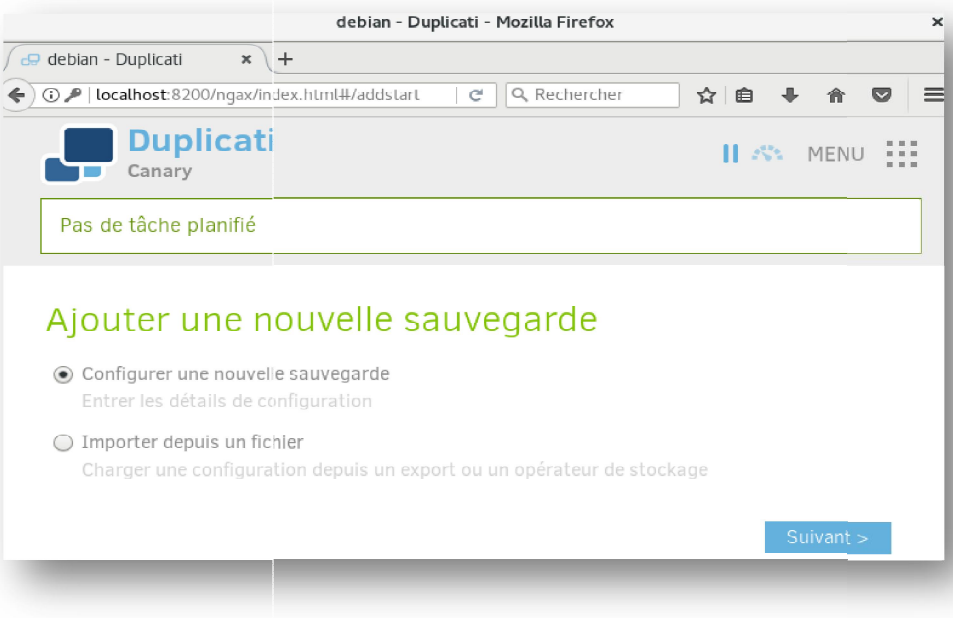

Figure 2.35 : *Création d'un backup*

✓ Nous choisissons un nom pour le backup, le type de chiffrement, puis une phrase sécrète pour le chiffrement.

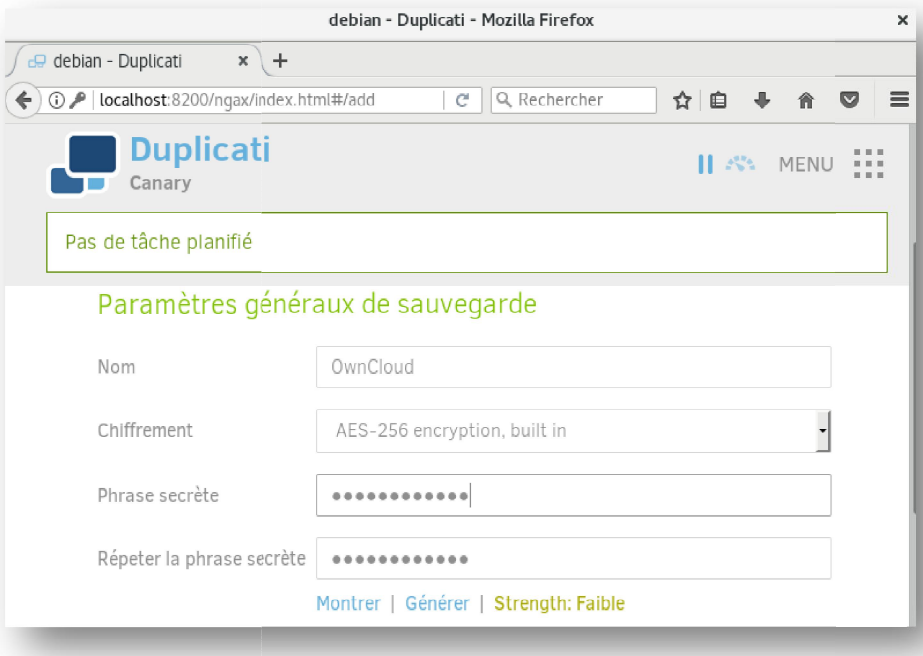

Figure 2.36 : *Paramètres du backup*

✓ Nous allons tester la connexion entre l'application Duplicati et le serveur de stockage par le biais du protocole FTP. Afin de s'assurer que les fichiers seront bien sauvegardés.

➢ Le protocole FTP

C'est un protocole de transfert de fichiers, il permet de faire un transfert de données d'une manière efficace entre deux machines distantes, ce protocole repose sur le modèle client-serveur, la machine cliente envoie des requêtes et le serveur les exécute.

Le protocole FTP est séparé en deux canaux, l'un pour les données et l'autre pour l'administration. Le canal de commande sert à l'échange des commandes entre les deux cotés le serveur et le client qui préparent les transferts des données.

Le serveur FTP utilise le protocole TCP, qui est un protocole de transport garantissant l'acheminement des données jusqu'au destinataire. La session FTP se déroule en quatre étapes :

- Authentification de l'utilisateur.
- Etablissement du canal de contrôle.
- Etablissement du canal de données.
- Fermeture de la connexion.

✓ Nous avons utilisé le serveur vsftpd pour utiliser le protocole FTP en toute sécurité.

➢ Le serveur Vsftpd

C'est un serveur FTP pour les systèmes d'exploitation qui fonctionne sur la plate forme Linux, il possède de nombreuse caractéristiques comme le très haut niveau de sécurité et de la haute vitesse, il est conçu avec la problématique d'une sécurité maximale contrairement aux autres serveurs FTP. Aucune faille majeure de sécurité n'a jamais été décelée dans vsftpd.

✓ La figure suivante nous montre une planification d'une prochaine tâche :

Figure 2.37 : *Planification d'une tâche*

✓ La connexion entre le client vsftpd et Duplicati est fonctionnelle :

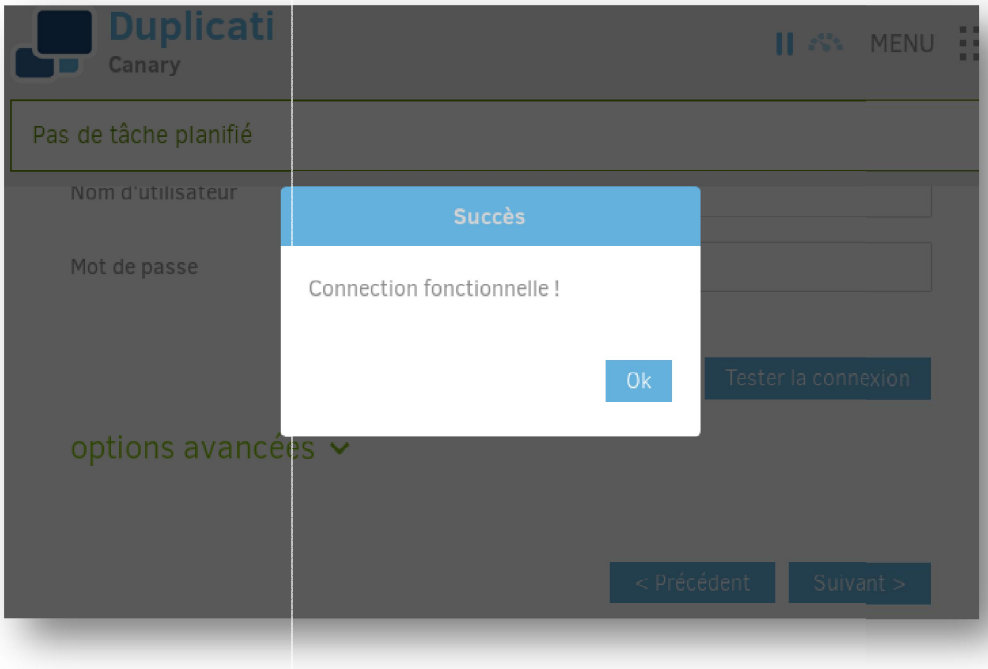

Figure 2.38 : *Teste sur le fonctionnement*

2.8. Discussion

Dans ce chapitre nous avons mis en place deux applications, OwnCLoud qui est une application pour le partage de fichiers et l'application Duplicati pour le stockage, ainsi nous avons proposés une nouvelle architecture réseau en ajoutant ces deux serveurs.

3.1. Préambule

La sécurité du réseau informatique vise généralement à protéger les données essentielles de l'entreprise. Donc, il est nécessaire de mettre en place une stratégie de sécurisation de notre réseau en sécurisant les applications misent en œuvre afin d'empêcher les menaces et les utilisations malveillantes.

3.2. Sécurisation de l'application OwnCloud

Les systèmes informatiques jouent un rôle de plus en plus important dans les sociétés, ils sont mis en place pour le stockage et la gestion des données, il est donc important des les biens sécurisés.

La sécurité des systèmes d'information est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.

3.3. Les objectifs de la sécurité informatique

La sécurité informatique a pour objectifs :

- **La disponibilité**

Garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

- **L'intégrité**

Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

- **La confidentialité**

Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

Dans le cas de notre application de sauvegarde « Duplicati », on utilise un chiffrement très performant AES, ce qui permet de garantir cet objectif.

- **L'authentification**

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

Dans notre cas, chaque utilisateur de Owncloud est identifié par un nom d'utilisateur et un mot de passe.

- **La non-répudiation**

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

3.4. Les types de piratage informatique

Le piratage (Hacking) est une pratique visant à un échange discret d'informations illégales ou personnelles. Cette pratique, établie par les hackers, le hacking peut se définir également comme un ensemble de techniques permettant d'exploiter les failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

✓ Il existe plusieurs types de pirates informatiques, on peut citer**[4]** :

3.4.1. Le hacker au chapeau blanc (White Hat Hacker)

Il s'agit souvent d'une personne qui a atteint une maturité d'esprit ainsi que des qualifications suffisante et approuvées par les autres.

Il aide les victimes, il aide à sécuriser les systèmes et combat contre la cybercriminalité, ce hacker au chapeau blanc est également le hacker éthique dont on parlera souvent, son slogan est « apprendre l'attaque pour mieux se défendre » et non pas pour causer des dommages.

3.4.2. Le hacker au chapeau noir (Black Hat Hacker)

Le hacker au chapeau noir peut être aussi expérimenté que celui au chapeau blanc, voir plus. Mais il agit par contre à des fins qui lui son propre, et qui sont illégaux. Il vole des données, il s'introduit illégalement dans les systèmes encore pirate des comptes.

3.4.3. Le hacker au chapeau gris (Grey Hat Hacker)

C'est un mélange de White Hat et Black Hat, ce hacker agit des fois pour la bonne cause, comme un White Hat le fait, mais peut commettre de temps en temps des délits.

Il s'introduit illégalement dans un système afin d'en prévenir ensuite les responsables des failles qu'il aura trouvées. Son action est louable, mais tout de même illégale.

3.4.4. Les hacktivistes

Ils agissent pour une cause souvent politique, ils attaquent généralement des entreprises et non pas des utilisateurs particuliers.

3.4.5. Les script-kiddies

Ils sont tous ces jeunes hommes qui sont loin d'avoir compris les grands principes du hacking et l'éthique du hacker, ils se servent des programmes tout faits pour causer des dommages qui peuvent être très gênants.

3.5. Les types de menaces

Les menaces sont classées en deux catégories :

3.5.1. Les menaces passives

Elles consistent essentiellement à copier ou à écouter l'information contenue dans un système. Ces attaques nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie ne cherche pas à altérer cette information ou le système.
Ce type de menace est difficile à détecter.

3.5.2. Les menaces actives

Elles nuisent à l'intégrité des données. Dans ce cas, l'intégrité ou l'existence même du système est menacé.

- Les menaces dues aux accidents représentent 26% des menaces .Elles sont le fait d'incendies, de panes d'équipements ou du réseau, défaut de qualité.
- 17% des menaces sont dues aux erreurs d'utilisation.
- 57% sont dues à la malveillance dont 80% sont d'origines interne.

Elles concernent les actes tels que :

Vol d'équipement, intrusions, écoute du réseau, attaque logique (virus, modification, …).

3.6. Les types d'attaques informatiques

Les hackers utilisent plusieurs techniques d'attaques, elles peuvent être regroupées en trois familles différentes :

3.6.1. Les attaques directes

C'est la plus simple des attaques, le hacker attaque directement sa victime à partir de son ordinateur, le grand nombre de logiciels de ce type de hacking envoient directement les paquets à la victime.

Dans ce type d'attaque il y a de grandes chances pour que nous puissions remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant. [6]

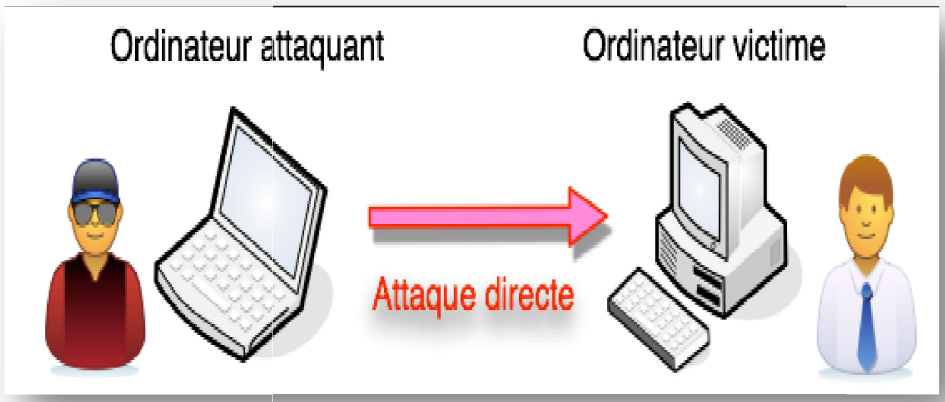

Figure 3.1: *Attaque directe*

3.6.2. Les attaques indirectes par rebond

Son principe est simple les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

Elles permettent de masquer l'identité (l'adresse IP) du hacker, ainsi utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant pour attaquer.

Si on y victime de ce genre d'attaque, il n'est pas facile de remonter à la source .Au plus simple nous remontrons à l'ordinateur intermédiaire. [6]

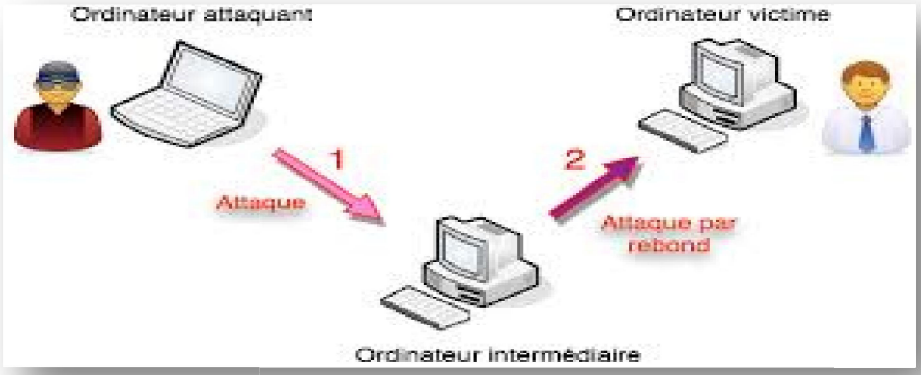

Figure 3.2 : *Attaque par rebond*

3.6.3. Les attaques indirectes par réponse

Cette attaque est une dérivée de la précédente, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinatrice victime.

Là aussi ; il n'est pas aisé de remonter à la source. [6]

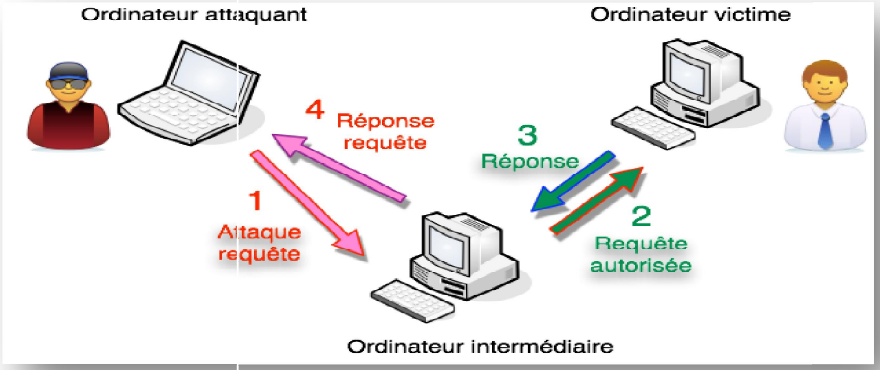

Figure 3.3 : *Attaque par réponse*

3.7. Les attaques les plus utilisées

- **Le cheval de Troie**

C'est un programme informatique malveillant parfois destructeur. Il est souvent porté par un logiciel sous licence et protégé, modifié par des hackers pour en faire cadeau à la communauté numérique. .[5]

- **Le virus**

C'est un programme malveillant conçu pour se propager à d'autres ordinateurs (équipements) en s'insérant dans des logiciels légitimes.[5]

- **Les vers informatiques**

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. [5]

- **Un spyware**

Logiciel espion qui s'installe sur un ordinateur, dans le but de collecter et transférer des Informations sans que l'utilisateur en ait connaissance. [5]

- **Le déni de service (attaque DOS)**

Le principe de cette attaque consiste à envoyer des paquets IP ou de données de taille ou de constitution inhabituelle afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher d'assurer les services voulus.

- **Attaque par usurpation d'adresse IP (IP spoofing)**

Cette attaque consiste à remplacer l'adresse IP du l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

- **Attaque par usurpation d'adresse MAC (MAC spoofing)**

Elle consiste à se faire passer pour une machine autorisée. Il suffit à l'intrus d'utiliser l'identité (adresse MAC) d'une machine autorisée à utiliser un service donnée.

- **ARP spoofing**

Cette attaque secrète à rediriger le trafic d'une machine vers une autre. Grace à cette redirection une personne mal intentionnée peut se faire passer pour une autre.

- **Attaque de mot de passe**

Il est très simple d'obtenir un programme permettant de retrouver le mot de passe utilisé pour l'accès à un service en utilisant des logiciels spéciaux comme les Keyloggers. Il permet de fait l'enregistrement de frappes qui espionne électroniquement l'utilisateur d'un ordinateur.

- **Les portes dérobées (backdoor)**

La porte dérobée est généralement introduite par un développeur de logiciels. Celui-ci crée un chemin non-surveillé pour accéder à l'ordinateur de la victime.
Une fois qu'une porte dérobée est installée avec le logiciel développé, l'attaquant a la possibilité de surveiller ce que fait l'utilisateur et de copier ou détruire les données ou bien la possibilité de prendre le contrôle d'un ordinateur (réseau).

- **Attaque Men In The Middle (MITM)**

Cette attaque est une redirection complète du flux échangé entre deux machines. Chacun des interlocuteurs croit dialoguer directement avec l'autre, mais en réalité il s'adresse à une 3ème machine qui joue le rôle d'un intercepteur de ces données.

3.8. Les outils de sécurité d'un réseau

Il existe plusieurs outils pour la sécurisation d'un réseau :

3.8.1. Le pare-feu (fire-wall)

C'est un ensemble de différents matériels et logiciels qui contrôlent le trafic intérieur/extérieur selon la politique de sécurité, il permet de surveiller donc les types de communications autorisés sur un réseau informatique.

3.8.2. La cryptographie

Vient du grec « Kruptos » qui signifie cacher et « Graphein » signifie écrire. Donc c'est un ensemble de technique permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale, C'est à dire il permet de contrôler le flux entrant et sortant.

Il existe deux principaux concepts de chiffrement qui sont présentés comme suit :

•Chiffrement à clé symétrique

Les clés de chiffrement et de déchiffrement sont identiques, $\mathbf{C_{chiffrement}=C_{déchfferement}=}$ **Clé**, la clé doit rester secrète tout au long de chiffrement et parmi les algorithmes qui utilisent cette technique on cite l'algorithme AES.

Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé, la taille des clés est souvent de l'ordre de 128 bits mais l'AES peut aller jusque à 256 bits. **[5]**

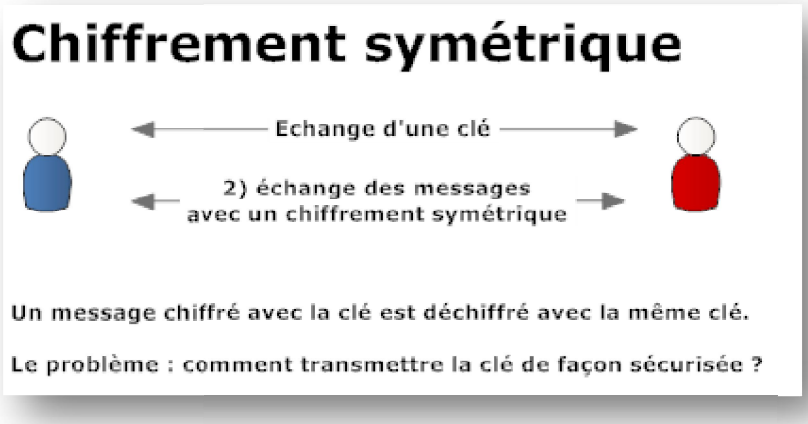

Figure 3.4 : *Chiffrement symétrique*

•Chiffrement à clé asymétrique

Le principe de ce type de chiffrement est d'avoir deux clés : une clé privée et l'autre publique, ce système permet la confidentialité d'un message transmis par conséquent personne ne peut lire le message sauf le destinataire. Il est pratiquement impossible de retrouver la clé privée à partir de la clé publique. Son but est de garantir la confidentialité d'une donnée. **[5]**

Dans ce type de cryptographie, chaque utilisateur comporte deux clés :

- Une clé privée qui doit être gardée secrète.
- Une clé publique qui est disponible pour tous les autres utilisateurs.

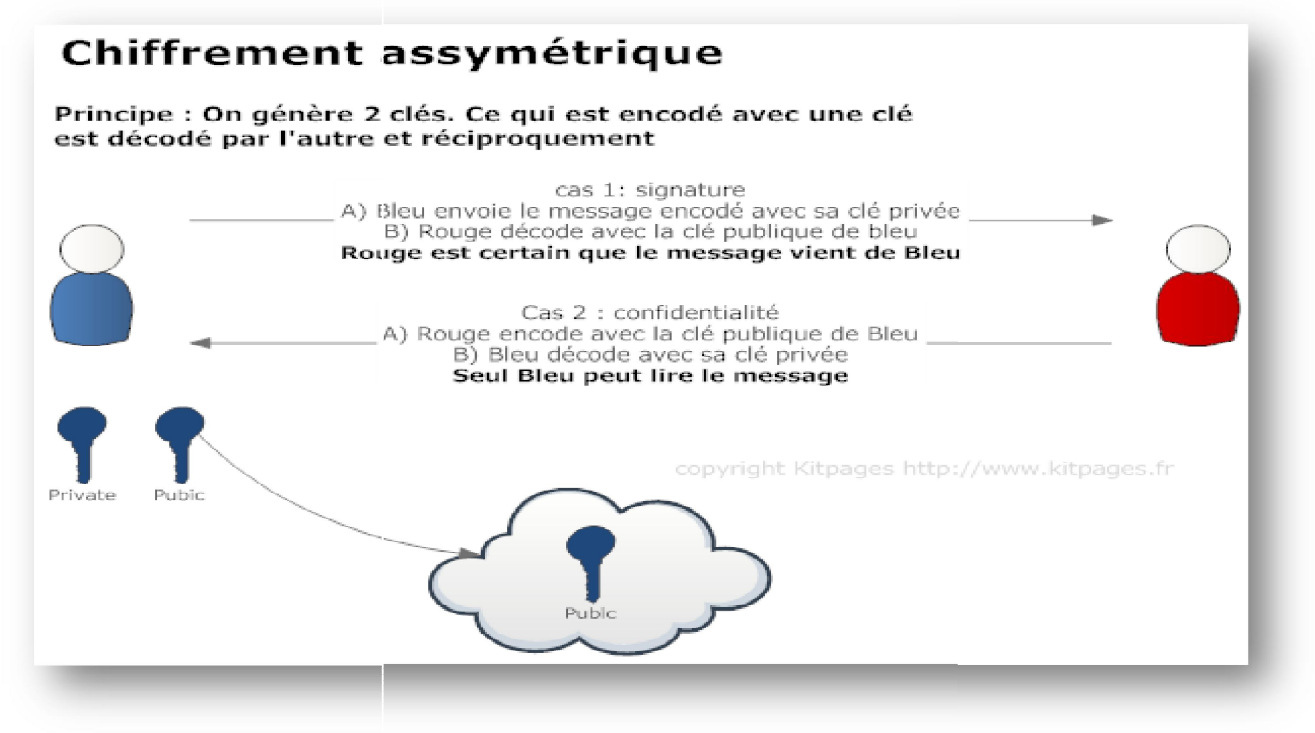

Figure 3.5: *Chiffrement asymétrique*

3.8.3. Le VPN

C'est un système permettant de créer un lien direct entre ordinateurs distants. C'est un tunnel sécurisé à l'intérieur d'un réseau (Internet).

Cependant, l'information VPN, dispose des informations permettant d'identifier l'utilisateur. **[14]**

3.8.4. L'IDS et l'IPS

Un système de prévention d'intrusion est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime. **[14]**

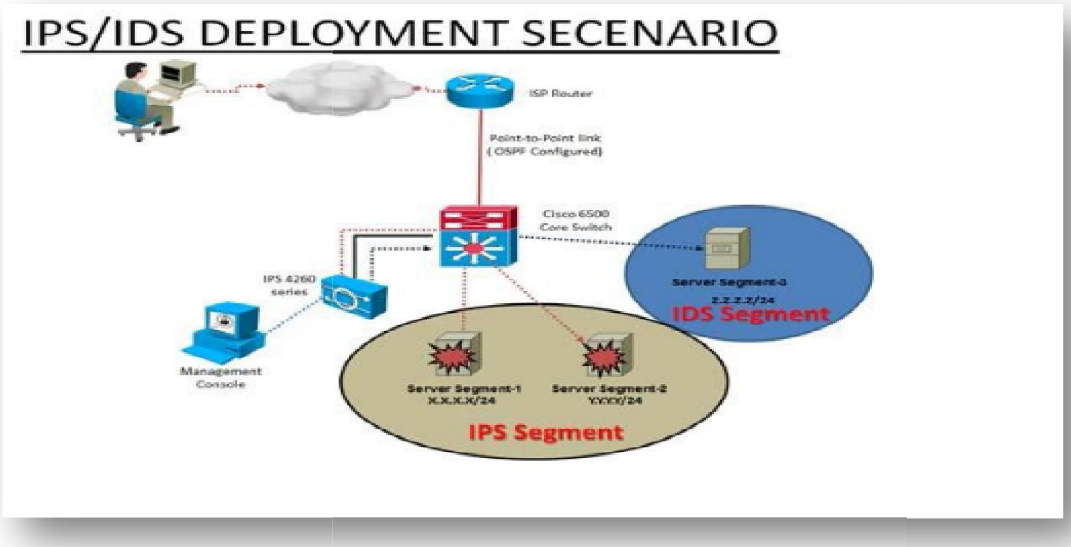

Figure 3.6 : *Sécurisation avec IPS*

3.8.5. Le VLAN

Un réseau local virtuel, qui est un réseau logique indépendant sert à segmenter le réseau en sous réseaux logiques. **[14]**

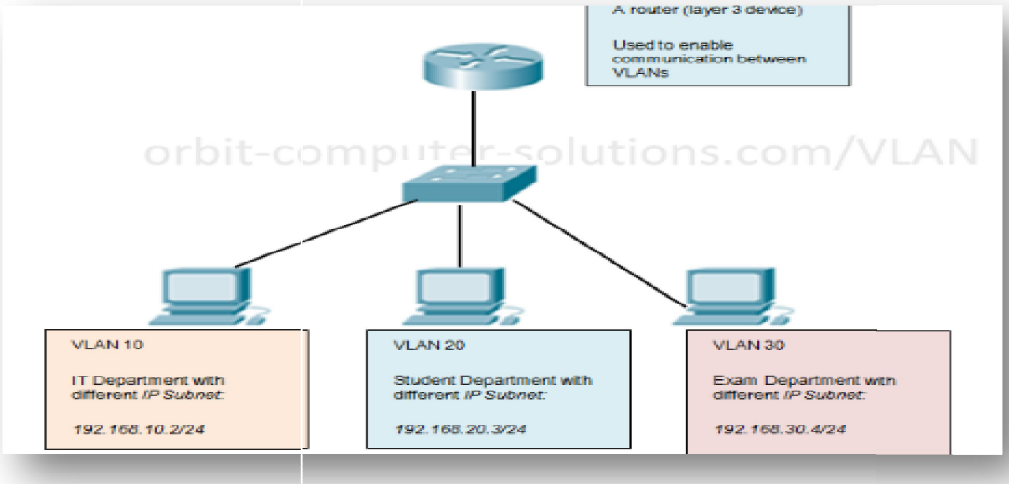

Figure 3.7 : *Architecture d'un VLAN*

3.8.6. La zone DMZ

C'est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local. **[14]**

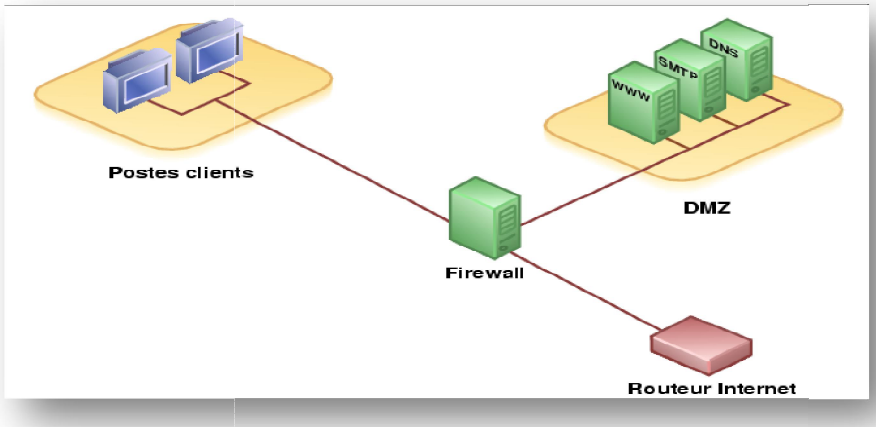

Figure 3.8 : *Sécurisation avec la DMZ*

3.8.7. Le proxy

C'est un composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre hôtes. Dans le cas des réseaux un proxy sert à une machine intermédiaire pour accéder à un autre réseau généralement internet. **[14]**

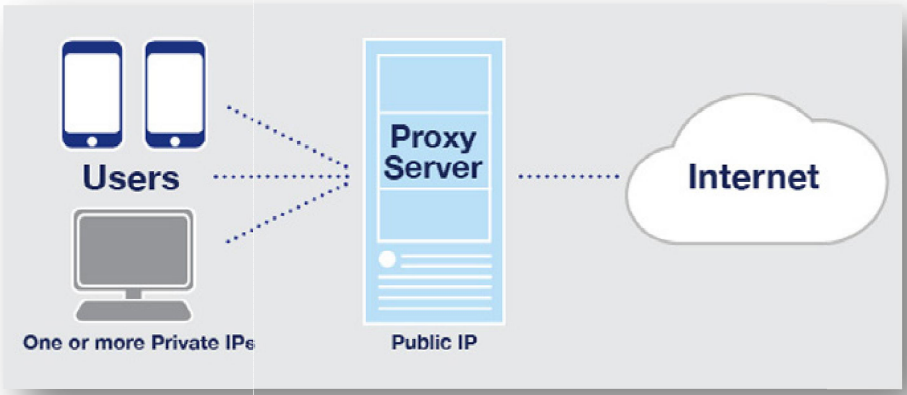

Figure 3 .9 : *Le proxy*

3.8.8. NAT

Dans un réseau informatique, on dit qu'un routeur fait du Network Address Translation (NAT) (translation d'adresse réseau) lorsqu'il fait correspondre des adresses IP privées à d'autres adresses IP publiques. En particulier, un cas courant est de permettre à des machines disposant d'adresses qui font partie d'un Intranet et ne sont ni uniques ni routables à l'échelle d'Internet, de communiquer avec le reste d'Internet.

Ainsi, l'objectif de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, afin de pallier à l'épuisement des adresses IPv4. **[14]**

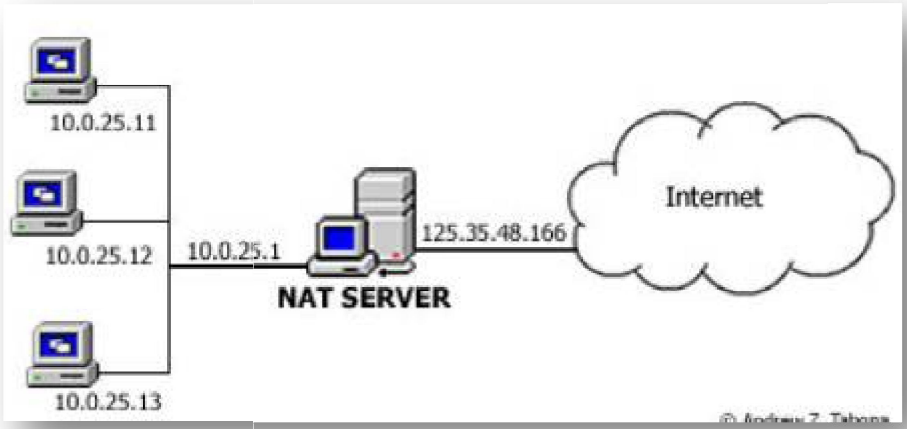

Figure 3.10 : *Serveur NAT*

3.8.9. Les anti-virus

Les anti-virus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

3.9. La solution de sécurité adoptée

3.9.1. Installation de l'antivirus ClamaAV de OwnCloud

Dans notre projet et afin de sécuriser notre application nous avons installé un antivirus et parmi les anti-virus qui nous étaient disponible nous avons choisi ClamAV.

ClamAV est un antivirus open source permettant de détecter les chevaux de Troie, les virus, les logiciels malveillants et d'autres menaces ; ainsi, il inclut un démon de scanner, pour l'analyse des fichiers à la demande et des mises à jour automatiques , bien qu'il s'agit d'un logiciel qui prend en charge plusieurs formats de fichiers et plusieurs langages. **[11]**

a. Les avantages de ClamAV

La grande force de ClamAV, réside dans sa capacité de détecter un très grand nombre de

virus, qui sont déclarés dans ce qu'on appelle la base des signatures des virus, elle se met à jour plusieurs fois par jour . La base des signatures des virus de ClamAV comprend la liste des virus connus sur le web afin de mieux détecter ces mêmes virus.

La rapidité de scanner ou d'examiner les fichiers dans un dossier ou dans une partition. Mais ClamAV, ne dispose pas de fonction de scan en temps réel dans le système. Il faut vérifier le ou les fichiers manuellement.

b. Installation de ClamAV

Pour installer ClamAV, nous allons suivre les étapes ci dessous :

- ✓ Nous allons saisir la commande suivante pour installer l'anti-virus ClamAV :

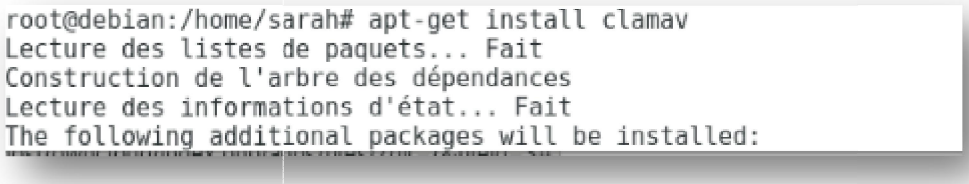

Figure3.11 : *Installation de ClamAV*

- ✓ Les étapes de téléchargement des paquets et configuration du ClamAV :

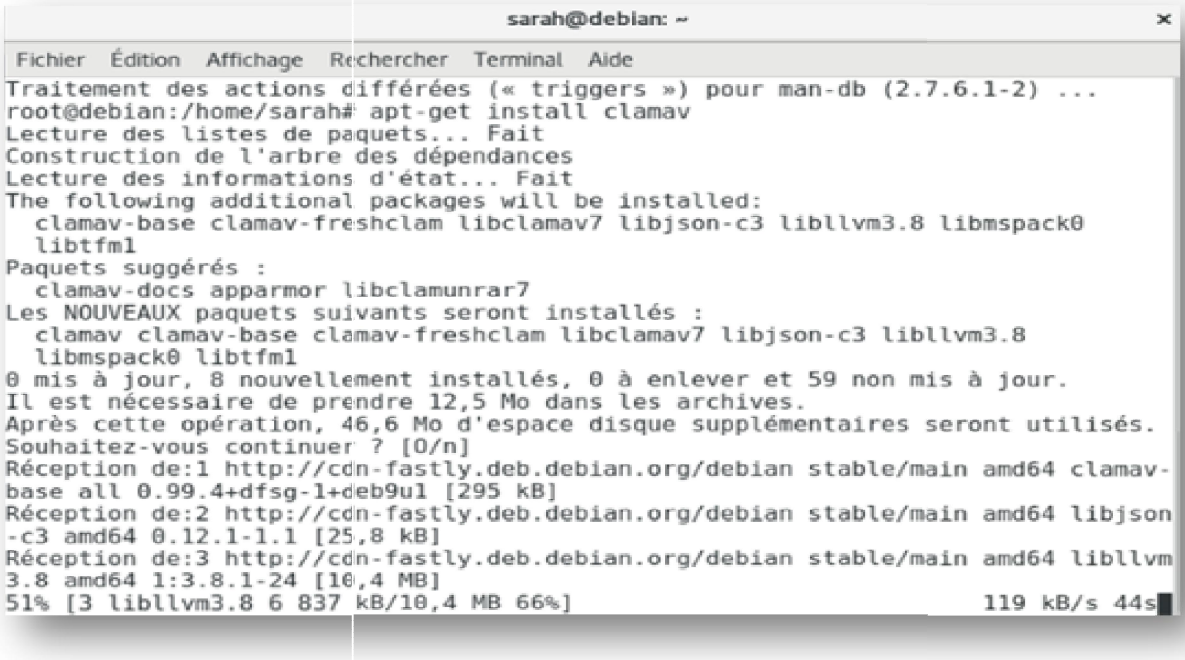

Figure 3.12 : *Téléchargements des paquets de ClamAV*

- ✓ pour tester le fonctionnement de ClamAV , nous allons maintenant téléchargé le virus Eicar :

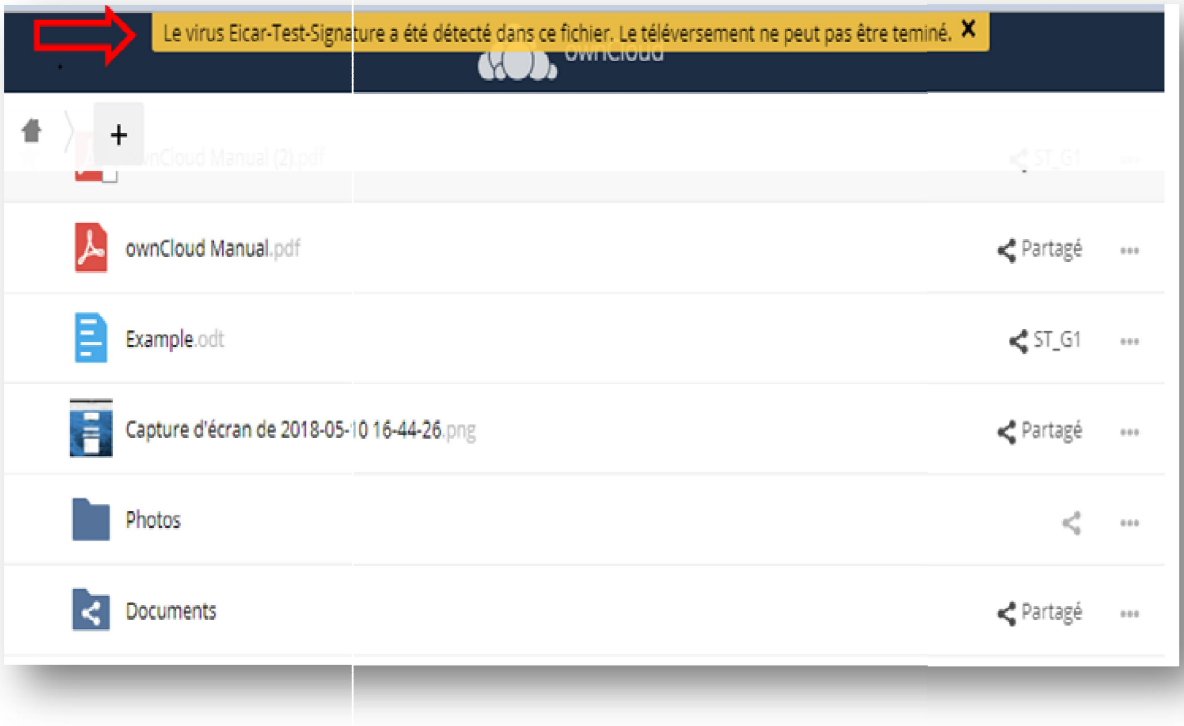

Figure 3.13 : *ClamAV est fonctionnel*

3.9.2. Activation de SSL (Secure Socket Layer)

Le SSL est un protocole de sécurité le plus répandu qui crée un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne, le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web, par exemple, les utilisateurs sont avertis de la présence de la sécurité SSL grâce à l'affichage d'un cadenas et l'URL commençant par « https:// » ou le « s » signifie « secured ».

En effet, le SSL repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de communication sécurisée (chiffré) entre les deux machines, après une étape d'authentification. Le système SSL est indépendant du protocole utilisé ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le web par le protocole hhtp que des connexions via des protocoles FTP **[6]**

Alors le SSL agit comme une couche supplémentaire permettant d'assurer la sécurité des données, situé entre la couche application et la couche transport dans le protocole TCP par exemple. **[13]**

- ✓ Avant l'activation de SSL, l'interface web de OwnCloud n'est pas sécurisée au départ :

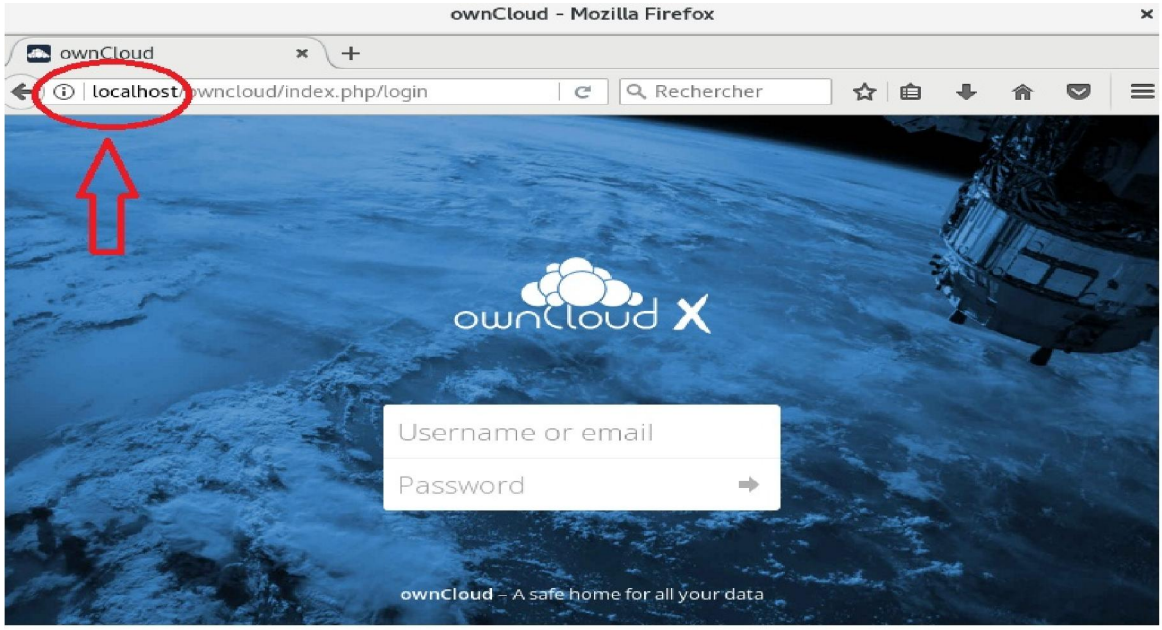

Figure 3.14: *Interface n'est pas encore sécurisée*

- ✓ Dans un terminal nous allons saisir les commandes suivantes pour activé le module SSL et le site SSL par default :

```
root@debian:/home/sarah# a2enmod ssl
```

Figure 3.15: *Activation de module SSL*

```
root@debian:/home/sarah# a2ensite default-ssl
```

Figure 3.16 : *Activation de site SSL*

- ✓ La commande permettant le redémarrage de service apache2 :

```
root@debian:/home/sarah# service apache2 reload
```

Figure 3.17 : *Redémarrage du service apache*

✓ L'application n'est pas encore sécurisée, elle nécessite d'autres paramètres en cliquant sur la case avancée puis sur la case autres paramètres :

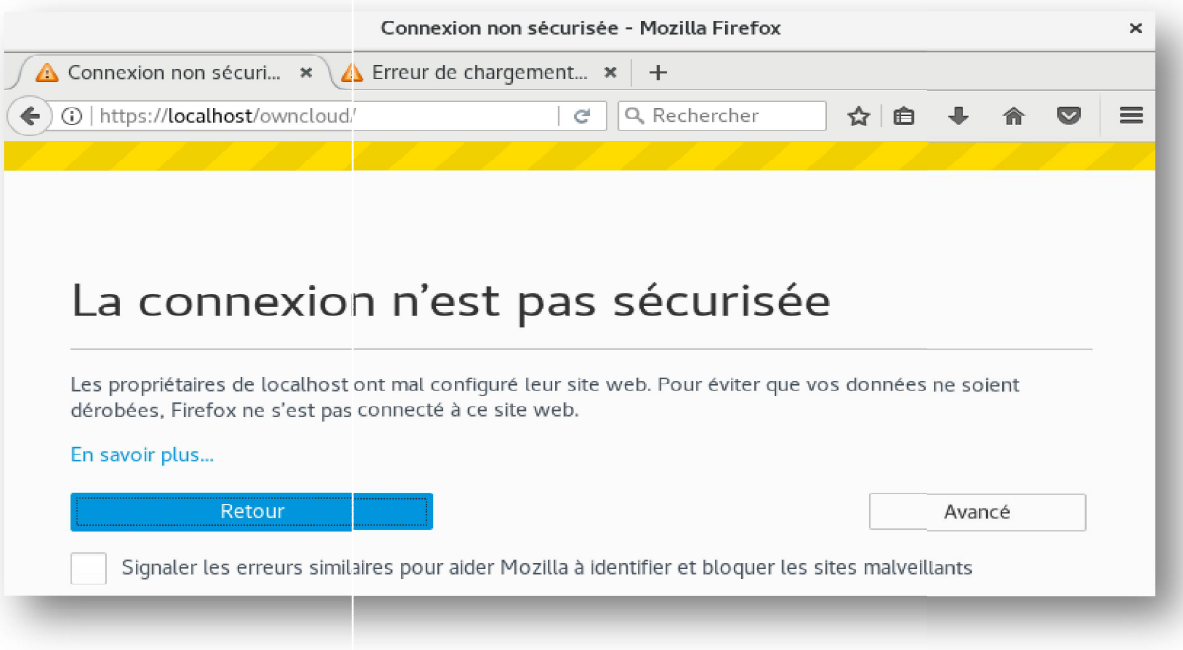

Figure 3.18 : *Page non sécurisée*

✓ Et par la suite on clique sur la case « obtenir le certificat » pour finir la configuration :

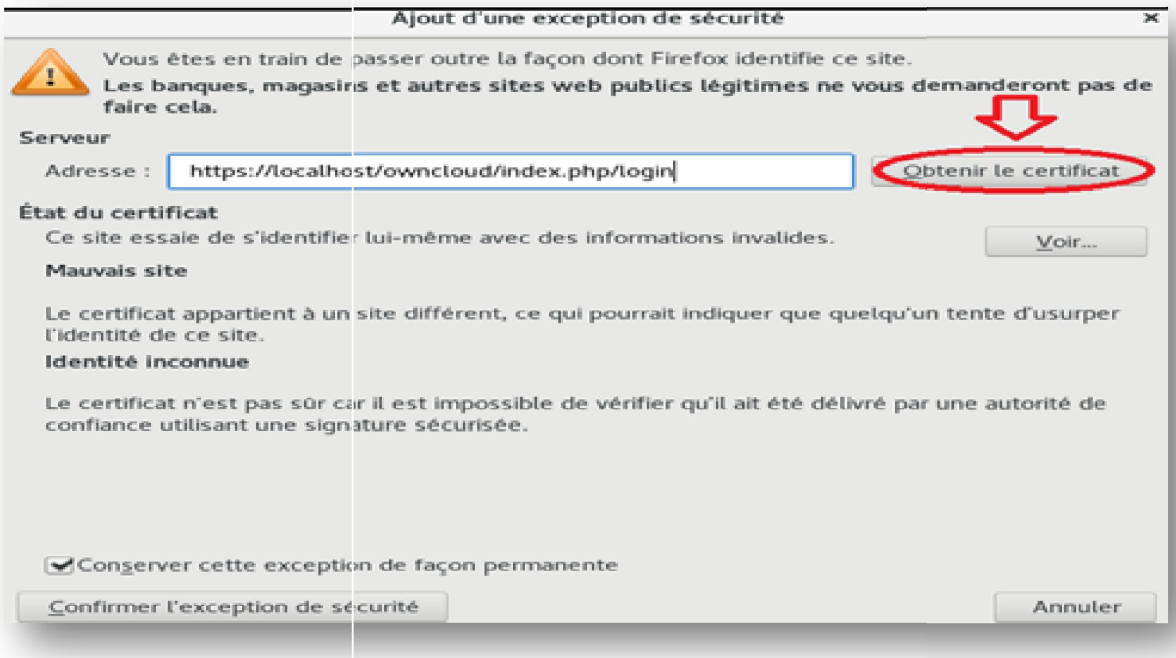

Figure 3.19 : *Configuration du SSL*

✓ Voilà donc notre application est devenue sécurisée:

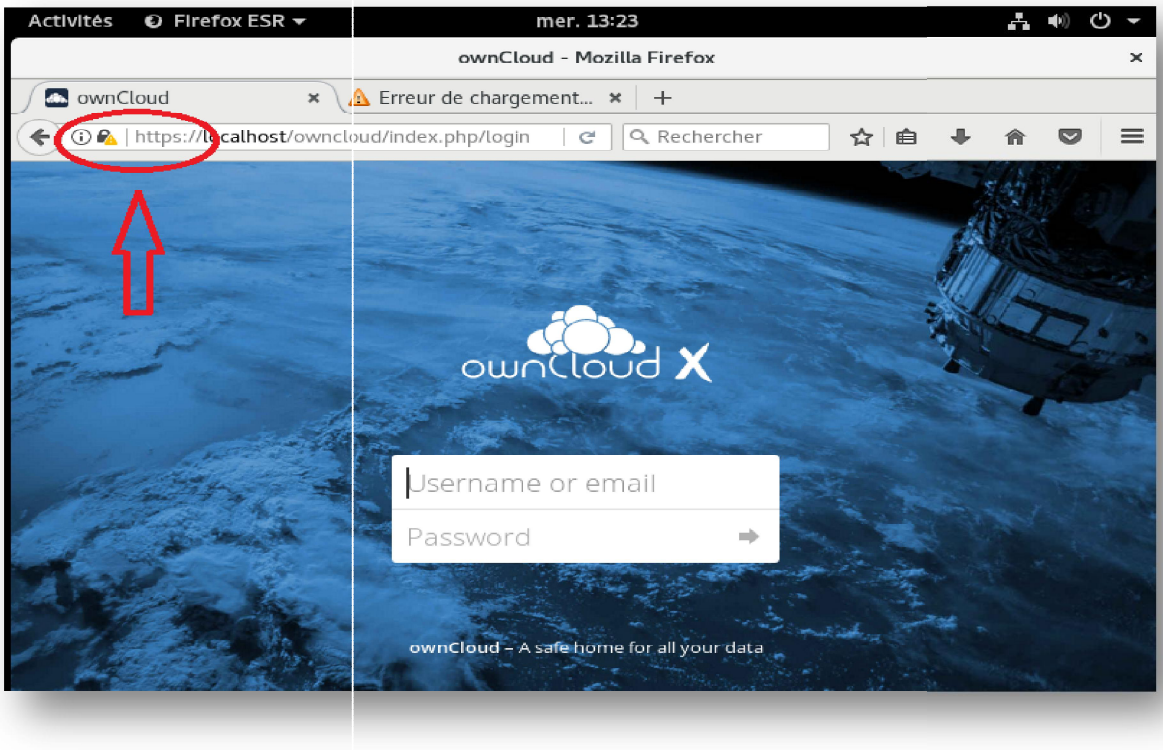

Figure 3.20 : *Page sécurisée*

3.9.3. Utilisation du cryptage AES dans le serveur Backup

L'application Duplicati permet d'effectuer des sauvegardes de données, ces données sont cryptées à l'aide de logiciel de cryptage AES.

Le cryptage AES est un chiffrement symétrique par bloc de données, il est destiné à remplacer le chiffrement DES qui est devenu trop faible au regard des attaques actuelles. L'algorithme AES est :

- Simple à implémenter sur une grande variété de plateforme et d'application.
- Ses besoins en ressources et mémoire sont très faible.
- Possibilité de l'implémenter sous forme logicielle ou matérielle (câblé).
- Il a un design très simple.
- Il supporte différentes combinaisons (longueur de clé et longueur de bloc) : 128-128 et 256-128 bits.

3.9. *Discussion*

Dans cette partie de notre travail, nous avons suivie des étapes d'avoir une première sécurité pour le serveur de partage « Owncloud ». En effet, nous avons installés un antivirus performant qui est ClamAV et activés le protocole SSL. Concernant le serveur Backup, l'utilisation du chiffrement AES par l'application « Duplicati » permet d'avoir des fichiers cryptés. Par conséquent, en cas d'interception de ces fichiers, ils ne seront pas utilisables.

Conclusion

Dans ce mémoire, nous nous sommes intéressées au réseau de l'entreprise 2INT Parteners. Après avoir fait une étude sur ce dernier, nous avons constatés le manque de deux types de serveurs basiques et indispensables dans n'importe quelle entreprise. Ces deux serveurs sont le serveur de partage de fichiers et le serveur de sauvegarde (Backup). Ces deux serveurs vont permettre aux différents utilisateurs du réseau 2INT (les enseignants, les étudiants ou le personnel de l'administration) de partager et de traiter les différents fichiers.

Comme serveur de partage, nous avons optés pour l'utilisation de l'application « OwnCloud ». Ce choix est motivé par les différents avantages de son utilisation par rapport aux autres applications. En effet, OwnCloud est open source et utilise une interface graphique pour les différentes configurations. Par contre, pour le serveur de sauvegarde nous avons choisis l'application « Duplicati ». Ce choix s'est fait après une étude comparative entre plusieurs autres applications. En effet, Duplicati est une application gratuite, ajoutant à cela qu'elle comporte un chiffrement fort qui est le cryptage AES-256, voir aussi que Duplicati permet de faire un sauvegarde automatique sans intervention humaine.

Une fois que les deux serveurs sont mis en marche, nous avons pensés à adopter une première politique de sécurité. Celle-ci s'articule autour de trois outils. Le premier est l'utilisation d'un antivirus. Le deuxième outil est l'utilisation du protocole SSL qui est appliqué pour l'application de partage Owncloud. Le troisième outil qui est la cryptographie symétrique AES est appliqué sur le réseau de sauvegarde.

Comme perspectives de ce travail, nous proposons de mieux sécuriser les deux serveurs déjà implémentés. En effet, quelques lacunes de sécurité nous ont été signalées. A commencer par le système d'exploitation Linux qui possède des modes permettant de détourner la méthodologie de sécurité déjà suivie.

BIBLIOGRAPHIE

[1] thèse : généralités sur le réseau info

[2] https //www.creately.com.html

[3] Installation pas à pas de Debian 9 (Stretch). pdf

[4] Introduction à la Sécurité Informatique pdf Hiver .2002 ; Louis Salvail

[5] Ylescop.free.fr pdf. 2002 ; LESCOP Yves

[6]LeGrandLivre.pdf.2006 ; Sécurité informatique

[7]Microapp.com pdf: W. KHADIR, (2014), « *Etude et mise en place d'un pot de miel virtuel basé sur le Respberry Pi 3 »,* Thèse, école 2INT Partners.

[8]Serveurs_cours1.pdf ; Réaliser par GUILLAEME BULEL

[9] Serveur de fichiers-Wikipédia(1).pdf

[10] https://owncloud.org, Consulté le 20/03/2018

[11] https://www.clamav.net , Consulté le 30/05/2018

[12] https://linux-pour-tous.blogspot.com, Consulté le 11/03/2018

[13] https://www.commentcamarche.com, Consulté le 22/03/2018

[14] http://www-igm.univ-mlv.fr/~dr/XPOSE/Securite/, Consulté le 20/06/2018

Résumé

Dans ce mémoire, nous nous sommes intéressées au réseau de l'entreprise 2INT Parteners. Après avoir fait une étude sur ce dernier, nous avons constatés le manque de deux types de serveurs basiques et indispensables dans n'importe quelle entreprise. Ces deux serveurs sont le serveur de partage de fichiers et le serveur de sauvegarde (Backup). Ces deux serveurs vont permettre aux différents utilisateurs du réseau 2INT (les enseignants, les étudiants ou le personnel de l'administration) de partager et de traiter les différents fichiers.

Comme serveur de partage, nous avons optés pour l'utilisation de l'application « OwnCloud ». Ce choix est motivé par les différents avantages de son utilisation par rapport aux autres applications. En effet, OwnCloud est open source et utilise une interface graphique pour les différentes configurations. Par contre, pour le serveur de sauvegarde nous avons choisis l'application « Duplicati ». Ce choix s'est fait après une étude comparative entre plusieurs autres applications. En effet, Duplicati est une application gratuite, ajoutant à cela qu'elle comporte un chiffrement fort qui est le cryptage AES-256, voir aussi que Duplicati permet de faire un sauvegarde automatique sans intervention humaine.

Une fois que les deux serveurs sont mis en marche, nous avons pensés à adopter une première politique de sécurité. Celle-ci s'articule autour de trois outils. Le premier est l'utilisation d'un antivirus. Le deuxième outil est l'utilisation du protocole SSL qui est appliqué pour l'application de partage Owncloud. Le troisième outil qui est la cryptographie symétrique AES est appliqué sur le réseau de sauvegarde.

Les mots clé

Réseaux informatique, Serveur, Serveur de partage, Serveur de stockage, Backup, Sécurité informatique, SSL, Vsftpd

Chapitre 1
Etude de l'existant

Chapitre 2
Solution proposée

Chapitre 3
Sécurisation de l'application

Introduction

Conclusion

Bibliographie

Glossaire

Annexe

Table des figures

Liste des tableaux

Sommaire

Annexe

Système Linux et installation de Debian9 [3]

Un système Linux

Linux est un système d'exploitation libre, qui peut être utilisé en lieu et place de systèmes d'exploitation commercialisés, tels que Windows, de Microsoft. Il est accompagné de nombreux logiciels libres complémentaires, offrant un système complet aux utilisateurs.

Il est conçu dans le but de remplacer Windows et Mac OS X. Il est disponible en téléchargement gratuit et peut être installé sur à peu près n'importe quel ordinateur.

À l'origine, le noyau Linux a été développé pour les ordinateurs personnels (PC) compatibles et devait être accompagné des logiciels GNU pour constituer un système d'exploitation. Depuis les années 2000, le noyau Linux est utilisé sur du matériel informatique.

Le noyau Linux a été créé en 1991 par Linus Thorvalds. C'est un logiciel libre. Les distributions Linux ont été, et restent, un important vecteur de popularisation du mouvement open source. **[12]**

Installation de Debian

Après le lancement de l’installation de Debian par une clé USB, Les étapes de l’installation sont les suivantes :

✓ **Etape 1 :** Sélectionner le mode d'installation graphique par défaut en, effet le mode Graphical propose une interface utilisable avec une souris :

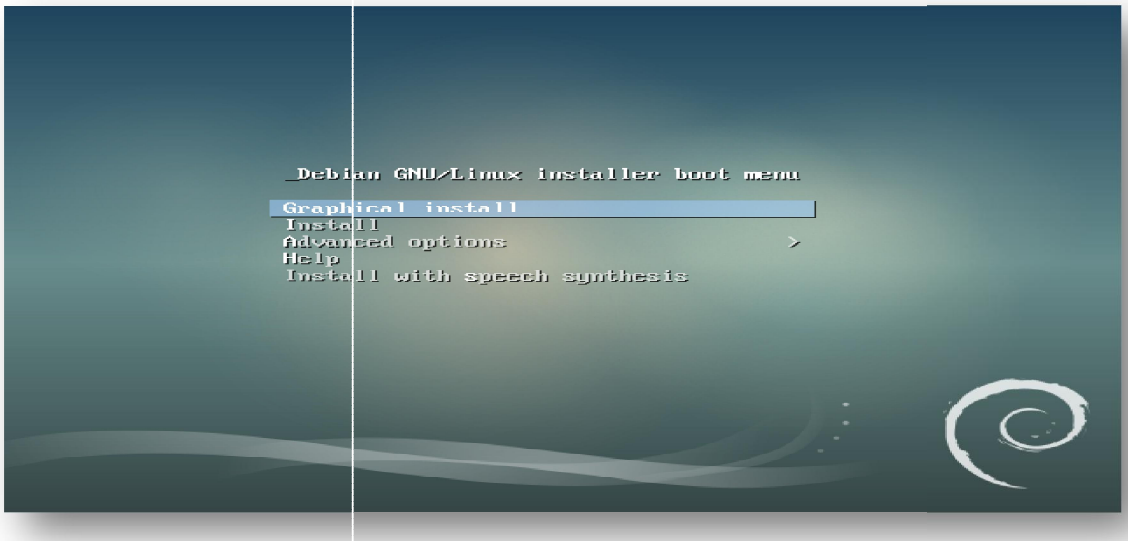

Figure 1 : *Installation de Debian*

✓ **Etape 2 :** Choix de la langue :

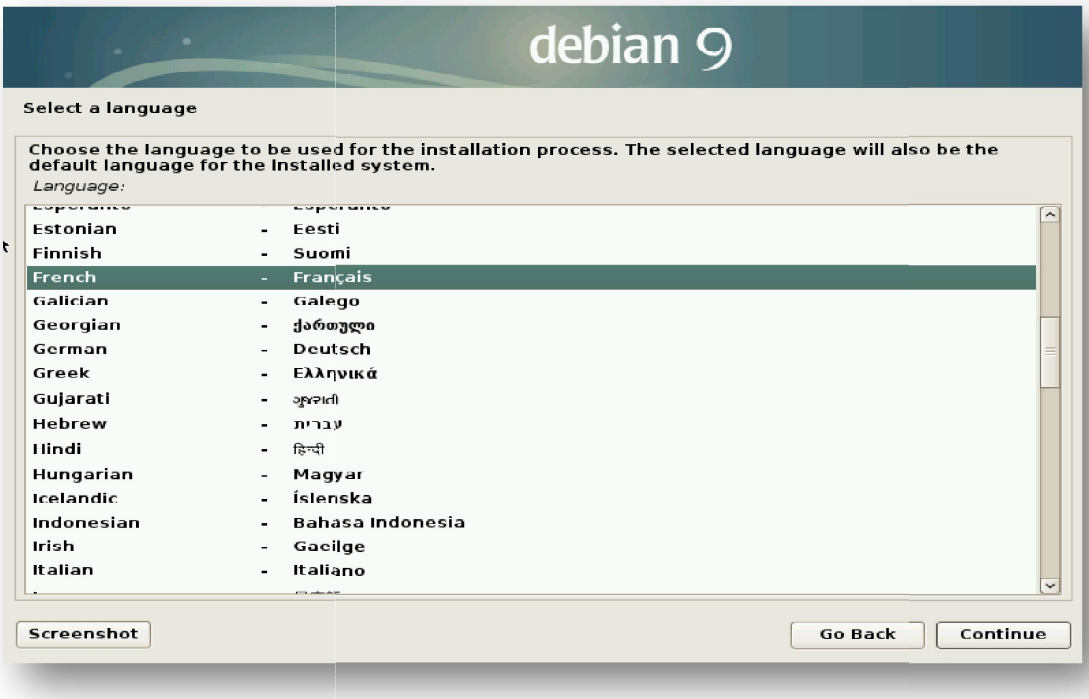

Figure 2 : *Sélectionner la langue*

✓ **Etape 3 :** Choix de la situation géographique :

Figure 3 : *Situation géographique*

✓ **Etape 4 :** Nous choisissons la langue française pour le clavier :

Figure 4 : *Choix de la langue*

✓ **Etape 5 :** Configurer le nom du système

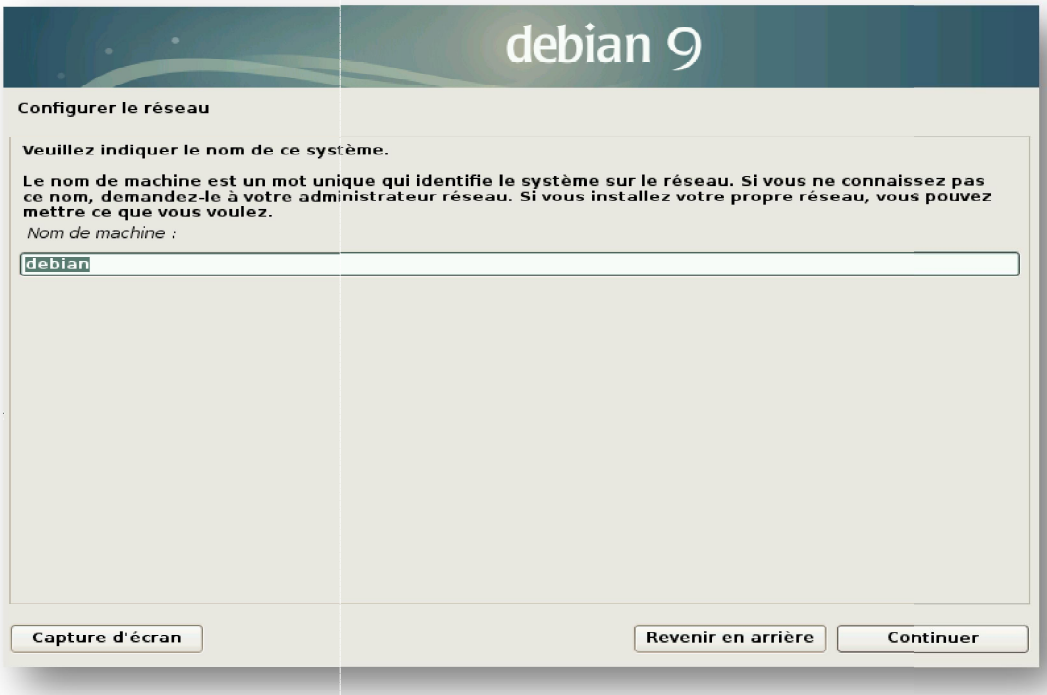

Figure 5 : *Nom de système*

✓ **Etape 6 :** Définir le mot de passe de super utilisateur « **root**» :

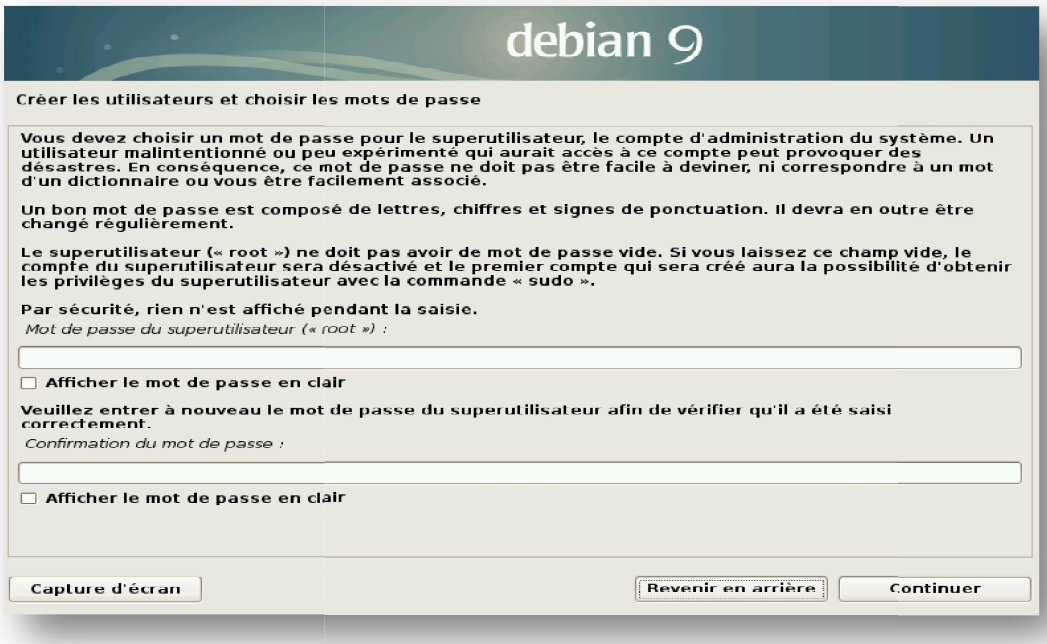

Figure 6 : *Création de l'utilisateur et mot de passe*

✓ **Etape 7** : Création du premier utilisateur :

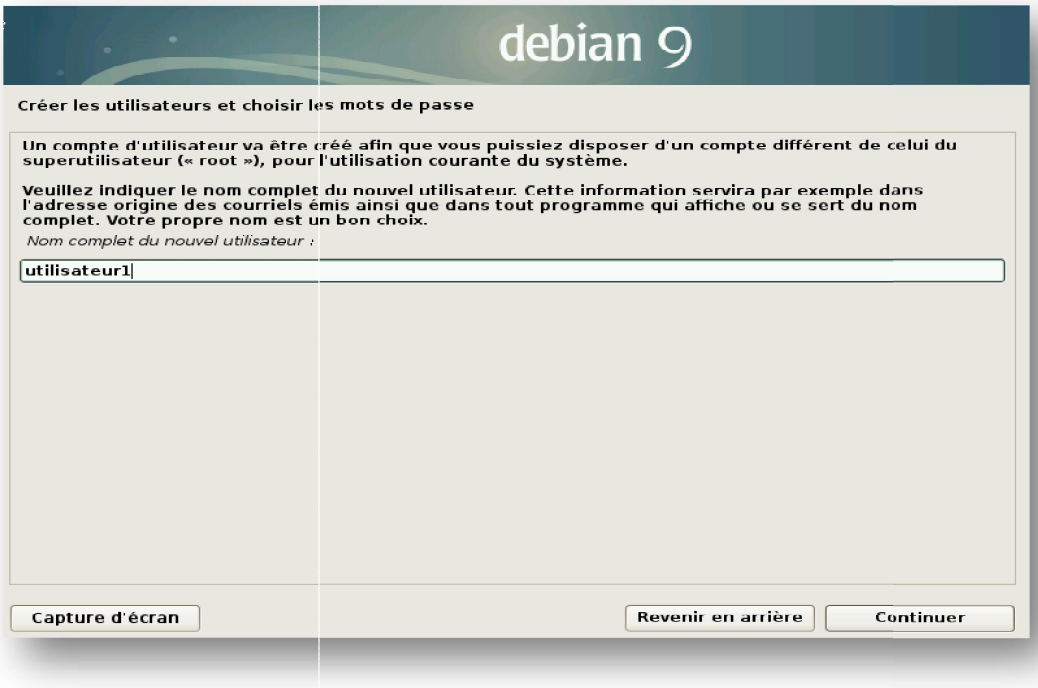

Figure 7 : *Nom de nouvel utilisateur*

✓ **Etape 8 :** Création d'un mot de passe pour le premier utilisateur :

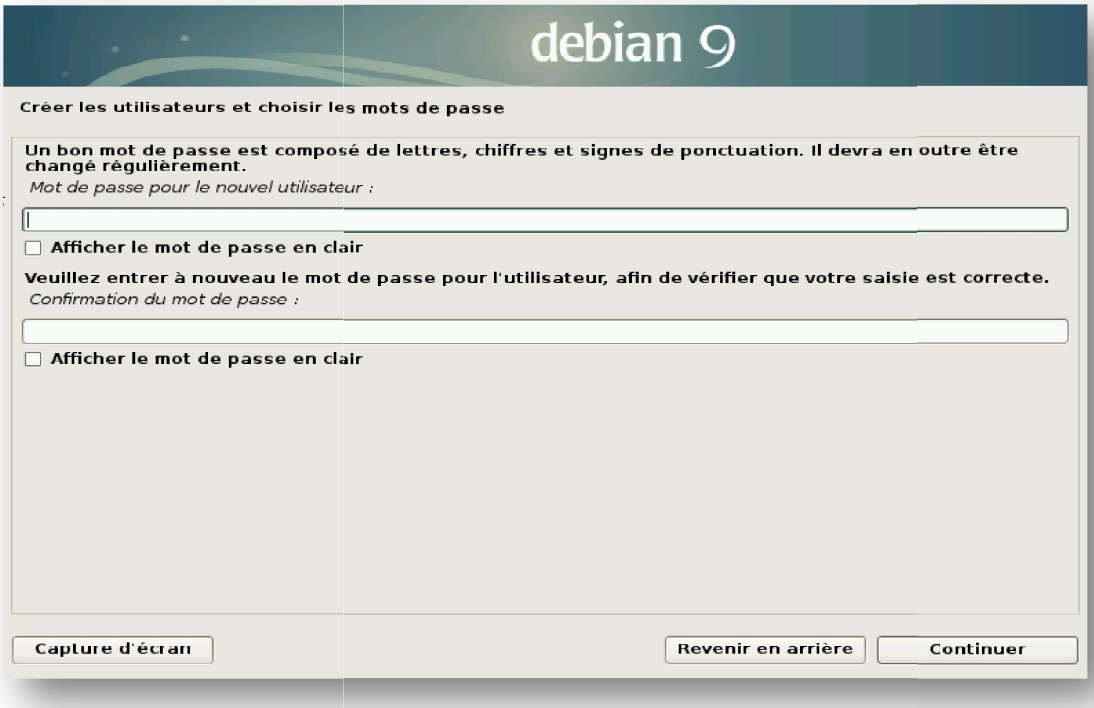

Figure 8 : *Créer un mot de passe*

✓ **Etape 9 :** Nous avons choisis un mode de partitionnement de disque dur entier :

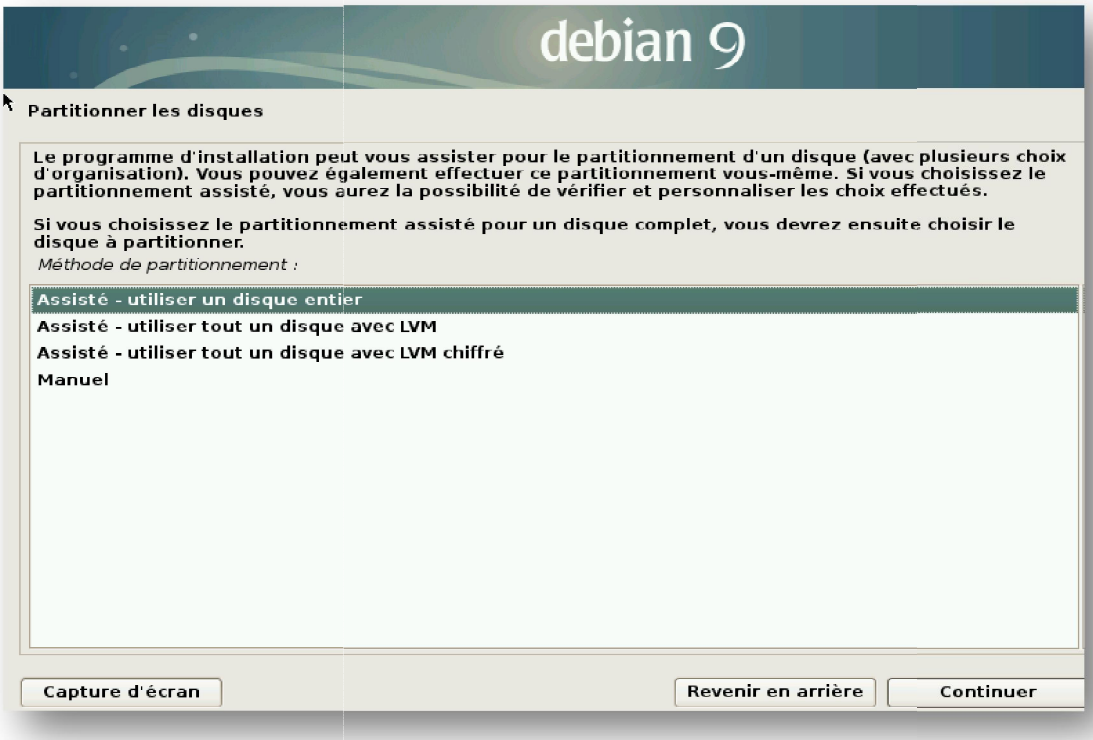

Figure 9 : *Partition de disque*

✓ **Etape 10** : Nous choisissons du disque sur lequel on va créer la partition :

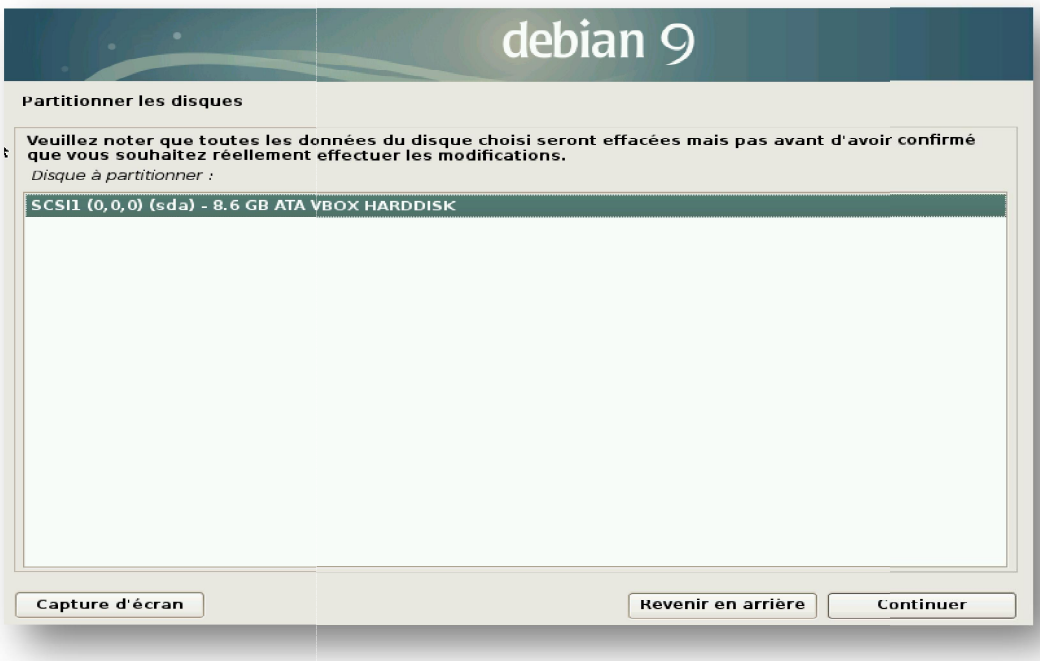

Figure 10 : *Disque à partitionner*

✓ **Etape 11 :** Le choix du partitionnement :

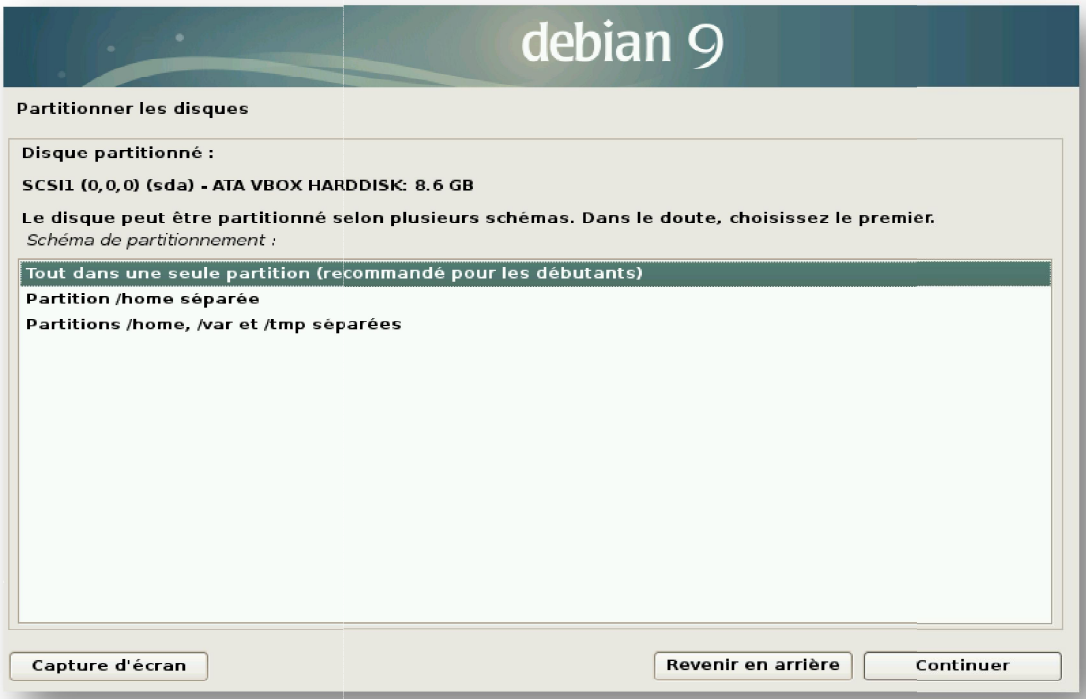

Figure 11: *Schéma de partitionnement*

✓ **Etape 12 :** Continuer ou terminer le partitionnement :

Figure 12 : *Fin de partitionnement*

✓ **Etape 13 :** Récapitulatif du partitionnement et lancement du formatage :

Figure 13 : *Accorder les changements sur le disque*

✓ **Etape 14 :** Configuration de la gestion des paquets et analyse du contenu des CD ou DVD supplémentaires si nécessaire :

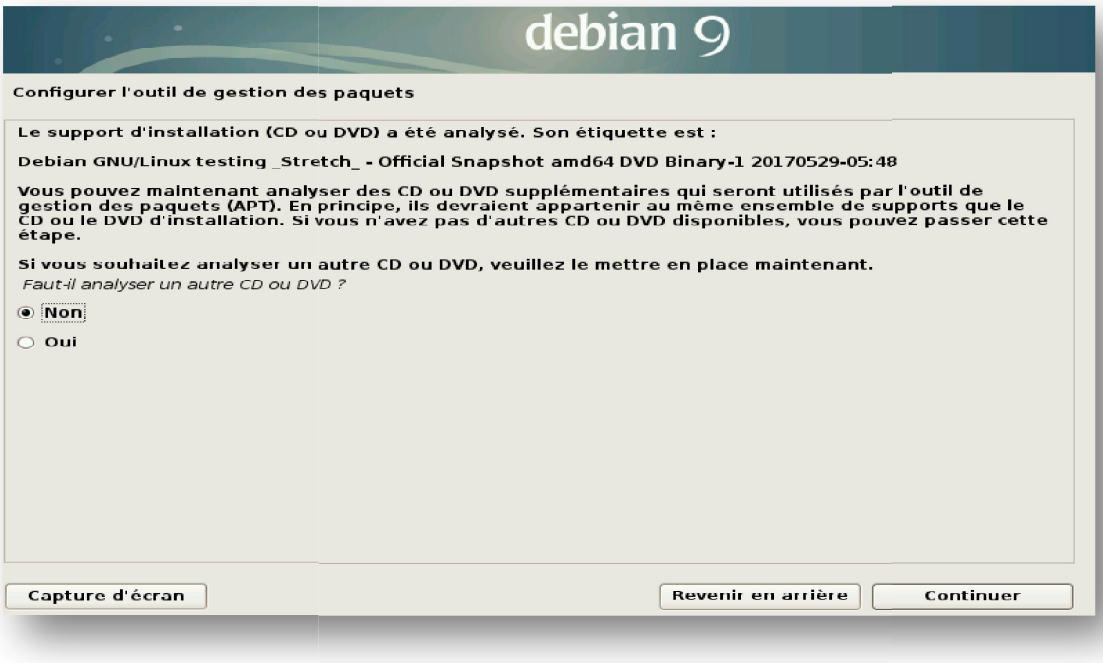

Figure 13 : *Refuser l'analyse d'un autre disque*

✓ **Etape 15 :** Utilisation d'un dépôt miroir :

En effet un dépôt miroir est un serveur informatique accessible qui héberge l'ensemble des paquets Debian. Si vous ne disposez pas de tous les CD, Debian viendra piocher les logiciels ou paquets dont vous avez besoin sur des serveurs miroirs.

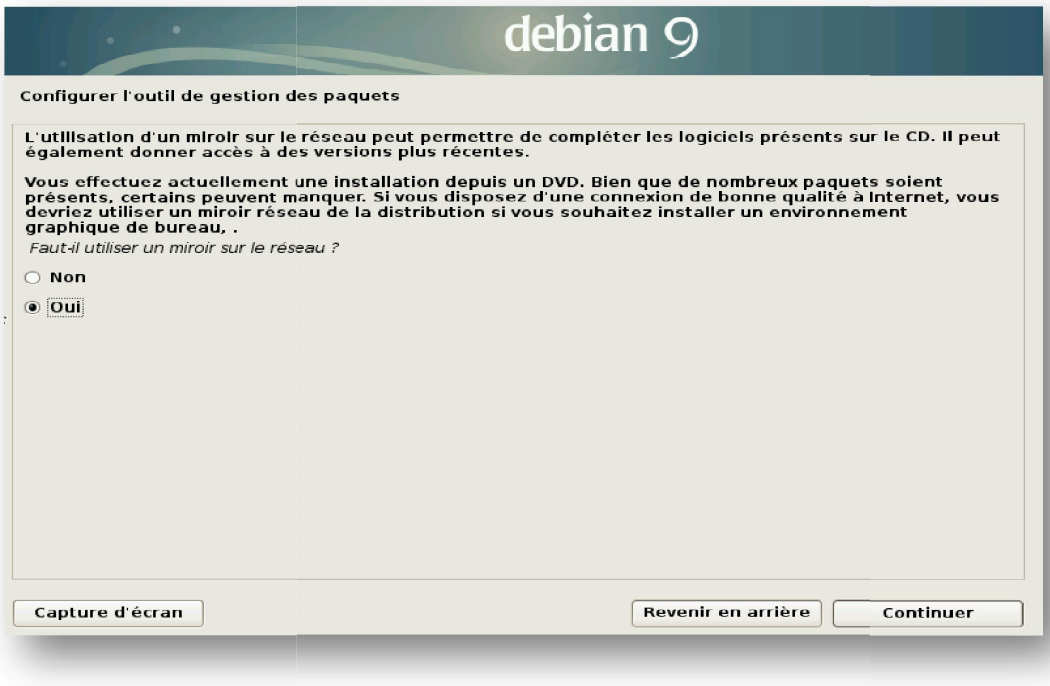

Figure 14 : *Utiliser un miroir sur le réseau*

✓ **Etape 16 :** Choix du pays dans lequel se trouve le miroir :

Figure 15 : *Pays du mémoire de l'archive Debian*

✓ **Etape 17 :** Choix du serveur hébergeant le miroir :

Figure 16 : *Miroir de l'archive Debian*

✓ **Etape 18 :** Configuration d'un serveur mandataire "ou proxy" si nécessaire :

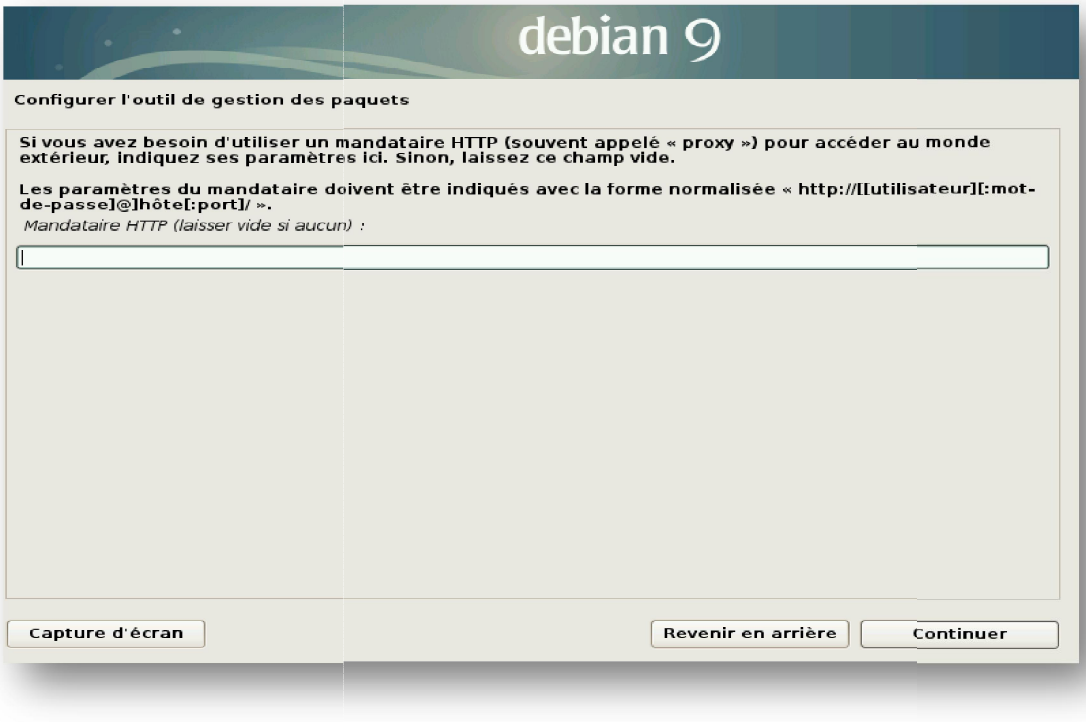

Figure 17 : *Mandataire http*

✓ **Etape 19 :** Participation ou pas aux statistiques Debian :

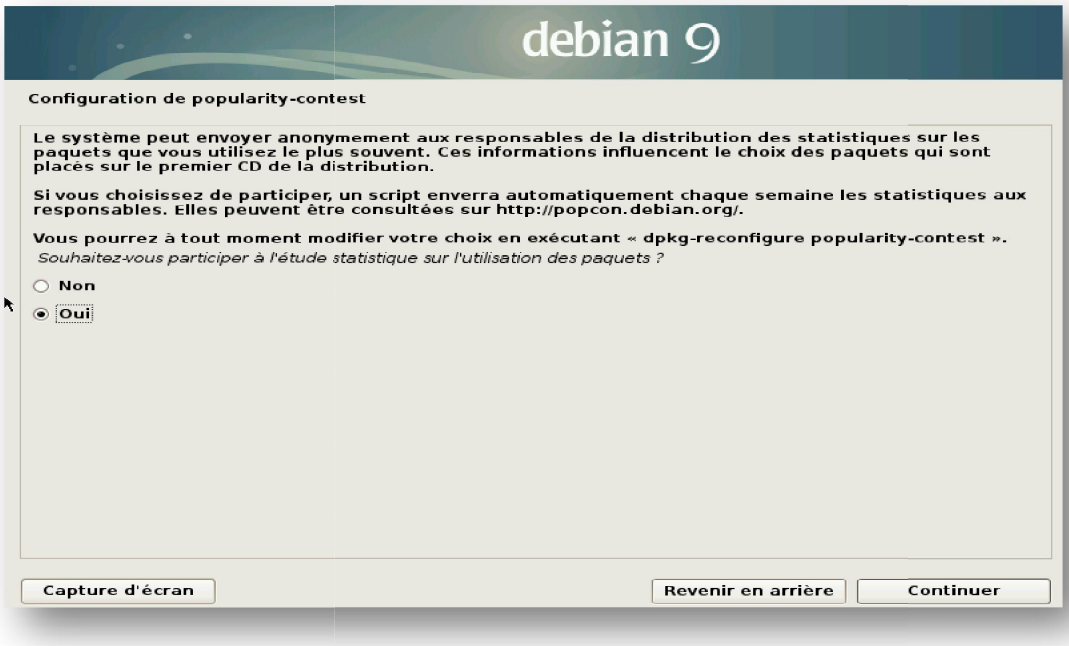

Figure 18 : *Etude statistique sur l'utilisation des paquets*

✓ **Etape 20 :** Sélection des logiciels :

Figure 19 : *Logiciel à installer*

✓ Etape 21 : Fin de configuration et installation des paquets Debian :

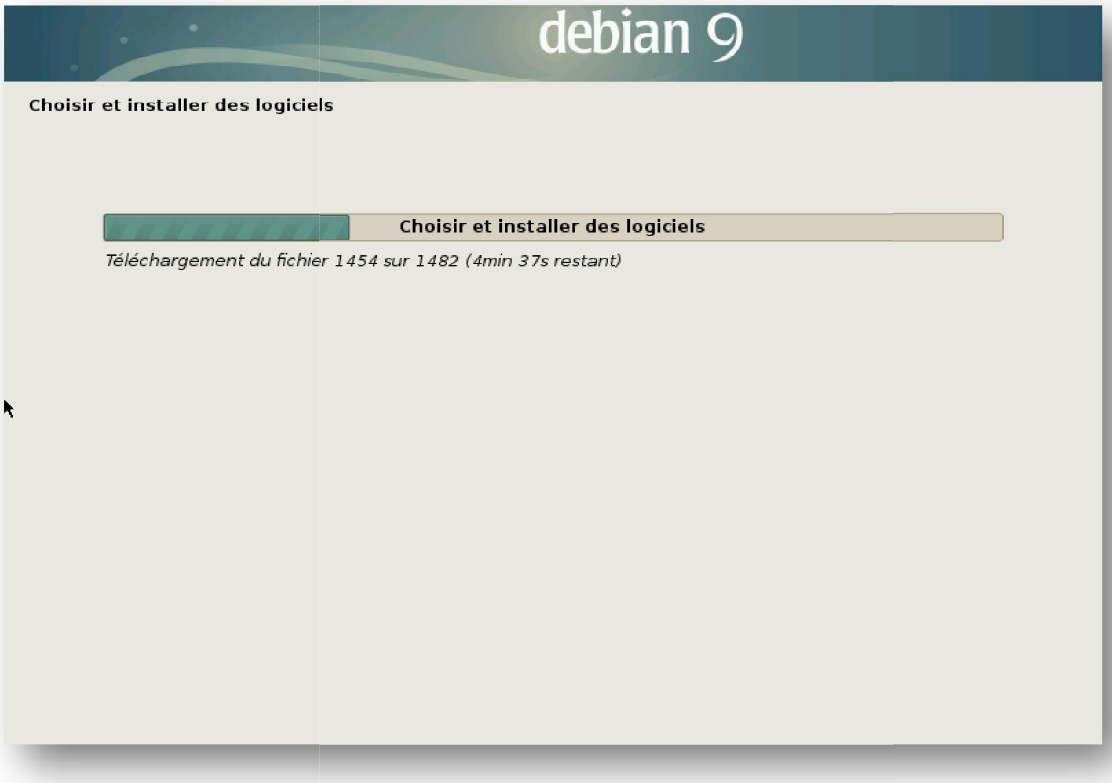

Figure 20 : *Choisir et installer des logiciels*

✓ **Etape 22 :** installation de GRUB :

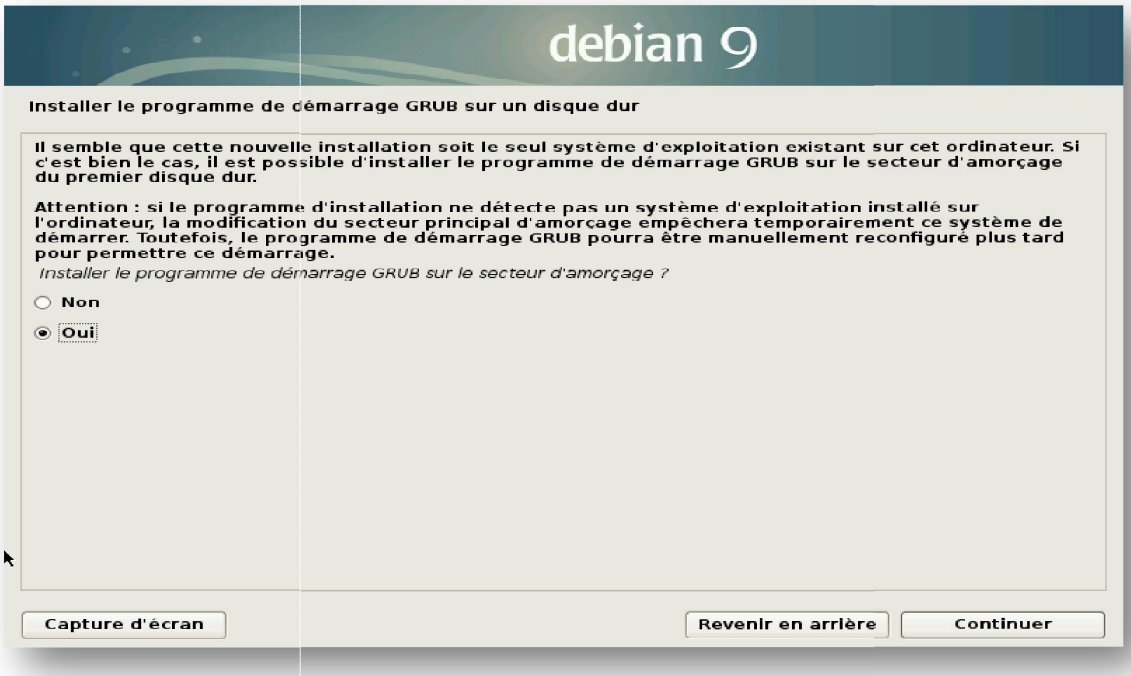

Figure 21 : *Installation de programme GRUB sur le serveur d'amorçage*

✓ **Etape 23** : choix de l'emplacement pour le GRUB :

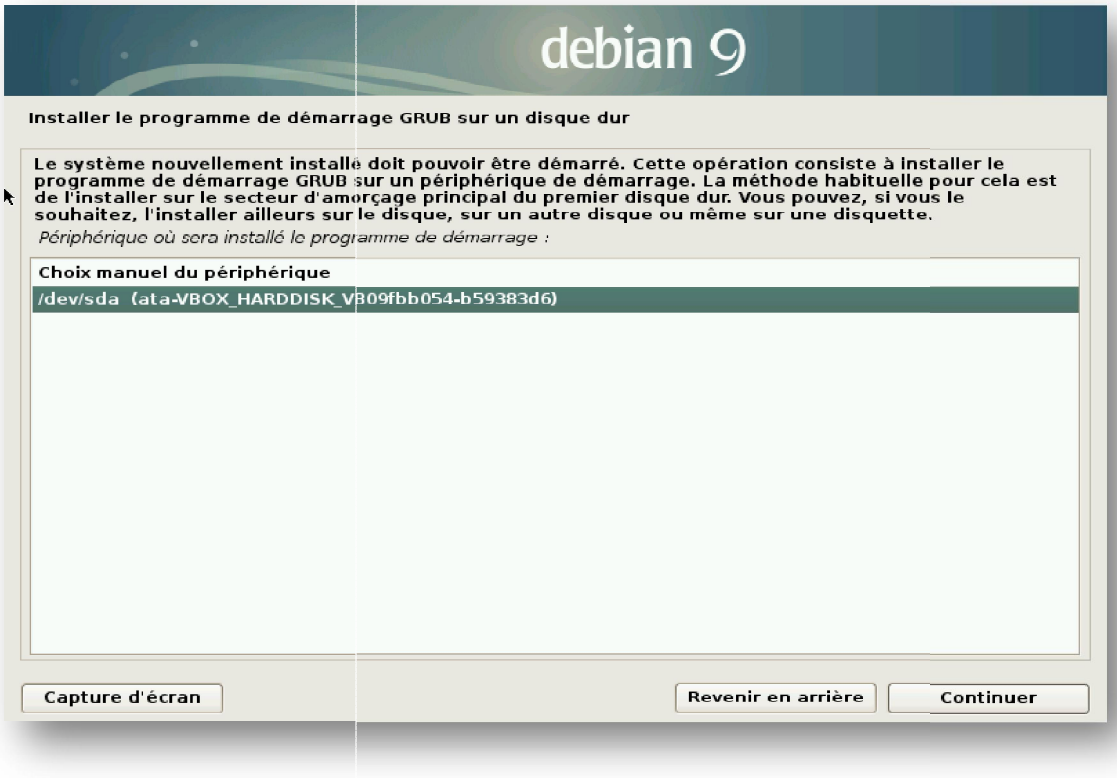

Figure 22 : *Choix de périphérique*

✓ **Etape 24 :** Fin d'installation et lancement de Debean9 sur notre ordinateur :

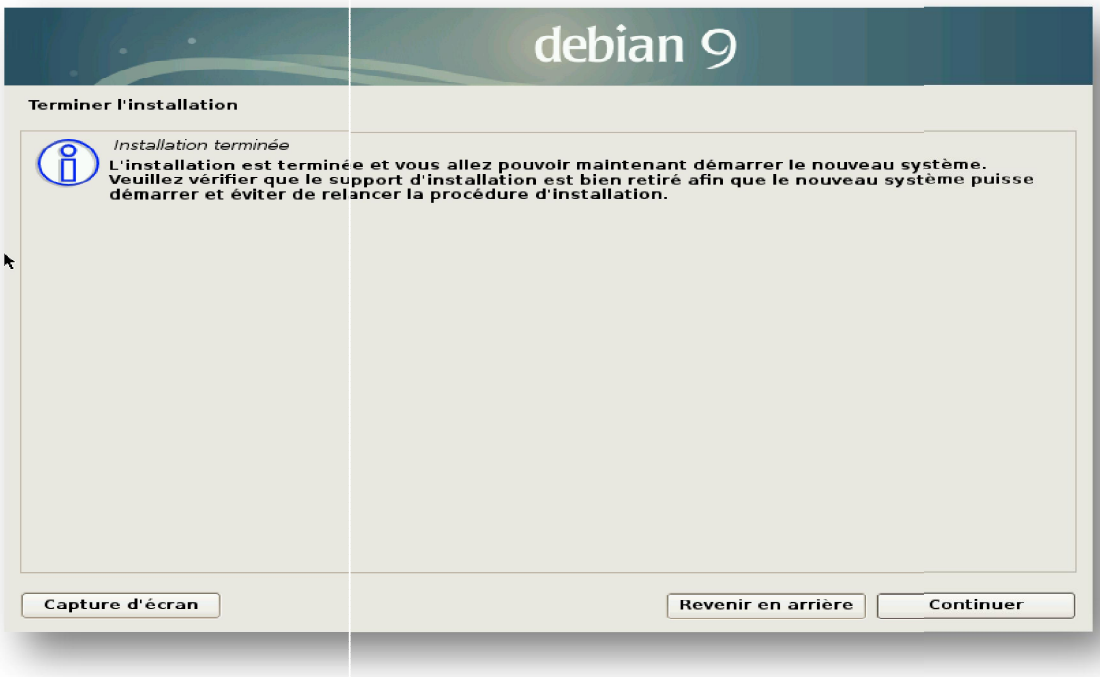

Figure 23 : *Installation terminée*

✓ **Etape 25 :** Le premier démarrage de Debian9 :

Figure 24 : *Démarrage de debian*

✓ **Etape 26 :** Le système est donc installé, voici l'ouverture de la session :

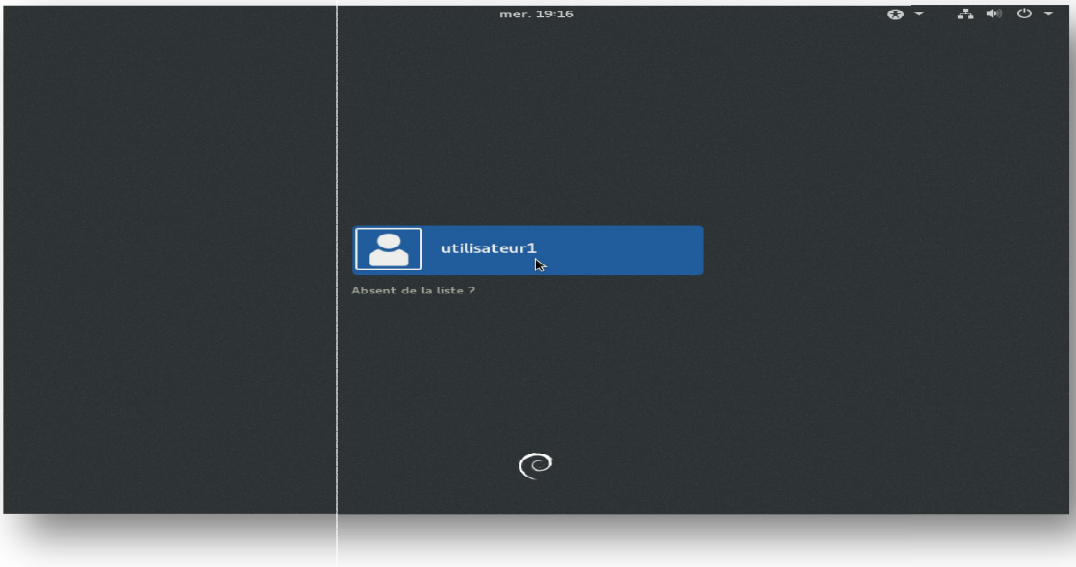

Figure 25 : *Ouverture de la session*

Glossaire

A :

AES : Standard d'**E**ncodage **A**vancé

ARP: Address **R**esolution **P**rotocol

C:

CD : Disque **C**ompact

D:

DES : Data **E**ncryption **S**tandard

DMZ: Demillitarized **z**one

DOS: Disk **O**perating **S**ystem

DVD: Digital **V**ersatelite **D**isk

F:

FTP: File **T**ransfer **P**rotocol

G:

GPL: General **P**ublic **L**icense

H:

HTTP: Hyper **T**ext **T**ransfer **P**rotocol

HTTPS: Hyper **T**ext **T**ransfer **P**rotocol **S**ecure

I:

IDS: Intrusion **D**etection **S**ystem

2INT : Institu **I**nternational des **N**ouvelles **T**echnologies.

IP: Internet **P**rotocol

IPS: Intrusion **P**revention **S**ystem

IPv4: Internet **P**rotocol **v**ersion 4

ISO: International **O**rganization for **S**tandardization

IT: Internet **T**echnology

L:

LAMP: Linux, **A**pache, **M**ySQL, **P**HP.

LAN: Local **A**rea **N**etwork

M:

MAC: Media **A**ccess **C**ontrol

MAC Spoofing: **M**edia **A**ccess **C**ontrol **S**poofing

MAN: Metropolitan **A**rea **N**etwork

MAMP: Mac Os **A**pache **M**ySQL **P**HP

MITM: Men **I**n **T**he **M**iddle

N:

NAS: Network **A**ttached **S**torage

NAT: Network **A**ddress **T**ranslation

O:

OSI: Open **S**ystems **I**nterconnexions

P:

PC: Personal **C**omputer

PHP: Hypertext **P**reprocessor

S:

SGBD: Système de **G**estion de **B**ases de **D**onnées

SQL: Structured **Q**uery **L**anguage

SSL: Secure **S**ocket **L**ayer

T:

TCP: Transmission **C**ontrol **P**rotocol

TLS: Transport **L**ayer **S**ecurity

U:

UDP: User **D**atagram **P**rotocol

URL: Uniform **R**esource **L**actor

USB: Universal **S**erial **B**us

V:

Vcard : Visit **C**ard

VLAN: Virtual **L**ocal **A**rea **N**etwork

VOIP: Voice Over **IP**

VPN: Virtual **P**rivate **N**etwork

VSFTPd:Very **S**ecure **FTP D**aemon

W:

WAMP: Windows **A**pache **M**ySQL **P**HP.

WAN: Wide **A**rea **N**etwork

WWW: World **W**ide **W**eb