**République Algérienne Démocratique et Populaire**

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**Université A/Mira de Béjaïa**

**Faculté des Sciences Exactes**

**Département d'Informatique**


# Mémoire de fin de cycle

*En vue d'obtention du diplôme de Master professionnel en Informatique.*
*Spécialité : Adminstration et Sécurité des Réseaux.*

Thème

---

# La solution de supervision Eyes Of Network. Cas d'étude : Sonatrach

---

Réalisé par :

*Mlle. SADOK Farah Yasmine et Mlle. RAHMANI Sara .*

*Evalué le 02/07/2023 devant le jury composé de :*

| | | |
|---|---|---|
| **Présidente** | **Dr. BACHIRI Lina** | **U. A/Mira Béjaïa.** |
| **Examinateur** | **Dr.OUZEGGANE Redouane** | **U. A/Mira Béjaïa.** |
| **Encadrant** | **Dr. MOKTEFI Mohand** | **U. A/Mira Béjaïa.** |

Année universitaire 2022/2023

## *Remerciements*

*D'emblée, nous tenons à exprimer notre profonde gratitude envers les personnes qui ont contribué de manière significative à la réalisation de ce mémoire.*

*Nous souhaitons exprimer notre reconnaissance à notre directeur de mémoire, Mr. MOKTEFI Mohand pour sa précieuse guidance, ses conseils éclairés et son soutien constant tout au long de ce travail.*

*Nos remerciements vont également à Mme BOUCHENNA Dalila et tout le personnel de la SONATRACH pour leur orientation et accueil sympathique durant la période de stage.*

*Nous remercions également les membres du jury d'avoir accepté d'examiner et de juger notre travail.*

*Nous exprimons notre gratitude envers nos camarades de classe qui ont partagé leurs idées et expériences avec nous. Leurs discussions stimulantes ont enrichi nos pensées et nous ont permis de considérer de nouvelles perspectives.*

*Enfin, nous sommes profondément reconnaissantes et nous remercions chaleureusement notre famille et nos amis pour leur soutien.*

# *Dédicace*

*En ce moment précieux où j'achève ce mémoire, je souhaiterais dédier ces mots empreints de gratitude et d'affection :*

*À ma mère, ma confidente et ma source d'inspiration. Je souhaite te remercier du fond du cœur pour tout ce que tu fais pour moi.*

*À mon père, modèle de persévérance, je t'adresse mes sincères remerciements.*

*À mes frères, « Yanis » et « Amine » compagnons de joie et de partage.*

*À mes grands-parents, mes tantes, mes oncles, mes cousins et cousines.*

*À ma meilleure amie « Sarah », ma sœur de cœur, à chaque étape de ce mémoire, tu étais là, prête à m'écouter, et me conseiller.*

*À mes chères copines « Serine », « Talia », « Kenza » et « Nihed » celles qui illuminent ma vie de rires et de précieux souvenirs.*

*À mon pilier et mon plus fervent supporter « Amine », Tu as su m'encourager lorsque j'en avais le plus besoin.*

*À mon professeur Mr. BELHOCINE Fayçal, guide précieux dans cette quête académique.*

*Je termine avec la personne qui a partagé tout le travail, « Sara », je tiens à te remercier pour ta contribution inestimable à ce mémoire.*

***FARAH YASMINE***

# *Dédicace*

*Avant tout je remercie Dieu de m'avoir donné la force et la patience de réaliser ce modeste travail que je dédie à :*

*Ma mère, ma Source d'inspiration , mon modèle dans la vie, à celle qui m'a tout donné, qu'elle trouve ici le témoignage de ma profonde reconnaissance.*

*L'âme de mon père, celui qui m'a toujours soutenu et cru en moi , que ce travail traduit ma gratitude et mon affection.*

*Mes frères Sofiane et Fawzi , à ma soeur Kenza, les personnes les plus chères à mon cœur ceux avec qui j'ai profiter pendant les moments de joie et avec qui j'ai affronter les moments de chagrin.*

*Mes neveux adam et Kylian que j'aime beaucoup.*

*Mon beau frère Fayçal et à ma belle soeur sadika qui font désormais partie de ma vie.*

*Ma grand mère, mes oncles, tantes, cousins et cousines.*

*Mes amis Melissa, Massilia, Yasmine, Tiziri, Celia, Lyna, Nihad et Selma qui m'ont toujours soutenu et cru en moi.*

*Mon professeur Mr. BELHOCINE Fayçal, guide précieux dans cette quête académique.*

*La dernière et pas des moindres à ma binôme Farah qui à partagé avec moi la réalisation de ce mémoire.*

***SARA***

# Table des matières

# Table des figures

# Liste des tableaux

# Liste des abréviations

| | |
|---|---|
| **ASI** | Asynchronous Serial Interface |
| **EON** | Eyes Of Network |
| **FTP** | File Transfer Protocol |
| **GNS3** | Graphical Network Simulator 3 |
| **GNU** | GNU's Not Unix |
| **GPL** | General Public Liicense |
| **HTML** | HyperText Markup Language |
| **ICMP** | Internet Control Message Protocol |
| **IEF** | Internet Engineering Task Force |
| **ITIL** | Information Technology Infrastructure Library |
| **IMAP** | Interactive Message Access Protocol |
| **IP** | Internet Protocol |
| **LAN** | Local Area Network |
| **MIB** | Management Information Base |
| **MN** | Managed Node |
| **MYSQL** | My Structured Query Language |
| **NT** | New Technology |
| **NMS** | Network Management System |
| **OID** | Object IDentifier |
| **OSI** | Open System Interconnection |
| **PDU** | Protocol Data Unit |
| **PHP** | HyperText Preprocessor |
| **PING** | Packet INternet Groper |
| **POP** | Post Office Protocol |
| **RFC** | Request For Comment |
| **RPM** | RedHat Package Manager |
| **SI** | System Information |
| **SMTP** | Simple Mail Transfer Protocol |
| **SNMP** | Simple Network Management Protocol |
| **TCP** | Transmission Control Protocol |
| **UDP** | User Datagram Protocol |
| **VLAN** | Virtual Local Area Network |
| **VTP** | VLAN Trunking Protocol |
| **WAN** | Wide Area Network |
| **WMI** | Windows Management Instrumentation |

# Introduction générale

De nos jours, le domaine des réseaux informatiques est au cœur des infrastructures technologiques. Les entreprises et les organisations dépendent de plus en plus de réseaux fiables et performants pour leurs opérations quotidiennes. Cependant, même avec l'avancée des technologies les plus sophistiquées, les problèmes de perte de données demeurent une réalité inévitable qui peut considérablement compromettre la fiabilité et les performances d'un réseau.

Dans ce contexte, la supervision des réseaux informatiques est apparue et joue un rôle essentiel pour garantir leur bon fonctionnement et leur sécurité. Elle consiste à surveiller en temps réel les activités et les performances du réseau afin d'identifier les anomalies et de prendre des mesures correctives. Ainsi, les administrateurs réseau peuvent anticiper les problèmes, minimiser les interruptions de service et optimiser les performances globales. Donc, Comment cette supervision joue-t-elle un rôle clé dans l'amélioration de la disponibilité ? Quels sont les avantages et les limitations spécifiques de cet outil de supervision Eyes Of Network par rapport à d'autres solutions disponibles sur le marché ?

Multiples logiciels permettent de réaliser ces tâches, telle que zabbix, shinken,Eyes Of Network et d'autres payant telle que PRTG Network Monitor, Cisco Prime.

Dans le cadre de ce mémoire de fin d'étude, nous allons nous intéresser spécifiquement à la supervision d'un réseau avec l'outil Eyes of Network. Notre objectif est visualiser l'efficacité de cet outil dans l'amélioration des performances et de la fiabilité du réseau supervisé. Nous chercherons à comprendre comment Eyes of Network peut contribuer à la détection précoce des incidents et à la ré-

solution rapide des problèmes.

Pour atteindre nos objectifs, nous suivrons une méthodologie rigoureuse qui comprendra la configuration de l'outil Eyes of Network dans un environnement de test représentatif au sein de l'entreprise de Sonatrach, la collecte de données pertinentes, l'analyse des résultats et la discussion approfondie des conclusions obtenues.

Pour mener à bien ce travail, nous avons organisé notre mémoire en quatre chapitres :

Nous verrons dans un premier temps les fondements sur lesquels la supervision se base, ses objectifs, ses principes, ainsi que les différents standards et le protocole qui permet la supervision d'infrastructures réseaux(chapitre 1) , nous allons également présenter l'organisme d'accueil de la SONATRACH avec la problématique posée de son réseau ainsi que la solution proposée pour la résoudre(chapitre 2) et par la suite nous ferons une présentation détaillée de la solution retenue (chapitre3) ,pour conclure on vas modéliser et implémenter notre solution de supervision ainsi que les étapes de configuration mises en place (chapitre 4).

Tout bien considéré, une conclusion générale sera présentée, résumant les éléments clés qui ont été abordés dans ce mémoire, ainsi que des perspectives potentielles pour ce projet.

# Chapitre 1

# Généralités sur la supervision

## 1.1 Introduction

Avec l'augmentation des réseaux et l'importance prédominante de ceux-ci dans le monde des affaires, la nécessité de surveiller la qualité et l'état du réseau en temps réel devient rapidement une priorité. C'est dans ce but que le concept de supervision d'un réseau est apparu maintenant il y a une vingtaine d'années.

Dans le cadre de ce chapitre nous allons présenter la supervision dans sa généralité, le moniteur de supervision le plus répondu (Nagios), et pour finir nous procéderons à une étude approfondie du protocole SNMP.
Cela nous aidera à bien comprendre le principe de fonctionnement du logiciel Eyes Of Network (EON).

## 1.2 Définition de la supervision

La supervision (ou monitoring) implique la surveillance du système et la récupération d'informations sur son état et son comportement, ce qui peut être fait par le biais d'interrogations périodiques ou d'un retour actif des périphériques réseau eux-mêmes. La plus grande préoccupation des administrateurs est le temps d'arrêt [12].

### 1.2.1 Objectifs et avantages de la supervision

— Surveillance du système d'information.

— Une information précise sur l'état du réseau et des applications.

— Visualisation de l'architecture du système.

— Déclenchement des alertes en cas de problème.

— Prendre des mesures en fonction des alertes.

— Réduction des attaques entrantes.

— Augmentation de la sécurité [4].

### 1.2.2 Pourquoi et comment superviser ?

« Si quelque chose peut mal fonctionner, ça ira inévitablement mal un jour ». Partant de ce constat, nous avons fait le choix d'une supervision qui permet de prévoir d'éventuelles pannes et de vérifier rapidement l'état et les performances des équipements informatiques [13].

De nombreuses solutions sont disponibles, certaines sont dédiées à la supervision des composantes du SI, d'autres sont plus globales. Une distinction est généralement faite par le nombre de paramètres disponibles et la granularité de leur analyse. Cependant, cette description ne doit pas empêcher les administrateurs de lire les tableaux de bord et les résumés. En revanche, il doit avertir d'un fonctionnement normal ou anormal [13].

Le fonctionnement est simple, des agents sont placés sur les équipements à surveiller, un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs par la suite une collecte de données active ou passive par un seul superviseur sera faite [13]. Cette acquisition se fera automatiquement grâce au protocole SNMP présent sur la plupart des parcs informatiques.

### 1.2.3 Les différents types de supervision

Ci-dessous nous énumérons les différents types de supervision existant[14] :

**a) La Supervision système :**
Elle comprend la surveillance des réseaux, des infrastructures et des machines des systèmes d'information (processeurs, mémoire, stockage).

**b) La supervision applicative :**
Cela comprend la surveillance des applications et des logiciels (bases de données, serveurs Web, etc.).

**c) La supervision Métier :**
Elle va consister à surveiller les processus métiers de l'entreprise (qui est un agrégat des indicateurs système, applicatif).

**d) Supervision de la sécurité :**
Cela comprend la surveillance des attaques potentielles sur les systèmes d'information (virus, intrusions).

**e) Supervision des performances réseau :**
Elle surveille les performances du réseau, notamment les temps de réponse, la latence, la bande passante, les congestions et les problèmes de connectivité.

### 1.2.4 Moyens de supervision

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes[7] :

a. **Supervision active :**
La supervision active est la plus classique. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Cette méthode est composée de trois étapes :
• Le serveur envoie une requête vers la ressource supervisée.
• La ressource répond à la requête du serveur.
• Le serveur analyse l'information et détermine un état pour la ressource.

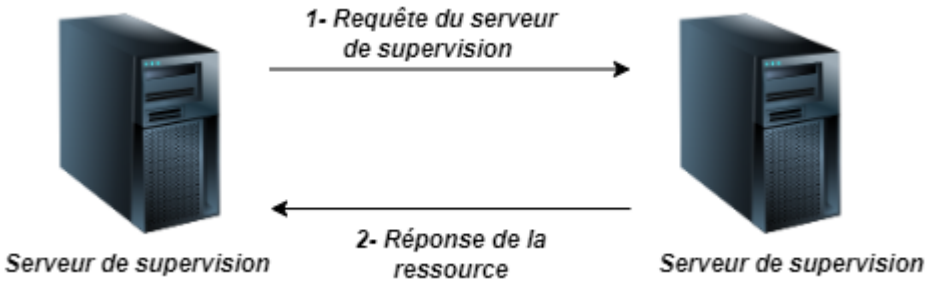



FIGURE 1.1 – Echange de messages dans une supervision active.

Cette méthode est la plus utilisée. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse. Les deux principaux protocoles de supervision active sont :
• Le protocole SNMP est le standard en matière de supervision active. Il est largement adopté et utilisé.

• Le protocole WMI (Windows Management Instrumentation) est un standard de supervision pour les systèmes Microsoft Windows.

b. **Supervision passive :**

La supervision passive l'est du point de vue du serveur de supervision : ce sont les ressources supervisées qui transmettent des alertes au serveur de supervision :

• La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision.

• Le serveur de supervision reçoit l'alerte et la traite.

• L'échange est unidirectionnel.

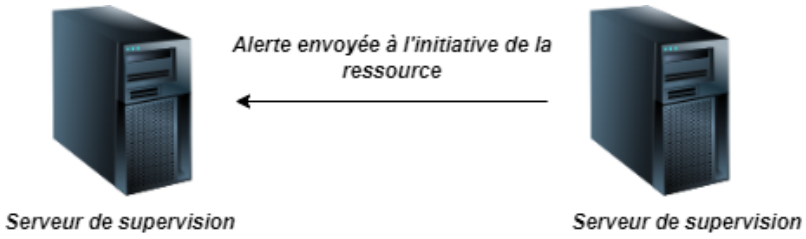



FIGURE 1.2 – Échange de messages dans une supervision passive.

La supervision passive présente des avantages en termes d'efficacité des ressources, mais elle est moins fiable en ce qui concerne la garantie de l'état correct des ressources supervisées. Elle est donc généralement utilisée en complément de la supervision active pour recevoir des alertes spécifiques, comme les traps SNMP.

### 1.2.5 Les moniteurs de supervisions

La supervision d'un réseau est devenue facile de nos jours car le monde de la surveillance regorge de logiciels. Fiable et sécurisé, ces logiciels qui existe sur le marché de la réglementation permettent d'effectuer des vérifications sur les machines et les services sur les réseaux locaux et distants, de collecter et de vérifier les résultats des tests de supervisions envoyés par les agents de supervision et d'alerter les administrateurs réseaux [2].

En se basant sur le coût d'achat de ces logiciels, ils peuvent être divisés en deux catégories :

**a) Les moniteurs de supervision payant :**

Les moniteurs de surveillance payants sont fournis par des éditeurs de logiciels qui, dès le début des réseaux, ont rapidement compris que la surveillance serait essentielle au succès des systèmes informatiques et un atout pour leurs entreprises. C'est pourquoi les entreprises n'hésitent pas à investir dans une solution de monitoring. parmi lesquels on peut citer [15] :

**HP OpenView :** c'est un logiciel qui est utilisé pour surveiller et gérer les performances et l'état des équipements du réseau, tels que les serveurs, les routeurs, les commutateurs, les pare-feu, les applications et les services.

**IBM Tivoli Monitoring :** c'est un logiciel conçu pour aider les entreprises à surveiller et gérer les matériels et les logiciels essentiels notamment les systèmes d'exploitation, les bases de données et les applications sur des environnements répartis.

**b) Les moniteurs de supervision libre :**

Les moniteurs de supervision libre sont des logiciels proposés gratuitement par des développeurs qui cherchent à se faire connaître à travers leurs produits en œuvrant dans le social. Parmi ces logiciels on peut citer [10] :

**Nagios :** C'est le moniteur de supervision le plus rependu parmi les logiciels open source et est suivi par toute une communauté de développeurs. Il permet la supervision du réseau et des systèmes.

**ZABBIX :** c'est un moniteur qui est beaucoup plus orienté du côté de la supervision système. Il a une architecture tout-en-un avec des agents dédiés que l'on doit installer sur les éléments distants. Il est facile à installer et à configurer.

**FAN :**Fully Automated Nagios est une distribution GNU/Linux basée sur la distribution CentOS. Son objectif était de fournir une installation de Nagios garnie de tous les outils que met à disposition la communauté Nagios. FAN était distribuée sous forme d'image disque [5].

**Shinken :** Est une application permettant la surveillance système et réseau. Elle

surveille les hôtes et services spécifiés, alertant lorsque les systèmes vont mal et quand ils vont mieux. C'est un logiciel libre sous licence GNU AGPL. Elle est complètement compatible avec le logiciel Nagios et elle a pour but d'apporter une supervision distribuée et hautement disponible facile à mettre en place.
**Eyes of network :** Est une solution open source de supervision . Elle offre une interface web conviviale et des fonctionnalités avancées, permet aux utilisateurs de bénéficier d'une solution complète et fiable pour superviser leurs infrastructures, détecter les anomalies et générer des rapports détaillés.

Ce sont ces mêmes produits qui seront soumis à une comparaison(voir chapitre 3).

### 1.2.6 Principe de fonctionnement de NAGIOS

Nagios est un moteur d'ordonnancement de vérifications diverses et variées. Ces dernières, dont le développement est séparé du noyau moteur, sont assurées par des plugins. La relation entre le moteur et les plugins est assurée d'une part par la configuration de Nagios afin que ce dernier sache quelles vérifications lancer et sur quelles machines. D'autre part, cette relation est garantie par la sortie retournée du plugin sous la forme d'un code retour. Ce code sera accompagné éventuellement d'un petit message décrivant le déroulement de l'exécution (dans le but d'aider l'utilisateur à faire le bon diagnostic en cas de problème). Ce sont donc ces états qui seront ensuite remontés au moteur qui prendra les décisions et lancera les actions adéquates et préalablement programmées [3].

Le code retour fourni par l'exécution du plugin est décrit dans le tableau ci-dessous.

| Code de retour | Etat de l'hôte | Etat du service | Description |
|---|---|---|---|
| 0 | UP | OK | Service Vérifier et fonctionne correctement |
| 1 | UP/DOWN | WARNING | Service vérifier ne mais fonctionne pas |
| 2 | DOWN | CRITICAL | Le plugin n'a même pas pu être vérifié |
| 3 | DOWN | UNKNOWN | incapable de vérifier l'état de l'hôte ou du service |

TABLE 1.1 – Correspondance de retour-état.

### 1.2.7 Le rôle des plug-ins

Plug-ins sont des programmes informatique ayant pour but de compléter un logiciel hôte, afin de lui apporter de nouvelles fonctionnalités ,ils sont également open source.

leurs rôle est d'ordonnancer les vérifications sur les éléments à superviser et de lancer une alerte si besoin [3] .

Leur conception est très simple. Cette facilité d'adaptation permet aux non-développeurs d'apporter leur pierre à l'édifice ,elle a un autre avantage majeur : elle permet de capitaliser sur les scripts de vérification déjà mis au point et utilisés par les administrateurs avant la mise en place de Nagios [3].

Nagios permet également de définir des plug-ins qui vont alerter les utilisateurs en cas de problème, ce qui permet d'être inventif en matière d'avertissement [3].

### 1.2.8 Les principaux plug-ins utilisés par Nagios

• **check_disk :** Vérifie l'espace occupé d'un disque dur.
• **check_http :** Vérifie le service "http" d'un hôte.
• **check_ftp :** Vérifie le service "ftp" d'un hôte.
• **check_mysql :** Vérifie l'état d'une base de données MYSQL.
• **check_nt :** Vérifie différentes informations (disque dur, processeur ...) sur un système d'exploitation Windows.
• **check_nrpe :** Permet de récupérer différentes informations sur les hôtes.
• **check_ping :** Vérifie la présence d'un équipement, ainsi que sa durée de réponse.
• **check_pop :** Vérifie l'état d'un service POP (serveur mail).
• **check_snmp :** Récupère divers informations sur un équipement grâce au protocole SNMP.

Il est également possible de créer son propre plugin. Dans ce cas, il faudra les créer de la sorte que celui renvoie à Nagios :
• L'état du résultat (OK, CRITICAL, DOWN, UP, ...).
• Une chaine de caractères (pour donner le détail du résultat).

## 1.3 Définition de SNMP

SNMP (Simple Network Management Protocol) est un protocole simple de gestion de réseau développé par un groupe de travail de l'IETF dans le cadre de la définition d'un système de gestion pour les réseaux. Il fournit un moyen de surveiller et de contrôler les périphériques réseaux, ainsi que de gérer les configurations, la collecte de statistiques, les performances et la sécurité [1].

Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau. Plusieurs versions se sont succédées dans le temps dont les principales sont : SNMPv1 (1990), SNMPv2 (1993) et SNMPv3 (1999). Il se situe au niveau de la couche application et de la couche transport du modèle TCP/IP et permet le dialogue entre la station d'administration et les équipements dotés d'agent SNMP [1]. Il utilise le protocole UDP (User Datagram Protocol), qui nécessite beaucoup moins de ressources que le protocole TCP. Il utilise également un paquet pour envoyer une seule opération de demande ou de réponse, de sorte que le protocole lui-même est sans état [1].

Deux types de communication sont effectués par SNMP, le premier est lorsqu'un manager envoie des requêtes à un agent. Il peut s'agir de requêtes de type « get », dans ce cas, le manager veut récupérer des informations auprès d'un agent. Si les informations doivent être modifiées, une requête « set » est envoyée. Un autre type de communication est celui où un agent souhaite informer un responsable d'un problème. Dans ce cas, une trap SNMP est envoyé, l'agent doit connaître l'adresse IP du manager à qui envoyer l'information. Celui-ci doit être à l'écoute des traps SNMP et doit réagir au problème [1].

Voici une illustration des types de communication SNMP possibles :

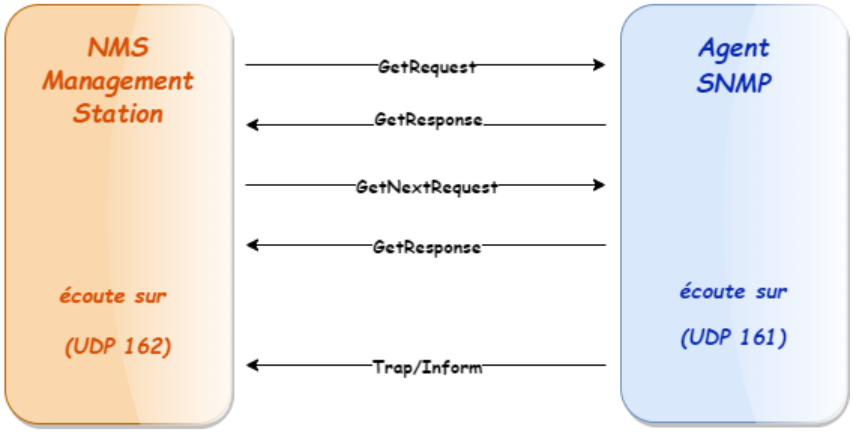



FIGURE 1.3 – Représente une communication SNMP.

### 1.3.1 Encapsulation du message SNMP

La couche application envoie l'ensemble de la trame aux couches inférieurs pour être encapsulée et transformée en datagrammes, puis en une trame IP jusqu'à la couche réseau [1].

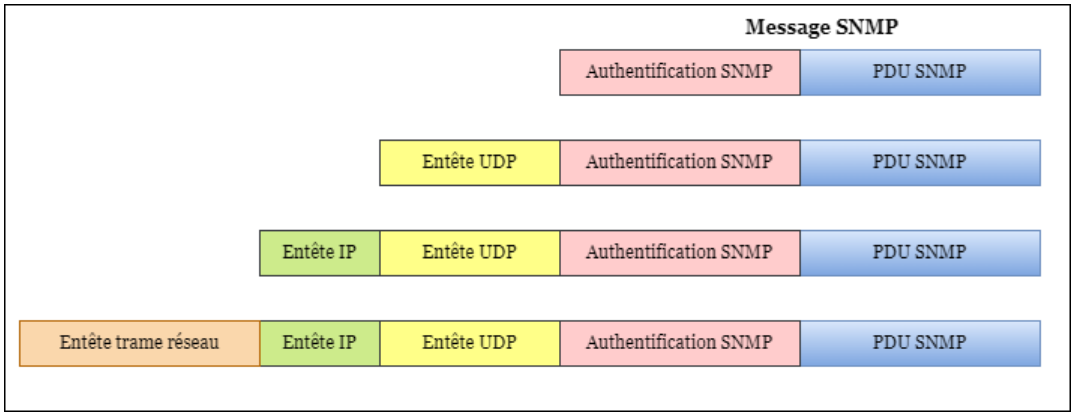



FIGURE 1.4 – Encapsulation du message SNMP.

### 1.3.2 Les Versions du protocole SNMP

• **SNMPv1 :** C'est la première version du protocole SNMP qui a été très utilisée et qui l'est encore, mais qui a un défaut majeur, une sécurisation très faible. Il n'y a pas de cryptage des données et aucune authentification, car elle est basée uniquement sur la chaine de caractère appelée "communauté"[6].

• **SNMPv2 :** C'est un protocole révisé, qui comprend les améliorations de SNMPv1 dans différents domaines tels que les types de paquets, les ´éléments de structure MIB et les requêtes protocolaires MIB (GETBULK et INFORM). Cependant ce protocole utilise la structure d'administration de SNMPv1 (à savoir "communauté") d'où le terme SNMPv2c. Cette version est toujours restée expérimentale et a laissé place à la version 3 [6].
• **SNMPv3 :** Cette version permet le cryptage des données. Il permet également aux administrateurs de spécifier des exigences d'authentification différentes sur une base granulaire pour les gestionnaires et les agents. Cela empêche l'authentification non autorisée et peut éventuellement utiliser le chiffrement pour les transferts de données [6].

### 1.3.3 Les composants de SNMP

• Des nœuds de réseau administrables qui peuvent être contrôlés à distance via SNMP. Une implémentation spécifique d'un moteur SNMP, qu'elle soit logicielle ou matérielle, est appelée agent [1].
• Au moins une unité SNMP composée d'applications avec lesquelles les agents peuvent être gérés. Cette unité est appelée un Manager [1].
• Un protocole avec lequel l'agent et le manager peuvent échanger des informations : le protocole de gestion de réseau simple (SNMP) [1].
• Une structure d'information bien définie, afin que les Managers et les agents puissent se comprendre : la base d'informations de Management Information Base (base d'informations de gestion) ou en bref, MIB [1].

### 1.3.4 Le fonctionnement de SNMP

Le protocole SNMP fonctionne au niveau 7 du modèle OSI, mais se situe directement au-dessus dUDP. Il fonctionne sur un modèle client-serveur, où il n'y a qu'un seul client, la station d'administration (NMS = Network Management Station) et de nombreux serveurs (chaque agent SNMP), le client interrogeant les serveurs pour récupérer les informations. Chaque agent est placé sur un nœud du réseau « administrable » (MN : Managed Node). Ces nœuds peuvent être soit des hôtes (stations de travail ou serveurs), soit des éléments

dinterconnexion (switchs, hubs, routeurs), soit des supports physiques (câbles) [1].

Le protocole SNMP fonctionne sur le principe des requêtes-réponses. Des alertes asynchrones peuvent être générées par des agents SNMP lorsqu'ils veulent avertir les systèmes d'administration du réseau d'un problème [1].

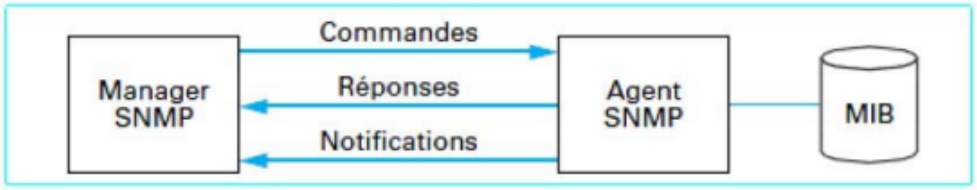



FIGURE 1.5 – Model Agent/Manager.

### 1.3.5 Le système de management de réseau

Le système de management de réseaux (NMS) appelé aussi gestionnaire SNMP est un ensemble de logiciels et de technologies qui permettent de surveiller, gérer et optimiser les réseaux informatiques.

Le NMS est composé de plusieurs éléments clés, notamment [3] :

1. **Les agents :** Ce sont des logiciels installés sur chaque équipement du réseau, tels que les routeurs, les commutateurs, les serveurs et les pare-feu.
2. **Le serveur de gestion :** C'est un logiciel installé sur un ordinateur ou un serveur dédié qui reçoit les données des agents et stocke les informations dans une base de données centralisée.
3. **Les protocoles de gestion :** Le NMS utilise des protocoles de gestion standardisés tels que SNMP, NetFlow, WMI et ICMP pour collecter des données de gestion à partir des équipements réseau.
4. **Les applications de gestion :** Le NMS est livré avec un ensemble d'applications de gestion intégrées pour surveiller et gérer les équipements réseau.

### 1.3.6 Management Information Base (MIB)

La MIB est une structure de données hiérarchique utilisée par le protocole

SNMP pour organiser les informations de gestion. La MIB est utilisée pour stocker et fournir des informations sur les équipements réseau, telles que les routeurs, les commutateurs et les serveurs. Elle contient une liste d'objets de gestion, chacun étant identifié par un numéro d'objet unique appelé OID (Object Identifier),ils sont organisés hiérarchiquement, créant une arborescence de données. Les objets de la MIB sont utilisés pour fournir des informations de gestion sur les équipements réseau, tels que les informations sur les interfaces réseau, les statistiques de trafic, les performances du système, les informations de sécurité et les événements système [1].

Les clients SNMP peuvent interroger les serveurs SNMP pour obtenir des informations sur les objets de la MIB en utilisant des requêtes SNMP. Les serveurs SNMP peuvent également envoyer des notifications SNMP pour informer les clients des événements de réseau importants [1].

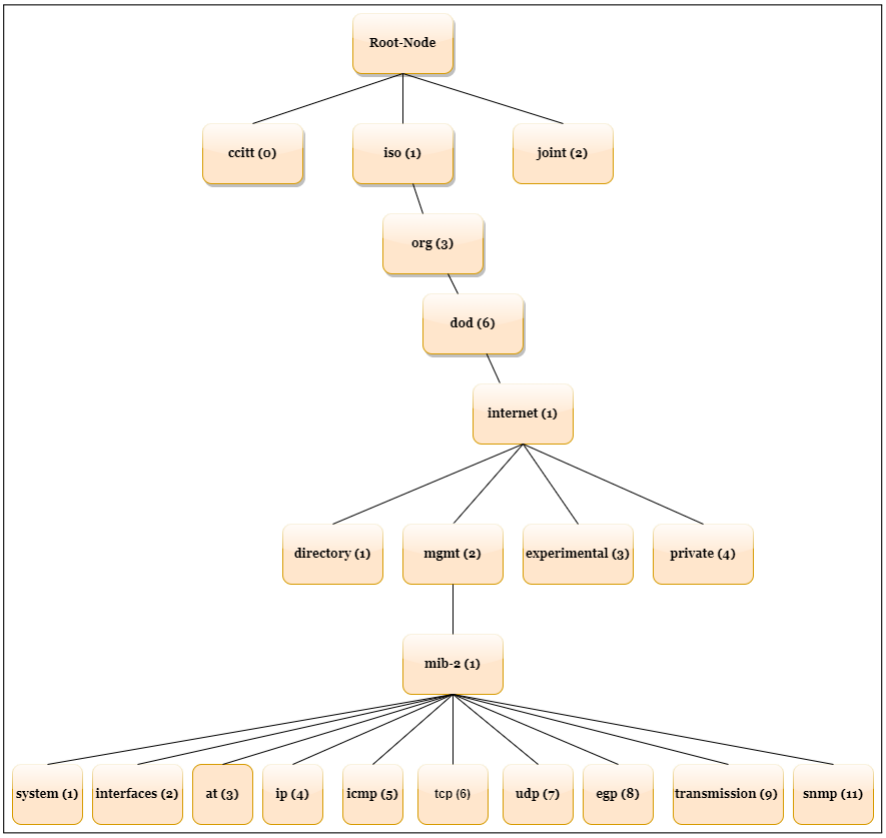



FIGURE 1.6 – Espace de noms SNMP en utilisant l'exemple de la MIB-II.

### 1.3.7 Les commandes SNMP

Les types de requêtes du manager SNMP vers l'agent SNMP sont [3] :
• **get-request :** Le Manager SNMP demande une information à un agent SNMP.
• **get-next-request :** Le Manager SNMP demande l'information suivante à l'agent SNMP.
• **set-request :** Le Manager SNMP met à jour une information sur un agent SNMP.
•**GetBulkRequest :** Ce type de message est utilisé pour demander une grande quantité de données en une seule requête.
Les types de requêtes de l'agent SNMP vers manager SNMP sont [3] :
• **trap :**L'agent SNMP envoie une alerte au Manager.
• **informRequest :**Ce type de message est utilisé pour notifier un gestionnaire SNMP qu'un événement important s'est produit sur un agent SNMP.
Les réponses ou informations de l'agent vers le manager sont :
• **get-response :** L'information a bien été transmise.
• **NoSuchObject :** Aucune variable n'a été trouvée.
• **NoAccess :**Les droits d'accès ne sont pas bons.
• **NoWritable :**La variable ne peut être écrite.

### 1.3.8 Les Traps SNMP

Les traps SNMP sont des messages d'alerte envoyés par les périphériques réseau, tels que les routeurs, les commutateurs et les serveurs, à un gestionnaire de réseau SNMP pour signaler des événements importants, tels qu'une panne du système, une erreur de transmission, une congestion du réseau, etc. Elles permettent aux administrateurs réseau de surveiller les événements critiques en temps réel et de réagir rapidement pour éviter les interruptions de service et les temps d'arrêt [1].

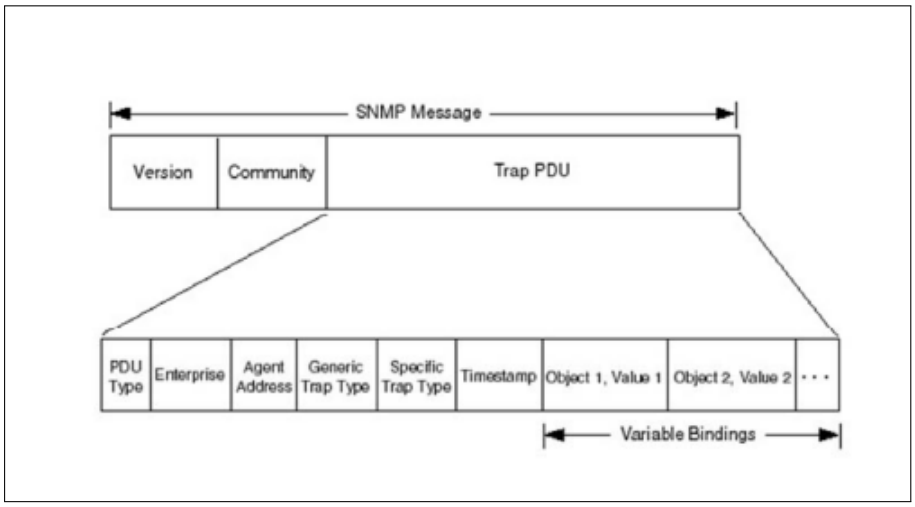



FIGURE 1.7 – format des message SNMPv1 de type trap.

• **Variablebindings :** Nom des variables avec leurs valeurs. Rq : Lors d'une opération Get, les valeurs sont NULL.
• **Enterprise :** Type de l'objet générant l'alarme.
• **Agent-addr :** Adresse de l'émetteur de l'alarme.
• **Generic-trap :** Identificateur de l'alarme.
• **Specific-trap :** Identificateur d'alarme spécifique.
• **Time-stamp :** Temps écoulé depuis la dernière réinitialisation de l'entité.

### 1.3.9 La surveillance avec SNMP

SNMP est défini avant tout pour surveiller et gérer les périphériques réseau. Cela signifie que l'on peut d'avoir non seulement un accès en lecture, mais aussi en écriture aux périphériques du réseau, de sorte que d'activer ou de désactiver un port spécifique d'un commutateur ou d'intervenir d'une autre manière [1].

Presque tous les périphériques compatibles avec le réseau qui peuvent également être adressés via TCP/IP peuvent gérer SNMP, et pas seulement les commutateurs et les routeurs. Pour les systèmes Unix il existe des deamons SNMP ; même les serveurs Windows contiennent une implémentation SNMP dans leur distribution standard, bien qu'elle doive être installée explicitement. Mais même les alimentations sans interruption (ASI) ou les capteurs compatibles avec le réseau sont compatibles avec SNMP [1].

Si on utilise Nagios, on ne peut pas éviter d'entrer en contact avec SNMP, car bien que nous ayons généralement un grand choix de techniques d'interrogation pour les systèmes Unix et Windows, lorsqu'il s'agit de composants spécifiques au matériel tels que les commutateurs, sans leur propre système d'exploitation sophistiqué, SNMP est souvent le seul moyen d'obtenir des informations du périphérique réseau [1].

# Conclusion

En conclusion, la supervision est un élément crucial pour garantir le bon fonctionnement des systèmes informatiques. SNMP et Nagios sont deux outils largement utilisés dans le domaine de la supervision offrant des fonctionnalités avancées pour la collecte de données, l'analyse et l'alerte.

SNMP fournit un protocole standard pour la collecte d'informations et la gestion des équipements réseau, tandis que Nagios est un logiciel de surveillance open source essentiel pour les entreprises qui cherchent à améliorer la disponibilité et la fiabilité de leur système informatique.

# Chapitre 2

# présentation de l’audit informatique et de l’organisme d’accueil

# 2.1 Introduction

Ce chapitre étudiera le réseau existant dans SONATRACH et les améliorations proposées.

D'abord, un aperçu de l'entreprise sera donné pour comprendre sa structure et ses objectifs. Ensuite, le réseau informatique et ses composants seront examinés afin de proposer des améliorations possibles.

# 2.2 Audit informatique pour les entreprises

## 2.2.1 Définition de l'audit informatique

C'est une analyse et une évaluation des systèmes, infrastructures, politiques et opérations informatiques. Une entreprise peut définir si les contrôles informatiques existants protègent les actifs de l'entreprise, garantissent l'intégrité des données et s'alignent sur les contrôles financiers et les activités de l'entreprise Grâce aux audits informatiques.

## 2.2.2 Objectif de l'audit informatique

— Évaluer les systèmes et les processus qui doivent protéger les données de l'entreprise.
— Identifier les risques qui pourraient compromettre vos informations et trouvez des solutions pour limiter ces risques.
— Surveiller la conformité des informations aux lois, politiques et normes de protection des données.
— Identifier les inefficacités dans des systèmes informatiques spécifiques.
— Vérifier la fiabilité et l'intégrité des informations.

## 2.2.3 Le processus de l'audit informatique

— **Planification :** Il s'agit d'une étape essentielle, car une mauvaise compréhension des procédures informatiques internes et une mauvaise évalua-

tion de l'effort et du temps requis peuvent conduire à des conclusions erronées et à une augmentation des coûts. Par conséquent, cette étape se termine par l'élaboration d'un plan d'audit détaillé.

— **Travail de terrain :** Cette étape peut prendre différentes formes, mais se fait généralement sur place. L'équipe d'audit identifie et analyse les principaux risques dans le processus et les systèmes d'audit.

— **Reporting :** Pendant et après l'audit, l'équipe doit documenter ses conclusions, notamment si certains contrôles sont inefficaces.

— **Suivi :** Les auditeurs internes ou externes s'assurent que les préconisations ou les plans d'action présentés dans les rapports d'audit sont suivis de manière appropriée et que les améliorations prévues sont effectivement mises en œuvre. L'audit se termine lorsque le suivi confirme que les améliorations proposées ont été correctement mises en œuvre.

## 2.3 Présentation de l'Organisme d'Accueil

### 2.3.1 Historique de SONATRACH

SONATRACH (Société Nationale pour le Transport et la Commercialisation des Hydrocarbures) a été créé le 31 décembre 1963 par le décret n°63/491, elle devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures".

SONATRACH est une entreprise publique algérienne, elle est classée la 1 ère entreprise d'Afrique, 11 ème parmi les compagnies pétrolières mondiales, 2 ème explorateur de GNL et 3 ème exportateur de gaz naturel.

Sa production globale (tout produit confondus) est de 202 millions de tonnes, ses activités constituent environ 30% du PNB (produit national brut) de l'Algérie, elle emploie 120 000 personnes.

Le 24/02 /1971, arriva la nationalisation du secteur des hydrocarbures, qui a conduit à une restructuration et une réorganisation efficace de la société qui a donné naissance à 18 entreprises parmi elles : NAFTAL, ENIP, ENGTP, ENAC, ASMIDAL, etc.


FIGURE 2.1 – Logo de l'entreprise SONATRACH.

## 2.4 Présentation de la direction régionale de Bejaia

### 2.4.1 Historique

L'historique de la DRGB remonte à 1959 lorsque la compagnie française des pétroles (CFP) et la société nationale de recherche et d'exploitation des pétroles en Algérie (SN REPAL) décédèrent le 12 aout 1957, la création de la société pétrolière de gérance (SOPEG).

Avec Arzew, Skikda, Ain Amenas et Haoud El Hamra, la direction générale de Bejaïa est l'une des régions couvrant l'activité de la branche transport par canalisation, la DRGB est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

### 2.4.2 Situation géographique

La DRGB est implantée dans la zone industrielle a l'entré et au sud de la ville de Bejaia, elle s'étend sur une superficie globale repartie comme suit :

— Terminal « sud et nord » Surface clôturée : 516 135 m².

— Surface ouverte : 7 832 m².

— Surface occupée par les bacs : 2 250 m².

— Hangar de stockage : 3 800 m².

— Surface couverte : 1 155 m².

— Surface clôturée : 19 841 m².
— Surface couverte : 300 m ².
— Surface occupée par les bacs de déballastage : 1 600 m².

### 2.4.3 Structure de la DRGB

La figure illustre les directions ainsi que les sous-directions de la DRGB centre informatique :

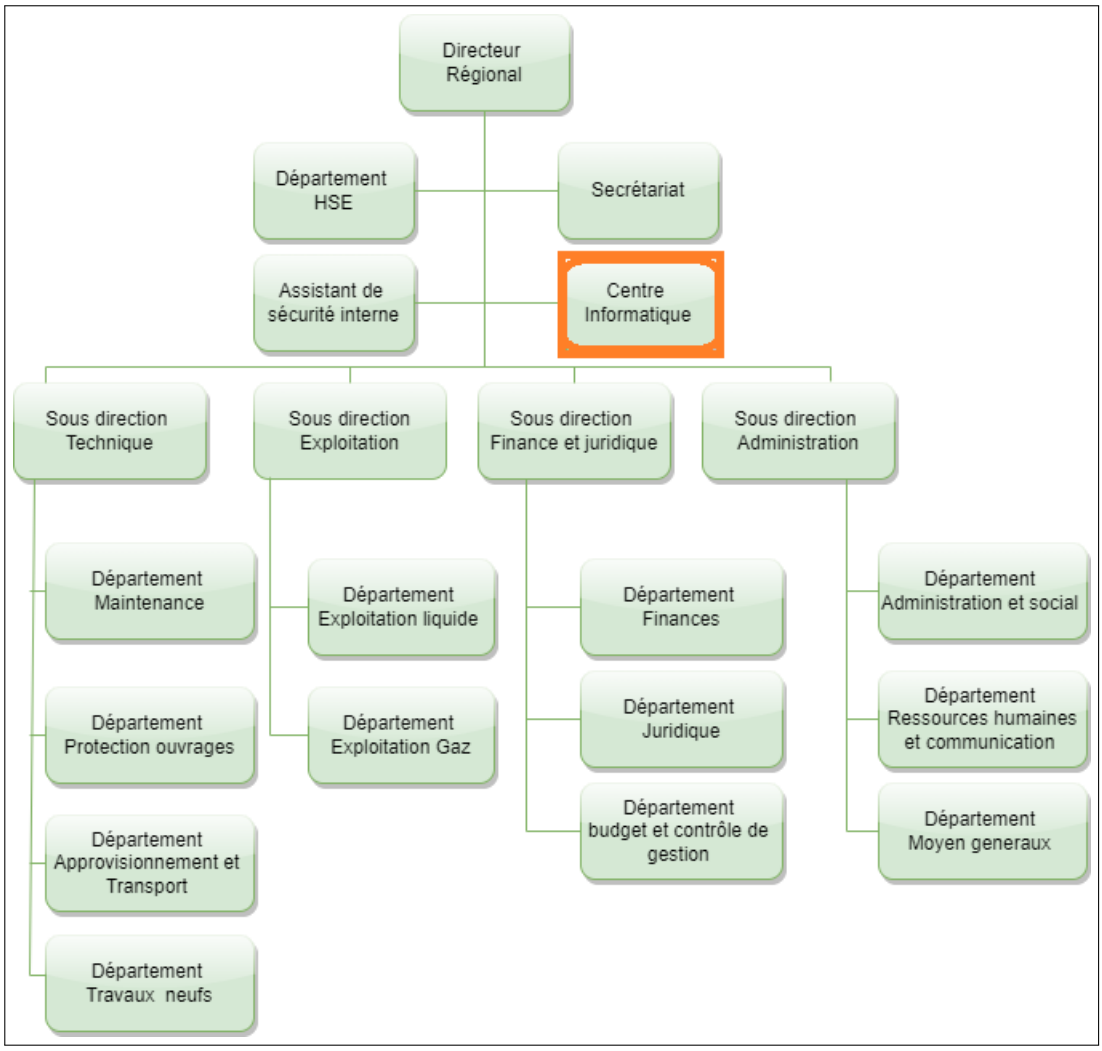



FIGURE 2.2 – Structure de la DRGB.

## 2.5 Présentation du centre informatique

Le centre informatique sert à regrouper les moyens d'exploitation et de développement des applications informatiques pour les différentes structures de RTC, il gère le réseau informatique interne. Il se constitue de trois services :

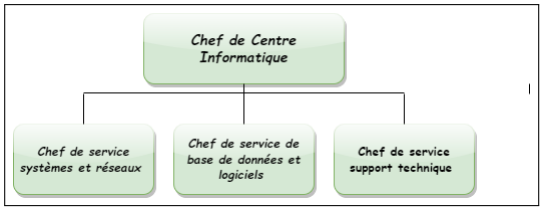



FIGURE 2.3 – Organigramme du centre informatique (RTC).

### 2.5.1 Service systèmes et réseau

Ce service est dirigé par un ingénieur système, un ingénieur système distribué et un ingénieur d'informatique industriel qui assure :

- **Système :**
  - Choix des équipements informatiques et logiciels de base.
  - Mise en œuvre des solutions matérielles et logicielles retenues.
  - Installation et configuration des systèmes.
  - Mise en œuvre des nouvelles versions de logiciels.
- **Réseau :**
  - Assurer le bon fonctionnement et la fiabilité des communications.
  - Assurer l'administration du réseau et organiser l'évolution de sa structure.
  - Etude et choix de l'architecture du réseau à installer et la participation à sa mise en place.
  - Définition des droits d'accès à l'utilisation du réseau.
  - Assurer la surveillance permanente pour détecter les pannes.

### 2.5.2 Service de base de données et logiciels

Ce service est dirigé par quatre ingénieurs systèmes d'information, qui assure :

— **Base de données :**

  — Conception des bases de données, optimisation et suivi des données informatiques.

  — Installation et configuration des systèmes.

  — Gestion de la sauvegarde, la restauration et la migration des données.

  — **Logiciel :**

  — Etude et conception des systèmes d'information.

  — Développement et maintenance des applications informatiques pour TRC.

  — Déploiement des applications et formation des utilisateurs.

### 2.5.3 Service de support technique

Ce service est dirigé par un chef de support technique. Il sert à installer les logiciels de gestion età assister les utilisateurs en cas des problèmes matériels ou logiciels.

## 2.6 Aspect réseau

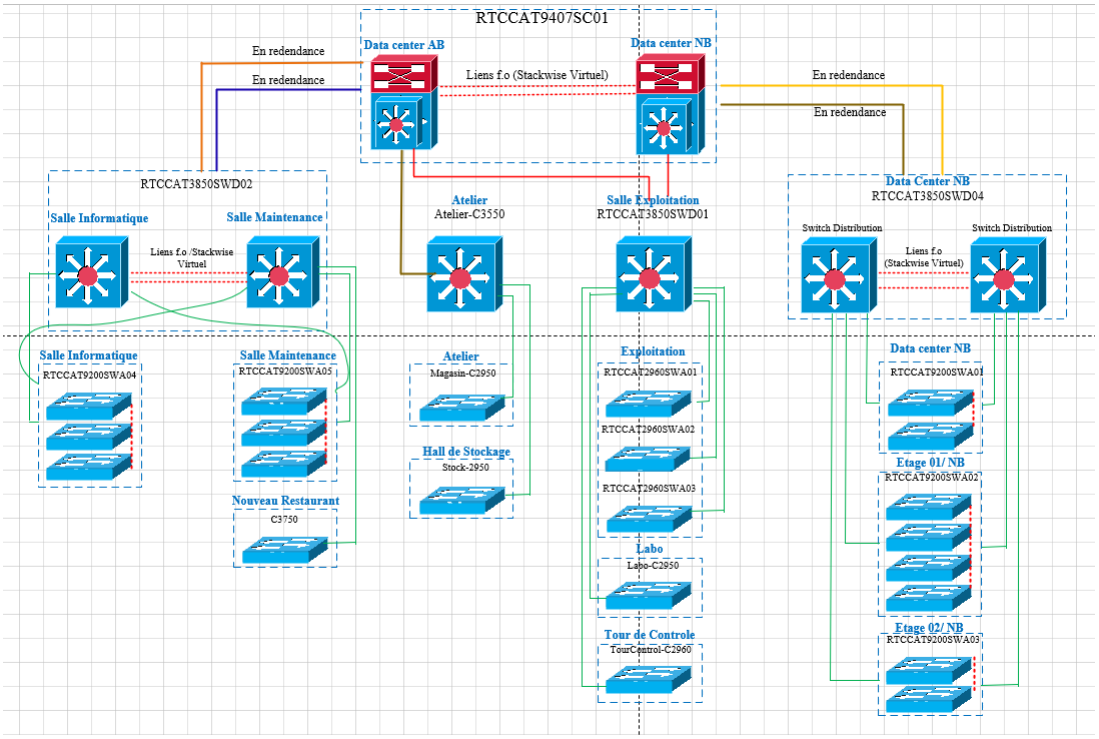



FIGURE 2.4 – La structure réseau de SONATRACH.

## 2.7 La structure hiérarchique du réseau SONATRACH

Afin de mieux répondre aux besoins des entreprises, la conception d'un réseau doit s'effectuer suivant un modèle hiérarchique (réseau commuté)

### 2.7.1 Le réseau commuté

Également appelé réseau de campus, utilisé pour les entreprises s'adaptent à ce mode de gestion des activités quotidiennes. La technologie permet le partage des ressources en temps réel entre plusieurs personnels distants. Le réseau prend en charge la qualité de service, sécurité renforcée, et des technologies sans fil.
Ce réseau est caractérisé par trois couches :

— **Couche accès :** Elle agit comme un terminal (ordinateur, imprimantes et téléphones IP) pour fournir un accès au reste du réseau. La couche d'accès peut comprendre des routeurs, des commutateurs, des ponts, concentrateurs et points d'accès sans fil. Sa principale fonction est de fournir un moyen, connecter et contrôler les appareils qui permettent la communication réseau.

— **Couche distribution :** Elle collecte les données reçues des commutateurs de la couche d'accès avant de les transférer à la couche cœur du réseau pour les livrer aux récepteurs. La couche de distribution gère le trafic réseau. Elle délimite le domaine de diffusion grâce à la fonction de routage entre un réseau local virtuel (VLAN) défini au niveau de la couche d'accès.

— **Couche Core :** C'est le réseau fédérateur, reliant plusieurs couches du réseau du campus, le but principal est d'assurer l'isolation des pannes et la connexion à haut débit du réseau.

### 2.7.2 Les commutateurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB utilise deux types de commutateurs :

1. **Des commutateurs intelligents** Sont des équipements réseau avancés qui sont capables de fournir des fonctionnalités de sécurité, de gestion, de surveillance et de contrôle avancées ainsi que le routage.
   Voici quelques exemples de ce type de commutateur dans le réseau de la DRGB.

   — **Catalyst 9407 :** Un commutateur haut de gamme. Il est conçu pour les réseaux de campus les plus exigeants en termes de bande passante, de sécurité et de haute disponibilité. Il offre une modularité élevée avec la possibilité de choisir différents modules pour ajouter des ports supplémentaires.

FIGURE 2.5 – Gamme catalyst cisco 9407.

— **Catalyst 3900 :** Un commutateur modulaire qui offre une performance élevée a. Il est conçu pour répondre aux besoins des entreprises de taille moyenne, offrant une haute densité de ports, et une sécurité avancée à un coût abordable.

FIGURE 2.6 – Gamme catalyst cisco 3900.

— **Catalyst 3850 :** Un commutateur empilable qui offre des capacités de commutation de couche 2 et de couche 3. Il est conçu pour les réseaux de campus de taille moyenne avec des capacités de convergence filaire et sans fil, une haute disponibilité et une sécurité avancée. Il offre une modularité réduite par rapport aux autres commutateurs de cette gamme, mais il est plus économique et plus facile à gérer.

FIGURE 2.7 – Gamme catalyst cisco 3850.

2. **Commutateur non intelligent** Ce type de commutateur ne permet pas de faire le routage. Le réseau de la DRGB contient :

— **Catalyst 2950 :** C'est une gamme de commutateurs CISCO, offrant une administration exceptionnelle et de nombreuses fonctionnalités avancées de qualité de service et de traitement des flux multicast.

FIGURE 2.8 – Gamme catalyst cisco 2950.

3. **Les routeurs utilisés dans le réseau de la DRGB** Le réseau de la DRGB contient les deux types de routeurs suivants :
   — **CISCO 1700 :** C'est une gamme de routeurs d'accès modulaires souples et sécurisés utilisée dans les réseaux WAN.
   — **CISCO 1941 :** C'est une gamme de routeurs à services intégré haut débit qui permet aux petits bureaux d'exploiter des services sécurisés simultanés comme le pare-feu, les VPN et les réseaux LAN sans fil.

## 2.8 Aspect sécurité

### 2.8.1 Serveur antivirus

Conçu pour identifier, neutraliser et éliminer les logiciels malveillants. Ceux-ci peuvent être basés sur l'exploitation d'une faille de sécurité, mais il peut également s'agir de programmes qui modifient ou suppriment des fichiers, qu'il s'agisse de documents utilisateur infectés ou de fichiers nécessaires au bon fonctionnement de l'ordinateur.

### 2.8.2 Serveur de filtrage web

Permet de bloquer l'accès aux sites Web au contenu inapproprié, ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont automatiquement mises à jour .

### 2.8.3 Serveur reporting

Il s'agit d'un outil de rapport complet et facile à utiliser qui évalue l'utilisation d'Internet par les employés de l'entreprise, identifiant tous les problèmes possibles d'accès à Internet ou d'utilisation de la bande passante du réseau en générant des rapports détaillés, des résumés ou des graphiques.

### 2.8.4 Firewall Juniper SSG 550

Est un dispositif de sécurité réseau qui permet de contrôler les flux de trafic entrants et sortants d'un réseau d'entreprise. Il offre une protection avancée contre les menaces en ligne, telles que les virus, les logiciels malveillants et les attaques de hackers.

FIGURE 2.9 – Firewall Juniper ssg 550.

Le pare-feu juniper ssg 550 illustré à la Figure contient un ensemble de règles structurées en trois zones comme suit :

— **La zone strust :** C'est la zone la plus fiable car elle autorise le trafic sortant et interdit le trafic entrant, c'est pourquoi RTC lui confie son réseau LAN.

— **La zone untrust :** Il s'agit d'une zone où le trafic entrant est autorisé et le trafic sortant est interdit.

— **La DMZ (Demilitarized Zone) :** Il s'agit de la zone tampon du réseau d'entreprise entre le réseau local et Internet derrière un pare-feu. Il s'agit d'un réseau intermédiaire qui regroupe des serveurs publics (DNS, HTTP, DHCP). Ces serveurs doivent être accessibles depuis le réseau interne de l'entreprise et, pour certains serveurs, également depuis le réseau externe. Le but est d'éviter toute connexion directe au réseau interne.

## 2.9 Aspect supervision

### 2.9.1 Cisco Prime

Cisco Prime est une plate-forme de gestion de réseau payante qui offre des capacités de supervision avancées pour les équipements de réseau Cisco.
Elle permet de surveiller en temps réel les performances, les configurations et les événements du réseau, afin de détecter les problèmes de manière proactive et de les résoudre rapidement avant qu'ils n'affectent les utilisateurs.

### 2.9.2 Eyes of network

Eyes of Network est une plateforme de supervision de réseau open source qui offre des fonctionnalités avancées de surveillance pour les infrastructures de réseau. Elle permet de surveiller en temps réel les équipements réseau tels que les routeurs, les commutateurs, les serveurs, les applications, les bases de données, etc., afin de détecter les problèmes de manière proactive. Eyes of Network fournit une interface graphique conviviale pour visualiser les informations de supervision, notamment les alertes, les événements et les performances.

## 2.10 Problématique

Après avoir analyser l'état actuel du réseau informatique de SONATRACH, nous avons soulevé les lacunes réseaux existantes, qui se résumer comme suit :

— L'adoption d'une ancienne version qui souffre d'un déficit de fonctionnalités essentielles constitue un véritable obstacle à l'efficacité des opérations.

— En cas de problème de fonctionnement, l'administrateur ne sera pas alerté, ce qui entrainera une perte de temps importante lors du diagnostic des pannes.

— Il ne permet pas de surveiller tous les services.

— L'utilisation de pnp4nagios pour les graphs.

## 2.11 Solution

Afin de résoudre les problèmes énumérés dans la problématique, nous suggérons les solutions suivantes qui permettront d'apporter des améliorations significatives :

— **La mise à niveau d'une nouvelle version :** La version 5.0 peut entraîner des limitations dans la gestion des processus, des lacunes dans la surveillance des performances, ainsi qu'une difficulté à répondre aux besoins en constante évolution de l'entreprise. Par conséquent, il devient impératif de mettre à jour le système vers une version 5.3 plus récente et complète, afin de bénéficier des fonctionnalités avancées, ainsi que d'un script d'exécution pour l'intégration de Grafana..

— **L'implémentation d'une solution de supervision globale offrant les avantages suivants :**

  — La mise en œuvre de la fonctionnalité d'alertes par courrier électronique.

  — L'ajout de nouveaux services à surveiller.

## 2.12 Conclusion

Dans ce chapitre nous avons présenté l'entreprise SONATRACH, on a ainsi présenté la DRGB ou nous avons suivi notre stage pratique qui nous a permis d'étudier l'entreprise en profondeur afin de comprendre ses lacunes et ses faiblesses, cette recherche nous a amenés à proposer des solutions pour surmonter ces problèmes.

# Chapitre 3

# Présentation de l’outil de supervision

## 3.1 Introduction

L'évolution constante des réseaux informatiques et la complexité croissante des infrastructures requièrent une supervision efficace pour garantir leur bon fonctionnement et leur sécurité. Cependant, choisir le bon outil peut être difficile. Dans ce chapitre, nous allons explorer Eyes of Network qui se présente comme une solution puissante et polyvalente.

Nous justifierons le choix de cette solution, une brief définition, ses principales caractéristiques, ses fonctionnalités ainsi que ses avantages et inconvénients.

## 3.2 Etudes comparatives des différents outils

Vu le nombre de solution de supervision existantes, nous avons pensées à faire une étude comparative de toutes ces solutions afin de choisir la mieux adaptée à notre demande.

Ci-dessous représente le tableau comparatif [16] :

| Critères | FAN | Nagios | Shinken | EyesOfNetwork | Zabbix |
|---|---|---|---|---|---|
| Licence | GPL | GPL | AGPL | GPLv2 | GPLv2 |
| Facilité d'installation | facile | difficile | moyen | facile | moyen |
| Configuration | facile | difficile | moyen | facile | difficile |
| Gestion des journaux et trace | NON | NON | NON | OUI | OUI |
| Envoie des mails d'alertes | OUI | OUI | OUI | OUI | OUI |
| L'outil est en français | NON | NON | NON | OUI | NON |
| Graphe | NON | NON | OUI | OUI | OUI |
| Cartographie | OUI | NON | NON | OUI | OUI |
| Communauté | limité | active | active | active | active |

TABLE 3.1 – Tableau comparatif des différentes solutions.

### 3.2.1 Raison du choix de Eyes Of Network

Eyes of Network (EON) est un choix judicieux par rapport aux autres outils de supervision pour plusieurs raisons. Tout d'abord, EON offre

une intégration avancée avec Nagios, l'un des systèmes de supervision les plus répandus et fiables. Cette intégration permet à EON de bénéficier de l'expertise de Nagios, ce qui facilite la configuration et l'extension de la solution.

De plus cette solution nous a convaincu du fait qu'elle intègre tout ce qui est nécessaire pour la supervision telle que Nagios, Nagvis, la métrologie Cacti, weathermap, la gestion d'un parc machine, Eonweb Etc.

En outre, EON se distingue par ses fonctionnalités de supervision avancées qui couvrent tous les aspects essentiels de la surveillance, tels que la surveillance réseau, la surveillance des serveurs, la surveillance des applications, la surveillance des performances, et bien plus encore.

Enfin, EON bénéficie d'une communauté active d'utilisateurs et de contributeurs, ce qui favorise l'échange d'expériences, le partage de bonnes pratiques et la résolution rapide des problèmes.

## 3.3 Définition de Eyes Of Network

EyesOfNetwork est une solution open source qui rassemble Processus ITIL pragmatiques (gestion de la disponibilité, capacité, incident, problèmes, etc.) [9].EON est une plateforme de supervision des réseaux informatiques qui permet d'obtenir une vision globale et détaillée de l'état et des performances des équipements réseau, des services et des applications qui y sont connectés, Il permet aux administrateurs système et aux professionnels de la sécurité de surveiller, gérer et optimiser les réseaux de manière proactive [11].

Il permet aussi de faire de la cartographie, de la métrologie et de générer des rapports, le tout centralisé dans une interface unique.

La solution Eyes of Network fonctionne sur le système d'exploitation linux CentOS édité par la société Red Hat [11].

### 3.3.1 Les caractéristiques de Eyes Of Network

Le "bundle" EyesOfNetwork est composé d'un système d'exploitation minimaliste incluant un ensemble intégré d'applications répondant aux différents besoins de supervision [9] :

— **GED (Generic Event Dispatcher) :** gestion multi sites et sécurisée des évènements.

— **Postfix :** est un serveur de messagerie qui permet d'envoyer des mails d'alerte.

— **Nagios :** est l'application qui va nous permettre de surveiller les équipements de notre architecture réseau.

— **Nagvis :** plugin permettant de visualiser des cartographies réseaux.

— **THRUK :** interface de supervision multibackend.

— **GRAFANA ET INFLUXDB :** gestion des performances.

— **Cacti :** logiciel permettant de mesurer la performance des éléments supervisés.

— **Weathermap :** plugin de Cacti permettant d'afficher une représentation graphique de l'état des liens réseaux.

— **EONweb :** est l'interface graphique de la solution qui centralise l'ensemble des outils.

— **SNMPTT :** traduction des traps SNMP.

— **GLPI :**gestion de parc et inventaire.

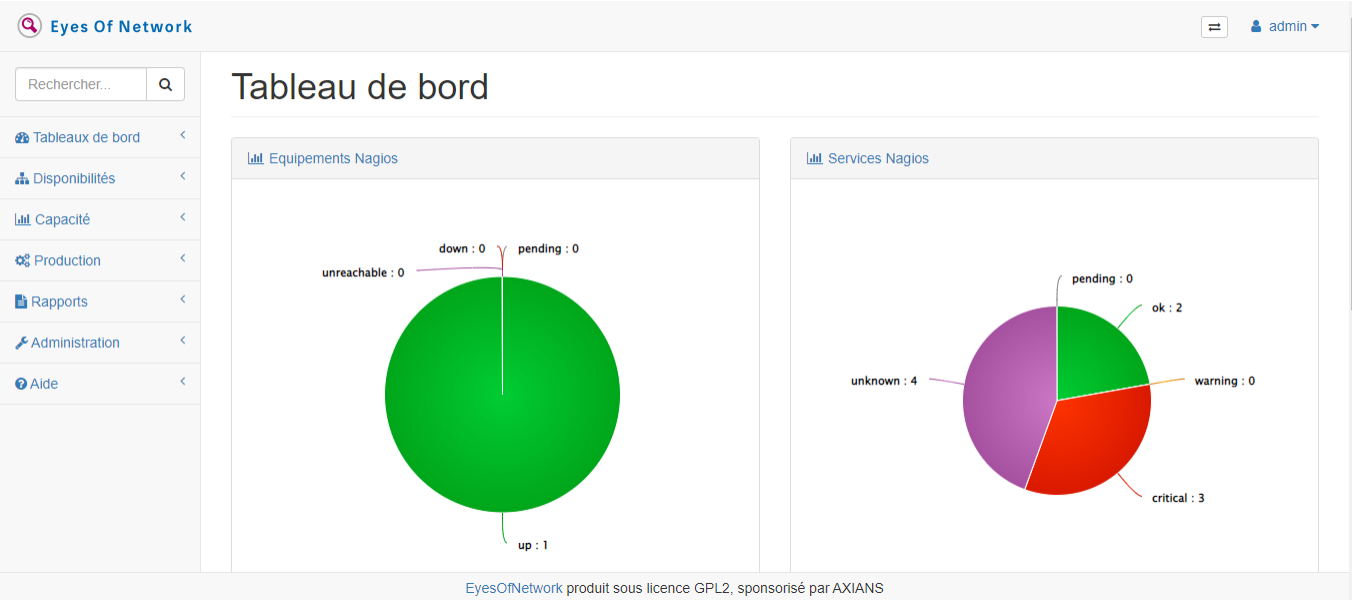



FIGURE 3.1 – plate-forme de Eyes of Network.

### 3.3.2 Fonctionnalités d'Eyes of Network

• **Surveillance complète :** Eyes of Network offre une surveillance globale de l'ensemble du réseau, permettant de détecter les dysfonctionnements, et les vulnérabilités potentielles [9].
• **Personnalisation des indicateurs :** L'outil permet de définir des indicateurs personnalisés en fonction des besoins spécifiques de l'infrastructure, offrant ainsi une flexibilité et une adaptabilité accrues [9].
• **Alerte et notification :** Eyes of Network est capable de générer des alertes en temps réel lorsqu'un événement anormal est détecté. Les administrateurs peuvent être informés via divers canaux, tels que des notifications par e-mail ou des messages d'alerte sur leur tableau de bord [9].
• **Analyse des performances :** Il offre des fonctionnalités d'analyse approfondie pour évaluer les performances du réseau, et prendre des mesures préventives pour optimiser les performances [9].
• **Génération de rapports :** Eyes of Network permet de créer des rapports détaillés sur l'état du réseau, les incidents passés, les tendances de performance et d'autres métriques clés. Ces rapports peuvent être

utilisés pour l'audit, la conformité réglementaire et la prise de décision [9].
• **Déployer facilement :** plusieurs modes d'installation sont disponibles tel que Ansible, Image ISO ou encore par groupe de paquets RPM. Ainsi quel que soit l'environnement cible, on trouvera une méthode de déploiement adaptée à notre besoin [9].

### 3.3.3 Avantages et inconvénients

**Avantages :**
• Permet de combiner tous les outils de surveillance ITIL + dans une même distribution.
• Gestionnaire de performances ajouté.
• Découverte automatique.
• Déploiement facile des outils de monitoring.
• Gain d'un temps précieux.
• Robustesse et fiabilité.
• Possibilité de gérer leurs appareils via SSH/Telnet depuis leur interface Web.
**Inconvénients :**
• Une configuration en interface web qui ne Supporte pas l'HTTPS.
• Une interface qui déborde d'onglets.

## 3.4 Conclusion

En résumé, il en ressort qu'EyesOfNetwork est un outil qui permet de superviser son réseau tout en y intégrant une approche ITIL, il est idéal pour offrir un environnement réseau fiable et sécurisé jusqu'aujourd'hui est une priorité absolue envers les entreprises et les organisations.

Sa facilité dans l'installation ainsi que son interface web de configuration permet de faire gagner un temps précieux. Malgré ses quelques défauts, nous pouvons donc dire qu'EON est un produit aboutissant pour la supervision et la gestion de son système d'information.

# Chapitre 4

# Implémentation de la solution de supervision Eyes of network

## 4.1 Introduction

À travers ce chapitre, nous allons décrire la phase de réalisation et d'implémentation de notre politique de supervision après la conception de l'architecture adopté. Pour ce faire, nous allons utiliser un outil de supervision (Eyes Of Network) et GNS3 comme moyen de simulation.

## 4.2 Composants utilisés

— Un Router.

— Un Switch cœur.

— Deux switchs de distribution.

— Trois switchs d'accès.

— Quatres Vpcs.

— Un client sous Windows 7.

## 4.3 Présentation des outils utilisés

L'implémentation de cette solution de supervision a nécessité l'installation de plusieurs outils dont nous avons besoin :
• **Gns3 :** (Graphical Network Simulator) est un simulateur graphique d'équipement réseau qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations.

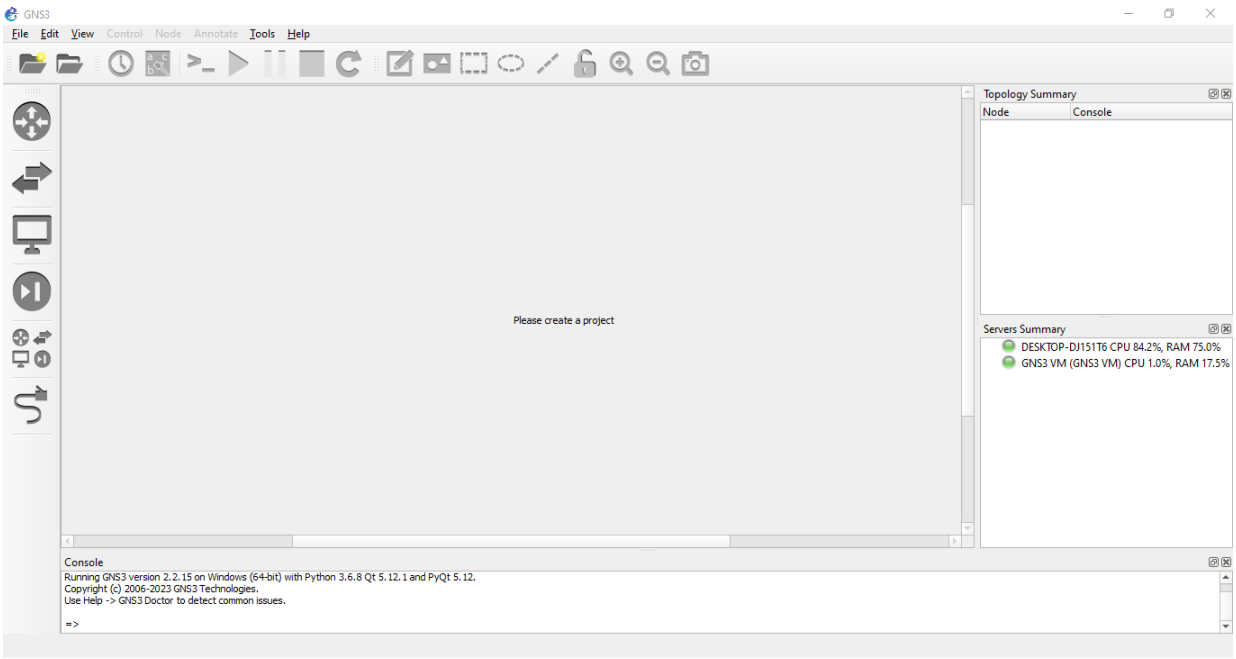



FIGURE 4.1 – Fenêtre principale du simulateur GNS3.

• **VM WARE Workstation 15 pro :** Le choix d'utiliser la VMware Workstation 15 pro a été fait Pour l'émulation de notre réseau, il s'agit d'un Outil de virtualisation qui permet de créer une ou plusieurs machines virtuelles au sein d'un même système d'exploitation. Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

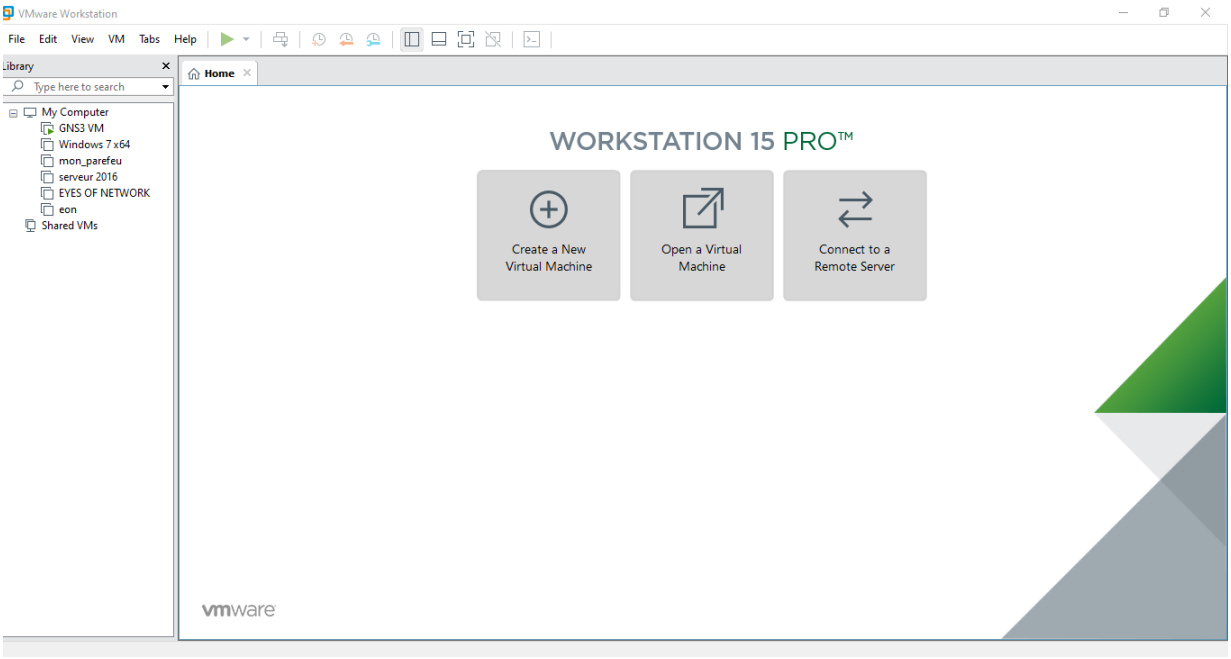



FIGURE 4.2 – Fenêtre principale du VMwere.

•**Windows Server 2016 :** Windows Server 2016 est un système d'exploitation serveur développé par Microsoft, il offre une plate-forme solide et sécurisée pour exécuter et gérer des services, des applications et des ressources réseau au sein d'une infrastructure informatique.
•**Pare-feu pfsense :** Est un système d'exploitation open source basé sur FreeBSD qui utilise des règles de filtrage pour contrôler le flux de trafic réseau entrant et sortant. Il permet de définir des politiques de sécurité granulaires en fonction de l'adresse IP, du port, du protocole, de l'interface réseau et d'autres critères.
•**Putty :** Est un émulateur de terminal UNIX gratuit, il permet de se connecter à distance à une machine ou un serveur, en utilisant les protocoles SSH, Telnet ou Rlogin [21].
•**Mozila Firefox :** Navigateur web libre permettant d'effectuer des recherches sur internet.

## 4.4 Implémentation du réseau LAN de SONATRACH

Afin de s'assurer que le réseau est contrôlé est surveillé, le réseau virtuel doit être établi sous le simulateur gns3 et ajuster les configurations nécessaires.

### 4.4.1 Partie théorique

1. **Réseau à superviser**
   L'ensemble des éléments de l'infrastructure à superviser sont :
   — Un pare-feu.
   — Un routeur.
   — Six switchs (un switch cœur, deux switchs distribution et trois switchs d'accès).
   — Un serveur windows 2016.
   — Un poste client Windows.
   — Un serveur Eyes Of Network qui s'occupera de la supervision.
2. **VLAN**
   VLAN pour (Virtual Local Area Network) est un réseau LAN virtuel et indépendant qui regroupe un ensemble de machines informatique. Le but du VLAN est d'améliorer la gestion du réseau, d'optimiser la bande passante, de séparer les flux et de renforcer la sécurité [19].

   Le tableau ci-dessous montre les noms des VLANs existant au niveau de l'entreprise ainsi que leurs adresses de sous-réseau :

| Nom du vlan | Id du vlan | Adresse IP | Description |
|---|---|---|---|
| DI | Vlan10 | 192.168.2.0/24 | Vlan pour le département informatique |
| DRH | Vlan20 | 192.168.3.0/24 | Vlan pour le département des ressources humaines |
| Serveur | Vlan30 | 192.168.4.0/24 | Vlan pour le serveur Windows 2016 |
| EON | Vlan40 | 192.168.5.0/24 | Vlan pour le serveur EON ainsi que la machine virtuelle |
| Management | Vlan50 | 192.168.6.0/24 | Vlan pour management des équipements |

TABLE 4.1 – Plan d'adressage IPv4.

3. **VTP**
   (vlan trunking protocole) est un protocole de niveau 2 utilisé pour la configuration et la gestion des VLAN sur les périphériques Cisco (commutateurs de niveau 2 et 3). Le principe est assez simple, on a un switch en mode serveur (dans notre cas, c'est le Switch Core), ou l'on effectue toutes les modification, suppression, ou création de vlan, et il se charge d'envoyer ces infos sur tous les switchs client, qui font partie du même domaine VTP [18].
4. **SNMP**
   (Simple Network Management Protocol) est un protocole de communication qui permet aux administrateurs réseau de superviser des équipements et de diagnostiquer des problèmes réseau et matériel à distance [17].
5. **Administration des équipements**
   Dans l'administration des équipements nous avons créé le VLAN 50 comme vlan de management.

### 4.4.2 Partie pratique

Afin de mener à bien notre projet, nous allons procéder à la configuration des équipements sous GNS3, pour ensuite les superviser avec l'outil Eyes Of Network.
Ci-dessous la figure présente l'architecture réseau LAN de SONATRACH sous GNS3 :

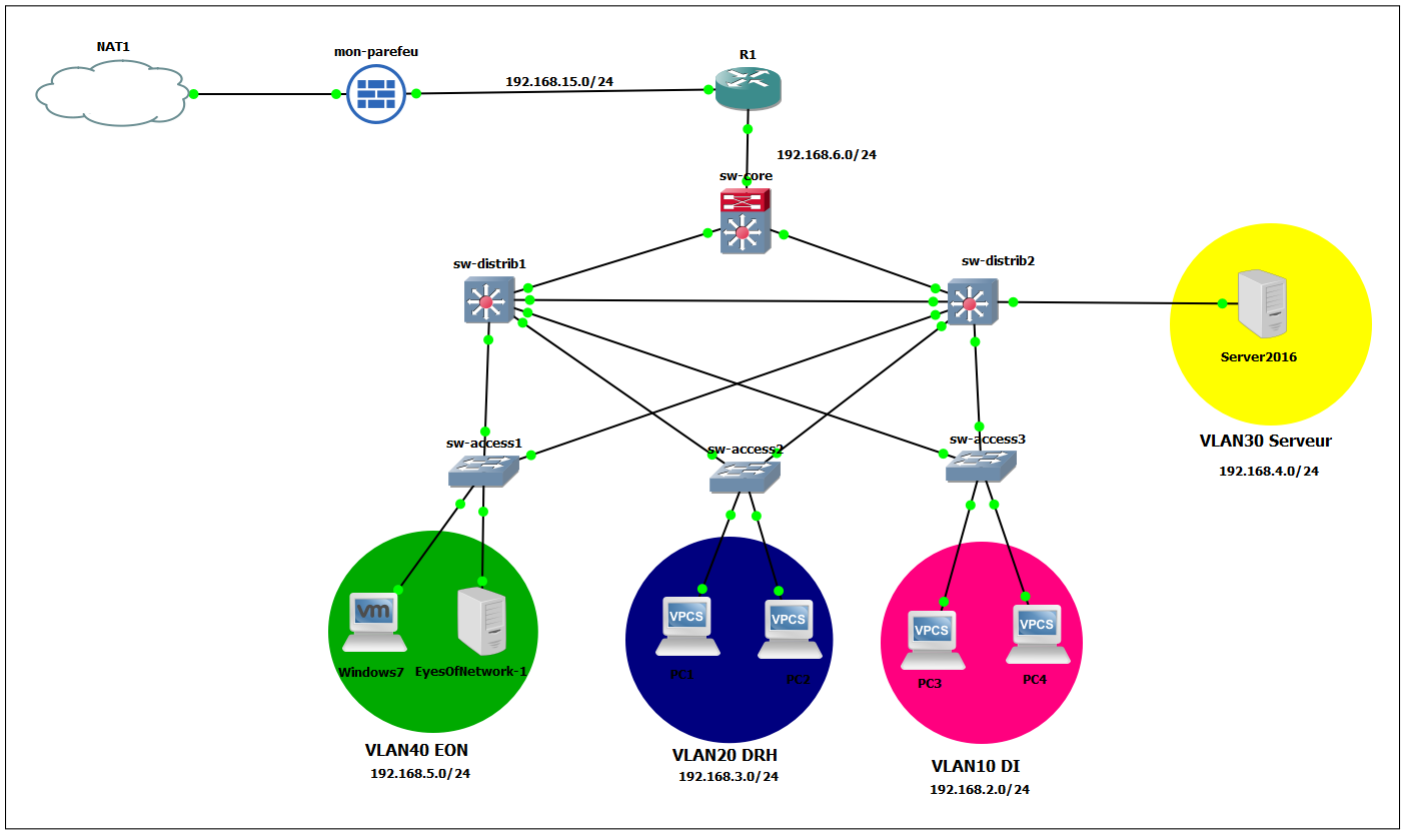



FIGURE 4.3 – Architecture adoptée.

1. **Configuration des équipements :** Pour configurer les équipements Cisco, nous avons utilisé la console appelé solar-putty.
2. **Configurations des Switchs :** Pour obtenir un bon réseau et une bonne configuration, nous avons suivis les étapes suivantes :
   - Configuration de hostname.
   - Configuration de mot de passe pour la ligne console et SSH.
   - Configuration de VTP.
   - Configuration des Vlans.
   - Configuration des interfaces.
   - Configuration du routage inter-vlan.
   - Configuration du protocole SNMP.

3. **Installation de Windows server 2016 :** Cette partie montre les différentes étapes de l'installation du serveur comme le montre la figure suivante :

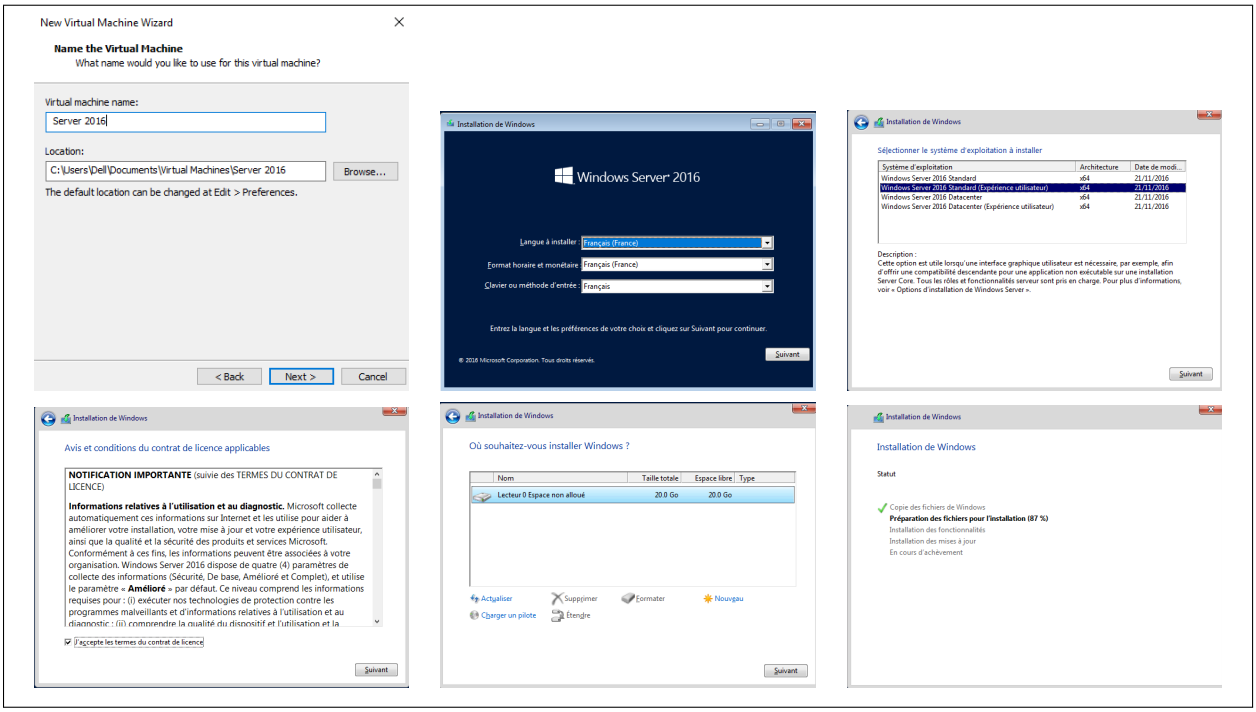



TABLE 4.2 – Installation du windows serveur 2016.

4. **Instalation de l'Active Directory :** L'installation de l'active directory sur Windows serveur 2016 ce fait comme suite :

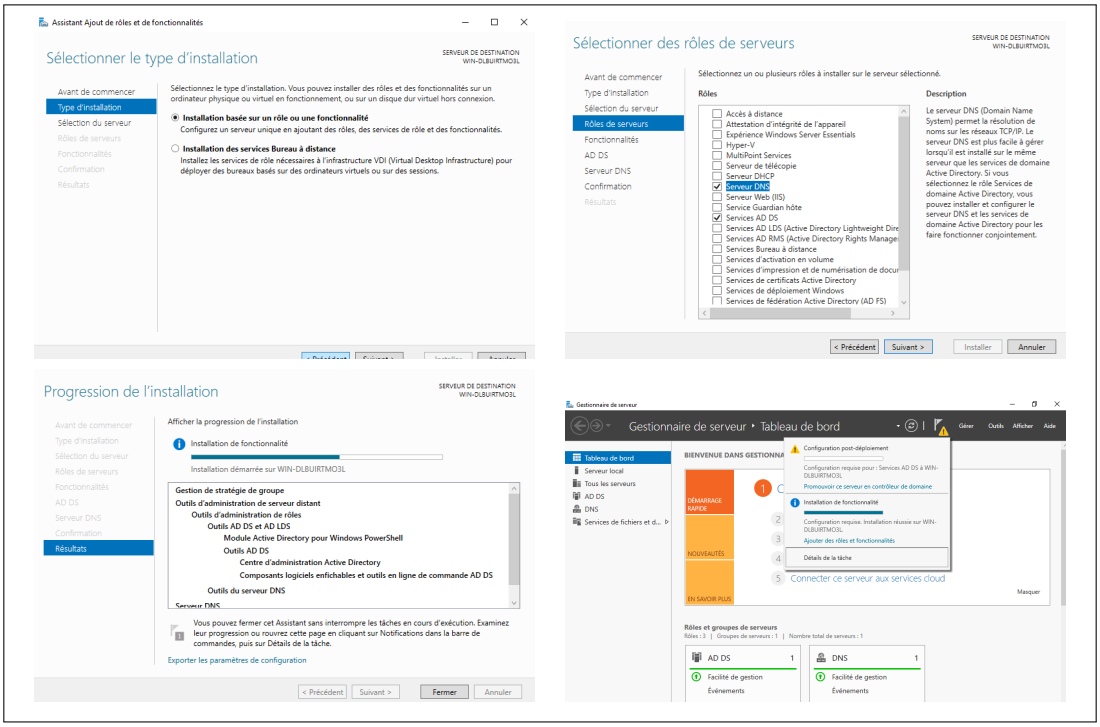



TABLE 4.3 – Installation de l'active directory.

5. **Exemple de configuration du switch cœur**
   **Configuration du Nom de l'équipement :** La configuration de hostname dans sw-core.

```
switchL3(config)#hostname sw-core
sw-core(config)#
```

FIGURE 4.4 – Configuration de hostname du sw-core.

**Configutation de la bannière de connexion :** Configurez la bannière de connexion pour chaque équipement, comme illustre dans la figure ci-dessus :

```
R1(config)#banner motd c ACCESS INTERDIT AUX PERSONNES NON AUTORISEES c
R1(config)#do wr
```

FIGURE 4.5 – Commande de configuration de la bannière de connexion sur R1.

**Configuration de SSH :** La figure montre la configuration de l'outil d'accès a distance SSH sur R1.

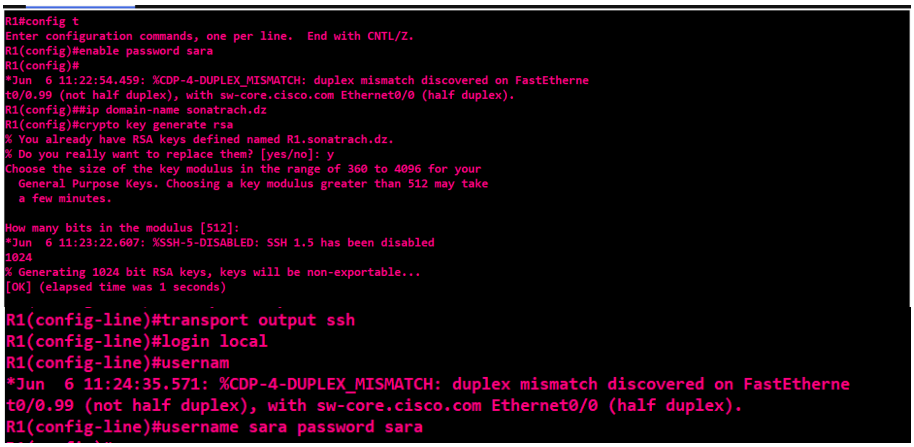



FIGURE 4.6 – Configuration de l'outil d'accès à distance SSH sur le router R1.

**Configuration de VTP :** Figure montrant la configuration de VTP dans le sw-core.

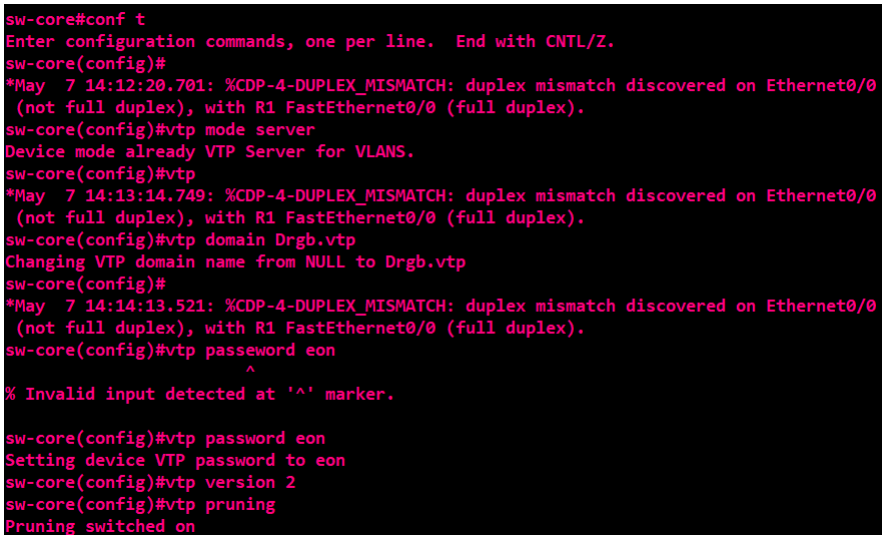



FIGURE 4.7 – Configuration de VTP dans le sw-core.

**L'implémentation de VTP :** Démonstration du status VTP dans le sw-core.

```
sw-core#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : Drgb.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 5-7-23 11:46:56
Local updater ID is 192.168.6.100 on interface Vl50 (lowest numbered VLAN interface fou
nd)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 11
Configuration Revision            : 8
MD5 digest                        : 0x94 0x59 0x59 0x8E 0x41 0x33 0x1C 0xCB
                                    0xB1 0x13 0xDB 0x2A 0xC6 0x0C 0xD2 0xC5
```

FIGURE 4.8 – Démonstration de l'implémentation de VTP dans le sw-core.

**Création des VLANs :** La figure montre la création des VLANs dans le sw-core.

```
sw-core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#vlan 10
sw-core(config-vlan)#name DI
sw-core(config-vlan)#vlan 20
sw-core(config-vlan)#name DRH
sw-core(config-vlan)#vlan 30
*May  8 08:48:51.413: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0
 (not full duplex), with R1 FastEthernet0/0 (full duplex).
sw-core(config-vlan)#vlan 30
sw-core(config-vlan)#name Serveur
sw-core(config-vlan)#vlan 40
sw-core(config-vlan)#name EON
sw-core(config-vlan)#vlan 50
sw-core(config-vlan)#name Management
sw-core(config-vlan)#vlan 99
sw-core(config-vlan)#name
% Incomplete command.

sw-core(config-vlan)#name native
```

FIGURE 4.9 – Création des VLANs dans le sw-core.

**Démonstration de l'implémentation des VLANs :** La figure suivante montre les VLANs créer.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/3, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et2/3, Et3/0, Et3/1, Et3/2
                                                 Et3/3
10   DI                                active
20   DRH                               active
30   Serveur                           active
40   EON                               active
50   Management                        active
99   native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

FIGURE 4.10 – Démonstration de la création des VLANs dans le sw-core

**Configuration des interfaces vlan en mode access :** La figure montre la configuration de l'interface vlan en mode access du vlan 40 qui est reliée au serveur de supervision et la machine virtuelle Windows .

```
sw-access1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-access1(config)#int e0/0
sw-access1(config-if)#switchport mode access
sw-access1(config-if)#switchport access vlan 40
sw-access1(config-if)#exit
sw-access1(config)#int e0/3
sw-access1(config-if)#switchport mode access
sw-access1(config-if)#switchport access vlan 40
```

FIGURE 4.11 – Configuration de l'interface vlan 40 en mode access du sw-access1.

**Configuration des interfaces vlan en mode trunk :**

```
sw-core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#int range e0/0-2
sw-core(config-if-range)#switchport trunk encapsulation dot1q
sw-core(config-if-range)#
*May  7 14:01:50.904: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0
 (not full duplex), with R1 FastEthernet0/0 (full duplex).
sw-core(config-if-range)#switchport mode trunk
```

FIGURE 4.12 – Configuration des interfaces vlan en mode trunk dans le sw-core.

**Démontration du routage inter-VLAN :** La figure montre l'implémentation du routage inter-vlan dans notre routeur R1.

```
router#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.10         192.168.2.1     YES NVRAM  up                    up
FastEthernet0/0.20         192.168.3.1     YES NVRAM  up                    up
FastEthernet0/0.30         192.168.4.1     YES NVRAM  up                    up
FastEthernet0/0.40         192.168.5.1     YES NVRAM  up                    up
FastEthernet0/0.50         192.168.6.1     YES NVRAM  up                    up
FastEthernet0/0.99         192.168.99.1    YES NVRAM  up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down down
FastEthernet0/1            192.168.15.2    YES NVRAM  up                    up
```

FIGURE 4.13 – Le routage inter-VLAN.

```
router#show ip ROUTE
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.15.1 to network 0.0.0.0

C    192.168.15.0/24 is directly connected, FastEthernet0/1
C    192.168.4.0/24 is directly connected, FastEthernet0/0.30
C    192.168.99.0/24 is directly connected, FastEthernet0/0.99
C    192.168.5.0/24 is directly connected, FastEthernet0/0.40
C    192.168.6.0/24 is directly connected, FastEthernet0/0.50
C    192.168.2.0/24 is directly connected, FastEthernet0/0.10
C    192.168.3.0/24 is directly connected, FastEthernet0/0.20
S*   0.0.0.0/0 [1/0] via 192.168.15.1
```

FIGURE 4.14 – Affichage de la table de routage.

### Test des ping :

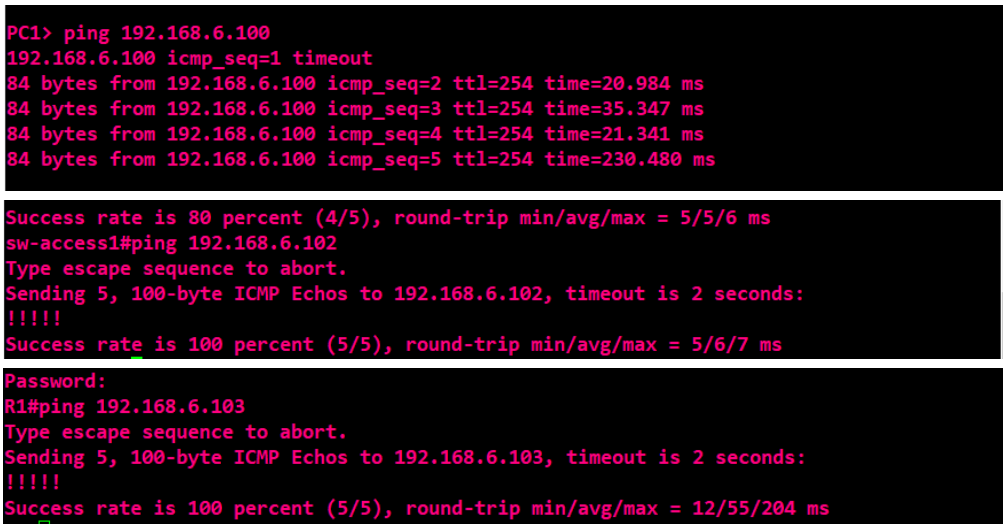



FIGURE 4.15 – test de ping entre les équipements.

6. **Configuration de base du pare-feu :** Après avoir installé et lancé PfSense nous tapons l'adresse 192.168.15.1 dans le navigateur pour accéder à l'interface de notre firewall pour commencer les configurations de base.

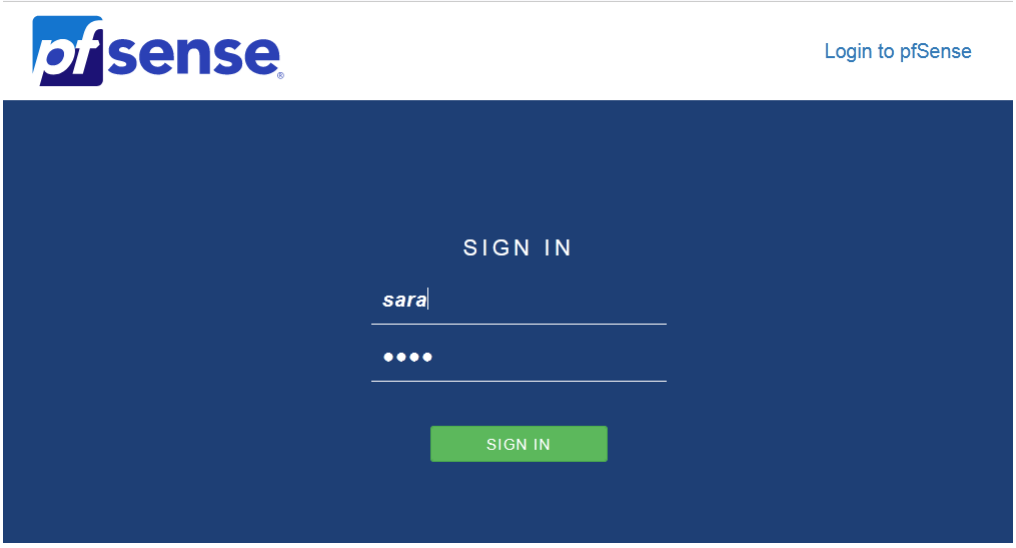



FIGURE 4.16 – Interface d'accueil du parefeu Pfsense.

1.Nous commencons par configurer l'interface LAN du parefeu.

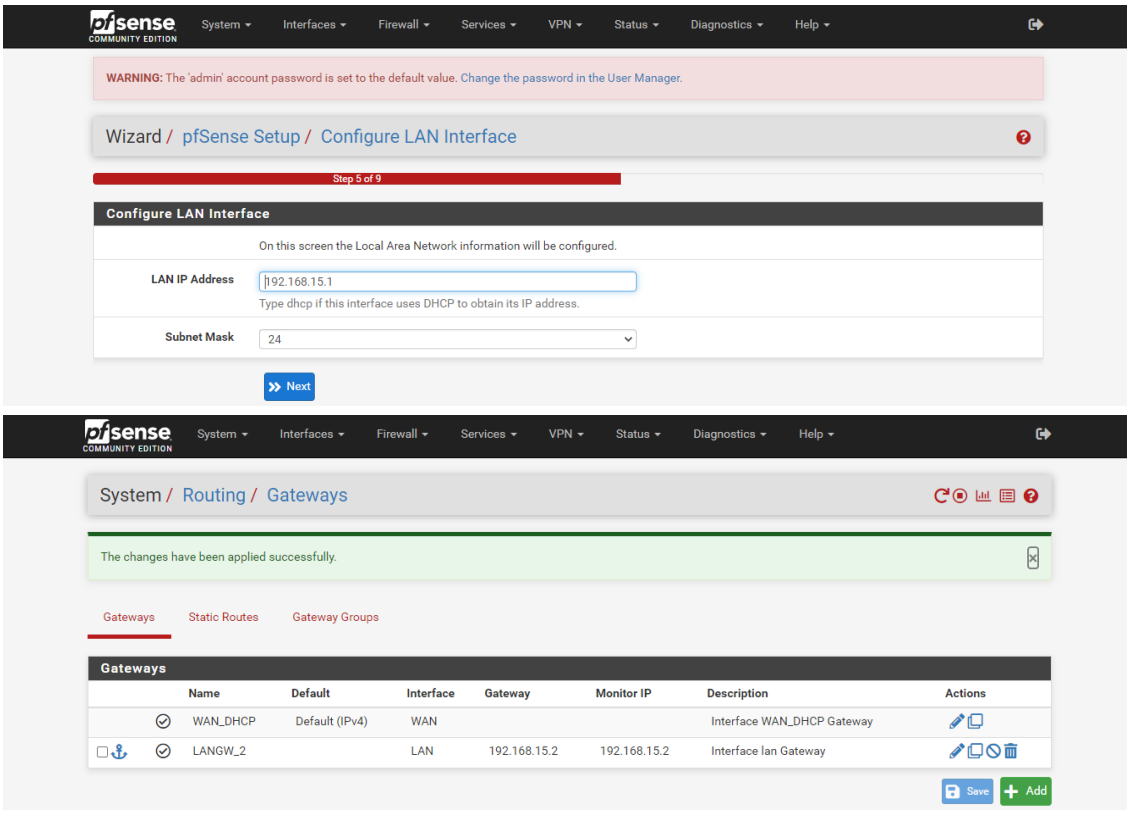



FIGURE 4.17 – Configuration de l'interface LAN.

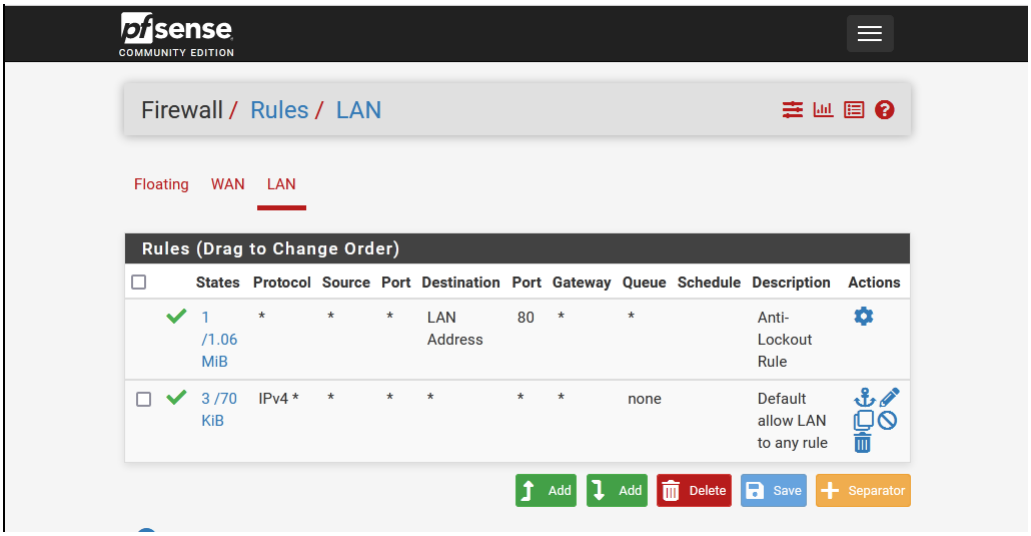



FIGURE 4.18 – Application des règles.

2.Nous devons créer et autoriser nos VlANs.

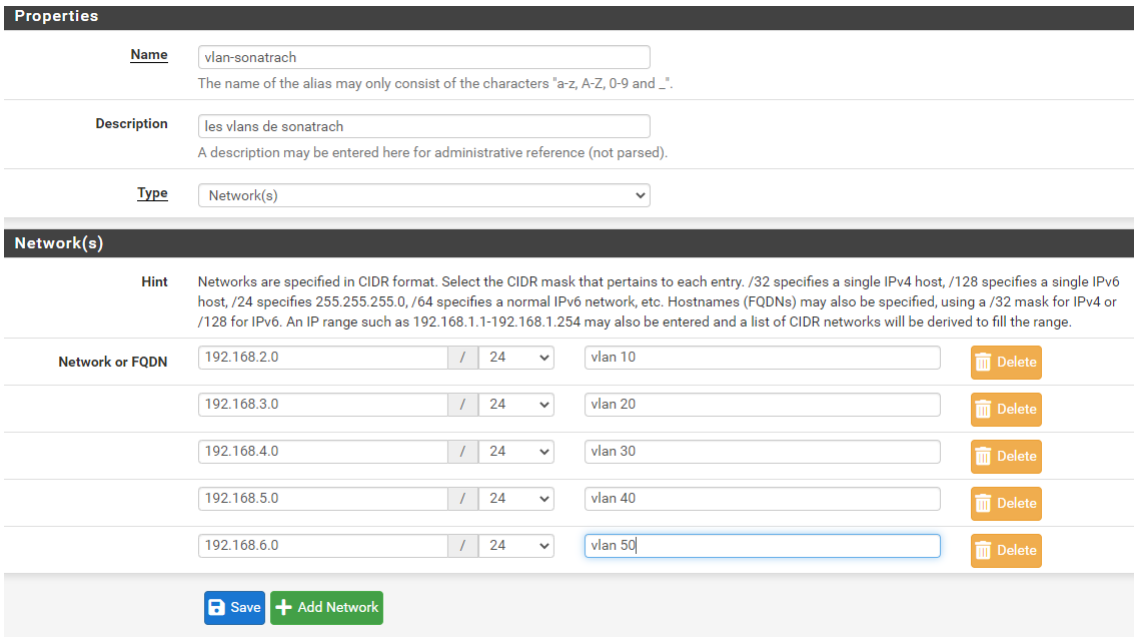



FIGURE 4.19 – création des VLANs.

3.Maintenant, nous devons routé notre pare-feu vers les VLANs.

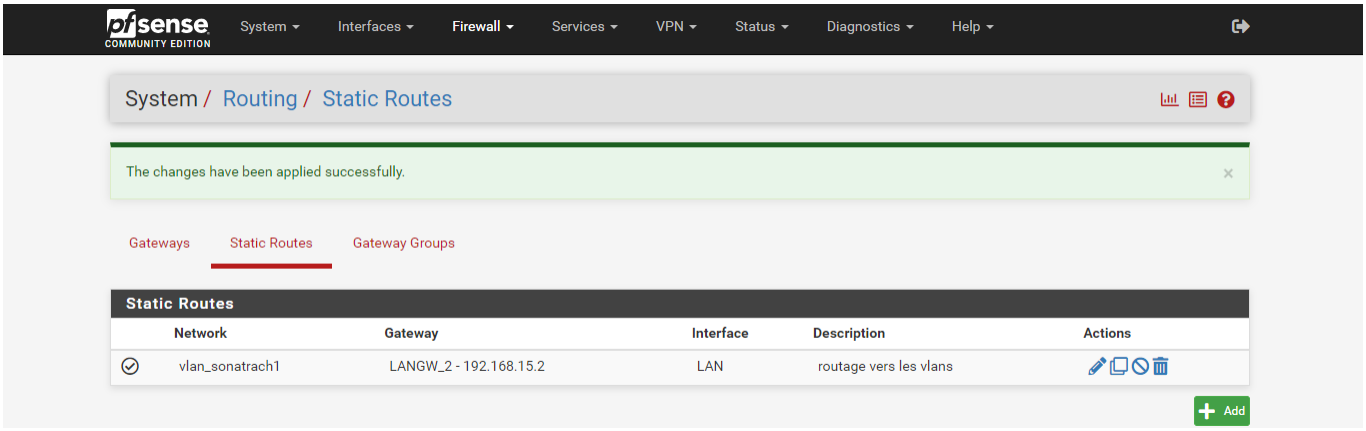



FIGURE 4.20 – Routage du pare-feu.

4.Ici, nous effectuant un ping afin de tester la connectivité entre les équipements comme le montre la figure 4.21 :

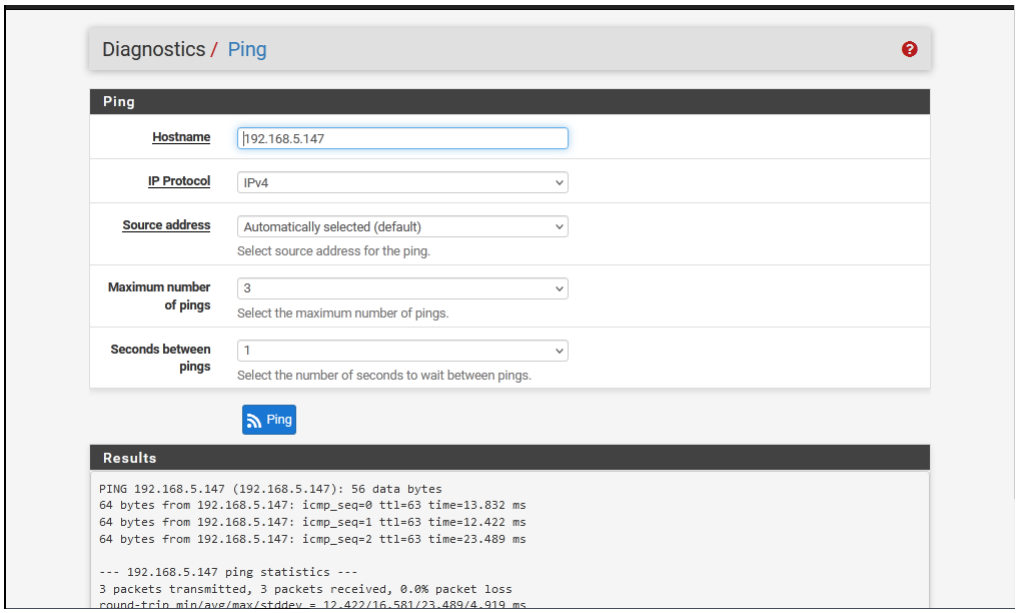



FIGURE 4.21 – test ping.

### 4.4.3 Implémentation de la politique de supervision

Après avoir installé et configuré Eyes Of Network (**voir Annexe A**), nous allons procéder à l'implémentation des fonctionnalités de celui-ci.

— **Création de la communauté**
-On va sur Administration puis Nagios Ressources,ensuite Dans le champ $USER2$ on saisit le nom de la communauté SNMP, dans notre cas c'est donc EON.

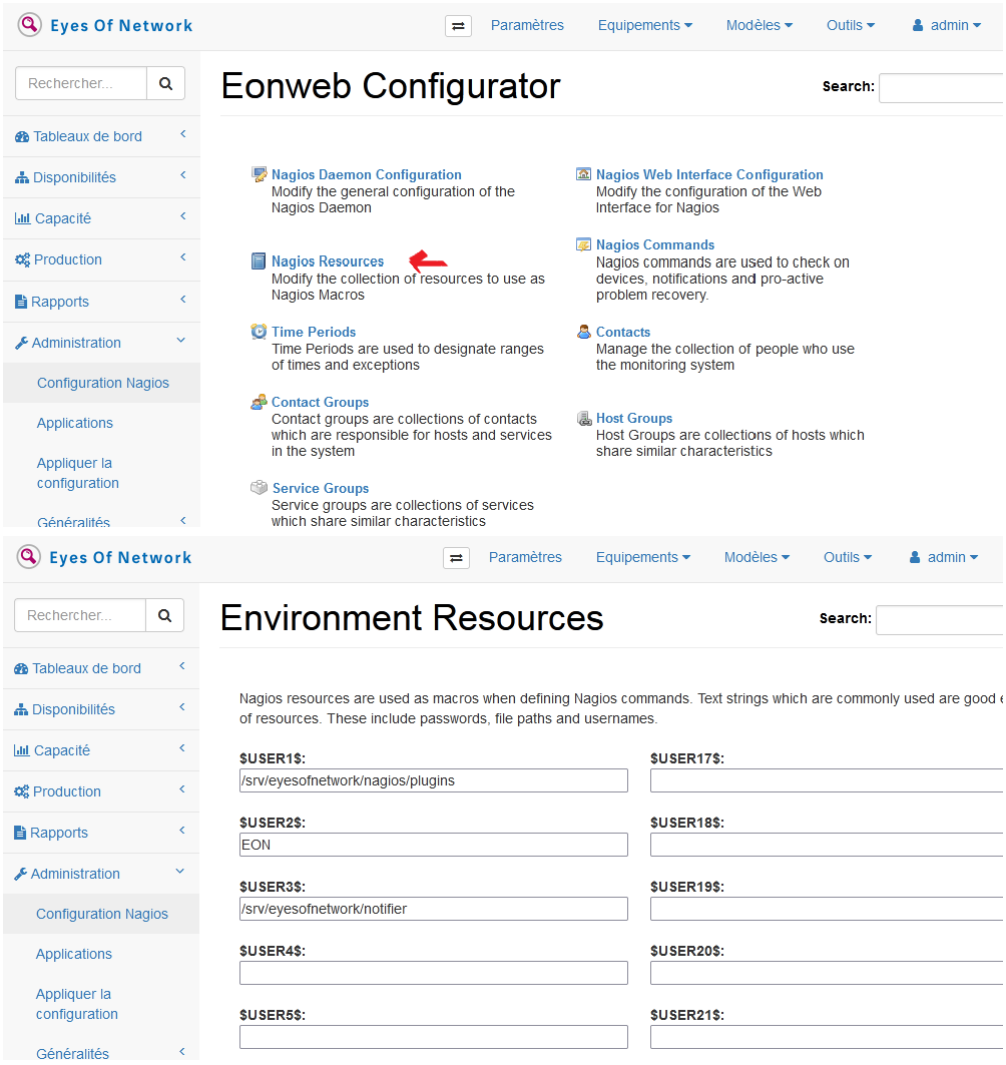



FIGURE 4.22 – Ajout de la communauté.

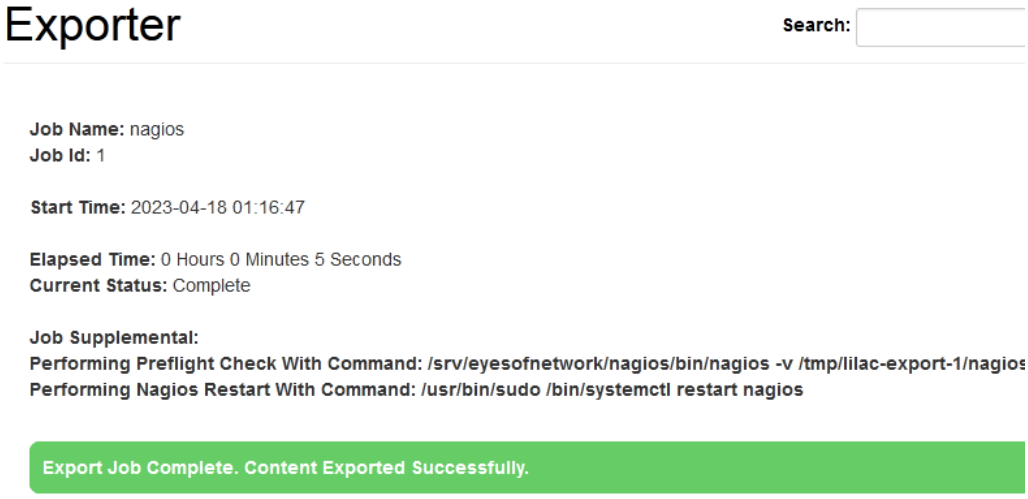



FIGURE 4.23 – Configuration appliquée avec succès.

— **Configuration de SNMP sur EON :**
-Il suffit de taper cette ligne de commande "yum install net snmp net snmpd-utils"comme ci-dessus :

```
[root@sonatrach ~]# yum install net snmp net snmpd utils
Modules complémentaires chargés : fastestmirror, product-id, search-disabled-repos, subscription-
                                : manager

This system is not registered with an entitlement server. You can use subscription-manager to regist
er.

Determining fastest mirrors
epel/x86_64/metalink                                                    |  61 kB  00:00:00
 * base: mirror.uv.es
 * epel: linuxsoft.cern.ch
 * extras: mirrors.evoluso.com
 * updates: centos.mirror.ptisp.pt
base                                                                    | 3.6 kB  00:00:00
eon-base                                                                | 3.6 kB  00:00:00
eon-updates                                                             | 3.6 kB  00:00:00
epel                                                                    | 4.7 kB  00:00:00
extras                                                                  | 2.9 kB  00:00:00
labs_consol_stable                                                      | 1.2 kB  00:00:00
updates                                                                 | 2.9 kB  00:00:00
(1/4): epel/x86_64/updateinfo                                           | 1.0 MB  00:00:05
(2/4): labs_consol_stable/x86_64/primary                                |  22 kB  00:00:05
(3/4): epel/x86_64/primary_db                                           | 7.0 MB  00:00:20
(4/4): updates/7/x86_64/primary_db                                      |  21 MB  00:00:24
```

FIGURE 4.24 – Configuration de SNMP sur EON.

— **Configuration SNMP sur les équipements :**

**Équipement Cisco :**

Dans cette configuration, nous lions notre sw-core au serveur de supervision (Eyes Of Network) basé sur le protocole SNMP.

```
sw-core(config)#snmp-server community EON RO
sw-core(config)#snmp-server host 192.168.5.147 EON
sw-core(config)#snmp-server enable traps
sw-core(config)#access-list 98 permit 192.168.5.147
sw-core(config)#access-list 99 permit 192.168.5.147
```

FIGURE 4.25 – Configuration de SNMP dans le sw-core.

```
access-list 98 permit 192.168.5.147
access-list 99 permit 192.168.5.147
!
!
snmp-server community EON RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps eigrp
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
snmp-server enable traps pw vc
```

FIGURE 4.26 – Démonstration des traps.

**Configuration du SNMP sur un serveur ou poste de travail :**
-Sur notre serveur dans « gestionnaire de serveur », puis « ajouter des rôles et des fonctionnalités » on installe Service SNMP.

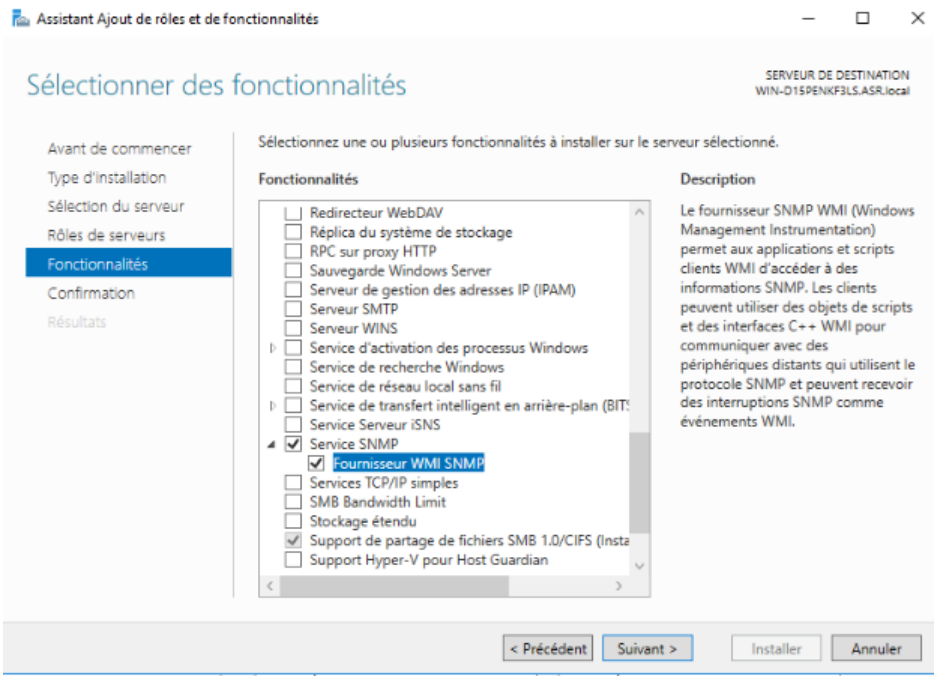



FIGURE 4.27 – Installation du service SNMP.

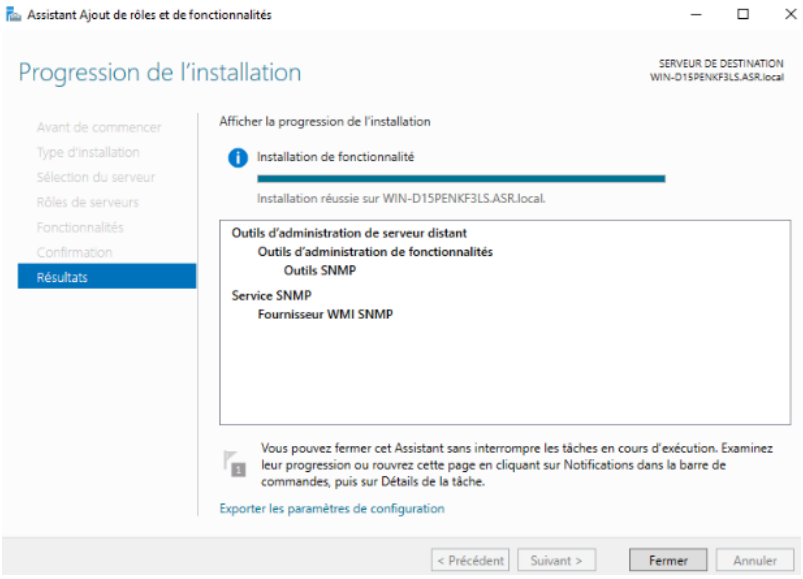



FIGURE 4.28 – Installation réussie.

-Se rendre dans la console de gestion des services rechercher service SNMP afin de modifier la communauté.

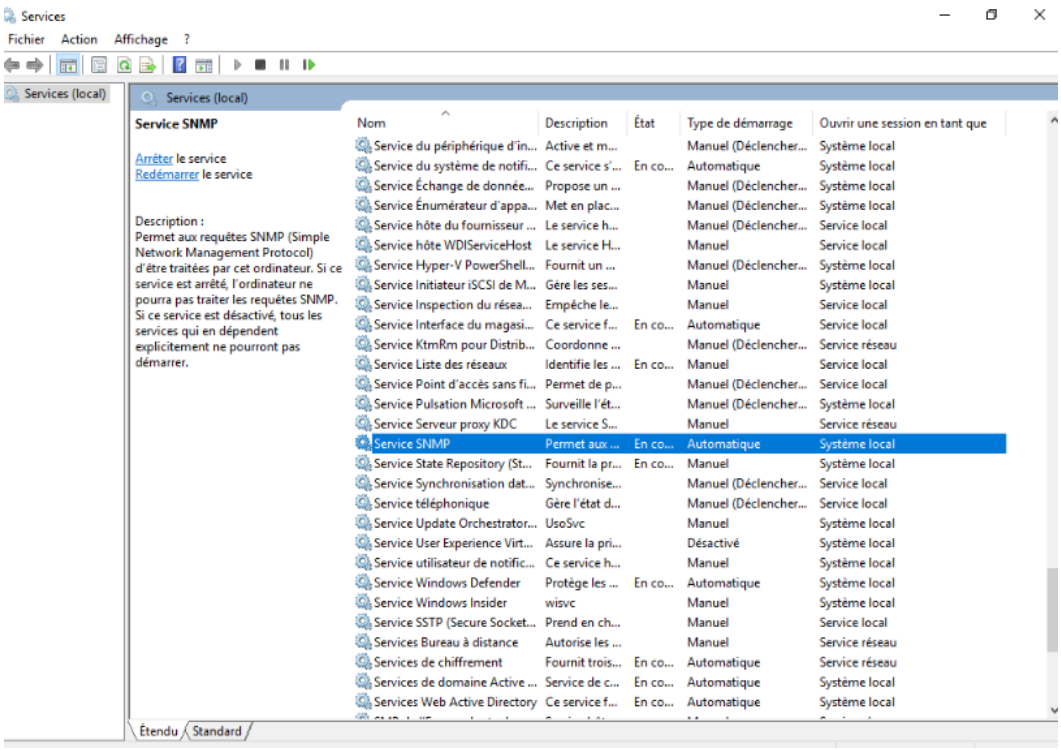



FIGURE 4.29 – Le service SNMP ajouté.

-Dans l'onglet sécurité on ajoutera le nom de la communauté que l'on a précédemment renseigné dans Eyes Of Network, dans notre cas c'est EON.
-On Ajoute par la suite l'adresse IP du serveur (EON) à autoriser.

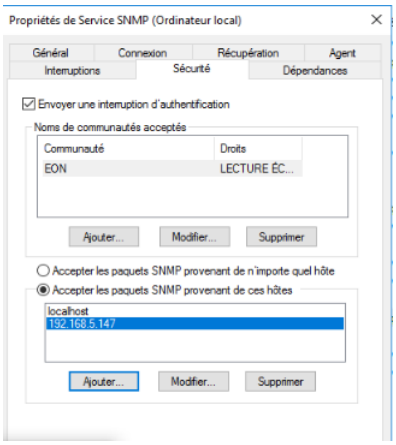



FIGURE 4.30 – Ajout de la communauté SNMP ainsi que l'adresse de Eyes Of Network.

**Configuration du service SNMP sur Pfsense :**
-Il suffit juste d'ajouter la communauté dans le service SNMP de Pfsense.

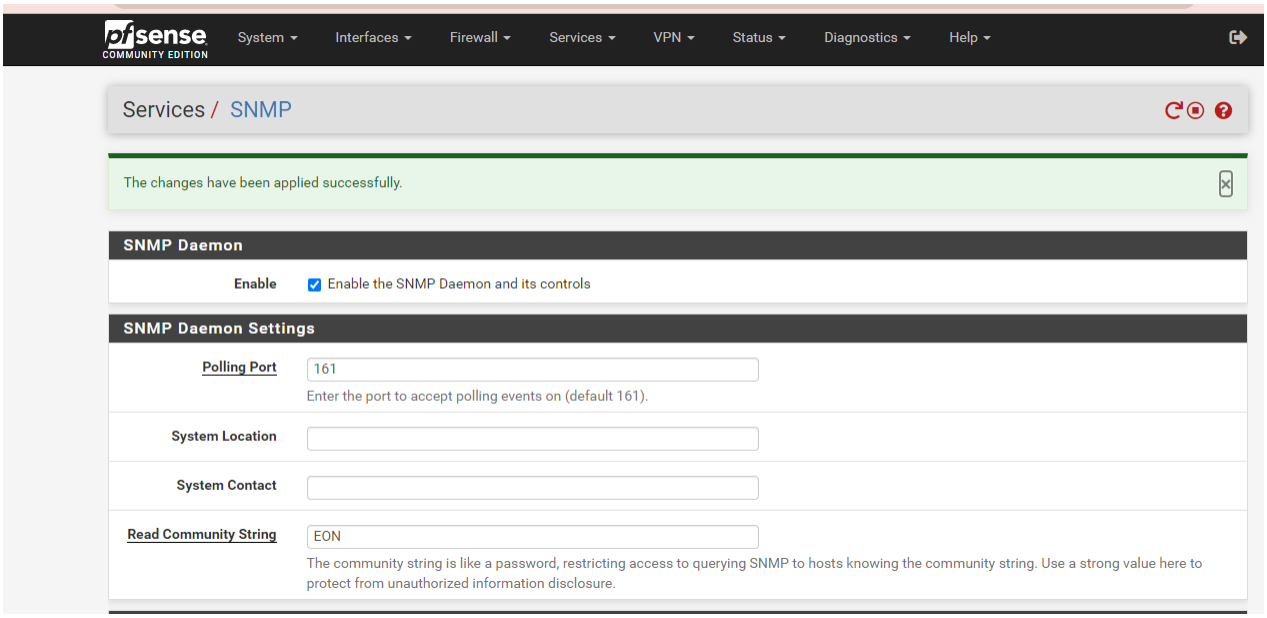



FIGURE 4.31 – Ajout de la communauté SNMP sur Pfsense.

— **Intégration des équipements réseaux dans EyesOfNetwork Équipements CISCO :** dans cet exemple nous prenons le routeur R1.

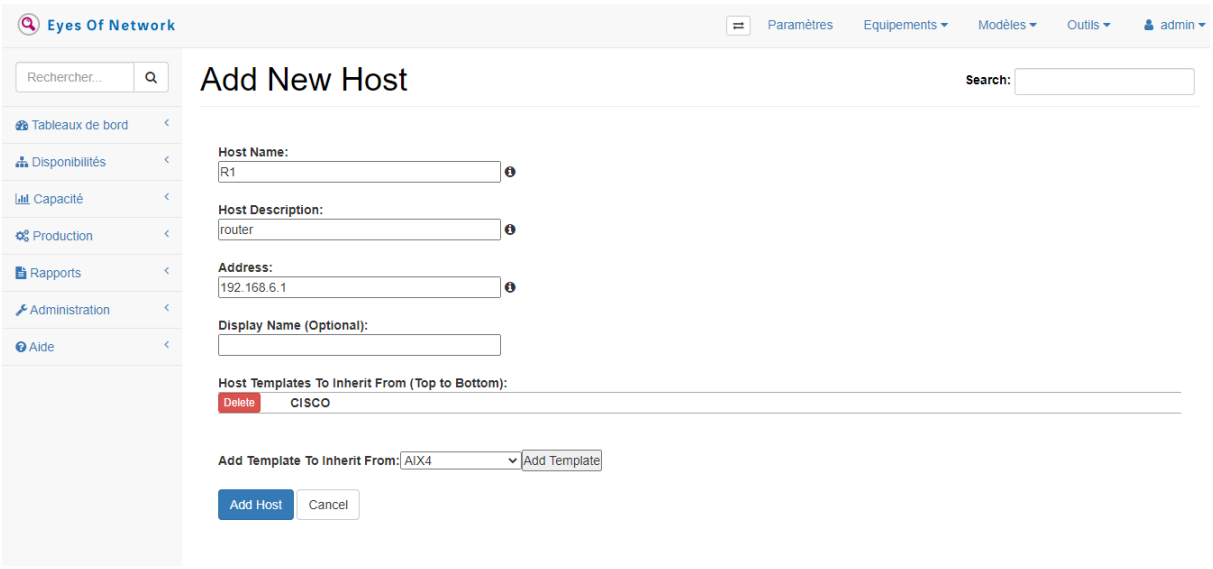



FIGURE 4.32 – Ajout du routeur R1 sur EON.

-Apres chaque ajout ou modification il est très important d'appliquer la configuration afin d'enregistrer.

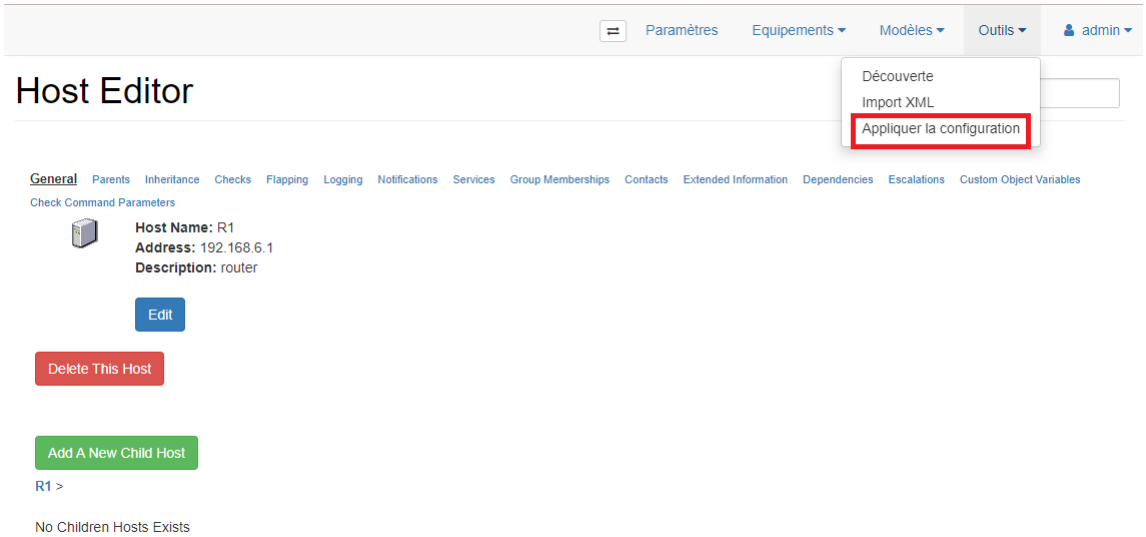



FIGURE 4.33 – application de la configuration sur R1.

## Serveur Windows 2016 :

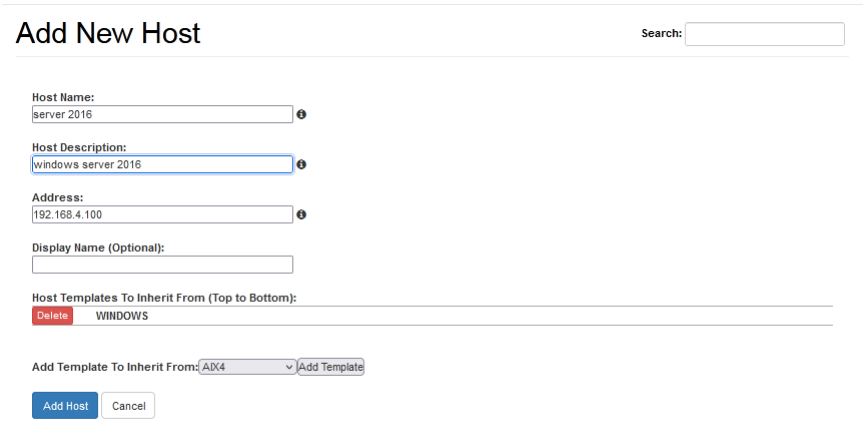



FIGURE 4.34 – Ajout du serveur windows 2016 sur EON.

## Pare-feu (Pfsense) :

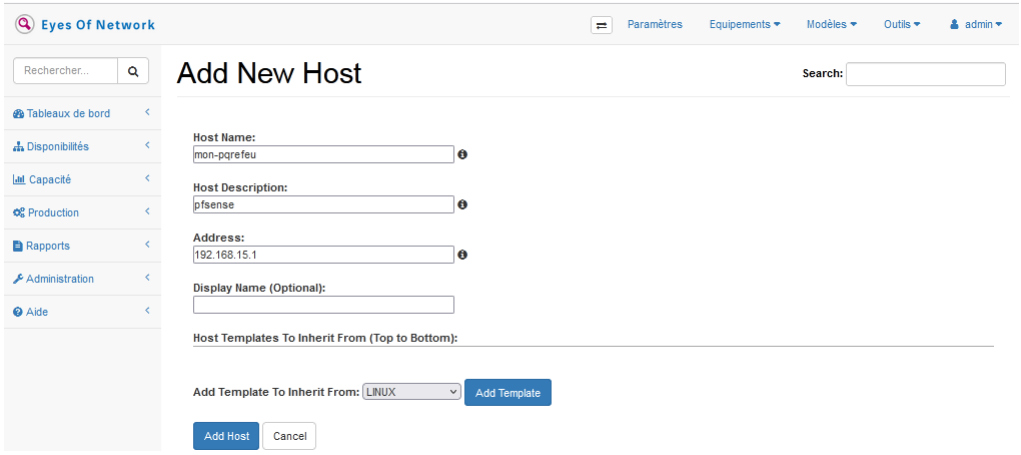



FIGURE 4.35 – Ajout du pare-feu sur EON.

### Windows 7 :

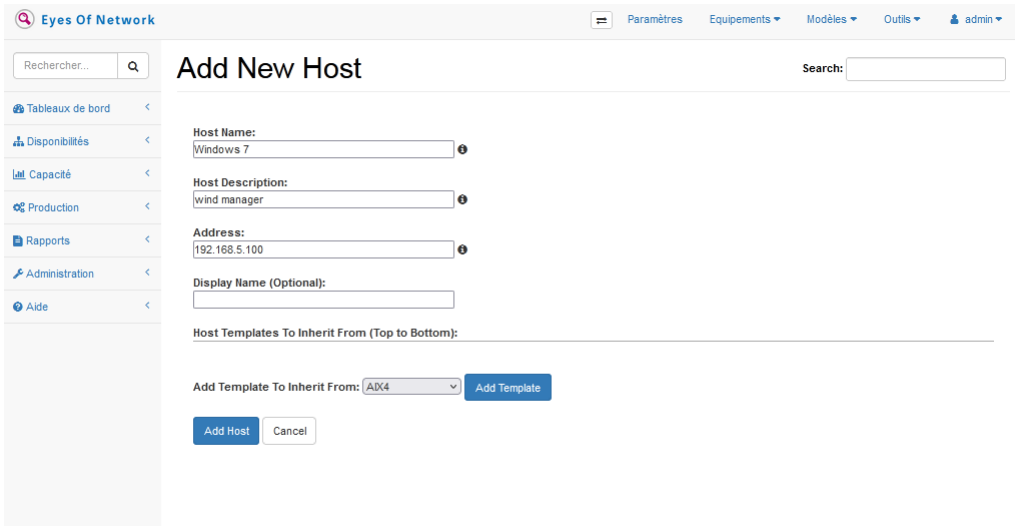



FIGURE 4.36 – Ajout du client Windows.

— **Insallation de NSClient++ :** -Afin d'ajouter un service a notre hôte Windows il faut d'abord installer NSClient++ sur la machine a superviser.

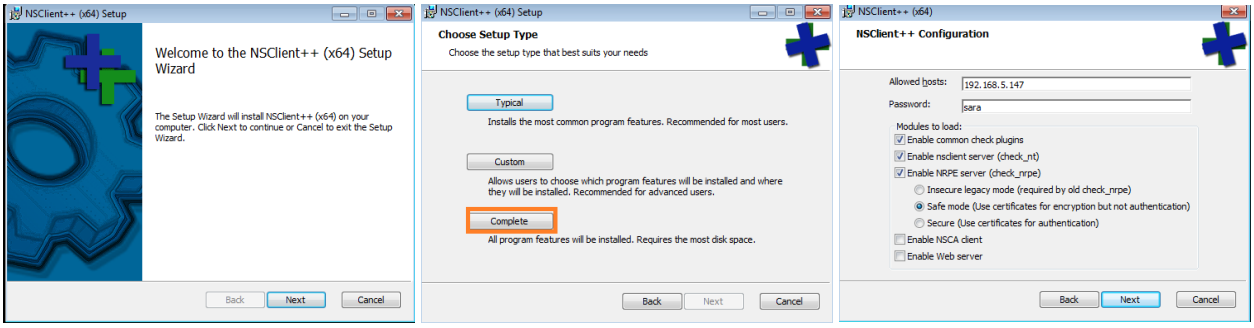



FIGURE 4.37 – Installation de NSClient++ sur la machine windows.

— **Ajout d'un service :**

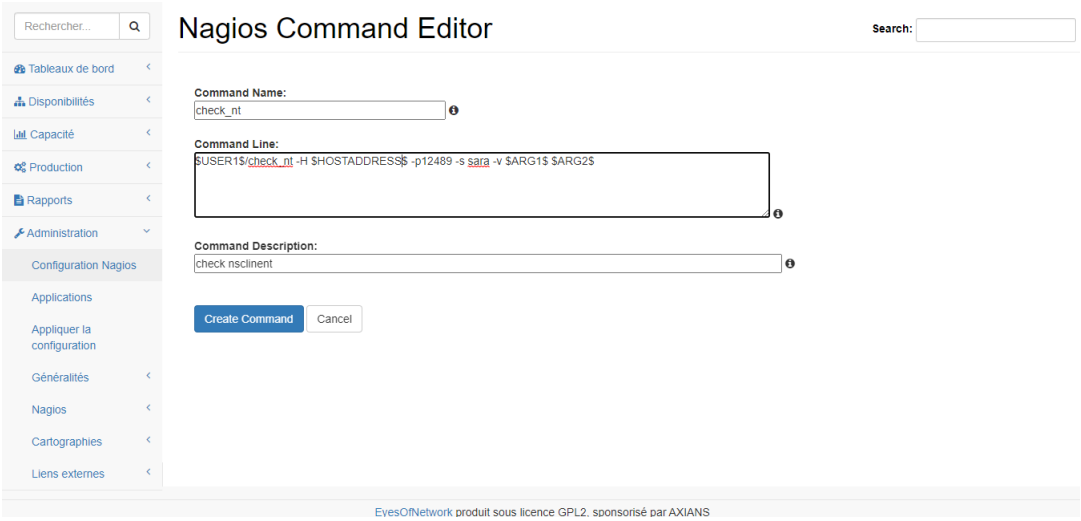



FIGURE 4.38 – Ajout de la commande check_nt.

— **Présentation des tests de fonctionnements :**

1.L'état des équipements supervisés DOWN/UP sont illustrés sur la figure 4.39 :

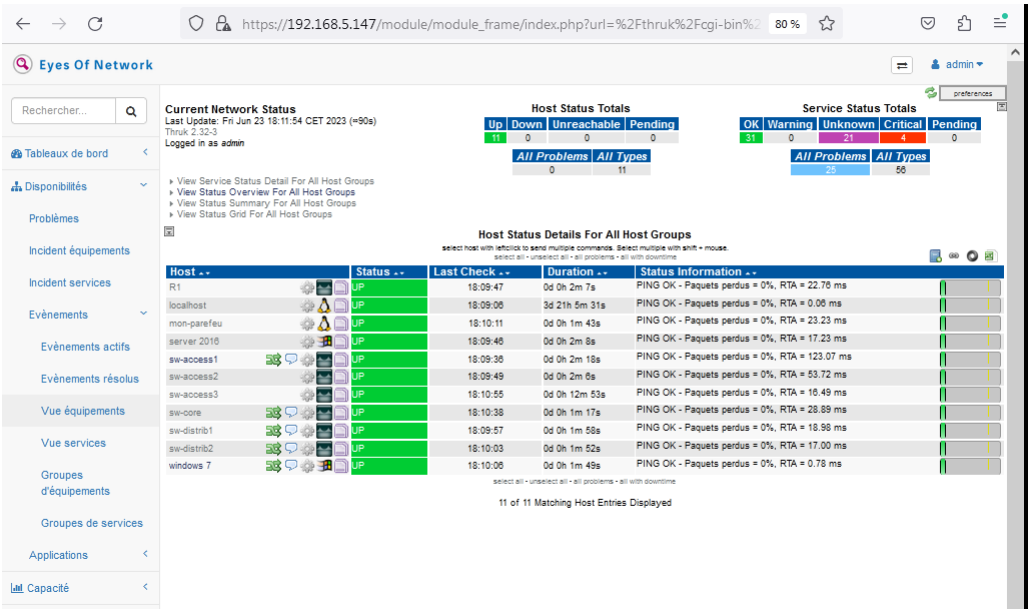



FIGURE 4.39 – Etat des équipement supervisé DOWN/UP .

2. Supervision de tous les services de chaque équipements est présentée par la figure 4.40 :

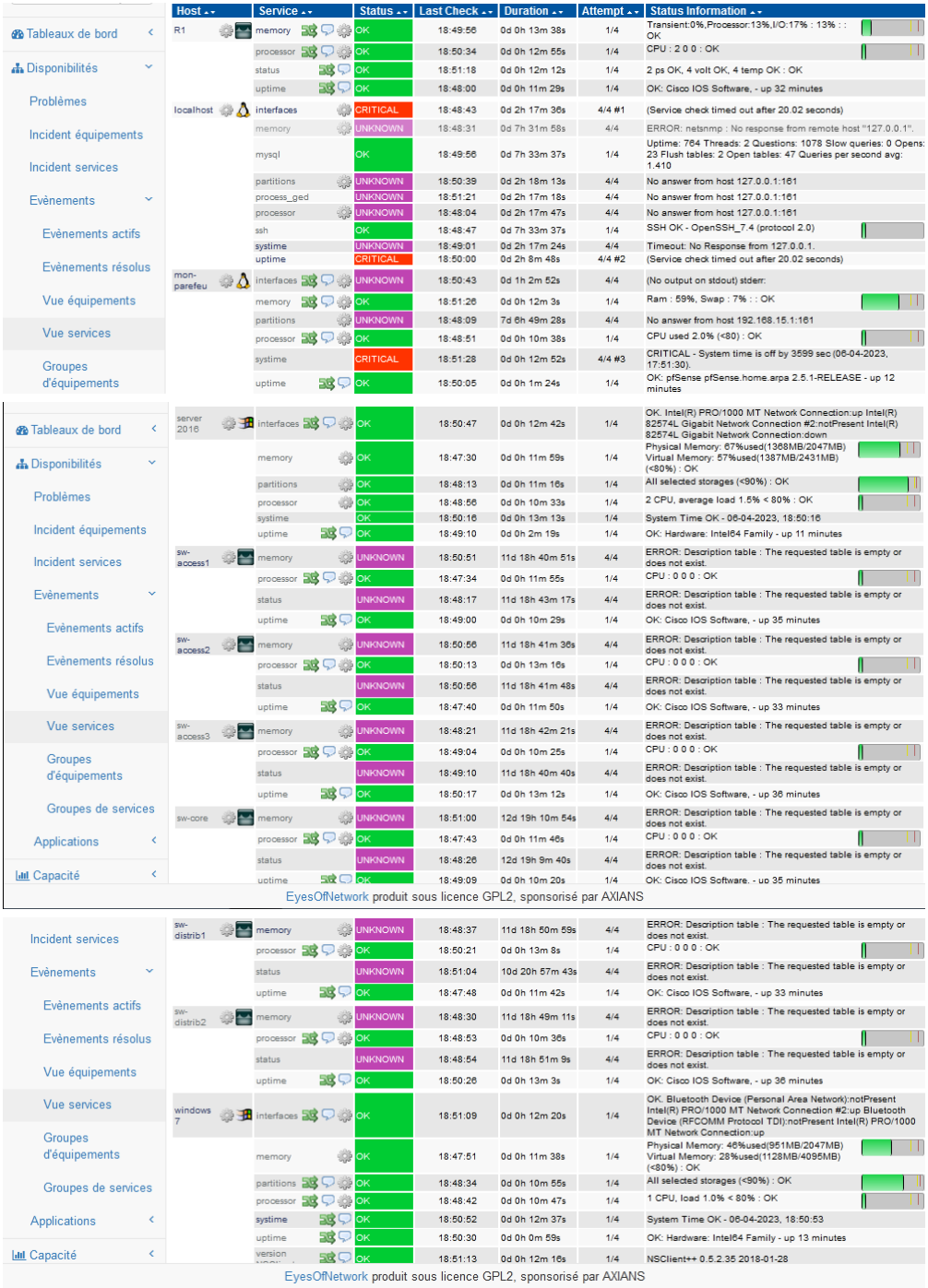



FIGURE 4.40 – Supervision des services de tous les équipements.

### 4.4.4 Génération de rapport

Les rapports sont utilisés pour visualiser ou présenter l'état d'un parc informatique au niveau d'un groupe d'équipements et/ou de services. Ils permettront ainsi de prendre les mesures nécessaires pour ajuster ou faire évoluer son parc [20].

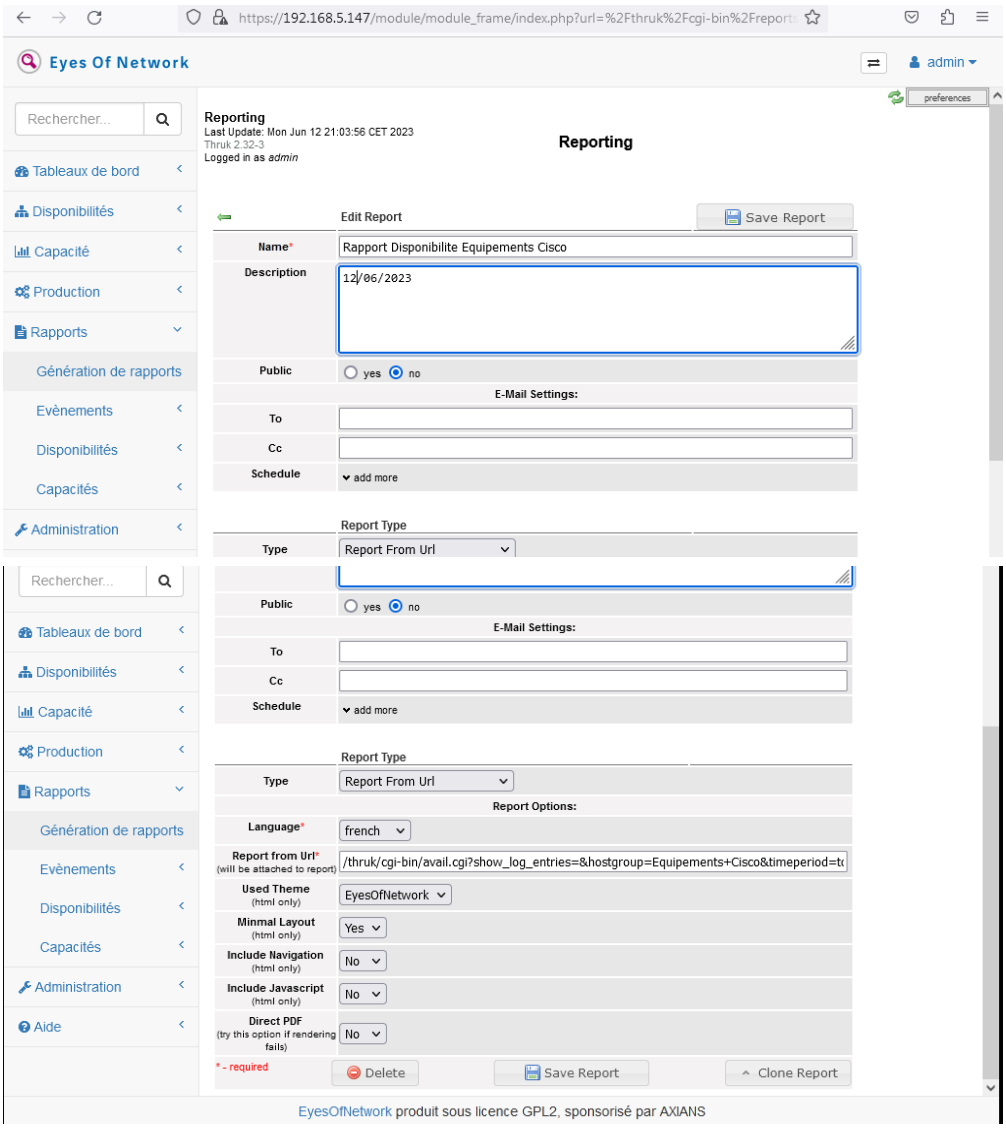



FIGURE 4.41 – Création du rapport.

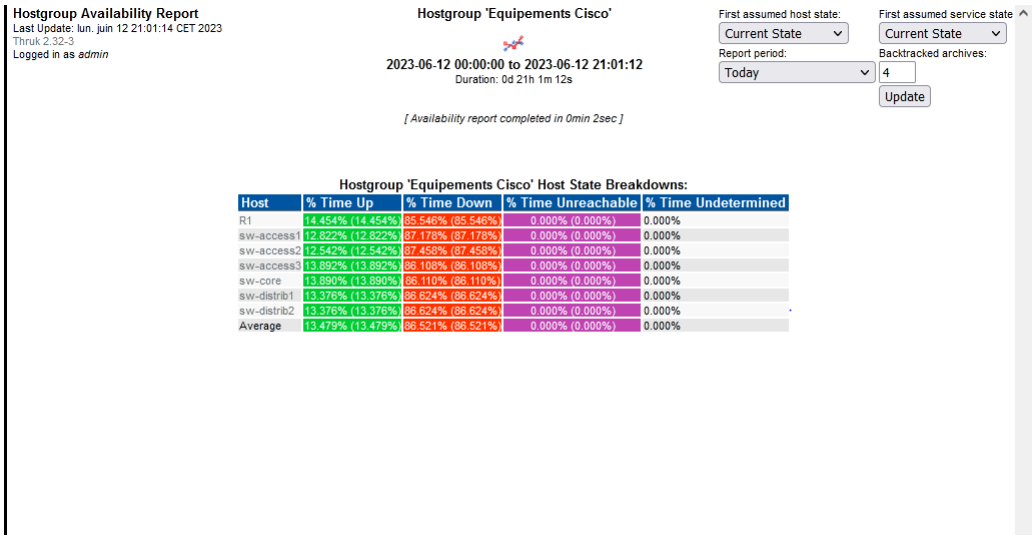



FIGURE 4.42 – Exemple de rapport.

### 4.4.5 Les logs

Un fichier log permet de stocker un historique des événements survenus sur un serveur, un ordinateur ou une application. Ce "journal" présenté sous la forme d'un fichier, ou équivalent, liste et horodate tout ce qui se passe [8].

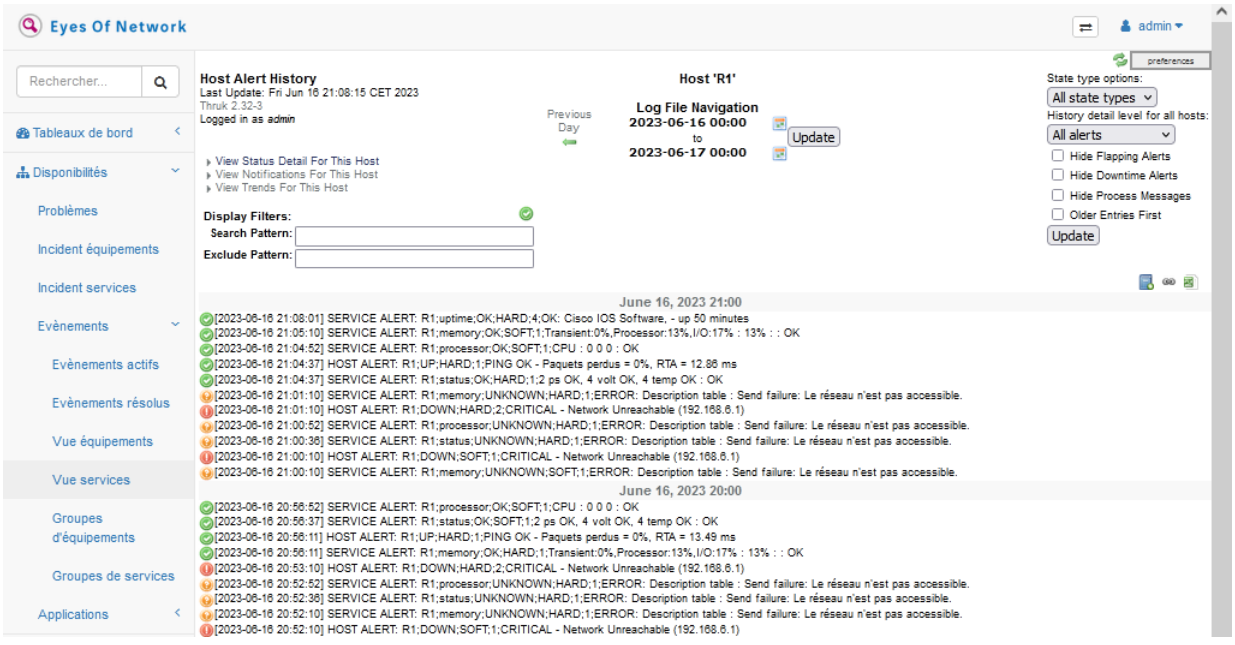



FIGURE 4.43 – Affichage des logs d'alerte du routeur R1.

### 4.4.6 La cartographie NagVis

NagVis est un addon de visualisation pour le système de gestion de réseau bien connu Nagios. Il peut être utilisé pour visualiser les données Nagios, par exemple une infrastructure réseau [9].

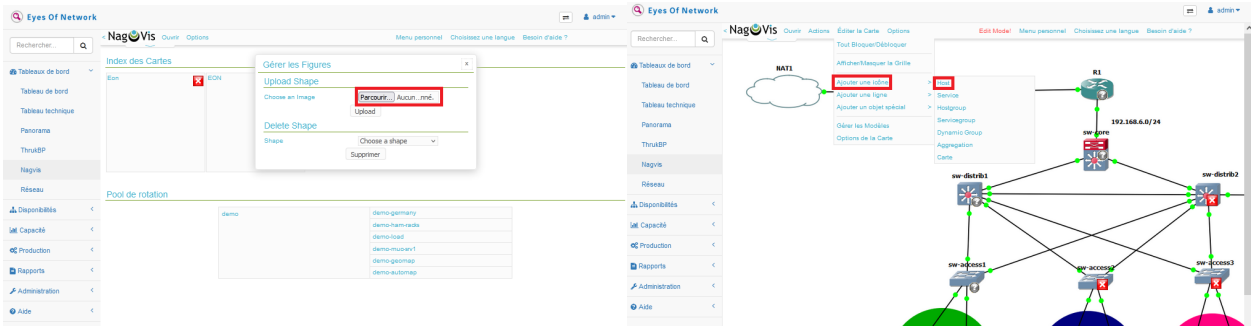



FIGURE 4.44 – Ajout de la cartographie.

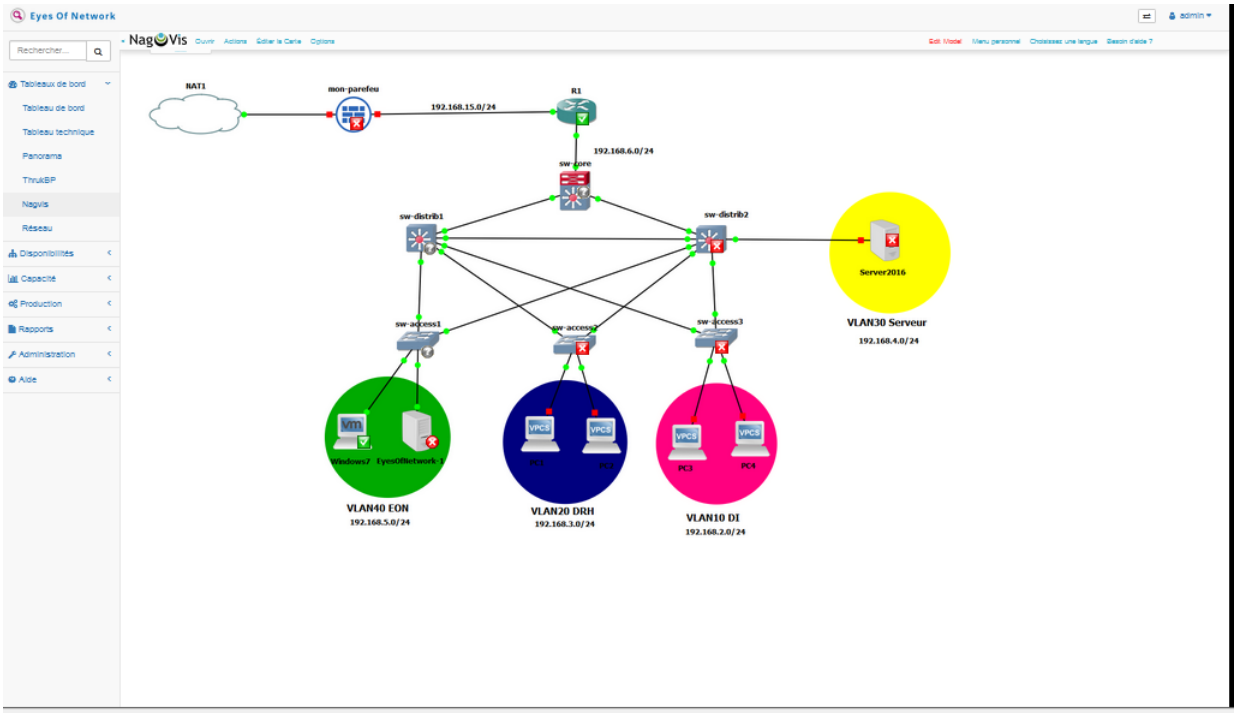



FIGURE 4.45 – Affichage de la carte.

### 4.4.7 Installation de Postfix

Installer le package illustrés dans la figure 4.46 sur le serveur EON pour que le serveur postfix fonctionne correctement avec un compte GMAIL.

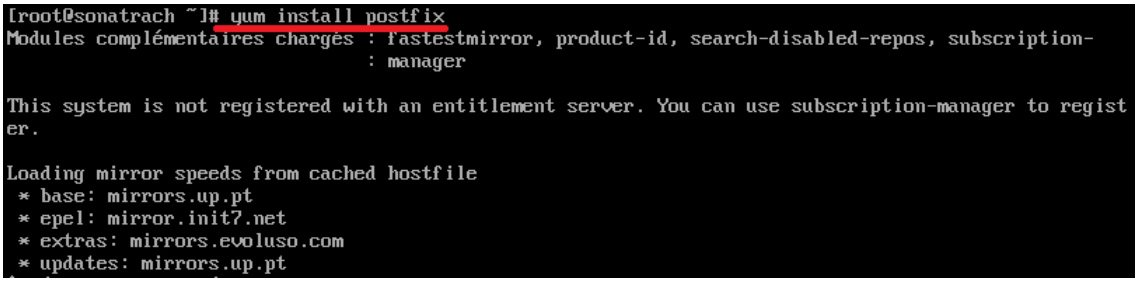



FIGURE 4.46 – Commande d'installation du package postfix.

### 4.4.8 Ajout du contact

- Avant d'ajouter un contact sur notre serveur de supervision, il est nécessaire d'installer un serveur de messagerie telle que HmailServeur**(voir Annexe B)**.

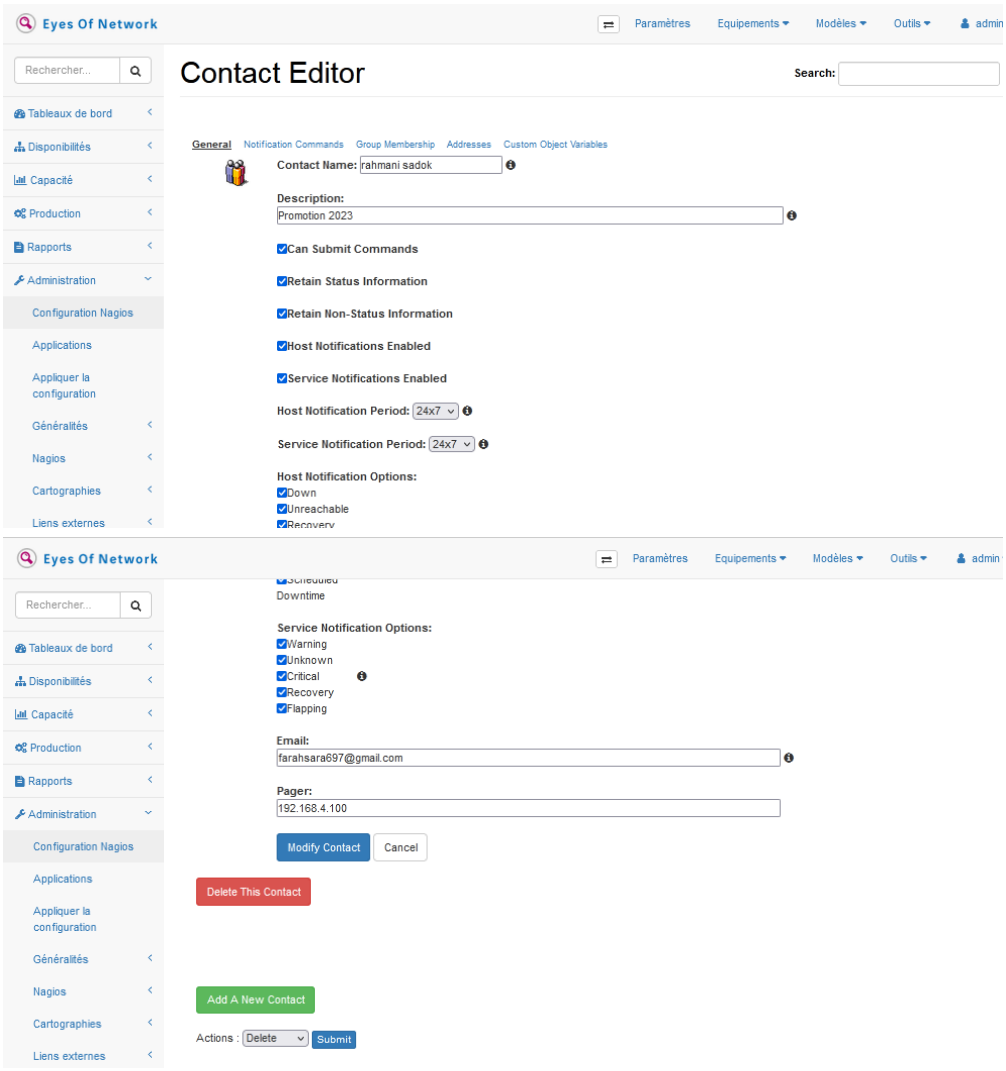



FIGURE 4.47 – Ajout du contact.

- Ensuite, on ajoute les notifications nécessaire afin de recevoir les e-mails.

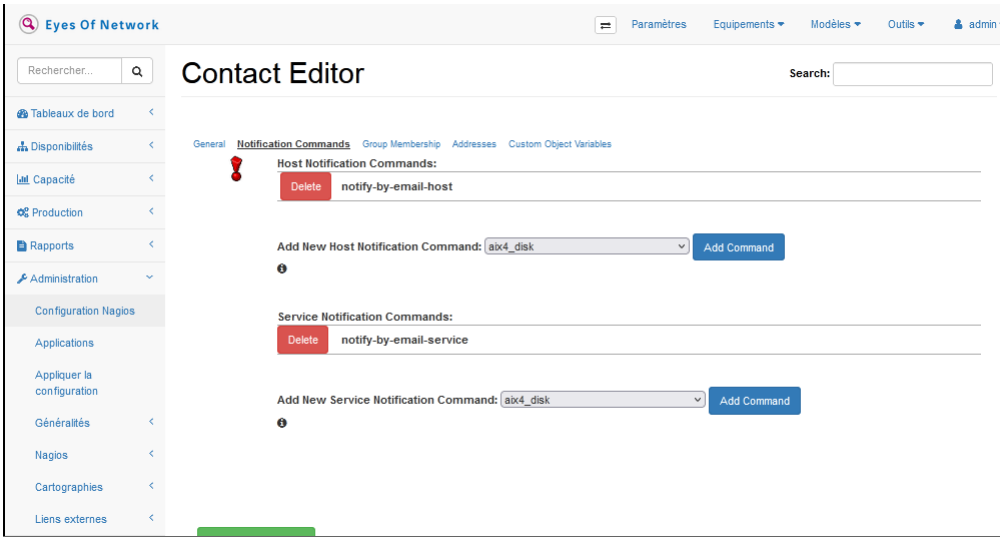



FIGURE 4.48 – Ajout des notifications.

-Réception du message d'alerte d'un des équipements.


FIGURE 4.49 – Réception du message d'alerte.

## 4.5 Conclusion

Dans ce chapitre nous avons mis en évidence l'aspect pratique de notre projet, tout d'abord nous avons détaillé les étapes de préparation. Par la suite nous avons reproduit le réseau LAN de SONATRACH sous GNS3 pour le superviser et enfin, nous avons décrit l'installation, la configuration de Eyes Of Network ainsi que l'implémentation de certaines de ses fonctionnalités.

# Conclusion générale

Notre étude approfondie sur les problèmes et les pertes de données rencontrés par un réseau informatique en l'absence de supervision a mis en évidence l'importance cruciale de mettre en place une solution de supervision adéquate. Nous avons souligné les risques liés à la sécurité des données et aux pertes économiques qui peuvent résulter d'un manque de supervision.

Au cours de notre étude, nous avons constaté que la mise en place de la solution Eyes of Network présente de nombreux avantages significatifs. Tout d'abord, elle permet une surveillance proactive en temps réel, permettant de détecter rapidement les anomalies et les problèmes potentiels. Cela contribue à minimiser les temps d'arrêt, à optimiser les performances du réseau, à améliorer la satisfaction des utilisateurs, mais aussi grâce à ses fonctionnalités d'alerte et de reporting, elle permet de facilité la résolution rapide des problèmes et la réductions des pannes.

En conclusion, La réalisation de ce projet s'est révélée extrêmement bénéfique et fructueuse pour nous, à plusieurs égards. Car, cela nous a offert l'opportunité de mettre en pratique les connaissances que nous avons acquises tout au long de notre formation. En appliquant concrètement les concepts théoriques, nous avons pu consolider nos compétences en administration système et réseaux.

Par conséquent, nous recommandons vivement l'adoption de cette solution aux entreprises qui souhaitent optimiser leur infrastructure réseau et assurer un fonctionnement fiable et sécurisé de leurs systèmes, tout en l'améliorant pour en tirer un maximum d'avantages, d'efficacité et de facilité d'emploi.

De ce fait, avec la multiplication des cyberattaques et des vulnérabilités, notre perspective inclus des fonctionnalités de sécurité renforcées.

# Annexe A

## Installation de Eyes Of Network

**1.**Configuration de la machine virtuelle

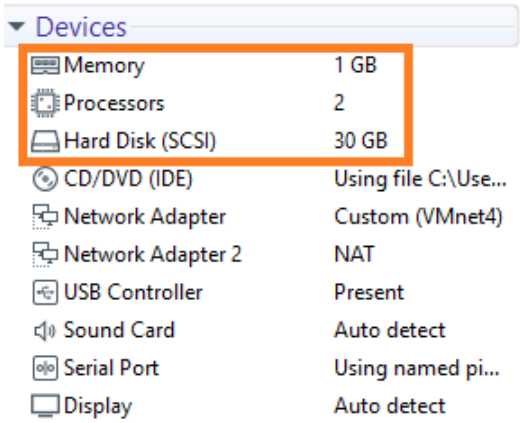



FIGURE 50 – Configuration de du serveur.

**2.**Choisir la langue d'installation, dans notre cas « français » :

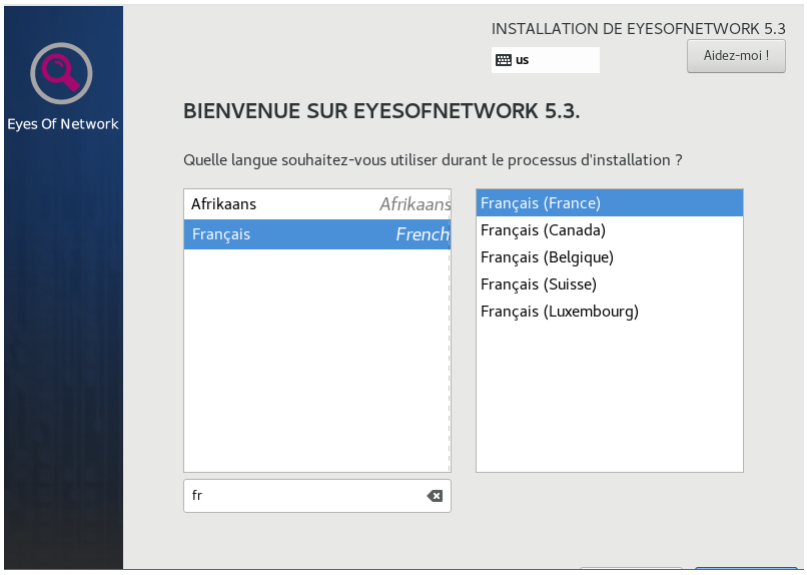



FIGURE 51 – choix de la langue.

**3.**On Sélectionne le disque sur lequel nous voulons faire l'installation. Puis on clique sur « Terminé ».

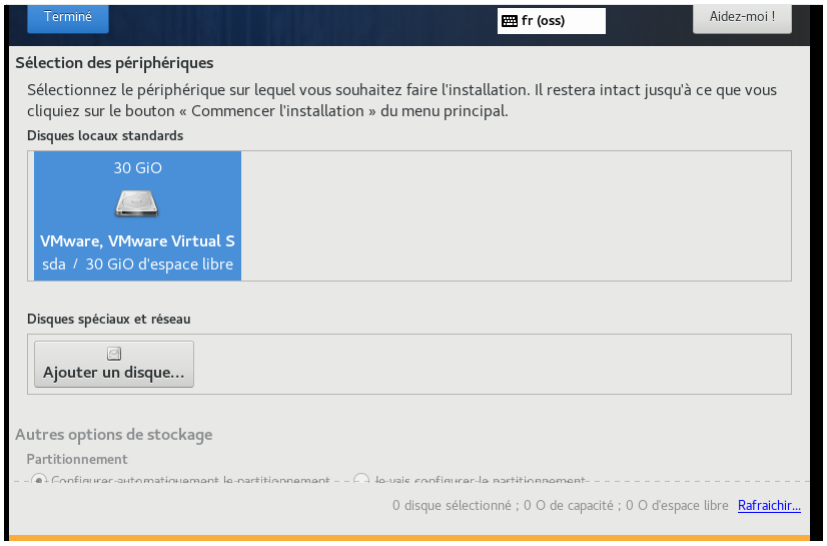



FIGURE 52 – Sélection du disque.

**4.**Ensuite nous allons sur « selection de logiciels » et nous choisirons « EyesOfNetwork Supervision ».

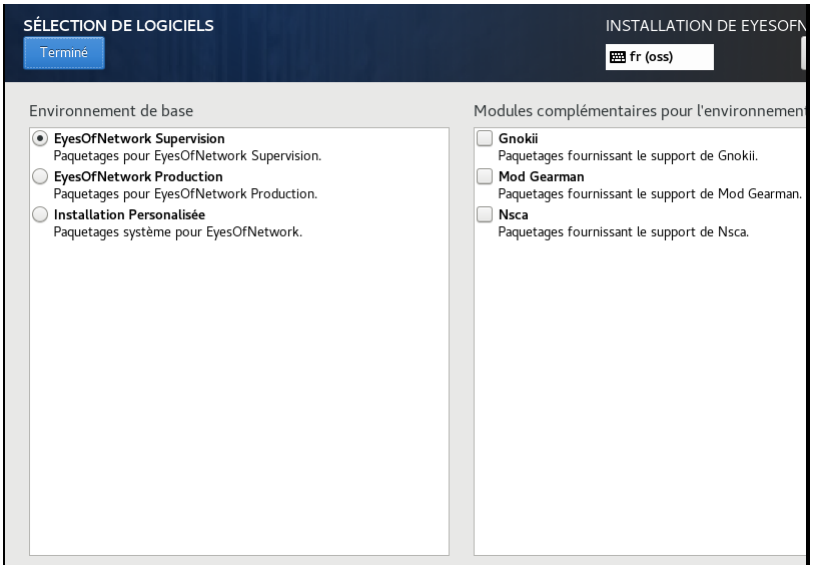



FIGURE 53 – Sélection de logiciels.

**5.**On va sur « nom d'hôte et réseau » pour configurer l'adresse ip, le masque et la passerelle comme suite :

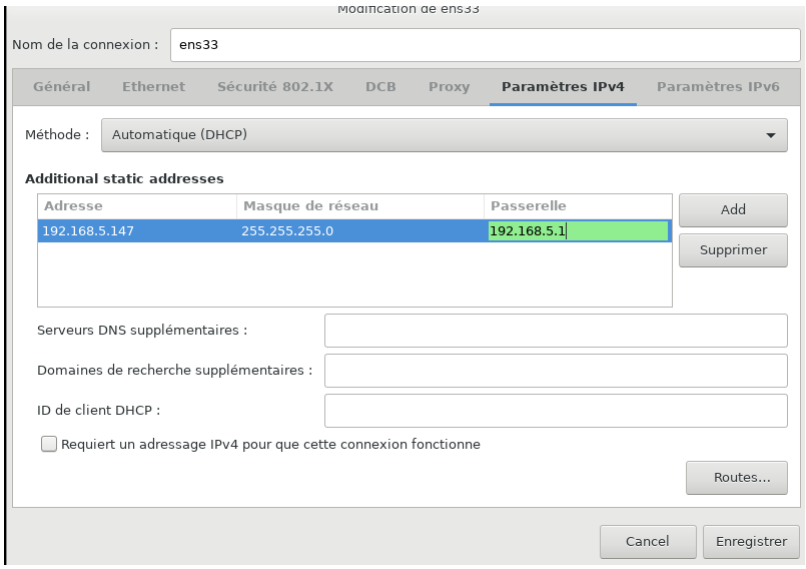



FIGURE 54 – Configuration de l'adresse ip du Serveur EON.

**6.**On donne un nom d'hôte

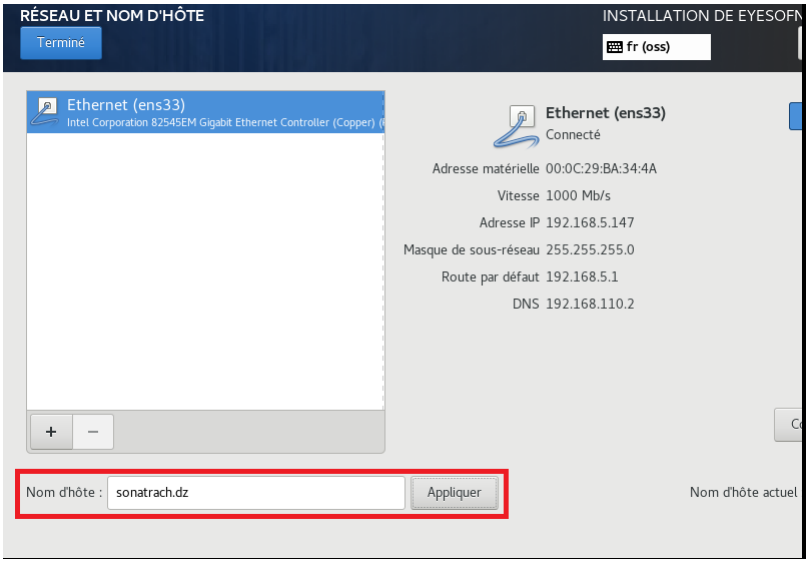



FIGURE 55 – Domaine ajouter.

**7.**Une fois la configuration IP terminée, on démarre l'installation, pendant l'installation on renseigne le mot de passe administrateur et on crée un utilisateur.

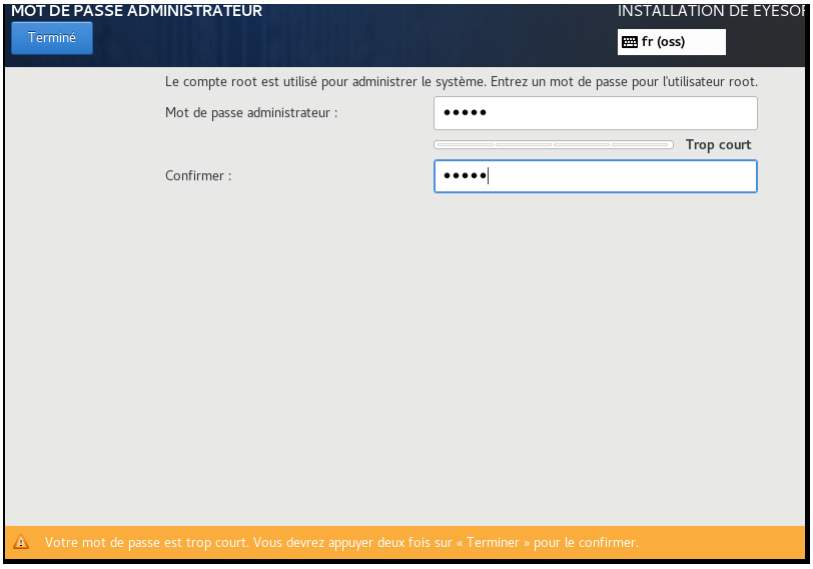



FIGURE 56 – Création du mot de passe.

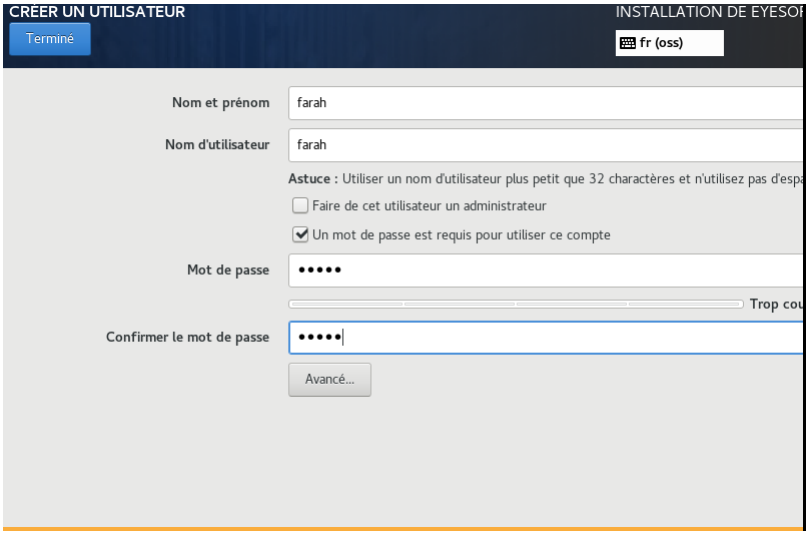



FIGURE 57 – Création de l'utilisateur.

**8.**On attend la fin de l'installation, puis on redémarre le serveur une fois le message terminé apparait comme suit :


FIGURE 58 – Installation terminé.

**9.**Une fois redémarrait Se connecter avec "root" et le mot de passe que nous avons enregistré tout à l'heure, puis vérifions l'adresse configurer précédemment à l'aide de la commande « ifconfig ».

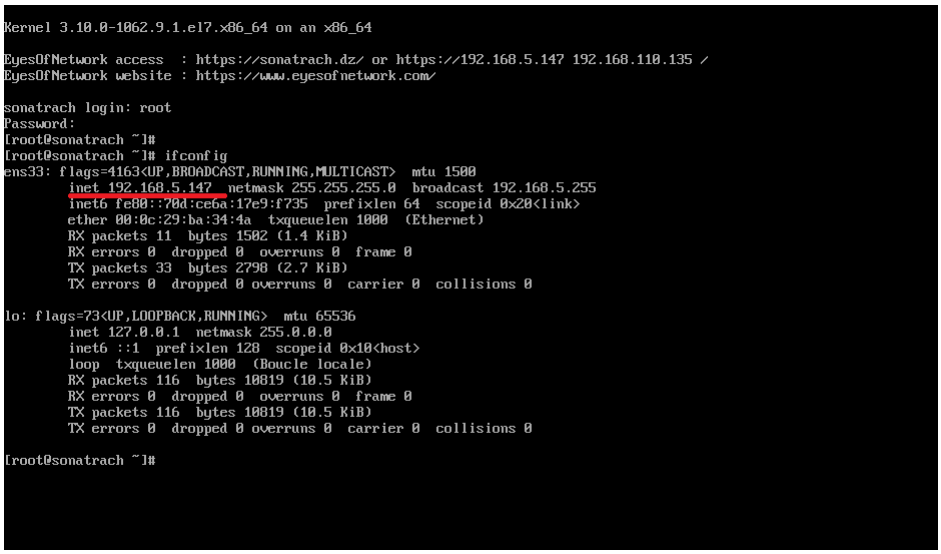



FIGURE 59 – Commande de vérification de l'addresse IP.

**10.**On se connecte sur le navigateur avec l'adresse 192.168.5.147 du serveur EON. Une fois sur cette page et il suffit simplement de se loger avec son login / mot de passe.

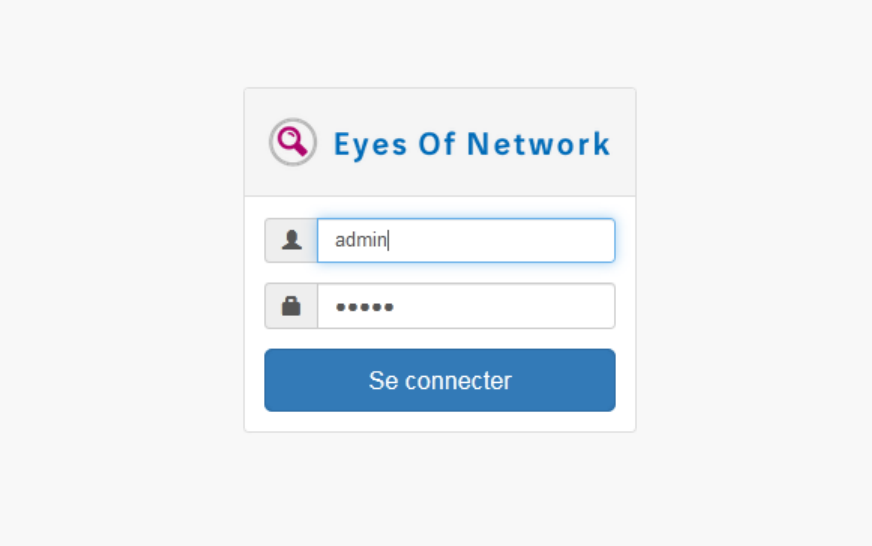



FIGURE 60 – L'interface de connexion.

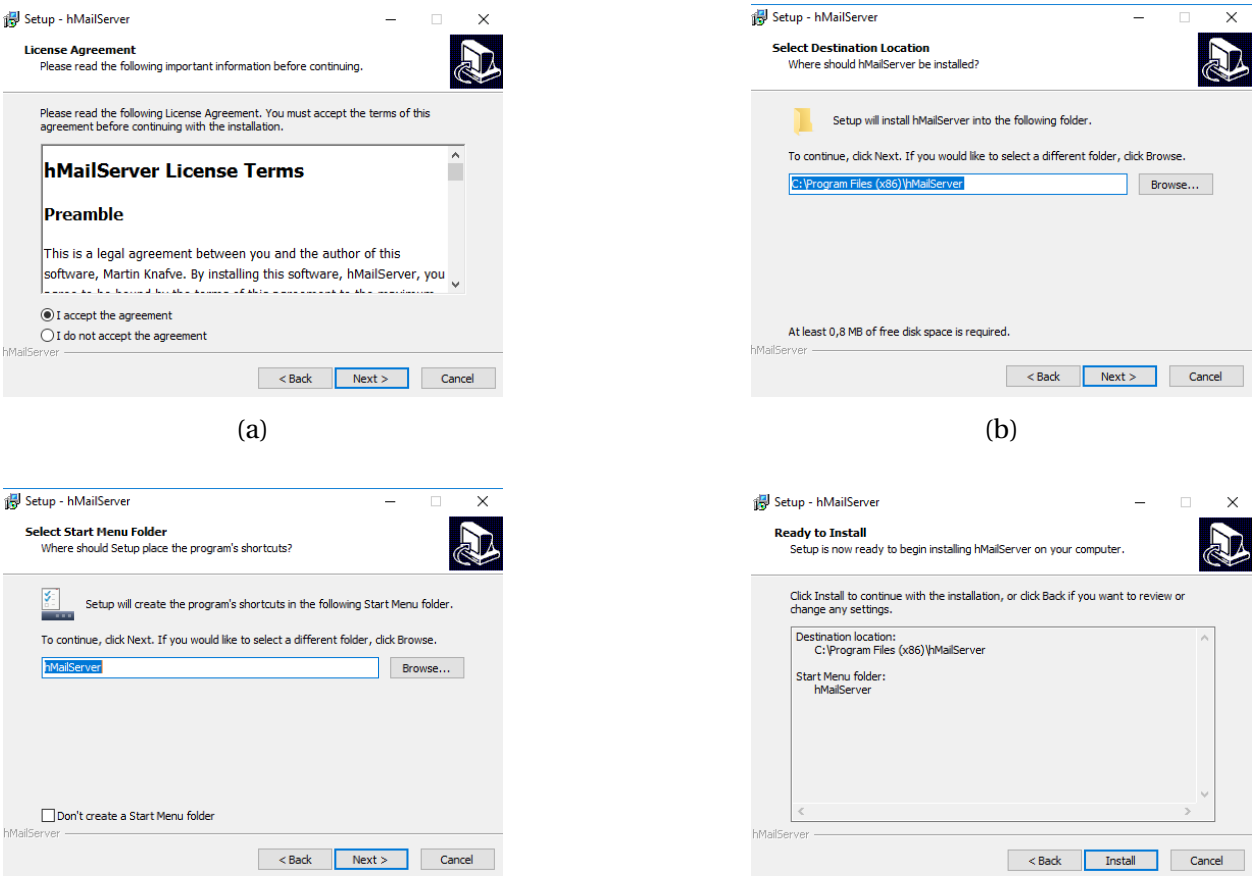
# Annexe B

## Installation et configuration de HMAILSERVER

### Présentation de HMAILSERVER

Hmailserveur est un logiciel de serveur de messagerie électronique, Les protocoles utilisés sont : SMTP, POP ou IMAP. Il permet de récupérer tous les comptes et les mots de passe grâce à un accès direct à Active directory, pour la création du compte de messagerie.

### Installation




(a) (b)

(c) (d)

FIGURE 61 – Installation de HmailServer.

# Configuration

1.Ajout du nom de domaine dans notre cas nous avons choisis "gmail.com".

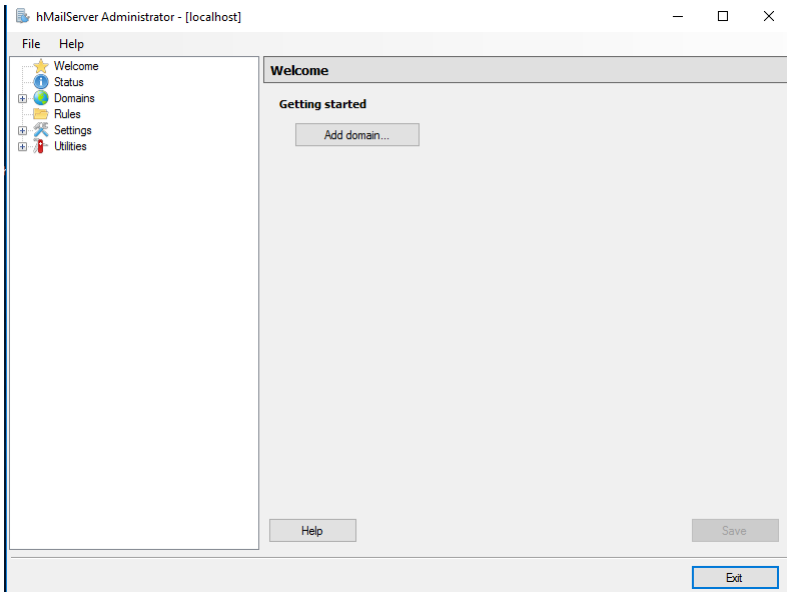



FIGURE 62 – Ajout du nom de domaine.

2.Ajout du compte Gmail ou nous allons recevoir nos alertes.

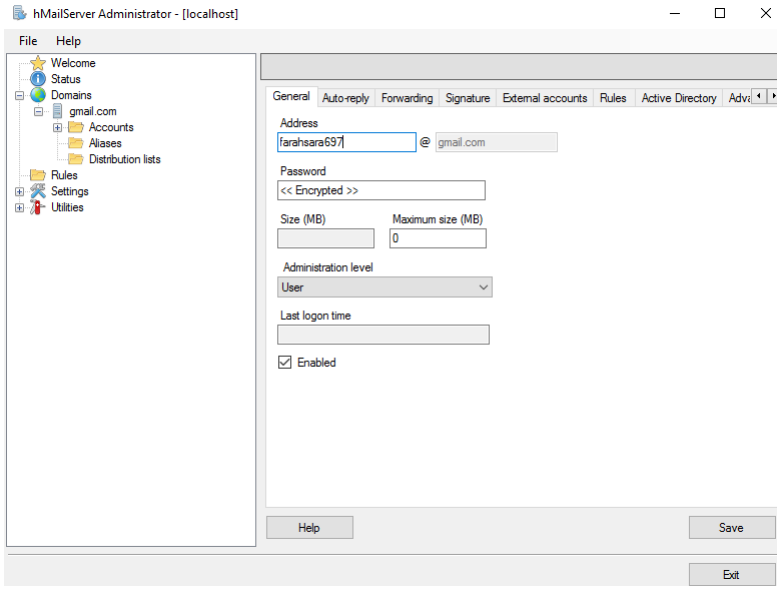



FIGURE 63 – Ajout de compte.

3.Attribution de l'adresse ip du serveur hmail et du port approprié au protocole IMAP.

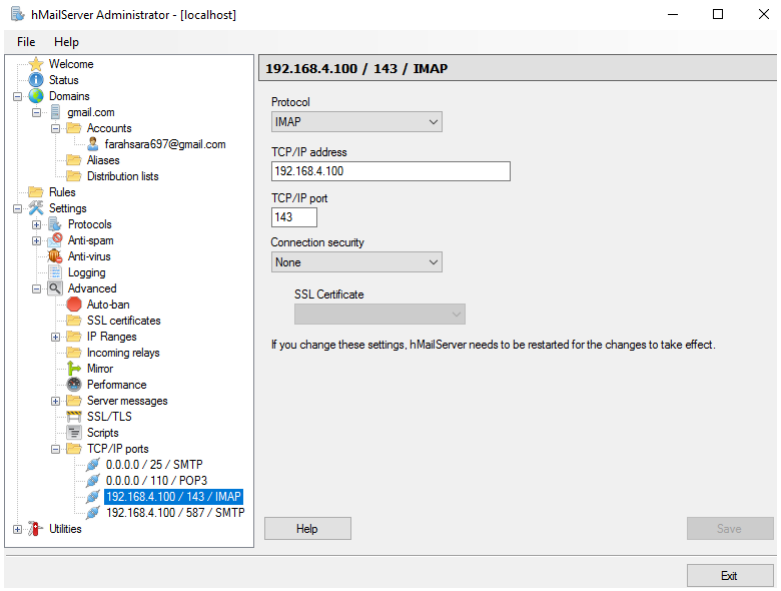



FIGURE 64 – Ajout du protocole IMAP.

4.Attribution de l'adresse ip du serveur hmail et du port approprié au protocole SMTP

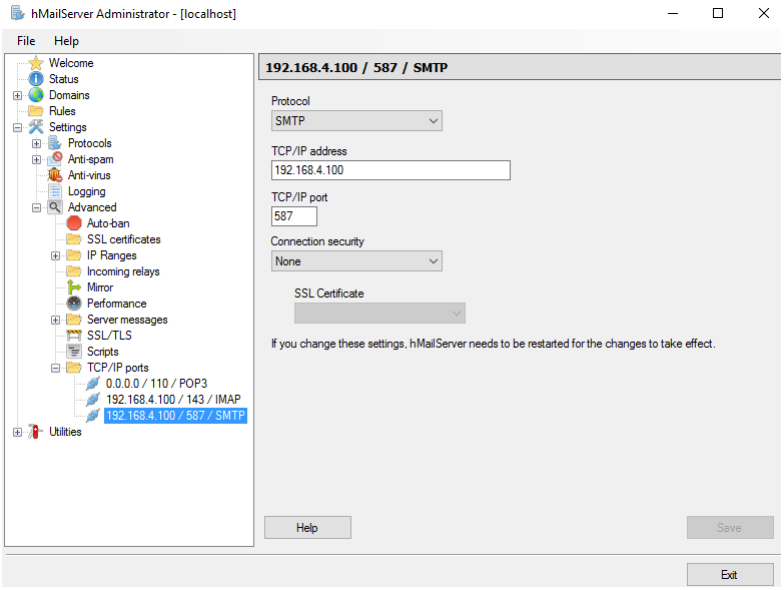



FIGURE 65 – Ajout du protocole SMTP.

# Bibliographie


[1] J.GABES, D.JEAN, A.TEMPLE, M.CEDRIC et B.MAKEREVITCH, NAT. Nagios3 pour la supervision et la metrologie. 20, rue des Grands-Augustins, 75006 Paris. : ÉDITIONS EYROLLES, 2009. ISBN : 978-2-212-12473-6.

[2] J.BROOKS, C.GROW, P.CRAIG, D.SHORT, Cybersécurité sécurisation des systèmes informatique, B. SUP, Éd., 2021, p. 712.

[3] W. Barth, Nagios : System and Network Monitoring, 2nd Edition, Kindle éd., W. Pollock, Éd., 2009, p. 822.

[4] B.Morin, C.Lorens, L.Levier, D.Valois, Tableaux de bord de la sécurité réseau, Eyrolles éd., Paris, 2010, p. 561.

[5] M.OZAN, DOCUMENTATION FAN, 2008.

[6] R.GOUPILLE, Technologie des ordinateurs et des réseaux : Cours et exercices corrigés, 8éme ed. Dunod, Paris, 2008.

[7] K.LOIC, F.BRUNO, Centreon-maitriser la supervision de votre system informatique. ENI, 2012.

[8] A.Pellen,(2018). EyesOfNetwork configuration (EON : 2/3). Récupéré sur https ://pellenalexandre.wordpress.com/2018/01/16/eyes-of-network/(consulté le : 22/04/2023).

[9] Disponible sur : https ://www.eyesofnetwork.com/fr/docs/5_3(consulté le : 22/04/2023).

[10] P.team,« Découvrez les 16 meilleurs outils de supervision réseau », Pandora FMS Monitoring Blog, 30 juin 2021. https ://pandorafms.com/blog/fr/outils-supervision-reseau/(consulté le : 12/05/2023).

[11] « Eyes Of Network : solution complète de supervision | memo-linux.com ». https ://memo-linux.com/eyes-of-network-solution-complete-de-supervision/(consulté le : 12/05/2023).

[12] F.PIGNET. Réseaux informatique : Supervision et Administration. ENI, Paris, Décembre 2007.

[13] Q.LOUSSE, J.LON, Supervision centralisée d'infrastructures distantes en réseaux avec gestion Des alarmes et notification des alertes. Ingénieur industriel, Institut supérieur industriel de Bruxelles, 2005.

[14] A.GHILI,A.MEZMAT. Etude et mise en place d'un outil de monitoring et de supervision des réseaux informatique : cas d'étude SONALGAZ. Mémoire master, Université de Bejaia, 2016.

[15] M.ABBOU, M.ABACHERIF. Mise en place d'une solution de supervision Cacti Cas d'étude : Cévital. Mémoire master, Université de Bejaia, 2021.

[16] B.IDRISSI, S.OUDRISS, Etude et mise en œuvre d'un outil de supervision de réseau. Rapport de stage, Ecole nationale des sciences appliquées de Tanger.

[17] « Protocole SNMP », FRAMEIP.COM, 23 septembre 2022. disponible sur : https ://www.frameip.com/snmp/(consulté le : 25/06/2023).

[18] D. Soulages, « Vlan Trunking Protocol : Introduction VTP », Formip, 6 septembre 2019. disponible sur : https ://formip.com/vlan-trunking-protocol-introduction-vtp/(consulté le : 10/06/2023).

[19] « Virtual Local Area Network - Vlan - Définition - Sewan », Sewan Groupe. https ://www.sewan.fr/lexique/vlan/(consulté le : 10/06/2023).

[20] Disponible sur : « EV Observe - Reportings - Rapports d'activité - XWiki »(consulté le : 25/06/2023).

# Résumé

Le Système d'information est désormais un élément essentiel de l'infrastructure organisationnelle des entreprises. En raison de son importance capitale, il est impératif de disposer d'outils de supervision permettant de garantir son bon fonctionnement et d'évaluer sa disponibilité.

De ce fait, la solution Eyes Of Network a été retenue. Nous l'avons choisi après une étude comparative des différents outils de supervision concurrents. L'outil déployé permet une surveillance complète d'un parc informatique. Plusieurs critères ont été pris en considération lors de la sélection de EON, notamment la disponibilité en tant que logiciel libre, les performances élevées, l'adaptabilité aux besoins spécifiques et la richesse des fonctionnalités proposées telles que son bundle (Nagios, Nagvis, Grafana…).

En bref, l'objectif de ce travail a pour but de mettre en évidence les avantages significatifs de l'implémentation d'EON en assurent une disponibilité ainsi qu'une surveillance proactive des réseaux informatiques, de performance et de résolution rapide des problèmes liée aux pannes. Nous avons démontré l'efficacité de l'outil de supervision Eyes Of Network, à base de protocoles SNMP, via plusieurs tests.



**Mots clés :** supervision, Eyes Of Network, SNMP, Nagios, Nagvis, Grafana.



# Abstract

The information system is now an essential part of a company's organizational infrastructure. Because of its vital importance, it is imperative to have monitoring tools that can guarantee its smooth operation and assess its availability.

That's why we chose the Eyes Of Network solution. We chose it after a comparative study of the various competing supervision tools. The tool deployed enables complete monitoring of an IT estate. A number of criteria were taken into account when selecting EON, including its availability as open source software, its high performance, its adaptability to specific needs and the wealth of features offered, such as its bundle (Nagios, Nagvis, Grafana...).

In short, the aim of this work is to highlight the significant advantages of implementing EON to ensure availability and proactive monitoring of computer networks, performance and rapid fault resolution. We have demonstrated the effectiveness of the Eyes Of Network monitoring tool, based on SNMP protocols, via several tests.



**Keywords :** supervision, Eyes Of Network, SNMP, Nagios, Nagvis, Grafana.