



RÉPUBLIQUE DU BÉNIN  
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR  
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE  
RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88  
<http://www.ifri-uac.net> Courriel : [contact@ifri.uac.bj](mailto:contact@ifri.uac.bj)



# MÉMOIRE

pour l'obtention du

**Diplôme de Licence en Sécurité Informatique**

Présenté par :

Armél Léonce OGOUNCHI

Thème:

**Centralisation et gestion des informations  
et événements de sécurité au Port  
Autonome de Cotonou**

Sous la supervision de :

M. Koudouss LANIGNAN

Ingénieur en Systèmes, Réseaux et Télécoms

Année Académique : 2016-2017

# Dédicace

À mon père, ma mère et tous mes proches.

# Remerciements

À Monsieur Koudouss LANIGNAN, le directeur de mémoire, pour les longs échanges, son soutien indéfectible malgré son agenda très chargé et son implication dans tous les aspects du travail.

À Monsieur Serge MONNOU, notre tuteur de stage, et Monsieur Lino de SOUZA pour toutes les informations utiles apportées, les conseils, leur suivi et leur intérêt porté sur le travail réalisé.

À tous les membres de l'équipe en charge de la sécurité du parc informatique du Port Autonome de Cotonou pour la qualité de leur travail et leur bonne humeur en toute épreuve.

# Sommaire

<b>Dédicace</b>	<b>i</b>
<b>Remerciements</b>	<b>ii</b>
<b>Liste des figures</b>	<b>v</b>
<b>Liste des tableaux</b>	<b>vi</b>
<b>Glossaire</b>	<b>vii</b>
<b>Sigles et Abréviations</b>	<b>viii</b>
<b>Résumé</b>	<b>ix</b>
<b>Abstract</b>	<b>x</b>
<b>Introduction Générale</b>	<b>1</b>
<b>1 Contexte d'étude</b>	<b>3</b>
1.1 Les concepts clés sur les informations et événements de sécurité . . . . .	3
1.2 Les caractéristiques des solutions de centralisation et gestion des logs . . . . .	7
1.3 Le principe de la centralisation et gestion des événements de sécurité . . . . .	8
<b>2 Approches de solution</b>	<b>11</b>
2.1 Quelques solutions existantes . . . . .	11
2.2 Le choix de la solution . . . . .	16
2.3 Exploitation et exploration des informations issues des logs . . . . .	21
2.4 Gestion des utilisateurs . . . . .	21
<b>3 Mise en place de la solution</b>	<b>24</b>
3.1 Les prérequis à la mise en place de Nagios Log Server . . . . .	24
3.2 Le déploiement de Nagios Log Server . . . . .	25
3.3 La Simulation . . . . .	26
<b>Conclusion Générale</b>	<b>32</b>
<b>Bibliographie</b>	<b>33</b>
<b>Table des matières</b>	<b>35</b>
<b>A Le choix des événements</b>	<b>xi</b>

<b>B</b>	<b>L'installation et le paramétrage de Nagios Log Server</b>	<b>xvi</b>
B.1	Le processus d'installation . . . . .	xvi
B.2	Le paramétrage de Nagios Log Server . . . . .	xix

# Table des figures

1.1	Vue détaillée d'un événement consigné dans un fichier log . . . . .	4
1.2	Vue détaillée d'un événement applicatif consigné par Windows Event Log . . . . .	6
2.1	Architecture de fonctionnement de Logstash intégré à Nagios Log Server . . . . .	17
2.2	Exemple de filtre Syslog . . . . .	17
2.3	Représentation des champs après filtrage . . . . .	18
2.4	Fonctionnement interne de Nagios Log Server . . . . .	19
2.5	Extrait d'une interface de visualisation d'événements indexés . . . . .	20
2.6	Interface permettant l'exploration d'événements indexés . . . . .	21
2.7	Interface d'ajout d'utilisateur de Nagios Log Server . . . . .	22
2.8	Interface d'attribution de droits des utilisateurs de Nagios Log Server . . . . .	23
3.1	Architecture de mise en place . . . . .	25
3.2	Création d'une règle de filtrage . . . . .	26
3.3	Interface de personnalisation du contenu des notifications par email . . . . .	27
3.4	Configuration d'une alerte sous Nagios Log Server à recevoir par mail . . . . .	28
3.5	Interface de configuration des paramètres SMTP . . . . .	29
3.6	Extrait de l'interface de Visualisation . . . . .	30
3.7	Extrait de la notification reçue par mail . . . . .	30
A.1	Événement consigné par Windows Eventlog . . . . .	xiv
A.2	Résultat de l'analyse faite par Nagios Log Server . . . . .	xv
B.1	Importation de la machine virtuelle de Nagios Log Server . . . . .	xvii
B.2	Finalisation de l'installation de Nagios Log Server . . . . .	xviii
B.3	Ajout d'une instance de Nagios Log Server . . . . .	xix
B.4	Extrait de la configuration de NXlog sous Windows . . . . .	xx
B.5	Configuration effectuée sur une machine linux . . . . .	xxi
B.6	Configuration effectuée sur une machine linux . . . . .	xxi

# Liste des tableaux

1.1	Comparaison entre les outils de gestion des événements de sécurité et des logs .	10
2.1	Analyse comparative des différents outils gratuits évoqués . . . . .	14
3.1	Configuration de l'alerte en théorie . . . . .	28
A.1	Comparaison entre les outils de gestion des événements de sécurité et des logs .	xi

# Glossaire

**Log** : Il s'agit d'une documentation produite automatiquement et horodatée des événements pertinents pour un système donné. Pratiquement toutes les applications et systèmes logiciels produisent des fichiers journaux.

**Elasticsearch** : Composant open source du Stack ELK permettant la sauvegarde des données (logs) centralisés.

**Cluster** : C'est le terme utilisé pour désigner toutes les instances travaillant ensemble à la fois.

**Instance** : Une instance représente une composante d'un cluster.

**Index** : Un index est représenté, dans notre cas, comme une base de données relationnelle.

**Tesson**<sup>1</sup> : Un tesson ou encore un éclat est un outil qui est géré par Elasticsearch.

**Centralisation des logs** : Cela consiste à mettre sur un même système, une même plateforme, l'ensemble des logs des systèmes, applications et services des machines environnantes.

**Actif informationnel** : Inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une entreprise ou d'une organisation, à l'exception des ressources humaines.

**Attaque par rebond** : Les attaques par rebond constituent une famille d'attaques de système d'information qui consistent à utiliser un ou des systèmes intermédiaires, participant à leur insu, et permettant à un assaillant de rester caché.

**RSyslog** : C'est le système de gestion et de traitement des logs (sous linux).

**Parc Informatique** : Ensemble du matériel informatique utilisé au sein d'une organisation.

**Supervision** : La supervision est la fonction qui permet de remonter/éditer les informations techniques relatives à un hôte ou à un ou des un équipement du réseau.

**Serveur de monitoring** : Le serveur de supervision (ou de monitoring) est le serveur qui permet d'avoir une vue centralisée des informations techniques relatives à un hôte ou un ou des un équipement du réseau qui lui sont parvenues.

**Active Directory**<sup>[1]</sup> : Nom du service d'annuaire de Microsoft, et est basé sur les standards TCP/IP : DNS, LDAP, etc.



# Sigles et Abréviations

**PAC** : Port Autonome de Cotonou

**IIS** : Internet Information Services

**SIEM** : Security Information and Events Management

**TCP** : Transmission-Control Protocol

**SaaS**<sup>[4]</sup> : Software as a Service

**SNMP** : Simple Network Management Protocol, un protocole de gestion ou d'administration des réseaux informatique

**IPS/IDS** : Intrusion Detection System / Intrusion Prevention System représentent respectivement un système de détection ou de prévention d'intrusions

**SOC**<sup>[3]</sup> : Security Operations Center

**NDRP** : Nagios Remote Data Processor

**IMAP** : Interactive Mail Access Protocol

**UDP** : User Datagram Protocol

**VPN** : Virtual Private Network

**LDAP**<sup>[2]</sup> : Lightweight Directory Access Protocol

**DNS** : Domain Name System

**OS** : Operating System

**SSL** : Secure VPN Sockets Layer

**PCI** : Payment Card Industry

**JSON** : JavaScript Object Notation

# Résumé

Les journaux d'événements liés aux parcs informatique sont l'une des ressources indispensables pour la gestion de la sécurité des systèmes d'information d'entreprise. Ils sont exploités pour l'analyse d'une activité, la détection d'une anomalie ou encore pour déclencher des alertes. Le but étant la détection des incidents de sécurité<sup>2</sup>, d'une part, et retrouver, d'autre part, les traces d'un incident afin d'évaluer l'impact de celui-ci sur les actifs informationnels de l'entreprise.

Le nombre important des logs liés à la forte utilisation des services informatique en phase avec les activités de l'entreprise demande alors une attention particulière afin d'en tirer le maximum d'informations utiles pour la validation des événements graves enregistrés sur le parc informatique en vue d'une réponse fiable. Les administrateurs du système d'information sont contraints à collecter, sauvegarder et analyser ces journaux afin de mieux maîtriser le parc informatique. Il existe, en effet, plusieurs normes, recommandations et bonnes pratiques[2] qui reviennent sur ces conditions de conformité.

Afin de répondre efficacement à ces normes de qualité, il existe de solutions simples embarqués par différents constructeurs de logiciels ou de systèmes d'exploitation (le rSyslog de Linux en passant par le service de journalisation de CISCO et l'Observateur d'événements de Windows).

Il se pose dès cet instant un problème de compatibilité ou d'intégration des logs de toutes les composantes.

Cette insuffisance notoire a suscité la proposition d'un outil de centralisation et de gestion du volume de données produites par toutes les composantes du parc informatique. Cet outil, bien configuré, permettra d'assurer, d'une part, la traçabilité de toutes les activités sur le système informatique et d'autre part, l'intégrité des journaux ainsi que des configurations faites.

Il est proposé dans ce document une approche de solution en vue de participer à la sécurité du système d'information dans un processus de défense en profondeur au Port Autonome de Cotonou (PAC).

---

<sup>2</sup>Voir l'annexe A.

# Abstract

Computer park event logs are one of the most important resources in the world of computer park management.

They are used for analyzing an activity, detecting an anomaly or triggering alerts. The aim is to detect security incidents<sup>3</sup> on the one hand, and track down the traces of an incident in order to assess its impact on the company's information assets.

The large number of logs linked to the high use of IT services in line with the company's activities requires special attention in order to obtain the maximum useful information for the validation of serious events recorded on the IT equipment in order to obtain a reliable response. Administrators of the information system are forced to collect, save and analyze these logs in order to better control the computer park. There are, in fact, several standards, recommendations and good practices[2] that go back on these conformity conditions.

In order to efficiently meet these quality standards, there are simple embedded solutions by different software or operating system manufacturers (the Linux rSyslog, the CISCO logging service and the Windows Event Observer).

From this moment on, there is a problem of compatibility or integration of the logs of all components.

This notorious inadequacy has prompted the proposal for a tool to centralize and manage the volume of data produced by all components of the computer park. This tool, which is well configured, will ensure traceability of all activities on the computer system and the integrity of the logs as well as the configurations made.

This document proposes a solution in order to participate in the security of the information system in an defence-in-depth process at Port Autonome de Cotonou (PAC).

---

<sup>3</sup>See appendix A.

# Introduction Générale

## Généralité

La mise en place d'un outil de centralisation et de gestion des logs permet d'avoir sur un même système, une même plate-forme, l'ensemble des logs des systèmes, applications et services des machines environnantes. Ces journaux d'événements permettent, d'une part la détection des incidents de sécurité. Dans ce cas, ces journaux sont consultés et analysés en temps réel. Ils permettent également de retrouver les traces d'un incident de sécurité ; l'analyse des journaux d'un ensemble de composants (postes de travail, équipements réseaux, serveurs, etc.) permet alors de comprendre le cheminement d'une attaque et d'évaluer son impact. L'activité de journalisation est un moyen de détection et d'analyse par complémentarité au système de gestion de la sécurité du système d'information. La mise en valeur des journaux d'événements dépend de leur génération et de leur collecte. L'architecture du système de journalisation suit donc l'évolution du système d'information (prise en compte des nouveaux équipements, des nouveaux usages, etc.).

## Problématique

Durant le stage effectué à la Direction des Systèmes d'Information du Port Autonome de Cotonou, il a été remarqué que malgré tous les dispositifs de gestion de la sécurité existant sur le parc informatique (pare-feu, serveur de monitoring, logiciel de gestion de la bande passante, etc.), les questions suivantes restent sans réponses :

- Qui a exécuté une tâche sur le parc informatique ? (L'identité ou l'identifiant de l'auteur et/ou de la source de l'exécution)
- Quelle était la nature de la tâche ? (Exécution d'un programme, modification d'un fichier, redémarrage d'un service, etc.)
- Quand l'a-t-il exécuté ?
- Comment l'a-t-il exécuté ? (Quelle était méthode de travail ?)
- Était-il autorisé à exécuter cette tâche ? (Quelle était la réaction du service de gestion des droits ?)

## Objectif

Il s'agira donc de résoudre les préoccupations sus énoncées en mettant en place un système de **Centralisation et de gestion des informations et événements de sécurité au Port Autonome de Cotonou** afin de permettre aux administrateurs concernés d'avoir une maîtrise complète du parc informatique. Les objectifs de ce travail seront :

- la mise en place d'un outil libre de centralisation et de gestion des logs prenant en compte toutes les composantes du parc informatique ;
- la sauvegarde des logs collectés ;
- l'analyse des différents journaux sauvegardés ;
- la configuration des alertes sms et email suivants les règles définis.

## Plan de travail

Ce document est de ce fait structuré en trois (03) chapitres. Ainsi, le premier présente les caractéristiques de la technologie de la centralisation et gestion des logs d'une part et des événements de sécurité d'autre part. Ensuite, la solution mise en place en tenant compte des recommandations et bonnes pratiques, du contexte local ainsi que des contraintes techniques sera présentée après avoir illustré quelques approches de solutions faites sur la base des directives *opensource* et *sous licences*. Enfin, il sera présenté une simulation de scénarios avec la solution mise en place après avoir présenté les différents prérequis à son installation et le processus d'installation et de paramétrage.

# Contexte d'étude

## Introduction

---

En raison du nombre croissant des activités d'entreprise sur les serveurs, postes de travail et d'autres dispositifs informatiques en réseau et du nombre toujours croissant de menaces contre les réseaux et les systèmes, il plus que nécessaire de se baser sur des technologies de gestion et de centralisation des informations et événements de sécurité afin d'assurer une réponse fiable. Ce chapitre lève toutes les ambiguïtés sur ces technologies[3].

## 1.1 Les concepts clés sur les informations et événements de sécurité

---

### 1.1.1 Les fichiers log

Les journaux contiennent une grande variété d'informations sur les événements qui se produisent dans les systèmes et les réseaux. Ces journaux sont consignés basiquement dans des fichiers log[5].

En effet, le fichier log est l'historique des événements (de sécurité ou non) et contiennent ainsi des fichiers textes simples ou autres formats. Ces fichiers comportent toutes les informations des processus qui ont été définis comme étant pertinents par les administrateurs du système de journalisation sur la base des actifs informationnels identifiés par les décideurs et propriétaires des données.

Les fichiers log sont générés automatiquement en fonction de la programmation initiale. En général, une ligne dans un fichier log contient des informations suivant le canevas ci-après :

**L'enregistrement d'un événement** : L'exemple du lancement d'un programme ;

**L'horodatage** : Ce qui associe une date et une heure à un événement.

En effet, les *informations* représentent les événements normaux permettant de mieux appréhender le fonctionnement normal du parc informatique. Il s'agit principalement des journaux consignés par les composants tels que les systèmes d'exploitation et applications, Les *événements de sécurité* sont les événements anormaux ou critiques (par exemple l'échec d'une connexion utilisateur, la saturation de la mémoire ou encore la tentative de d'accès à distance à une ressource, etc.).

## 1.1.2 Les journaux de systèmes d'exploitation

Il s'agit des journaux standards associés à différents types de processus. Par exemple le système d'exploitation Windows (client et serveur) enregistre les informations des événements normaux de l'application, du système, de l'installation ou de la sécurité. Les administrateurs peuvent ainsi avoir un aperçu dans le fichier log correspondant à l'information, ce qui est utile pour corriger un problème. (Voir figure 1.1)

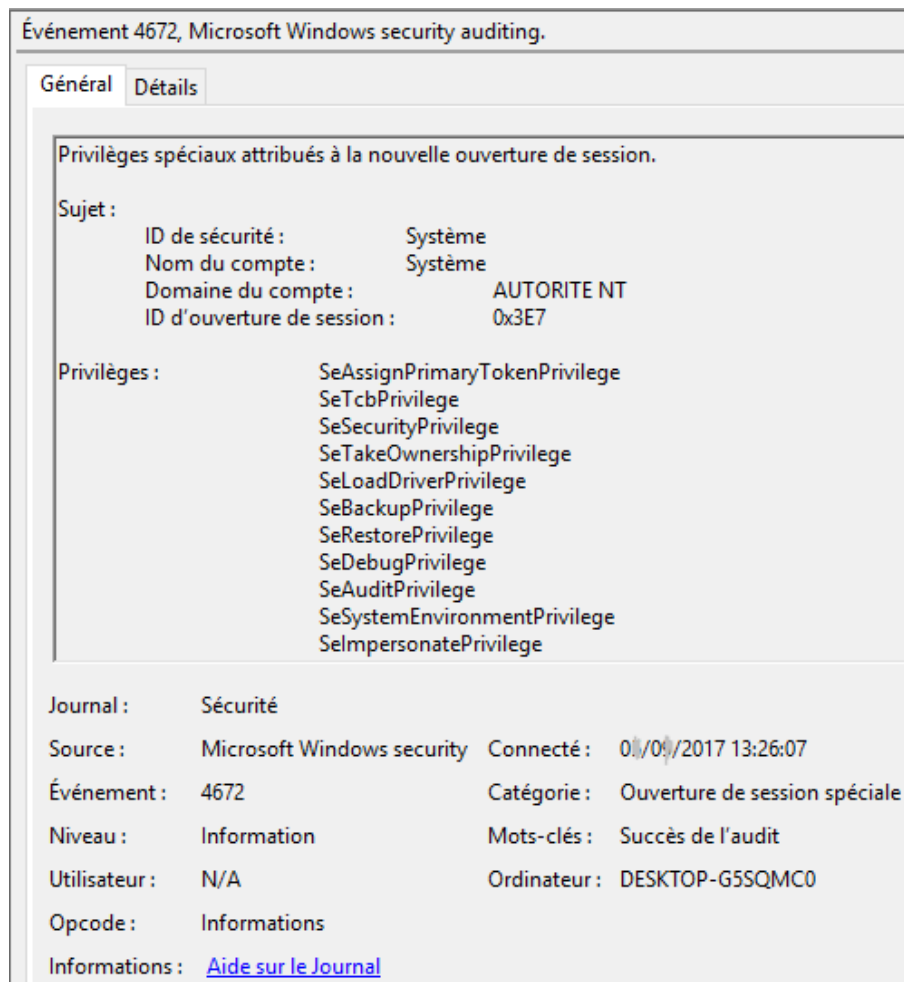


FIGURE 1.1 – Vue détaillée d'un événement consigné dans un fichier log

Clairement, les types de données les plus courantes liées au système d'exploitation sont les suivants :

- **Les événements du système** : Ce sont des actions opérationnelles réalisées par des composants OS, tels que l'arrêt du système ou le démarrage d'un service.
- **Les enregistrements d'audit** : Ils contiennent des informations sur les événements de sécurité telles que la réussite et l'échec des tentatives d'authentification, les accès aux fichiers, les modifications apportées au compte (par exemple, la création, suppression et attribution de privilège de compte) et l'utilisation de privilèges.

### 1.1.3 Les journaux de quelques logiciels de sécurité

Il s'agit principalement des journaux consignés par les logiciels tels que :

- **Les Systèmes de détection et de prévention d'intrusion** : Ils enregistrent des informations détaillées sur les comportements suspects et les attaques détectées, ainsi que tous les systèmes de prévention des intrusions mis en place pour arrêter les activités malveillantes en cours. Certains systèmes de détection d'intrusion, tels que le logiciel de vérification de l'intégrité des fichiers, fonctionnent périodiquement et génèrent un vaste éventail de journal.
- **Les logiciels d'accès à distance aux ressources** : Ils regroupent les accès via VPN et enregistrent généralement des tentatives de connexion réussies et échouées, ainsi que les dates et les heures de connexion de chaque utilisateur, la quantité de données envoyées et reçu par chaque utilisateur. Aussi, le SSL peut enregistrer des informations détaillées sur l'utilisation des ressources.
- **Les Proxy web** : Ils font des demandes de pages Web au nom des utilisateurs et gardent en mémoire des copies des contenus Web récupérés pour rendre plus efficaces les accès supplémentaires à ces pages. Les proxy Web peuvent également être utilisées pour restreindre l'accès Web et ajouter une couche de protection entre les clients Web et les serveurs Web.
- **Les Logiciels de gestion des vulnérabilités** : Ils enregistrent des données supplémentaires et des informations sur les configurations des hôtes. Le logiciel de gestion de la vulnérabilité fonctionne généralement occasionnellement, pas en continu, et est susceptible de générer de gros lots d'entrées de journal.
- **Les Serveurs d'authentification** : Étant composés de serveurs d'annuaire et de connexion unique, ils permettent l'enregistrement de chaque tentative d'authentification, l'origine, le nom d'utilisateur, la réponse du serveur (Succès ou Échec) ainsi que la date et l'heure de la tentative d'authentification.
- **Les équipements réseaux** : Il s'agit de routeurs, commutateurs, points d'accès. Selon leurs configuration, ils peuvent autoriser ou bloquer certaines transactions sur le réseau en fonction de la politique de sécurité mise en place. Les routeurs qui bloquent le trafic, par exemple, sont généralement configurés dans ces cas pour notifier les tentatives de transactions bloquées.
- **Pare-feu** : Comme les routeurs, les pare-feu permettent ou bloquent les activités en fonction de la politique de sécurité mise en place ; cependant, les pare-feu utilisent des méthodes beaucoup plus



sophistiquées pour examiner le trafic réseau. Les pare-feu eux aussi notifient via leur fonctionnalité de journalisation les tentatives bloquées ou autorisées selon les règles définies.

- **Les logiciels antivirus** : Ils enregistrent entre autres le résultat des scans de logiciels malveillants qui ont été effectués, les mises à jour de signature virale ou de logiciel antivirus qui se sont produites. Les Antispyware qui permettent également la détection de rootkit<sup>1</sup> sont également de sources fiables d'informations de sécurité.

### 1.1.4 Les journaux d'applications

Certaines applications intègrent des fonctionnalités de journalisation. Elles génèrent donc leurs propres fichiers journaux, tandis que d'autres utilisent les fonctions de journalisation du système d'exploitation sur lequel elles sont installées. Les applications varient considérablement selon les types d'informations qu'elles consignent.

La figure 1.2 présente le contenu d'un événement dont l'application *Netlimiter* est l'auteur qui est consigné par Windows Eventlog.

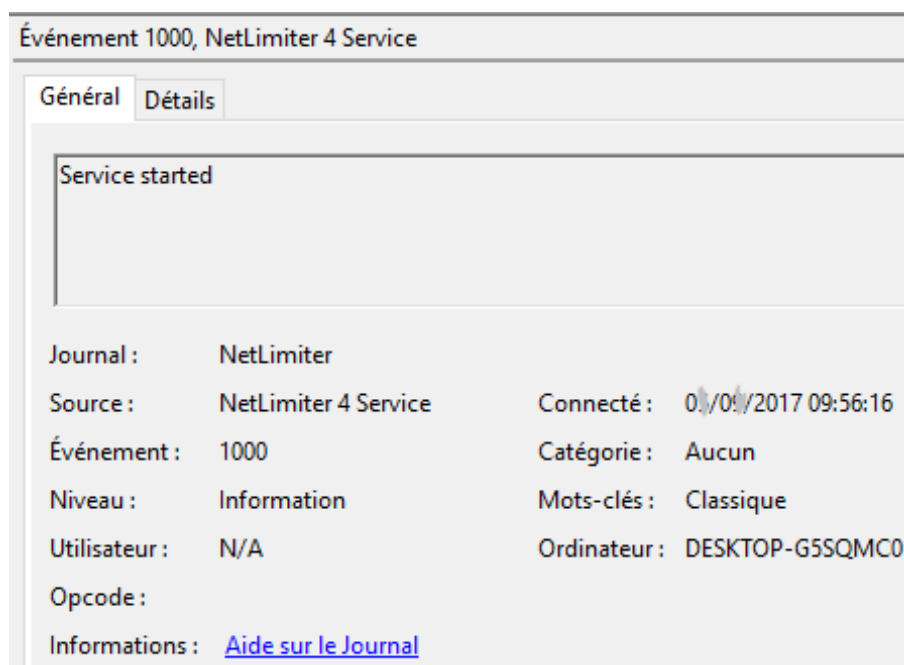


FIGURE 1.2 – Vue détaillée d'un événement applicatif consigné par Windows Event Log

Il est bien visible que NetLimiter se base sur la fonctionnalité de journalisation de Windows.

<sup>1</sup>Le constructeur de logiciel antivirus Avast (<https://www.avast.com/fr-fr/c-rootkit>) définit un rootkit comme un programme conçu pour fournir aux pirates informatiques un accès avec les droits d'administrateur aux ordinateurs à l'insu des utilisateurs.

### 1.1.5 Les cas d'utilisation des fichiers logs

Les fichiers logs sont utilisés pour quatre raisons principales :

- Explication d'une erreur ou un comportement anormal ou encore un dysfonctionnement d'un service (l'exemple d'un service web);
- Traçabilité du parcours numérique d'un utilisateur, d'une application, d'un paquet sur un réseau, des travaux d'un proxy et des éléments réseau par exemple;
- Compréhension du fonctionnement d'une application, d'un protocole, d'un système comme les étapes de démarrage d'un service telnet;
- Notification d'un comportement, d'une action, d'une modification tel qu'une extinction ou un redémarrage du système ou encore une saturation de la mémoire de stockage des informations.

## 1.2 Les caractéristiques des solutions de centralisation et gestion des logs

---

La plupart des administrateurs cherchent à disposer de la majorité des fonctions ci-dessous lorsqu'ils choisissent une solution basée sur le principe simple de centralisation et gestion des logs.

### 1.2.1 La collecte des données de consignation

Cette fonction permet de recueillir toutes les données de consignation<sup>2</sup> disponibles à l'aide de méthodes basées ou non sur un agent collecteur, voire d'une combinaison des deux.

### 1.2.2 La conservation rationnelle

Cette fonction est essentielle aux systèmes de gestion des logs étant donné le nombre de réglementations incluant des conditions spécifiques exigeant la conservation des données de consignation, très souvent pendant plusieurs années tout en fournissant des fonctions de recherche et d'accès rapides.

### 1.2.3 La recherche

C'est le principal moyen d'accéder aux informations contenues dans l'ensemble des fichiers logs, y compris celles issues des applications personnalisées<sup>3</sup> En outre, elle est indispensable pour utiliser les logs à

---

<sup>2</sup>Logs générés par les différents composants du système d'information destinées à l'analyse

<sup>3</sup>Applications professionnelles développées en vue de répondre à une exigence précise d'un métier (l'exemple des prises en charge à l'infirmerie, etc.)

des fins d'enquête, mener des analyses d'expert et identifier les défaillances tout en dépannant les applications à l'aide des logs. Par conséquent, il est essentiel que les systèmes de gestion des logs comprennent une interface de recherche interactive, réactive et disposant d'une bonne ergonomie.

Ce processus de recherche concerne tous les logs collectés disponibles dans leur format brut d'origine, tout comme Google passe en revue les pages Web.

### 1.2.4 L'indexation et l'analyse des logs

La technologie d'indexation crée une structure de données appelée un index. Ce dernier permet d'effectuer des recherches très rapides à l'aide de mots-clés ou d'opérateurs logiques sur l'ensemble du système de stockage des logs.

### 1.2.5 La création de rapports standards et planifiés

Ces fonctions concernent toutes les données recueillies par la solution de gestion des logs. Elles sont similaires aux fonctions de création de rapports comprise dans les outils SIEM. Les rapports sont créés dans les brefs délais, personnalisables et faciles à utiliser à diverses fins.

Contrairement au processus de recherche, les rapports standards se fondent sur les logs analysés au sein d'une base de données.

## 1.3 Le principe de la centralisation et gestion des événements de sécurité

---

Selon une étude statistique menée par Ernst & Young<sup>4</sup> en 2010[1], le principe de la centralisation et de gestion des événements de sécurité est la technologie la plus implémentée dans les entreprises pour prévenir ou détecter une attaque et réagir à cette attaque. Cette discipline est l'apanage de solutions que l'on baptise régulièrement SIM (Security Information Management) ou SIEM (Security Information and Event Management).

En effet, il s'agit de gérer uniquement les événements ayant trait à la sécurité du parc informatique en cinq points.

### 1.3.1 La collecte des données de contexte et des logs

Cette fonction consiste à recueillir des logs et des données de contexte, notamment des informations d'identité ou les résultats des analyses de vulnérabilité, à l'aide d'une combinaison de méthodes basées ou non sur un agent.

---

<sup>4</sup>Ernst & Young (ou EY), est l'un des plus importants cabinets d'audit et notamment d'audit financier au monde.  
Source : [www.ey.com/](http://www.ey.com/)

### 1.3.2 La normalisation et la catégorisation

Elles permettent la conversion des logs originaux collectés dans un format compréhensible par la solution SIEM. Par ailleurs, les événements sont classés dans des catégories serviables : Modifications de la configuration, Accès aux fichiers ou encore, en fonction des règles définies par les administrateurs de l'outil.

### 1.3.3 La corrélation, la notification et l'alerte

Ces fonctions incluent la corrélation algorithmique, statistique ou basée sur des règles ainsi que d'autres méthodes, comme la mise en relation de différents événements entre eux ou la mise en relation d'événements avec des données de contexte ; le déclenchement de notifications ou d'alertes auprès d'opérateurs ou de gestionnaires. Les mécanismes d'alerte courants comprennent les e-mails, les SMS ou même les messages envoyés via le protocole SNMP.

### 1.3.4 La hiérarchisation et les vues en temps réel

Celles-ci comprennent différentes options qui mettent en évidence et en temps réel, les événements de sécurité importants par rapport à ceux moins graves. Il est donc possible de corréler les événements de sécurité avec des données de vulnérabilité ou d'autres informations sur les ressources. Les algorithmes de hiérarchisation utilisent souvent des informations sur la gravité fournies par le log original. Le résultat de ces fonctionnalités est visualisé dans des tableaux de bord de supervision de la sécurité du parc informatique. Ainsi, les analystes peuvent voir les informations collectées mais aussi les résultats des corrélations pratiquement en temps réel, y compris les événements archivés suivant les paramétrages.

### 1.3.5 La création de rapports et Workflow des rôles de sécurité

La création de rapports standards et planifiés prend en compte toutes les vues historiques des données recueillies par l'outil SIEM. Les rapports sont envoyés aux différents membres de l'équipe en charge de la sécurité du parc informatique suivant les règles définies.

Une fois envoyé, ce rapport permet alors à l'équipe d'initier le processus de réponse à cet incident notifié et validé.

La notification au sujet d'un utilisateur suspect dans un environnement web étant une tâche difficile la corrélation les différents logs centralisés permettra aux investigateurs de mener une enquête efficace dans le cyberspace[4].

Dans le tableau ci-dessous, il est présenté les principales fonctionnalités des outils de centralisation et gestion des logs et événements de sécurité.

TABLE 1.1 – Comparaison entre les outils de gestion des événements de sécurité et des logs

Fonctionnalités	SIEM (Security Information and Event Management)	Gestion des logs
Collecte des logs	Collecte des logs relatifs à la sécurité	Collecte de tous les logs, y compris les logs opérationnels et applicatifs personnalisés
Sauvegarde des logs	Conservation limitée des données de consignation analysées et normalisées	Conservation plus longue des données de consignation brutes et analysées
Analyse	Corrélation, évaluation des menaces et hiérarchisation des événements	Analyse en texte intégral et étiquetage
Création de rapports	Génération de rapports en temps réel pour des fins de sécurité du parc	Création de rapports génériques et historiques
Alertes et notifications	Notification en fonction des règles définies suivie de rapports succincts et/ou avancés pour des fins de sécurité	Alerte simple pour tous les journaux
Autres fonctionnalités	Aide à la validation et la réponse sur incidents ; analyses avancées des données de sécurité	Évolutivité élevée en termes de collecte et de recherche

On y remarque aisément que la technologie SIEM se base principalement sur la technologie traditionnelle de gestion des logs et tient uniquement compte des événements de sécurité.

## Conclusion

Les logs ou journaux d'événements sont la consignation ou un reportage de toutes les activités des utilisateurs ou des tâches programmées identifiées par les composants du parc informatique qui en sont d'ailleurs les acteurs principaux.

La suite de ce document présente les résultats d'une étude technique de quelques solutions open source et payantes s'imposant aux administrateurs de la sécurité.

# Approches de solution

## Introduction

---

La mise en place d'un système de centralisation et de gestion des logs et événements se base avant tout sur la politique de sécurité en vigueur dans l'entreprise.

Ce chapitre présente d'une part, les résultats d'une étude technique de quelques solutions *open source* et payantes par une analyse comparative; et d'autre part, la solution choisie dans le cadre des activités du PAC.

## 2.1 Quelques solutions existantes

---

### 2.1.1 Les solutions gratuites

Il est important de savoir que les solutions Open Source se caractérisent par leur code source qui est ouvert. Il peut donc y avoir une communauté autour de l'outil, une version gratuite et une version payante. L'offre est portée par une société et à un moment ou à un autre il intervient afin de répondre à une sollicitation au sujet du produit acheté.

Les solutions libres s'expliquent par un code source ouvert comme dans le cas du open source. La différence est qu'il y a une communauté plus ou moins importante. Le logiciel libre dispose d'une unique **version gratuite** pour tout le monde. On suppose dans ce cas que l'utilisateur de ce logiciel libre possède les compétences requises pour le mettre en place ou il fait appel à un prestataire de services.

Les solutions identifiées se basent sur ces différents principes.

#### 2.1.1.1 Fail2ban

Fail2ban[9] est un IDS/IPS basé sur les logs. Les logs produits vont permettre à Fail2ban de détecter certaines intrusions et déclencher des actions d'avertissement ou de protection (envoyer un mail, interdire

un accès à une machine suivant son adresse IP, etc.);

### 2.1.1.2 SIEMonster

Il est un gestionnaire d'incident et de gestion de sécurité open source conçu avec des produits open source stables se basant principalement sur l'outil ELK et d'outils développés pour la sécurité et l'adaptation à l'évolution du système d'information. L'objectif était de mettre en place un outil permettant aux opérateurs de la sécurité de détecter les anomalies du réseau à partir de l'un des outils. Pour ce faire, il fonctionne avec les *monstres*[8] suivants :

- **Proteus**, le moteur de gestion du processus de collecte des logs;
- **Capricorn**, le serveur de visualisation et de corrélation des logs collectés et sauvegardés;
- **Kraken**, la base de données principale pour la sauvegarde des logs;
- **Tiamat**, la base de données secondaire pour l'assurance de la réplique;
- **Ikuturso**, le moteur de supervision des activités qui se déroulent dans un réseau en se basant sur Bro et Tardis;
- **Hydra**, le serveur de données à distance, collecteur de données strictement relatives à la sécurité du parc.

Par ailleurs, il existe une version payante offrant plus de fonctionnalités comme la mise à niveau, l'intégration de l'annuaire Active Directory de Windows.

### 2.1.1.3 ELK : Elasticsearch, Logstash et Kibana

**Elasticsearch** est un moteur de recherche et d'analyse distribué, basé sur JSON et conçu pour une évolutivité en fonction des exigences du parc informatique, une fiabilité maximale et une gestion facile;

**Logstash** est un canal de collecte dynamique des données avec un système de plugins extensible permettant une fonction fiable de recherche avec Elasticsearch;

**Kibana** modélise les données et offre une interface utilisateur extensible afin de configurer et gérer tous les aspects de l'Elastic Stack.

Ces produits sont maintenus par la société Elastic[7]. Ces outils sont des solutions SIEM.

## 2.1.2 Les solutions payantes

Dans le cadre de la mise en place d'une solution payante, cette dernière est achetée, puis payée suivant les termes définis dans le contrat de vente. L'utilisateur dispose d'un service après vente ou encore d'une assistance complète pour la mise en place.

Il est donc aussi bien dépendant qu'il utilise le logiciel dans la limite des fonctionnalités de ce dernier.

### 2.1.2.1 Splunk

Il permet aux administrateurs systèmes et réseau de consolider et indexer toutes les données de journal et de machine, y compris les journaux d'application multi-lignes structurés, non structurés et complexes. À l'instar des autres solutions, Splunk[11] permet la collecte, le stockage, la conservation et l'analyse des logs pour des fins de sécurité informatique.

### 2.1.2.2 Sumo Logic

Sumo Logic[6] est une solution de gestion et de suivi des logs *cloud* utilisée par les équipes informatiques, de sécurité et de développement.

Il permet l'utilisation des résultats d'analyses de sécurité avancées pour une sécurité plus robuste et évolutive. L'analyse de sécurité utilise les logs pour repérer les anomalies et visualiser l'utilisation des ressources en temps réel, ce qui permet de prendre des décisions fiables en réponse aux menaces de sécurité complexes. Les données machine aident les équipes informatiques à mettre en contexte les données.

### 2.1.2.3 Nagios Log Server

Nagios Log Server[10] est une application qui fournit aux entreprises un emplacement central de gestion des logs générés par les différents composants du parc à l'instar des précédents outils. Il permet également la sauvegarde des données pour une récupération ultérieure et même leur exploitation suivant des requêtes s'effectuant en temps réel.

## 2.1.3 Une analyse comparative

Le tableau suivant présente les résultats d'une étude comparative faite sur les différentes solutions gratuites et payantes.



TABLE 2.1 – Analyse comparative des différents outils gratuits évoqués

Natures	Solutions Gratuites	Particularités et conformité aux normes	Limites
OPEN SOURCE	<b>Fail2ban</b>	<ul style="list-style-type: none"> <li>• Déclenche des actions d'avertissement et de protection suivant les entrées de log ;</li> <li>• Audit les logs de différents équipements du parc informatique.</li> </ul>	<ul style="list-style-type: none"> <li>• Ne permet pas l'analyse d'un nombre plétorique de logs enregistrés ;</li> <li>• Plus performant en environnement Linux.</li> </ul>
	<b>ELK Stack</b>	<ul style="list-style-type: none"> <li>• Mise en place rapide et suivant les besoins ;</li> <li>• Possibilité de la faire évoluer avec les produits.</li> </ul>	<ul style="list-style-type: none"> <li>• Il n'est pas possible de recevoir des alertes sur des conditions précises ;</li> <li>• N'importe quel utilisateur peut accéder à l'ensemble des logs enregistrés dans le cluster Elasticsearch sauf en cas d'intégration d'un outil payant appelé SHIELD.</li> </ul>
	<b>SIEMonster</b>	<ul style="list-style-type: none"> <li>• Dispose d'un système de Load Balancing basé sur Elasticsearch assurant une duplication de toutes les données afin d'assurer la réplique en cas de défaillance du système principale de gestion des logs ;</li> <li>• Basé sur des modules open source, il intègre l'ensemble des tableaux de bord, plugins et outils de réponse aux incidents.</li> </ul>	<ul style="list-style-type: none"> <li>• Sollicite énormément de ressources mémoire : Cinq machines ayant au minimum 2 GB de mémoires ram ;</li> <li>• Retours d'expériences non mises à jour.</li> </ul>

SOUS LICENCE	<b>Splunk</b>	<ul style="list-style-type: none"> <li>• Simplicité et rapidité de mise en œuvre ;</li> <li>• Facilité d'utilisation et documentations mises à jour disponibles.</li> </ul>	<ul style="list-style-type: none"> <li>• Limite le nombre de nouvelles données pouvant être indexées par jour ;</li> <li>• La version gratuite plafonne à 500 Mo/jours.</li> </ul>
	<b>Sumo Logic</b>	Permet la surveillance des applications et de l'infrastructure en temps réel en se basant sur les logs.	<ul style="list-style-type: none"> <li>• Les prix des différents services de Sumo Logic sont élevés ;</li> <li>• Il assure correctement uniquement la fonction de stockage des données.</li> </ul>
	<b>Nagios Log Server</b>	<ul style="list-style-type: none"> <li>• Il gère tous les processus (collecte, sauvegarde, traitement, alerte et visualisation, etc.) en une seule instance et autorise l'ajout d'autres instance permettant d'assurer la continuité de ses activités même en cas de défaillance ;</li> <li>• Permet d'envoyer les résultats de ses analyses à Nagios Core afin de permettre à ce dernier de mieux appréhender l'état réel du parc.</li> <li>• Facilité d'utilisation et documentations mises à jour disponibles.</li> </ul>	<ul style="list-style-type: none"> <li>• Une limite de 500mb par jours pendant des 60 jours d'essai de toutes les fonctionnalités.</li> </ul>

## 2.2 Le choix de la solution

---

De l'analyse des solutions gratuites et payantes identifiées, les sections suivantes illustrent et justifient les critères de choix de la solution.

### 2.2.1 Le choix technique

Sur la base des contraintes techniques liées aux types et fonctionnalités de la solution à étudier, il a été retenu **Nagios Log Server**.

En effet cette solution offre des facilités de gestion de la traçabilité des événements qui se déroulent dans le parc informatique. Suivant les configurations faites, elle envoie ses résultats d'analyses vers Nagios Core, la solution de supervision du parc informatique.

### 2.2.2 Le principe de fonctionnement de Nagios Log Server

#### 2.2.2.1 La collecte et l'expédition

La collecte s'effectue sur tout les composants du parc informatique. Il s'agit de collecter les journaux afin de les expédier vers le serveur de centralisation. Cette collecte est soit assurée par NXlog<sup>1</sup>, l'agent open source de collecte des logs certifié et utilisé par Nagios Log Server, soit par le serveur qui aspire<sup>2</sup> directement les logs depuis les composants du système informatique.

#### 2.2.2.2 Le filtrage

Une fois les logs collectés et parvenus à Nagios Log Server, un filtrage est effectué grâce à Logstash, l'un des composants de Nagios Log Server. (Voir figure 2.1)

---

<sup>1</sup>L'agent de collecte sous forme de SaaS installé sous Windows (Client et/ou Serveur).

<sup>2</sup>Collecte par lui-même les différents logs des machines linux et équipements réseaux.

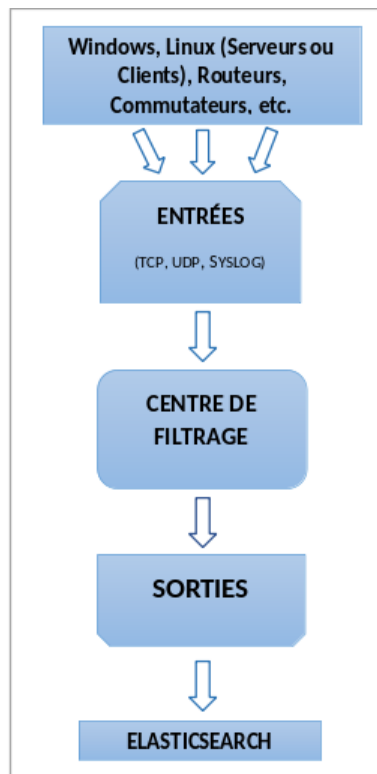


FIGURE 2.1 – Architecture de fonctionnement de Logstash intégré à Nagios Log Server

Avant que les filtres ne soient appliqués, les logs ne sont généralement pas structurés dès leurs arrivées et n'ont pas de champs appliqués.

D'après cette figure, le composant open source logstash regroupe un processus de traitement à trois étapes :

- **Les entrées** (inputs) qui reçoivent les logs entrants et les transmettent à la chaîne de filtrage :

Les journaux parviennent à l'entrée via les protocoles TCP et/ou UDP grâce à NXLog ;

Dans le cas de l'entrée Syslog, chaque log qui y entre aura automatiquement le filtre syslog appliqué. (Voir figure 2.2)

```
"match" => { "message" => "<{%POSINT:priority}>{%SYSLOGLINE}"
```

FIGURE 2.2 – Exemple de filtre Syslog

- **Les filtres** (filters) qui analysent les logs transmis de la chaîne d'entrée aux filtres personnalisés définis ;

Après le filtrage, les champs sont représentés d'une manière permettant l'identification des informations contenues dans les logs de façon succincte et plus compréhensible. (Voir figure 2.3).

Field	Action	Value
<input checked="" type="checkbox"/> @timestamp ▼	Q Ø ▢	2017-09-01T08:09:02.000Z
<input type="checkbox"/> @version	Q Ø ▢	1
<input type="checkbox"/> _id	Q Ø ▢	AV48fHN_TcYoYrU0j1yF
<input type="checkbox"/> _index	Q Ø ▢	logstash-2017.09.01
<input type="checkbox"/> _type	Q Ø ▢	syslog
<input type="checkbox"/> facility	Q Ø ▢	10
<input type="checkbox"/> facility_label	Q Ø ▢	security/authorization
<input type="checkbox"/> highlight	Q Ø ▢	[object Object]
<input checked="" type="checkbox"/> host	Q Ø ▢	192.168.102.108
<input type="checkbox"/> logsource	Q Ø ▢	localhost
<input checked="" type="checkbox"/> message	Q Ø ▢	nagios : TTY=unknown ; PWD=/var/h
<input type="checkbox"/> priority	Q Ø ▢	85
<input type="checkbox"/> program	Q Ø ▢	sudo
<input type="checkbox"/> severity	Q Ø ▢	5
<input type="checkbox"/> severity_label	Q Ø ▢	Notice
<input type="checkbox"/> timestamp	Q Ø ▢	Sep 1 09:09:02
<input checked="" type="checkbox"/> type	Q Ø ▢	syslog

FIGURE 2.3 – Représentation des champs après filtrage

- **Les sorties** (outputs) sont responsables de l'exportation des données issues du filtrage vers elasticsearch.

L'administrateur se servira donc des analyses faites par Nagios Log Server afin de définir des règles de notifications et d'alertes.

### 2.2.2.3 La centralisation et la bancarisation

La centralisation des logs, leur sauvegarde, archivage et exploitation depuis la base de données sont des tâches à l'actif de Elasticsearch. L'ensemble du système reste robuste, résilient et intègre grâce à un système de redondance mis en place pour chaque instance de Nagios Log Server. Le fonctionnement interne de Elasticsearch est présenté dans la figure 2.4.

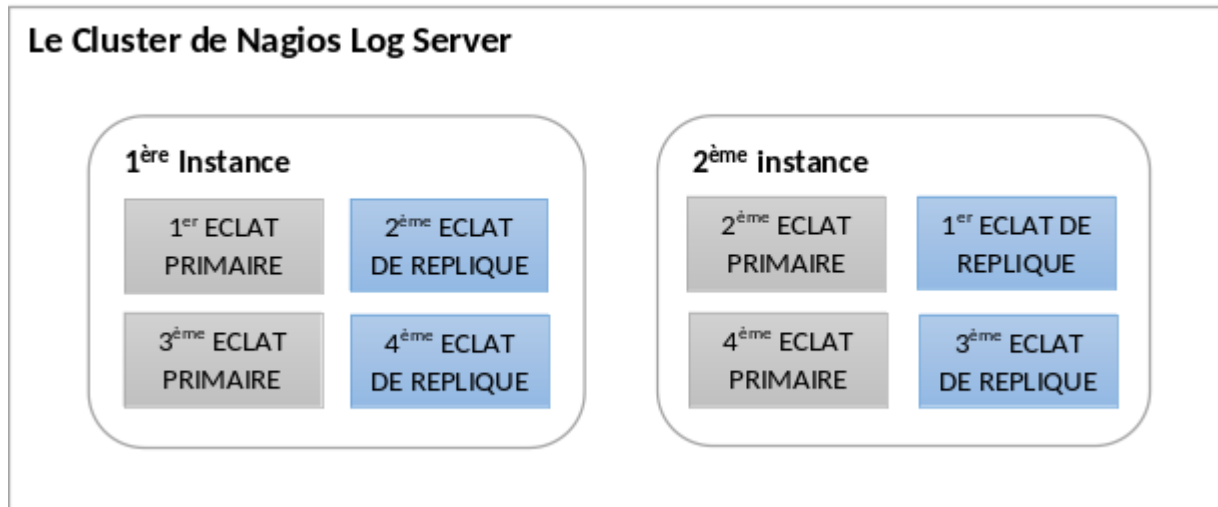


FIGURE 2.4 – Fonctionnement interne de Nagios Log Server

Conformément à cette figure, il y a deux instances réunies en un seul cluster. Chaque instance contient deux tessons (éclats) primaires et deux tessons répliques. Elasticsearch n'attribue jamais un tesson primaire et une réplique de tesson correspondant à la même instance. Cette méthode permet la haute disponibilité des services et des données gérées par Nagios Log Server.

En effet, Nagios Log Server s'explique par les points suivants :

- Un cluster de Nagios Log Server est un ensemble de deux instances ou plusieurs ;
- Plusieurs instances de Nagios Log Server connectées forment un cluster. Généralement, les instances sont installées sur des machines virtuelles ou physiques distinctes ;
- Les index sont responsables de la cartographie des éclats primaires et des éclats de répliques. Un index doit correspondre à un ou plusieurs tessons primaires, et au moins un ou plusieurs tessons de réplique ;
- Un tesson peut être primaire ou une réplique. Par défaut, dix tessons composent chaque index : cinq primaires et cinq répliques ;
- Chaque log envoyé à Nagios Log Server est stocké dans un éclat primaire. Une fois que le tesson a été indexé sur le tesson primaire, il est dupliqué sur un tesson de réplique. De cette façon, la redondance est créée ;
- Par défaut, chaque éclat primaire (dans le groupe de cinq (05) tessons primaire) a un éclat de réplique (cinq tessons correspondant aux tessons primaires), ce qui fait un total de dix (10) tessons. Un tesson de réplique est simplement une copie d'un tesson primaire et est toujours stocké sur une instance séparée en respect avec les normes en vigueur ;
- Chaque fois qu'une instance est ajoutée au Cluster, Elasticsearch s'assure que sa base de données est répartie sur tous les nœuds de manière appropriée en se déplaçant autour des différents fragments d'une manière qui augmente la résilience des données.

### 2.2.2.4 Les alertes et notifications

Les alertes sont créées en fonction d'une ou plusieurs expressions régulières, partant de la sévérité du message notifiant le programme l'ayant généré. Nagios Log Server dispose de la possibilité d'envoi de ces messages par courrier électronique directement aux utilisateurs choisis par l'administrateur. Les alertes peuvent également être envoyées à Nagios XI et/ou Nagios Core via NRDP<sup>3</sup>, ou à travers les traps SNMP ou même exécuter un script personnalisé (messagerie instantanée par SMS, par exemple).

### 2.2.2.5 Le tableau de bord

L'interface d'interrogation des événements centralisés est servie par le composant Kibana de Nagios Log Server. Il s'agit d'une interface web permettant de construire un tableau de bord personnalisé et qui affiche à la fois les messages et les métriques.

La figure 2.5 présente un extrait d'une interface de visualisation :

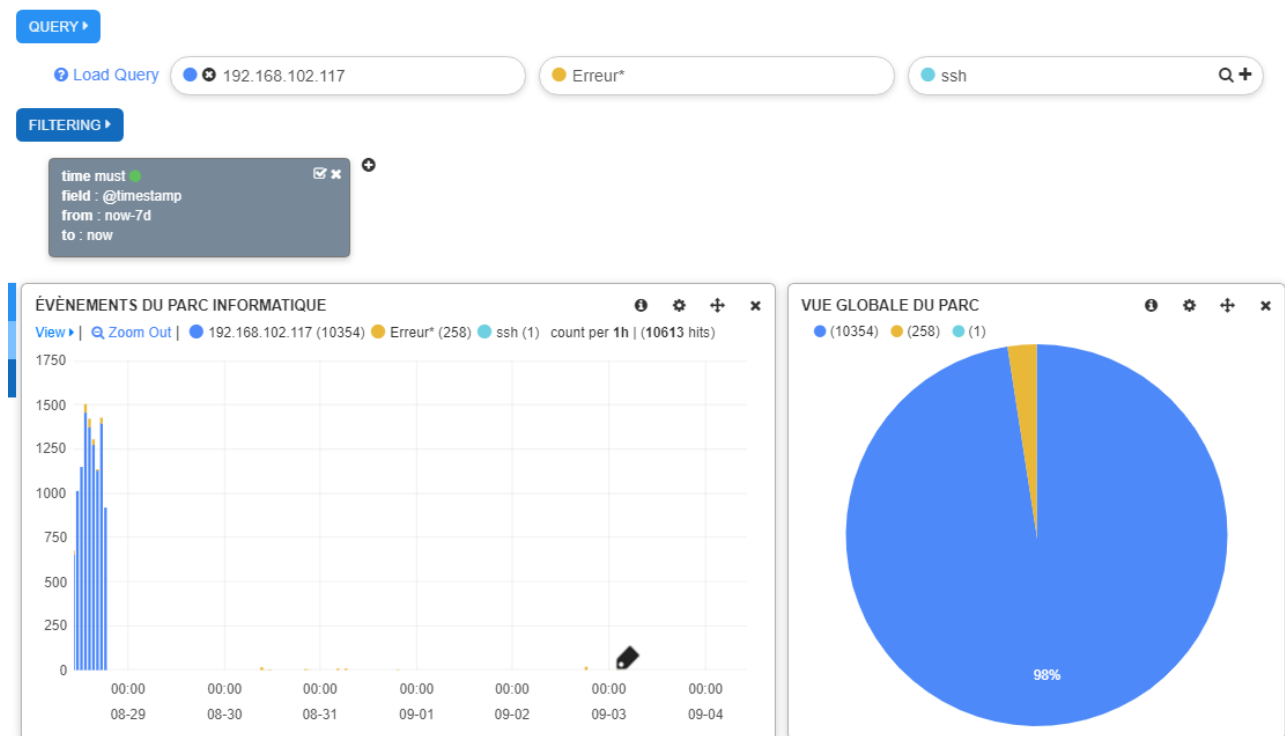


FIGURE 2.5 – Extrait d'une interface de visualisation d'événements indexés

<sup>3</sup>Un service interne de nagios permettant l'envoi de notifications entre les produits Nagios (Principalement Nagios Log Server, Nagios XI et Nagios Core).

## 2.3 Exploitation et exploration des informations issues des logs

---

Les logs, étant indexés<sup>4</sup>, peuvent être facilement analysés à l’aide des outils de sélection sur le tableau de bord. Nagios Log Server permet une recherche approfondie sur les événements indexés par l’outil en offrant une **exploration** directe des logs sur les moteurs de recherches comme *Google*, *Bing* ou encore *StackOverflow*. (Voir figure 2.6)

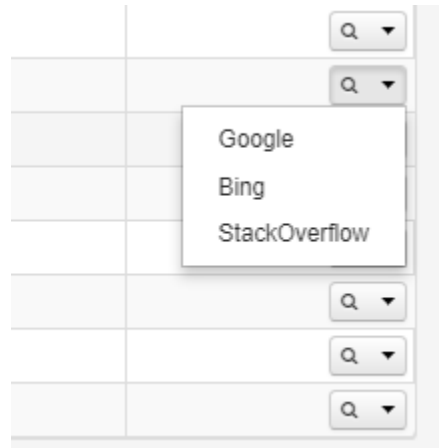


FIGURE 2.6 – Interface permettant l’exploration d’événements indexés

## 2.4 Gestion des utilisateurs

---

Nagios Log Server peut être utilisé par plusieurs utilisateurs en même temps, ce qui permet à l’équipe en charge de la sécurité du parc informatique de travailler plus efficacement ensemble. Les administrateurs peuvent ajouter, modifier et supprimer des utilisateurs, ainsi qu’octroyer différents droits aux utilisateurs à leurs guises.

La figure 2.7 présente une interface d’ajout d’un utilisateur du système.

---

<sup>4</sup>L’indexation se produit généralement dans les cinq (05) secondes à partir de l’arrivée



## Create User

Please enter all fields of the new users information below. Starred fields are required

### User Details

Full Name:

Email:

### Account Information

Username:

Password:

Confirm Password:

Language:

### Authentication Settings

User accounts can be authenticated in many different ways either from your local database or external programs such as Active Directory or LDAP. You can set up external authentication servers in the [LDAP/AD Integration settings](#).

Auth Type:

FIGURE 2.7 – Interface d'ajout d'utilisateur de Nagios Log Server

La figure 2.8 présente une interface d'attribution de droits des utilisateurs de Nagios Log Server.

### User Access Level

Set the user level of access inside the UI.

- ☐ **Admin - Full Access.** Admins can change/delete all items including saved queries, alerts, indexes and backup snapshots. They can also update the Nagios Log Server configuration and manage users.
- ☒ **User - Limited Full Access.** Users can see everything except the Configure section, Administration section and Administrator reports. However, they can not edit anything except their own dashboards, reports, alerts, profile's password, contact info, and api key.

### API Access

If you want to allow this user to use the external API via an access key.

- ☐ Yes
- ☒ No

FIGURE 2.8 – Interface d'attribution de droits des utilisateurs de Nagios Log Server

## Conclusion

---

Les différentes solutions identifiées se basent sur les prérequis pour la mise en conformité des entreprises. La suite du document présente le processus de déploiement de Nagios Log Server sur le parc informatique du PAC.

## Mise en place de la solution

### Introduction

---

En vue de garantir la traçabilité des différents événements, il a été ajouté à Nagios Core la solution de supervision du parc informatique actuellement en déploiement, une solution de centralisation et de gestion des logs qui communique désormais avec celui-ci .

Ce chapitre présente les prérequis et procédures d'installation de Nagios Log Server.

### 3.1 Les prérequis à la mise en place de Nagios Log Server

---

Conformément aux exigences pour le déploiement de Nagios Log Server, il a été mis en place une instance de Nagios Log Server dans le réseau local de l'entreprise munie d'une passerelle unique d'accès à internet tout en étant connecté à toutes les machines susceptibles de lui envoyer leur logs.

Une fonctionnalité de journalisation sur les différentes machines hôtes (Windows, Linux, Équipements réseau, etc.) est nécessaires afin d'alimenter le système de centralisation et de gestion des logs ; puis une fois que les tests de connectivité sont validés entre ces machines et Nagios Log Server, un choix des événements à notifier suivant un seuil et suivant la priorité est fait pour une traçabilité complète des événements.

Une liste quelques peu exhaustive des événements à prioriser est définie et expliquée à l'annexe A.

La figure 3.1 présente l'architecture de déploiement utilisée sur la base de celle globale du parc.

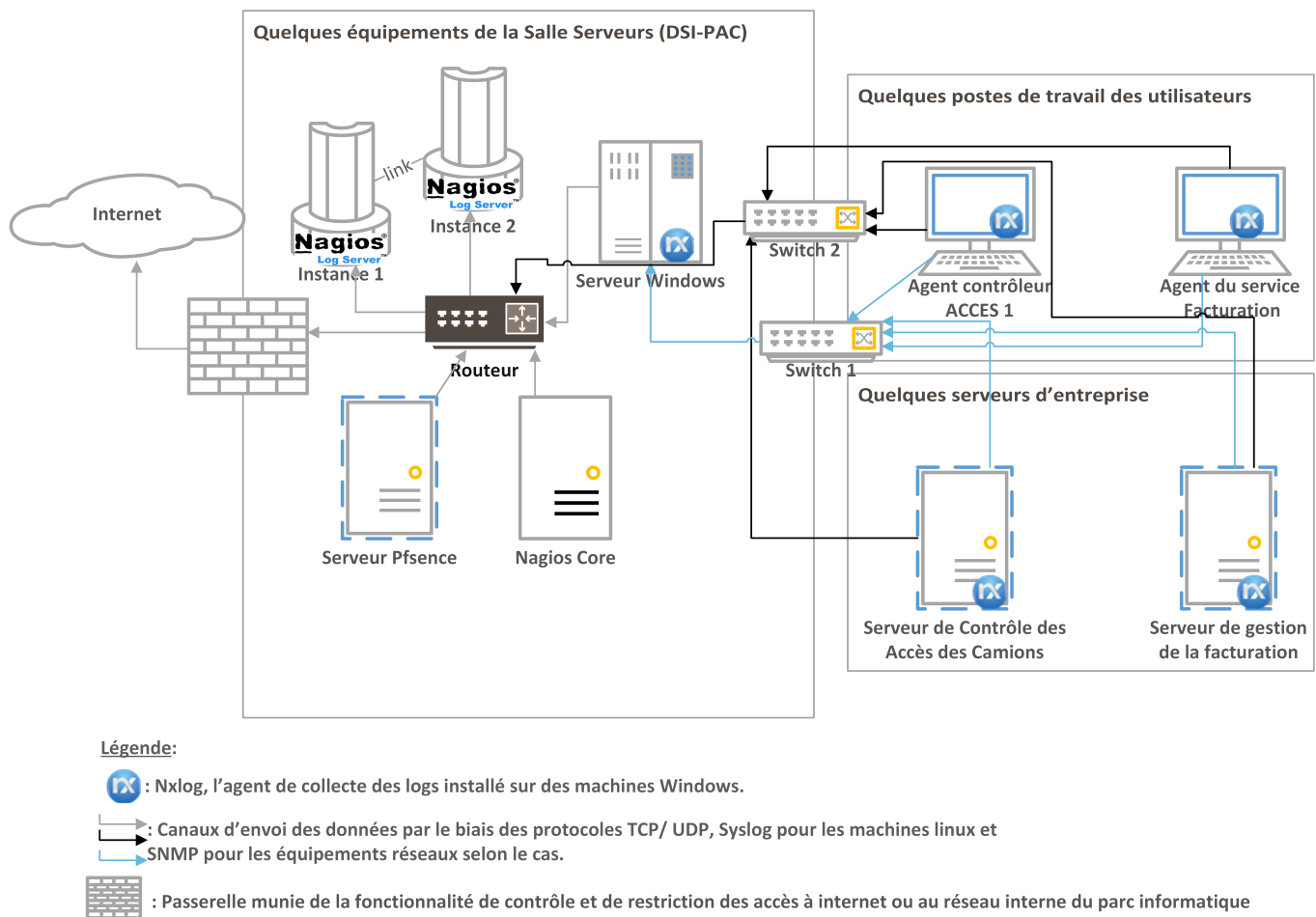


FIGURE 3.1 – Architecture de mise en place

En effet, l'agent **NXlog** permet la lecture des fichiers logs tiers provenant des machines mises "sous écoute".

Les commutateurs 1 et 2 permettent respectivement la communication entre les différents serveurs et les postes clients pour l'exécution de leurs différentes fonctions ; et la notification des événements (consignés dans les fichiers de log) à Nagios Log Server qui se charge de les analyser.

## 3.2 Le déploiement de Nagios Log Server

Le déploiement se fait en plusieurs étapes que sont l'installation et le paramétrage de Nagios Log Server et la configuration des différentes sources d'envois de logs.

### 3.2.1 L'installation de Nagios Log Server

L'installation de Nagios Log Server sont présentés à l'annexe B.1.

### 3.2.2 Le paramétrage de Nagios Log Server

Ce paramétrage se fait aussi bien sur le serveur de centralisation des logs que sur toutes les composantes du parc informatique, y compris les fichiers de logs tiers. Le processus de configuration de ces composantes et de personnalisation des paramètres d'alerte est illustré à l'annexe B.2.

## 3.3 La Simulation

### 3.3.1 La création d'une règle de filtrage

La règle de filtrage des informations contenues dans les logs a été créée sur la base de l'adresse IP du serveur Windows qui a été renseignée. (Voir figure 3.2)

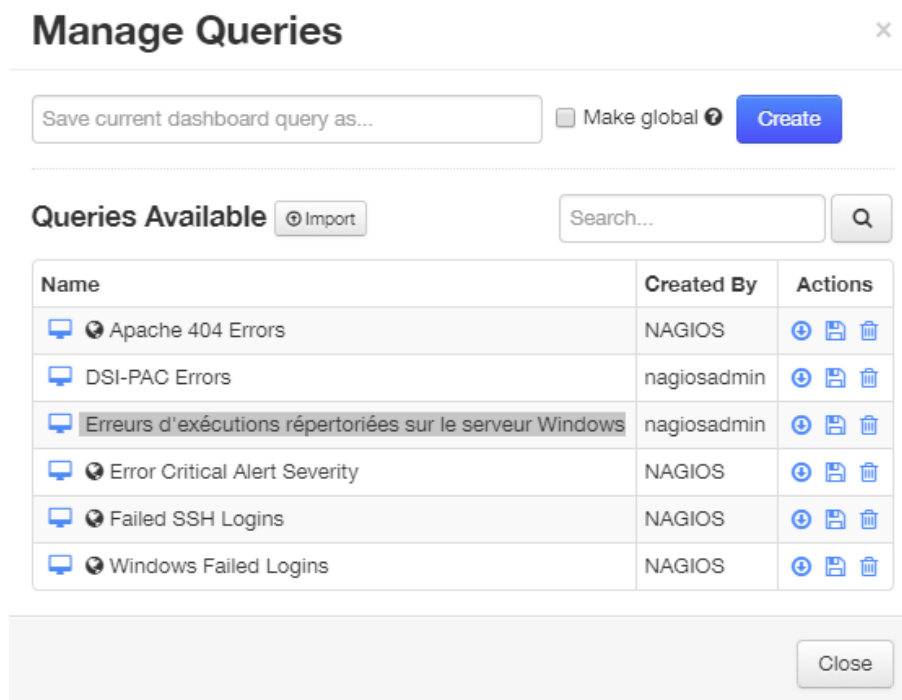


FIGURE 3.2 – Création d'une règle de filtrage

### 3.3.2 La personnalisation du contenu des notifications par email sous Nagios Log Server

La personnalisation du contenu des notifications à envoyer pour plus de compréhension s'est faite en ajoutant un modèle de contenu de notifications avec les variables<sup>1</sup>. (Voir figure 3.3)

<sup>1</sup>Les données essentielles changeants en fonction des logs collectés

## Add Email Template ✕

Manage email templates for alerts. You can use the macros below inside the email message and they will be populated before the message is sent.

```

<p>Le %alertname% est actuellement à l'état <b>%state%</b>.

<p>L'alerte a été générée suivant les règles ci-après:<br>
<div>Période de recherche: %lookback%</div>
<div>Messages d'avertissements: %warning%</div>
<div>Messages critiques: %critical%</div>
</p>
<p>
Voici le contenu complet de cette notification: <br>
<div>%output%</div>
<b>Nombre de logs par source : </b>
<div>%uniquehosts%</div>
</p>
<p>Visualisez le résultat des dernières recherches effectuées en %lookback%
en cliquant <a href="%url%">sur ce lien</a>.</p>
<br>

```

Load ▾

Cancel

Add

FIGURE 3.3 – Interface de personnalisation du contenu des notifications par email

### 3.3.3 La configuration d'une alerte

Le tableau 3.3.3 présente un exemple de configuration d'alerte.

TABLE 3.1 – Configuration de l’alerte en théorie

ÉTAPES	DÉSIGNATION
Nom de l’alerte	PARC INFORMATIQUE DU PAC
Choix d’une requête à prendre en compte	Erreurs d’exécutions répertoriées sur le serveur Windows
Intervalle de temps de consultation des résultats (En seconde / minute / heure / jour) <sup>2</sup>	5 Minutes (5m)
Période de recherche (En seconde / minute / heure / jour) <sup>3</sup>	Depuis 14 Jours (14 d) à l’instant
Seuil des événements	Dix (10) Messages d’avertissements et deux (02) Messages portant des événements critiques
Méthode d’alerte	Par courrier électronique

En effet, la requête “*Erreurs d’exécutions répertoriées sur le serveur Windows*” a été créée sur un tableau de bord affichant les erreurs disponibles à partir de la requête créée.

La figure 3.4 présente l’interface de création de l’alerte sous Nagios Log Server.

**Create an Alert**

Alert Name: PARC INFORMATIQUE DU PAC

Query: Apache 404 Errors (dropdown menu open showing: Apache 404 Errors, DSI-PAC Errors, Erreurs d'exécutions répertoriées sur le serveur Windows, Error Critical Alert Severity, Failed SSH Logins, Windows Failed Logins)

Check Interval: (empty)

Lookback Period: (empty)

Thresholds: 10, 02 # of events

Alert Method: Email Users

Select Users: nagiosadmin

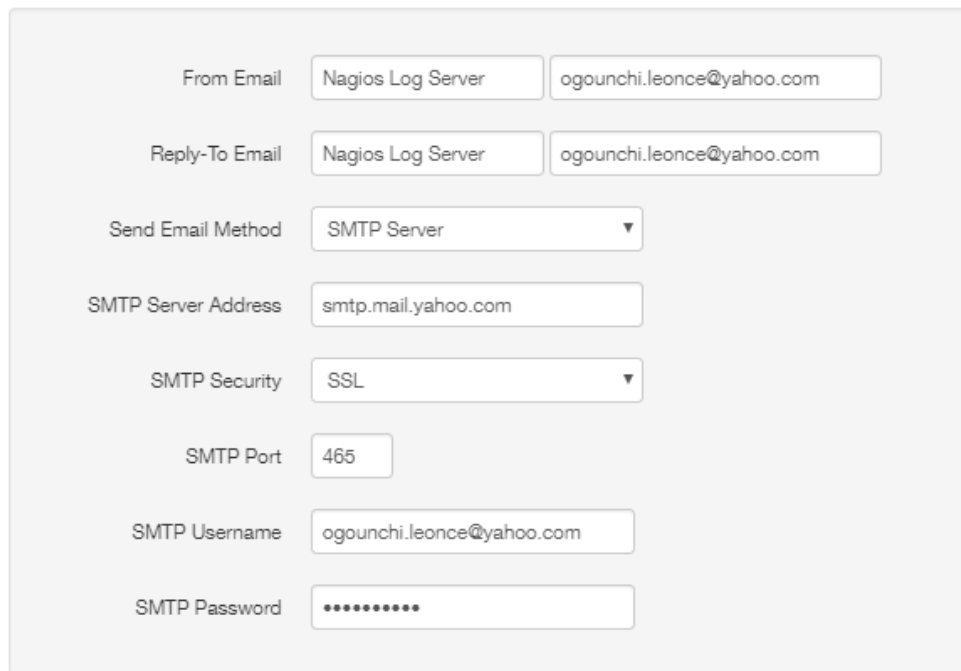
Email Template: DSI PARC TEMPLATE

Create Alert Close

FIGURE 3.4 – Configuration d’une alerte sous Nagios Log Server à recevoir par mail

Afin de garantir l'envoi des notifications par mail, une configuration a été faite au niveau du serveur SMTP de Nagios Log Server.

La figure 3.5 présente l'interface de configuration des paramètres SMTP.



The image shows a web-based configuration interface for SMTP settings. It contains several input fields and dropdown menus arranged vertically. The 'From Email' and 'Reply-To Email' fields are split into two parts: a label and a text input. The 'Send Email Method' is a dropdown menu. The 'SMTP Server Address' is a text input. The 'SMTP Security' is a dropdown menu. The 'SMTP Port' is a text input. The 'SMTP Username' is a text input. The 'SMTP Password' is a text input with masked characters (dots).

From Email	Nagios Log Server	ogouchi.leonce@yahoo.com
Reply-To Email	Nagios Log Server	ogouchi.leonce@yahoo.com
Send Email Method	SMTP Server ▼	
SMTP Server Address	smtp.mail.yahoo.com	
SMTP Security	SSL ▼	
SMTP Port	465	
SMTP Username	ogouchi.leonce@yahoo.com	
SMTP Password	*****	

FIGURE 3.5 – Interface de configuration des paramètres SMTP

### 3.3.4 La visualisation de l'état du parc informatique

#### 3.3.4.1 La visualisation dans un tableau de bord

Sur la base de l'alerte définie précédemment, il y a une création d'un tableau de bord dont l'extrait est présenté dans la figure 3.6.



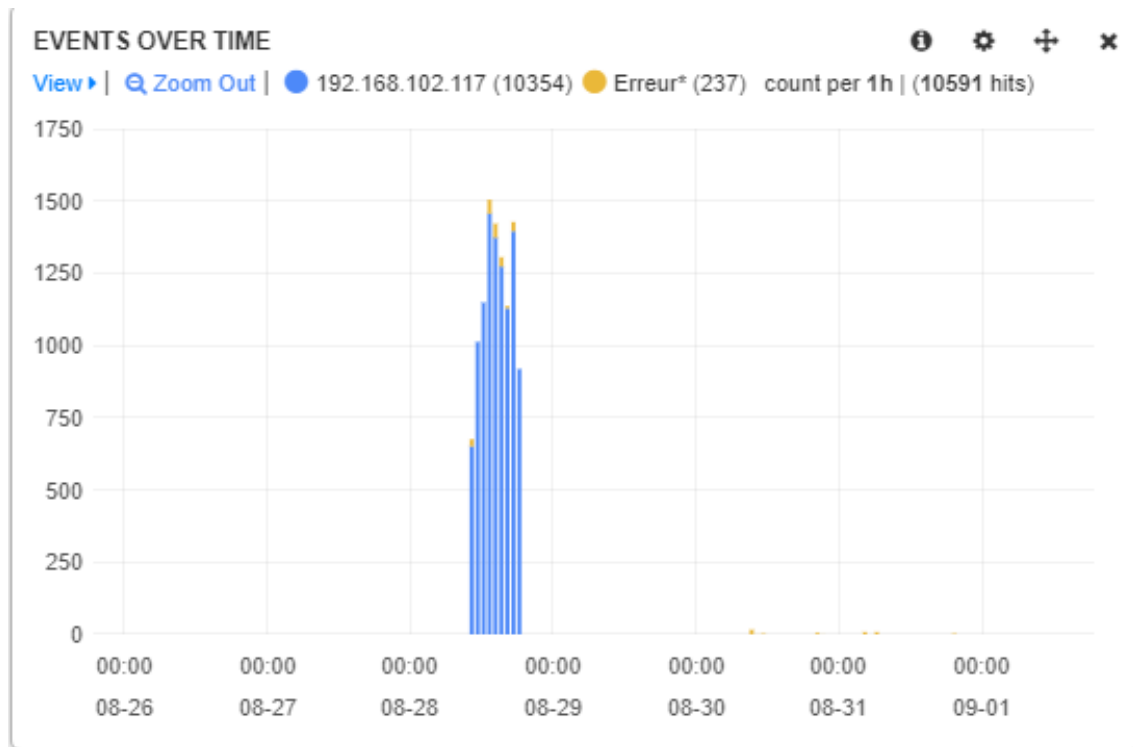


FIGURE 3.6 – Extrait de l’interface de Visualisation

### 3.3.4.2 La visualisation de la notification reçue par courrier électronique

La figure 3.7 présente une visualisation de cette alerte notifiée par mail à l’utilisateur renseigné à Nagios Log Server.

● **Nagios Log Server** <root@dsipac.alo>  
 À ogouchi.leonce@yahoo.com

Le PARC INFORMATIQUE DU PAC est actuellement à l'état **CRITICAL**.  
 L'alerte a été générée suivant les règles ci-après:  
 Période de recherche: 14d  
 Message d'avertissement: 10  
 Message critique: 10  
 Voici le contenu complet de cette notification:  
 CRITICAL: 10420 matching entries found ||logs=10420;10;10  
**Nombre de logs par source:**  
 192.168.102.117 (10354)  
 192.168.102.128 (41)  
 192.168.102.118 (22)  
 192.168.102.141 (3)

Visualisez le résultat des dernières recherches effectuées en 14d cliquant [sur ce lien](#).

**Système de Centralisation et de Gestion des Logs du parc informatique du Port Autonome de Cotonou**

FIGURE 3.7 – Extrait de la notification reçue par mail

---

Les analyses de Nagios Log Server ayant montré que le parc informatique est dans un état critique, le service en charge de la sécurité informatique prendra alors des mesures afin de lire le contenu des quelques messages détaillés affichés sur le tableau de bord.

## Conclusion

---

La mise en place d'une telle solution SIEM n'a de l'effet qu'une fois alimentée par tous les fichiers log du parc informatique afin accroître la capacité du service en charge de la sécurité informatique à répondre aux attentes de l'équipe d'exploitation des ressources.

Elle ne prouvera son offre de facilité de maîtrise du parc informatique qu'une fois déployée en environnement de production.

# Conclusion Générale

La gestion des informations et événements de sécurité constitue une interrogation majeure quant à sa valeur ajoutée réelle à l'atteinte des objectifs de l'entreprise tout en assurant la sécurité des actifs informationnels de celle-ci.

L'objectif de ce document était de trouver une réponse fiable à cette interrogation. Il a donc été retenu une solution SIEM appelée Nagios Log Server qui permet la collecte, la centralisation et la gestion des logs.

En effet, il assure l'analyse des logs tout en notifiant les événements graves aux administrateurs suivant les méthodes paramétrées. Il peut également envoyer le résultat de ses investigations au serveur Nagios Core qui se charge de faire valider aux administrateurs les différents dysfonctionnements sur le parc informatique.

La solution SIEM mis en place est actuellement en environnement de test sur la base d'une architecture inspirée de celle du parc informatique du PAC.

Ce travail a été enrichissant professionnellement par les connaissances théoriques et surtout pratiques au sujet de l'impact de la traçabilité des opérations sur la sécurité informatique en entreprise.

Cet aspect de la sécurité informatique ne suffit pas pour assurer la sécurité de tout le parc informatique dans une démarche de défense en profondeur surtout quand il s'agit de faire un choix des événements à indexer. Toutes les fonctionnalités de la solution SIEM précédemment présentées n'ont pas été mise à l'épreuve compte tenue des contraintes techniques liées à la disponibilité des ressources permettant une simulation approfondie. Ainsi, il est prévu à la suite de ce travail :

- d'assurer l'intégrité des actifs informationnels grâce à la solution SIEM ;
- de mettre en place un système de notification et d'alerte instantanée par SMS permettant à l'équipe en charge de la sécurité informatique d'être informé de l'état du parc informatique sans avoir forcément un accès à internet ;
- de configurer un système de notification via NDRP permettant à Nagios Core, la solution de monitoring actuelle d'être informé des résultats des analyses faites par Nagios Log Server et de lui envoyer aussi ses log pour analyse.

# Bibliographie

- [1] La gestion de logs : un impératif pour assurer la sécurité de son si, consulté le 10 mars 2017 , publié le 26 Octobre 2011.
- [2] BSC BAS BAI and MRR. *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, volume 1. Etalab, 1.0 edition, 2013.
- [3] Dr Anton Chuvakin. *Le guide complet de la gestion des logs et événements*. Dr Anton Chuvakin, 2016.
- [4] Nikhil Kumar Singh, Deepak Singh Tomar, and Bhola Nath Roy. An approach to understand the end user behavior through log analysis. *International Journal of Computer Applications*, 5(11) :27–34, 2010.

# Webographie

- [1] Active Directory, <http://www.commentcamarche.net/contents/1-active-directory>, consulté le 15 mars 2017.
- [2] LDAP, <http://www.commentcamarche.net/contents/525-le-protocole-ldap>, consulté le 15 juin 2017
- [3] SOC, <http://www.lemagit.fr/definition/SOC>, consulté le 16 mars 2017.
- [4] Software as a Service, <http://www.journaldunet.com/solutions/saas-logiciel/saas-definition.shtml>, consulté le mars 18, 2017.
- [5] Fichiers de Log, <https://www.landl.fr/:https://www.landl.fr/digitalguide/web-marketing/analyse-web/les-fichiers-log-lenregistrement-des-processus-informatiques/>, consulté le 20 juin 2017.
- [6] Sumo Logic, <https://www.sumologic.com/how-it-works/>, consulté le 02 juin 2017
- [7] Elastic, The Open Source Elastic Stack, <https://www.elastic.co/products>, consulté le 14 mars 2017
- [8] SIEMonster, <https://siemonster.com/monsters/>, consulté le 14 juin 2017
- [9] Fail2ban, [https://www.fail2ban.org/wiki/index.php/Main\\_Page](https://www.fail2ban.org/wiki/index.php/Main_Page), consulté le 16 juillet 2017
- [10] Nagios Log Server, <https://www.nagios.com/products/nagios-log-server/>, consulté le 14 juillet 2017
- [11] Splunk, <https://www.splunk.com>, consulté le 18 mai 2017

# Table des matières

Dédicace	i
Remerciements	ii
Liste des figures	v
Liste des tableaux	vi
Glossaire	vii
Sigles et Abréviations	viii
Résumé	ix
Abstract	x
Introduction Générale	1
<b>1 Contexte d'étude</b>	<b>3</b>
1.1 Les concepts clés sur les informations et événements de sécurité . . . . .	3
1.1.1 Les fichiers log . . . . .	3
1.1.2 Les journaux de systèmes d'exploitation . . . . .	4
1.1.3 Les journaux de quelques logiciels de sécurité . . . . .	5
1.1.4 Les journaux d'applications . . . . .	6
1.1.5 Les cas d'utilisation des fichiers logs . . . . .	7
1.2 Les caractéristiques des solutions de centralisation et gestion des logs . . . . .	7
1.2.1 La collecte des données de consignation . . . . .	7
1.2.2 La conservation rationnelle . . . . .	7
1.2.3 La recherche . . . . .	7
1.2.4 L'indexation et l'analyse des logs . . . . .	8
1.2.5 La création de rapports standards et planifiés . . . . .	8
1.3 Le principe de la centralisation et gestion des événements de sécurité . . . . .	8
1.3.1 La collecte des données de contexte et des logs . . . . .	8
1.3.2 La normalisation et la catégorisation . . . . .	9
1.3.3 La corrélation, la notification et l'alerte . . . . .	9
1.3.4 La hiérarchisation et les vues en temps réel . . . . .	9
1.3.5 La création de rapports et Workflow des rôles de sécurité . . . . .	9

---

<b>2</b>	<b>Approches de solution</b>	<b>11</b>
2.1	Quelques solutions existantes . . . . .	11
2.1.1	Les solutions gratuites . . . . .	11
2.1.2	Les solutions payantes . . . . .	12
2.1.3	Une analyse comparative . . . . .	13
2.2	Le choix de la solution . . . . .	16
2.2.1	Le choix technique . . . . .	16
2.2.2	Le principe de fonctionnement de Nagios Log Server . . . . .	16
2.3	Exploitation et exploration des informations issues des logs . . . . .	21
2.4	Gestion des utilisateurs . . . . .	21
<b>3</b>	<b>Mise en place de la solution</b>	<b>24</b>
3.1	Les prérequis à la mise en place de Nagios Log Server . . . . .	24
3.2	Le déploiement de Nagios Log Server . . . . .	25
3.2.1	L'installation de Nagios Log Server . . . . .	25
3.2.2	Le paramétrage de Nagios Log Server . . . . .	26
3.3	La Simulation . . . . .	26
3.3.1	La création d'une règle de filtrage . . . . .	26
3.3.2	La personnalisation du contenu des notifications par email sous Nagios Log Server . . . . .	26
3.3.3	La configuration d'une alerte . . . . .	27
3.3.4	La visualisation de l'état du parc informatique . . . . .	29
	<b>Conclusion Générale</b>	<b>32</b>
	<b>Bibliographie</b>	<b>33</b>
	<b>Table des matières</b>	<b>35</b>
<b>A</b>	<b>Le choix des événements</b>	<b>xi</b>
<b>B</b>	<b>L'installation et le paramétrage de Nagios Log Server</b>	<b>xvi</b>
B.1	Le processus d'installation . . . . .	xvi
B.2	Le paramétrage de Nagios Log Server . . . . .	xix
B.2.1	L'installation et la configuration de l'agent de collecte sous Windows . . . . .	xix
B.2.2	La configuration du système de collecte des <i>Syslog</i> de Linux . . . . .	xx
B.2.3	La personnalisation des paramètres d'alerte . . . . .	xxi

## Le choix des événements

Il est important de procéder à la sélection des événements (messages) journalisés par les différents composants du système d'information. Journaliser la totalité des événements peut entraîner une consommation excessive des ressources (processeur, mémoire, stockage, bande passante, etc.) et engendrer une quantité de données difficilement exploitable. À l'inverse, une politique de journalisation trop ciblée ne produira pas suffisamment de données utiles.

Cette liste de haut niveau n'est pas exhaustive, elle peut être enrichie en fonction des exigences du Port Autonome de Cotonou.

TABLE A.1 – Comparaison entre les outils de gestion des événements de sécurité et des logs

Types d'événements	Exemples
<b>Authentification</b>	<ul style="list-style-type: none"> <li>- Réussites et échecs d'authentifications</li> <li>- Utilisations des différents mécanismes d'authentification</li> <li>- Élévations de privilèges</li> </ul>
<b>Gestion des comptes et des droits</b>	<ul style="list-style-type: none"> <li>- Ajouts ou suppressions de comptes, groupes ou rôles</li> <li>- Affectations/suppressions de droits aux comptes/groupes/rôles</li> <li>- Modifications des données d'authentification</li> </ul>



<b>Accès aux ressources</b>	<ul style="list-style-type: none"> <li>- Accès ou tentatives d'accès aux ressources en lecture, écriture et/ou exécution</li> </ul>
<b>Modification des méthodes de sécurité</b>	<ul style="list-style-type: none"> <li>- réinitialisation ou modification de configurations</li> <li>- détection de rootkits dans le système d'exploitation</li> </ul>
<b>Activités des processus</b>	<ul style="list-style-type: none"> <li>- démarrages ou arrêts des processus</li> <li>- dysfonctionnements spécifiques</li> <li>- chargements et/ou déchargements de modules</li> </ul>
<b>Activités des systèmes</b>	<ul style="list-style-type: none"> <li>- démarrages ou arrêts des systèmes d'exploitations</li> <li>- surcharges du système</li> <li>- chargements ou déchargements de modules</li> <li>- activités matérielles (défaillances, connexions ou déconnexions physiques, etc.)</li> </ul>

Prioriser l'analyse des entrées de journal peut être difficile. Bien que certaines sources de log assignent leurs propres priorités pour chaque entrée, ces priorités utilisent souvent des échelles ou des notes incompatibles<sup>1</sup>, ce qui rend difficile la comparaison des valeurs de priorité.

En outre, les critères utilisés par les différents produits pour prioriser les entrées sont susceptibles d'être basés sur différents ensembles d'exigences, dont certains ou tous pourraient être incompatibles avec les exigences de l'organisation.

Les administrateurs sont donc contraints de se baser sur les thématiques décrites ci-dessus en fonction d'une combinaison de facteurs, y compris les suivants :

- Type d'entrée (par exemple, code de message 103, classe de message `CRITIQUE` ou `CRITICAL`;
- La nouveauté du type d'entrée (**Vérification de la redondance**);
- Source du journal;

---

<sup>1</sup>Par exemple : haut / moyen / bas, 1 à 5, 1 à 10

- 
- Adresse IP de la/les machine(s) hôte(s) (par exemple, adresse source sur une liste noire, adresse de destination d'un système critique, événements précédents impliquant une adresse IP particulière afin de faciliter la corrélation des événements)
  - L'heure du jour ou le jour de la semaine choisi ;
  - Fréquence de l'entrée (par exemple, 10 fois en 5 secondes).

La hiérarchisation des priorités pourrait également inclure l'utilisation de la corrélation pour fournir un contexte pour les entrées de journal afin qu'elles puissent être validées.

En supposant que le logiciel de détection d'intrusion basé sur l'hôte (HIDS) surveille un fichier et qu'il ait remarqué que ce fichier a subi une modification sur un système d'exploitation, si le système de journalisation de l'hôte contient une entrée d'audit indiquant que le fichier a été modifié avec succès et les données des deux entrées de journal sont corrélées entre elles, elles fourniraient une plus grande assurance d'une attaque réussie que n'importe quelle source de journal saurait seule faire valider une attaque.

Un autre exemple de l'utilisation de la corrélation comme facteur de priorisation consiste à utiliser des informations sur les vulnérabilités connues dans les systèmes d'exploitation et les applications installées de l'organisation pour attribuer une priorité plus élevée aux entrées de journal qui sont liés à ces vulnérabilités.

Les figures A.1 et A.2 expliquent un exemple de corrélation effectuée avec l'architecture mise en place.

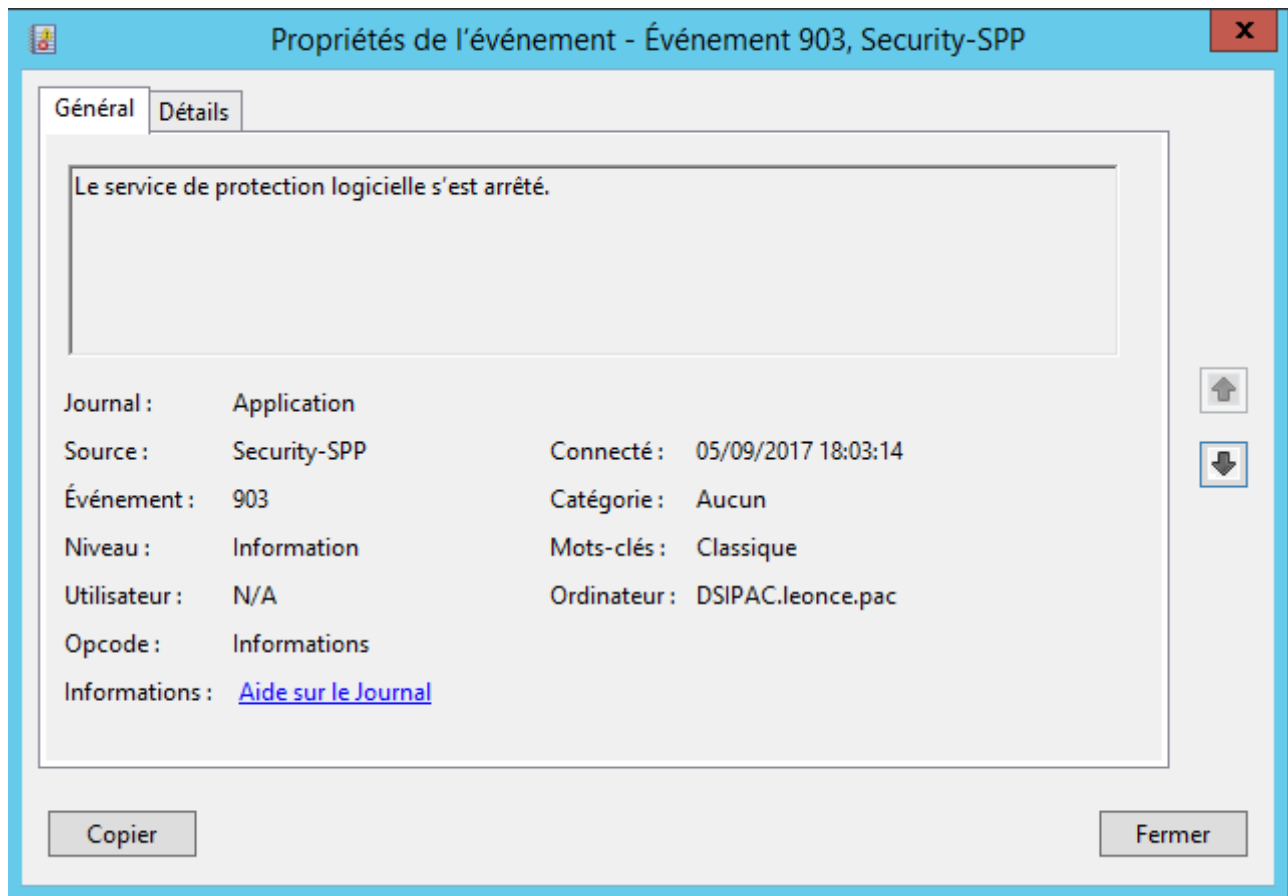


FIGURE A.1 – Événement consigné par Windows Eventlog

Le fichier log contenant une consignation de cet événement sera envoyé à Nagios Log Server pour analyse.

Field	Action	Value
<input checked="" type="checkbox"/> @timestamp ▼	Q Ø	2017-09-05T02:28:13.314Z
<input type="checkbox"/> @version	Q Ø	1
<input type="checkbox"/> Channel	Q Ø	Application
<input type="checkbox"/> EventID	Q Ø	903
<input type="checkbox"/> EventReceivedTime	Q Ø	2017-09-05 18:03:14
<input type="checkbox"/> EventTime	Q Ø	2017-09-05 18:03:14
<input type="checkbox"/> EventType	Q Ø	INFO
<input type="checkbox"/> Hostname	Q Ø	DSIPAC.leonce.pac
<input type="checkbox"/> Keywords	Q Ø	36028797018963970
<input type="checkbox"/> OpcodeValue	Q Ø	0
<input type="checkbox"/> ProcessID	Q Ø	0
<input type="checkbox"/> ProviderGuid	Q Ø	{E23B33B0-C8C9-472C-A5F9-F2BD FEA0F156}
<input type="checkbox"/> RecordNumber	Q Ø	1650
<input type="checkbox"/> Severity	Q Ø	INFO
<input type="checkbox"/> SeverityValue	Q Ø	2
<input type="checkbox"/> SourceModuleName	Q Ø	eventlog
<input type="checkbox"/> SourceModuleType	Q Ø	im_msvistalog
<input type="checkbox"/> SourceName	Q Ø	Microsoft-Windows-Security-SPP

FIGURE A.2 – Résultat de l’analyse faite par Nagios Log Server

Ce résultat de l’analyse sera notifié aux administrateurs dédiés au systèmes ou au serveur de supervision, Nagios Core.




# L'installation et le paramétrage de Nagios Log Server

## B.1 Le processus d'installation










---

La première étape est relative au téléchargement et l'importation d'une machine virtuelle sous laquelle tourne Nagios Log Server. (Voir figure B.1)

## nagioslogserver

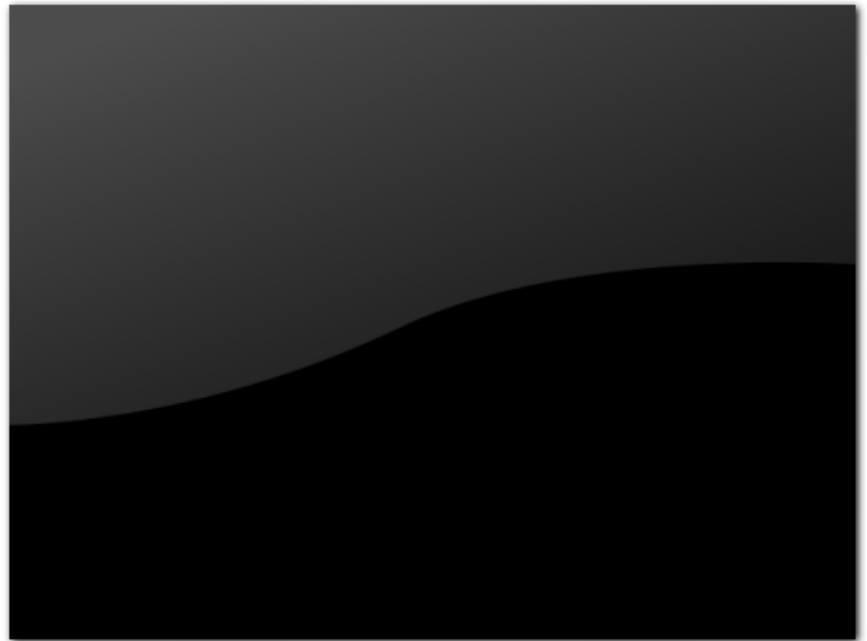
-  Power on this virtual machine
-  Edit virtual machine settings
-  Upgrade this virtual machine

### ▼ Devices

 Memory	2 GB
 Processors	1
 Hard Disk (SCSI)	100 GB
 CD/DVD (IDE)	Auto detect
 Floppy	Using drive A:
 Network Adapter	Bridged (Autom...
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

### ▼ Description

Première Instance de Nagios Log Server



### ▼ Virtual Machine Details

**State:** Powered off  
**Snapshot:** GNS3 Linked Base for clones  
**Configuration file:** F:\VMWare\Virtual Machines\nagioslogserver\nagioslogserver.vmx  
**Hardware compatibility:** Workstation 6.5-7.x virtual machine

FIGURE B.1 – Importation de la machine virtuelle de Nagios Log Server

Après démarrage, une adresse IP s'affiche sur la page d'accueil indiquant la localisation de l'interface de paramétrage et de visualisations des données qui seront collectées. (Voir figure B.2)

## Final Installation Steps

Almost done! You can create a fresh install or connect to existing cluster.

### New Install?

Is this a new install or are we adding a instance to an existing cluster?

☒ New Install ☐ Add Instance

### License Setup

Choose a trial license, enter your key, or [get a license now](#).

☐ Free 60 Day Trial ☒ I already have a key

License Key:

### Admin Account Setup

Choose or enter your admin profile and account settings. The default username is nagiosadmin, which you can change.

Username:

Password:

Confirm Password:

Email:

Language:

Timezone:

[Finish Installation >](#)

FIGURE B.2 – Finalisation de l'installation de Nagios Log Server

Il est donc définit un nom d'utilisateur, un mot de passe ainsi qu'une adresse électronique fonctionnelle. Á tout ceci s'ajoute la la synchronisation du fuseau horaire avec celui des machines qui enverront leurs données au serveur.

En cas d'ajout d'une instance, on reprend le même processus. Puis l'ajout de l'instance se fait sous l'autorisation de l'administrateur qui délivre un identifiant unique du Cluster<sup>1</sup>. (Voir figure B.3)

<sup>1</sup>Voir Glossaire

## Final Installation Steps

Almost done! You can create a fresh install or connect to existing cluster.

### New Install?

Is this a new install or are we adding a instance to an existing cluster?

☐ New Install ☒ Add Instance

### Connect to Existing Cluster

Enter your Cluster ID and hostname or IP address from one instance of the existing cluster. The Cluster ID may be obtained from Administration -> Cluster Status from any active Instance.

Hostname:

Cluster ID:

[Finish Installation >](#)

FIGURE B.3 – Ajout d’une instance de Nagios Log Server

## B.2 Le paramétrage de Nagios Log Server

Il sera présenté le processus d’installation et de paramétrage de l’agent de collecte NXlog, le paramétrage de la fonctionnalité d’aspiration des logs générés par les machines linux du parc et des équipements réseaux connectés au serveur de centralisation.

### B.2.1 L’installation et la configuration de l’agent de collecte sous Windows

- Après téléchargement<sup>2</sup> et installation de NXlog, le contenu du fichier de configuration est modifié<sup>3</sup> de Nagios Log Server par l’identification de la ligne dédiée à la valeur du paramètre `Host` puis son remplacement par l’adresse IP de Nagios Log Server. (Voir figure B.4)

<sup>2</sup><https://nxlog.co/system/files/products/files/348/nxlog-ce-2.9.1716.msi>

<sup>3</sup>Généralement localisé au : “C:\Program Files (x86)\nxlog\conf\nxlog.conf”.



```

50 <Output out>
51   Module om_tcp
52   Host NagiosLS
53   Port 3515
54
55   Exec $tmpmessage = $Message; delete($Message); rename_field("tmpmessage","message");
56   Exec $raw_event = to_json();
57
58   # Uncomment for debug output
59   # Exec file_write('%ROOT%\data\nxlog_output.log', $raw_event + "\n");
60 </Output>

```



```

50 <Output out>
51   Module om_tcp
52   Host 192.168.102.108
53   Port 3515
54
55   Exec $tmpmessage = $Message; delete($Message); rename_field("tmpmessage","message");
56   Exec $raw_event = to_json();
57
58   # Uncomment for debug output
59   # Exec file_write('%ROOT%\data\nxlog_output.log', $raw_event + "\n");
60 </Output>

```

FIGURE B.4 – Extrait de la configuration de NXlog sous Windows

- En console, on entre la commande suivante : `net start nxlog`. Le service NXlog démarre donc le processus de collecte et d'envoi des logs générés au composant **Logstash** de Nagios Log Server.

## B.2.2 La configuration du système de collecte des *Syslog* de Linux

Le seul prérequis est d'avoir installé rsyslog sur la machine puis une fois que les tests de connectivité sont validés entre la machine linux et Nagios Log Server, les commandes linux ci-après sont exécutées dans l'ordre avec un compte disposant d'un privilège d'administrateur. (Voir figure B.5)

```
[root@localhost ~]# curl -s -O http://192.168.102.108/nagioslogserver/scripts/setup-linux.sh
[root@localhost ~]# sudo bash setup-linux.sh -s 192.168.102.108 -p 5544
Detected rsyslog 5.8.10
Detected rsyslog work directory /var/lib/rsyslog
Destination Log Server: 192.168.102.108:5544
Creating /etc/rsyslog.d/99-nagioslogserver.conf...
SELinux is disabled.
rsyslog configuration check passed.
Restarting rsyslog service with 'service'...
Shutting down system logger: [ OK ]
Starting system logger: [ OK ]
Okay.
rsyslog is running with the new configuration.
Visit your Nagios Log Server dashboard to verify that logs are being received.
[root@localhost ~]#
```

FIGURE B.5 – Configuration effectuée sur une machine linux

### B.2.3 La personnalisation des paramètres d’alerte

La figure B.6 présente un exemple de personnalisation des paramètres contenus dans les notifications à envoyer par mail.

```
<p>La %alertname% est actuellement à l'état <b>%state%</b>.</p>

<p>L'alerte a été générée suivant les règles ci-après:<br>
<div>Période de recherche: %lookback%</div>
<div>Message d'avertissement: %warning%</div>
<div>Message critique: %critical%</div>
</p>
<p>
Voici le contenu complet de cette notification: <br>
<div>%output%</div>
<b>Nombre de logs par source : </b>
<div>%uniquehosts%</div>
</p>
<p>Visualisez le résultat des dernières recherches effectuées en %lookback% en
cliquant <a href="%url%">sur ce lien</a>.</p>
<br>
<b>Système de Centralisation et de Gestion des Logs du parc informatique du Port
Autonome de Cotonou</b>
```

FIGURE B.6 – Configuration effectuée sur une machine linux

---