N° d'ordre : 467/RS/TCO Année universitaire : 2017 / 2018

UNIVERSITÉ D'ANTANANARIVO

INSTITUT D'ENSEIGNEMENT SUPERIEUR
ANTSIRABE VAKINANKARATRA (IES-AV)

MENTION TELECOMMUNICATION

MEMOIRE

en vue de l'obtention

du diplôme de LICENCE

Domaine : Science de l'Ingénieur

Mention : Télécommunication

Parcours : Réseaux et Systèmes

Par : **RAELINIAINA Tsirisoa**

Titre : CONCEPTION D'UNE SOLUTION DE SAUVEGARDE DE DONNEE AVEC ELKARBACKUP (cas de l'Alternateeve Technology Lab)

Soutenu le 29 avril 2019 à 10 heure devant la commission d'examen composée de :

Président de Jury **:** ***ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécom***

Examinateurs **:**

RASOANAIVO Andrianirina, Master à visée de Recherche

RALAIBOZAKA Tahina, Assistante d'Enseignement Supérieur

Directeur de mémoire : **RAKOTONDRAMANANA Radiarisainana Sitraka, Master à visée de Recherche**

TENY FISAORANA

Alohan’ny zavatra rehetra dia misaotra an’Andriamanitra lehibe nohon’ny fahasoavany sy ny famindram-pony izay nahafahana nanatanteraka izao famaranana ny fianarana izao.

Tolorana fisaorana lehibe ihany koa:

- Andriamatoa RAMANOELINA Panja, Talen’ny oniversite Antananarivo.
- Andriamatoa RAJAONARISON Eddy Frank, Talen’ny anjerimanontolo eto Vakinankaratra.

Hisaorana indrindra ihany koa andriamatoa ANDRIANAIVONDRIAKA Nirina Alain, Dokotera amin’ny fifandraisan-davitra izay nanaiky handrindra sy hitsara izao fotoana sy asa izao.

Hankasitrahana feno koa Andriamatoa RAKOTONDRAMANANA Radiarisainana Sitraka, mpampianatra mpikaroka sady talen’ny fanatanterahana ny boky, izay nandany fotoana sy nanampy ary nanitsy tamin’ny zavatra rehatra.

Mankasitraka indrindra ny mpikamban’ny mpitsara izay voalaza anarana eto ambany ihany koa izay nanaiky nitsara ity asa ity :

- Andriamatoa RASOANAIVO Andrianirina, mpampianatra mpikaroka
- Ramatoa RALAIBOZAKA Tahina Nancy, mpampianatra eo anivon’ny sampam-pampianarana ambony.

Fisaorana manokana koa no atolotra an’ Andriamatoa RATRIMOSOA Radomalala Eugène, Talen’ny orinasa Alternateeve Technology Lab sy ny ekipa rehetra miaraka aminy izay namela ahy hanatanteraka ny fianarana asa tao amin’ny orinasa ary niara-nifandrimbona tamin’ny fanatanterahana ara-teknika rehetra. Indrindra ny torohevitra sy ny fanampiana izay isan’ny mampahomby izao asa izao.

Ary farany nefa tena lehibe indrindra dia ianareo Ray aman-dReny, fianakaviana ary namana rehetra, ianareo no toko telo mahamasa-nahandro miombona amin’ireo mpanabe izay nanosika sy nampahery mandrakariva mba hahatontosa ny fianarana antasakany sy andavany, koa dia misaotra sy mankasitraka indrindra tompoko. Andriamanitra mana-karem-pahasoavana anie hamaly ny soa vitanareo.

REMERCIEMENTS

Avant tout, je glorifie Dieu Tout Puissant pour sa grâce d'avoir planifié toute ma mémoire et de m'avoir donné Sa bénédiction pour que je puisse tout réaliser.

Mes sincères remerciements à :

- Monsieur RAMANOELINA Panja, Directeur de l'université d'Antananarivo.
- Monsieur RAJAONARISON Eddy Franck, Directeur de l'Institut d'Enseignement Supérieur Antsirabe Vakinankaratra (IES-AV).

J'adresse mes vifs remerciements à Monsieur ANDRIANAIVONDRIAKA Nirina Alain, Président de jury qui m'a permis la réalisation de ma mémoire et qui a fait l'honneur de présider cette soutenance.

Ma gratitude et ma reconnaissance les plus sincères à Monsieur RAKOTONDRAMANANA Radiarisainana Sitraka, Directeur de mémoire qui est toujours disponible et m'a beaucoup aidé pendant la réalisation.

Je suis très reconnaissante aussi envers les membres de jury suivants, qui ont accepté d'examiner ce travail et consacré leur temps à assister à cette présentation, ainsi qu'envers tous les enseignants du Mention télécommunication :

- Monsieur RASOANAIVO Andrianirina, Master à visée de Recherche.
- Madame RALAIBOZAKA Tahina Nancy, Assistante d'Enseignement Supérieur.

J'exprime également ma gratitude à Monsieur RATRIMOSOA Radomalala Eugène ainsi que les équipes de l'Alternateeve Technology Lab qui ont beaucoup contribué au succès de mon stage et qui m'ont aidé lors de la réalisation de ce mémoire. Vos conseils ont été très enrichissants, très indispensables et qui sont la source de ladite réalisation.

Particulièrement mes vifs remerciements à mes très chers Parents qui m'ont toujours encouragé et donné la chance de poursuivre mes études. Votre soutient m'a aidé à persévérer.

Enfin, je ne peux minimiser aides et conseils de la part de mes proches parents ainsi que mes amis. Mes remerciements les plus chaleureux.

TABLE DES MATIERES

NOTATIONS ET ABREVIATIONS

1. Minuscules latines

h	Fonction de hachage
m	Entier naturel
n	Entier naturel

2. Majuscules latines

H	Application de fonction de hachage
M	Message claire
M_0	Message claire diffèrent de M

3. Abréviations

AAL	ATM Adaptation Layer
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Control Protocol
DMZ	Demilitaries Zone
DNS	Domain Name System
EGP	Exterior Gateway Protocol
ETR	Early Token Release
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
Gbps	Gigabits
GHz	Gigahertz
Go	Gigat octet

Host ID	Host Identity
HTML	Hypertext Mark-Up Language
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machine Corporation
ICMP	Internet Control Message Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
Kbit/s	Kilobits par segonde
Ko	Kilo octet
LAN	Local Area Network
MAC	Message Authentifcation Code
MAC	Media Access Control
MAN	Metropolitan Area Netowrk
MDC	Manipulation Détection Code
MD4	Message Digest 4
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
Mod	Modulo

MPLS	MultiProtocol Label Switching
MYSQL	My Structured Query Langauge
Net ID	Network Identity
NIST	Standards and Technology
NS	Name Server
OSI	Open System Interconnexion
PAN	Personal Area Network
PC	Personal Computer
PDF	Portable Document Format
PDH	Plesiochronous Digital Hierarchy
PGCD	Plus Grand Commun Diviseur
PHP	Préprocesseur Hypertexte
PHY	Physique
POP	Post Office Protocol
RARP	Reverse Adress Resolution Protocol
RFC	Representational State Transfer
RSA	Ron Rivest AShamir
SDH	Synchrone Digitale Hierarchie
SGBD	Système de Gestion de Bases de Données
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Managemen0t Protocol
SQL	Structured Query Languag0e
SONET	Synchronous Optical Network

SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TELNET	Tele Network
TLS	Transport Layer Security
TLS	Transport Layer Security
To	Téra octet
TPDDI	Twisted Pair Distributed Data Interface
TTL	Time To Live
UDP	User Datagram Protocol
UIT	Union International Télécommunication
URL	Uniform Resource Locator
USB	Universal Serial Bus
V	Volt
VTY	Virtual Terminal
WAN	Wide Area Network
WIFI	Wireless Fidelity
WPAN	Wireless Personal Area Network
WWW	World Wide Web

LISTES DES TABLEAUX ET DES FIGURES

1. Liste des tableaux

2. Liste des figures

INTRODUCTION GENERALE

Auparavant, les données font partie des matériels utilisés par les entreprises pour le fonctionnement de leur tâche, en cas de perte ou destruction, le renouvellement est la solution apportée pour récupérer toutes les données. Mais actuellement elles constituent un des grands trésors incontournables à protéger, elles sont plus coûteuses qu'une vie humaine. L'existence de plusieurs entreprises dépend de son bon fonctionnement et sa disponibilité. L'optimisation de la sauvegarde est la méthode la plus pratique pour les protéger et les récupérer.

Malgré tout, la sauvegarde sur des supports physiques classiques conservés dans les locaux même de l'entreprise présente des limites et des risques ; des limites comme la perte ou destruction des données par erreur, l'indisponibilité des données, et le piratage. Les supports physiques ne garantissent pas une récupération totale des données en cas d'incident. La perte et le temps d'arrêt de données peuvent suffire pour qu'une entreprise ferme ses portes.

C'est pourquoi une solution plus performante de sauvegarde est apporté pour répondre à ses besoins et pour résoudre ses problèmes. Les objectifs principaux de ce mémoire constitut à une meilleure organisation de réseau de sauvegarde dans une entreprise, leur sécurité contre les intrus et la récupération totale des données en cas de perte ou endommagement. Au cours du stage du mois de novembre 2018 au mois de février 2019 dans la société Alternatteve Technology Lab que l'essai de la mise en place a été effectué.

Ce travail s'intitule « CONCEPTION D'UNE SOLUTION DE SAUVEGARDE DE DONNEE AVEC ELKARBACKUP (cas de l'alternateeve Technology Lab) »

Le travail est divisé en trois grands chapitres. Le premier chapitre parle du réseau d'entreprise, ce qui détaille les différents réseaux qui existent, les normalisations et les fonctionnements de chaque protocole, puis la mise en place du réseau, ce qui résume l'utilité du réseau dans une entreprise. Le deuxième chapitre explique la technique de sauvegarde, qui illustre les différents types de sauvegarde, les techniques utilisées pour sauvegarder et la sécurisation des données, ce qui résume l'utilité de la sauvegarde et comprendre les techniques de fonctionnement. Ensuite, dans le troisième chapitre la technique de sauvegarde pour résoudre les problèmes de désastre dans une entreprise, ce qui conclue la solution de sauvegarde apporté dans une entreprise.

CHAPITRE 1
NOTIONS SUR LES RESEAUX D'ENTREPRISE

1.1 Introduction

Le réseau existe depuis longtemps, destiner à transporter des informations. Pendant longtemps, cette communication s'est faite directement par l'homme, comme dans le réseau postal. Il y a un peu plus d'un siècle, la première révolution des réseaux a consisté à automatiser le transport des données. Il y a plusieurs types de réseau selon la fonction et l'utilisation. Il existe trois grandes catégories des réseaux : les réseaux de télécommunication, les réseaux informatiques et les réseaux vidéo. Le réseau d'entreprise fait partie des réseaux informatiques. Les protocoles et les normes sont utilisé pour garantir l'échange. Ce chapitre explique la généralité sur les réseaux qu'utilisent les entreprises et illustre les différentes techniques de fonctionnement, la mise en place du réseau dans une entreprise est aussi détaillée.

1.2 Définition

Définition 1.01 :

Le réseau d'entreprise est l'infrastructure qui assure la communication dans une entreprise, il permet de relier chaque ordinateur entre eux via un serveur qui va gérer l'accès internet, les mails, les droits d'accès des donnés partagés et les travails. L'entreprise a besoin du réseau pour centraliser ses données, les sécuriser et pour permettre aussi le travail en équipe. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe est authentifié par le serveur. L'utilisateur peut accéder aux données et aux partages des fichiers. Ce qui résume que le réseau est né pour échanger des informations de manière simple et rapide entre machines. Le réseau a aussi pour objectifs de :

- Partager les ressources : un utilisateur peut changer de poste de travail sans pour autant devoir transporter ses fichiers sur des supports de stockage, circulation des données.
- Accroître la résistance aux pannes : maintenance d'un ordinateur à partir d'un autre.
- Économiser les ressources comme argent et temps.
- Sécurisation des données : protection contre les intrus et les espions.
- Sauvegarde et restauration : récupération des données en cas de panne ou désastre.

Le réseau est mis en place dans le but de transférer des données d'un système à un autre ou de fournir des ressources partagées comme par exemple les serveurs, les bases de données et l'imprimante sur le réseau. Les réseaux sont classifiés selon la taille et la portée de l'entreprise.

1.3 Différentes categories du réseaux

Le réseau est différencié selon la dimension géographique qui la contienne : [1.02]

- Les réseaux PAN (Personal Area Network)
- Les réseaux LAN (Local Area Network)
- Les réseaux MAN (Metropolitan Area Network)
- Les réseaux WAN (Wide Area Network)

1.3.1 Réseaux PAN

Les réseaux PAN permettent de faire l'échange de données des appareils modernes comme les smartphones, tablettes, ordinateurs portables et les ordinateurs de bureau, on parle aussi de réseau domestique. Les techniques de transmission courantes sont l'USB (Universal Serial Bus).

Le réseau personnel sans fil WPAN (Wireless Personal Area Network) repose sur des technologies comme le Bluetooth, USB sans fil. Les WPAN et les PAN ne couvrent généralement que quelques mètres et ne sont pas adaptés pour connecter des appareils se trouvant dans des pièces ou bâtiments différents. Ce réseau a les possibilités d'utilisé la bande de spectre sans licence de 2.45 GHz, utilisation d'une couche MAC jusqu' à 100 Kbit/s, connexion de seize machines au moins et la mode sans connexion. La figure suivante représente un ordinateur connecté à des périphériques comme le smartphone, le tablette, le téléphone et l'imprimante. [1.02]

La structure d'un réseau PAN est représentée par la Figure 1.01 ci-dessous :

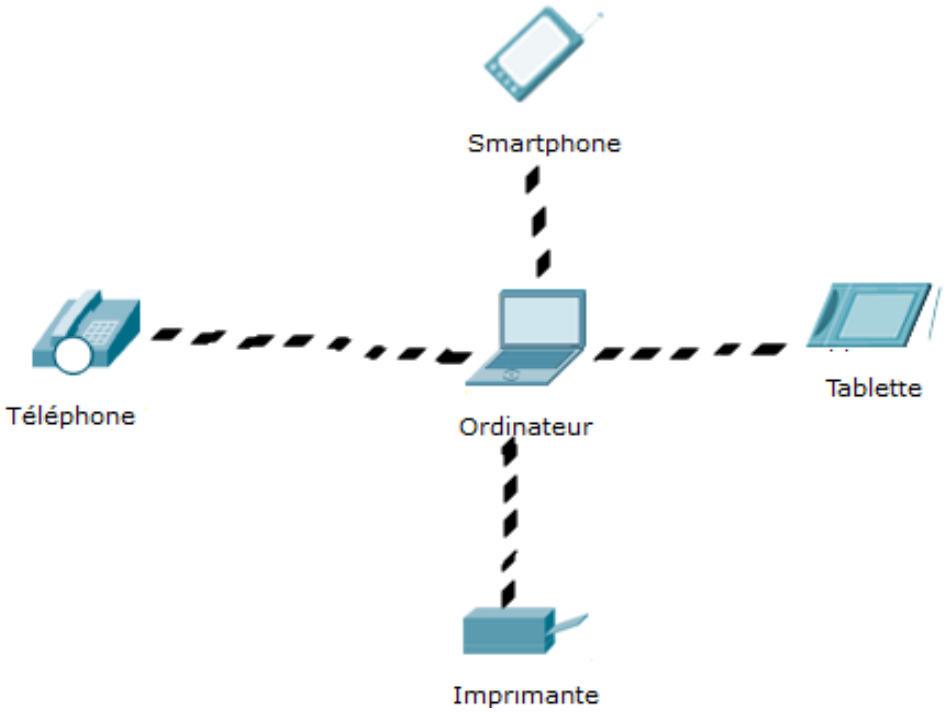


Figure 1.01 : *Structure d'un réseau PAN*

1.3.2 Réseaux LAN

Si plusieurs ordinateurs doivent être réunis sur un réseau, cela se fait généralement sous la forme d'un réseau local ou LAN. Les réseaux locaux peuvent couvrir d'une salle jusqu'à 1km de région : cas dans un établissement, dans un bâtiment ou dans un campus. Ils interconnectent physiquement des unités adjacentes, en utilisant des équipement réseaux comme le concentrateur (ou hub) qui permet de concentrer le câblage en un point provenant de plusieurs lignes, le pont (ou bridge) qui permet de filtrer les trames et laisse passer les blocs destinés au réseau raccordé et commutateur réseau (ou switch) pour le couplage des matériels. Les ordinateurs sont gérés par le serveur, par exemple les clients envoient une requête au serveur d'imprimer un document.

La portée d'un réseau LAN est tributaire de la norme utilisée et du support de transmission, pouvant être augmenté par l'amplificateur de signal. Une plage de signal de plusieurs kilomètres est possible avec Gigabit Ethernet. Cette catégorie de réseau est le plus utilisé dans les entreprises. Comme la figure ci-dessous montre le réseau LAN est composé par exemple des ordinateurs, des imprimantes liées par un équipement informatique et connecté par un serveur. [1.02]

La structure d'un réseau LAN est représentée par la Figure 1.02 :

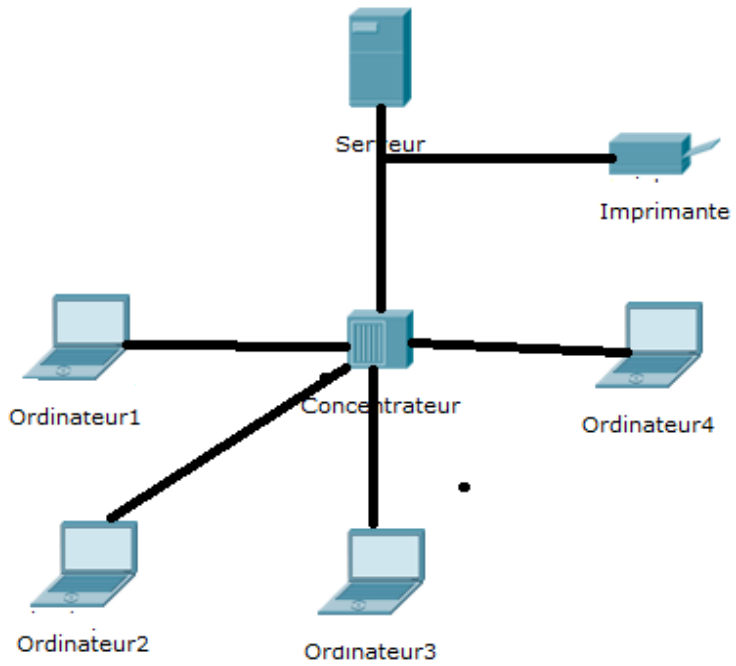


Figure 1.02 : *Structure d'un réseau LAN*

1.3.3 Réseaux MAN

Les réseaux MAN ou réseaux métropolitain est un réseau de télécommunication à large bande qui relie plusieurs LAN. Les routeurs de haute performance et les connexions de fibres optiques hautes performances sont utilisés, ce qui permet de fournir un débit de données beaucoup plus élevées.

La vitesse de transmission entre deux nœuds (routeur) éloignés est comparable à la communication dans un réseau local. L'infrastructure pour le MAN est assurée par les opérateurs de réseaux internationaux. En tant que réseau métropolitain, les villes câblées peuvent être intégrées dans les réseaux étendus WAN. En cas de besoin de relier deux entreprises par exemple. [1.02]

La structure d'un réseau MAN est représentée par la Figure 1.03 ci-dessous :

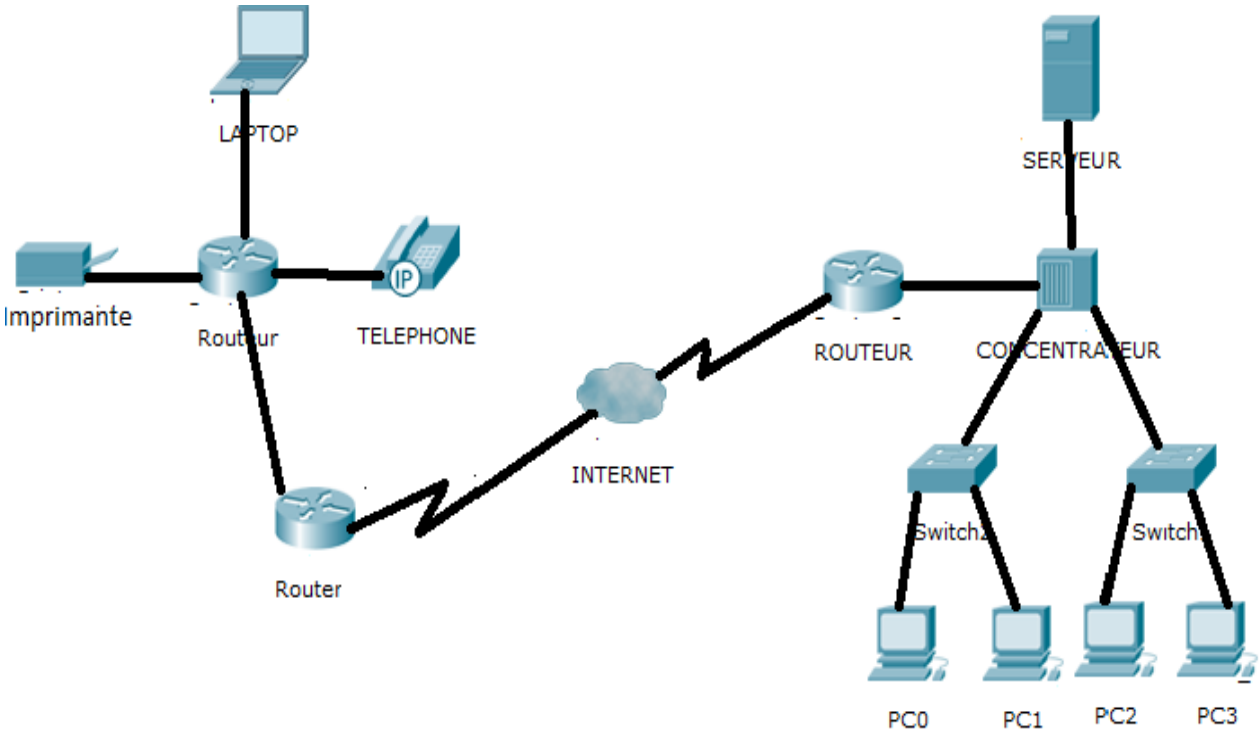


Figure 1.03 : *Structure d'un réseau MAN*

1.3.4 Réseaux WAN

Les réseaux WAN ou réseaux étendus couvrent des vastes zones géographiques à l'échelle d'un pays ou d'un continent par exemple. En principe, le nombre de réseaux locaux ou d'ordinateurs connectés à un réseau étendu est illimité. Ils utilisent des techniques comme MPLS (MultiProtocol Label Switching) qui assure l'intégrité des protocoles IP, PDH (Plesiochronous Digital Hierarchy) qui assure le transport direct des trames sur les support physique, SDH (Synchrone Digitale Hierarchie) et SONET (Synchronous Optical Network) prend en compte la numérisation de la parole avec échantillonage, ATM (Asynchronous Transfer Mode) pour le contrôle des paquets perdues et l'assurance des qualités de services. Les réseaux étendus sont généralement détenus par une organisation ou une entreprise et sont donc exploités en privé ou loués, ils peuvent relier plusieurs entreprises dans le monde. Par exemple le fournisseur de service internet utilise le WAN, qui relie plusieurs serveurs dans une zone contenant un point d'accès. Ce type de réseau utilise le protocole Ethernet pout transporter les trames sur des longues distances.

La structure d'un réseau WAN est représentée par la Figure 1.04 :

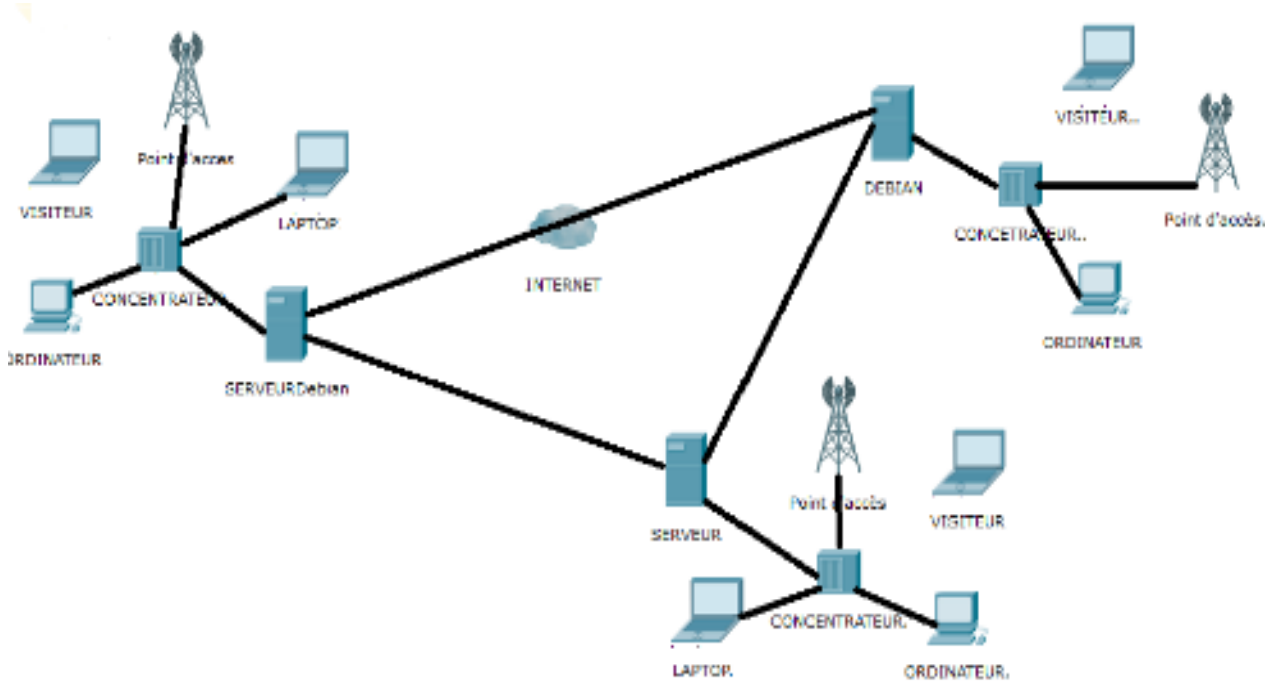


Figure 1.04 : *Structure d'un réseau WAN*

1.4 Normalisation utilisée par les réseaux

Définition 1.02 :

La normalisation des réseaux permet aux réseaux de différente entité de se communiquer entre eux. Prenons l'exemple d'un réseaux WAN, pour permettre la communication des différentes réseaux LAN dans le WAN, Il leur faut d'avoir un même langage, c'est là que naît la création du modèle Open Système Interconnexion ou OSI (Open System Interconnexion) de L'International Organization of Standardization ou ISO. Et puisque le fonctionnement de ce dernier n'a pu satisfaire aux besoins c'est là que naît le modèle TCP/IP (Transfert Control Protocole/ Internet Protocol). [1.03]

1.4.1 Modèle OSI

Définition 1.03 :

Le modèle OSI est le premier modèle standard utilisé pour assurer la compatibilité ou l'interopérabilité entre les équipements réseaux hétérogènes. Ainsi tous les équipements, ou ensemble d'équipements à interconnecter deviennent un système ouvert s'il respecte les normes d'interconnexions. Le modèle OSI est une architecture abstraite de communication, décrit dans la norme X.200 de l'UIT (Union International Télécommunication). Il est composé de sept couches, chacune remplissant une partie bien définie des fonctions permettant l'interconnexion. [1.04]

La représentation du sept couches du modèle OSI est représenté par la Figure 1.05 :

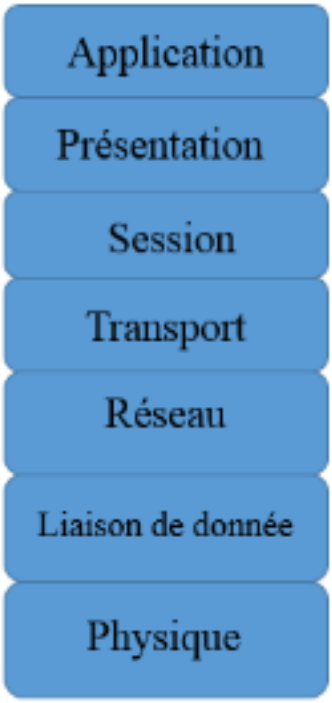


Figure 1.05 : *Sept couches du modèle OSI*

1.4.1.1 Couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche garanti la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie…), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données. L'unité d'information typique de cette couche est la trame binaire, représenté par une certaine différence de potentiel.

1.4.1.2 Couche liaison de donnée

Cette couche transforme la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cette couche est capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission c'est à dire détecter et corriger les erreurs intervenues sur la couche physique.

Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur. L'unité d'information de la couche liaison de données est la trame qui est composée de quelques centaines à quelques milliers d'octets maximum.

1.4.1.3 Couche réseaux

C'est la couche qui permet de gérer le sous-réseau c'est à dire le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, la détermination du mécanisme de routage et le calcul des tables de routage (tables statiques ou dynamiques) sont importante. La couche réseau contrôle également l'engorgement du sous-réseau. L'unité d'information de la couche réseau est le paquet.

1.4.1.4 Couche transport

Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche est aussi responsable :

- Acheminement des messages complets au destinataire et effectue le réassemblage du message à la réception des morceaux.
- Optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.
- Fournir à la couche session et aux utilisateurs du réseau le service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la foi. Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau. L'unité d'information dans la couche transport est le message.

1.4.1.5 Couche session

Cette couche synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue. Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

Cette couche a pour rôle de transmettre cette fois les informations de programmes à programmes.

1.4.1.6 Couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

1.4.1.7 Couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie.

Le modèle OSI est peut-être trop complet et trop complexe. La distance entre l'utilisation concrète (l'implémentation) et le modèle est parfois importante. En effet, peu de programmes peuvent utiliser ou utilisent mal l'ensemble des 7 couches du modèle : les couches session et présentation sont fort peu utilisées et à l'inverse les couches liaison de données et réseau sont très souvent découpées en sous-couches tant elles sont complexes.

OSI est en fait trop complexe pour pouvoir être proprement et efficacement implémenté. Le comité rédacteur de la norme a même dû laisser de côté certains points techniques, comme la sécurité et le codage, tant il était délicat de conserver un rôle bien déterminé à chaque couche ainsi complétée. Ce modèle est également redondant (le contrôle de flux et le contrôle d'erreur apparaissent pratiquement dans chaque couche) au niveau de l'implémentation, c'est pourquoi on a adopté la norme TCP/IP qui est beaucoup plus optimisée et efficace.

1.4.2 Modèle TCP/IP

Définition 1.04 :

Le protocole TCP/IP est la langue de communication élémentaire qu'utilise Internet. TCP/IP sert aussi de protocole de communication sur les réseaux privés, de type intranet ou extranet. TCP/IP est un programme à deux couches : la couche supérieure et la couche inférieure. La couche supérieure, le protocole de contrôle de transmission (TCP), gère la division d'un message ou d'un fichier en paquets plus petits, qui sont alors transmis via Internet, puis reçus par une autre couche TCP qui réassemble les paquets pour reconstituer le message d'origine. La couche inférieure, le protocole Internet (IP), gère l'adresse de chaque paquet pour garantir que chacun arrive à destination. Chaque ordinateur passerelle du réseau consulte cette adresse pour transférer le message. TCP/IP utilise le modèle de communication client/serveur. [1.04]

La représentation du modèle TCP/IP est représentée le suivant :

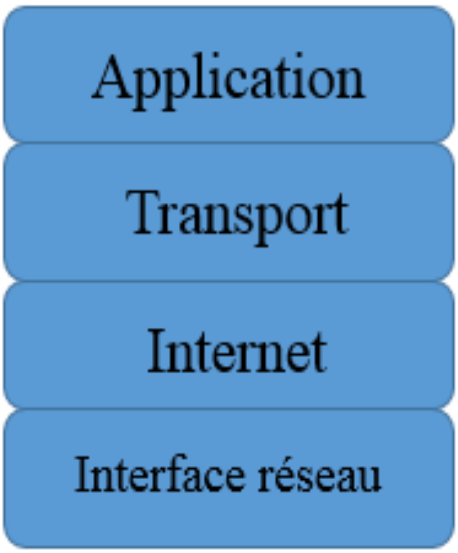


Figure 1.06 : *Quatre couche du modèle TCP/IP*

1.4.2.2 Couche interface réseaux

Cette couche intègre les services des couches physiques et liaison de donnée du modèle OSI. Elle a en charge la communication avec l'interface physique dans le but de transférer ou de récupérer les paquets qui lui sont transmis de la couche Internet. Cet interfaçage peut être assuré par divers protocoles. Mais cela dépend du réseau utilisé (Ethernet en LAN, X25 en WAN).

1.4.2.3 Couche internet

La couche internet réalise l'interconnexion des réseaux distants sans connexion. Elle permet de faire l'injection de paquets dans les réseaux et assure l'acheminement de ces paquets indépendamment les uns des autres jusqu' à la destination. Cela intègre alors en lui la fonction de routage et de commutation de paquets à travers différents nœuds par rapport au trafic et à la congestion du réseau. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'utilisateur qui souhaite émettre sur internet doit ranger ses données dans des paquet IP.

1.4.2.4 Couche transport

Cette couche, comme celle du modèle OSI, gèrent le fractionnement et le réassemblage en paquets du flux de données à transmettre. Ainsi, elle est chargée de l'ordonnancement des paquets à l'arrivée après la commutation. En plus elle prend aussi en charge les questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. Les principaux protocoles qui assurent les services de cette couche sont le protocole TCP (Transmission Control Protocol) et le protocole UDP (Unit Datagram Protocol).

1.4.2.5 Couche application

La couche application gère les protocoles de haut niveau : représentation, codage et contrôle de dialogue. Elle correspond aux différentes applications utilisant les services réseaux pour communiquer à travers un réseau. Un grand nombre de protocoles de haut niveau permettent d'assurer les services de cette couche, comme : Telnet, FTP (File Transfer Protocol), HTTP (HyperText Transfert Protocole).

1.5 Protocoles correspondent aux normes

Les protocoles sont l'ensemble de règles à respecter aux deux extrémités communicantes d'un réseau pour que le transport d'information soit possible parce que les données ne sont pas transmises telles quelles est. Ce sont les différents protocoles sont mise en charge pour garantir leur fonctionnement et leur interconnexion que chaque couche a ses protocoles correspondants. Les protocoles sont implantés dans tous les équipements du réseau (machines et routeurs). Il comprend la définition du plan d'adressage, la structure des informations transférées (le datagramme IP) et les règles de routage. Ils sont acheminés à travers l'interconnexion, en fonction des adresses IP publiques (source et destination). Les différents routeurs choisissent un chemin à travers les réseaux. [1.05]

Les protocoles correspondants à chaque couche sont représentés par la Figure 1.07 :

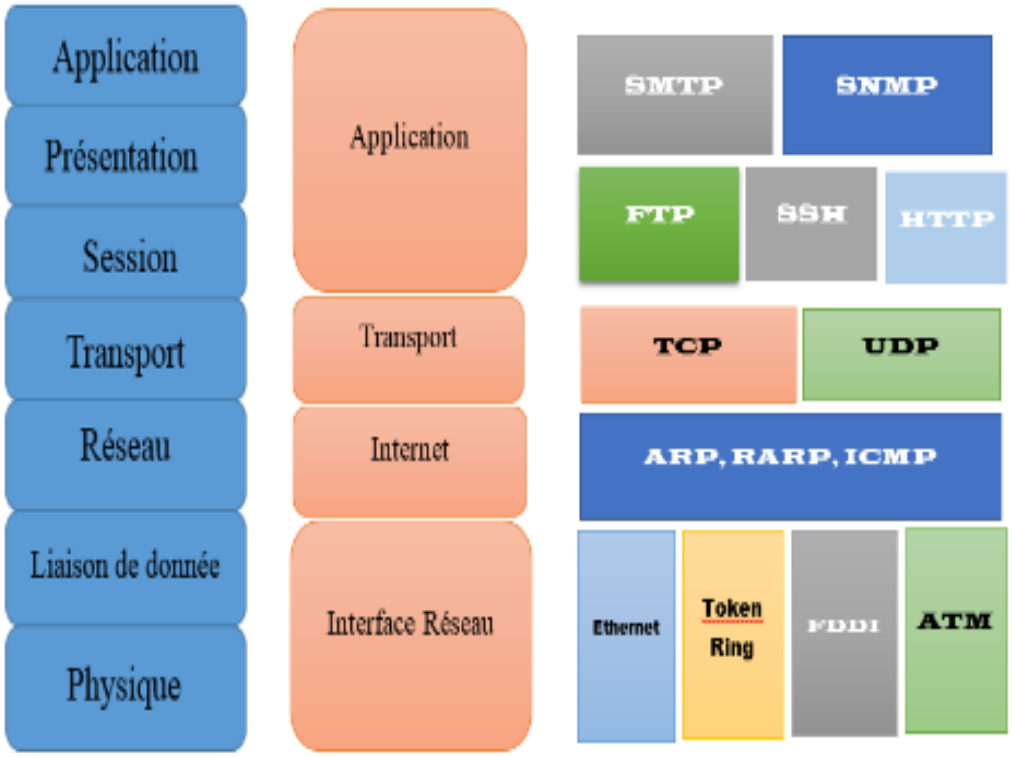


Figure 1.07 : *Protocoles correspondants aux normes*

1.5.1 Protocoles Ethernet, Token Ring, FDDI, ATM

Tableau 1.01 : *Définitions et rôles des protocoles Ethernet, Token Ring, FDDI, ATM*

Protocoles	Définitions	Rôles
Ethernet	L'Ethernet est un protocole à une norme de réseau local à commutation de paquets.	Protocole mise en charge pour la transmission des données.
Token Ring	Le Token Ring ou IEEE 802.5 est un protocole utilisé par la topologie en anneau, c'est un cas particulier d'une liaison multipoint, il implique une circulation unidirectionnelle des messages.	Emettre le jeton transmis à la station qui suit physiquement celle qui le détient (jeton non adressé). [1.07]
FDDI (Fiber Distributed Data Interface)	FDDI est un réseau en anneau optique sur fibre optique multimode. Le débit nominal est de 100 Mbit/s pour une distance maximale de 100 km (200 si l'on tient compte du double anneau). FDDI supporte jusqu'à 1 000 stations, distantes l'une de l'autre de moins de 2 km. Une version de FDDI sur paire torsadée TPDDI (Twisted Pair Distributed Data Interface) autorise des débits de 100 Mbits sur 100 m.	Emettre des données et génère un nouveau jeton. [1.07]
ATM (Asynchronous Transfer Mode)	L'ATM est une technologie de réseau récente, qui est contrairement à l'Ethernet, token ring, et FDDI, permet de transférer simultanément sur une même ligne les données et les voix.	Permettre le transport de tous les types de message comme la voix, les données et les images, indépendamment du support physique. Il est souvent utilisé avec des fibres optiques monomodes, et généralement déployé à des vitesses de 2,5 Gbps ou 10 Gbps.

1.5.2 Protocoles ARP, RARP, ICMP, IGMP

Tableau 1.02 : *Définitions et rôles des protocoles des couches réseau et internet*

Protocoles	Définitions	Rôles
ARP (Address Resolution Protocol)	Le protocole ARP consiste à la conversion d'une adresse logique (IP) en adresse physique (MAC). Pour transmettre une trame sur internet. le logiciel réseau doit convertir l'adresse IP en une adresse physique.	Déterminer l'adresse d'un équipement à partir de l'adresse de ce même équipement à un autre niveau protocolaire. Dans le cas d'une requête ARP, l'émetteur place son adresse logique dans une réponse ARP, ce champ révèle l'adresse recherchée alors que l'adresse physique du récepteur est vide.
RARP (Reverse Address Resolution Protocol)	Le protocole RARP est un protocole inverse de la protocole ARP, qui permet à une machine d'utiliser son adresse physique ou adresse MAC pour déterminer son adresse logique ou adresse IP. Ce protocole est souvent utilisé entre une machine et un serveur d'adresse.	Son fonctionnement ne diffère pas beaucoup de l'ARP sauf qu'au lieu d'envoyer son adresse IP dans le paquet de requête ARP, on envoie son adresse MAC.[1.08]
ICMP (Internet Control Message Protocol)	Le protocole ICMP est un protocoles de la pile TCP/IP, qui permet de comprendre plus facilement ce qui se passe sur un réseau quand il y a un problème ou des erreurs inattendue.	-Indique automatiquement les erreurs survenues dans un réseau -Fournir des outils pour étudier un problème réseau.

IGMP (Internet Group Management Protocol)	Le protocole IGMP effectue le contrôle de communications entre les membres du groupe de diffusion de réseau. Une machine peut se rattacher à un groupe ou le quitter à tout moment, l'hôte devrait être seulement capable d'émettre et de recevoir des datagrammes en multicast.	-Contrôle de communication -Emmètre et recevoir des datagrammes multicast.

1.5.3 Protocoles TCP et UDP

Tableau 1.03 : *Définitions et rôles des protocoles de couche transport*

Protocoles	Définitions	Rôles
TCP (Transmission Control Protocol)	Le protocole TCP est un protocole complexe qui met en œuvre la détection et la correction d'erreur, gère le contrôle de flux et négocie les conditions du transfert de données. Il est à noter que ce protocole n'est implanté que sur les machines des utilisateurs.	Mode de transfert avec connexion (fiable)
UDP (User Datagram Protoco	Ce protocole permet de découper l'information à transmettre en plusieurs paquets, les transporter les uns des autres et de recomposer le message initial à l'arrivée. Il a besoin des numéros de port des applications pour fournir ses services.	Mode de transfert sans connexion (n'est pas fiable)

1.5.4 Protocoles HTTP, FTP, SNMP, SMTP, RIP

Tableau 1.04 : *Définitions et rôles de protocole application*

Protocoles	Définitions	Rôles
HTTP (HyperText Transfer Protocol)	Le protocole HTTP est un protocole de la couche application qui utilise TCP. L'une des forces de HTTP est sa simplicité grâce à son implémentation du type client-serveur. Le navigateur comme par exemple Firefox est le client de HTTP. Le navigateur utilise le port 80 pour communiquer avec le serveur à travers un port TCP. [1.11]	Transport des messages
FTP (File Transfer Protocol)	Le protocole FTP est un autre protocole de communication. Le port utilisé par défaut est le 21. Les échanges ne sont pas chiffrés. Les serveurs FTP publics peuvent récupérer des fichiers de manière anonyme. C'est également avec ce protocole qu'effectue la possibilité du transfert de site Web chez l'hébergeur. [1.11]	- Envoie et récupération des fichiers sur un serveur. - Possibilité de télécharger des logiciels sur la plupart des sites Internet. - L' installation d'un client FTP permet la connexion au serveur (navigateur comme Firefox)
SNMP (Simple Network Management Protocol)	Le protocole SNMP est un protocole de communication. Le protocole SNMP est un protocole sans connexion, qui adopte le protocole UDP. [1.09]	-Permet aux administrateurs réseaux de gérer le équipement du réseaux, de superviser et de diagnostiquer les problèmes de réseaux et matériels à distance.

SMTP (Simple Mail Transfer Protocol)	Le protocole SMTP est un protocole client-serveur en mode texte. Le 25 est le numéro de port utilisé, qui est généralement utilisé par le serveur pour recevoir une connexion. [1.09]	Automatisation des envois mails pour recevoir des informations. L'envoi des mails met en œuvre d'autres techniques tel que l'usage du DNS, l'encodage MIME ou Multipurpose Internet Mail Extensions et l'envoi de pièces jointes.

1.6 Technique de mise en place du réseau dans une entreprise

La mise en place du réseau dans une entreprise est nécessaire pour permettre l'unification et la facilitation des tâches. L'implémentation du réseau permet de relier chaque ordinateur entre eux via un serveur qui va gérer l'accès à Internet, les mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau peut se connecter avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. Le principal objectif du réseau dans une entreprise est alors l'offre des services aux utilisateurs.

1.6.1 Adressage IP

1.6.1.1 Définition

Définition 1.05 :

La fonction d'adressage est un système d'identification cohérent au sein du réseau pour différencier les équipements terminaux. Dans un réseau TCP/IP, toutes les machines connectées possèdent des adresses qui peuvent les identifier au sein du réseau et par les autres réseaux. Ce sont les adresses IP et les adresse MAC que leur différence est illustrée par le Tableau 1.01. Donc à première étape à faire pour la mise en place du réseau est l'adressage IP. [1.12]

Une adresse IP est décomposée en deux parties :

- La première partie qui contient l'adresse réseau de la machine ; c'est le netID.
- La deuxième partie l'adresse de la machine dans un réseau ; c'est le hostID.

Tableau 1.05 : *Comparaison de l'adresse MAC et l'adresse IP*

	Adresse MAC ou Adresse physique	Adresse IP ou Adresse logique
Localisation	Encapsulées dans l'en-tête et l'en-queue de la trame de la couche liaison de données du modèle OSI	Se trouve dans l'en-tête des paquets échangés
Caractéristique	Composée de 48 bits et représentée par des nombres hexadécimaux	Composée de 32 bits représentés par 4 octets séparés par des points et notés en décimal
Fonctionnalité	Communication des machines dans un même réseau	Communication de deux machines appartenant à deux différents réseaux
Représentation	8C:A9: 82:46:97:6C	192.168.25.2

1.6.1.2 Classes des addresses IP

On distingue deux types de réseaux qu'on peut adresser en IP :

- Le réseau public Internet où chaque équipement connecté possède une adresse unique et enregistrée au niveau mondial. [1.12]
- Les réseaux privés dans lesquels le choix des adresses de chaque réseau est libre et que les adresses ne sont uniques que dans ce réseau. [1.12]

Les adresses IP avec classes concernent les adresses privées. Quatre classes d'adresses existent, différencié par le nombre de réseaux et le nombre de machines, représenter par la Figure 1.08 :

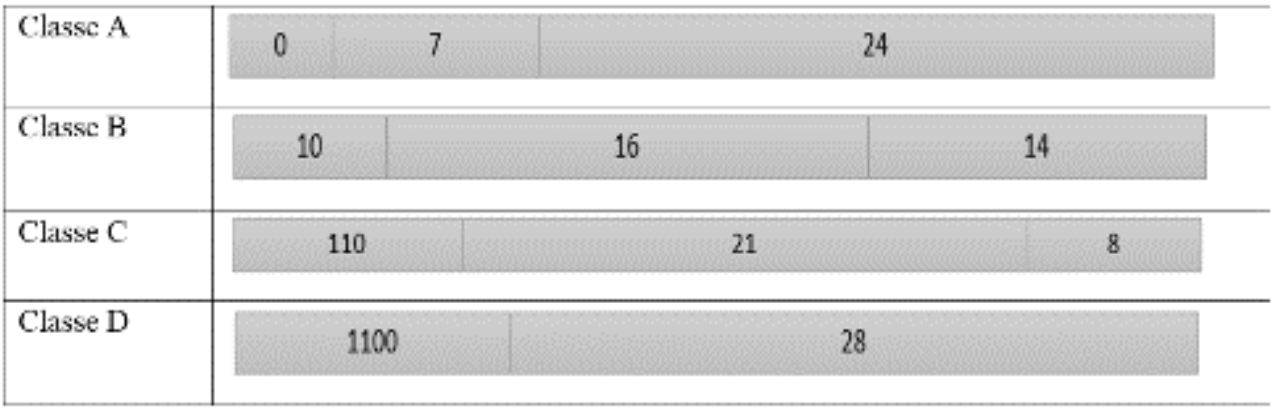


Figure 1.08 : *Classes d'adresse IP*

- Classe A : 7 bits pour les réseaux et 24 pour les hôtes.
- Classe B : 14 bits pour les réseaux et 16 pour les hôtes.
- Classe C : 21 bits pour les réseaux et 8 pour les hôtes.
- Classe D : 28 bits pour les hôtes appartenant à un même groupe.

1.6.2 Interconnexion des machines

Après avoir effectué l'adressage IP, l'interconnexion est la deuxième étape pour lier les nœuds et les terminaux des machines. La topologie est la méthode pour effectuer cette tâche. On distingue trois types de topologies : la topologie en étoile, la topologie en bus et la topologie en anneau. Ils peuvent être combinées pour obtenir des topologies hybrides. [1.06]

1.6.2.1 Topologie en étoile

La topologie en étoile est une technique d'interconnexion qui permet de centraliser toutes les machines à un nœud central, représente la Figure 1.09. Une étoile pouvant jouer le rôle d'un bus ou d'un anneau. Ces caractéristiques la rendent capable de satisfaire aux besoins à la fois des télécoms et de l'informatique. Du fait de sa centralisation, la structure en étoile peut toutefois présenter une certaine fragilité parce que les extensions du réseau sont limitées par la capacité du nœud. [1.06]

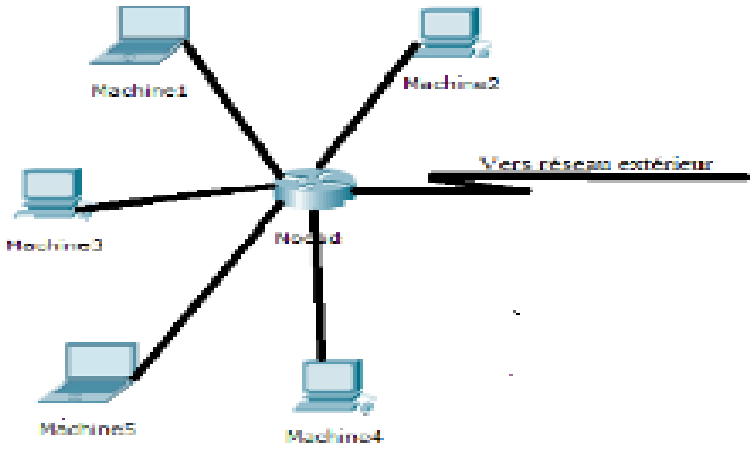


Figure 1.09 : *Topologie en étoile*

Remarque : les nœuds sont les équipements réseaux comme le hub, switch, bridge, routeur.

1.6.2.2 Topologie en bus

La topologie en bus consiste à raccordée les machines à liaison physique commune. La Figure 1.10 représente une topologie en bus, avec un câble sur lequel se connectent de nombreuses machines. Les dispositifs de connexion sur un bus sont passifs, ce qui est un avantage en matière de sécurité. Il est important de noter que ces connexions passive sont simples à réaliser sur câble coaxial ou paire de fils métalliques, réclament cependant des équipements spécifiques sur fibre optique. [1.06]

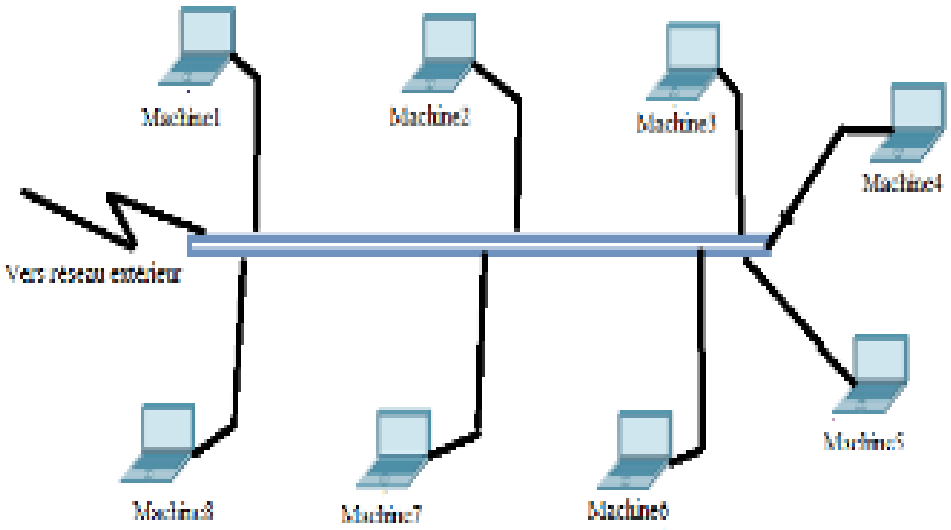


Figure 1.10 : *Topologie en bus*

1.6.2.3 Topologie en anneau

La topologie en anneau consiste à relier les machines de manière à former un circuit boucle comme représente la Figure 1.11 ci-dessous. Les informations circulent dans une seule direction, le long du support de transmission. Alors c'est possible de réaliser un réseau bidirectionnel en utilisant deux anneaux. [1.06]

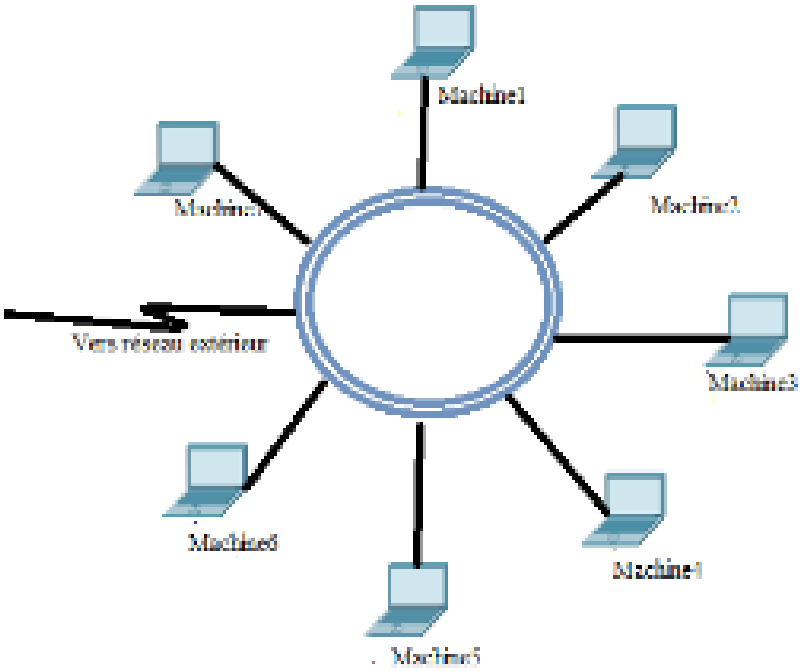


Figure 1.11 : *Topologie en anneau*

1.6.3 Routage

La mise en place du réseau a besoin de la configuration des routeurs. Chaque routeur est connecté directement à deux ou plusieurs réseaux, les utilisateurs étant généralement connectés à un seul réseau. Un routage direct s'effectue lorsque deux machines souhaitant communiquer sont rattachées au même réseau. Elles ont, dans ce cas, le même numéro de réseau IP.

Il peut s'agir de deux utilisateurs ou d'un routeur et d'un utilisateur. Pour envoyer le paquet IP sur le réseau, il suffit de l'encapsuler dans une trame et de déterminer l'adresse physique du destinataire. Si plusieurs chemins existent pour atteindre une destination précise, ils choisissent le plus optimal tout en mettant en réserve un autre meilleur chemin en cas d'indisponibilité du premier.

Il existe deux familles de protocoles de routage dynamique :

- L'IGP ou Interior Gateway Protocol : permet d'acheminer les données à l'intérieur d'un système autonome.
- L'EGP ou Exterior Gateway Protocol : permet de router les données entre différents systèmes autonomes (ensemble de réseaux gérés par un administrateur commun) contrôlés par des administrateurs différents.

1.6.4 Sécurisation

Comme les données d'une entreprise sont privées et ne doivent pas tomber à la portée de tous, le serveur doit protéger l'entreprise des intrusions extérieures. Les machines autorisées et configurés sont les seules à pouvoir accéder. Le serveur est équipé d'un pare-feu qui repousse les intrusions et un antivirus qui permet de se prémunir contre les attaques venant. Le système de cryptage aussi est une meilleure solution que même si l'intrus peut y accéder il ne peut pas lire les fichiers. La sécurisation est très importante dans une structure réseau, la négligence de cette étape entraine un grand danger dans la vie d'une entreprise, alors c'est très important de mettre en place et de sécuriser le réseau. [1.06]

Figure 1.12 : *Sécurisation du réseau*

1.7 Conclusion

Le réseau est un élément très indispensable dans une entreprise, ce qui assure la communication et le partage nécessaire. L'entreprise utilise les différentes catégories des réseaux comme le PAN, LAN, MAN et WAN selon sa dimension géographique convenable à sa disposition. Ces différents réseaux adoptent la normalisation tels que la modèle OSI et la modèle TCP/IP. Cette normalisation est le langage utilisé par différents réseaux pour leurs communications. La modèle OSI ont sept couches qui a chacun ses protocoles correspondants, ses protocoles assurent le fonctionnement des circulations des données et assure la sécurité dans un réseau. Ils ont des rôles très important c'est pourquoi les explications sont longuement étudié. La modèle TCP/IP est l'amélioration de la modèle OSI, il a quatre couches qui fonctionnent également à celle du modèle OSI. Après avoir connu toutes les notions sur le réseau d'entreprise, les techniques de mise en place a été effectué. Ces techniques sont basées sur l'adressage IP, l'interconnexion des machines, le principe de routage et la sécurisation du réseau. On peut conclure que si une entreprise n'est pas mise en réseau, aucune communication n'est faisable. Dans une entreprise, cette communication est parfois le partage des données d'une machine vers un autre, si ces données sont perdues où endommager les communiquant peuvent être en désordre grâce à le faux message arrivé au destinateur. C'est pourquoi le chapitre suivant apporte des solutions de protection ; ce sont la sauvegarde ou backup et la surveillance à l'aide de hachage.

CHAPITRE 2
TECHNIQUE DE SAUVEGARDE OU BACKUP

2.1 Introduction

La première sauvegarde est apparue en 1956, elle était fournie par le RAMAC 350 d'IBM (International Business Machine Corporation) permettait d'enregistrer 5Mo dans une machine qui faisait la taille d'une salle, puis en 1965 permet de stocker quelque dizaine de Mo sur des bandes magnétiques, en plus le disque dur fait son apparition en 1980 qui possède une capacité de 5Mo. Tant que la technologie ne cesse d'évoluer qu'aujourd'hui on trouve même des disques durs externes de 1 To. Mais l'utilisation des disques de stockages ne sont plutôt pas praticable dans une entreprise grâce au partage des données volumineuses qui peut prendre un certain temps, c'est pourquoi il y a naissance du réseau pour faciliter la sauvegarde, le transfert, et aussi la récupération des données. Ce chapitre apporte l'explication à propos de la sauvegarde ainsi que les technologies utilisées, puis ses fonctionnements et enfin la sécurisation des données via à hachage.

2.2 Sauvegarde

Définition 2.01 :

Le terme « Backup » est un mot anglais qui veut dire sauvegarde, c'est-à-dire une action d'enregistrement. La sauvegarde est une action de copie des données ou des bases de données dans le but de les protéger en cas de désastre, notamment la défaillance des équipements pour pouvoir les restaurer en cas de perte. Elle a pour but de faire une copie, récupérer rapidement les données, maintenir les activités de l'entreprise en cas de perte d'information essentielles ainsi que sa sécurisation. Le déploiement d'une solution de sauvegarde permet non seulement de préserver son activité, mais aussi d'assurer une disponibilité continue de ses données pour une meilleure productivité. Comme dans une entreprise, plusieurs ordinateurs fonctionnent en même temps, les données de tous les jours sont alors sauvegardées dans le premier serveur automatiquement utilisant les différents types de logiciels de sauvegarde comme, ElkarBackup, Next Cloud etc.... Tandis que le premier serveur effectue uniquement la sauvegarde des fichiers modifiés, le deuxième serveur effectue la sauvegarde totale de tous les jours ou de toutes les semaines, classifié par la date d'enregistrement. Cette deuxième sauvegarde s'appelle la réplication. Elle utilise le Daemon appelé « cron » qui est un programme tournant en tâche de fonds. Chaque minute, le cron regarde dans un fichier appelé « crontab », alors une commande lance à la date et heure précise de configuration, c'est là que l'exécution commence. [2.01]

La Figure 2.01 suivante représente le fonctionnement de la sauvegarde :

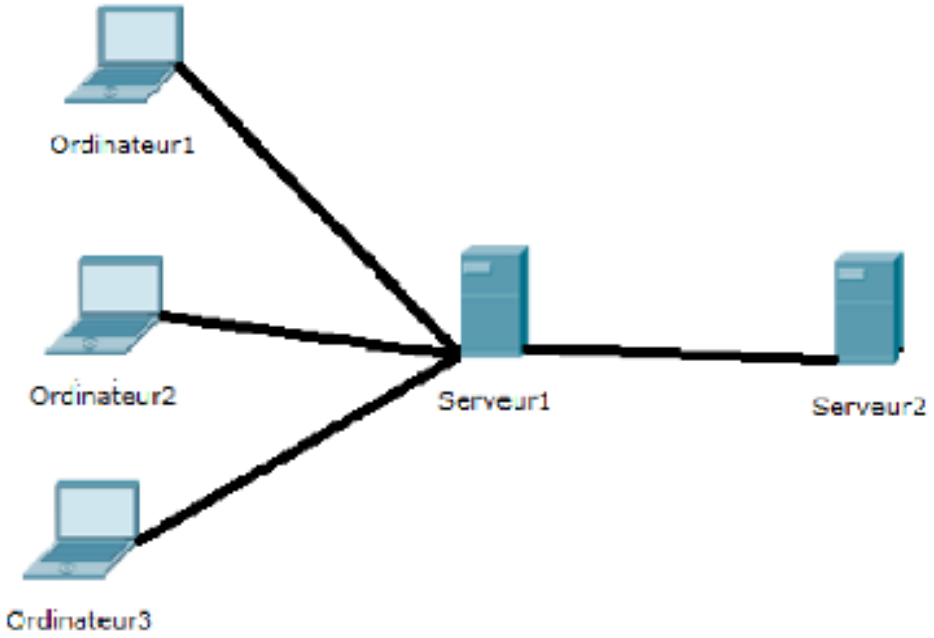


Figure 2.01 : *Fonctionnement de la solution de sauvegarde*

2.2.1 Les types de sauvegarde

2.2.1.1 La sauvegarde complète ou « Full Backup »

La sauvegarde complète est le fait de réaliser l'intégrité de la sauvegarde. Cette méthode est la plus simple à effectuer. Ce type de sauvegarde ne prend pas en compte les tâches effectuées précédemment et est très consommateur en espace, il se fait parfois hebdomadairement ou mensuellement.

Tableau 2.01 : *Exemple d'utilisation de la sauvegarde complète*

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
Complète (1 To)	Complète (1 To)	Complète (1 To)	Complète (1 To)	Complète (1 To)	Complète (1 To)	Complète (1 To)

Avantages :

- Facile à utiliser car la connaissance des techniques est inutile, effectue tout simplement la totalité de la sauvegarde.
- Fiable car son utilisation ne dépend d'aucune autre sauvegarde précédente, alors la restauration des données pourra s'effectuer sans erreur.

Inconvénients :

- L'exécution de cette sauvegarde complète est relativement plus longue que celle des autres types de sauvegarde.
- Besoin d'espace de stockage important, d'après le Tableau 2.01 précédent, on stocke 7 To de backup pour avoir 7 points de restauration.

A noter qu'il a une sauvegarde appelée partielle qu'en cas de défaut de sauvegarde (perte de connexion, erreurs...) les fichiers sauvegardés sont conservés et peuvent être consultés ou restaurés comme toute sauvegarde et constituent donc une sauvegarde « partielle ». Ils peuvent servir de base pour reprendre la sauvegarde complète avec rsync. [2.02]

2.2.1.2 La sauvegarde différentielle ou « Differential Backup»

Après la réalisation d'une première sauvegarde complète, la sauvegarde différentielle consiste à effectuer la sauvegarde de la toute première sauvegarde et l'état actuel des données. Cette méthode requiert moins d'espace que celle du précédente. La restauration de la première puis la dernière sauvegarde est nécessaire.

La sauvegarde différentielle consiste à recourir à la sauvegarde complète, puis ajouter par les modifications suivant comme représente le tableau 2.02 ci-dessous.

Tableau 2.02 : *Exemple d'utilisation de la sauvegarde différentielle*

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
Complète (1 To)	Différentielle 10 Go	Différentielle (10Go+20Go = 30 Go)	Différentielle (30Go+30Go =60Go)	Différentielle (60Go+40Go =100Go)	Différentielle (100Go+50Go =150Go)	Différentielle (150Go+20Go =170Go)

Avantages :

- Moins de consommation d'espace sur le stockage et plus rapide qu'une sauvegarde complète.
- Plus fiable que la sauvegarde incrémentielle. Chaque sauvegarde différentielle comprend toutes les modifications apportées après une sauvegarde complète. Pour restaurer une donnée de mercredi soir, il faudra restaurer la sauvegarde complète (dimanche) puis la sauvegarde différentielle de mercredi = 1.010 To à charger sur 2 sauvegardes (1To + 60Go).

Inconvénients :

- A long terme, la consommation de stockage n'est pas efficace parce que chaque sauvegarde différentielle duplique les données de la précédente sauvegarde et celle du jour. [2.02]

2.2.1.3 La sauvegarde incrémentielle ou « Incremental Backup »

Seuls les éléments ajoutés ou modifiés seront enregistrés depuis la dernière sauvegarde. Tout comme pour la sauvegarde différentielle mais la différence entre la sauvegarde précédente et les données actuelles sont sauvegardées. Ainsi, pour effectuer une restauration le retour à la toute première tâche est nécessaire.

Tableau 2.03 : *Exemple d'utilisation de la sauvegarde incrémentielle*

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
Complète (1 To)	Incrémentielle (10 Go)	Incrémentielle (20 Go)	Incrémentielle (30 Go)	Incrémentielle (40 Go)	Incrémentielle (50 Go)	Incrémentielle (20 Go)

Avantages :

- Occupe moins d'espace de stockage par rapport à la sauvegarde complète et à la sauvegarde différentielle.
- Vitesse de sauvegarde est plus rapide qu'une sauvegarde complète.

Inconvénients :

- La restauration d'une sauvegarde incrémentielle peut être longue : pour restaurer une donnée de mercredi soir, nécessaire de restaurer la sauvegarde complète de dimanche puis toutes les sauvegardes incrémentales les unes après les autres jusqu'à mercredi.
- Fiabilité de la restauration mais si une sauvegarde incrémentielle dans la chaîne est perdue, la sauvegarde complète est irrécupérable. Il sera donc nécessaire d'avoir au moins une sauvegarde complète périodique pour assurer un point de restauration fiable, raison pour laquelle le serveur de réplication est implémenter. [2.02]

2.2.1.4 La sauvegarde Miroir ou « Mirror Backup »

Une sauvegarde miroir est proche de la sauvegarde complète : ce type de sauvegarde crée une copie exacte de données source, mais seule la dernière version de données est stockée dans le référentiel de sauvegarde sans suivi des différentes versions des fichiers. Contrairement aux autres types de sauvegarde, tous les fichiers de sauvegarde individuels ne sont pas stockés dans un seul fichier conteneur compressé / chiffré, mais séparément, comme dans la source.

Avantages :

- Obtenir un accès direct aux fichiers de sauvegarde sans effectuer d'opération de restauration.

- Rapidité de la sauvegarde, la sauvegarde ne contient pas de fichiers anciens ou obsolètes avec une capacité de restauration rapide.

Inconvénients :

- Espace de stockage nécessaire pour le Mirror Backup est élevé.
- Risque élevé d'accès non autorisé et de corruption ou de mauvaise utilisation des données.

Si un fichier dans la source est supprimé, le même fichier dans le « miroir » est également supprimé (erreur humaine, sabotage interne, hacking, …) et perturbe directement le miroir. [2.02]

Tableau 2.04 : *Exemple d'utilisation de la sauvegarde miroir*

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
Miroir 1 To – nouvelle version de chaque jour						

2.2.1.5 Résumé

Après avoir étudier chaque technique de sauvegarde, chacune a ses avantages et ses inconvénients quelques-unes d'entre elles ont besoins des autres à un moment ou à un cas pour sa bonne fonctionnalité, alors ils sont dépendants les uns que les autres. Le Tableau 2.05 ci-dessous résume le fonctionnement, le temps nécessaire pour chaque sauvegarde, le temps de restauration et le stockage nécessaire pour chaque sauvegarde.

Tableau 2.05 : *Résumé des quatre types de sauvegarde*

Type de sauvegarde	Données sauvegardées	Temps nécessaire pour sauvegarde	Temps nécessaire pour restauration	Stockage nécessaire pour sauvegarde
Sauvegarde complète	Toutes les données	Le plus lent	Rapide	Elevé
Sauvegarde incrémentielle	Seulement les nouvelles et les modifiées	Rapide	Modéré	Le plus fiable
Sauvegarde différentielle	Toutes les données depuis la dernière	Modéré	Rapide	Modéré
Sauvegarde Miroir	Seulement les nouvelles et les modifiées	Le plus rapide	Le plus rapide	Le plus élevé

2.2.2 Technologie en fonction pour la sauvegarde

2.2.2.1 Secure Shell

Le protocole SSH permet aux administrateurs d'accéder à distance un ordinateur en toute sécurité. Désigne également l'ensemble des utilitaires qui mettent en œuvre le protocole. Ce protocole assure une authentification forte chiffrée sécurisée entre deux ordinateurs connectés sur un réseau. Il est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications, car il leur permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre. [2.02]

En résumé SSH effectue les commandes à distance telles que :

- Gestion des serveurs auxquels il n'est pas possible d'accéder localement
- Transfert de fichiers sécurisé
- Création sécurisée de sauvegardes
- Connexion entre deux ordinateurs utilisant le chiffrement de bout en bout
- Télémaintenance d'autres ordinateurs

a. Authentification

Le SSH utilise plusieurs techniques de chiffrement et d'authentification. D'une part, cela garantit que les flux de données ne peuvent être ni plus ni manipulés. Par contre, seuls les participants autorisés peuvent se contacter entre eux. Dans un premier temps, le serveur SSH et le client s'authentifient mutuellement. Le serveur envoie un certificat au client pour vérifier s'il s'agit bien du bon serveur. Ce n'est que lors du premier contact qu'un tiers risque de commuter entre les deux participants et d'intercepter ainsi la connexion. Comme le certificat lui-même est également crypté, il ne peut pas être imité. Une fois que le client sait quel est le bon certificat, personne d'autre ne peut prétendre contacter le serveur approprié. [2.03]

b. Chiffrement

Après l'authentification mutuelle des deux participants à la communication, ils établissent une connexion cryptée. Une clé est générée pour être expirée à la fin de la session. La clé utilisée pour le chiffrement asymétrique est valable que pour cette seule session. Le client et le serveur ont la même clef, donc tous les messages échangés peuvent être cryptés et décryptés. Le client et le serveur créent la clé simultanément, mais indépendamment l'un de l'autre. Dans l'algorithme d'échange de clés, les deux parties utilisent certaines informations publiques et secrètes pour créer la clé, la clé publique pour la partie client et clé privé pour le côté serveur. [2.03]

Une autre forme de cryptage a lieu avec SSH par la fonction de hachage. Un hachage est une forme de signature des données transmises. À l'aide d'un algorithme, un hachage unique est généré à partir des données. Si les données sont manipulées, la valeur de hachage change également automatiquement. Cela permet au destinataire de voir si les données ont été modifiées par des tiers en cours de route. Les valeurs de hachage sont conçues de telle sorte qu'elles ne peuvent pas être simplement simulées. Idéalement, il n'est jamais possible de créer deux transmissions différentes.

2.2.2.2 Architecture client- serveur

La sauvegarde utilise une technique étant comme le client-serveur (requête-réponse) comme représente la Figure 2.02. Le modèle client-serveur peut être utilisé par des programmes d'un même ordinateur, mais le concept est surtout utile dans le cadre d'un réseau. Dans ce cas, le client établit une connexion au serveur sur un réseau local (LAN) ou étendu (WAN), tel qu'Internet.

La sécurité est très importante car il faut que le PC (Personal Computer) client ne voit que le serveur, et non les autres PC clients. De même, les serveurs sont en général très sécurisés contre les attaques de pirates. Il est aussi très fiable car en cas de panne, seul le serveur fait la réparation, et non le PC client. Une architecture client-serveur est très évolutive car il est très facile de rajouter ou d'enlever des clients, et même des serveurs. Plusieurs architectures existent selon les types de réseaux et le client qui la contient. [2.04]

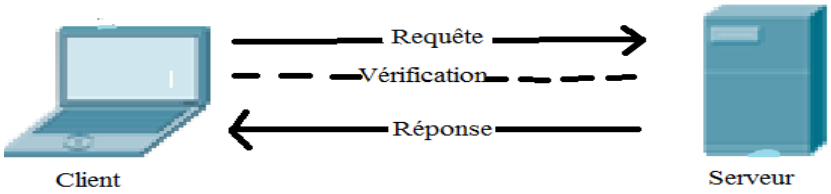


Figure 2.02 : *Architecture client-serveur*

a. Architecture « Pair à Pair »

Il existe deux types pour cette architecture, le centralisé et le décentralisé. Le réseau est dit pair à pair (peer-to-peer en anglais), lorsque chaque ordinateur connecté au réseau est susceptible de jouer tour à tour le rôle de client et celui de serveur. [2.04]

b. Architecture à 2 niveaux :

L'architecture à deux niveaux (aussi appelée architecture 2-tier, tiers signifiant rangée en anglais) caractérise les systèmes client-serveur pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service. [2.04]

c. Architecture à trois niveaux :

Dans cette architecture (3-tier en anglais), existe un niveau supplémentaire, un client équipé d'une interface utilisateur (généralement un navigateur web) chargé de la présentation. Un serveur d'application (appelé middleware) qui fournit la ressource, mais en faisant appel à un autre serveur. Un serveur de données qui fournit au serveur d'application les données requises pour répondre au client. [2.04]

d. Architecture à N niveaux

L'architecture à N niveau consiste à une spécialisation d'un serveur a une tâche précise similairement à l'architecture à trois niveaux. Avantage de flexibilité, de sécurité et de performance. Potentiellement, l'architecture peut être étendue sur un nombre de niveaux plus important. Cette solution de sauvegarde utilise cette architecture. [2.04]

2.2.2.3 Serveur Maitre/Esclave

C'est un type de secours quand il y a une panne de serveur en fonction. Le serveur maitre c'est le serveur principal comme le serveur de restauration précédent. Quand ce serveur est en cas de panne il passe automatiquement ses taches vers une serveur esclave qui est l'un de ses clients. Il existe un système d'arbitrage pour veuillez ses serveurs. L'application cliente communique avec le nœud maître pour ses transactions d'écriture et de lecture. Sur le nœud Esclave, la lecture seule est autorisée. Le nœud Arbitre n'a qu'un rôle de supervision, si le nœud maître connait un arrêt de service, le nœud arbitre désigne alors l'esclave comme nouveau maître. L'opération est invisible aux applications clientes et aucune perte de données n'est à déplorer. Cette structure permet de garantir une forte cohérence des données, car seul le maître s'occupe des clients. [2.05]

2.3 Elément de sauvegarde

2.3.1 Base de données

Une base de données représente l'ensemble cohérent des informations nécessaires au fonctionnement d'une entreprise, dont la gestion est assurée par un logiciel appelé système de gestion de bases de données ou SGBD. Une base de données permet de stocker et de retrouver l'intégralité de données brutes ou d'informations en rapport avec un thème ou une activité ; celles-ci peuvent être de natures différentes et plus ou moins reliées entre elles. Dans la très grande majorité des cas, ces informations sont très structurées, et la base est localisée dans un même lieu et sur un même support. Le dispositif comporte un SGBD ou un logiciel moteur qui manipule la base.

2.3.2 MySQL

2.3.2.1 Présentation

MySQL est un Système de Gestion de Bases de Données Relationnelles qui utilise le langage SQL. C'est un des SGBDR les plus utilisés. Sa popularité est due en grande partie au fait qu'il s'agit d'un logiciel open source, ce qui signifie que son code source est librement disponible et que quiconque peut l'utiliser et peut aussi modifier MySQL pour l'améliorer ou l'adapter à ses besoins.

2.3.2.2 Fonctionnement

Une base de données permet de collecter et gérer des données brutes ou d'informations, isolées ou liées entre elles et dont la nature est très variée. MySQL est indispensable pour créer un site Web dynamique et plus complexe. MySQL permet de manipuler ces bases de données et de diriger l'accès à leur contenu. Il emploie SQL ou Structured Query Language comme langage de requête.

2.4 Solutions de sauvegarde

2.4.1 Sauvegarde et restauration

La technique de sauvegarde se fait en deux étapes, premièrement la sauvegarde complète, après la sauvegarde incrémentielle qui se fait à chaque modification des contenus. Cette opération consiste à enregistrer automatiquement toutes les données de l'entreprise pour le mettre en sécurité et pour assurer sa disponibilité.

La sauvegarde de données répond à un problème de récupération de données supprimées comme par exemple :

- La restauration complète ou partielle des données d'une boite email (agenda, contact…).
- La restauration d'une base de données à un instant T.
- La restauration de données des fichiers utilisateurs (documents Office, PDF…).

Une solution de sauvegarde doit permettre notamment de définir une fréquence de sauvegarde (ponctuelle, quotidienne, hebdomadaire…) des fichiers et dossiers sélectionnés. Elle peut être configurée afin de s'enclencher automatiquement pour envoyer les données chiffrées vers un centre d'hébergement sécurisé. Les données sauvegardées, perdues lors d'un crash serveur pourront être restaurés afin que l'utilisateur puisse récupérer l'ensemble de ses informations numériques. Les données sont fondamentalement importantes pour les organisations et les entreprises. L'altération de ces dernières constituerait un dommage non négligeable. Voilà pourquoi, la restauration des données est primordiale après un sinistre informatique. La restauration des données est l'objectif le plus important du plan de continuité des activités dans les entreprises. La récupération des données qui ont été perdues à cause d'un problème technique ou d'une mauvaise manipulation. Il s'agit alors de remettre à leur emplacement initial les données précédemment sauvegardées, dupliquées sur un emplacement différent et plus sûr. C'est l'opération réciproque d'une sauvegarde, sauf que, dans la

plupart des cas, une restauration concernera un ensemble de fichiers tandis qu'une sauvegarde concerne le plus souvent l'ensemble des fichiers d'un système. [2.06]

2.4.2 Replication

La réplication de données quant à elle, répond à une problématique de perte de service. Lors d'une interruption de service (site web, serveur de messagerie, plateforme collaborative, etc.) il va être possible d'opérer un basculement des applicatifs touchés vers un autre serveur ou un autre site d'hébergement données, géographiquement éloigné du site primaire.

On différenciera d'ailleurs les réplications synchrones et asynchrones pour des utilisations différentes. [2.07]

2.4.2.1 Replication synchrone

Une réplication de base de données « Exchange » pour remonter un MailboxStore sur un autre serveur. Une réplication sur de multiples disques durs.

2.4.2.2 Replication asynchrone

Un cluster de base de données avec des données d'importance faible à moyenne. Réplication de fichiers entre plusieurs sites. Réplication d'annuaire (Active Directory par exemple).

2.5 Méthode de sauvegarde

La mise en pratique de la sauvegarde est planifiée dans cette sous chapitre. En prenant l'exemple qu'une entreprise a 100Go de donnée critique par semaine. Ces données sont fréquemment modifiées, à raison d'environ 1Go/jour et du fait de leur criticité on souhaite conserver un certain historique de ces modifications.

2.5.1 Exemple de plan de sauvegarde

L'entreprise effectue :

- Une sauvegarde complète de donnée par mois (1 mois effectuée).
- Une sauvegarde différentielle par semaine (4 semaines effectuées).
- Une sauvegarde incrémentielle par jour (14 jours effectués).

2.5.2 Espace disque necessaire

- La sauvegarde complète mensuelle : 1 sauvegarde complète : 4*100Go = 400Go.

Conservation de la sauvegarde complète en cours et la précédente.

-La sauvegarde différentielle : 4 sauvegarde : 25+25 = 50Go ; 50+25= 75 ; 75+25=100 Go.

C'est une conservation de 4 semaines de sauvegarde différentielle hebdomadaire.

Cette sauvegarde se base sur la dernière sauvegarde complète, le volume de données augmente donc d'autant plus que la sauvegarde complète est ancienne.

-La sauvegarde incrémentielle : 3,5 Go*1Go = 3,5Go. C'est la conservation d'une semaine soit 7 jours (le dimanche la sauvegarde différentielle a lieu) de sauvegarde incrémentale.

2.6 Sécurisation avec la fonction de hachage

Définition 2.02 : [2.08]

La fonction de hachage est une méthode permettant de caractériser une information ou une donnée, en leur faisant subir une suite de traitements reproductibles à une entrée, elle génère une empreinte servant à identifier la donnée initiale. On a besoin de ce type de fonction dans la sauvegarde pour comparaison des données quand il y a une modification, protection contre les intrus et la collision qui est le principal rôle de cette fonction. La définition de la fonction de hachage est représentée dans l'équation 2.01 ci-dessous :

$$H: \{0,1\}* \quad ---\rightarrow \quad \{0,1\}^n$$

Avec $h\ et\ x\ \epsilon\ \{0,1\}*$ (2.01)

2.6.1 Rôles de hachage

La fonction de hachage a beaucoup de rôle dans le fonctionnement des serveurs, tels que :

- L'intégration des données : utilise le code de détection de manipulation appelé Manipulation Détection Code ou MDC qui assure l'intégrité d'un message, à l'instar des bits de parité.
- Protection de mot de passe
- Authentification de message : utilise le code d'authentification de message appelé Message Authentification Code ou MAC qui gèrent à la fois l'intégrité et l'authentification de la source d'une donnée.
- Signature numérique : utilise le MD5 (Message Digest) ou SHA (Secure Hash Algorithm) pour avoir un « condensat » ou résumé numérique signé, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon.

2.6.2 Théorie de fonctionnement

Le hachage consiste à calculer une donnée de petite dimension à partir d'une donnée de grande dimension afin de s'en servir comme repère dans différents processus algorithmiques comme montre la Figure 2.02. La valeur obtenue par hachage est un nombre ou une chaine binaire et dans ce dernier cas généralement représenté en hexadécimal.

Lorsque les fonctions de hachage sont utilisées dans les bases de données, le seul écueil à éviter réside dans des collisions accidentelles : si deux entrées d'une même base s'avèrent avoir la même empreinte, elles seront considérées comme identiques. Pour éviter que cela se produise, les fonctions de hachage sont construites de manière à ce que les empreintes soient réparties uniformément sur l'ensemble d'arrivée de la fonction.

Dans le domaine de la cryptographie, les fonctions de hachage sont utilisées comme brique de base de différents mécanismes. La robustesse de ces mécanismes repose en partie sur sa résistance qu'ils utilisent à différentes attaques. Bien que d'autres chemins d'attaque soient possibles, la sécurité est surtout évaluée dans les trois scénarios tels que la collision, le préimage et le second préimage.

– Collisions : l'attaquant doit trouver deux messages différents M et M0 tels que H(M)=H(M0).

– Préimages : étant donné une valeur x de l'ensemble des hachés, l'attaquant doit trouver M tel que H(M) = x. Avec x est le préimage de M.

– Secondes préimages : étant donné un message M, l'attaquant doit trouver M différent de M0 tel que H(M) = H(M0).

Les algorithmes de hachage les plus connus sont : MD2, MD4, MD5 (16 octets / 128 bits en sortie), SHA (ou SHA-0), SHA-1 (20 octets / 160 bits en sortie), SHA-2 (224 à 512 bits). [2.08]

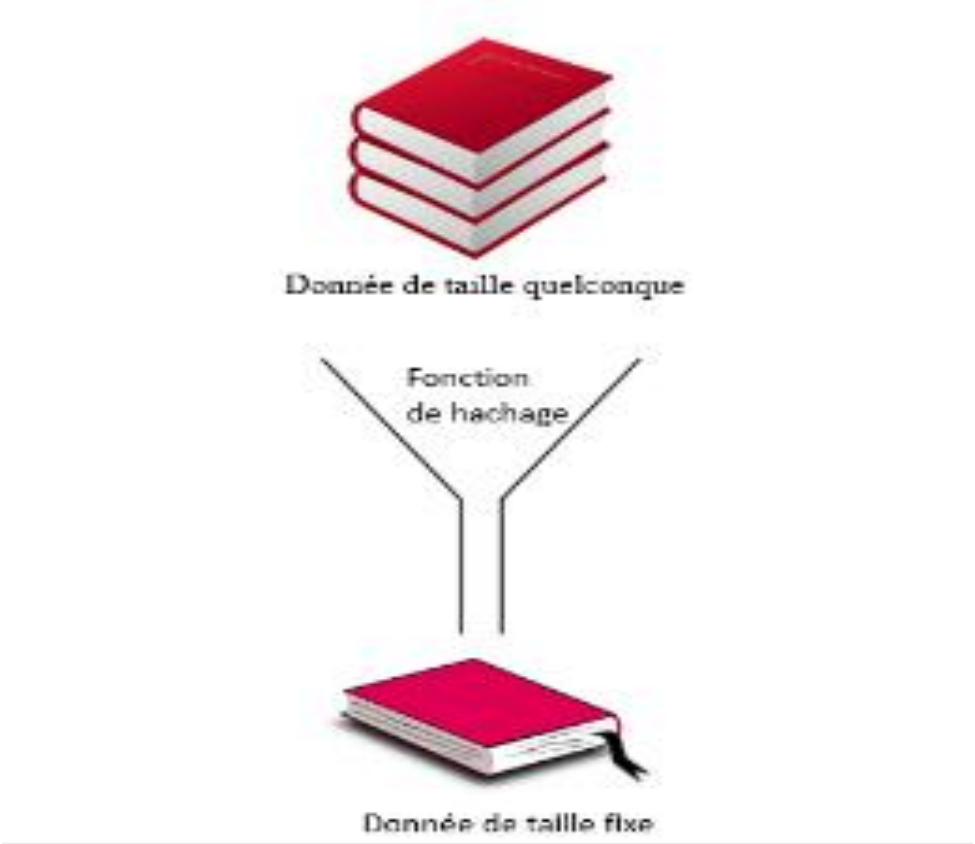


Figure 2.03 : *Principe de fonctionnement de fonction de hachage*

2.6.2.1 Collision

Les fonctions de hachage sont utilisées pour calculer des empreintes de taille fixe à partir de données de taille variable et potentiellement grande. Le domaine de définition d'une fonction de hachage est donc plus grand que l'ensemble des empreintes. Ceci implique l'existence de collisions. La sécurité repose donc sur la difficulté de trouver ces collisions dans la pratique.

De plus, pour n'importe quelle fonction de hachage H, il existe des attaquants qui renvoient des collisions de manière immédiate. Si M et M'sont deux messages différents tels que H(M) = H(M'), alors l'algorithme qui renvoie simplement M et M'permet de trouver une collision pour H. La résistance à la recherche de collisions ne peut donc pas être définie comme l'impossibilité de l'existence d'un tel attaquant, mais comme la difficulté à en trouver un dans la pratique. [2.09]

2.6.2.2 Compression

Pour des applications pratiques, il est souvent nécessaire de hacher un gros volume de données. La fonction de compression doit permettre le traitement rapide de ces données. La même contrainte pesante sur les primitives de chiffrement symétrique, les principes de conception des fonctions de compression sont souvent proches des principes de conception de ces primitives. Dans cette section, nous commençons par décrire quelques méthodes classiques permettant de construire une fonction de compression à partir d'un algorithme de chiffrement par blocs.

L'algorithme de Merkle-Damgård permet de calculer des empreintes pour des données de taille variable en utilisant une fonction de compression. L'idée consiste à diviser la donnée à hacher M en blocs de taille fixe M1, . . ., Mk et à traiter dans les blocs Mi itérativement. La Figure 2.03 montre la construction de fonction de hachage de Merkle-Damgârd tels que h :

{0,1} m * {0,1} n ---------- > {0,1}n.

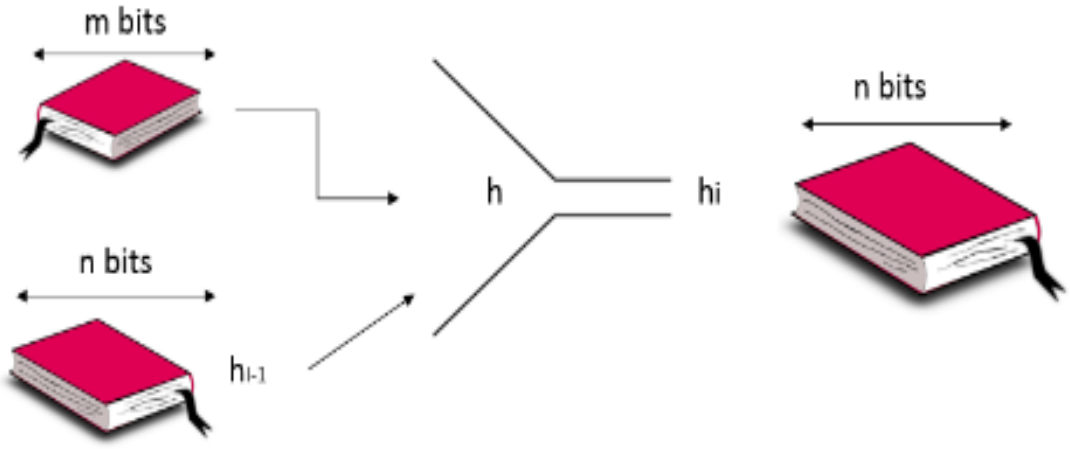


Figure 2.04 : *Fonction de compression de Merkle-Damgârd*

2.7 Differents logiciels de sauvegarde

Plusieurs types de logiciels et de techniques de sauvegarde existe déjà. Mais chacun a ses avantages ses inconvénients possibles. Le tableau suivant montre la performance de trois types de sauvegarde.

Tableau 2.06 : *Comparaison de trois types de logiciels de sauvegarde*

	Propriété	**Avantages**	**Inconvénients**
Elkarbackup	Logiciel libre Open source	N'utilise pas un logiciel client -Utilise SSH, RSYNC, FTP. -Permet la sauvegarde avec Windows en utilisant samba -Compression des fichiers de sauvegarde automatique.	-Disponibilité du serveur
NextCloud	Logiciel libre Open source	-Synchronisation des fichiers avec ordinateur et les mobiles. -Stockage sécurisé, chiffrement des fichiers et chiffrement de la connexion point à point. -Avoir une antivirus clamAV.	Disponibilité du serveur
Rsync	Logiciel libre Open source	Peut synchroniser avec d'autre logiciels par exemple le Daemon « Cron », MD5, SHA.	Besoin de la création d'une interface graphique convenable

2.8 Conclusion

Ce chapitre a permis d'étudier en profondeur les aspects de sauvegarde dans une entreprise pouvant amener à évaluer son avantage. Parmi ces aspects sont les concepts de sauvegarde et de réplication des données afin de pouvoir effectuer la restauration, la technique d'utilisation de la fonction de hachage pour permettre la protection des données ; les différents types de logiciels de sauvegarde ainsi que leur performance. Dans le chapitra suivant, la solution plus fiable et plus performante est apportée, ensuite la mise en place du serveur de sauvegarde au sein d'un réseau.

CHAPITRE 3
CONCEPTION D'UNE SOLUTION DE SAUVEGARDE DANS UNE ENTREPRISE

3.1 Introduction

Actuellement, il y a déjà plusieurs types de techniques de sauvegarde, que chacun a sa performance et sa fonctionnalité. Ce chapitre apporte une technique de sauvegarde plus performante utilisant la logiciels Elckarbackup, ensuite la réplication des données avec Rsync, ce sont la réalisation du schéma synoptique dans le Figure 2.01. Qui a pour but de protéger les données en cas de perte ou endommagement.

3.1.1 Cadre d'essai du projet

La société Alternateeve est une entreprise privée se situe principalement à Montréal mais annexée à Antsirabe Madagascar et a pour principale mission de faire la conception sur mesure des logiciels.

- Dénomination : Alternateeve Technologies Lab
- Siege: Montreal (Paris) - Antsirabe (Madagascar)
- Site : https://www.alternateeve.com

3.1.2 Organigramme

Alternateeve possède 3 grandes directions qui sont les équipes à Montréal, l'administrateur à Madagascar et le R&D Madagascar. L'organigramme est illustré par la Figure 3.01 et leurs tâches respectives par la Figure 3.02.

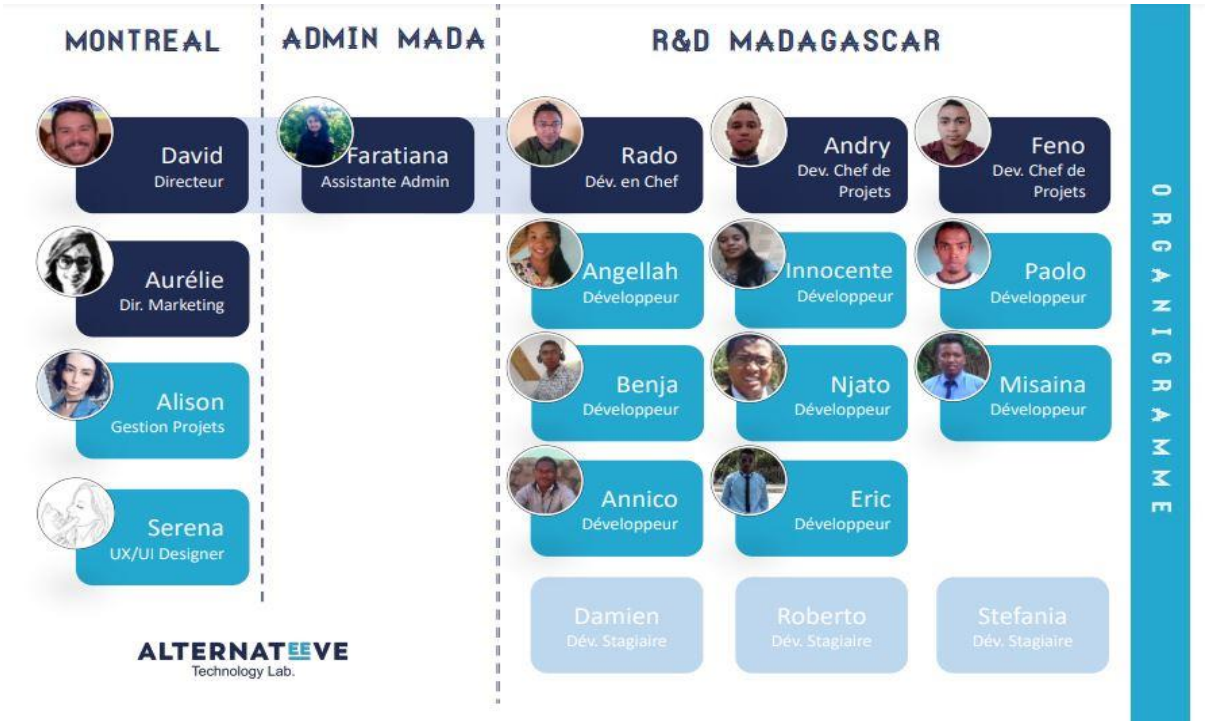


Figure 3.01 : *Organigramme de l'Alternateeve*

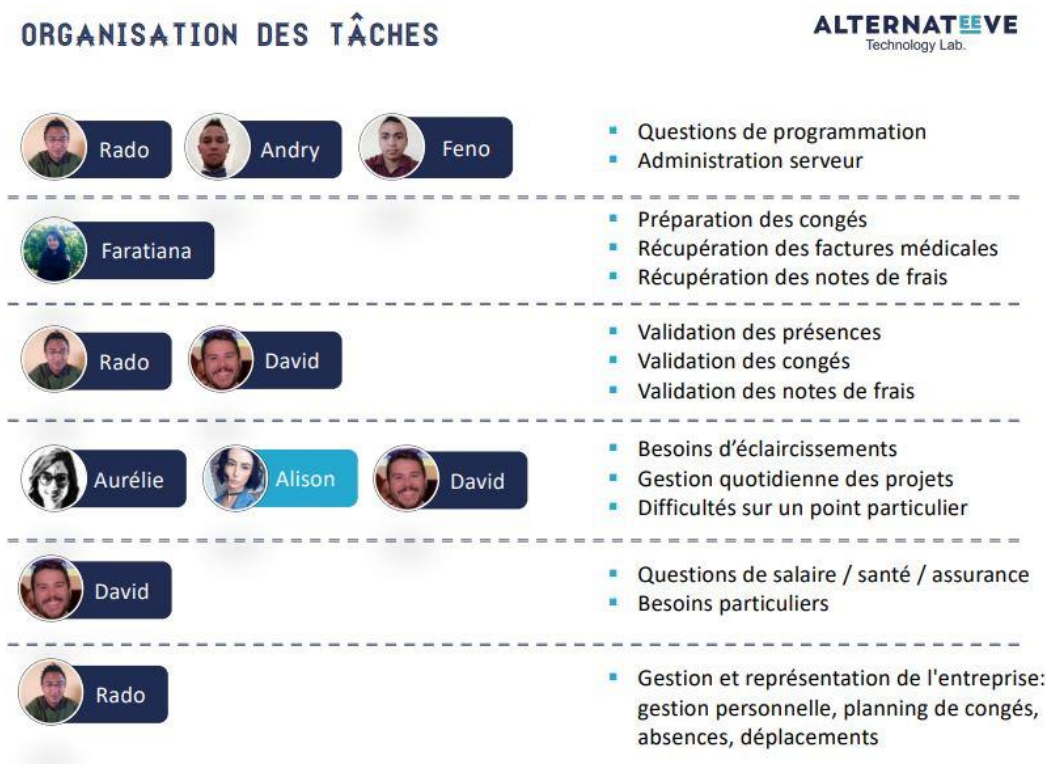


Figure 3.02 : *Organisation des tâches*

3.1.3 Problèmes rencontré par l'entreprise

L'entreprise possède plusieurs développeurs qui travail personnellement sur son poste. Puisque le travail est une création de logiciel, chacun fassent ses propres tâches et à la fin de la journée il y a intégration de toutes les parties finalisées. Apres l'intégration de toutes les parties, toutes les données sont centralisé dans un serveur. Ce serveur qui se situe même dans l'entreprise. Alors au cas d'une incendie ou endommagement des matériels, l'entreprise risque de perdre toutes ses données, cela engendre une grave faillite.

C'est pourquoi l'idée de la solution de sauvegarde est née pour protéger et pour préserver l'entreprise contre ces désastres. La conception de la solution de sauvegarde a été faite au sein de l'entreprise durant le stage mais la simulation qui a été présenté dans ce livre.

3.2 Présentation

3.2.1 Description de la machine utilisée

3.2.1.1 Machine

Pour la simulation une machine qui a la configuration suivante est utilisée :

- Marque : HP Probook 6560b
- Processeur : Intel(R) HD Graphics

- Mémoire : 4 Go RAM
- Système d'exploitation : Windows 7 Professionnel

3.2.1.2 VirtualBox

VirtualBox est un logiciel libre qui permet de créer un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation, fonctionnant sur MAC, Linux et Windows. La virtualisation permet, sur un même PC, de faire tourner plusieurs systèmes d'exploitation en concurrence. Le système d'exploitation « principal » fait tourner plusieurs applications servant au partage des ressources et à l'émulation d'un PC un autre système d'exploitation. [3.01]

Figure 3.03 : *Oracle VirtualBox*

Pour la simulation, trois machines sont installées dans le VirtualBox, ce sont des machines Linux.

- DebianReplication : serveur debian 7 qui effectue la réplication des données de la serveur nextcloud, avec une adresse IP de 192.168.135.5.
- DebianTsirisoa : machine cliente debian 7 avec une adresse IP 192.168.135.2.
- Nextcloud-tsirisoa : serveur de sauvegarde debian 9 avec une adresse IP 192.168.135.4.

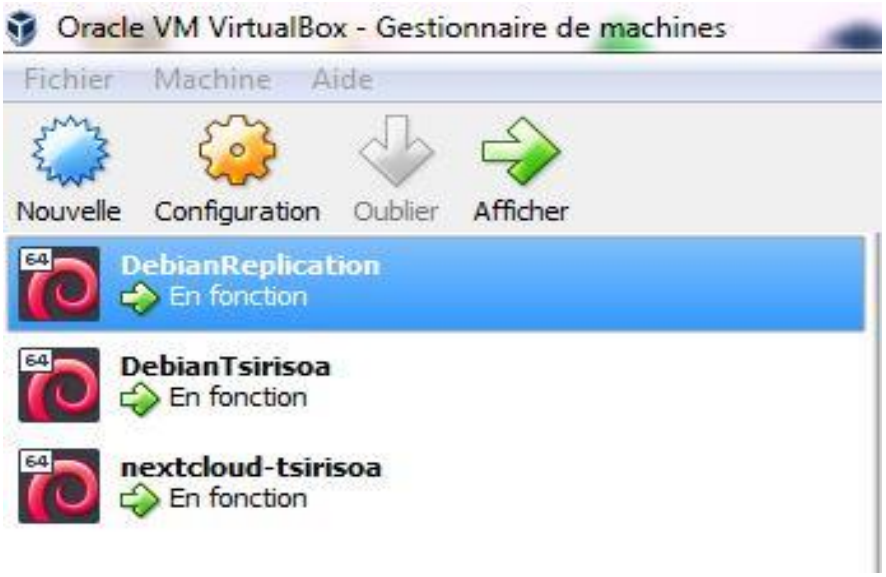


Figure 3.04 : *Machine utilisées*

3.2.2 Installations

Toutes les installations des machines sont identiques. On installe trois machines virtuels dans VirtualBox. Le suivant sont les étapes de l'installation.

1ère étape : ouvrir le logiciel VirtualBox

2ème étape : cliquez sur nouvelle, une fenêtre apparait et trois formulaires apparaissent, ce sont :

- Nom : remplir par le nom de la machine, exemple : DebianReplication.
- Types : c'est le type de système utilisé, le linux est la machine utilisant ici, alors cliquez sur Linux
- Version : Version du système, par exemple Debian 64 bits.

3ème étape : choix de la mémoire utilisée, la machine DebianReplication a 1024 Mo de mémoire. Puis il y a choix de disque dur utilisée, la machine ici utilise le disque dur VDI ou Virtual Disque Image. En plus, il y a le choix de l'emplacement de fichier.

4ème étape : Cliquer sur la machine et cliquer sur le bouton démarrer, monter le disque de Debian sur la machine et l'installation se poursuit.

3.2.3 Configurations

Tous les configurations se fait dans un terminal, alors avant toutes choses ouvrir d'abord un terminal.

1ère étapes : Entrer en tant que Super utilisateur avec la commande # su root, puis activer l'interface eth0 par la commande #ifup eth0

Quand cette indice dièse (#) apparait, le terminal est en mode super utilisateur. Pour revenir en mode utilisateur, il suffit de tapez la commande #exit pour revenir.

2ème étapes : Donner une adresse IP à chaque machine.

Pour cette étape taper la commande nano /etc/network/interfaces, une page s'affiche, puis remplissant par une adresse IP, un masque du réseau, une passerelle, et un adresse broadcast. Cette configuration est faite manuellement. Après un enregistrement, la machine porte l'adresse IP donnée. Pour la machine DebianReplication on a :

```
auto lo
iface lo inet loopback
allow-hotp eth0
iface eth0 inet static
        address 192.168.135.5
        netmask 255.255.255.0
        network 192.168.135.0
        broadcast 192.168.135.2
        gateway 192.168.135.1
```

La commande nano veut dire d'ouvrir une éditeur texte, et ouvrir le fichier interfaces dans le dossier etc et dans network. Le fichier interfaces existe déjà lors de l'installation de la machine.

Enregistrer la modification, puis taper la commande #ifconfig pour voir si la configuration a été bien placer.

```
root@debian:/home/nextcloud-tsirisoa/Documents# ifconfig
```

Cette commande affiche les détails de la configuration faite.

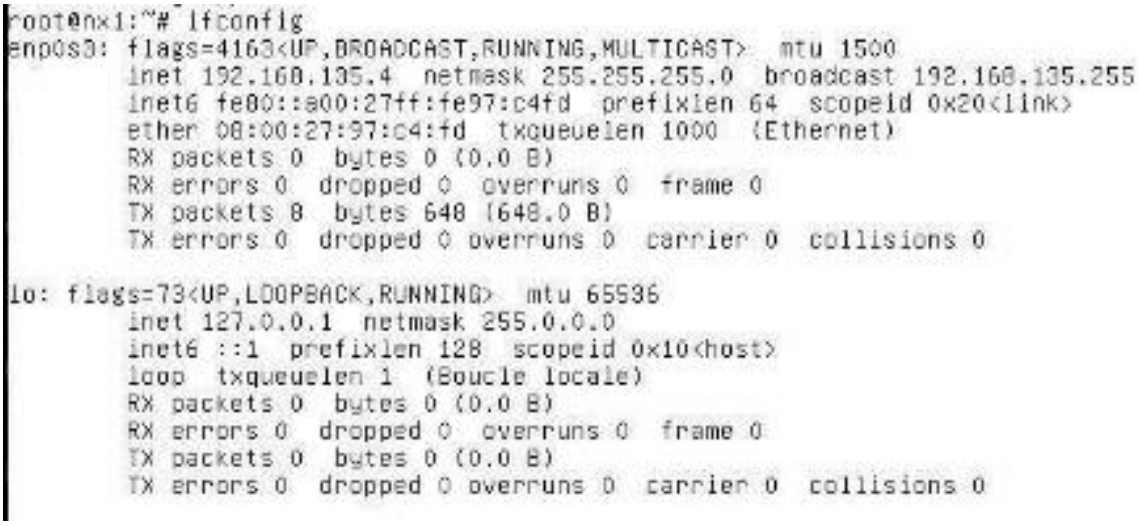
```
eth0      Link encap:Ethernet  HWaddr 08:00:27:6e:26:00
          inet adr:192.168.135.5  Bcast:192.168.135.2  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe6e:2600/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:254 (254.0 B)  TX bytes:9508 (9.2 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:1536 (1.5 KiB)  TX bytes:1536 (1.5 KiB)
```

Les trois machines sont configurées identiquement à cela, et ont leurs adresse IP respectifs.

Pour la 2ème machine DébianTsirisoa, la configuration est la suivante :

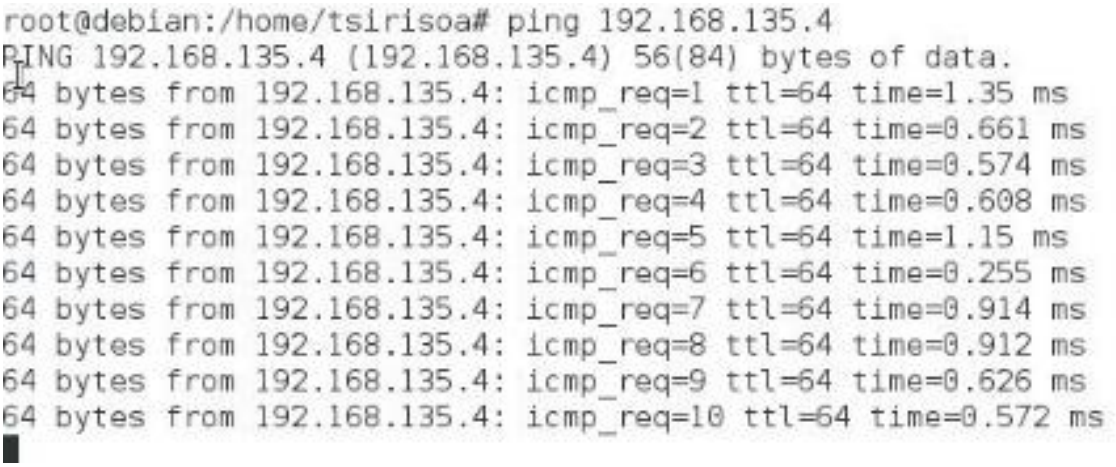
```
tsirisoa@debian:~$ su root
Mot de passe :
root@debian:/home/tsirisoa# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:48:e3
          inet adr:192.168.135.2  Bcast:192.168.135.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe4c:48e3/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:0 (0.0 B)  TX bytes:12098 (11.8 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:2474 (2.4 KiB)  TX bytes:2474 (2.4 KiB)
```

Et la 3ème machine nextcloud-tsirisoa, a la configuration suivante :



3.3 Réalisation de la sauvegarde

Pour réaliser la sauvegarde, les trois machines doit être dans la même réseau. Pour savoir que les trois machines sont liées, entrer dans un terminal, et taper la commande #ping suivie de l'adresse IP de la machine cible.



La machine cliente DebianTsirisoa ping la machine serveur nextcloud-tsirisoa.

3.3.1 Machine Client

La machine client est la machine utilisée par les utilisateurs, par exemple dans une boite informatique ce sont les machines utilisées par les développeurs. Une machine nommée DebianTsirisoa est ici considéré comme client.

A la fin de la journée chaque utilisateur fait la sauvegarde de chaque travail vers le serveur de sauvegarde, ou le serveur absorbe tous les travails permettez par l'utilisateur. Dans cette simulation le serveur de sauvegarde utilisé est Elkcarbackup.

3.3.1.1 Secure Shell

La machine client a besoin d'une serveur SSH, pour se connecter au serveur. C'est un serveur qui permet d'accéder une machine à distance. Ce serveur est très sécurisé qui demande un mot de passe sécuriser par le cryptage. Mais pour une sauvegarde, l'authentifications n'est pas utile puisque ça énerve le rôle de serveur pendant l'absorption des travails. Une commande # | ssh-keygen est la commande qui effectue l'authentification sans mot de passe, très sécuriser.

Tableau 3.01 : *Commande d'installation du serveur*

Commande	Exécution
Apt-get install ssh server	Installation du serveur SSH
Ssh-keygen	Authentication sans mot de passe
Ssh-copy-id root@192.168.135.4	Lancement de copie sur le serveur distant

```
root@debian:/home/tsirisoa# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

Cette commande nécessite un mot de passe durant l'exécution seulement pour la protection et un nom de fichier d'enregistrement nommée « tsiry ».

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): tsiry
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in tsiry.
Your public key has been saved in tsiry.pub.
The key fingerprint is:
19:70:ac:c6:96:00:bd:51:5d:86:0c:1f:55:fa:1a:7a root@debian
The key's randomart image is:
+--[ RSA 2048]----+
|   .o .+=o++..   |
|     +  +=o .    |
|      = oo .     |
|     . *  o .    |
|      o  S . .   |
|         . o     |
|        . E      |
|         .       |
|                 |
+-----------------+
```

3.3.1.2 Mysql

La machine cliente peut contenir des bases de donnée, des fichiers, des images qu'il peut tous les sauvegarder.

Tableau 3.02 : *Commande d'installation de Mysql*

Commande	Exécution
Apt-get install mysql server	Installation du mysql serveur

3.3.2 Machine serveur de sauvegarde

Cette machine sert comme serveur, lors de l'installation du réseau, la mise en place de la topologie en étoile est utilisée, qui a pour but de centraliser toutes les données des utilisateurs vers le serveur. Dans la simulation, la machine nommée nextcloud-tsirisoa est utilisée comme serveur. Cette machine doit avoir une très grande capacité de disque dur pour sauvegarder une grande capacité de donné. Plusieurs logiciels sont nécessaires pour configurer ce serveur, parmi eux ; le logiciel de sauvegarde, une base de donnée et quelques configurations.

3.3.2.1 Configurations

- La première démarche à faire c'est d'installer le serveur SSH pour la connexion à distance avec les machines clients.

Tableau 3.03 : *Installation du serveur ssh*

Commande	Exécution
Apt-get install ssh	Installation du serveur ssh
Ssh-keygen	Authentification sans mot de passe
Ssh-copy-id root@192.168.135.2	Lancement de copie sur le serveur distant

- Puis, l'installation du serveur web apache.

Tableau 3.04 : *Installation du serveur web apache*

Commande	Exécution
Apt-get install apache2	Installation du serveur apache
Systemctl start apache2	Démarrage du serveur
Systemctl enable apache2	Autorisation

- Installation de php7 permettant de se connecter au serveur Mysql

Tableau 3.05 : *Installation du php version 7*

Commande	Installation
apt install php7.0 libapache2-mod-php7.0 php7.0-common php7.0-gd php7.0-json php7.0-mysql php7.0-curl php7.0-mbstring php7.0-intl php7.0-mcrypt php7.0-imagick php7.0-xml php7.0-zip	Installation de php version 7

- Installation du serveur Mysql

Tableau 3.06 : *Installation du Mysql serveur*

Commande	Installation
Mysql_secure_installation	Installation d'un type de sécurité mysql

Après cette installation, il y a les rêquete suivante :

- Set root password? [Y/n] Y
- Remove anonymous users? [Y/n] Y
- Disallow root login remotely? [Y/n] Y
- Remove test database and access to it? [Y/n] Y
- Reload privilege tables now? [Y/n] Y

- La prochaine étape consiste à la connexion du serveur Mysql en tant qu'utilisateur root.

Tableau 3.07 : *Connexion au serveur mysql*

Commande	Exécution
Mysql -u root -p	Connexion au serveur

3.3.2.2 Installation du serveur de sauvegarde Elkarbackup

- Elkarbackup est un logiciel avec interface qui gère le fonctionnement de la synchronisation des fichiers. Il fournit une solution de sauvegarde de système de fichier open source puissante et facile à configurer, développé pour faciliter la gestion de la sauvegarde, quel que soit le système d'exploitation de la machine cliente. Basé sur les technologies open source comme rsnapshot, rsync, php et sympfony. Il a les caractéristiques suivantes :

- Sauvegardes centralisées.
- Sauvegarde des ordinateurs GNU, Linux et Windows.
- Utilisation minimale du disque en raison de l'utilisation de liens durs, mais possibilité de récupérer l'ensemble de la sauvegarde en un clic de souris.
- Interface Web facile à utiliser et multilingue. [3.03]

- Installation

```
root@nx1:~# apt install php-cli rsnapshot apache2 mysql-server php-mysql acl bzi
p2php-xml libapache2-mod-php libapache2-mod-php7.0 libssh2 mysql-client
Lecture des listes de paquets... Fait
```

- Configuration du Mysql

```
root@nx1:~# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none): _
Set root password? [Y/n] y
New password:
Re-enter new password: _
```

- Installation de Elkarbackup

```
root@nx1:~# apt-get install elkarbackup
Lecture des listes de paquets... Fait
```

- Clé de référentielle des paquets et le repértoire Elkarbackup

```
root@nx1:~# wget -O - http://elkarbackup.org/apt/archive.gpg.key | apt-key add -
--2019-04-25 02:10:21--  http://elkarbackup.org/apt/archive.gpg.key
Résolution de elkarbackup.org (elkarbackup.org)… 150.241.235.5
Connexion à elkarbackup.org (elkarbackup.org)|150.241.235.5|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 964 [application/pgp-keys]
Sauvegarde en : « STDOUT »

root@nx1:~# echo "deb http://elkarbackup.org/apt/debian stretch main" > /etc/apt
/sources.list.d/elkarbackup.list
root@nx1:~# apt-get update
0% [En cours]
```

- Présentation de l'interface

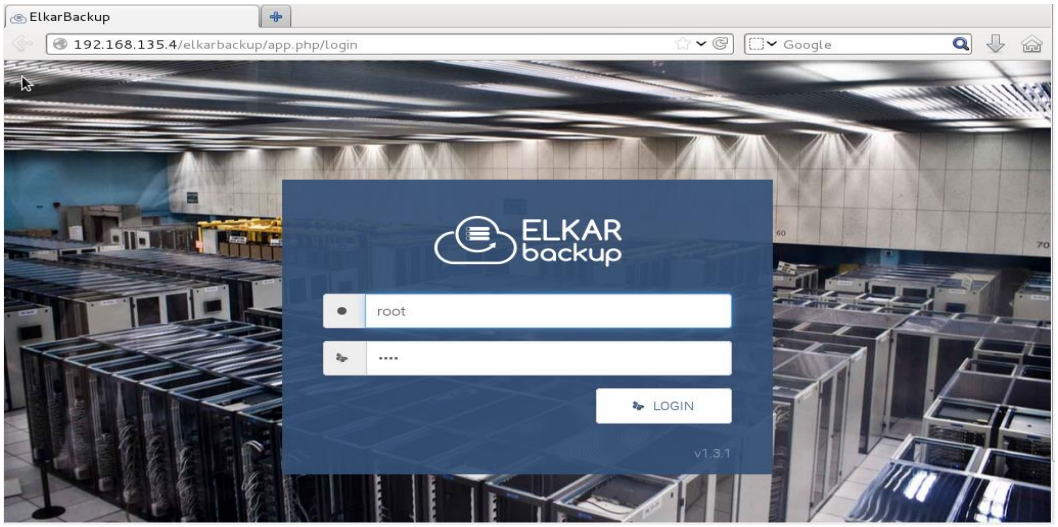


Figure 3.05 : *Interface graphique de Elkarbackup*

Maintenant que Elkarbackup est installé la figure suivante représente l'interface graphique utilisé pour effectuer la sauvegarde.

3.3.3 Exécution d'une sauvegarde

Après toutes les installations, la machine client peut alors effectuer une sauvegarde vers la machine serveur.

- Démarrer le serveur, ouvrir la machine client, puis ouvrir une navigateur web et taper l'adresse IP du serveur. Après avoir effectué cette opération que la page d'accueil s'affiche.
- Ajout de la machine client au serveur : primordialement, l'ajout de la machine client de sauvegarde est incontournable. L'interface présent dans la Figure 3.04 fait la configuration de la machine à sauvegarder. Dans Jobs puis Edit Client, il y a l'ajout du nom de la machine, puis son url c'est-à-dire son adresse IP, il y a Quota c'est à dire pas de limite d'utilisation du disque dur, il y a le choix d'espace disque nécessaire pour effectuer la sauvegarde.

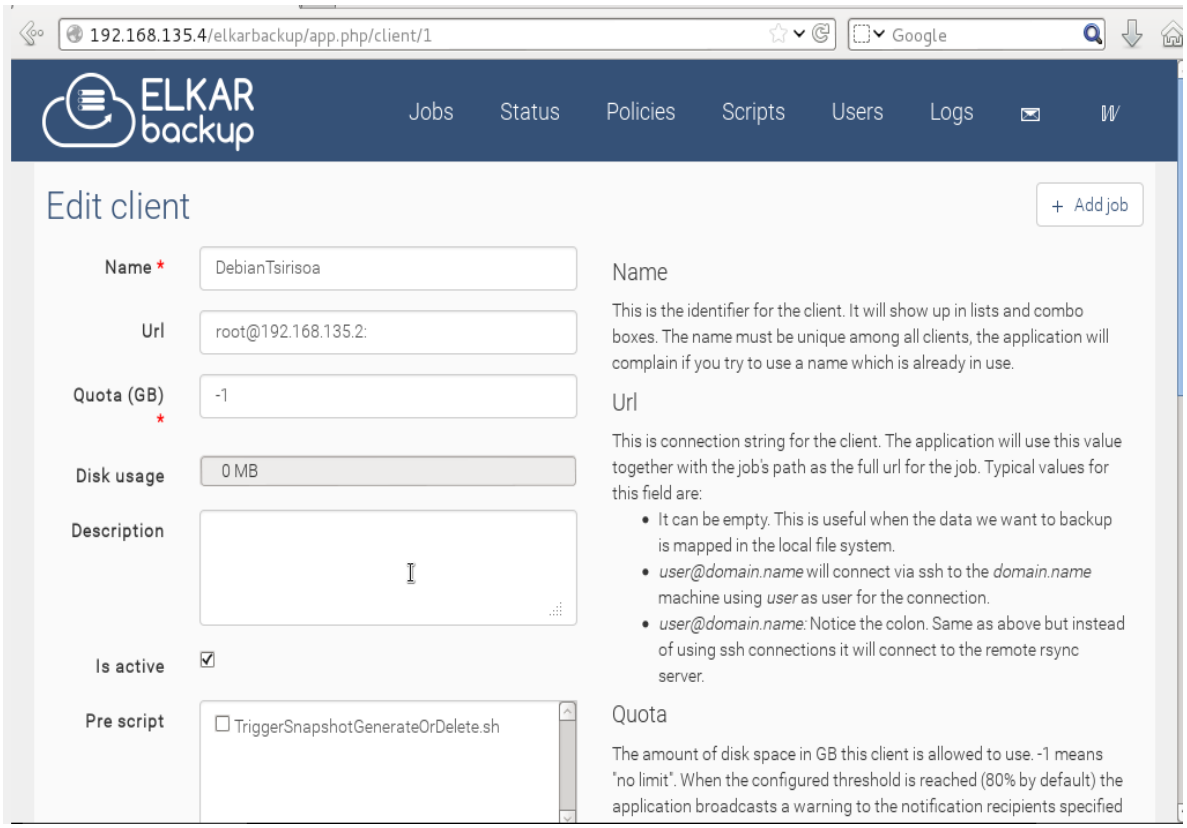


Figure 3.06 : *Elkarbackup jobs*

- Destination de la sauvegarde : après avoir ajouté la machine dans le réseau de sauvegarde, la configuration du lieu de stockage dans le serveur est maintenant la deuxième tâche à effectuer. Cette destination est déjà créée pendant la configuration du programme. Dans cette onglet, l'utilisateur fait le choix de la destination de la sauvegarde de donnée.

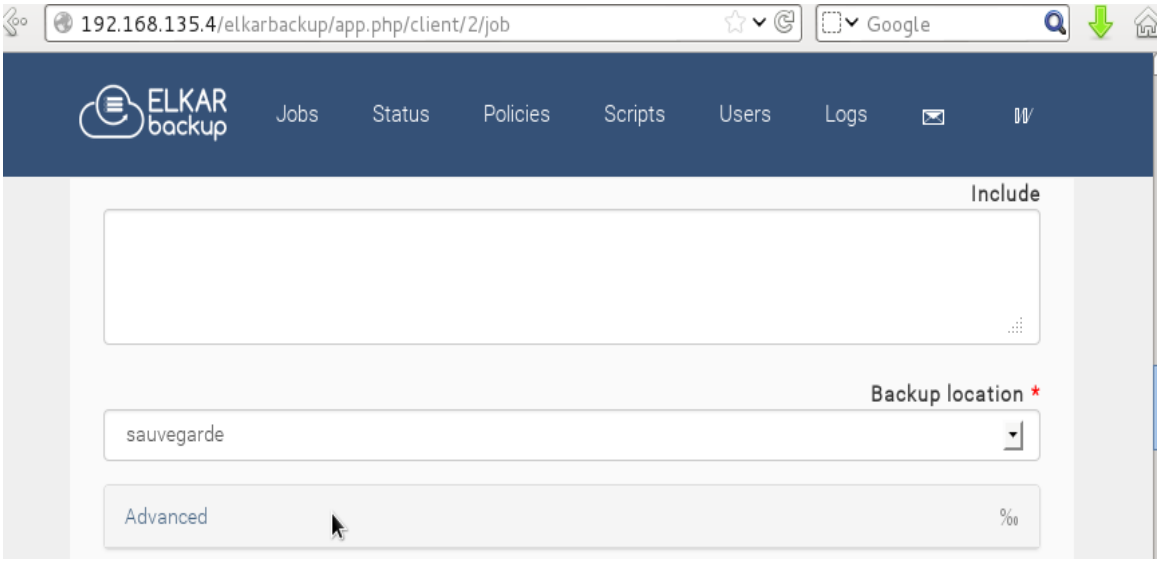


Figure 3.07 : *Destination de la sauvegarde*

- Réalisation de la sauvegarde :

- Créer d'abord un fichier ou une base de donnée ou autres dans la machine client

```
root@debian:/home/tsirisoa# mkdir dossier_important
```

- Lancement de la sauvegarde des données. En ajoutant la machine DebianTsirisoa et puis le chemin de sauvegarde de fichier. Dans l'onglet status que tous les statuts ou tâches effectué sont afficher comme représente la figure 3.06. Pour faire une sauvegarde, cliquer sur « Action » puis « Enqueue now ».

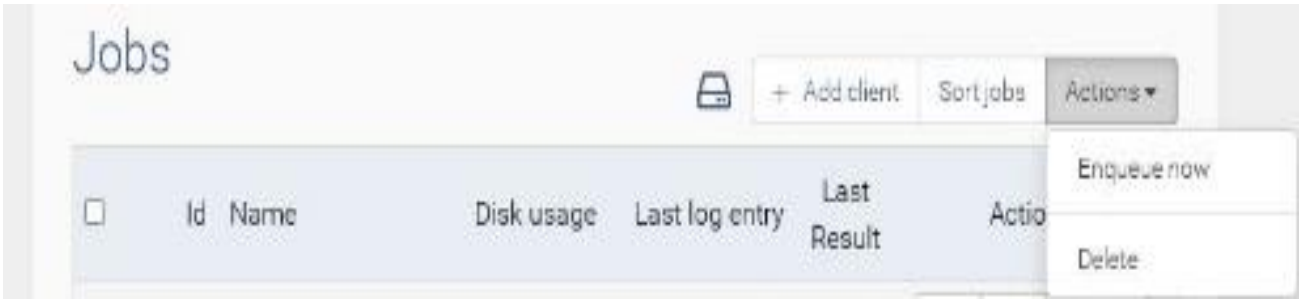


Figure 3.08 : *Réalisation de la sauvegarde*

- Attente pendant la réalisation de la sauvegarde.

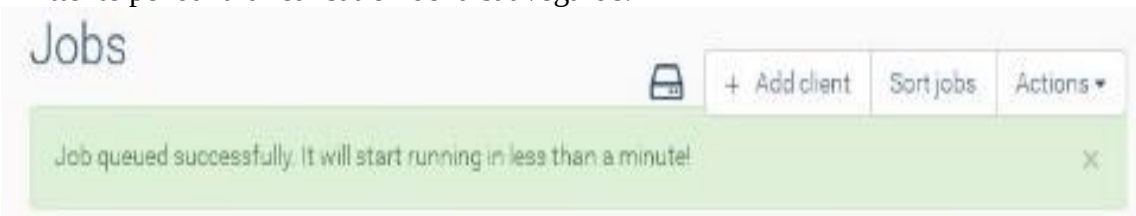


Figure 3.09 : *Attente pendant la sauvegarde*

- Quand le sauvegarde ne réussisse pas, il y a une message « Fail » en rouge qui se présente sur l'interface, mais si le sauvegarde est réussi il y a message de notification « OK » en vert. [3.05]

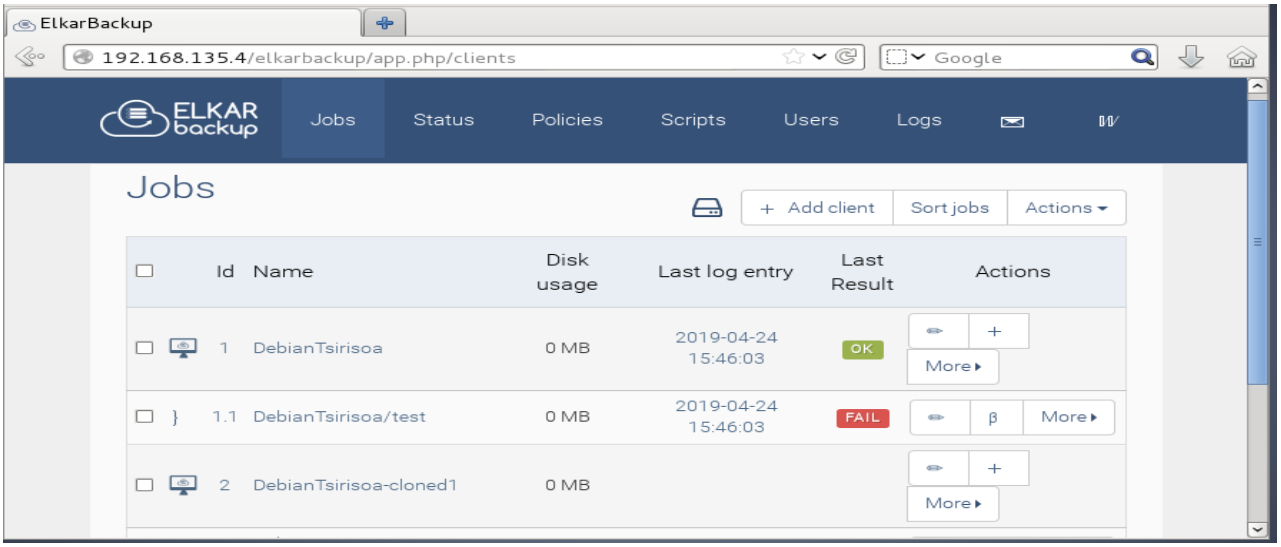


Figure 3.10 : *Sauvegarde effectué par DebianTsirisoa*

Lors de cette sauvegarde, dans l'onglet statuts se fait les détails de toutes action, comme l'Id de la sauvegarde, le nom, le temps qu'effectue l'opération et aussi le statut de l'opération. Quand l'opération de sauvegarde s'achève, ce statut disparaitra.

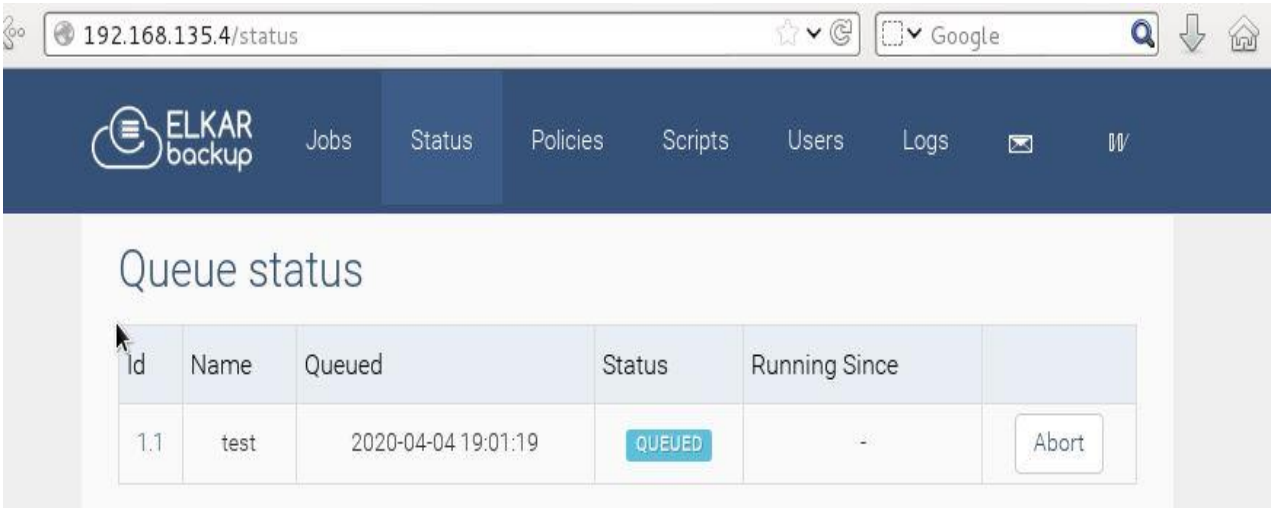


Figure 3.11 : *Statuts de la sauvegarde*

- Configuration de la date et heure de backup dans l'onglet Policies, la sauvegarde est effectuée chaque jour, qui consiste à effectuer la sauvegarde des fichiers modifié. A 11 heures, à 14 heures et à 17 heures de lundi jusqu'au vendredi. Ces logiciels ont des configurations manuelles, pas simplement à une heure par jour, mais aussi par semaine ou par mois. [3.06]

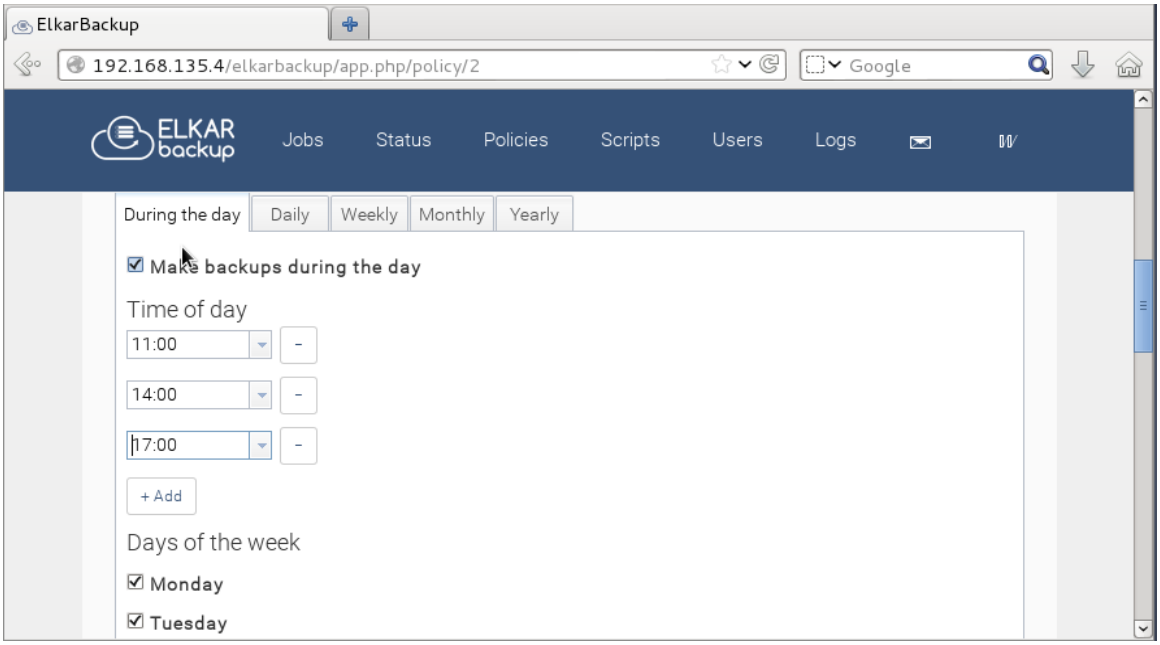


Figure 3.12 : *Configuration du date et heure de sauvegarde*

- La notification par mail aussi est possible pour avertir les utilisateurs par les actions effectuer dans son compte de sauvegarde. Le choix du message peut être tous les messages, ou certaines erreurs seulement, ou aussi quelque avertissement, présenté par la Figure 3.11.

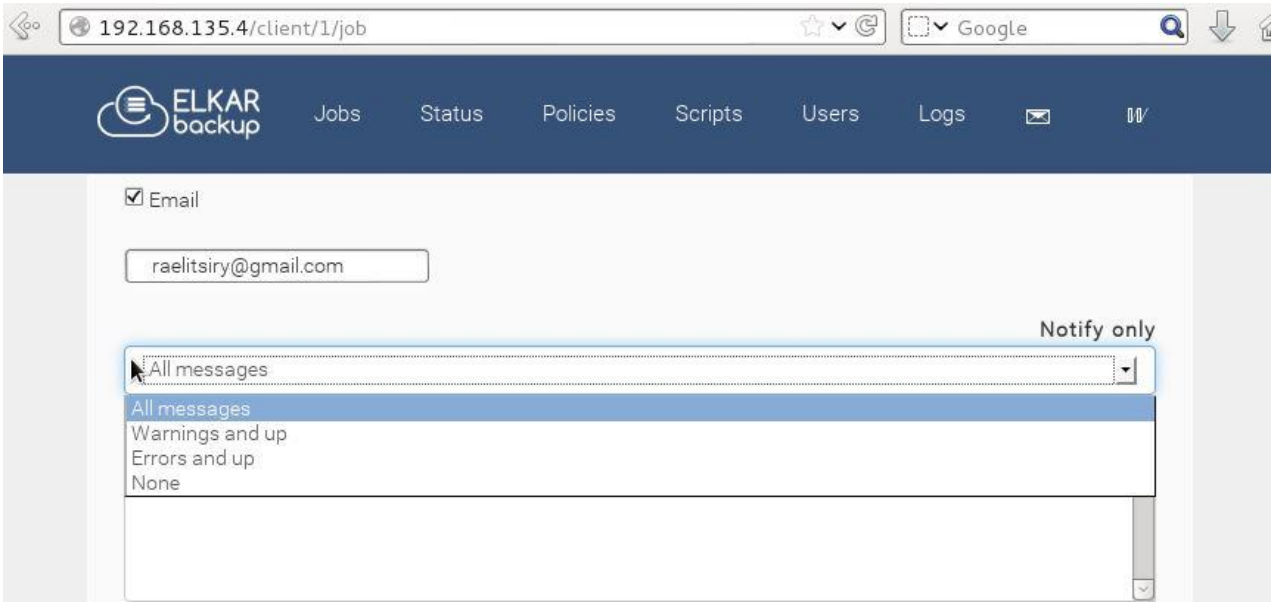


Figure 3.13 : *Notification par email*

3.3.4 Restauration

Pour la restauration des données sauvegardé, cliquer sur le logo de restauration comme montre la Figure 3.12, entouré par la zone rouge.

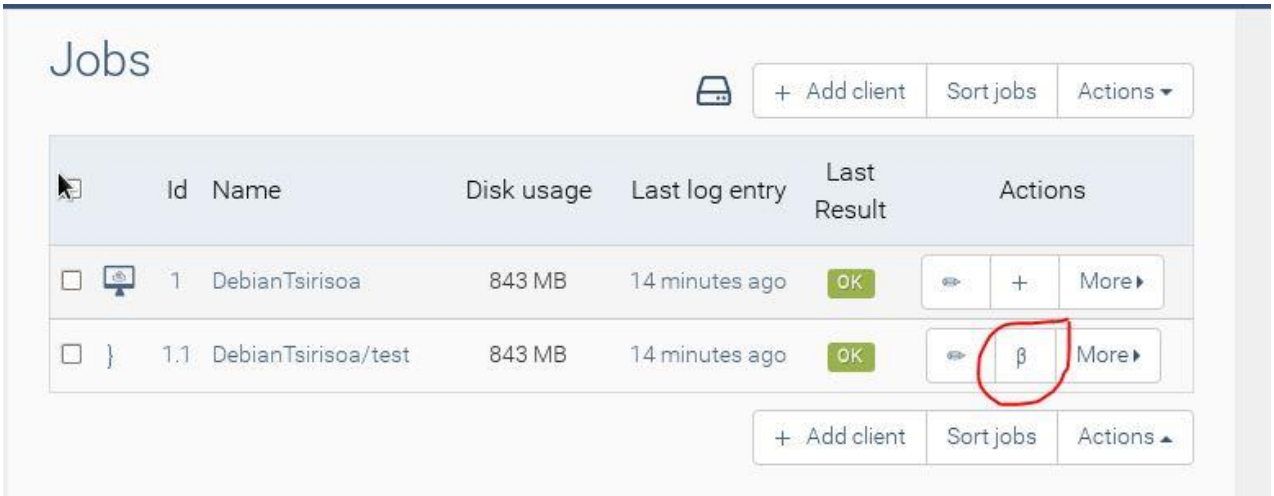


Figure 3.14 : *Point de restauration*

La page de restauration s'affiche et les détails de toutes les sauvegardes effectuer y aussi. Cliquer sur le lien « restore to client » et la page 3.13 s'affichera qui s'appelle restore backup task, qui comporte le nom de machine qui a effectué la sauvegarde, le lieu de la sauvegarde et enfin la destination de la restauration qui sont à remplir manuellement. Dans la figure ci-dessous, on effectue une restauration de la machine DebianTsirisoa, le dossier est mis dans « .sync » et on veut le restaurer dans le fichier « Documents » de la machine client.

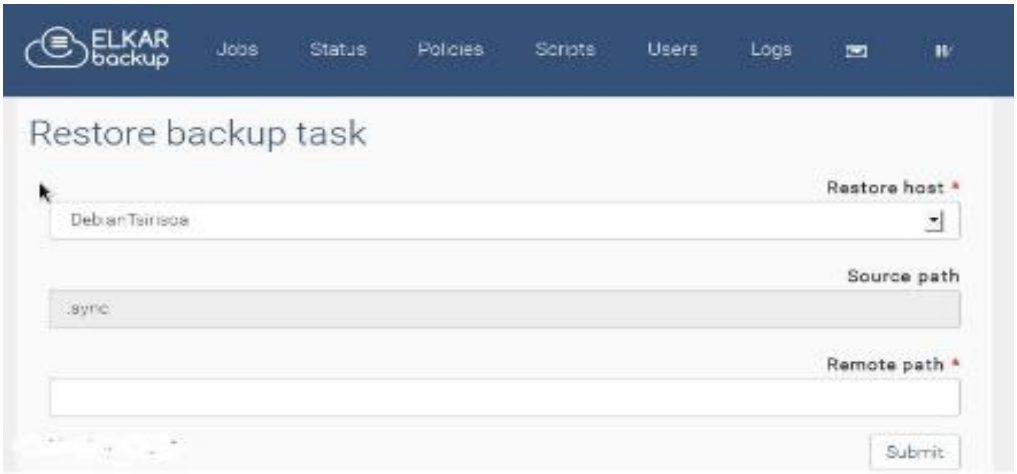


Figure 3.15 : *Restore backup task*

3.3.5 Etat du disque de sauvegarde

L'état du disque de sauvegarde est le plus importante lors d'une sauvegarde ou backup dans une entreprise. Car ou cas ou le disque est endommagé, on peut perdre un certain nombre de donnée, ou aussi le disque est plein, il ne recevra aucune donnée envoyée par les clients. Alors c'est très important de le surveiller et l'entretenez. L'espace et l'état du disque se trouve dans l'onglet ou montre la Figure 3.14 entourer par la zone rouge.

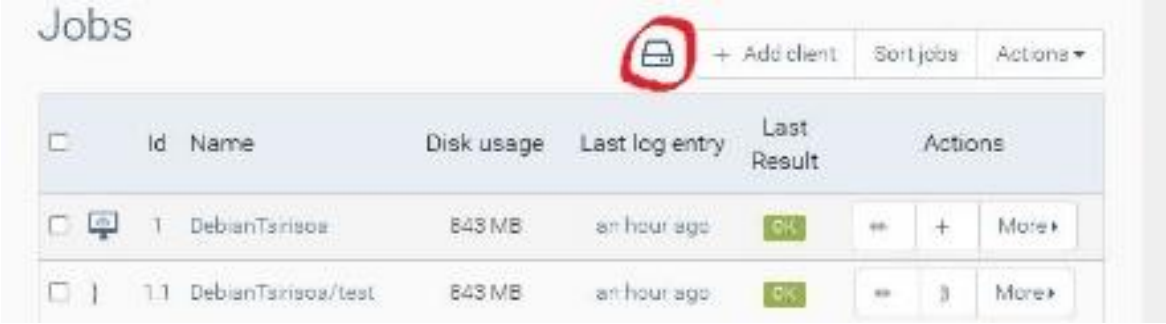


Figure 3.16 : *Etat du disque*

3.4 Replication

La réplication des données est le fait de faire une sauvegarde de toutes les données déjà sauvegardé dans la machine de sauvegarde. Cette sauvegarde est probablement une sécurité, puisqu'en cas d'endommagement du disque de sauvegarde ou perditions, on peut se sauver de la machine de réplication. Cette système de réplication ne consomme pas beaucoup de disque puisqu' il y a des systèmes de compression utilisée, alors dans ce cas, la restauration des données se réfère par les dates de réplication. Deux logiciels prennent des rôles très importantes dans cette réplication ; ce sont rsync pour la synchronisation des données et crontab pour l'automatisation des tâches.

3.4.1 Rsync

Rsync est un logiciel libre qui permet la synchronisation de fichiers de manière unidirectionnelle ; souvent utilisé pour la réalisation de sauvegardes. Ce système de réplication est apporté pour effectuer une autre sauvegarde du serveur de sauvegarde, qu'en cas de non disponibilité du serveur de sauvegarde, le serveur de réplication peut intervenir au fonctionnement. La simulation consiste à la réplication de toutes les données du serveur nextcloud-tsirisoa d'adresse IP 192.168.135.4 vers le serveur DebianReplication d'adresse IP 192.168.135.5.

Tableau 3.08 : *Installation de rsync*

Commande	Exécution
Rsync options sources destination	Installation de rsync

3.4.1.1 Configurations

Par défaut, rsync utilise SSH. Ce qui veut dire que pour chaque commande rsync, un mot de passe vous sera demandé. Puisque les sauvegardes sont habituellement automatisées, ce n'est pas l'idéal. Il faut donc en amont générer une paire de clés pour SSH puis faire la propagation sur le serveur distant afin de pouvoir s'authentifier sans mot de passe (authorized_keys). La paire de clés suivante génère après l'installation de rsync.

Tableau 3.09 : *Commande d'installation de ssh*

Commandes	Exécution
Ssh-keygen	Générer une paire de clé
Ssh-copy-id root@192.168.135.4	Copie sur le serveur distant

Après avoir effectué cette commande, la permission d'accès à distance est donnée, alors les deux serveurs peuvent se connecter sans mot de passe. La commande suivant montre ces accès autorisés.

```
root@debian:/home/replicationserv# ssh-copy-id root@192.168.135.4
root@192.168.135.4's password:
Permission denied, please try again.
root@192.168.135.4's password:
Now try logging into the machine, with "ssh 'root@192.168.135.4'", and check in:

  ~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

3.4.1.2 Sauvegarde complète

Dans ce cas, la sauvegarde complète des données de la machine nextcloud-tsirisoa vers la machine DebianReplication est nécessaire. C'est-à-dire la sauvegarde de l'intégralité des données. Montrer par la commande suivante.

Tableau 3.10 : *Réplication complète*

Commande	Exécution
Rsync -avHP --numeric-ids root@192.168.135.4:/ /backups/	Réplication des données dans la machine 192.168.135.4 dans le dossier backups vers le serveur de réplication

Après avoir lancer cette commande, la sauvegarde complète est effectuée. Pendant la sauvegarde, on peut voir le temps écrouler de la sauvegarde. La réplication effectue 378kbits par seconde de transfert de donnée. Ce transfert se fait sans connexion internet, seulement la connections sans mot de passe avec ssh.

La commande suivante peut afficher la taille des données dupliqué complètement.

```
root@debian:/home/replicationserv# du -hs /var/backups/
2,9G    /var/backups/
```

3.4.1.3 Sauvegarde incrémentielle

Après avoir effectué la sauvegarde complète, on effectue tout simplement une sauvegarde incrémentielle. C'est-à-dire, on fait la sauvegarde des fichiers ajouter, modifié ou supprimé seulement, la commande est la suivante :

```
root@debian:/var/backups# rsync -auvHP --numeric-ids --delete --backup --backup --backup-dir=/backup/old-srv-1/$
date/ root@192.168.135.4:/var/backups/ /backups/
```

Explications des diverses commandes :

- u : mettre à jour uniquement les fichiers modifiés.
- delete : efface les fichiers qui n'existent pas dans le répertoire source.
- backup : effectue une sauvegarde des fichiers modifiés/supprimés.
- backup-dir : précise l'emplacement de sauvegarde des fichiers modifiés/supprimés.
- $date : la variable d'environnement qui nous permet de créer un dossier à la date du jour.

3.4.1.4 Variable d'environnement date

Pendant la réalisation d'une sauvegarde incrémentielle, dont le but que tous les fichiers qui ont été modifiés ou supprimés aillent dans un autre répertoire. Pour faire les choses proprement, et ainsi avoir une arborescence claire dans les dossiers, le mieux est d'avoir des répertoires avec dates. Pour permettre d'inclure la date dans une commande rsync, c'est pourquoi l'ajout une variable d'environnement date est nécessaire.

On édite le fichier /etc/profile et on ajoute la ligne par le code suivant :

Tableau 3.11 : *Commande d'environnement date*

Commande	Exécution
`root@debian:/etc# nano profile`	Ouvrir le fichier profile dans l'éditeur nano
`date=$(date +%d-%m-%y)`	Commande ajouter dans le fichier profile pour ranger chaque sauvegarde par date, d (day), m (mounth), y (year)
`eplicationserv@debian:~$ echo $date`	Affichage des dates des réplications

Après cette commande, toutes les données sont rangées par la date de réplication, alors si quelqu'un consulte certaines données c'est très facile de les trouver.

3.4.2 Crontab

Toutes ces configurations sont faites manuellement, mais les sauvegardes incrémentielles doivent se faire automatiquement. C'est pourquoi on a besoin de ce logiciel libre qui sert à automatiser les taches. Le fichier de configuration de crontab se trouve dans /etc/crontab.

Tableau 3.12 : *Syntaxes de crontab*

Champ	Description	Valeur accepter
M	Minute	0-59
H	Heure	0-23
Dom	Jour du mois	1-31
Mon	Mois	1-12
Dow	Jours de la semaine	0-6
User	Utilisateur	N'importe quel utilisateur
command	Commande	N'importe quel commande

3.4.2.1 Configurations

- Installation

```
root@debian:/home/replicationserv# apt-get install cron
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
cron est déjà la plus récente version disponible.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

- Exécution de la sauvegarde avec crontab

Ouvrir le dossier /etc/crontab puis écrire la commande ci-dessous, qui veut dire faire une sauvegarde incrémentielle chaque vendredi à 18 heures. C'est possible aussi d'envoyer un mail automatique vers les utilisateurs qui planifie une tache.

```
00 18 * * 5 root rsync -auvHP --numeric-ids --delete --backup --backup-dir=
$r=/backups/$date/ root@192.168.135.4:/datas/ /backups/
```

3.4.3 Compression des fichiers

Pour gagner plus d'espace, la compression des fichiers est la manière la plus proche. Cette compression est effectuée après la sauvegarde ce qui entraine la compression et la suppression du répertoire.

- Compression simple du fichier

```
root@debian:/var# tar -czvf /backups.gz /backups/
```

```
/backups/dpkg.diversions.3.gz
/backups/dpkg.diversions.4.gz
/backups/dpkg.statoverride.3.gz
/backups/dpkg.status.5.gz
/backups/passwd.bak
/backups/dpkg.diversions.5.gz
/backups/alternatives.tar.2.gz
/backups/dpkg.status.6.gz
/backups/dpkg.statoverride.1.gz
/backups/alternatives.tar.1.gz
/backups/apt.extended_states.1.gz
/backups/apt.extended_states.3.gz
/backups/dpkg.statoverride.4.gz
/backups/dpkg.status.2.gz
/backups/data/
/backups/dpkg.statoverride.2.gz
/backups/dpkg.status.4.gz
/backups/dpkg.diversions.0
/backups/alternatives.tar.0
/backups/dpkg.status.3.gz
/backups/dpkg.diversions.2.gz
```

- Compression et suppression du répertoire

```
root@debian:/var# tar -czvf /backups.gz /backups/ && rm -R /backups
/backups/passwd.bak
/backups/dpkg.diversions.5.gz
/backups/alternatives.tar.2.gz
/backups/dpkg.status.6.gz
/backups/dpkg.statoverride.1.gz
/backups/alternatives.tar.1.gz
/backups/apt.extended_states.1.gz
/backups/apt.extended_states.3.gz
/backups/dpkg.statoverride.4.gz
/backups/dpkg.status.2.gz
/backups/data/
/backups/dpkg.statoverride.2.gz
```

- Décompression des fichiers

```
root@debian:/var# tar -xzvf /backups.gz -C /backups/
```

```
backups/dpkg.diversions.3.gz
backups/dpkg.diversions.4.gz
backups/dpkg.statoverride.3.gz
backups/dpkg.status.5.gz
backups/passwd.bak
backups/dpkg.diversions.5.gz
backups/alternatives.tar.2.gz
backups/dpkg.status.6.gz
backups/dpkg.statoverride.1.gz
backups/alternatives.tar.1.gz
backups/apt.extended_states.1.gz
backups/apt.extended_states.3.gz
backups/dpkg.statoverride.4.gz
backups/dpkg.status.2.gz
backups/data/
backups/dpkg.statoverride.2.gz
backups/dpkg.status.4.gz
backups/dpkg.diversions.0
backups/alternatives.tar.0
backups/dpkg.status.3.gz
backups/dpkg.diversions.2.gz
backups/dpkg.statoverride.0
backups/group.bak
```

3.5 Conclusion

Ce chapitre a permis la conception d'une solution de sauvegarde dans une entreprise ou locaux. La simulation a été faite avec une logiciel de sauvegarde appelé Elkarbackup. La conception consiste à sauvegarder les données dans un serveur de sauvegarde puis les répliquer vers un autre serveur. Quant aux divers matériels de stockage comme le disque qui ne cessent d'évoluer dans le temps, les plus appréciés pour les tâches de sauvegarde demeurent considérablement coûteux. Ce qui présente un autre handicap pour la réalisation de ce projet. Cependant, ses avantages demeurent pertinents. Sans parler de la portabilité et de la flexibilité du système car l'essai effectué dans l'entreprise a été très réussit. Cette essaie a été suivie par la comparaison des différents logiciels de sauvegarde mais Elkarbackup a été le plus fiable et réalisable dans une entreprise. En perspectives, l'entreprise envisages réaliser ce projet, et aussi crée un autre serveur pas pour eux simplement mais pour les autres entreprises qui ont besoin de stocker leurs données ailleurs pour les protéger.

CONCLUSION GENERALE

Une entreprise doit être capable de se relever rapidement suite à un sinistre dont la principale cause peut être la simple défaillance d'un composant ou bien la destruction complète d'une machine contenant les données vitales. Avec une planification adaptée, les services de sauvegarde et de restauration permettent de remédier à la situation. La mise en place du système de sauvegarde sur le réseau exige qu'on y consacre du temps précieux notamment dans les paramétrages. D'un autre côté, le choix du type de sauvegarde peut laisser perplexe. Ceci dit, il faut parfaitement maîtriser les principes utilisés en termes de sauvegarde et considérer chaque situation comme un cas exceptionnel. La sécurisation aussi prend un grand rôle dans la sauvegarde, plusieurs types comme le système cryptographie, la sécurité via DMZ ou DeMilitarize Zone et Firewall peuvent être utilisée en analysant le cas et la situation de l'entreprise. Les performances des logiciels de sauvegarde ont une importance cruciale pour assurer la sécurité des données, incluant l'encryptions des données qui est l'une des nouvelles technologies de sécurisation moderne. En effet, la fiabilité et la performance doivent être à la hauteur des enjeux et des besoins de l'entreprise qu'il doit satisfaire. Quant aux restaurations, il existe plusieurs types mais certain sont de faible fiabilité, donc le choix de la technique est vraiment important. Afin de satisfaire les attentes des utilisateurs sur l'utilisation de la sauvegarde.

Des améliorations telles que la répartition des différentes tâches sur différents équipements, l'utilisation de protocoles et de techniques pour assurer une meilleure utilisation des ressources ont été identifiées. En plus, dans ce projet seul les bases des données, les fichiers, les dossiers sont à la disposition de sauvegarde donc la réalisation d'une sauvegarde des machines comme sa configuration et son intégrité des données est un sujet très intéressant pour pouvoir récupérer tous les fonctionnements en cas de sinistre ou endommagement.

ANNEXE

Annexe : INSTALLATION ET COMMANDES DES MACHINES

A1.1 Installation de machine clients sur Virtualbox

Cliquez l'enveloppe jaune, insérez une disque Debian puis démarrez l'installation.

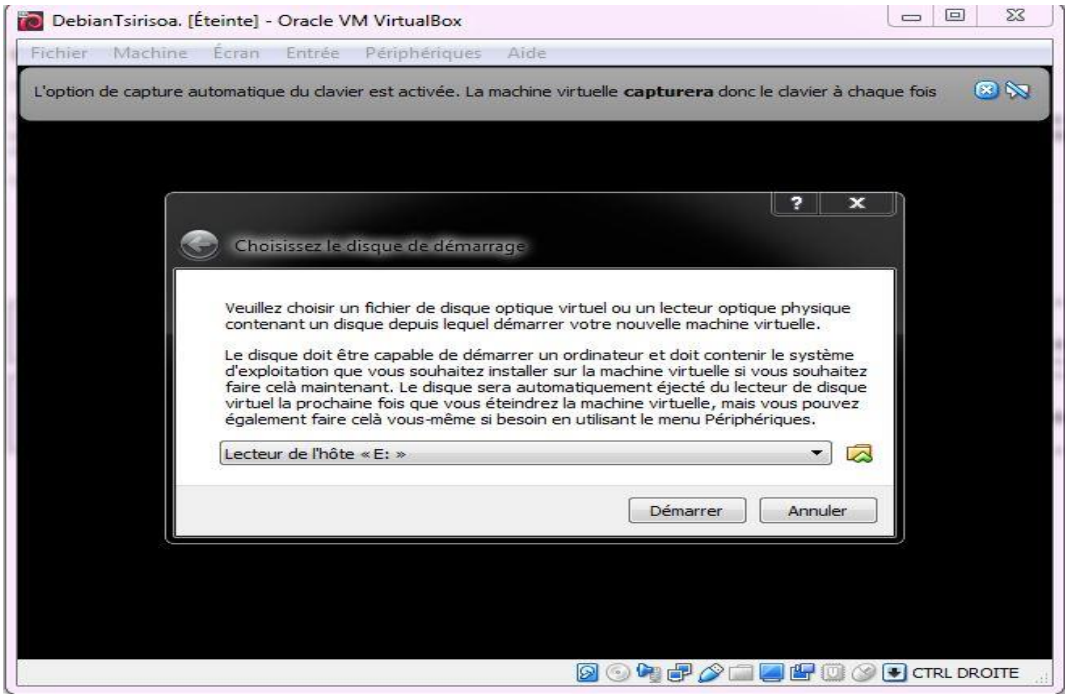


Figure A1.01 : Montage du disque Debian

Choisir le langage de machine

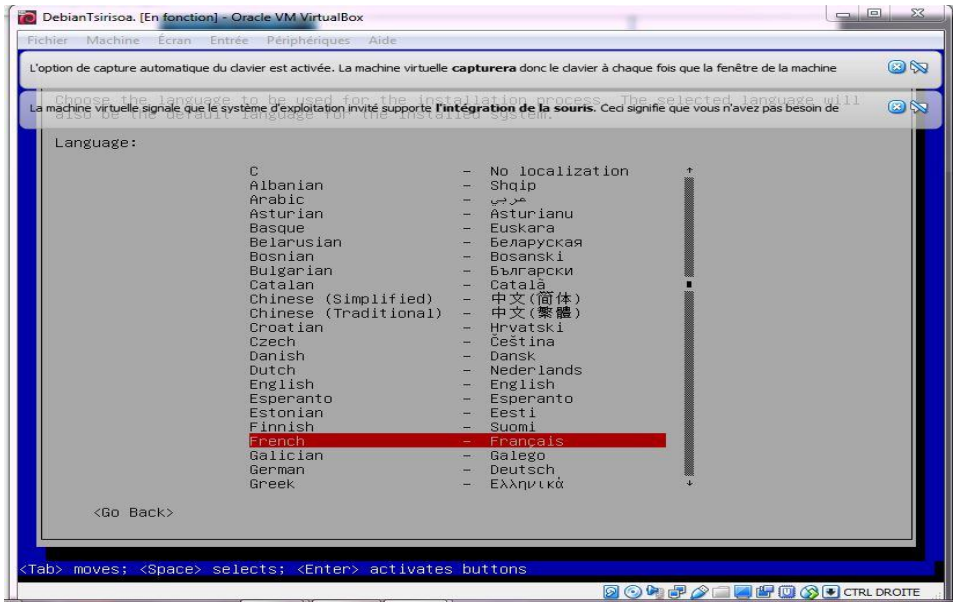


Figure A.02 : Montage du disque Debian

Le mot de passe du Super utilisateur Root est très important pendant l'installation. Remplir les vides et poursuivre l'installation jusqu'à la fin.

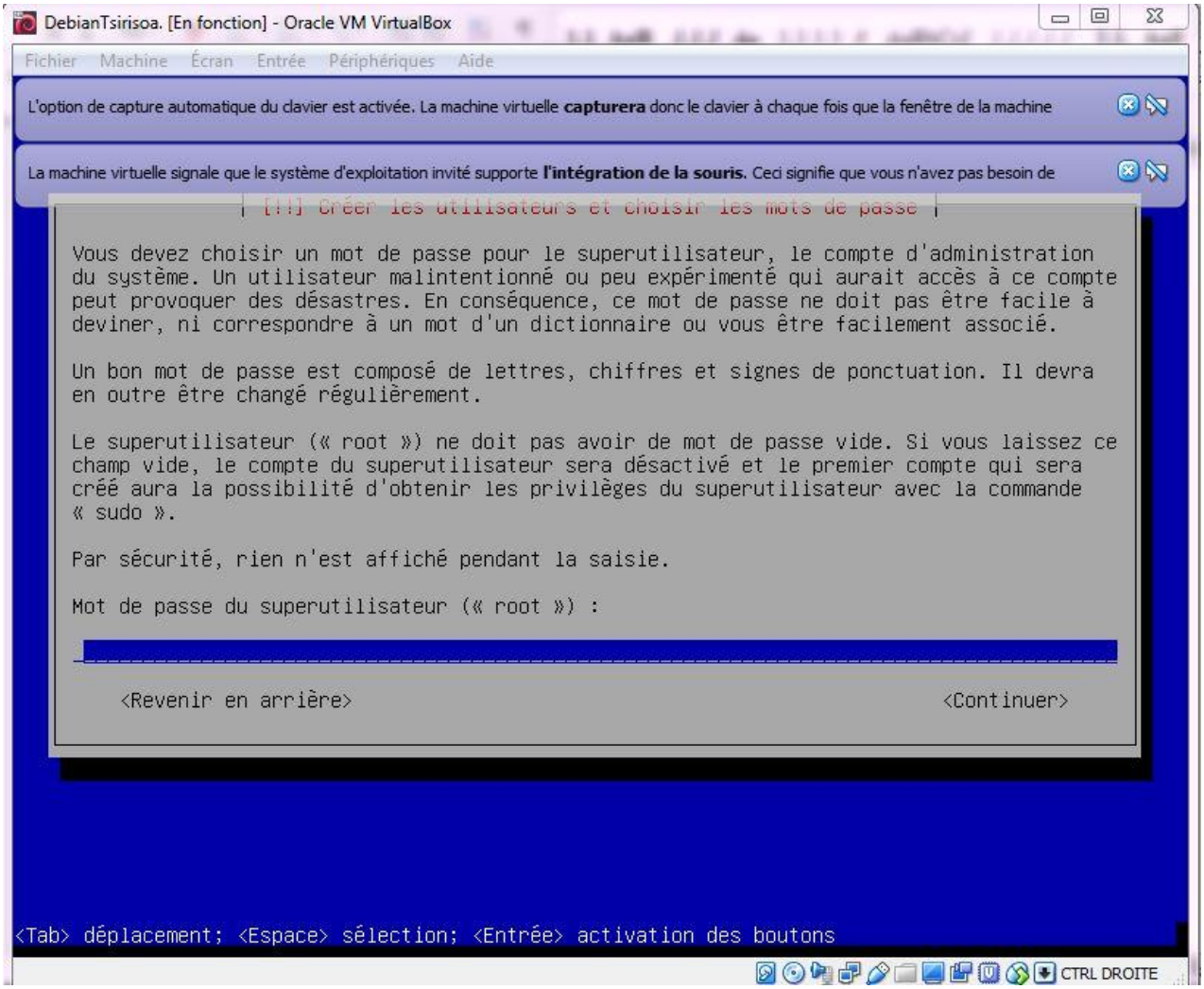


Figure A.03 : Mot de passe de super utilisateur Root

L'installeur Debian installe automatiquement la configuration reseau par DHCP. Mais pour que les trois machines installées sont au même réseaux dans Virtualbox, la configuration du carte réseaux est très nécessaire pour faire fonctionner la liaison des trois machines.

Figure A.04 : Configuration du reseau avec DHCP

A1.2 Quelques périphériques utiles

Les périphériques suivant ne correspondent à aucun matériel mais ce sont des périphériques spéciaux très utiles.

Tableau A1.01 : L'arborescence d'un système Linux

Répertoire	Description
/	Répertoire racine, point d'entrée du système de fichiers
/boot	Répertoire contenant le noyau le noyau Linux et l'amorceur
/bin	Répertoire contenant les exécutables de base, comme par exemple cp, mv, ls, …
/dev	Répertoire contenant des fichiers spéciaux nommé devices qui permettent le lien avec les périphériques de la machine.
/etc	Répertoire contenant les fichiers de configuration du système
/home	Répertoire contenant les fichiers personnels des utilisateurs (un sous-répertoire par utilisateur)
/lib	Répertoire contenant les librairies et les modules du noyau (/lib/modules)
/media	Répertoire contenant les « points de montage » des médias usuels : CD, DVD, disquette, clef USB
/root	Répertoire personnel de l'administrateur
/sbin	Répertoire contenant les exécutables destinés à l'administration du système
/tmp	Répertoire contenant des fichiers temporaires utilisés par certains programmes
/usr	Répertoire contenant les exécutables des programmes (/usr/bin et /usr/sbin), la documentation (/usr/doc), et les programmes pour le serveur graphique (/usr/X11R6).
/var	Répertoire contenant les fichiers qui servent à la maintenance du système (les fichiers de journaux notamment dans /var/log)

A2.1 Quelques commandes très utiles sur Debian

Tableau A1.02 : Commande important sur Debian

Utilisation	Commande	Description
Configuration de la carte réseaux	ifconfig -a	Obtenir la liste des interfaces réseaux détecté
	ifconfig <interfaces> <adresse IP>	Ajouter une adresse IP sur une carte réseaux
	Ifconfig eth0	Voir si l'adresse est bien configuré
Passerelle	route add default gw <adresse ip>	Ajouter une passerelle
Teste	Ping <adresse IP>	Tester le réseaux
Nom d'hôte	/etc/init.d/hostname.sh	Démarre le système

NFS (Network File System) (Permet le partages des fichiers entre des machines)	Ps ax | grep nfsd (coté serveur)	Vérification des daemons NFS si elle est déjà lance ou pas
	/etc/init.d/nfs-kernel-server start	Lancement du daemons NFS coté serveur
	/etc/init.d/nfs-user-server start	Lancement du daemons NFS coté utilisateur (on peut remplacer start par restart pour le redémarrage)
	/home <nom ou IP de la machine autorisées à se connecter> (rw) <autre machine> (ro)	Configuration des répertoires a partagés • rw : lecture/ ecriture (option) • ro : lecture seule
	/etc/init.d/nfs-kernel-server reload	Relancer NFS pour prendre en compte les modifications
	Mount –t nfs <machine distante> :<repertoire partagé> <repertoire local> -o <option>	Installation coté client
Apache	/var/log/apache2/error.log	Pistes pour trouver la solution quand il y a une problème
	/etc/init.d/apache2 reload	Commande à lancer après une certaine modification
	/etc/apache2/mods-available	Répertoire qui contient les modules installés
	/etc/apache2/mods-enable	Répertoire qui contient les modules activés
	htpasswd –c /etc/apache2/my_passwd tsirisoa	Créer Tsirisoa comme première utilisateur
	Htpasswd /etc/apache2/my_pass tsiry	Ajouter ou modifier un utilisateur à un fichier de mots de passe existant
SSH (Secure SHell)	/etc/init.d/ssh	Manipulation du daemon
	Ssh –l <login> <adresse du serveur SSH>	Pour s'authentifier dans le serveur SSH
	Ssh-keygen –t dsa	Pour générer un couple de clés
FTP (File Transport Protocol)	aptitude install lftp	Installation du paquet FTP
	cp ~ /fichiers-config/lftp.conf /etc/	Installation du fichier de configuration
	lftp ftp://tsirisoa@ftp.debian.org	Utilisateur tsirisoa sur le serveur ftp.debian.org
DHCP (Dynamic Host Configuration Protocol)	/etc/init.d/dhcp-server restart	Redémarrer le serveur DHCP
	/etc/dhcp/dhcpd.conf	Fichier de configuration du serveur dhcp

REFERENCES

[1.01] K. Razafimahaleo, *« Conception de réseau de campus d'entreprise »*, Antananarivo 2016.

[1.02] K. Razafimahaleo, *« Conception de réseau de campus d'entreprise »*, Antananarivo 2016.

[1.03] O. Aubert, « *Gestion de réseaux*», Paris 2005.

[1.04] D. DROMARD et D. Seret, *« Architecture des réseaux »,* Pearson Education France 2009.

[1.05] E. Lattie, *« Cours réseau »* ; Openclassroms, Professeur réseau.

[1.06] G. Pujolle, *« Initiation aux réseaux »,* www.editions-eyrolles.com, Edition 2001.

[1.07] C. Servin, *« Réseaux et Télécoms »,* Chargé de cours au CNAM de Paris et en école d'ingénieur, Paris 2003.

[1.08] R. Guichard, *« Apprenez le fonctionnement du réseau TCP/IP »,* www.openclassroms.com, Licence Créative Commons 6 2.0

[1.09] G. Pujolle, *« Les réseaux »,* www.editions-eyrolles.com, édition septembre 2004.

[1.10] *« L'informatique simplement »*, www.ccm.com, publié le 22 octobre 2014.

[1.11] Nicolas Jean, http ://www.nicolasjean.com, www.iprelax.fr,

[1.12] G. Pujolle, *« Les réseaux »,* www.editions-eyrolles.com, édition 2008.

[2.01] J. Y. Rétif, *« Installation d'une nouvelle salle avec les outils Backup »,* Echirolles Janvier 2000.

[2.02] Https ://www.johannesrabeyrin.fr/backup-les-differents-types-de-sauvegardes, consulté le 20 mars 2019.

[2.03] M. Rakotomalalanirina, *« Solution de stockage et de partage de données »*, Fianarantsoa 2012.

[2.04] M. Le Cocq , *« Applications Client/Serveur et Web »*, Licence Pro SIL, 17 Janvier 2017.

[2.05] M. Rakotomanolo, *« Migration d'une base de données SQL vers NoSQL »*, mémoire fin d'étude d'obtention du diplôme d'Ingénieur, ESPA, AU :2017-2018.

[2.06] https ://www.oodrive.fr/blog/securite/restauration-des-données-sinistre-informatique, consulté le 20 mars 2019.

[2.07] https ://www.digitalocean.com/community/tutorials/how-to-set-up-master-slave-replication-in-mysql, consulté le 20 mars 2019.

[2.08] Thomas Fuhr https://pastel.archives-ouvertes.fr/pastel-00674580. Conception, preuves et analyse de fonctions de hachage cryptographiques, consulté le 20 mars 2019.

[2.09] R.S. Rakotondramanana, *« Post-quantum crypto spécifié par l'organisation nist»* , Mémoire fin d'étude d'obtention du diplôme d'Ingénieur , ESPA, AU : 2015-2016.

[2.10] Y. MORERE, *« Mise en place de serveur de sauvegarde à moindre coût »*, édition 23 octobre 2009.

[3.01] https://www.commentcamarche.net/download/telecharger-3673479-virtualbox, consulté le 12 avril 2019.

[3.02] https ://www.elkarbackup-installation, consulté le 20 mars 2019.

[3.03] https://www.nextcloud-documentation, consulté le 12 avril 2019.

[3.04] Y. MORERE, *« Système de sauvegarde »*, édition avril 1999.

[3.05] R. Bizoï, *« Sauvegarde et sécurité »*, édition Eyrolles 2011.

[3.06] www.sauvegarde_restauration.com/france, consulté le 15 avril 2019.

[3.07] https://www.acronisbackups_advanced, consulté le 24 mars 2019.

FICHE DE RENSEIGNEMENTS

Nom : RAELINIAINA

Prénom : Tsirisoa

Adresse de l'auteur : 0708 K 274 Ambohimena Antsirabe

Téléphone : +261 34 29 364 97

E-mail : **raelitsiry@gmail.com**

Titre du mémoire : CONCEPTION D'UNE SOLUTION DE SAUVEGARDE DE DONNEE AVEC ELKARBACKUP (cas de l'Alternateeve Technology Lab)

Nombre de pages : **57**

Nombre de tableaux : 23

Nombre de figures : **30**

Directeur de mémoire : Monsieur RAKOTONDRAMANANA Radiarisainana Sitraka

Téléphone : +261 34 40 400 80

Mail : radiarisainanasitraka@yahoo.fr

FAMINTINANA

Ankehitriny dia mivoatra hatrany ny teknolojia, indrindra amin'ny tontolon'ny informatika. Orinasa maro be izao no mampiasa ny rafi-tahiry afovoany mba hanamorana ny fivezivezin'ny fampahalalana, mahita an'io fanatontosana sy io fikajiana loza io mihodinkodina. Manoloana izany dia teraka ny foto-kevitra momba ny fitahirizana mba hisorohana ny loza mety hitranga amin'ny orinasa. Vahaolana nomaniny ho solon'izay natao hamahana ireo olany. Rindrambaiko sy teknika marobe no efa novolavolain'ny mpikaroka hamahana ny olany. Amin'ity toe-javatra ity, ny vahaolana nomanina ho solon'izay miaraka amin'i Elckarbckup mba hananana angona azo antoka sy voaaro tsara amin'ny orinasa iray. Noho izany, ity boky ity dia mampiseho ny ankapobeny amin'ny tambajotran'ny solosaina ary avy eo ny dingana sy ny teknika samihafa amin'ny famerenana ny tahiry ary amin'ny farany ny fanatanterahana miaraka amin'ny Elckarbackup.

Teny misongadina : Fitahirizana, Fanavaozana, Fitahirizana tanteraka,Tahiry, Fitantanana

RESUME

De nos jours la technologie ne cesse de s'évoluer surtout dans le monde du domaine informatique. Grand nombre d'entreprise utilise maintenant le système de centralisation de données pour faciliter la circulation de l'information, voir cette centralisation et cette circulation plusieurs dangers tourne autour. Face à cela, le concept de sauvegarde est né afin d'éviter les risques de destruction de l'entreprise. Une solution de sauvegarde a été conçu pour résoudre ses problèmes. Plusieurs logiciels et techniques ont déjà développé par les chercheurs pour résoudre ses problèmes. Dans ce contexte, la solution de sauvegarde avec Elckarbckup afin d'avoir une donnée assurer et bien protéger dans une entreprise. De ce fait, ce livre illustre la généralité sur les réseaux informatiques puis les protocoles et les différents techniques de sauvegarde de donnée et enfin la réalisation de la sauvegarde avec Elckarbackup.

Mots clés : Sauvegarde, Restauration, Réplication, Données, Administration.

ABSTRACT

Today technology continues to evolve, especially in the informatic world. A large number of companies now use the centralized data system to facilitate the flow of information, seeing this centralization and this flow several dangers revolve around. Faced with this, the concept of backup was born in order to avoid the risk of destruction of the company. A backup solution was designed to solve its problems. Several software and techniques have already developed by researchers to solve its problems. In this context, the backup solution with Elckarbckup in order to have data to be insured and properly protected in a company. Therefore, this book illustrates the generality on computer networks then the protocols and the different techniques of data backup and finally the realization of the backup with Elckarbackup.

Keywords : Backup, Restore, Replication, Data, Administration.