Remerciement

Nos remerciements vont droit à Madame Achemoukh d'avoir accepter de nous encadrer. Nous vous remercions pour la gentillesse et la spontanéité avec lesquelles vous avez bien voulu diriger ce travail. Nous avons eu le grand plaisir de travailler avec vous, et avons trouvé auprès de vous la conseillère et la guide qui nous a reçu avec sympathie et bienveillance.Veuillez trouver dans ce modeste travail l'expression de notre haute considération, de notre sincère reconnaissance et de notre profond respect,

Nos remerciements vont droit aux membres du jury, c'est pour nous un grand honneur de vous voir siéger dans notre jury. Nous vous sommes très reconnaissants, de L'amabilité avec laquelle vous avez accepté de juger notre travail. Veuillez trouver le témoignage de notre grande reconnaissance et de notre profond respect.

Nos remerciements vont droit à Monsieur Nadour, chef de service du centre des réseaux et des systèmes informatiques, d'avoir accepté notre demande de stage, de nous avoir encouragé avec vos conseils fructueux, de nous avoir laissé manipulé les équipements réseaux du service. Nous vous remercions pour votre sympathie et spontanéité avec lesquelles vous nous avez reçu. Veuillez, trouver dans ce modeste travail l'expression de notre haute considération, de notre sincère reconnaissance et de notre profond respect .

Dédicaces

Je tiens à dédier notre modeste travail :

À la mémoire de mon père

J'aurais tant aimé que tu sois présent. Que Dieu ait ton âme dans sa sainte miséricorde.

À ma chère mère

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.

A mes chers frères et sœurs

Tsouma, Farida, Louiza, Belkacem, Arezki, Djamel , Massinissa En témoignage de mon affection fraternelle, de ma profonde tendresse et reconnaissance, je vous souhaite une vie pleine de bonheur et de succès.

A mes chers et adorables beaux frères et belles sœurs

En témoignage de mon affection fraternelle, de ma profonde tendresse et reconnaissance, je vous souhaite une vie pleine de bonheur et de succès et que Dieu, le tout puissant, vous protège et vous garde.

A mes adorables nièces et neveux

Votre joie et votre gaieté me comblent de bonheur. Que Dieu, le tout puissant, vous protège et vous garde.

À mes cousines et amis

En souvenir de notre sincère et profonde amitié et des moments agréables que nous avons passés ensemble. Veuillez trouver dans ce travail l'expression de mon respect le plus profond et mon affection la plus sincère.

À mes collègues de travail,

Nous avons eu le grand plaisir de travailler avec vous pendant se stage, et avons trouvé auprès de vous les conseillers et les guides qui nous ont reçu en toute circonstance avec sympathie, sourire et bienveillance merci .

À toutes les personnes qui ont participé à l'élaboration de notre modeste travail.

OULARBI GHANIA

Dédicace

Je tiens à dédier notre modeste travail :

A ceux qui m'ont tout donné sans rien attendre en retour mis à part ma réussite, à ceux qui m'ont appris à aller au bout de mes ambitions, à ceux qui ont toujours cru en moi , à la lumière de ma vie, à mes très chers parents. Même si on inventerait des mots, je doute qu'ils seraient suffisants pour exprimer toute ma reconnaissance envers ce que vous m'apporté. Que dieu, vous accorde santé, bonheur, et une longue vie.

A mes adorables chères soeurs : Taous, nacera et hassina et leurs maris.

A mes frére : djamel,youcef, smail et leurs femmes.

A mon beau frère kamel qui est toujours été à mes coté, merci mon frère.

A mes sœurs de cœur Ryma, yassmina, lilya merci pour votre amitié et tous les moments de folie passés ensemble.

A mes meilleur Thileli, katia et mellisa avec qui j'ai partagé les bons et les mauvais moments.

A tous mes autres ami(e)s et mon entourage qui m'ont aidé dans mes études, contribuer de près ou de loin dans l'élaboration de mon travail. Merci à vous tous.

OULD FELLA NORA

Table des matières

1. Hypertext Preprocessor

Table des figures

Liste des tableaux

Introduction générale

Ce projet s'inscrit dans le cadre d'un mémoire de fin d'étude en vue de l'obtention du diplôme Master 2 spécialité Systèmes Informatiques au niveau du département informatique de l'université Mouloud MAMMERI de Tizi Ouzou. Ce projet se déroule au niveau du centre réseaux et système informatiques dont l'infrastructure hétérogène est sensible aux attaques(Attaque par Deni de Service, Attaque par Bruteforce, Attaque par Injection de code, Cross-Site Scripting) et cela vu la multitude d'application Web , service internet, sites internet et le portail de l'université qui y sont hébergés, ainsi qu'une infrastructure réseau de l'université qui y est configurée, la disponibilité de ses services est plus que primordial au niveau du centre, les administrateurs réseaux consultent et se réfèrent aux messages émis par les différents programmes en local et en ligne de commande, cette tâche très fastidieuse et qui peut être impossible en cas de crash d'un serveur client vu l'indisponibilité des messages émis par les programmes chose qui pénalisera ces derniers à trouver une solution ou à comprendre un problème inattendu, c'est dans cette optique que le centre réseau , nous ont posé le problème de sauvegardes des messages émis par les différents systèmes. Nous avons proposé, après étude du problème, une solution de centralisation et d'analyse des fichiers logs du centre des réseaux.

En effet les fichiers de logs sont des ensembles séquentiels de messages émis par un programme informatique rendant compte de son exécution. Un log est un message texte, avec des métadonnées [2] ou non, contenant des informations sur un évènement s'étant produit au sein du programme. L'ensemble des logs révèle donc l'histoire du programme. Ce caractère historique est très précieux quand il s'agit d'identifier un problème qui est survenu. Il suffit d'analyser le fichier de logs pour diagnostiquer le problème et prendre les mesures nécessaires

2. Les métadonnées sont des données qui en décrivent d'autres

L'analyse en temps réel de l'utilisation du système est une opération qui permet de détecter une attaque, voire de l'empêcher, et d'alerter les administrateurs en cas de problème. La seconde est l'étude des traces laissées par l'exploitation d'une vulnérabilité :

cela peut permettre de comprendre la méthode employée par l'attaquant, de mettre en place des contre-mesures ou même de mieux sécuriser l'application c'est dans cet aspect que nous devons orienté notre recherche afin de proposer un solution qui répond aux attentes du service réseau.

Le recours a la centralisation des logs est la garantie du bon fonctionnement de tout système informatique hétérogène qui fonctionne avec des systèmes de plus en plus varié et complexes, dont les réseaux viennent interconnecté tout ces élément entre eux. Cette exploitation assure un niveau de sécurité favorable aux enjeux de ce système et cela n'est possible que par la mise en place des moyens de supervisions étudies et ciblés.

Ce rapport est organisée, en quatre chapitres où il présente l'ensemble des étapes suivies pour développer la solution. Le premier chapitre sera dédié à la présentation des Concepts liés aux traitements des logs Nous commencerons par la définition des fichiers journaux, suivie de l'importance de leur exploitation tout en détaillant les concepts important des fichiers logs et enfin nous allons exposer les différents outils d'analyses, de centralisation, traitement et de récupération des fichiers journaux. Le second chapitre sera consacré à la présentation de l'organisme d'accueil. Ensuite la description du contexte du projet, la problématique et le travail à réaliser. nous exposons par la suite, la méthodologie de travail admise. Le troisième chapitre, analyse et conception, sera consacré à l'architecture de notre application et l'étude détaillée de chaque package avec les différents scénarios possibles afin de concevoir une application réalisable, fiable et efficace. Le quatrième chapitre, la réalisation, nous présenterons l'environnement matériel et logiciel dans lequel le projet a été réalisé. Ainsi que les différents choix techniques liés à cette application, et les contraintes de réalisation. Nous terminons par la présentation de l'interface de l'application.

Chapitre 1

Définitions et Concepts liés aux traitement de logs

1.1 Introduction

Les systèmes informatiques sont devenus de plus en plus complexes et hétérogènes. Tous ces équipements fonctionnent avec des systèmes de plus en plus variés et complexes et les réseaux viennent interconnecter tous ces éléments entre eux. C'est ainsi que dans chaque élément, chaque système et chaque réseau, se posent de nombreux problèmes de sécurité. L'exploitation des logs est devenu la solution incontournable dans la détection des anomalies liés à l'utilisation des systèmes informatiques, vu que le contenu de ces derniers nous renseignes clairement sur la traçabilité des différentes exécutions du système.

Nous présenteront dans ce chapitre les différents concepts liés aux logs , les différents utilitaires de traitement de logs , les étapes à suivre pour la réalisation des serveurs de logs . Nous commencerons par la définition des fichiers journaux, suivie de l'importance de leur exploitation tout en détaillant les concepts important des fichiers logs et enfin nous allons exposer les différents outils d'analyses, de centralisation, traitement et de récupération des fichiers journaux.

1.2 Généralités sur la réalisation des serveurs de logs

1.2.1 les fichier logs

Les fichiers logs nommés dans la littérature les fichiers journaux, sont des fichiers qui contiennent des messages relatifs au système, y compris au noyau, aux services et aux applications qui s'y rapportent. Ils se présentent sous formes d'ensembles séquentiels de messages émis par un programme informatique rendant compte de son exécution.

Un log est un message texte, avec des métadonnées contenant des informations sur un évènement s'étant produit au sein du programme. L'ensemble des logs révèle donc l'histoire de l'exécution d'un programme. Ce caractère historique est très précieux quand

il s'agit d'identifier un problème qui est survenu. Il suffit d'analyser le fichier de logs pour diagnostiquer le problème et prendre les mesures nécessaires. Par ailleurs, les logs sont générés en temps réel. Il est donc possible de s'en servir pour surveiller l'exécution des programmes dont la structure et le contenu de ce fichier permettent d'obtenir de plus amples informations après certains traitements. Le format le plus répandu de fichier log est le format ELF [1] . Chaque ligne de ce fichier donne une information sur l'utilisateur, son matériel, la date et l'heure de la requête, la page requise, le statut de la page requise, la page de référence ainsi que quelques informations liées au protocole d'échange de données. Et le format CLF [2] a la même structure qu'Elf mais ne contient pas le « référer » (désignant le navigateur, le système exploitation de l'ordinateur client et ainsi d'autres paramètres éventuels. [CHARRAD.M, 2005] [BOURGET.E, 2016]

la figure suivante représente un exemple de fichier log

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console
by pr on vty0 (203.200.80.75)

CI-3-TEMP: Overtemperature warning

Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed
state to down
```

FIGURE 1.1 – exemple de fichier log

1.2.2 L'importance de l'exploitation des fichiers logs

En informatique les logs présentent un intérêt d'une importance cruciale, ils nous permettent :

1. Expliquer une erreur, un comportement anormal, un crash sur un service comme un service web.

1. Extended log format
2. common log format

2. Retracer la vie d'un utilisateur, d'une application, d'un paquet sur un réseau sur les logs d'un proxy et des éléments réseau par exemple.
3. Comprendre le fonctionnement d'une application, d'un protocole, d'un système comme les étapes de démarrage d'un service SSH [3] sous Linux.
4. Être notifié d'un comportement, d'une action, d'une modification tel qu'une extinction ou un démarrage système

1.2.3 les types des fichiers logs

Chaque action d'un système informatique produit un fichier log. Ces fichiers textes listent chronologiquement les évènements exécutés par un serveur ou une application informatique. Ils s'avèrent utiles pour comprendre la provenance d'une erreur en cas de bug. Parmi ces types, nous pouvons citer les exemples suivants :

— Les fichiers log issus des serveurs .
— Les fichiers log issus des sites web.
— Les fichiers log issus des systèmes de détection d'intrusion .
— Les fichiers log issus des systèmes de surveillance de réseau .
— Les fichiers log issus des pare-feu .
— Les fichiers log d'accès
— Les fichiers log d'erreurs.

1.3 la centralisation des fichiers logs

1.3.1 Définition

La centralisation des logs consiste à mettre sur un même système, une même plateforme, l'ensemble des logs des systèmes, applications et services des machines environnantes. Elle peut présenter un grand intérêt au niveau de la sécurité au sein d'un

3. secure shell

système d'information. Sa fonction principale est d'être capable de récupérer un historique des évènements qui se sont produit sur une machine ou l'ensemble des machines d'un réseau . En effet, il est plus facile pour des outils d'analyse de logs de comparer, lire et scanner des fichiers se situant sur un seul et unique serveur plutôt que de le faire à distance ou via des agents distants. De plus en cas de crash serveur client, vous serez capable de récupérer les erreurs et actions menées sur votre serveur avant que celui-ci ne crash, facilitant ainsi la remise en activité de celui-ci et sa sécurisation future.

1.3.2 Intérêt de La centralisation des logs

L'intérêt de la centralisation des logs vient du faite de l'existence de plusieurs environnements, serveurs et beaucoup d'application, pas d'accès facile aux machines, temps de diagnostic des problèmes trop long ainsi que le volume de stockage important des logs . A fin de tirer toute les valeurs de logs on va pas hésiter de les centraliser et principalement lors du crash d'une machine ou une destruction de ces logs où ces derniers vont nous permettre de retracer les évènement qui ont amené a l'indisponibilité de la machine. D'un autre côté la centralisation des logs peut avoir un objectif de contrôle et de supervision a fin de mieux surveiller l'ensemble des machines.[DOGNY.M, 24/10/2014]

1.3.3 Étapes de la centralisation

La centralisation des logs implique plusieurs étapes de mise en place. Communication entre différents systèmes, parcours des paquets au travers différents réseaux pour arriver à une même cible, catégories/organisation à avoir, informations à exporter et informations à mettre de côté. en fonction de notre besoin nous pourrons rehausser et abaisser la criticité des logs à générer. La réalisation d'un serveur de logs respecte les étapes suivantes :

Génération des logs : Il est important d'optimiser correctement la génération des logs. Il faut savoir que plus un service, un système ou une application produit des logs,

plus celle-ci va consommer des ressources Il faut donc veiller à correctement définir ce que l'on souhaite voir, ce que l'on souhaite garder en local et ce que l'on souhaite envoyer sur un serveur de logs distant. Cela demande une vision globale du système d'information, car il est nécessaire d'effectuer cette tâche sur tous les systèmes et les applications qui en ont besoin, tout dépendra donc de la taille de notre système d'information.[8]

Envoi des logs sur un serveur centralisé : Une fois que l'on sait exactement quoi envoyer et centraliser, il faut maintenant savoir les envoyer sur la plate-forme destinée à recevoir ces logs. Il faut bien évidemment auparavant avoir configuré et installé le service nécessaire à la bonne réception et au bon stockage de l'ensemble des logs envoyés. Par exemple dans CISCO [4] la génération des logs n'est pas activée par défaut d'où la nécessité d'une configuration préalable en ligne de commande.[8]

Analyser Filtrer et Organiser les logs : D'abord il faut trier ce flux d'information, on peut par exemple créer un répertoire par machine puis un fichier par service, ou alors un fichier par service dans lequel on pourra distinguer la provenance des lignes de logs par le nom de la machine l'ayant produit. L'organisation et le tri des logs se fait de toute manière par le service qui gèrera sa réception (Rsyslog par exemple sous Linux). Une fois que nos logs sont ordonnés, il va alors être possible de les lire, les examiner, corriger leur position éventuellement pour arriver à l'objectif final de la centralisation des logs c'est la production d'un outil utile à la bonne gestion du système d'information. [8]

Rapport de traitement et Génération des alertes

- Une fois que les logs sont correctement organisés on peut faire des traitements dessus.
- La centralisation des logs va également permettre leur intégration dans un système de supervision, on va pouvoir plus facilement détecter les comportements des logs

4. Computer Information System COmpany

anormaux par rapport à un comportement standard. Par exemple, une détection des évènements anormaux, mettre une stratégie de supervision.

— Mettre en place des actions de protection et de prévention du système d'information. Avec des logs centralisés, il sera possible d'effectuer une analyse en temps réel des journaux d'évènements et cela de façon beaucoup plus simple, cela parce que les logs se situeront tous sur la même machine.

— Il est fréquent, en tant qu'administrateur système, de se faire envoyer des rapports par des scripts qui analysent les logs des machines par exemple. Avec des logs centralisés, on pourra avoir un rapport pour un ensemble/un groupe de machines plutôt que d'avoir un rapport individuel par machine. Cela, car tous les logs analysés se situeront sur la même machine.

1.4 la stratégie de stockage

La gestion des logs, dans une perspective de sécurité, nécessite de trouver un équilibre pertinent entre des ressources de stockage contraintes et une génération de données qui s'opère en continu. Le type de données de logs générées doit également être examiné. Les incohérences entre contenus et formats de journaux peuvent accroitre le volume de stockage nécessaire et les temps de traitement associés aux efforts d'analyse. Les logs sont générés par presque tous les appareils informatiques des systèmes réseaux, et sont dirigés vers un serveur centralisé pour le traitement. On peut envisager l'exportation des logs via le protocole FTP [5]et n'envoyer que les logs concernés par le système de supervision, et Cette opération doit assurer une fiabilité et une cohérence des données de fichier volumineux à traiter , un accès rapide et ceci n'est possible qu'avec une stratégie de sauvegarde, mise en place au niveau du système informatique à superviser .

L'analyse effective de grands volumes de divers journaux peuvent poser de nombreux défis, tels que :

— Le volume : les journaux/logs peuvent atteindre des centaines de giga-octets de

5. File Transfert Protocol

données par jour pour une grande organisation. La collecte, la centralisation et le stockage de données à ce volume peut être difficile d'où le recours à des utilitaires de sauvegarde existants.

— Normalisation : les journaux sont produits dans de multiples formats. Le processus de normalisation est conçu pour fournir une sortie commune pour l'analyse de diverses sources

— Vitesse : La vitesse à laquelle les journaux .

— sont produits à partir de dispositifs peut rendre la collecte et l'agrégation difficile.

— Véracité : Journal des évènements peut ne pas être exacte. Cela est particulièrement problématique à partir de systèmes qui effectuent la détection, tels que les systèmes de détection d'intrusion.

La gestion du journal au niveau d'un système informatique suppose une acquisition des (sous)systèmes de fournisseurs commerciaux ou construire leur propre outil de gestion de logs et outils d'intelligence, ou bien utiliser un assemblage de composants open-sources. La gestion des journalisations est un processus complexe qui demande beaucoup de réflexion dans l'approche adoptée. [11]

1.5 Traitement et analyse

L'acquisition et l'analyse des données à partir du réseau permettent :

— De savoir comment l'intrus a pénétré dans le réseau

— De montrer le chemin suivit par l'intrus

— De révéler les techniques d'intrusion

— La collecte des traces et des preuves

Sous Linux il existe plusieurs outils. Le plus connue est Syslog qui représente Un service de journalisation se reposant sur les deux démons « syslogd » et « klogd ».[LABIDI.T, 2010]

Les outils d'analyse et de récupération des fichiers journaux centralisés

Fail2ban : Est un outil pour IDS [6] basé sur les logs. Il est donc d'une importance capitale , car les logs qu'il produit vont permettre à Fail2ban de détecter certaines intrusions et ainsi déclencher des actions d'avertissement ou de protection . [8]

DenyHost : Est un outil de sécurité anti-intrusion basé sur le journal pour les serveurs SSH écrits en Python. Il est destiné à empêcher les attaques par force brute sur les serveurs SSH en surveillant les tentatives de connexion non valides dans le journal d'authentification et en bloquant les adresses IP d'origine. Il reprend le même principe que Fail2ban, il se base sur les logs dans le fichier /var/log/auth.log des machines Linux pour détecter des tentatives de brute force sur le port SSH. Il est malheureusement restreint qu'au service SSH.

RSYSLOG : Est le système rapide pour le traitement des logs sous linux. Il offre des fonctionnalités de sécurité hautes performances et une conception modulaire. Alors qu'il a commencé comme un syslogd régulier, rsyslog a évolué pour devenir un des plus important outils de journalisation, capable d'accepter des entrées provenant d'une grande variété de sources, de les transformer et d'afficher les résultats vers diverses destinations. RSYSLOG peut fournir plus d'un million de messages par seconde vers des destinations locales lorsqu'un traitement limité est appliqué (basé sur la version 7 de décembre 2013). Même avec des destinations éloignées et un traitement plus élaboré, la performance est généralement considérée comme satisfaisante. [3]

Splunk : Est un outil complet qui permet la navigation d'un grand nombre de messages de journal de différents types, la création de rapports et affichage graphique des résultats souhaités. Il permet de consolider et indexer , rechercher, corréler, visualiser, analyser toutes les données machines et de logs, y compris les logs structurés, non structurés et multi-ligne complexes. [EREMEJIA.M, TODOSIJERIC.A, DESPIC.D, march 2016]

6. système de détection d'intrusion

EventLog : C'est un outil pour le balayage, stockage, et manipulation des évènements sur une machine dans un LAN [7]. Il stocke les évènements de toutes les machines sur une base de données puissante, où on peut récupérer tous les détails tels que l'identification d'évènement, type, catégorie, source, SID des utilisateurs, suivi de message et de date d'évènement.[LABIDI.T, 2010]

Syslog : Le protocole Syslog est un protocole très simple et très largement utilisé dans le monde Unix. Son but est de transporter par le réseau les messages de journalisation générés par une application vers un serveur hébergeant un serveur Syslog. Un autre but est aussi d'assurer la fonction de concentration des journaux, un serveur Syslog intermédiaire pouvant retransférer les messages Syslog qu'il reçoit vers un autre serveur Syslog.[2]

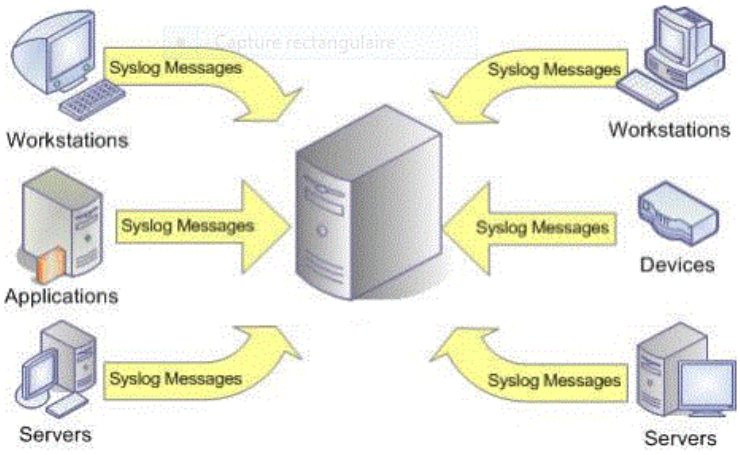

FIGURE 1.2 – centralisation des logs avec Syslog

SNARE [8] C'est une collection d'outils logiciels qui collectent des données de journaux d'audit à partir de divers systèmes d'exploitation et applications pour faciliter l'analyse centralisée des journaux. Les agents d'entreprise sont disponibles pour Linux, OSX, Windows, Solaris, Microsoft SQL Server, une variété de navigateurs, et plus encore. Snare Entreprise Epilog pour Unix fournit une méthode pour collecter tous les fichiers journaux basés sur le texte, sur les systèmes d'exploitation Linux et Solaris.[4]

7. Local Area Network
8. System Intrusion Analysis and Reporting Environment

ELK Est une solution open source, de la société elastic, composée de trois produits qui sont Elasticsearch, Logstash et Kibana, qui permettent de parser, indexer et présenter de gros volumes de données issues de vos logs et de faire des recherches au sein de vos logs comme vous pourriez le faire avec un moteur de recherche.[5]

Syslogd Le démon syslogd existe par défaut sous UNIX. Mais ces fonctionnalités sont néanmoins limitées. Lors de son lancement, « syslogd » lit le fichier «/etc/syslog.conf» afin de pouvoir ensuite décider le milieu d'enregistrement de chaque message. [LABIDI.T,2010]

Syslog ng C'est le système standard de journalisation de nouvelle génération disponible au format source et binaire, il est libre. Son principal avantage est sa grande flexibilité et sa simplicité dans sa configuration. En effet il permet :

- Filtrage des messages par leur contenu et selon plusieurs critères (contenu, gravité...)
- Transport des journaux via le protocole TCP et UDP
- Une large portabilité
- Sécurité du transport des données par le cryptage
- Synchronisation des horloges avec un client NTP [9]
- compatible IPV6 [LABIDI.T, 2010]

Le tableau compare de manière non exhaustive un panel de solutions de recueil de journaux.

9. Network Time Protocol

	Avantage	inconvénient
Syslog-ng	— Solution mature. Ayant évoluée depuis son apparition en 1998 — Stockage des journaux en BDD possible — Grande compatibilité — Grande communauté	— Toutes les options ne sont pas disponibles dans la version communautaire — Limitation à environ 75 000 logs / jours /serveur
RSYSLOG	— +Stockage des journaux en BDD possible — Grande compatibilité — Grande communauté — Basé sur syslog-ng — Ajoute des modules réservés à la version payante de syslog-ng — Client Windows disponible et modulable	— Nécessite une configuration précise pour traiter les journaux « eventlogs »
SNARE	— Intègre une interface de gestion — Grand nombre d'options de configuration	— Agent open source mais serveur payant — Appliance

TABLE 1.1 – comparatif des solutions de gestion des journaux d'évènements [GOULAIS.F, 2014]

sawmill Est un outil d'analyse de journaux puissant et hiérarchique qui fonctionne sur toutes. les grandes plateformes. Il est particulièrement bien adapté aux fichiers journaux de serveur Web, mais peut traiter presque n'importe quel fichier « log » notamment ceux du Proxy Squid. Les rapports que Sawmill génère sont hiérarchiques, attrayants et fortement réticulés pour faciliter la navigation. Cependant, cet outil n'est pas gratuit ce qui reste un grand inconvénient par rapport aux autres outils disponibles [MEZNI.B, 2014-2015]

XpoLog Est une plate-forme d'analyse du journal pour les applications, les serveurs et les applications de cloud computing. Centre XpoLog fournit la gestion du jour-

nal, journal de l'observation, l'analyse des journaux, rapports, analyse des problèmes, la corrélation et de nombreuses autres fonctionnalités qui aident les groupes d'applications, les opérations et les administrateurs pour accélérer l'investigation et le monitoring d'application.[MEZNI.B, 2014-2015]

WebAnalizer Est un programme d'analyse de fichier journal de serveur Web qui produit des statistiques d'utilisation au format HTML [10] pour l'affichage avec un navigateur. Les résultats sont présentés sous forme de colonnes et de graphiques, ce qui facilite l'interprétation. Des statistiques d'utilisation annuelles, mensuelles, quotidiennes et horaires sont présentées, ainsi que la possibilité d'afficher l'utilisation par site, URL [11], référent, agent utilisateur (navigateur), nom d'utilisateur, chaînes de recherche, pages d'entrée / sortie et pays (certaines informations peuvent ne pas être disponible s'il n'est pas présent dans le fichier journal en cours de traitement)[7]

Advanced Log Analyzer Est un puissant logiciel d'analyse de trafic de site Web. Il génère un grand nombre de compte-rendu traditionnel comme les sites référant au visiteur, le nombre de téléchargements par jour, le nombre de clics et d'hôtes par jour, les moteurs de recherche les plus populaires, les mots-clés de recherche, etc. Il peut être utilisé en tant que compteur de visiteurs normaux et outil de suivi pour surveiller l'activité d'un site Web. L'avantage principal de cet outil d'analyse réside dans son compte-rendu. Il peut recréer le chemin du visiteur à partir des fichiers log, créer un modèle Web du site et produire des comptes rendus sur le flux d'utilisateurs sur le site. Il possède un langage intégré, semblable à SQL, qui permet la création du compte-rendu configurable. Avec le petit client FTP vous pouvez simplement télécharger (avec fonction de reprise) les fichiers log sur votre machine locale. Il supporte les formats log Apache et Microsoft Internet information Serveur (IIS). Il peut fonctionner comme une application Windows normale avec une interface utilisateur graphique, une application console avec des paramètres en ligne de commande. [8]

10. HyperText Transfer Protocol
11. Uniform Resource Locator

1.5.1 Exemple d'envois des logs sur un serveur distant « cas Rsyslog »

1.5.1.1 Étape de configuration CISCO pour exporter les logs

— Paramétrage de l'heur sur CISCO : l'horodatage a une importance particulier dans le centralisation des logs il permet en effet de retracer précisément les logs entre le routeurs cisco et le serveur de centralisation des logs. « clock set 20 :11 :00 avril 19 2018 ».

— Activer l'horodatage. « service timestamps ».

— Configurer les déférents paramètre propre a l'envoie des logs.

1. On commence par l'adresse IP [12] du serveur de log« logging 10.2.0.57 ».
2. paramétrage du log facility qui permet de trier les logs sur le serveur« logging facility local15 ».

— Pour des raison de performance nous pouvons choisir de ne pas envoyer la totalité des logs mais juste sélectionner les logs selon le niveau de criticité . « logging trap informationnal ».

```
>en
#clock set <heure>:<minute>:<seconde> <mois> <numéro_jour> <année>
//Configuration manuelle de la date et l'heure
#conf t
(config)#ntp serveur <adresse_ip__ou_hostname_serveur_ntp> //Configuration de
la date et l'heure avec un serveur NTP
(config)#service timestamps
(config)#logging trap <nom_niveau_logging>
(config)#logging facility <nom_facility_log>
(config)#logging <adresse_ip_serveur_syslog>
(config)#end
#show logging
#copy run start
```

FIGURE 1.3 – visionnage de paramétrage des logs dans cisco [DOGNY.M, 24/10/2014]

— Après avoir configuré le routeur cisco pour l'envoie des logs au serveur de log distant, il faut mettre ces logs dans un fichier spécifique. « local17.*/var/log/cisco »

— Maintenant que les logs sont mise dans un fichier spécifique on va redémarrer le service « service rsyslog restart »[DOGNY.M, 24/10/2014]

12. Internet Protocol

1.5.1.2 Notions de fonctionnalités des fichiers logs

La fonctionnalité d'un message log correspond au type d'application qu'a générer ce dernier. Le choix du numéro de la fonctionnalité et de la responsabilité du projet et du développeur de l'application. Le tableau 1.2 représente les notions de fonctionnalité des fichiers logs.

Numéro de fonctionnalité	Usage
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log allert
15	clock daemon
16	local use 0
17	local use 1
18	local use 2
19	local use 3
20	local use 4
21	local use 5
22	local use 6
28	local use 7

TABLE 1.2 – Notions de fonctionnalités des fichiers logs
[2]

1.5.1.3 Les niveaux de sévérité

Il est très important de configurer le **log-level** a partir du quelle on prendra soin d'envoyer les logs. Pour différentes raisons comme la performance, on peut pas vouloir envoyer tout les logs au serveur distant, on va alors choisir d'envoyer les logs a partir d'un

certain niveaux de criticité. Le tableau 1.3 représente les déférent niveau de sévérité.

degré	sévérité	signification
0	emerg (emergency)	Message urgent. Le système est inutilisable ou risque de le devenir à très court terme.
1	alert (alerte)	Message alertant l'administrateur système qu'une action de sa part est requise.
2	crit (critique)	Message critique.
3	err (erreur)	Message d'erreur.
4	Warning(ou warn) (avertissement)	Message d'avertissement.
5	notice (note)	Message de fonctionnement normal, sans gravité particulière.
6	info (Information)	Message à titre informatif.
7	debug (debogage)	Message de débogage

TABLE 1.3 – Les niveaux de sévérité
[LABIDI.T, 2010]

1.5.1.4 priorité des fichiers logs

La priorité d'un message Syslog est définie par sa fonctionnalité et sa sévérité. Cette priorité est le résultat de la multiplication de la fonctionnalité par 8 auquel est ajoutée la sévérité .La priorité maximale prend la valeur 191, elle est définie par la fonctionnalité 23 et la sévérité 7 : (23*8)+7=191. [2]

1.5.2 Étude générale des logs

1.5.2.1 Code de réponse serveur

Lorsque vous essayez d'accéder à un contenu sur un serveur exécutant internet information Services (OIS) 7.0, 7.5 ou 8.0 via le protocole PUTTY, les services OIS [13] renvoient un code numérique qui indique l'état de la réponse. Le code d'état HTTP est enregistré dans le journal IIS [14]. En outre, le code d'état HTTP s'affiche dans le navigateur client. Ce code permet de savoir si une requête aboutit ou non. Il peut également

13. Office of Information Services
14. Iternet Information Serveur

indiquer la raison exacte pour laquelle une requête n'aboutit pas. Ces codes ont été divisés en 5 familles, le tableau 1.4 présente les différents codes de chaque famille ainsi que ces significations. [MEZNI.B, 2014-2015]

code	signification
1XX	**Information**
100	Continue
101	Changement de protocole
2XX	**Succès**
200	OK
201	Créé
202	Accepté
203	information ne faisant pas autorité
204	Pas de contenu
205	Rétablir le contenu
206	Contenu partiel
3XX	**Redirection**
301	Déplacement définitif
302	Déplacement temporaire
303	Voir autre
304	Non modifié
305	Utiliser un proxy
307	Redirection temporaire
4XX	**Erreur de client**
400	Mauvaise demande
401	Non autorisé
403	Interdit
404	Non trouvé
405	Méthode non admise
406	Pas acceptable
408	Délai écoulé pour la requête
410	Page indisponible définitivement
5XX	**Erreur du serveur**
500	Erreur interne du serveur
501	Non mise en œuvre
502	Mauvaise passerelle
503	Service indisponible
504	Expiration de la passerelle
505	Code d'extension de version http non prise en charge.

TABLE 1.4 – liste des codes de repense serveur
[6]

1.6 journalisation centralisé

La centralisation des fichiers journaux permet une meilleure gestion et supervision des messages systèmes générés par les applications web et matériel informatique. Cette opération est très délicate et fastidieuse, lorsqu'elle doit être faite manuellement.

1.6.1 Principe de la centralisation

La centralisation nous permet d'acheminer tous les fichiers journaux des routeurs, commutateurs et serveurs vers serveur de journaux. Tous les équipements réseau et serveurs UNIX/Linux peuvent être stockés avec une version de syslog. Windows peut également utiliser syslog avec des outils supplémentaires. L'enregistrement des fichiers journaux se fait en local ainsi que sur un serveur de journaux central. La figure 1.3 représente l'architecture centralisée des logs.

La réalisation de la centralisation suppose :

— Le stockage des journaux dans un lieu sûr où ils peuvent être facilement inspectés.

— Au niveau du serveur de journaux central les fichiers journaux peuvent être triés à l'aide des attributs facility (fonctionnalités) et level (sévérité).

— une Analyse des fichiers journaux et un contrôle en continu est effectué vu les informations importantes qu'ils contiennent [1]

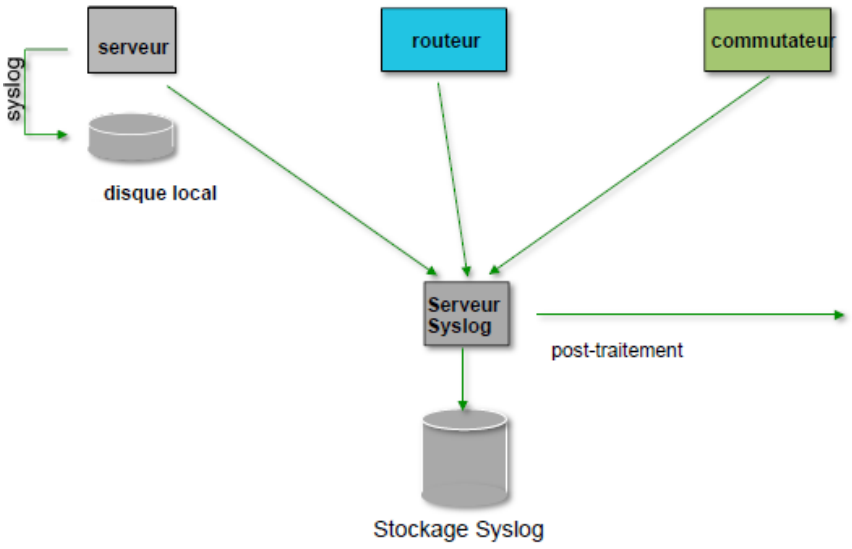

FIGURE 1.4 – architecture centralisée des logs
[1]

1.6.2 exemple de fichier journaux généré par un routeur

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console
by pr on vty0 (203.200.80.75)

CI-3-TEMP: Overtemperature warning

Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed
state to down
```

FIGURE 1.5 – fichier journaux générés par un routeur
[1]

1.6.3 exemple de fichier journaux généré par un serveur linux

```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from
169.223.1.130 port 2039 ssh2
```

FIGURE 1.6 – fichier log généré par un serveur linux
[1]

1.7 Dictionnaire des attaques

Le grand nombre d'attaque et le changement perpétuel de leurs formes ont amené a une création d'une BD sous forme d'un dictionnaire englobant toutes les attaques ainsi que leurs structures les plus connues. La comparaison entre un log et une expression rationnelle se fait en se référant à ce dictionnaire. Les composants de dictionnaire d'attaques sont : l'identifiant de l'attaque, la catégorie d'attaque, l'impact et la description de chaque ligne d'attaque. [MEZNI.B, 2014-2015]

1.8 Complixité des fichiers logs

L'évolution de l'utilisation du réseau Internet a été suivie en parallèle par l'augmentation des attaques cybernétiques telles que les effacements web, phishing, attaque virale (malware), etc. Pour cela on doit utiliser tous les moyens et les techniques possible d'acquérir afin de renforcer la sécurité du cyberespace. Parmi les difficultés qui peuvent survenir :

les requêtes inutiles Chaque fois qu'il reçoit une requête, le serveur enregistre une ligne dans le fichier Log. Ainsi, pour charger une page, il y aura autant de lignes dans le fichier que d'objets contenus sur cette page (les éléments graphiques). Un prétraitement est donc indispensable pour supprimer les requêtes inutiles

les firewalls Ces protections d'accès à un réseau masquent l'adresse IP des utilisateurs. Toute requête de connexion provenant d'un serveur doté d'une telle protection aura la même adresse et ce quel que soit l'utilisateur. Il est donc impossible, dans ce cas, d'identifier et de distinguer les visiteurs provenant de ce réseau.

Le Web caching Afin de faciliter le trafic sur le Web, une copie de certaines pages est sauvegardée au niveau du navigateur local de l'utilisateur ou au niveau du serveur Proxy afin de ne pas les télécharger chaque fois qu'un utilisateur les demande. Dans ce cas, une page peut être consultée plusieurs fois sans qu'il y' ait autant d'accès au serveur. Il en résulte que les requêtes correspondantes ne sont pas enregistrées dans le fichier Log.

L'utilisation des robots Les annuaires du Web, connus sous le nom de moteurs de recherche, utilisent des robots qui parcourent tous les sites Web afin de mettre à jour leur index de recherche. Ce faisant, ils déclenchent des requêtes qui sont enregistrées dans tous les fichiers Logs des différents sites, faussant ainsi leurs statistiques.

L'identification des utilisateurs L'identification des utilisateurs à partir du fichier Log n'est pas une tâche simple. En effet, en employant le fichier Log, l'unique identifiant disponible est l'adresse IP de l'utilisateur. Cet identifiant présente plusieurs limites :

— Adresse IP unique / Plusieurs sessions serveurs : La même adresse IP peut être attribuée à plusieurs utilisateurs accédant aux services du Web à travers un unique serveur Proxy.

— Plusieurs adresses IP / Utilisateur unique : Un utilisateur peut accéder au Web à partir de plusieurs machines.

— L'identification des sessions : Toutes les requêtes provenant d'un utilisateur identifié constituent sa session. Le début de la session est défini par le fait que l'URL de provenance de l'utilisateur est extérieure au site. Par contre, aucun signal

n'indique la déconnexion du site et par suite la fin de la session.

— Le manque d'information :le nombre de visites d'une page ne reflète pas nécessairement l'intérêt de celle-ci. En effet, un nombre élevé de visites peut simplement être attribué à l'organisation d'un site et au passage forcé d'un visiteur sur certaines pages. [MEZNI.B, 2014-2015]

1.9 Conclusion

la définition et la description des concepts liés aux traitements des logs, nous ont permis de mieux nous orienté dans notre processus de développement et par conséquent nous ont conduit à proposer une solution adaptée à l"hétérogénéité au système informatique du l'organisme d'accueil. Le chapitre suivant est consacré à la présentation de l'organisme et spécification des besoins du projet.

Chapitre 2

Organisme d'accueil et étude préalable

2.1 Introduction

L'étude de l'existant au niveau de l'organisme d'accueil, prendre contact avec ses éléments et comprendre l'architecture réseau de ses équipements est la garantie ver une solution fiable et cohérente. Nous allons présenter dans ce chapitre la société d'accueil « Service de réseaux et systèmes informatiques » au sein du quel nous avons effectué notre projet. Ensuite la description du contexte du projet, la problématique et le travail à réaliser et nous exposons la méthodologie de travail admise. nous mettrons .enfin, nous présentons notre application avec ses problématiques différentes.

2.2 Historique

Le centre Universitaire de tizi-Ouzou est crée en 1977 (décret exécutif No 17-77 du 20 juin 1977). La première rentrée universitaire avait accueilli 490 étudiants dont une cinquante de nationalités étrangères, encadrés par 27 jeunes enseignants qui y firent leur entrée en 1977. Le C.U.T.O avait alors démarré avec (05) départements :

- Département des Sciences Exactes
- Département de Biologie
- Département des Sciences Juridiques et Administratives
- Département de Langues et Littérature Arabes
- Département des Sciences Économiques

En 1984, le centre universitaire (C.U.T.O), éclate en neuf (09) Instituts Nationaux d'Enseignement Supérieur (I.N.E.S).

- I.N.E.S de Génie Civil
- I.N.E.S des Sciences Médicales
- I.N.E.S des Sciences Juridiques et Administrative
- I.N.E.S des Sciences Économiques - I.N.E.S de Biologie - I.N.E.S de Langue et Littérature Arabes
- I.N.E.S d'Électrotechnique

— I.N.E.S d'Informatique

— I.N.E.S d'Agronomie

En 1989, cet important pôle a été élevé au rang d'université (U.T.O) par décret exécutif N° 89-139 du 01/08/1989

En 1991, L'Université de tizi-Ouzou enrichit son offre en formation par la création du département de langue et cultures amaigries par l'arrêté Ministériel N° 11 du 1/1990.

2.2.1 Structure de l'Université

Les structures de l'UMMTO (Université Mouloud Maamerie de tizi Ou zou) sont implantées sur sept (07) sites, il s'agit des campus suivants :

— Hasnaoua I, abritant le rectorat et les services centraux, la faculté des sciences économiques et de gestion, la faculté des lettres et des langues ainsi que cinq laboratoires de recherche

— Hasnaoua II, il abrite essentiellement les filières technologiques à savoir la faculté du Génie Électrique et Informatique et la faculté du Génie de la Construction, la faculté des Sciences Biologiques et Agronomiques et la faculté des sciences fondamentales.

— Le campus Biomédical, abrite la faculté des Sciences Médicales et quatre laboratoires de recherche

— Le site de Tamda, le plus récent, Il abrite la faculté des sciences humaines et sociale

— Le site Habitat , est exploité par les étudiants en TACT

— Le site de Boukalfa, il, regroupe les départements de la faculté de droit et des sciences politiques.

L'Université comprend : Le rectorat, les services communs et de nombreuses Facultés réparties sur plusieurs pôles : Hasnaoua I, Hasnaoua II, Boukhalfa et Tamda.

2.2.2 Organisation de l'UMMTO

Le Rectorat est placé sous l'autorité du Recteur et comprend :

— Les vices rectorats

— Le Secrétariat Général

— Les Services Communs

— Les Facultés et Département.

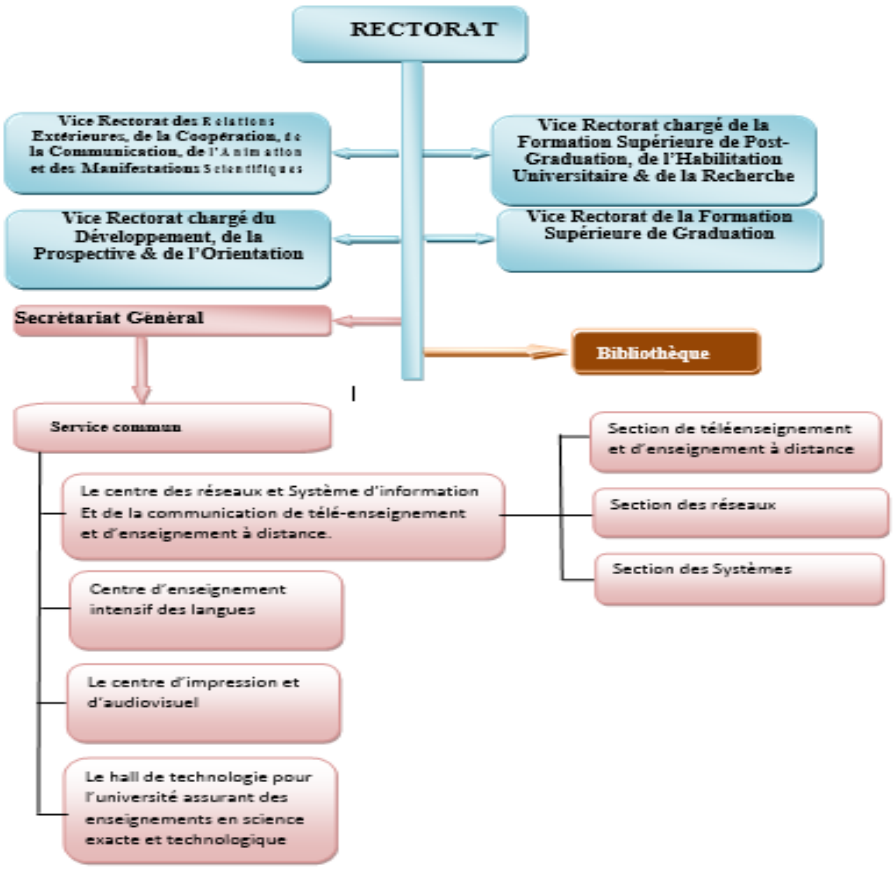

FIGURE 2.1 – organigramme de l'université

2.3 Structures de recherche

En plus de la formation notre université dispose de 29 laboratoires de recherche nous citerons parmi eux :

— Laboratoire de Ressources Naturelles

— Laboratoire de Technologies Avancées en Génie Électrique
— Laboratoire de Reformes Économiques & Dynamiques Locales
— Laboratoire de Production, Amélioration & Production des Végétaux & des Denrées
— Laboratoire de Mécanique, Structure & Énergétique (LÈSE)
— Laboratoire de Néo matériaux Environnement & Aménagement (LOGEA)

2.4 Présentation de l'organisme d'accueil

Créé suite à l'arrêté interministériel du 24 Aout 2004, fixant la nouvelle organisation administrative de l'université et ses services communs, le centre des Systèmes et Réseaux d'Information, de Communication, de Télé-enseignement et Enseignement à Distance .

2.4.1 Présentation du centre

Le centre des Systèmes et Réseaux d'Information, de Communication, de Télé-enseignement et Enseignement à Distance est chargé de :

— L'exploitation, l'administration et la gestion des infrastructures de réseaux
— L'exploitation et le développement des applications informatiques de gestion pédagogique
— Le suivi et l'exécution des projets de Télé-enseignement et enseignement à distance
— Assurer l'appui technique à la conception et à la production de cours en ligne
— La formation et l'encadrement des intervenants dans l'enseignement à distance

Chaque département, chaque laboratoire de recherche et chaque service administratif du rectorat et des facultés se sont vus dotés de l'outil internet. Les trois composants de l'université (étudiant, enseignant et administration) bénéficient ainsi de ce service, devenu une nécessité pour le bon déroulement des différentes activités de notre établissement.

2.5 Organisation du Centre de calcul et réseau

2.5.1 Organigramme

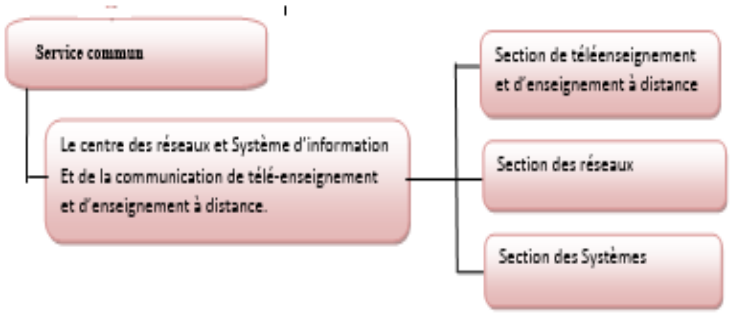

FIGURE 2.2 – organigramme de l'organisme d'accueil

2.5.2 Section des systèmes

La Section Système d'Information (S.I), a pour mission de mettre en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication , la gestion d'une manière plus générale à tout ce qui touche au traitement automatique de l'information. L'objectif principale de la section système de est le Développement d'application web pour l'université à savoir l'informatisation des ressource humains.

2.5.3 Section des réseaux

La section réseau a pour missions de maintenir le fonctionnement normal du réseau intranet de l'université, d'assurer la sécurité des équipements réseaux et des services offerts par le réseau au système d'information et aux applications et enfin de fournir des services de connexion internet, de messagerie électronique, de support utilisateur, d'étude et de suivi des projets réseau de l'université Mouloud Maamerie.

2.5.4 Section de Télé-enseignement et Enseignement à Distance

Le domaine technique englobe la mise en place d'une solution e-learning répondant à la fois aux besoins et aux ambitions de cette université. Il s'agit notamment de l'installation, de l'administration, création de sites web pour les facultés et labo de recherche et de la maintenance des plates formes de e-learning. En plus de cela, cette cellule gère une salle de visioconférence.

2.6 Personnels Administratifs et Techniques

Le personnel du service des réseaux, géré par le responsable du centre, compte actuellement dix-neuf (19) dont 06 ingénieurs d'état en informatique, 05 ingénieurs principaux 07 techniciens supérieurs en informatique et une Secrétaire de Direction. Ils interviennent dans la mise en place de l'intranet et participent à l'intégration des nouvelles technologies de la communication dans les différents services administratifs et les structures pédagogiques. En plus de l'exploitation locale du service internet au niveau des différentes structures de notre université, le service de messagerie électronique permet l'ouverture d'une boite aux lettres électronique (e-mail) à chaque enseignant, disposant d'un compte sur le réseau de l'Université.

2.7 Les besoins du centre réseau

Après avoir présenté les différentes section de l'organisme d'accueil et énumération des mission de chacune d'elle, nous avons constaté l'importance du bon fonctionnement des différents services offert au niveau de l'université et la la complexité du système informatique de ce dernier, et par conséquent une supervision difficile à gérer vu l'absence d'une plateforme, qui permet aux administrateurs de palier aux différents problèmes éventuels de fonctionnement de l'infrastructure dans un temps optimal.

Les administrateurs auront besoins :

— De prévenir toute tentative d'intrusion (exemple plusieurs tentative de connexion avec mots de passe erronés) .

— De recevoir des alertes en cas d'arrêt ou dysfonctionnement d'une application WEB.

— D'être alerter quant à tout arrêt de service (apache, mysql...)

— D'être alerter pour des problèmes de démarrage de serveurs (surcharge disque dur, panne critique).

— alerte de dysfonctionnement après lecture des logs issus des pare-feu ou des routeur Cisco.

2.7.1 Problématique

L'inexistence d'un serveur de logs au niveau du centre réseau et la sensibilité des services offert par ce dernier nécessite une lecture et analyse quotidienne des logs des déférents systèmes existants, cette opération pénible aux administrateurs réseau, n'est possible actuellement que par l'accès en local et lecture du journal très volumineux. Cette dernière peut aboutir à des analyses erronées vu le nombre d'information importantes à traiter, et l'accès fréquent avec des manipulations peut provoquer des problèmes au niveau des systèmes existants. Le centre réseau a besoin aussi d'un rapport d'analyse en temps réel pour les appareils sensibles comme par exemple les routeurs Cisco, ainsi que des informations sur le trafic réseau et le rapport de consultations des applications web existantes.

2.7.2 Solution proposée

Afin de palier aux problèmes de l'inexistence d'une telle solution au niveau du centre réseau, nous allons proposé une plate forme de centralisation des logs au niveau d'un serveur dédié a fin de garantir la sauvegarde des logs générés par les différents systèmes du service, de retracer toutes les opérations dû à une intrusion externe dont les données

du fichier journal ont été supprimées par l'attaquant , et qui traitera ces derniers en temps réel et aux besoins des administrateurs. cette plate forme nous permettra aussi de générer des rapports d'analyses et des statistiques.

2.8 Comparative entre les méthodologies

Pour assurer un bon rendement de développement en termes de qualité et de productivité le choix de la méthodologie en informatique est primordial. Vue la complexité des systèmes de nos jours, le génie logiciel doit tenter de remédier à cette complexité en offrant une démarche à suivre avec des étapes bien précises. C'est le principe des méthodologies de travail.

Le tableau 3. 2 contient un comparatif entre les principales méthodologies de développement que nous avons choisi vu la diversité de ces méthodes.

Méthodologie	**Description**	**avantage**	**Inconvénient**
cascade	les phase sont deroulé d'une façon séquentiel	Distingue clairement les phases du projet.	— Non itératif — Pas de modèles pour les documents.
RUP(rationnal unified process)	— Promu par rational — Le RUP est à la fois une méthodologie et un outil prêt à l'emploi. — Cible des projets de plus de 10 perssonnes.	— Itératif, — Spécifie le dialogue entre les différents intervenants du projet. — Propose des modèles de documents pour des projets types.	— Assez flou dans sa mise en oeuvre. — Ne couvre pas les phases en amont et en aval au développement.
2TUP (Two Truck Unified Process)	— S'articule autour de l'architecture — Propose un cycle de développement en Y. — Cible des projets de toutes tailles.	— Itératif — Laisse une large place à la technologie et à la gestion des risques. — Définit les profils des intervenants, les plannings, les projets types.	— Plutôt superficiel sur les phases situées en amont et en aval du développement — Ne propose pas de documents types.

TABLE 2.1 – Comparaison entre les principales méthodologies de développement [MEZNI.B, 2014-2015]

2.8.1 Choix des méthodologie a adopter

Suite à la comparaison entre les principales méthodologies de développement et afin de de mener à bon terme notre projet, nous avons opté pour le processus 2TUP pour les raison suivantes :

— 2 TUP [1] donne une grande importance à la technologie ce qui est important pour notre projet.

— 2 TUP est un processus en Y qui contient une branche technique, une branche fonctionnelle et une branche réalisation.

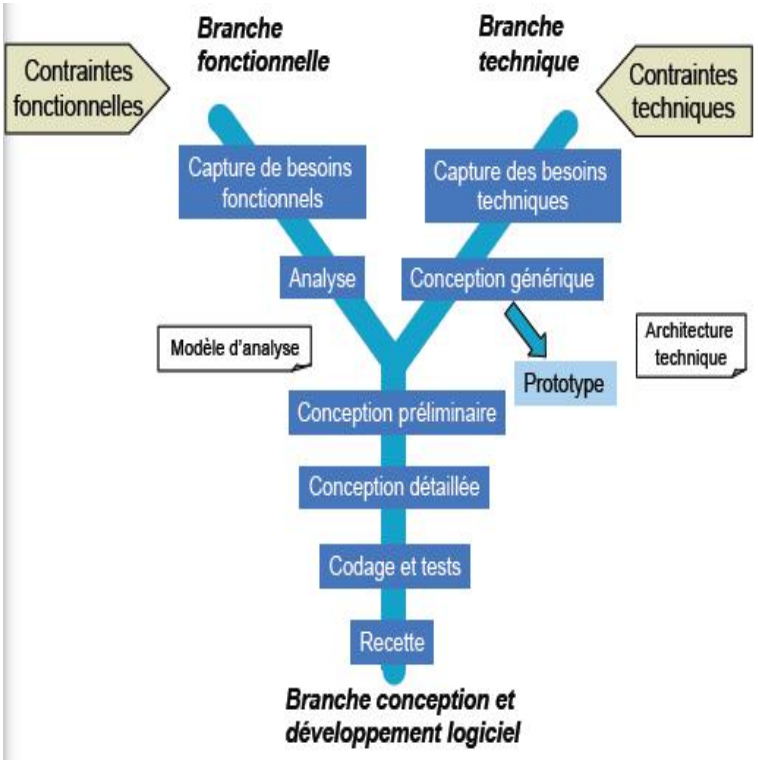

FIGURE 2.3 – les étapes de développement des trois branches du processus 2TUP.

2.8.2 Choix du langage

La modélisation permet d'abstraire la réalité pour mieux comprendre le système à réaliser, c'est également un bon moyen pour maitriser sa complexité et d'assurer sa cohérence. Pour cela nous avons choisi le langage de modélisation UML [2] qui permet

1. Team Unifying Platform
2. Unified Modeling Language

de :

- Obtenir une modélisation de très haut niveau indépendante des langages et des environnements.
- Visualiser : Chaque symbole graphique possède une sémantique.
- Spécifier : De manière précise et complète, sans ambigüité.
- Faire des simulations avant de construire un système.
- UML est un support de communication performant.
- Faire collaborer des participants de tous horizons autour d'un même document de synthèse..
- Il facilite la compréhension de représentations abstraites complexes.
- Exprimer dans un seul modèle tous les aspects statiques, dynamiques, juridiques, spécifications, etc...[10]

2.9 conclusion

Au cours de ce chapitre nous avons présenté l'organisme d'accueil, nous avons identifié le cadre général de notre projet, l'étude préalable nous a permis de comprendre la problématique et le travail à réaliser Finalement, nous avons analysé la méthodologie de développement ainsi que le langage de modélisation à mettre en œuvre. Le chapitre sera consacré pour l'analyse et conception.

Chapitre 3

Analyse et Conception

3.1 Introduction

La troisième étape de notre processus de développement sera consacrée en présentant les spécifications des besoins tout en exprimant les échanges effectués entre l'utilisateur et les différents composants de notre solution. Tout au long de ce chapitre, définir les besoins fonctionnels et non fonctionnels du système, Cette description sera explicite notamment à partir des diagrammes des cas d'utilisation, des diagrammes des séquences et des diagrammes des classes.

3.2 Énumération des besoins Service du service

L'étape de spécification est déterminante pour la suite de notre projet. En effet elle permet de préciser les fonctionnalités que le système doit fournir à ses utilisateurs et le lien entre ces différentes fonctionnalités. Dans cette étude, nous allons tous d'abord spécifier les besoins fonctionnels et non fonctionnels de notre application, ensuite nous allons dresser le diagramme de cas d'utilisation correspondant.

3.2.1 Besoin Fonctionnel

Les besoins fonctionnels doivent répondre aux exigences de notre future application en termes de fonctionnalités, et comme notre projet consiste à développer une application de supervision, cette application doit couvrir les besoins fonctionnels suivants :

- La gestion d'accès à la plateforme de supervision via un login et un mot de passe.
- L'ajout d'un utilisateur à la plateforme.
- Attribution des droits d'accès
- récupération automatique des logs.
- filtrage des logs selon plusieurs critère
- mise a jour des la tables de la base de donnée
- consulter rapport.
- Consulter statistique.

— Télécharger rapport.

3.2.2 Besoin Non Fonctionnel

A part les besoins fondamentaux, notre future application doit répondre aux critères suivants :

— Réutilisation : Le code doit être facile à réutiliser, à modifier et à étendre.

— Maniabilité : C'est un critère important dans la mesure où la clarté et la visibilité des informations journalières permettront de comprendre à tout moment l'activité du réseau.

— La sécurité au niveau de session de l'utilisateur : Les informations concernant l'identité de la personne connectée sont cryptées.

— La compatibilité de la plateforme avec n'importe quel navigateur web ou système d'exploitation.

— La disponibilité de la plateforme en continue.

— L'intégrité des données : Il y a certains traitements pour les mauvaises entrées des données, tel que les alertes immédiates pour l'utilisateur en cas d'erreur.

— La convivialité : la future application doit être facile à utiliser. En effet, les interfaces utilisateurs doivent être conviviales c'est-à-dire simples, ergonomiques et adaptées à l'utilisateur.

3.3 Architecture du système

Au niveau de cette section, nous avons proposé l'architecture physique à adopter pour notre application. Notre choix s'est porté sur l'architecture client-serveur et plus précisément sur l'architecture 2-tiers pour les raisons suivantes :

— Elle correspond le mieux à la structure de notre système qui composera d'un serveur d'application qui est au même temps un serveur de base des données et des clients.

— Elle permet l'utilisation d'une interface utilisateur riche .

— Elle a permis l'adaptation des applications par l'utilisateur .

— Elle a introduit la notion d'interopérabilité.

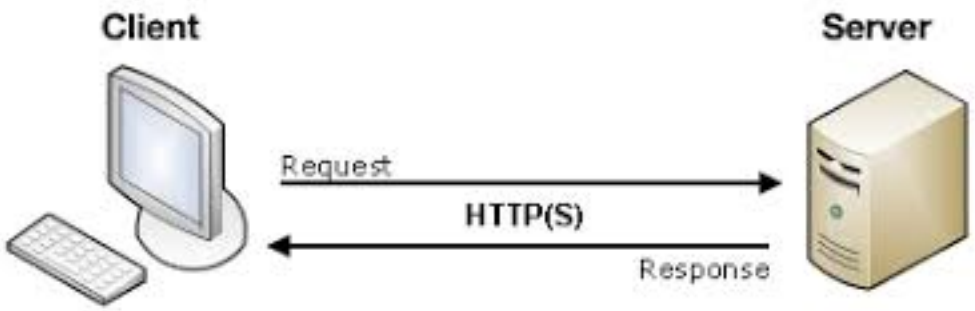

FIGURE 3.1 – Architecture de Systèmes

3.4 Présentation du protocole Syslog

Le protocole Syslog est un protocole réseau qui permet de transporter les messages de journalisation générés par les applications vers une machine hébergeant un serveur Syslog. Il définit la notion de périphérique , de relais et de collecteur ainsi que les notions de fonctionnalités, de sévérité et de priorité ont étaient définit dans le chapitre précédant.

— La notion de périphérique est une machine ou une application qui génère des messages Syslog.

— La notion de relais est une machine ou une application qui reçoit des messages Syslog et les transmet à une autre machine

— La notion de collecteur est une machine ou une application qui reçoit des messages Syslog mais ne les transmet pas (Centralisation des logs).

Le protocole syslog est un protocole on mode texte, il utilise les caractère du code ASCII.[2]

3.5 Caractéristique de la trame de protocole Syslog

La longueur totale d'une trame Syslog doit être de 1024 au moins, elle est composé de trois partie[16] :

— La partie PRI.

— La partie HEADER

— La partie MSG.

3.5.1 La partie PRI

La partie PRI d'un message Syslog est composée obligatoirement de 3, 4 ou 5 caractères. Le premier caractère est toujours le caractère "<" suivi par un nombre qui représente la priorité (en base 10) du message et suivi par le caractère ">".

3.5.2 La partie HEADER

La partie HEADER d'un message Syslog contient 2 champs :

— Le champ TIMESTAMP : représente le format de date utilisé par le champ TIMESTAMP est "Mmm dd hh :mm :ss".

— Le champ HOSTNAME peut contenir :

1. Le nom de machine sans son nom de domaine.
2. Une adresse IP au format IPv4 (format décimal pointé 192.168.1.1 par exemple).
3. Une adresse IP au format IPv6 (voir la RFC RFC 2373 pour les différentes notations supportées).
4. Rien, le champ HOSTNAME est facultatif. Un caractère espace (" ") doit obligatoirement suivre le champ HOSTNAME (même si ce champ est vide).

3.5.3 La partie MSG

La partie MSG d'un message Syslog comprend le message texte à transférer.

3.6 Modélisation des besoin

3.6.1 Acteurs

L'administrateur, le superviseur sont les acteurs interagissent avec notre système.

L'administrateur peut :

— S'authentifier.

— Paramétrer le profil.

— Ajouter un utilisateur.

— Gérer superviseur.

— Consulter statistique.

— visualiser les fichiers logs

— filtrer les logs

— Télécharger rapport.

Superviseur peut :

— S'authentifier.

— choix du message

— visualiser les fichiers logs

— filtrer les logs

— traitements et diagnostics

— Télécharger le rapport.

— consulter rapports générer.

— consulter statistique

3.6.2 Diagramme de cas d'utilisation

3.6.2.1 Diagramme de cas d'utilisation générale

La figure 3.1 représente le diagramme de cas d'utilisation général de notre système d'investigation de log. Nous y retrouvons les acteurs principaux et leurs rôles.

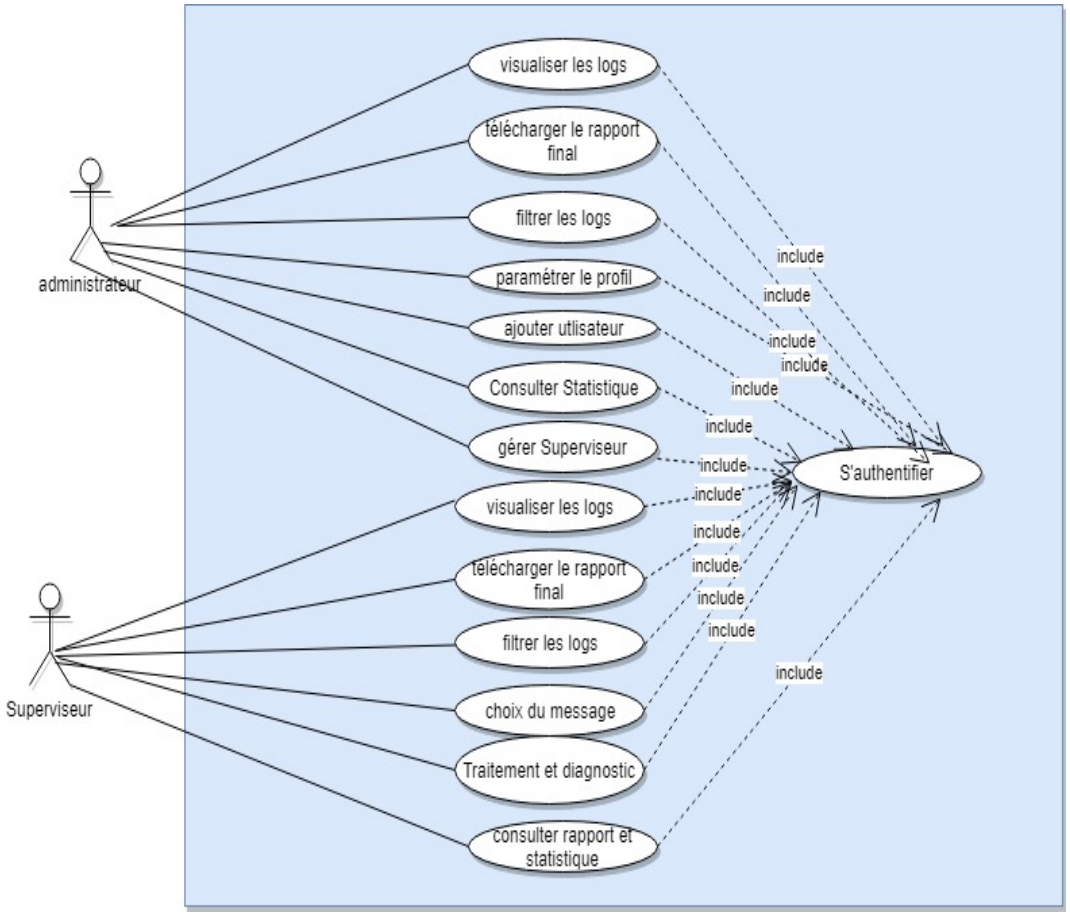

FIGURE 3.2 – Diagramme de cas d'utilisation général

3.6.2.2 Cas d'utilisation «Gérer superviseur » pour administrateur

La figure 3.2 présente de façon plus détaillé les différentes fonctions pour gérer un investigateur, alors il est possible de créer, modifier, supprimer ou consulter un investigateur.

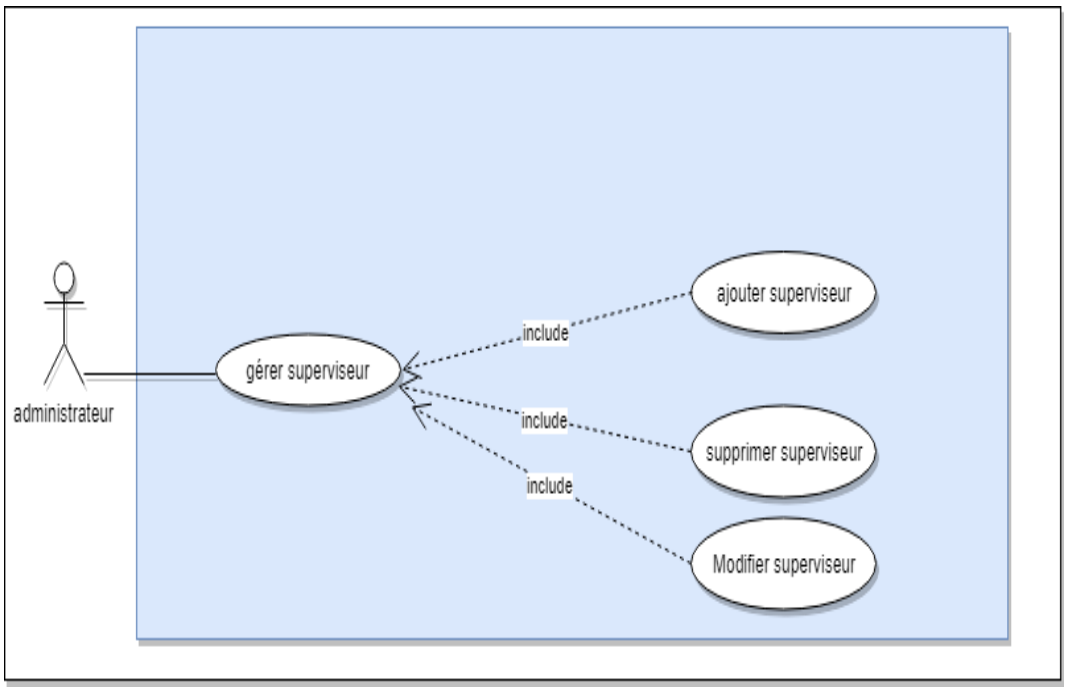

FIGURE 3.3 – Diagramme de cas d'utilisation « Gérer superviseur »

3.6.2.3 Description du cas d'utilisation : « Gérer superviseur »

Étapes	Description
Résumé	— Acteurs : Administrateur — Titre : Gérer superviseur — Description : Le système affiche a l'administrateur la fenêtre de gestion des superviseurs.
Pré-condition	— Le système est opérationnelle — L'administrateur peux ajouter, modifier ou supprimer un superviseur
Scénario Nominal	— L'administrateur clics sur le lien « Gérer superviseur » — Le système affiche la page de gestion des superviseur. — L'administrateur va choisir l'opération à effectuer. — le système va le diriger vers la fenêtre d'ajout,de suppression ou de modification. — Le système affiche un message de confirmation concernant l'opération effectue.
Scénario Alternatif	— L'utilisateur existe déjà. — Validation ou annulation des modifications — Le système affiche le message d'erreur concernant les données saisie.
Post-condition	— Le système renvoie sur la page d'accueil d'administrateur — Le système attend désormais qu'il exécute une nouvelle action.

TABLE 3.1 – Description du cas d'utilisation : « Gérer superviseur »

3.6.2.4 Cas utilisation « Paramétrer le profil »pour l'administrateur

La figure 3.4 présente de façon plus détaillé les différentes fonctions pour gérer un profil, alors il est possible de mettre a jour ou consulter un profil..

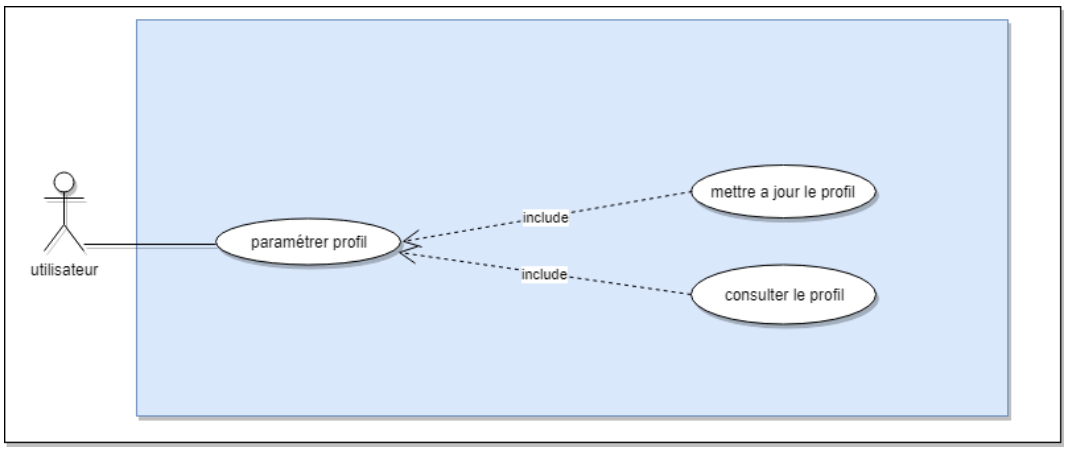

FIGURE 3.4 – Diagramme de cas utilisation « Paramétrer profil »

3.6.2.5 Cas utilisation« consulter base de donnée » pour superviseur

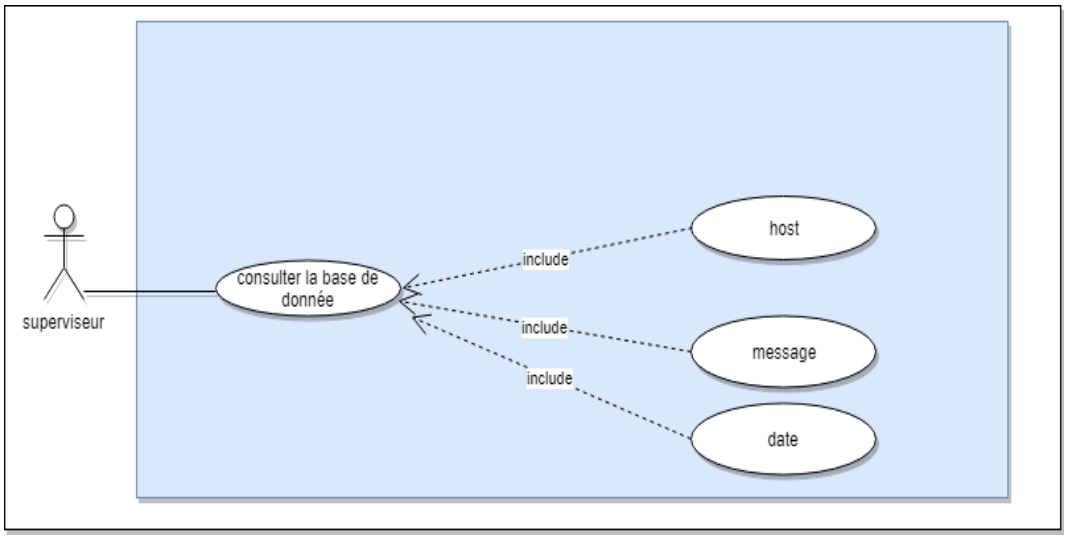

FIGURE 3.5 – Cas utilisation« consulter base de donnée » pour superviseur

3.6.2.6 Description du cas d'utilisation : « consulter base de donnée »

Étapes	Description
Résumé	— Acteurs : superviseur — Titre : « consulter base de donnée ». — Description : Le système affiche au superviseur la fenêtre de chargement des logs.
Pré-condition	— Le superviseur s'est authentifié. — Le superviseur veux charger un fichier log.
Scénario Nominal	— Le superviseur clics sur le lien « consulter base de donnée » — Le système affiche la fenêtre de chargement. — le superviseur précise le type de fichier log. — Le superviseur précise le chemin a suivre pour le chargement de log. — le système récupère le fichier log.
Scénario Alternatif	— le fichier est chargé — Le système affiche le message d'erreur concernant le fichier demandé.
Post-condition	— Le système renvoi sur l'espace de travail de le superviseur. — Le système attend désormais qu'il exécute une nouvelle action.

TABLE 3.2 – Description du cas d'utilisation : « consulter base de donnée »

3.6.2.7 Cas utilisation « traitement et diagnostic »pour superviseur

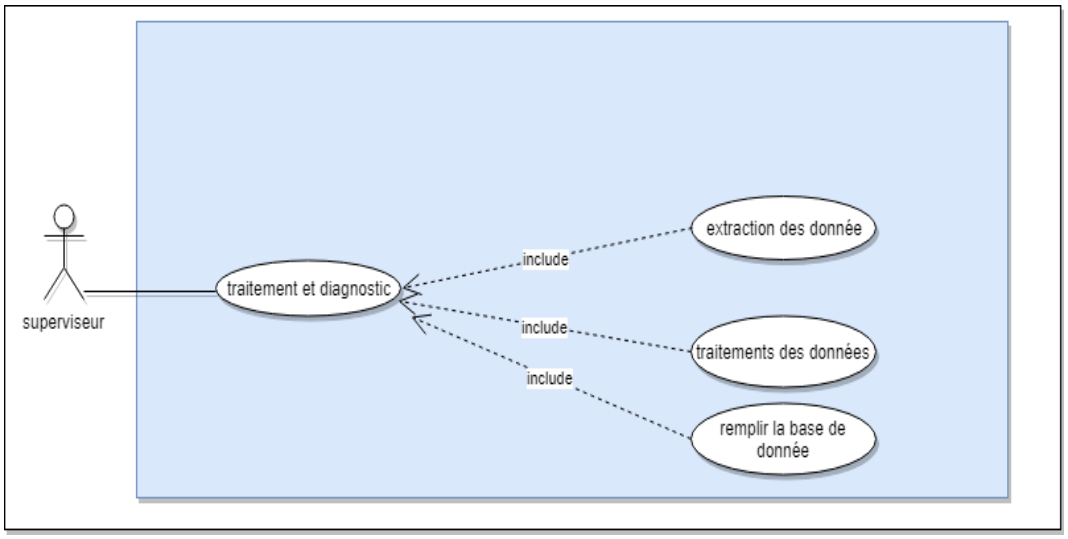

FIGURE 3.6 – Cas utilisation « traitement et diagnostic »pour superviseur

3.6.2.8 Description du cas utilisation « traitement et diagnostic »

Étapes	Description
Résumé	— Acteur : superviseur — Titre :traitement et diagnostic. — Description : Le système affiche au superviseur la fenêtre des traitements et diagnostics..
Pré-condition	— Le superviseur s'est authentifié. — Le superviseur veux extraire les données , traiter les données ou remplir la base de donnée..
Scénario Nominal	— le superviseur clic sur le lien traitement et diagnostic. — le système va le rédiger vers la fenêtre de traitement et diagnostic. — le superviseur va paramétrer le traitement à effectuer. — le système va le diriger vers la page demandé.
Scénario Alternatif	— annulation du traitement.
Post-condition	— Le système renvoi sur l'espace de travail de le superviseur. — Le système attend désormais qu'il exécute une nouvelle action.

TABLE 3.3 – Description du cas d'utilisation : « traitement et diagnostic »

3.6.2.9 Cas utilisation« consulter rapport et afficher statistique »pour superviseur

La figure 3.7 présente les fonctions nécessaires pour gérer un rapport, le superviseur télécharge le rapport pour le vérifier et modifier son statut. Si le rapport n'est pas validé, le superviseur le supprime.

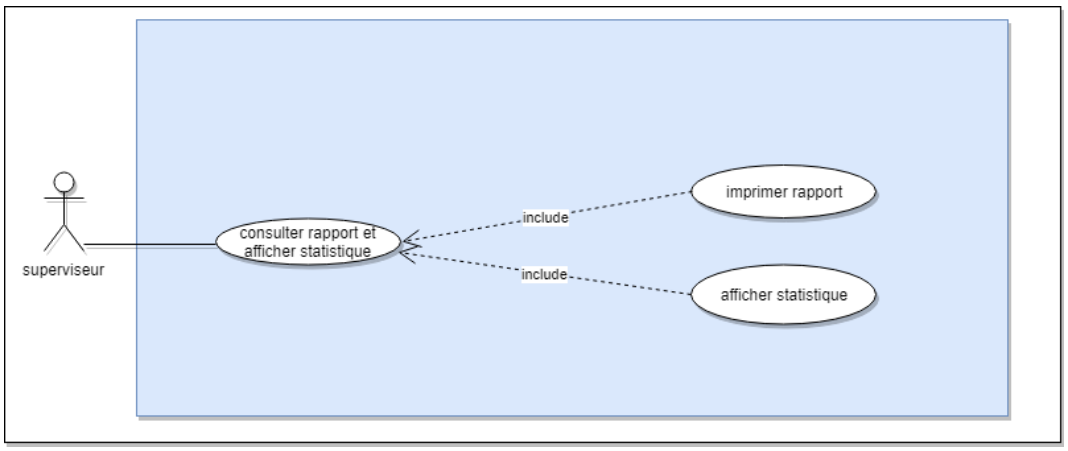

FIGURE 3.7 – Diagramme de cas utilisation≪ consulter rapport et afficher statistique ≫

3.6.2.10 Description du cas d'utilisation : « consulter rapport et afficher statistique »

Tapes	Description
Résumé	— Acteurs : superviseur — Titre : Consulter le rapport et afficher les statistiques des attaques. — Description : Le système affiche à l'administrateur les statistique des logs choisis et le rapport correspondant.
Pré-condition	— L'administrateur s'est authentifié. — Le système est opérationnel. — Les rapports ont généré. — Les logs ont été filtrés. — L'administrateur accède à son espace de travail.
Scénario Nominal	— L'administrateur clique sur le lien « consulter rapport et afficher statistique » — Le système renvoi sur sa page le graphe indiquant le pourcentage et le nom de chaque catégorie d'attaque et le rapport correspondant .
Post-condition	— Les statistiques des catégories des attaques ont affiché. — Le système attend désormais qu'il exécute une nouvelle action.

TABLE 3.4 – Description du cas d'utilisation : « consulter rapport et afficher les statistique de l'attaque »

3.6.2.11 Description du cas d'utilisation : « S'authentifier »

Tapes	Description
Résumé	— Acteur : Utilisateur (Administrateur) — Titre : Authentifier (Administrateur,Superviseur) — Description : le système identifie l'administrateur, superviseur qui veut utiliser la plateforme
Pré-condition	— L'administrateur, le superviseur s'est connecté aux systèmes. — Le systèmes est opérationnelle.
Scénario Nominal	— L'administrateur, le superviseur entre leur paramètre de connexion login et mot de passe. — Le système vérifie les information saisie. — Le systèmes affiche l'espace de travail de chaque utilisateur.
Scénario alternatif	— Les données sont erronées. — Le système affiche un message d'erreur que l'utilisateur n'existe pas.
Post-condition	— L'utilisateur est sur son espace de travail. — Le système attend qu'il exécute une nouvelle action

TABLE 3.5 – Description du cas d'utilisation : « S'authentifier »

3.7 Diagramme de déploiement

La figure 3.8 présente le diagramme de déploiement qui modélise l'architecture physique de notre système ainsi qu'il affiche les relations entre les composants logiciels et matériels de notre système.

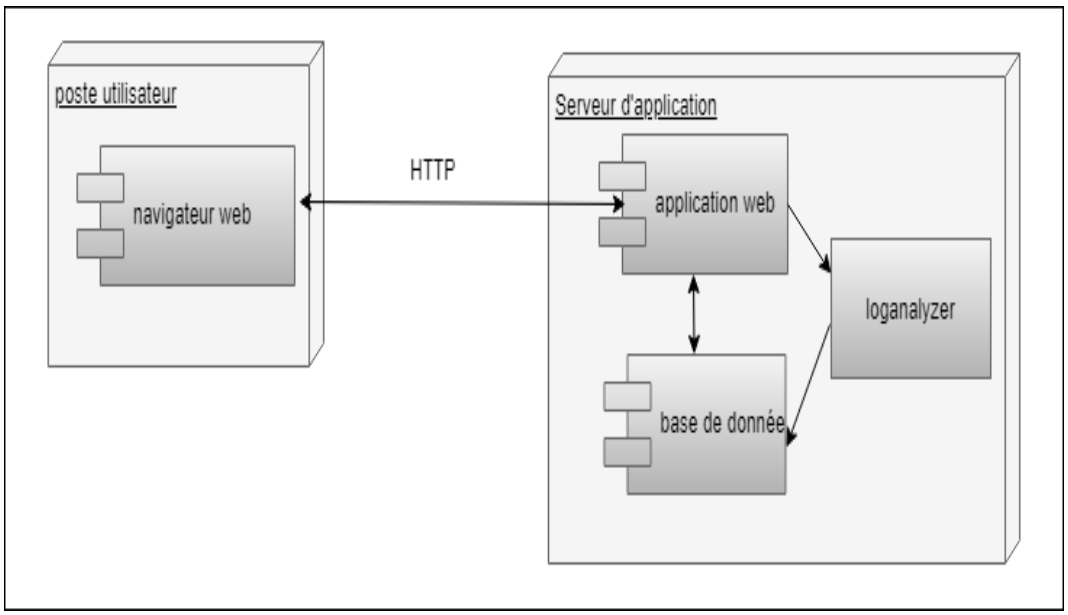

FIGURE 3.8 – diagramme de déploiement

3.8 Conception

Après l'élection des besoins exprimer ce la forme de la fonctionnalité modélisé comme des cas d'utilisation et scénarios nous pouvons passer a une nouvelle vue du modèle statique et dynamique qui nous permettra de modéliser la structure logique du système a réaliser. Cette vue exprime les modules et les exécutables physiques sans aller à la réalisation concrète du système. cette modélisation est effectué dans des diagrammes de séquences.

3.8.1 Digramme de séquence

Le diagramme de séquence présente la vue dynamique du système. L'objectif du diagramme de séquence est de représenter les interactions entre les objets en indiquant la chronologie des échanges (scénarios) réalisées par un acteur. Cette représentation se réalise par cas d'utilisation.

3.8.1.1 Digramme de séquence de cas d'utilisation « S'authentifier »

La figure 3.13 montre le Digramme de séquence de cas d'utilisation « S'authentifier »

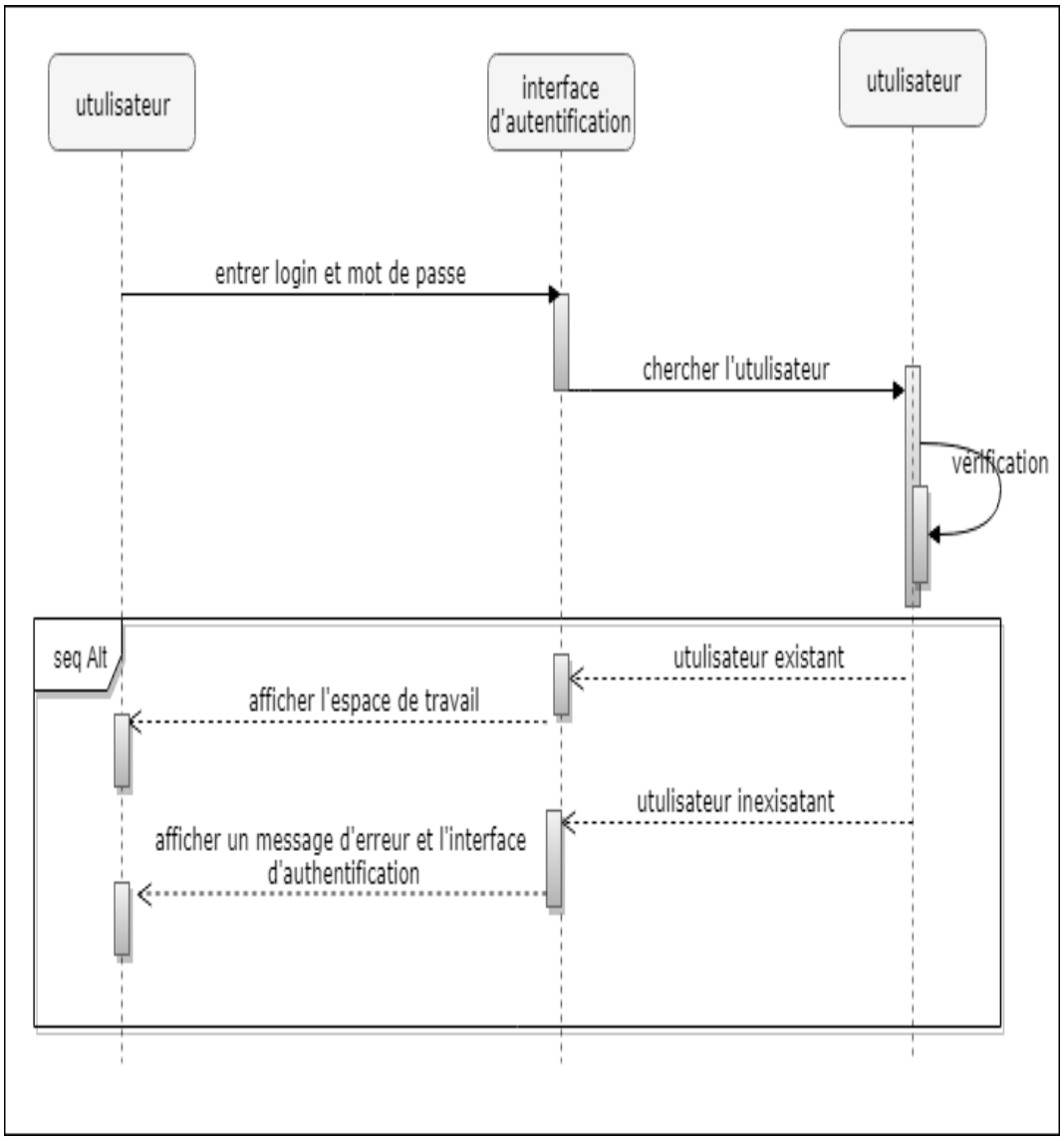

FIGURE 3.9 – Digramme de séquence de cas d'utilisation « S'authentifier »

3.8.1.2 Digramme de séquence de cas d'utilisation «Ajouter un utilisateur »

La figure 3.14 montre digramme de séquence de cas d'utilisation «Ajouter un utilisateur »

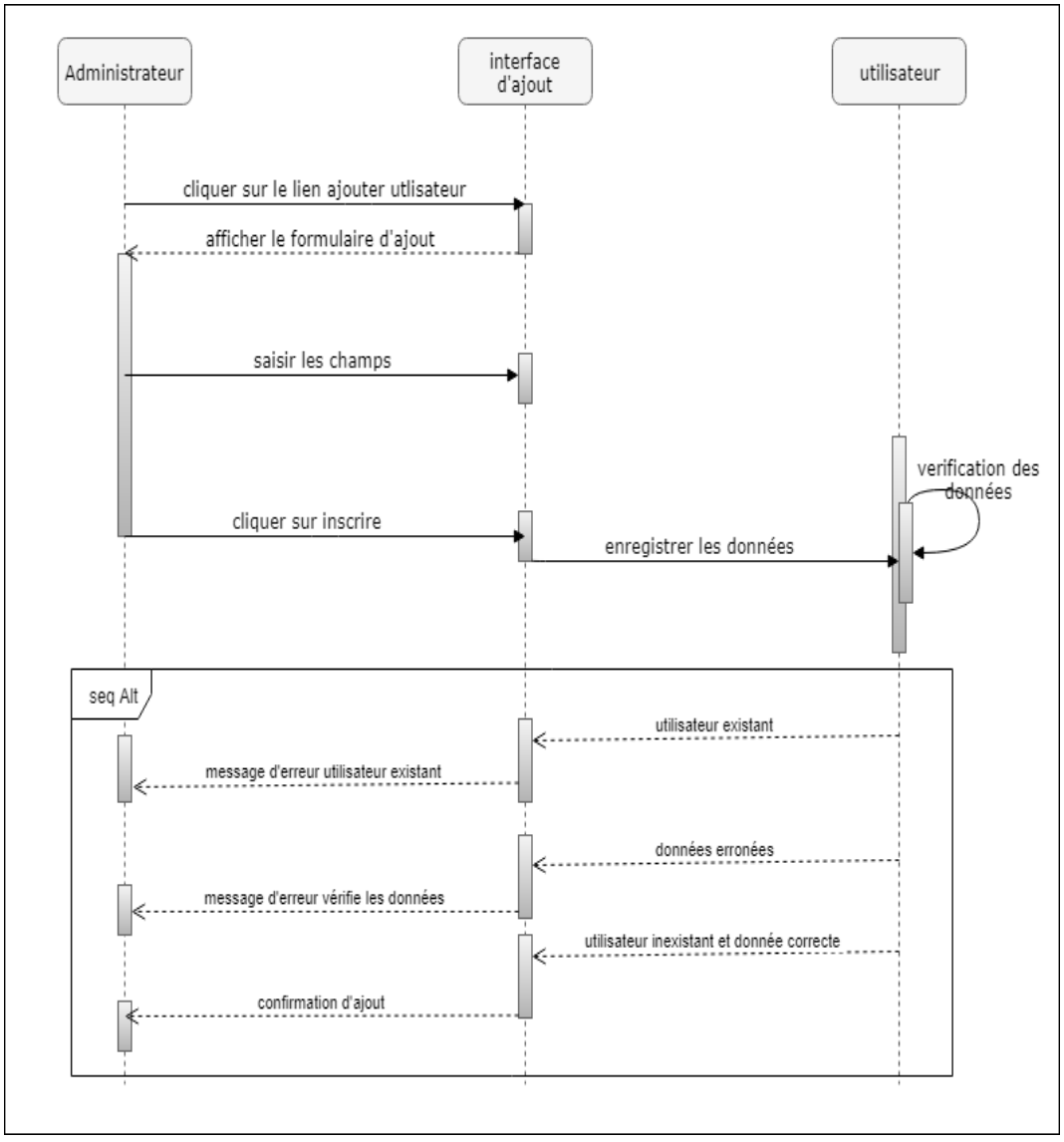

FIGURE 3.10 – Digramme de séquence de cas d'utilisation « Ajouter utilisateur »

3.8.1.3 Digramme de séquence de cas utilisation « traitement et diagnostic »

La figure 3.15 montre digramme de séquence de cas d'utilisation «traitement et diagnostic »

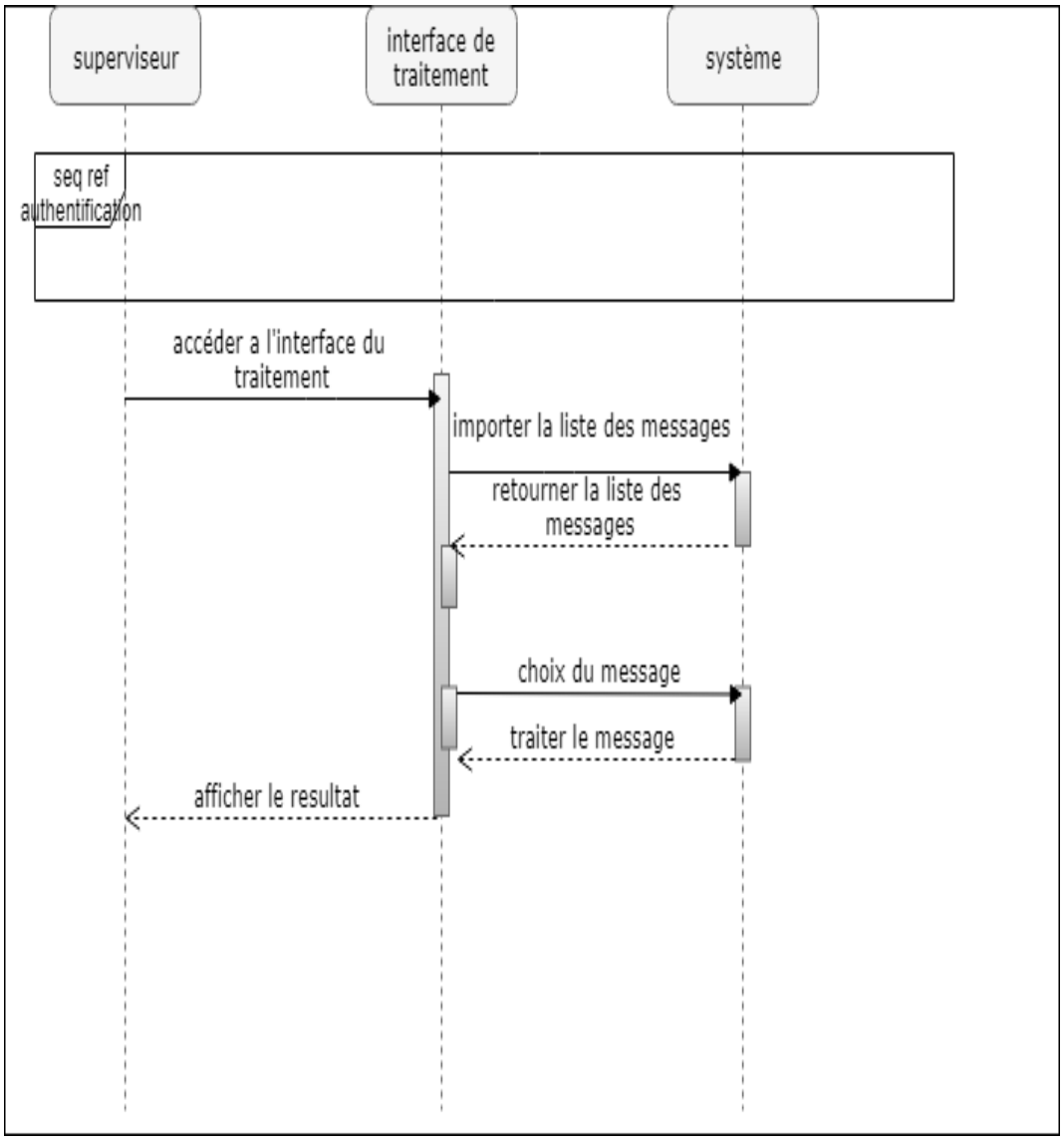

FIGURE 3.11 – Digramme de séquence de cas utilisation « traitement et diagnostic »

3.8.1.4 Digramme de séquence de cas utilisation« afficher les statistique de l'attaque »

La figure 3.16 montre digramme de séquence de cas d'utilisation «Afficher les statistique de l'attaque »

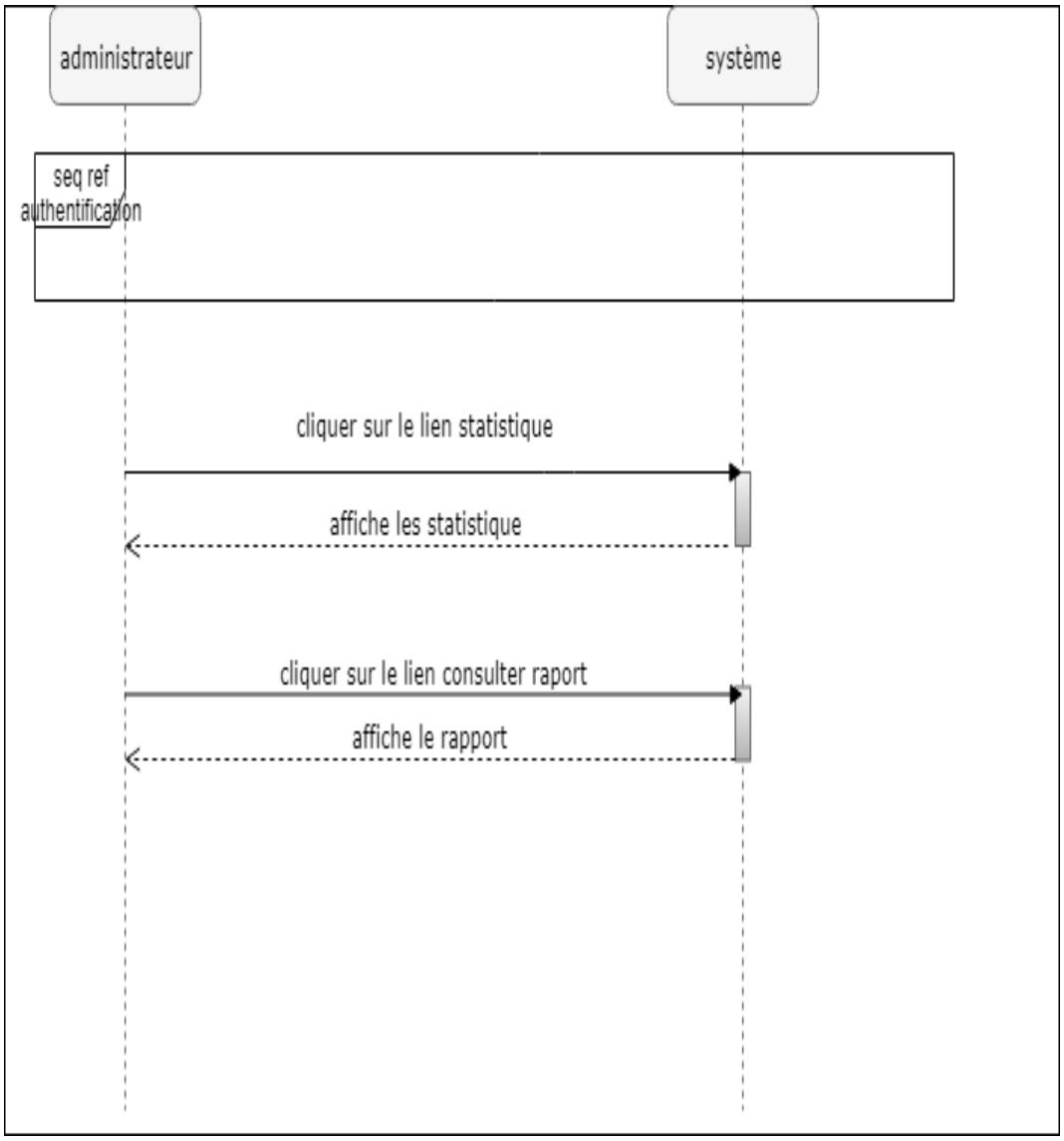

FIGURE 3.12 – Digramme de séquence de cas utilisation« afficher les statistique de l'attaque »

.

3.9 Conclusion

Au cours de ce chapitre, nous avons analysé les besoins fonctionnels de notre système, nous avons cerné les différentes relations et interactions de ce dernier. Cette étape nous a permis de mettre en avant les phases nécessaires à la réalisation de notre application à savoir l'architecture du système et les diagrammes de séquences. En se basant sur les diagrammes du langage UML, nous avons présenté les composants logiciels collaborant pour la réalisation des fonctionnalités de notre système tout en nous concentrant sur les cas d'utilisation les plus significatifs et représentatifs. Lors du chapitre suivant à savoir la réalisation, nous présenterons l'environnement matériel et logiciel.

Chapitre 4

Réalisation

4.1 Introduction

Nous avons organisé la partie réalisation en deux étapes tout en respectant la méthode 2TUP qui, nous le rappelons, donne une grande importance à la technologie utilisée.

Nous présentons dans cette partie la mise en œuvre des composants issus de la conception dont nous avons présenté les composants logiciels collaborant pour la réalisation des fonctionnalités de notre système tout en nous concentrant sur les cas d'utilisation les plus significatifs et représentatifs.

nous présentons l'environnement matériel et logiciel utilisés et cela après recensement des besoins fonctionnels et non fonctionnels dans la partie analyse et conception.

4.2 présentation de la plateforme de réalisation

4.2.1 Architecture de la plateforme

L'architecture utilisée comme nous l'avons expliqué dans le chapitre 3 est à 2 tiers comme le montre la figure la figure 4.1 et elle permet de spécifier les composants physiques nécessaires pour l'application à savoir :

- Tiers 1 : Les équipements à écouter
- Tiers 2 : Une machine d'application et la base de données de notre application.

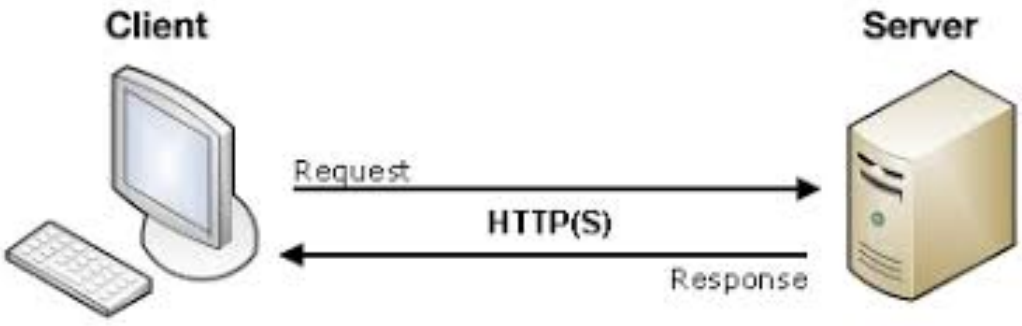

FIGURE 4.1 – l'architecture 2 tiers

4.2.2 Organisation de la phase de réalisation

L'hétérogénéité des équipements disponibles au niveau de l'organisme d'accueil ainsi que la contrainte de la disponibilité des ressources ainsi que l'environnement de production induisent des contraintes nécessitant une adaptation de la phase de réalisation. Ces éléments sont expliqués ci-après.

4.2.2.1 RESSOURCES EXPÉRIMENTALES

Toute configuration se fait au niveau d'un poste pilote qui nous permet de tester les configurations à apporter ainsi que des capture écran des configurations initiales sont sauvegardées, afin de palier à toute interruption de la disponibilité d'un service pour palier à tout incident sur les postes clients pilotes

4.2.2.2 CONTRAINTES ENVIRONNEMENTALES

Cependant, l'ensemble des équipements actifs réseau est actuellement très hétérogène. Lors de l'étude de l'existant effectué au début du projet, plusieurs modèles différents d'équipement fournis par plusieurs constructeurs, cette variété d'équipement induit une forte Complexité de configuration Par ailleurs, il n'est pas possible de mettre à notre disposition tous l'existant du ce nte réseau à savoir les modèles des différents d'équipements pour la phase de réalisation du projet. Ce qui nous a amené à planifier la réalisation avec l'équipe réseau de l'utilisation des postes clients. Ce point précis a donc conditionné la planification de la phase de réalisation.

4.2.2.3 PLANIFICATION

Dans la phase planification nous procèderons à choisir une configuration pour chaque modèle des équipements réseaux à superviser, comme il nous est impossible de toucher à toute l'infrastructure réseau , nous avons catégoriser l'infrastructure en trois classes :

Catégorie 1 : le matériel qui regroupe tout les équipement matériel Routeur Cisco, Switch

Catégorie 2 : les applications Web.

Catégorie 3 : les serveurs des différentes plateformes.

une fois les tests et les contrôles sont validés par l'équipe réseau, nous rédigerons par la suite générons un prototype de configuration qui sera appliqué à chaque catégorie.

la figure 4.2 résume l'architecture de notre application

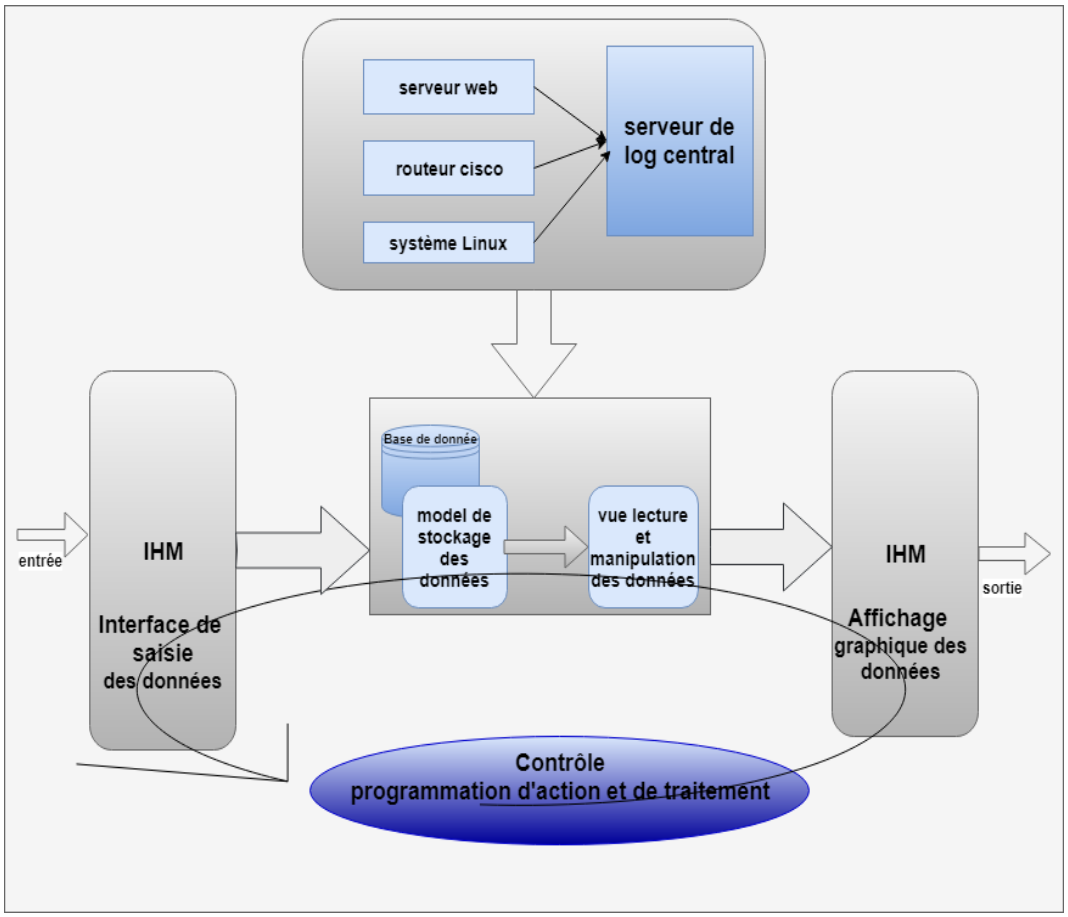

FIGURE 4.2 – Architecture générale de la plateforme

4.2.3 Environnement de travail

Dans cette partie, nous présentons les différents outils requis pour le développement et la mise en œuvre de notre application.

4.2.3.1 Environnement matériel

Nous avons utilisé principalement un seul ordinateur portable dont leur configuration est la suivante :

— Un ordinateur tournant sous Debian 9.4 64 bit.

— Processeur Intel core i7-6500U

— 8 GO de RAM.

— 2TERA de disque dur.

De plus nous avons accès aux équipements suivants pour l'obtention des fichiers journaux pour les tests de l'application :

— Pare-feux ASA

— routeur Cisco 6000 le nœud principale

— routeur Cisco biologie

4.2.4 Environnement logiciel

Dans cette section, nous présentons les différents outils de développement ainsi que le SGBD(Système de Gestion de Base de Données) et l'outil de conception, qui sont liés à notre projet. Nous avons utilisé l'éditeur Sublimtext pour l'écriture des scripts Php pour le développement différents modules de notre application.

4.2.4.1 draw.io

draw.io est une application de création de diagrammes basée sur un navigateur. Il est disponible en tant qu'application en ligne avec intégration facultative a diverses options de stockage en nuage. draw.io est en permanence gratuit pour un usage personnel et académique.[

4.2.4.2 Le SGBD Mysql

Le serveur de base de données MySQL est très rapide, fiable et facile à utiliser. Il dispose aussi de fonctionnalités pratiques, développées en coopération avec ces utilisa-

teurs puisqu'il est Open Source. Le serveur MySQL a été développé à l'origine pour des grandes bases de données plus, et a été utilisé avec succès dans des environnements de production très contraints et très exigeant, depuis plusieurs années. Bien qu'en développement, le serveur MySQL offre des nombreuses fonctions puissantes. Ses possibilités de connexion, sa rapidité et sa sécurité font du serveur MySQL un serveur hautement adapté au développement des applications.

4.2.4.3 PHP [1]

Est un langage informatique, ou un langage de script, utilisé principalement pour la conception de sites web dynamiques. Il s'agit d'un langage de programmation sous licence libre qui peut donc être utilisé par n'importe qui de façon totalement gratuite.[12]

4.2.4.4 Serveur web apache

Le serveur HTTP Apache est un serveur Web multiplateforme gratuit et open-source, publié sous licence Apache License 2.0. Apache est développé et maintenu par une communauté ouverte de développeurs sous les auspices de la Fondation Apache Software.

4.2.4.5 Service Rsyslog

Le service rsyslog fournit une installation pour exécuter un serveur d'enregistrement et pour configurer des systèmes individuels pour qu'ils envoient leurs fichiers journaux sur le serveur d'enregistrement. Le service rsyslog doit être installé sur le système qu'on a utlisé en tant que serveur d'enregistrement et sur tous les systèmes qui seront configurés pour y envoyer leurs journaux.[13]

4.2.4.6 LogAnalyseur

LogAnalyzer fait partie de la gamme d'applications de surveillance MonitorWare d'Adiscon. Il fonctionne à la fois sous Windows et Unix / Linux. La base de données peut

1. Hypertext Preprocessor

être peuplée par MonitorWare Agent, WinSyslog ou EventReporter du côté Windows et par rsyslog du côté Unix / Linux. LogAnalyzer présente plusieurs avantages :

— Solution gratuite
— Interface compatible eventlog et Syslog
— Possibilité de configuration importante
— S'adapte à plusieurs formats de stockage
— Grande communauté.[14]

4.2.4.7 Sublimtext

un éditeur de texte qui se démarque des autres par son interface et ses fonctionnalités. L'application supporte la coloration syntaxique selon les langages de programmation utilisés. Sublime Text dispose d'une interface pratique qui comprend un panel avec l'arborescence des dossiers des différentes sources éditées. Ensuite, on retrouve la gestion d'onglets pour un accès rapide aux fichiers en cours d'édition. Enfin, Sublime Text offre des fonctionnalités d'édition avancées telles que la modification de variables instantanées ou encore l'affichage en miniature du code sur un volet à droite du texte édité.[15]

4.2.4.8 Linux distribution debian version 9.4 en ligne de commande

Debian est un système d'exploitation de type Unix (distribution Linux) et une distribution de logiciels libres. Debian a toujours au moins trois versions activement maintenues :

— La distribution stable contient la dernière distribution officiellement sortie de Debian.C'est la version de production de Debian, celle que nous recommandons en premier d'utiliser.Actuellement, la distribution stable de Debian est la version 9, nom de code Stretch. Elle a été initialement publiée en tant que version 9 le 17 juin 2017 et sa dernière mise à jour, version 9.4, a été publiée le 10 mars 2018.
— La distribution testing contient les paquets qui n'ont pas encore été acceptés dans

la distribution stable, mais qui sont en attente de l'être. Le principal avantage d'utiliser cette distribution est qu'elle contient des versions plus récentes des logiciels.

— ILa distribution unstable est celle sur laquelle les activités de développement se déroulent. Généralement, cette distribution est utilisée par les développeurs et par ceux qui aiment vivre sur le fil.[16]

4.3 Processus de centralisation

la figure 4.3 présente le processus de centralisation

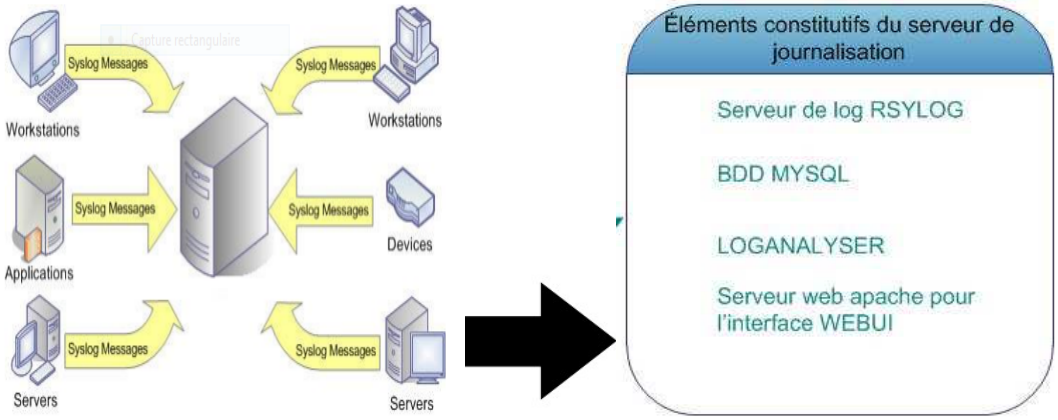

FIGURE 4.3 – processus de centralisation

4.3.1 Log envoyé par le service apache

Le serveur HTTP Apache fournit toute une variété de mécanismes différents pour la journalisation de tout ce qui peut se passer au sein de serveur, depuis la requête initiale, en passant par le processus de mise en correspondance des URLs jusqu'à la fermeture de la connexion, y compris toute erreur pouvant survenir au cours du traitement. Le journal des erreurs du serveur, dont le nom et la localisation sont définis par la directive ErrorLog, est le journal le plus important. C'est dans celui-ci que le démon Apache httpd va envoyer les informations de diagnostic et enregistrer toutes les erreurs qui surviennent lors du traitement des requêtes.

4.3.2 Logs envoyé par les diffèrent programme du système d'exploitation

les messages envoyés par d'autres démons, services ou par le noyau Linux peuvent être redirigés vers des fichiers ou des terminaux. Syslogd est un démon permettant de centraliser centraliser sur un seul serveur les logs en provenance de routeurs ou d'autres serveurs sous Linux ou sous Windows. Par exemple les messages d'informations ou d'erreurs émis par le système de messagerie (ex : Postfix), sont enregistrés grâce à syslogd dans le fichier « /var/log/mail.info ».

Dans chaque ligne d'évènement on distingue :

— La date à laquelle l'évènement a été déclenché

— Le processus déclencheur de l'évènement

— Le processus ayant demandé l'ajout du message correspondant au log

— Le niveau de gravité du message (priority)

4.3.3 Les logs routeur Cisco

Les équipements Cisco stockent les logs de différentes manières : non stockés, stockés localement, et syslog. Il est ainsi possible d'envoyer les logs vers un serveur Syslog, où ils seront stockés sous forme de fichier texte.Les logs stockés localemnt sont inscrits directement dans le terminal, mais le reste des logs n'est pas sauvegardé, faute de stockage. La méthode de gestion n'étant pas configurée par défaut, il faut donc le faire manuellement.

4.4 Procédure de la centralisation

4.4.1 Configuration coté client

Linux

— On accède au fichier /etc/rsyslog.conf. Dans rules on ajoute la ligne suivantes

pour envoyer tout les logs vers un serveur de centralisation.

```
*.* @ip de serveur de centralisation des logs : ports
```

— on redémarre le service Rsyslog .

```
service rsyslog restart
```

Application web : serveur web apache

— Dans le fichier /etc/apache2/sites-available/default on commente les deux ligne customlog et errorLog qui specifie ou envoyer le logs.

```
customlog [$apache_apache_log_dir]/acces.log combined
errorLog[ $apache_apache_log_dir]/error.log
```

— On spécifié le schéma ou envoyer les logs et la facility

```
— errorlog « |/usr/bin/logger -t apache -p local6.info »
— customlog « |/usr/bin/logger -t apache -p local6.info »proxy
```

— On remplace loglevel warn par loglevel info

— On accède dans le fichier /etc/rsyslog.conf on ajoute la ligne

```
local6.* @du serveur central et le port
```

— On redémarre le service apache

```
#service apache2 restart
```

Routeur CISCO faculté :

— On va commencer par ouvrir un terminal. Une fois sur celui-ci, on va passer en mode enable :

```
enable
```

— L'heure que vont avoir les journaux exportés a une importance particulière dans le système de centralisation des logs. Il permet en effet de retracer précisément les logs entre plusieurs machines, c'est pour cela que la première chose à faire est de mettre notre machine à la bonne date et la bonne heure :

```
clock set 14 :00 :00 june 05 2018
```

— On va ensuite passer en mode configuration afin de paramétrer l'envoi des logs

```
conf t
```

— On commence par activer l'horodatage des logs

```
service timestamps
```

— On configure les différents paramètres propres à l'envoi des logs, on commence par l'IP du serveur distant

```
logging 10.2.0.67
```

— On peut préciser le log facility qui va nous permettre, sur le serveur distant, de trier les logs

```
logging facility local5
```

— Configurer le log-level à partir duquel on prendra le soin d'envoyer les logs.

```
logging trap informational
```

Notre système Cisco va maintenant commencer à envoyer ses logs au serveur distant. On va pouvoir récapituler la configuration présente en retournant en mode enable puis en saisissant "show logging" :

```
>en
#clock set <heure>:<minute>:<seconde> <mois> <numéro_jour> <année>
//Configuration manuelle de la date et l'heure
#conf t
(config)#ntp serveur <adresse_ip__ou_hostname_serveur_ntp> //Configuration de
la date et l'heure avec un serveur NTP
(config)#service timestamps
(config)#logging trap <nom_niveau_logging>
(config)#logging facility <nom_facility_log>
(config)#logging <adresse_ip_serveur_syslog>
(config)#end
#show logging
#copy run start
```

FIGURE 4.4 – les etapes de configuration de routeur Cisco

4.4.2 Configuration coté serveur

Linux

— On doit paramétrer le serveur et on va effectuer des modification dans rsyslog.conf

```
vim /etc/rsyslog.conf
```

— On dé-commente le protocole de transport a utiliser

```
$modload imudp
$UDPServeurRun 514
$modload imtcp
$InputTCPServeurRun 514
```

— On redémarre le serveur rsyslog

```
service rsyslog restart
```

— on fait la commande netstat -nul pour vérifie que le port 514 est ouvert a l'extérieur.

Application web : serveur web apache

— on va afficher les logs

```
cd /var/log/syslog-centrale
```

```
tail -f /var/log/syslog-centrale/messages
```

Routeur CISCO faculté

— Dans le fichier "/etc/rsyslog.conf" et ajouter la ligne suivante pour que tous les logs arrivant en log-facility 5 (local5) soient mis dans un fichier spécifique. On mettra par exemple tous les logs des machines Cisco sur ce logs level :

```
local5.* /var/log/cisco.log
```

— On va ensuite redémarrer ce service

```
service Rsyslog restart
```

la figure suivante montre le dossier de centralisation

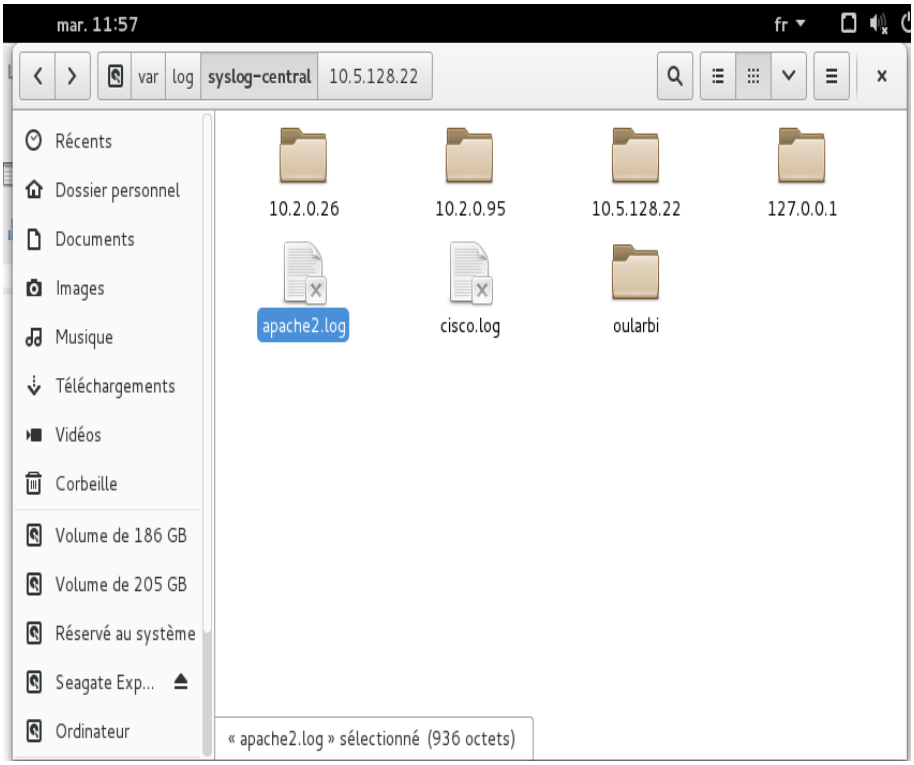

FIGURE 4.5 – serveur centrale des logs

4.5 Résultat de la centralisation

4.5.1 les logs linux

La figure suivante présente les logs linux

```
tail: aucun fichier restant
root@oularbi:/var/log/syslog-central/10.2.0.95# cd ..
root@oularbi:/var/log/syslog-central# tail -f 10.2.0.95/systemd.log
Jun  3 09:49:49 lynx3 systemd[1]: Started Make remote CUPS printers available locally.
Jun  3 09:59:42 lynx3 systemd[1]: Starting Cleanup of Temporary Directories...
Jun  3 09:59:42 lynx3 systemd[1]: Started Cleanup of Temporary Directories.
Jun  3 09:59:48 lynx3 systemd[1]: anacron.timer: Adding 2min 22.692052s random time.
Jun  3 10:02:59 lynx3 systemd[1]: Started Run anacron jobs.
Jun  3 10:02:59 lynx3 systemd[1]: anacron.timer: Adding 57.635142s random time.
Jun  3 10:07:55 lynx3 systemd[1623]: Starting Evince document viewer...
Jun  3 10:07:55 lynx3 systemd[1623]: Started Evince document viewer.
Jun  3 11:00:59 lynx3 systemd[1]: Started Run anacron jobs.
Jun  3 11:00:59 lynx3 systemd[1]: anacron.timer: Adding 3min 7.638325s random time.
^C
root@oularbi:/var/log/syslog-central# tail -f 10.2.0.95/su.log
May 30 10:53:42 lynx3 su[4000]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=lion rhost=  user=root
May 30 10:53:44 lynx3 su[4000]: pam_authenticate: Authentication failure
May 30 10:53:44 lynx3 su[4000]: FAILED su for root by lion
May 30 10:53:44 lynx3 su[4000]: - /dev/pts/0 lion:root
^C
root@oularbi:/var/log/syslog-central# tail -f 10.2.0.26/su.log
May 29 10:38:47 debian su[30088]: pam_unix(su:auth): authentication failure; logname=biologie uid=1000 euid=0 tty=/dev/pts/1 ruser=biologie rhost=  user=root
May 29 10:38:49 debian su[30088]: pam_authenticate: Authentication failure
May 29 10:38:49 debian su[30088]: FAILED su for root by biologie
May 29 10:38:49 debian su[30088]: - /dev/pts/1 biologie:root
May 29 10:39:01 debian su[30090]: Successful su for root by biologie
May 29 10:39:01 debian su[30090]: + /dev/pts/1 biologie:root
May 29 10:39:01 debian su[30090]: pam_unix(su:session): session opened for user root by biologie(uid=1000)
Jun  3 12:02:05 debian su[6500]: Successful su for root by root
Jun  3 12:02:05 debian su[6500]: + /dev/pts/0 root:root
Jun  3 12:02:05 debian su[6500]: pam_unix(su:session): session opened for user root by biologie(uid=0)
^C
root@oularbi:/var/log/syslog-central# tail -f 10.2.0.26/systemd.log
May 29 10:34:07 debian systemd[1]: Starting LSB: Raise network interfaces....
May 29 10:34:09 debian systemd[1]: Started LSB: Raise network interfaces..
May 29 12:20:18 debian systemd[1]: Starting Cleanup of Temporary Directories...
May 29 12:20:18 debian systemd[1]: Started Cleanup of Temporary Directories.
Jun  3 12:01:43 debian systemd[1]: Stopping System Logging Service...
Jun  3 12:01:43 debian systemd[1]: Starting System Logging Service...
Jun  3 12:01:43 debian systemd[1]: Started System Logging Service.
Jun  3 12:02:43 debian systemd[1]: Stopping LSB: Raise network interfaces....
Jun  3 12:02:44 debian systemd[1]: Starting LSB: Raise network interfaces....
Jun  3 12:02:47 debian systemd[1]: Started LSB: Raise network interfaces..
^[[B
```

FIGURE 4.6 – les logs linux retourné par ligne de commande

4.5.2 les logs cisco

la figure suivante présente les logs retournés par un routeur cisco

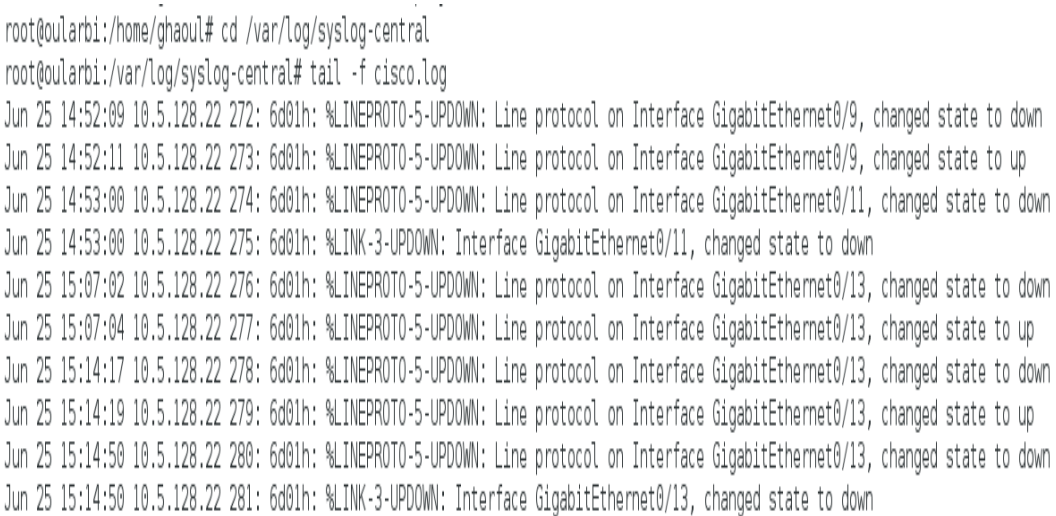

FIGURE 4.7 – les logs cisco retourne par ligne de commande

4.5.3 les logs d'apache

La figure suivante présente les logs retournés par un service apache

FIGURE 4.8 – les logs d'apache retourné par ligne de commande

4.6 Traitements des logs

4.6.1 Enregistrement des logs dans une base de donnée

— Pour que le serveur Rsyslog soit fonctionnel, il nous faut installer un certain nombre de paquets. Nous commençons d'abord par mettre à jour notre machine

avec :

```
apt-get update && upgrade
```

— Ensuite, nous allons installer beaucoup de dépendances :

```
apt-get install python-software-properties rsyslog rsyslog-mysql unzip zip binutils cpp fetchmail flex gcc libc6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules zlib1g-dev autoconf libtool bison autotools-dev g++ mysql-server mysql-client libmysqlclient-dev apache2 apache2-doc apache2-mpm-prefork apache2-utils libexpat1 ssl-cert libapache2-mod-php5 php5 php5-common php5-curl php5-dev php5-gd php5-intl php-pear php5-imagick php5-imap php5-json php5-mcrypt php5-memcache php5-common php5-mysql php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl
```

— On va rentrer un mot de passe pour la base de donnée.

— Pour vérifier que les services Apache2 et MySQL sont bien sur écoute, nous pouvons utiliser la commande netstat -tapn qui devrait nous montrer ces lignes :

```
tcp 0 0 127.0.0.1 :3306 0.0.0.0 :* LISTEN 25240/mysqld
tcp 0 0 0.0.0.0 : :80 0.0.0.0 :* LISTEN 25844/apache2
```

Après avoir installé Rsyslog , nous passons à la configuration du fichier de configuration : nano /etc/rsyslog.conf on a suivi les étapes suivante :

— On de-commente les paramètre suivant :

```
$ModLoad imtcp
$InputTCPServerRun 1514 (il faut remplacer 514 par 1514)
$ModLoad imudp
$UDPServerRun 1514
```

— On remplace rsyslogUserName par rsyslog qui est le nom d'utilisateur par défaut, SyslogDatabase par le nom de la base qui est Syslog puis rsyslogUserPassword par le mot de passe qui a été choisi durant l'installation de Rsyslog et cella apres avoir rajouter les lignes suivantes :

```
$ModLoad ommysql
*.* :ommysql :127.0.0.1,<SyslogDatabase>,<rsyslogUserName>,<rsyslogUserPassword>
```

— Nous allons maintenant redémarrer notre service

— Rsyslog : /etc/init.d/rsyslog restart

4.6.2 Visualisation des logs avec logAnalyzer

— Pour installer logAnalyzer on utilise les commandes suivantes :

```
cd /usr/local/src
wget http ://download.adiscon.com/loganalyzer/loganalyzer-3.6.6.tar.gz (cette version est la dernière version stable en Juin 2016)
tar -zxvf loganalyzer-3.6.6.tar.gz
mv loganalyzer-3.6.6/src/* /var/www/html
chown www-data :www-data -Rf /var/www/html/*
cp loganalyzer-3.6.6/contrib/* /var/www/html
chmod +x /var/www/html/configure.sh /var/www/html/secure.sh
cd /var/www/html
./configure
```

— Maintenant que LogAnalyzer est installé, nous allons accéder à l'interface web avec

```
http ://localhost/install.php
```

4.6.2.1 les étapes importante de configuration de LogAnalyzer

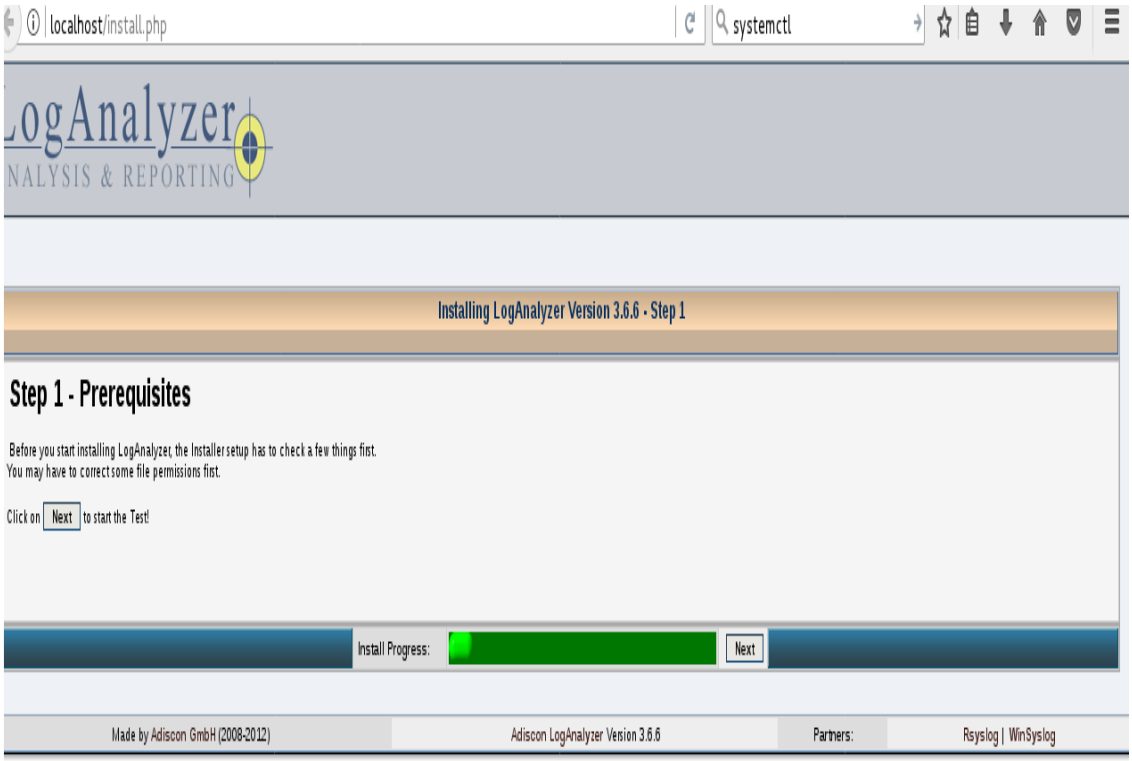

FIGURE 4.9 – interface LogAnalyzer

dans l'etape qui suiv on a remplis les informations. on a cocher la case Enable User Database puis rentrer les informations comme le port (1514), le nom de la base (Syslog), enlever la Table Prefix changer le nom d'utilisateur par rsyslog et rentrer son mot de passe puis cocher la case Require user to be logged in.

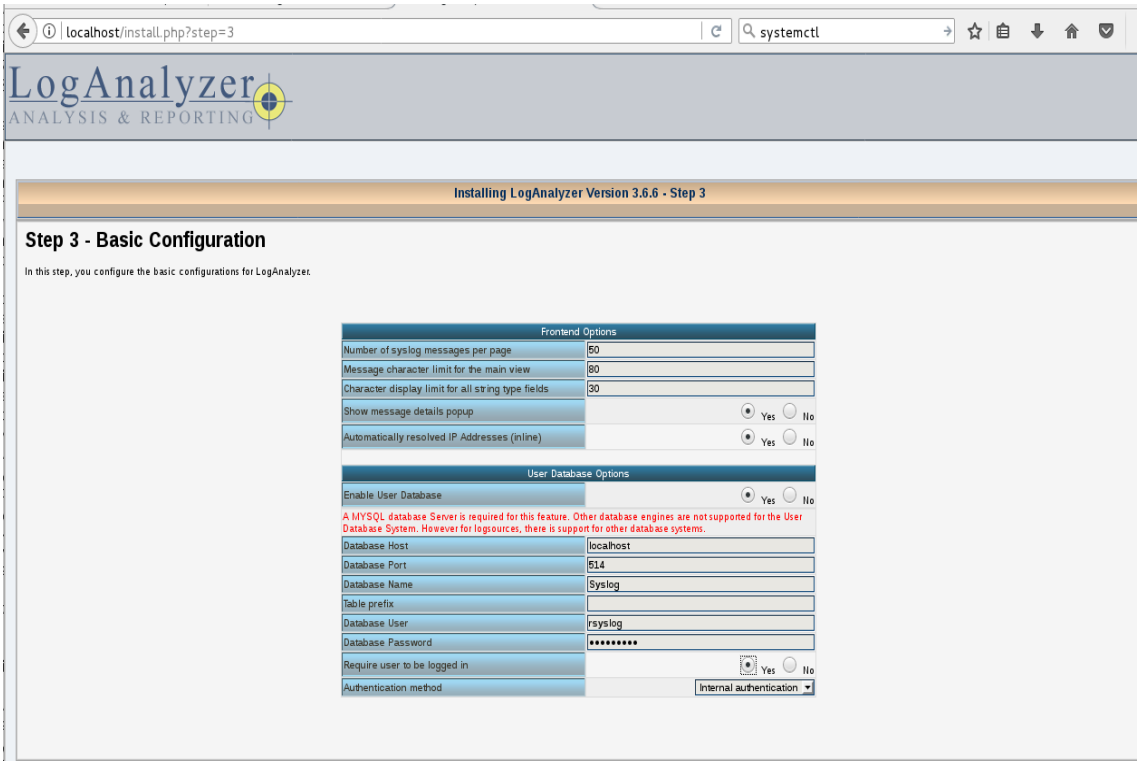

FIGURE 4.10 – l'étape 3 de configuration de LogAnalyzer

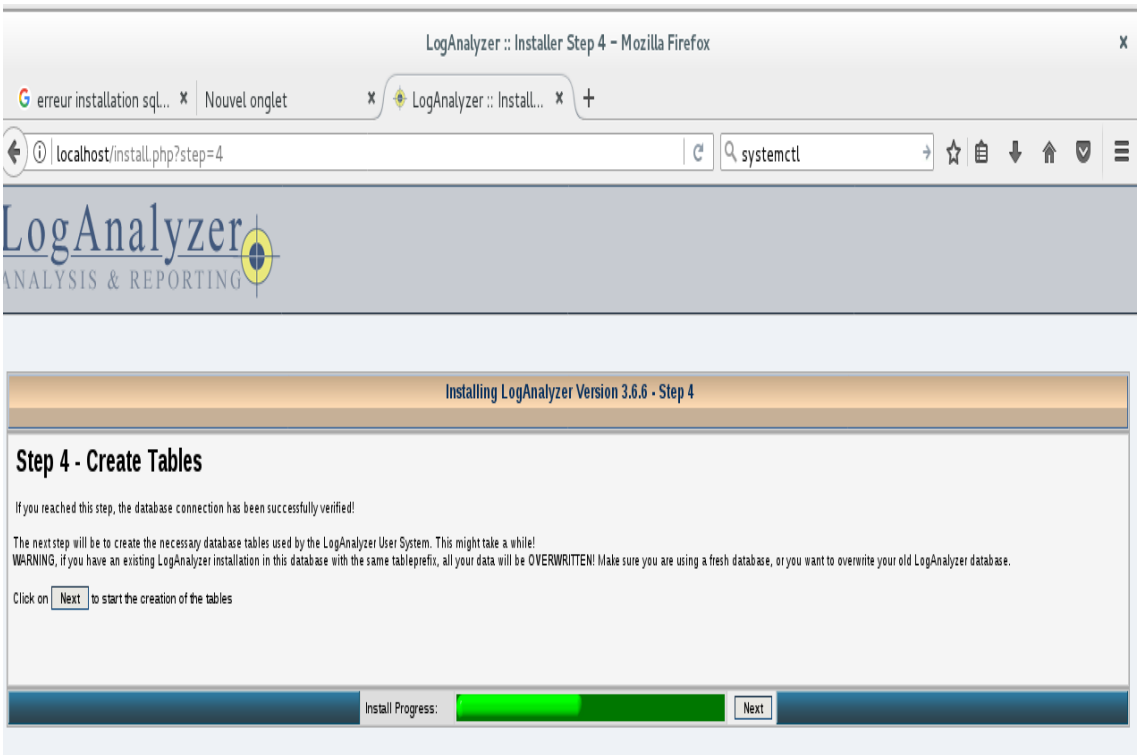

FIGURE 4.11 – Étapes 4 de configuration de logAnalyzer

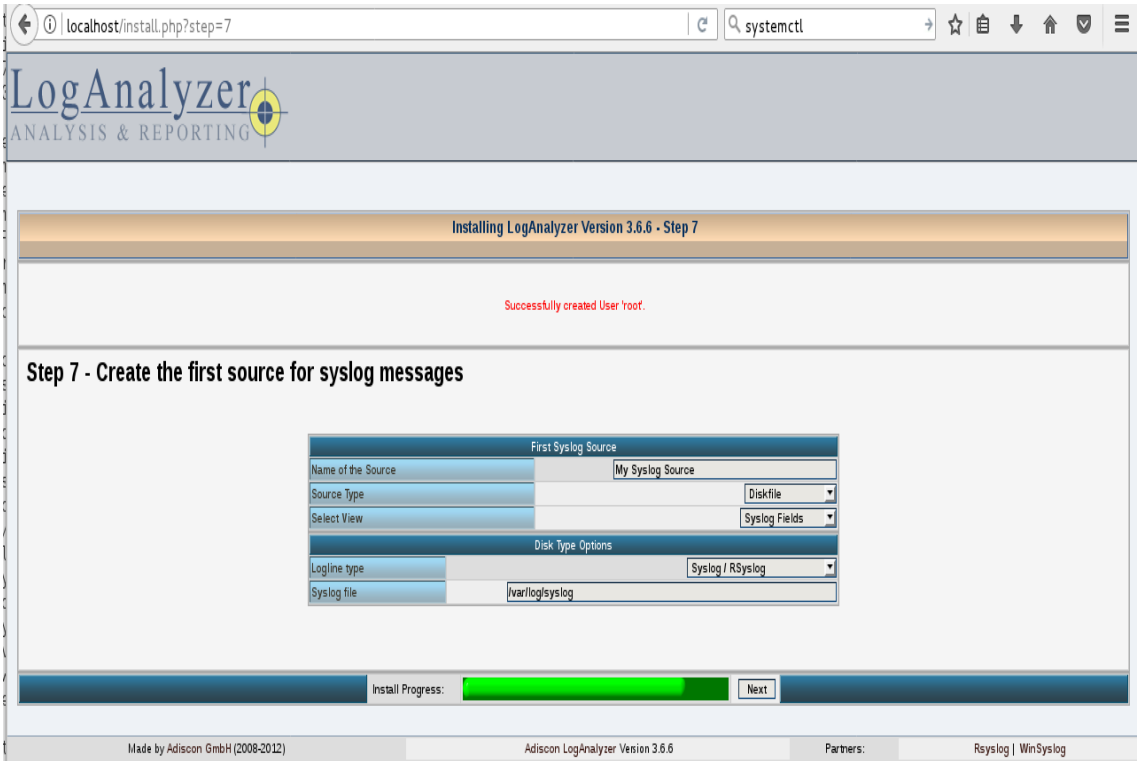

FIGURE 4.12 – l'etape 7 de configuration de LogAnalyzer

4.6.2.2 L'interface LogAnalyzer

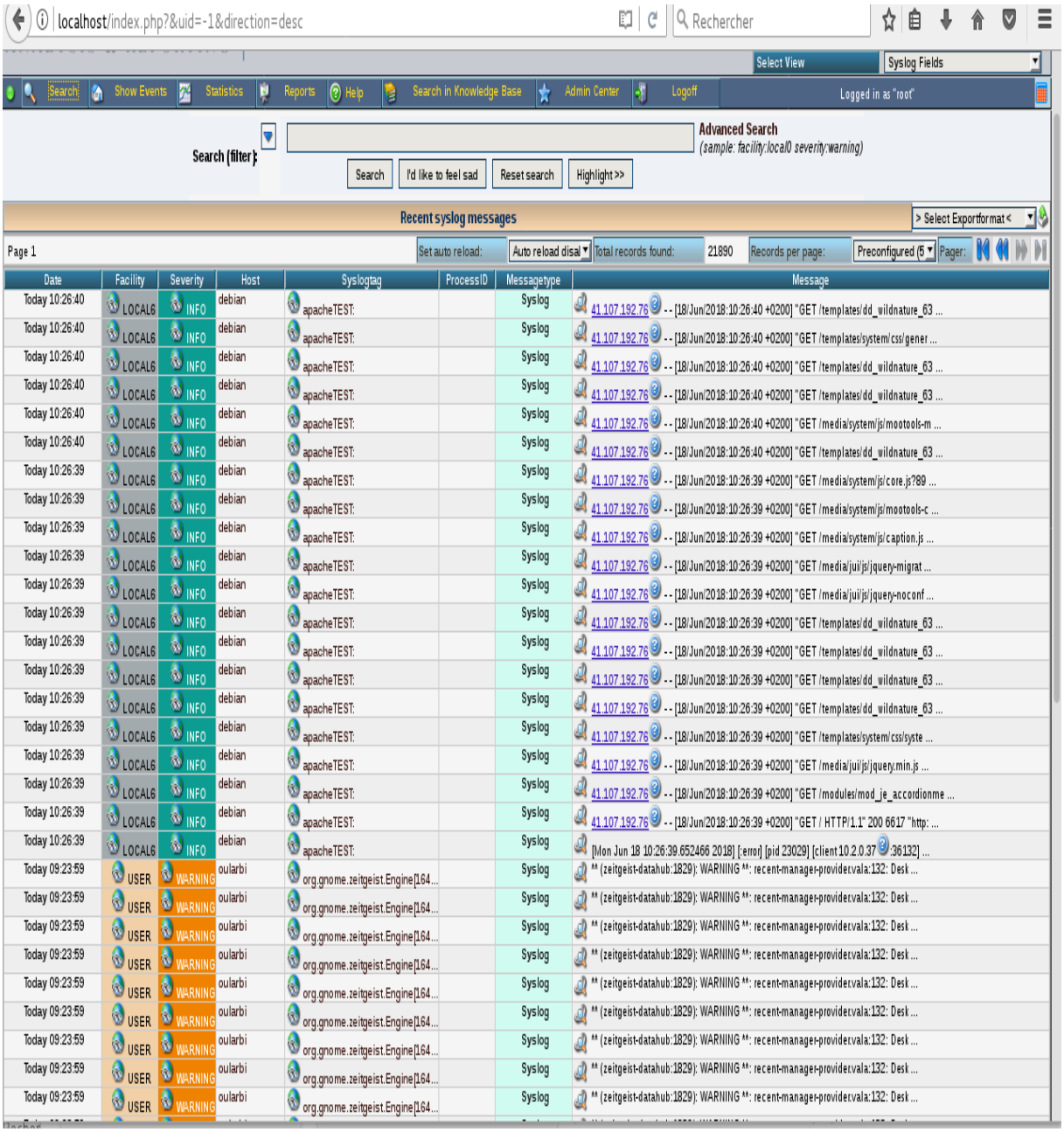

FIGURE 4.13 – L'interface de LogAnalyzer

4.7 Traitement des logs

L'exploitation et le traitement des fichiers logs transférés vers notre serveur de centralisation, nous amènent vers une discipline de l'informatique qui est la sécurité réseau. Tant que la maitrise de ce domaine n'est pas acquise, nos requêtes de traitements peuvent générées des erreurs de diagnostic qui bien sûr se reflètera sur une mauvaise prise de décision par les administrateurs réseaux. Pour éviter ce désagrément nous avons orienté notre travail sur la recherche des attaques connus au niveau de la sécurité réseau, pour ce faire nous avons limité cette exploration aux deux domaines celui des applications web et le matériel Cisco.

Nous allons pouvoir expliquer les attaques les plus répondus. Elles sont donc au nombre de quatre :

— les attaques par force brute

— les injections de code

— le Cross-Site Scripting

— le déni de service.

4.7.1 Le log format d'apache

Afin de bien comprendre ces attaques nous rappelons la nature et le format d'un log apache. En effet remonter une attaque suite au piratage d'un site avec les logs d'Apache, s'assurer que nous avons bien configuré son transfert vers le serveur de centralisation donc nous partirons du principe qu' Apache est déjà configuré pour mettre ses logs dans /var/log/Syslog-central/HostIp/apache2.log.

La documentation d'apache explique très bien comment est formée une ligne typique d'un fichier de log, mais découpons finement la ligne suivante pour voir ce que ça signifie :

93.184.216.34 - - [20/Apr/2015 :21 :54 :21 +0200] "GET /2015/01/25/NSA-bullrun.html HTTP/1.1" 200 8766 "https ://www.libwalk.so/" "Mozilla/5.0 (X11 ; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36" 0

cette dernière correspond au LogFormat suivant :

"%{LOGIN}e %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %T"at .

4.7.2 Interprétation du message log Aapche2

Pour la comprendre plus facilement, on peut imaginer la lire comme un journal de bord dans lequel la personne qui s'en chargerait raconterait tout avec le plus de détails possible. Dans l'exemple ci-dessus, les logs nous racontent que : J'ai eu une requête provenant de l'adresse IP 93.184.216.34 le 20 avril 2014 à 21h54 et 21 secondes (+0200 indiquant la timezone de votre serveur), elle m'a demandé (GET) d'accèder à la ressource /2015/01/25/NSA-bullrun.html en utilisant le protocole HTTP/1.1. J'indique ensuite le statut de cette ressource (200), ainsi que sa taille (ici le nombre d'octets envoyés, y compris les en-têtes) (8766). Elle m'indique venir du site https ://www.libwalk.so (referer) et m'affirme l'avoir fait en utilisant le logiciel Mozilla/5.0 [...] (user-agent). Et j'ai mis 0 seconde à servir cette ressource. Détaillons chaque zone du message : Les logs du serveur Apache sont répartis dans différents fichiers en fonction de leur nature. Nous nous intéresserons ici au journal des accès dont les entrées sont regroupées dans un seul fichier. C'est un fichier de texte brut dans lequel chaque entrée est enregistrée sur une et une seule ligne. Le contenu de chaque ligne est cependant organisé selon une nomenclature configurable par l'utilisateur. Étudier cette nomenclature en amont de l'analyse automatique des logs permet de gagner en efficacité (car les informations sont facilement identifiables) et en temps (car l'analyse se fait alors sur des chaînes plus petites). La configuration de base des logs permet d'accéder immédiatement aux informations suivantes :

— L'adresse IP de l'hôte distant. Attention, dans le cas où un serveur mandataire est présent entre le client originel et le serveur, l'adresse affichée sera celle du serveur mandataire. Pour palier à ça nous utilisons {Foreign for}

— L'identité du client, définit un protocole permettant d'identifier rapidement une machine lors d'une connexion TCP. Ce champ n'est renseigné que si la directive

IdentityCheck est positionnée sur On.

— L'identifiant de la personne qui a demandé le document, dans le cas d'un document protégé par un mot de passe.

— L'heure et la date de la réception de la requête.

— La requête du client. C'est une ligne de texte elle aussi paramétrable.

— Le code statut de la réponse retournée au client. La liste des codes statuts.

— La taille de l'objet retourné au client.

Par défaut, la configuration du serveur Apache employé fournit également deux champs supplémentaires :

— Le « Referer », c'est-à-dire le site depuis lequel le client a lancé sa requête. c'est une information fournie par le client et que celui-ci peut donc modifier à volonté. Il peut également ne pas être renseigné par celui-ci. Par conséquent, il est fortement Déconseillé de ce fier à cette information.

— Le « User-Agent », autrement dit le navigateur utilisé par le client pour envoyer sa requête. Encore une fois, c'est une information que le client peut masquer ou altérer. La version 2.4 du serveur Apache nous permet cependant de modifier les informations enregistrées dans les journaux.

Il est possible d'y inclure du texte fixe afin de séparer plus précisément les paramètres dans le but d'aider lors de la lecture ou l'analyse des logs, ainsi que d'autres informations pouvant s'avérer utiles lors de la recherche d'attaques ou d'anomalies : — Le temps passé par le serveur à effectuer la requête.

— Le nombre de requêtes persistantes (pipelining) en cours pour la connexion http actuelle.

— Le port et le nom canoniques du serveur qui a servi la requête.

— Le chemin de la requête.

Il est également possible de ne cibler que certaines opérations en conditionnant l'enregistrement de certains paramètres à la présence d'autres paramètres. On peut par exemple choisir de n'enregistrer que les logs dans le cas où le serveur créé un document

(statut HTTP 201), ou au contraire de ne jamais enregistrer les créations de document.

Méthode HTTP • GET : demande une ressource (la requête étant normalement sans effet sur celle-ci ressource)

• POST : transmet des données en vue d'un traitement. Le résultat peut être la création de nouvelles ressources (fichiers...) ou la modification de fichiers existants.

• HEAD : demande seulement des informations sur la ressource (sans demander la ressource elle-même)

À noter qu'il existe d'autres méthodes (DELETE, PUT, TRACE...) mais qui apparaissent très, très rarement.

4.7.3 présentation des attaques les plus répondue

4.7.3.1 Attaque par Déni de Service

Une attaque DoS peut prendre plusieurs formes. Le but est néanmoins toujours le même : nuire à la disponibilité du système. Comme son nom l'indique, c'est une attaque qui vise à empêcher le serveur de servir ses clients. Une attaque DoS commune est le SYN flood. C'est une attaque sur la couche 4, la couche transport, utilisant le protocole TCP et cherchant à surcharger les ressources du serveur. Afin d'établir une connexion TCP avec un serveur, un client va lui envoyer un segment SYN. Le serveur va réserver des ressources pour la communication et renvoyer un segment SYN-ACK pour accepter la connexion. Le client répond alors par un segment ACK. Une attaque SYN flood consiste, pour le client, à ne jamais envoyer le segment ACK et à bombarder le serveur de segments SYN. De cette façon, le serveur va réserver des ressources pour chaque segment SYN reçu sans les libérer parce que le segment ACK ne sera jamais reçu. Le serveur peut alors consommer toutes ses ressources (espace mémoire, temps de calcul) et n'être plus capable de répondre à des requètes SYN de clients légitimes voire même de planter tout simplement. Une autre façon de réaliser du déni se service est de surcharger les canaux de communication reliant les clients au serveur. Un serveur

web est capable de fournir plusieurs types de données : des pages HTML, des images, des vidéos, etc... Certaines données sont plus volumineuses que d'autres. Un robot demandant beaucoup de données volumineuses à un serveur le forcera à consommer sa bande passante et pourra réduire l'espace disponible pour le reste des clients. Les clients demandant simultanément beaucoup de ressources peuvent sans nul doute provoquer un ralentissement sur le serveur. Une autre conséquence de cela est, dans un environnement Cloud, de forcer le serveur à utiliser plus de ressources et donc d'augmenter sa facture auprès de son fournisseur de Cloud. Une simulation d'une telle attaque se résume à la recherche d'un contenu multimédia le plus lourd hébergé par le serveur et une fois que celui-ci a été identifié, il va bombarder le serveur de requêtes demandant cette ressource. En effet demander la ressource la plus lourde permet de consommer un maximum de ressources par requête reçue.

4.7.3.2 Attaque par Bruteforce

Une authentification sur un site web est souvent réalisée au moyen d'un nom d'utilisateur et d'un mot de passe. Le nom d'utilisateur est généralement public car il permet aux membres du site de s'authentifier entre eux. Le mot de passe, quant à lui, est privé, connu de son propriétaire uniquement. Il existe plusieurs façons de trouver le mot de passe d'un autre membre et l'attaque par force brute (ou bruteforce) est l'une d'entre elles. Les attaques par force brute possèdent différents niveaux de sophistication, allant du test de toutes les combinaisons possibles d'un ensemble de caractères données à celui de quelques valeurs. La procédure de ce genre d'attaque est assez rudimentaire : l'attaquant essaie de se connecter avec tous les mots de passe de sa liste. Il s'arrête dès que le mot de passe est trouvé. De part le grand nombre de mots de passe à tester, ces attaques sont toujours automatisées. Il existe des contremesures bien connues permettant de se prémunir contre ce type d'attaque comme les célèbres captcha ou bien le verrouillage du module d'identification après plusieurs échecs.

4.7.3.3 Attaque par Injection de code

Les attaques de type injection de code sont les attaques les plus fréquentes sur les serveurs web. Le but de ces attaques est d'envoyer du code à un interpréteur (SQL, Shell, LDAP, etc.), à travers des commandes ou des requêtes, afin d'exécuter des instructions non désirées. Ce type d'attaque est possible lorsque des points d'entrée dans le système n'ont pas été sécurisés par les administrateurs. Il faut toujours vérifier les données fournies par des utilisateurs. Lorsque cela n'est pas fait, les injections de code sont possibles. Dans un site web utilise une base de données SQL et contient un formulaire ayant une vulnérabilité qui sera utilisée afin d'y insérer une instruction SQL dans laquelle nous demanderons de vider le contenu d'une table. Une requète SQL a généralement la forme suivante :

INSERT INTO 'table1 ' (' attribut1 ', 'attribut2 ') VALUES (" valeur1 ",En **" valeur2 ") ;**
changeant valeur2, on peut facilement insérer une deuxième instruction. Nous prendrons donc par exemple pour valeur2 le texte ") **DELETE FROM 'table1'** et nous obtenons :

INSERT INTO 'table1' (' attribut1 ', 'attribut2 ') VALUES (" valeur1 ", "") ; DELETE FROM 'table1 ' ; -- ") ;

L'interpréteur SQL va donc envoyer la première instruction qui génèrera l'insertion d'une nouvelle entrée dans la table relation avec la valeur valeur1 pour l'attribut attribut1 et une valeur vide pour l'attribut attribut2. Ensuite, l'interpréteur exécutera la deuxième instruction qui supprimera toutes les données de la table table1. La partie après les deux tirets – correspond à des commentaires et ne sera pas interprétée. Un mécanisme de protection contre ce genre d'attaque consiste à contrôler la présence de caractères spéciaux et de les traiter correctement afin qu'ils ne puissent pas permettre de générer de nouvelles commandes que l'interpréteur traiterait. Un exemple d'attaque injecter du code sur un Drupal.

En regardant les fichiers modifiés récemment du site, par exemple avec la commande find et son option -mtime(fichier dont les données ont été modifiées il y a n*24 heures).

Après un piratage, on trouve souvent des fichiers avec des lignes en plus (souvent en base64 ou avec des chaînes de caractères étranges) :

```
$YLbgPfj524 = "vh46afl7tm2ik*n3pws.bu;0j)(qo_erzxy51dg9c8/";$oDJXw7301 =
$YLbgPfj524[16].$YLbgPfj524[31].$YLbgPfj524[30].$YLbgPfj524[38].$YLbgPfj524[29].$YLbgPfj524[31
```

4.7.3.4 Cross-Site Scripting

Le Cross-Site Scripting, en abrégé XSS, est une attaque similaire à l'injection de code. Qui cherche à injecter du code sur le site web mais les leviers utilisés sont cependant différents. L'injection de code telle que nous l'avons vu plus haut consiste à envoyer du code au serveur que celui-ci exécutera via un interpréteur. Dans le cas du XSS, c'est au contraire le client qui exécutera le code. La plupart des navigateurs web activent le JavaScript par défaut ce qui en fait un choix populaire parmi les hackers. Néanmoins, n'importe quel langage exécuté chez le client, comme le Flash ou même le HTML5, est un potentiel vecteur d'attaques. Étant exécuté chez le client, le code injecté permet de récupérer des informations le concernant et permet donc le vol de session. XSS sont les troisièmes attaques les plus répandus. La vulnérabilité responsable de l'attaque est généralement la même que pour une injection de code : une entrée non protégée dans un formulaire qui utilise est JavaScript au niveau du client lorsqu'il cherchera à afficher le contenu de ce dernier.

4.8 Présentation des interfaces

Nous exposerons quelques interfaces de notre application, en essayant à chaque fois de décrire les différents objets interactifs mis à la disposition de l'utilisateur.

4.8.1 interface d'authentification

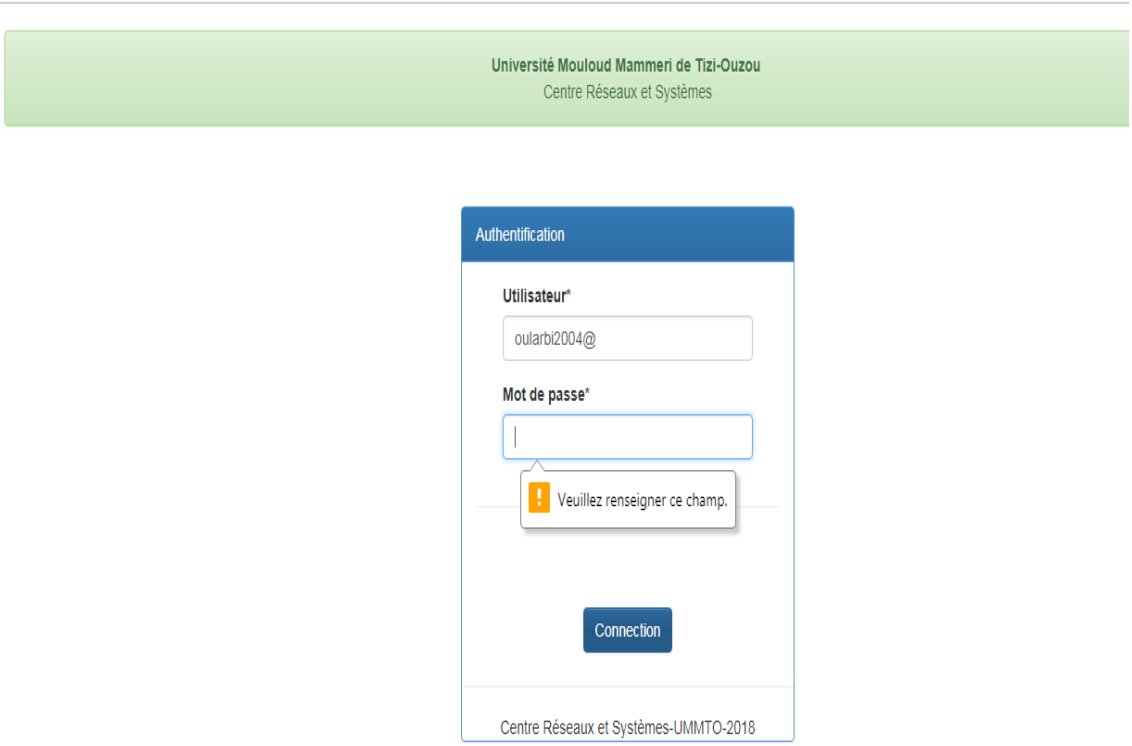

FIGURE 4.14 – interface d'authentification

4.8.2 interface d'inscription

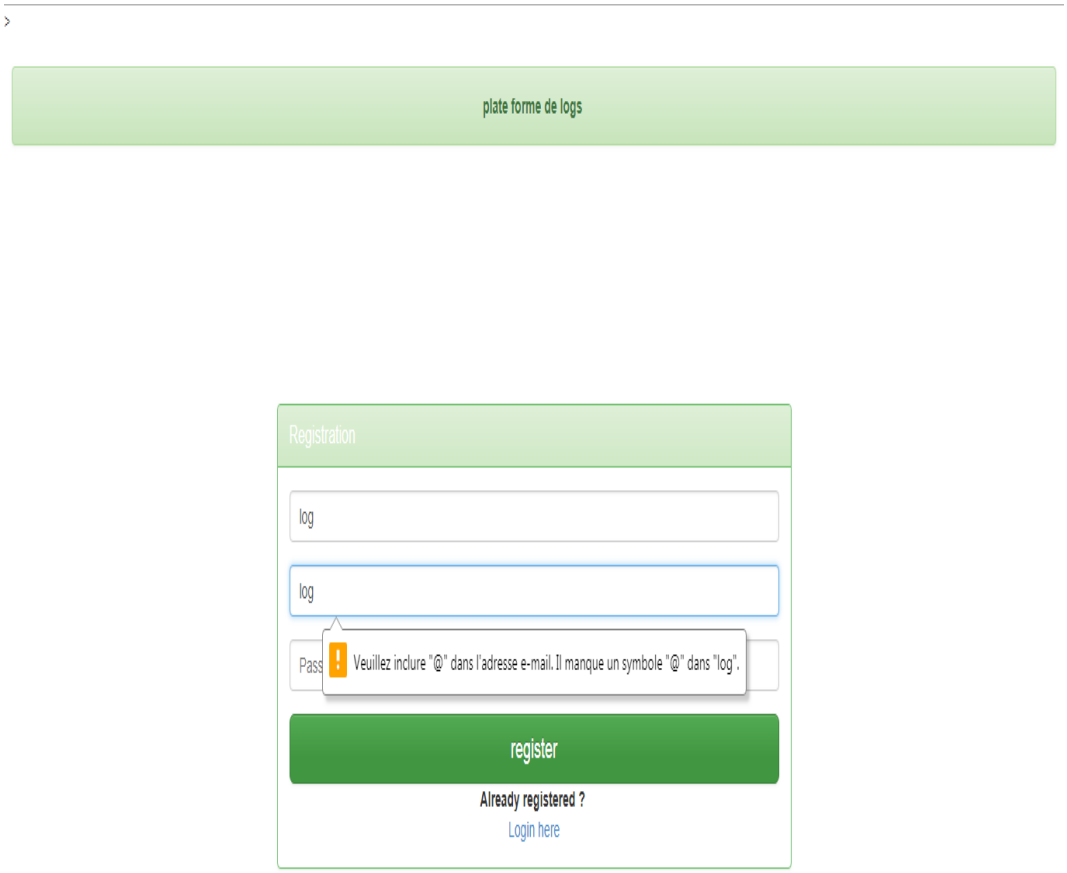

FIGURE 4.15 – interface d'inscription

4.8.3 interface de modification

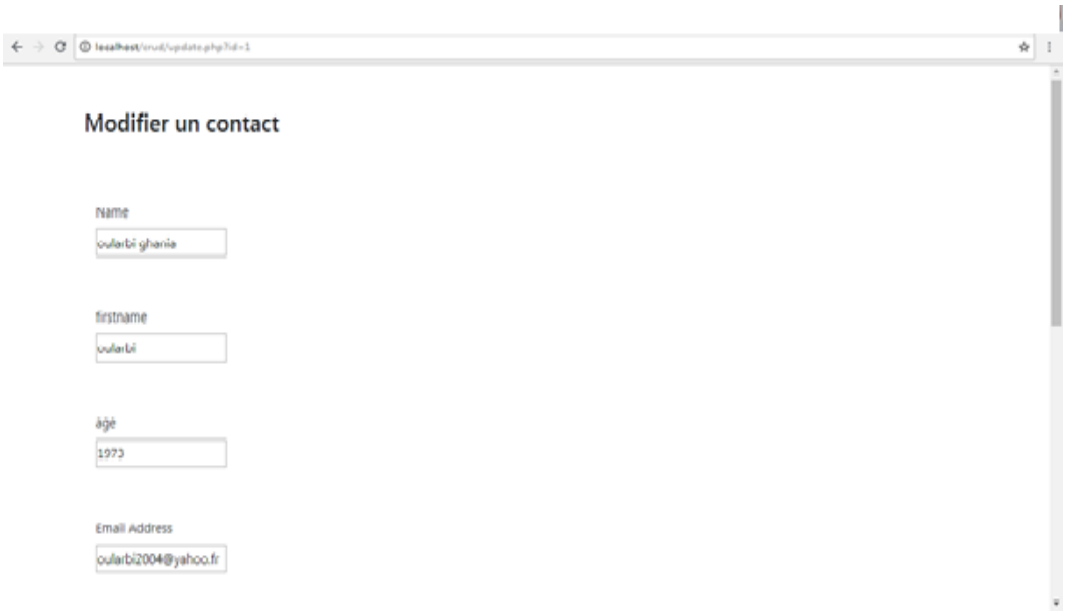

FIGURE 4.16 – interface de modification

4.8.4 interface du traitement des logs

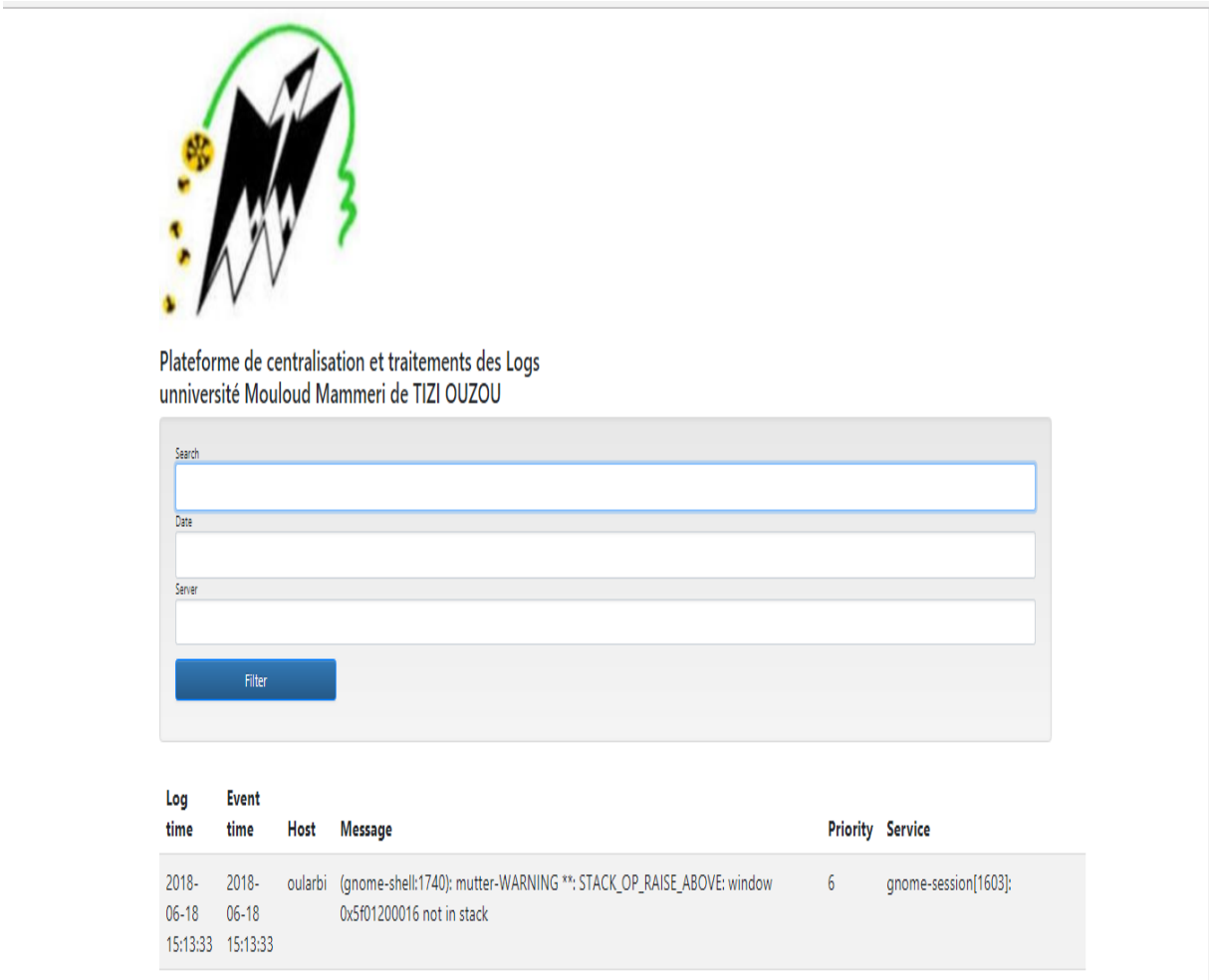

FIGURE 4.17 – interface du traitement des logs

4.9 Conclusion

Nous avons présenté dans ce dernier chapitre, la partie consacrée à la partie Centralisation avec explications de tout le processus de mise en ouvre, nous avons présenté par la suite la phase de transfert des messages Log vers une base de données MySql et l'exploitation de cette dernière par une application web dédié au service réseau avec la présentation de ses différents interfaces fonctionnement de notre système de gestion et d'analyse de fichiers journaux en expliquant le fonctionnement de quelques menus et interfaces.

Conclusion générale

La démarche que nous avons suivi nous a permis d'aboutir à apriori aux principaux objectifs sollicités par le centre des réseaux à savoir le déploiement d'une plateforme de centralisation des logs au niveau d'un serveur dédié sous linux distribution debian 14. avec une stratégie de rotation de logs dont le but et de gérer la capacité du disque dur vu le volume important d'information des logs réseau. de transférer les logs envoyés par les différents équipement dans des répertoires qui seront créés automatiquement et cela grâce au Template que nous avons ajouté au fichier de configuration Rsyslog dont le nom est l'adresse IP de l'hôte. Nous avons ensuite approfondi l'utilisation du protocole syslog qui nous permis de mettre à la disposition du centre réseau une base de données qui est alimenté au temps, pour ce faire une documentation sur les instructions en ligne de commande Linux nous ont permit la réalisation de cette tâche , l'utilisation de plusieurs utilitaires n'a fait qu'enrichir nos connaissances et la manipulation au niveau de l'infrastructure nous a permit de voir et d'avoir en temps réel les résultats de notre travail. La base de données Rsyslog-Mysql est exploité par notre plateforme Web qui permet aux administrateurs réseaux de filtrer visualiser les logs selon des critères mis à leur disposition, cette application se voit extensible et beaucoup de modules qui sont en perspectives viennent se greffer à cette dernière afin de mieux exploiter notre travail et cela en appliquant plusieurs domaine de l'informatique à savoir les Systèmes de détection d'intrusion, la messagerie.

Perspectives

Notre projet se voit ouvert sur plusieurs domaines de l'informatique allant d'une simple supervision ne serait ce que visuelle de l'état de l'infrastructure réseau d'une structure vers :

— une supervision à temps réel de toute l'infrastructure réseau complété par un module de messagerie qui permettra de générer des messages par SMS et e-mail aux administrateurs réseaux avec des profils ciblés selon la nature de l'alerte.

— Traitement des différents logs en se basant sur la maitrise de la sécurité informatique afin de générer des rapports crédibles qui répondent aux normes universelles de la sécurité

— Déployer l'application sous forme d'un web service pour des raisons : d'interopérabilité, afin d'accompagner toute application Web pour un audit d'audience.

— transposer des techniques de détection d'anomalies au sein d'un programme dans un contexte de sécurité afin de reconnaitre des attaques informatiques.