République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA-BEJAIA

جامعة بجاية

Tasdawit n Bgayet

Université de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique


# MÈMOIRE

## EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER PROFESSIONNEL

**Domaine :** Mathématiques et Informatique **Filière :** Informatique

**Spécialité :** Administration et sécurité des réseaux

**Présenté par**


**Mlle DJENNANE Lynda**

**Mlle KASSA Radia**


***Thème***

# Etude et proposition d'une solution de supervision réseau basée sur Pandora FMS au profit de l'EPB

**Soutenu le 24 Septembre 2020 devant le jury composé de :**

| Nom et Prénom | | Grade | | |
|---|---|---|---|---|
| M. | AISSANI Sofiane | MCA | Univ. de Béjaia | Président |
| M. | YAZID Mohand | MCA | Univ. de Béjaia | Rapporteur |
| M. | MOKTEFI Mohand | MAA | Univ. de Béjaia | Rapporteur |
| Mme. | HOUHA Amel | MAA | Univ. de Bouira | Examinateur |

**Année Universitaire : 2019/2020**

# *Remerciements*

Il nous est particulièrement agréable d'exprimer ici notre reconnaissance et gratitude envers tout ce qui ont rendu possible ce travail.

Tout d'abord, nous remercions Dieu le Tout-Puissant qui nous a donné le courage, la force et la volonté tout au long de notre parcours.

Un grand merci pour nos familles, surtout nos parents qui nous ont soutenus tout au long de ce projet.

Notre reconnaissance s'adresse plus particulièrement à notre encadrant **Mr. YAZID Mohand** et notre Co-encadrant **Mr. MOKTEFI Mohand** pour tous les précieux conseils qu'ils nous ont prodigués.

Nos vifs et chaleureux remerciements s'adressent également à **Mr TOUATI Badreddine** et tout le personnel de l'EPB pour leur orientation et accueil sympathique durant la période de stage.

Enfin, nous tenons à remercier également tous les membres de jury pour avoir accepté d'évaluer notre travail.

# *Dédicaces*

Ce modeste travail est dédié :

À nos chers parents, à nos frères et sœurs, à nos enseignants, à nos amis et à tous ceux qui nous ont soutenus de près ou de loin.

*DJENNANE Lynda et KASSA Radia*

# TABLE DES MATIÈRES

# TABLE DES FIGURES

# LISTE DES TABLEAUX

# LISTE DES ABRÉVIATIONS

| | |
|---|---|
| ACL | Access Control List |
| ADSL | Asymmetric Digital Subscriber Line |
| AIX | Advanced Interactive eXecutive |
| AP | Access Point |
| API | Application Programming Interface |
| A-PON | ATM Over PON |
| ASN | Access Serving Network |
| ASN.1 | Abstract Syntax Notation 1 |
| ASN-GW | Access Serving Network Gateway |
| ATM | Asynchrounous Transfer Method |
| BDD | Base De Donnée |
| BS | Base Station |
| BSD | Berkeley Software Distribution |
| BSS | Basic Service Set |
| CCITT | Comité Consultatif International Téléphonique et Télégraphique |
| CMIP | Common Management Information Protocol |
| CMIS | Common Management Information Service |
| CPU | Central Processing Unit |
| CRC | Cyclic Redundancy Check |
| CSN | Connectivity Serving Network |
| DHCP | Dynamic Host Configuration Protocol |
| DIX | Digital Equipment Corp, Intel et Xerox |
| DMAP | Distributed Management Application Processus |

| | |
|---|---|
| DMZ | DeMilitarized Zone |
| DNS | Domain Name System |
| DSI | Direction des Systèmes d'Information |
| DSL | Digital Suscriber Line |
| DSLAM | Digital Suscriber Line Access Module |
| EPB | Entreprise Portuaire de Bejaia |
| EPE-SPA | Entreprise Publique Économique, Société par Actions |
| E-PON | Ethernet Passive Optical Network |
| ERP | Enterprise Resource Planning |
| ESS | Extended Service Set |
| ESSID | Extended Service Set Identifier |
| FDSE | Full-Duplex Switched Ethernet |
| FMS | Flexible Monitoring System |
| FTP | Foiled Twisted Pair |
| FTP | File Transfer Protocol |
| FTTC | Fiber-To-The-Curb |
| FTTH | Fiber-To-The-Home |
| FTTN | Fiber-To-The-Node |
| FTTT | Fiber-To-The-Terminal |
| GED | Gestion Electronique de Document |
| GMAO | Gestion de la Maintenance Assistée pour Ordinateurs |
| GNS3 | Graphical Network Simulator-3 |
| G-PON | Giga Passive Optical Network |
| HD | High-Definition |
| HDSL | High bit rate DSL |
| HP-UX | Hewlett Packard Unix |
| HSPA | High Speed Packet Access |
| HTTP | HyperText Transfer Protocol |
| IBSS | Independent Basic Service Set |
| ICMP | Internet Control Message Protocol |
| IDSL | Integrated Service Digital Network DSL |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |

| | |
|---|---|
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPMI | Intelligent Platform Management Interface |
| KVM | Keyboard, Video (monitor) and Mouse |
| LAN | Local Area Network |
| LMS | LAN Management Solution |
| LTE | Long Term Evolution |
| MAN | Metropolitan Area Network |
| MIB | Management Information Base |
| MSA | Managed System and Agents |
| NAS | Network-Attached Storage |
| NMS | Network Management Station |
| OHSAS | Occupational Health and Safety Assessment Series |
| OID | Object IDentifier |
| OLT | Optical Line Terminal |
| ONT | Optical Network Terminal |
| ONU | Optical Network Unit |
| OSI | Open System Interconnexion |
| PD | Power Delivery |
| PHP | Hypertext Preprocessor |
| PKI | Public Key Infrastructure |
| PoE | Power over Ethernet |
| PON | Passive Optical Network |
| PRTG | Paessler Router Traffic Grapher |
| RAID | Redundant Array of Independent Disks |
| RGT | Réseau de Gestion des Télécommunications |
| RJ45 | Registered Jack45 |
| RLE | Réseau Local d'Entreprise |
| RMON | Remote Network Monitoring |
| RNIS | Réseau Numérique à Intégration de Service |
| RRDtool | Round-Robin Database tool |
| RRM | Radio Resource Management |
| SC | Subscriber Connector |

| | |
|---|---|
| SDSL | Symetric Digital Suscriber Line |
| SGMP | Simple Gateway Monitoring Protocol |
| SHDSL | Single-pair High-speed Digital Subscriber Line |
| SI | Système d'Information |
| SLA | Service Level Agreement |
| SMAE | System Management Application Entity |
| SMAP | System Management Application Process |
| SMFA | Specific Management Function Area |
| SMI | Structure of Management Information |
| SNMP | Simple Network Management Protocol |
| SQL | Structured Query Language Server |
| SS | Subscriber Station |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| ST | Straight Tip |
| STP | Spanning Tree Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| Telnet | TELetype NETwork |
| TMN | Telecommunications Management Network |
| UDP | User Datagram Protocol |
| UIT-T | Union internationale des Télécommunications-Telecommunication |
| UPS | Uninterruptible Power Supply |
| VDSL | Very high speed Digital Suscriber Line |
| VLAN | Virtual Local Area Network |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| VTP | Vlan Trunking Protocol |
| WAN | Wide Area Network |
| WDS | Windows Déploiement Services |
| Wi-Fi | Wireless Fidelity |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WLAN | Wireless local Area Network |
| WMAN | Wireless Metropolitan Area Network |

| | |
|---|---|
| WMI | Windows Management Instrumentation |
| WUX | WEB User eXperience |
| WWAN | Wireless Wide Area Network |

# INTRODUCTION GÉNÉRALE

Depuis le développement de l'informatisation des entreprises, la question de la sécurité et de la robustesse du système d'information est au cœur des préoccupations des administrateurs réseau et système, et leur maîtrise est devenue cruciale. Ils doivent fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité requise, et surtout travailler à réduire les problèmes de défaillances, les pannes, les coupures et les différents problèmes techniques qui peuvent causer des pertes considérables. Ces craintes sont donc à l'origine de la création et du succès des outils de surveillance. C'est pourquoi les administrateurs réseau font appel à ces outils afin de vérifier l'état du réseau en temps réel et d'avoir une vue de l'ensemble du parc informatique, il peut être aussi averti (par email, par SMS) en cas de problèmes.

Grâce à un tel système, le temps d'intervention est considérablement réduit et les anomalies peuvent être traitées immédiatement avant que l'utilisateur ne s'en aperçoive. Ainsi, la supervision des réseaux s'avère nécessaire et indispensable. Elle permet entre autres d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau, mais aussi d'avoir des indicateurs sur la performance de notre architecture.

L'objectif visé par ce projet est la mise en place d'un outil de supervision pour l'administration et la surveillance du parc informatique de l'EPB (Entreprise Portuaire de Bejaïa).Pour mener à bien ce travail, nous avons structuré notre manuscrit en quatre chapitres :

Le premier chapitre aborde des concepts et généralités sur les réseaux d'entreprise.

Le deuxième chapitre portera sur la présentation des notions de base de l'administration et la supervision des réseaux.

Le troisième chapitre sera consacré à la présentation de l'organisme d'accueil et l'étude de son architecture afin de tirer une problématique et énumérer les différentes solutions, et par la suite nous ferons une présentation détaillée de la solution retenue.

Le quatrième chapitre concerne la modélisation et l'implémentation de la solution de supervision retenue.

Enfin, notre projet s'achève par une conclusion générale et des perspectives.

# CHAPITRE 1

# CONCEPTS ET GÉNÉRALITÉS SUR LES RÉSEAUX D'ENTREPRISE

## 1.1 Introduction

Le besoin de communication et de partage a poussé les entreprises à s'orienter vers les réseaux informatiques et travailler davantage pour les améliorer. À travers ce chapitre nous allons présenter les réseaux d'entreprise, les différentes technologies utilisées, ainsi que les équipements actifs et passifs.

## 1.2 Réseaux d'entreprise

Un réseau d'entreprise est un ensemble d'équipements matériels , connectés ensemble dans un bâtiment ou dans une zone particulière, qui appartiennent tous à la même entreprise ou aux mêmes institutions, et ce pour atteindre les objectifs suivants [22] :

- Le partage de ressources (fichiers, applications ou matériels) ;
- La communication entre personnes (courrier électronique, discussion en direct, etc.) et le travail coopératif ;
- La communication entre processus (entre des machines industrielles par exemple) ;
- La garantie de l'unicité de l'information (base de données).

Il existe différentes catégories de réseaux d'entreprise, on peut les classifier selon leur taille, leur vitesse de transfert des données ainsi que leur étendue, on définit généralement les catégories de réseaux suivantes :

- Local Area Network (LAN) ou réseau local ;

- Metropolitan Area Network (MAN) ou réseau métropolitain ;
- Wide Area Network (WAN) ou réseau étendu.

La connexion physique qui relie ces types de réseau peut être câblée (filaire) ou bien réalisée à l'aide de la technologie sans fil.

La figure 1.1 illustre les réseaux LAN, MAN, WAN :

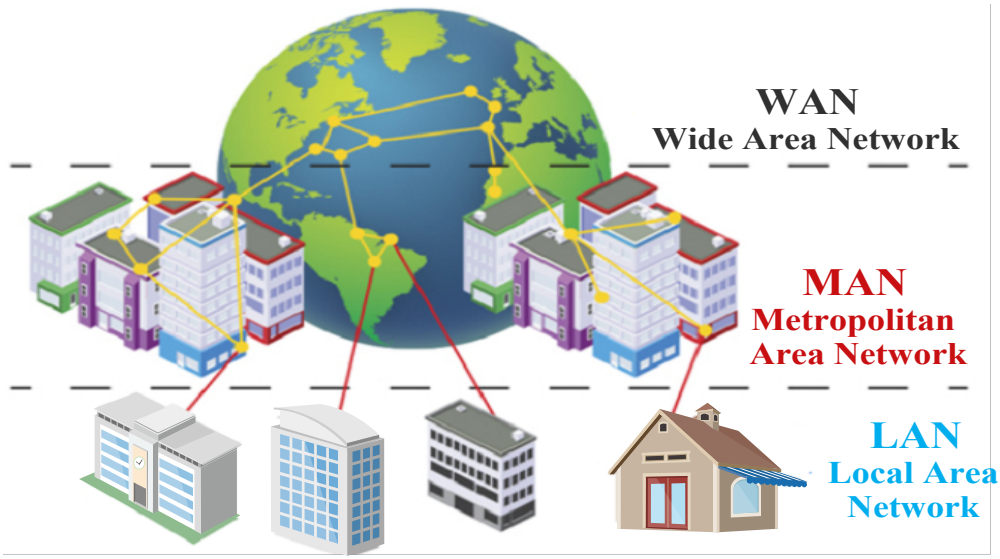


FIGURE 1.1 – Les réseaux LAN, MAN, WAN.

## 1.3 Réseaux locaux d'entreprise

Un réseau local, appelé aussi réseau local d'entreprise (RLE), désigne un réseau habituellement privé, il permet d'interconnecter les ordinateurs d'une entreprise ou d'une organisation. Il offre des débits importants, et sa taille est limitée à quelques kilomètres. Si un réseau local est implémenté par radio, on le nomme WLAN (Wireless local area network) ou réseau local sans fil [10].

On distingue généralement deux technologies qui sont déployées dans les entreprises :

- Le LAN filaire qui est basé sur la technologie Ethernet ;
- Le LAN sans fil qui est basé sur la technologie Wi-Fi (Wireless Fidelity).

### 1.3.1 Technologie Ethernet commuté

L'Ethernet commuté consiste à utiliser la trame Ethernet dans un réseau de transfert dont les nœuds sont des commutateurs. On utilise dans ce cas un Ethernet particulier, ou Ethernet FDSE (Full-Duplex Switched Ethernet), sur les lignes de communication duquel il est possible

d'envoyer des trames Ethernet dans les deux sens simultanément. L'avantage de la commutation Ethernet par rapport à l'Ethernet partagé est de ne pas imposer de distance maximale entre deux nœuds étant donné qu'il n'y a plus de risque de collision.

Ethernet est actuellement «le standard» utilisé sur les réseaux locaux de gestion, c'est un réseau local (LAN) à diffusion dont les spécifications sont définies par la norme IEEE (Institute of Electrical and Electronics Engineers ) 802.3 [32].

Les réseaux Ethernet sont symbolisés par Ethernet x base y. Un nom de la forme x B y se lit de la façon suivante :

B : modulation de base ;

x : bande passante (en mégabits par seconde) ;

y : définie le type de câble utilisé :

- **5 :** câble coaxial de 1.7 cm de diamètre (gros Ethernet) ;
- **2 :** câble coaxial de 0.5 cm de diamètre (Ethernet fin) ;
- **T :** paires torsadées ;
- **F :** fibre optique.

  **Exemple** : 10 base T

#### 1.3.1.1 Domaines d'application Ethernet

Ethernet couvre les domaines suivants :

- La vidéosurveillance ;
- La gestion des bâtiments ;
- Panneaux numériques ;
- Distributeurs et systèmes d'information commerciale ;
- Points d'accès sans fil, téléphones VoIP (Voice over IP) et autres dispositifs alimentés (PD, Power Delivery) ;
- Les foyers, les entreprises et l'industrie.

#### 1.3.1.2 Évolution de la technologie Ethernet

Le tableau 1.1 présente l'évolution de la technologie Ethernet [2] :

| **Année** | **Standard** | **Description** |
|---|---|---|
| 1973 | Ethernet | Invention d'Ethernet par le Dr Robert Metcalf de Xerox corp. |
| 1980 | Norme DIX Ethernet II | DIX (Digital Equipment Corp, Intel et Xerox) mettent au point une norme Ethernet de 10 Mbit/s sur un câble coaxial. |
| 1983 | IEEE 802.3 10 BASE -5 | Ethernet 10 Mbit/s sur un câble coaxial épais. |
| 1985 | IEEE 802.3a 10 BASE -2 | Ethernet 10 Mbit/s sur un câble coaxial fin. |
| 1990 | IEEE 802.3i 10 BASE -T | Ethernet 10 Mbit/s sur un câble à paires torsadées. |
| 1993 | IEEE 802.3j 10 BASE -F | Ethernet 10 Mbit/s sur un câble à fibre optique. |
| 1995 | IEEE 802.3u 100 BASE -xx | Fast Ethernet : Ethernet 100 Mbit/s sur des câble à paires torsadées et fibre (plusieurs normes). |
| 1998 | IEEE 802.3z 1000 BASE -X | Gigabit Ethernet sur un câble à fibre optique. |
| 1999 | IEEE 802.3ab 1000 BASE -T | Gigabit Ethernet à paires torsadées. |
| 2002 | IEEE 802.3ae 10G BASE -xx | 802.3at PoE (Power over Ethernet). |
| 2006 | IEEE 802.3an 10 G BASE -T | Optimisation de l'alimentation PoE. |
| 2009 | 802.at (PoE) | Optimisation de l'alimentation PoE. |
| 2015 | 100GbE et 40GbE | 100G/40G pour la fibre optique. |
| 2016 | 2,5 et 5GBASE -T | 2,5 Gigabits et 5 Gigabits Ethernet sur un câble à paires torsadées. |

TABLE 1.1 – Évolution de la technologie Ethernet.

#### 1.3.1.3 Avantages et inconvénients de la technologie Ethernet

Le tableau 1.2 présente les avantages et inconvénients de la technologie Ethernet :

| **Avantages** | **Inconvenients** |
|---|---|
| • Vitesse très rapide ;<br>• Connexion stable, sans interruption ;<br>• Échanges sécurisés à travers un câble ;<br>• Transfert de données plus fiable. | • Les échecs de dépannage : Un réseau câblé a plus de points de défaillance qu'un réseau sans fil ;<br>• Mobilité des équipements presque nulle ;<br>• Ajout d'équipements plus difficile puisque des travaux de câblage sont nécessaires ;<br>• Utilisation de câbles encombrants ;<br>• Coût d'installation élevé causé par le câblage. |

TABLE 1.2 – Avantages et inconvénients de la technologie Ethernet.

### 1.3.2 Technologie WiFi

Le Wi-Fi (Wireless Fidelity) est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11. Grâce aux normes WiFi, il est possible de mettre en place des réseaux locaux sans fils à haut débit sous réserve d'être à proximité d'un point d'accès. Le wifi permet de relier tous les périphériques de liaison à haut débit sur un rayon de plusieurs dizaines de mètres [22].

#### 1.3.2.1 Architecture WiFi

L'architecture 802.11 repose sur la notion de cellule BSS (Basic Service Set), de station et de point d'accès AP (Access Point). Un réseau sans fil peut exploiter deux modes de fonctionnement :

- **Mode infrastructure :** en mode infrastructure le client sans-fil est en liaison avec la station de base qui sert de pont avec le réseau câblé. Cette configuration de base est dite cellule BSS ou ensemble de services de base. Si plusieurs BSS sont connectées sur le même réseau câblé, on forme un ESS (Extended Service Set) ou ensemble de services étendu. Chaque BSS ou ESS est repérable par un SSID (Service Set Identifier) ou ESSID (Extended Service Set Identifier) [18].

La figure 1.2 présente le mode infrastructure :

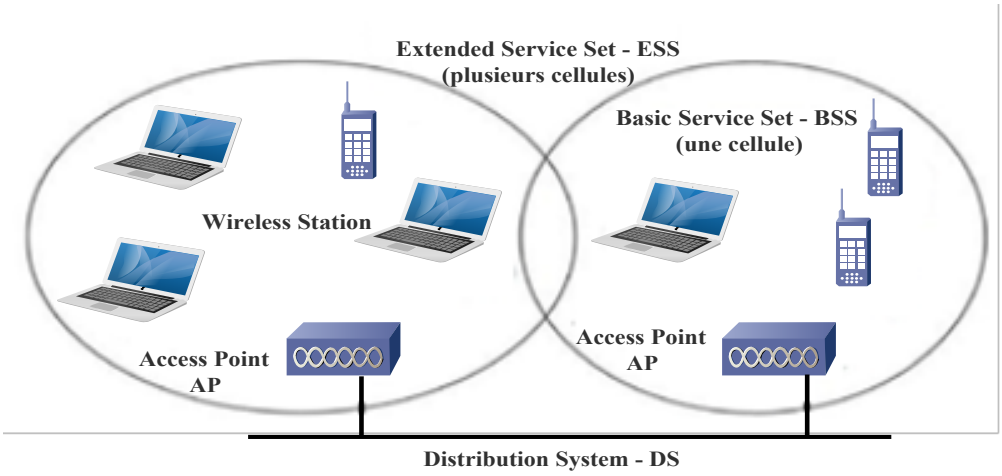


FIGURE 1.2 – Mode infrastructure.

- **Mode Ad-Hoc :** le mode *ad hoc*, également appelé mode sans infrastructure ou IBSS (Independent Basic Service Set), permet à des stations de communiquer directement entre elles sans utiliser un point d'accès. Ce mode simplifié permet de réaliser rapidement une communication entre deux stations sans fil [23].

La figure 1.3 suivante présente le mode ad hoc :

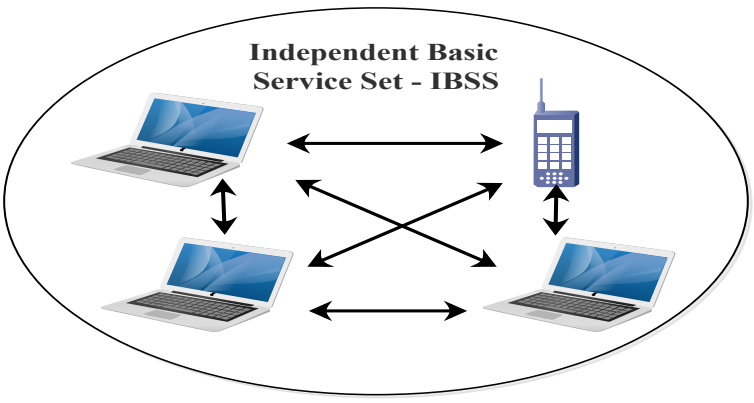


FIGURE 1.3 – Mode Ad-Hoc.

#### 1.3.2.2 Domaines d'application WiFi

La technologie WiFi couvre les domaines suivants :

- L'industrie, et le domaine militaire ;
- L'extension du réseau d'entreprise ;

- Le Wi-Fi à domicile ;
- Le point à point ;
- Desserte de lieux collectifs (campus, facultés, hôpitaux ...).

#### 1.3.2.3 Évolution de la technologie WiFi

Le tableau 1.3 présente l'évolution de la technologie WiFi :

| **Norme** | **Description** |
|---|---|
| **norme 802.11b** | Elle propose un débit théorique de 11 Mbits/s (6 Mbits/s réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé [21]. |
| **norme 802.11a** | Elle permet d'obtenir un haut débit (dans un rayon d'environ 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels) [21]. |
| **norme 802.11g** | Offre un débit plus élevé (54 Mbit/s théoriques, 25 Mbit/s réels). Cette norme offre une compatibilité ascendante avec la norme 802.11 [21]. |
| **norme 802.11n** | Offre un débit théorique de 300 Mbit/s, mais réel constaté plus proche de 40 Mbit/s dans un rayon de 100 mètre. Cette norme apporte des améliorations par rapport aux normes IEEE 802.11a/b/g [22]. |
| **norme 802.11ac** | Offre un débit pouvant atteindre 500 Mbps chacun, soit jusqu'à 7 Gps de débit global [22]. |

TABLE 1.3 – Évolution de la technologie WiFi.

#### 1.3.2.4 Avantages et inconvénients de la technologie WiFi

Le tableau 1.4 présente les avantages et inconvénients de la technologie WiFi :

| **Avantages** | **Inconvenients** |
|---|---|
| • Mobilité ;<br>• Facilité d'installation ;<br>• Coût : La plupart des éléments du réseau WiFi (point d'accès, répéteurs, antennes...) peuvent être simplement posés. L'installation peut donc parfois se faire sans le moindre outillage, ce qui réduit les coûts de main-d'œuvre ;<br>• Évolutivité : La facilité d'extension ou de restriction du réseau permet d'avoir toujours une couverture WiFi correspondant aux besoins réels. | • Sécurité : Le WiFi étant un réseau sans fil, il est possible de s'y connecter sans intervention matérielle ;<br>• Portée limitée ;<br>• Chute rapide des débits ;<br>• Interférences : les ondes peuvent aller polluer les communications d'un réseau voisin, qui devient moins performant. |

TABLE 1.4 – Avantages et inconvénients de la technologie WiFi.

## 1.4 Réseaux métropolitains d'entreprise

Un réseau métropolitain, appelé aussi réseau métropolitain d'entreprise, désigne un réseau privé ou public, qui permet l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit, sa taille est limitée à quelques dizaines de kilomètres [34]. Si un réseau métropolitain est implémenté par radio, on le nomme WMAN (Wireless Metropolitan area network) ou réseau métropolitain sans fil qui est basé sur la technologie WiMAX (Worldwide Interoperability for Microwave Access).

### 1.4.1 Technologie WiMAX

WiMAX signifie *Worldwide Interoperability for Microwave Access*. Il s'agit d'un standard de réseau sans fil métropolitain créé par les sociétés Intel et Alvarion en 2002 et ratifié par l'IEEE sous le nom IEEE-802.16. Le débit théorique maximum supporté par le WiMAX est de 70 Mbit/s sur une portée de 50 Km. En pratique, WiMAX permet d'atteindre 12 Mbit/s sur une portée de 20 km. L'objectif du WiMAX est de fournir une connexion internet à haut débit sur une zone de couverture de plusieurs kilomètres de rayon [22].

#### 1.4.1.1 Architecture WiMAX

L'architecture de la technologie WiMAX se compose principalement de stations de base (BS, Base Station), et des stations mobiles (SS, Subscriber Station). La station de base joue le rôle d'une antenne centrale chargée de communiquer et de desservir les stations mobiles qui, à leur tour, servent les clients utilisant le WIFI ou l'ADSL (Asymmetric digital subscriber line) [26].

La figure 1.4 représente l'architecture générale d'un réseau d'accès à large bande :

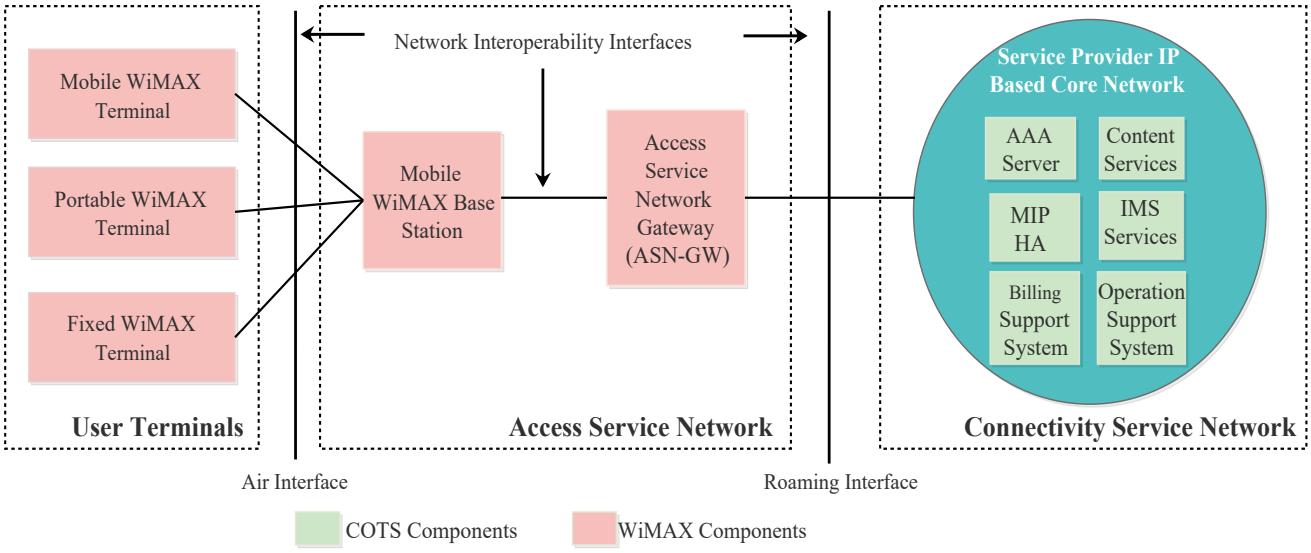


FIGURE 1.4 – Architecture du réseau WiMAX.

Le réseau WiMAX est constitué de la partie d'accès aux services (ASN), de la partie de connexion aux services (CSN) et des terminaux d'abonnés.

- **Access Serving Network (ASN) :** C'est le réseau d'accès radio du WiMAX, il regroupe un ou plusieurs passerelles et des stations de base BS. L'ASN assure la couverture radio et la gestion des fonctionnalités d'accès MAC comme le paging, la gestion des ressources radio (RRM Radio Resource Management) et la mobilité entre les BS (pour la norme 802.16e). Les passerelles ASN-GW (ASN Gateway) assurent l'interconnexion avec le CSN [26].
- **Connectivity Serving Network (CSN) :** C'est un ensemble de fonctionnalités assurant la connectivité IP aux stations d'abonnés WiMAX. Le CSN regroupe des passerelles pour l'accès Internet, des routeurs, des serveurs et des « proxy » de sécurité ainsi que des bases de données. Il permet également le contrôle d'admission et gère la mobilité inter-ASNs (pour la norme 802.16e) [26].

- **Les terminaux d'abonnés :** Sont des équipements spéciaux équipés d'une carte WiMAX qui permet la communication avec ce réseau, ils sont situés dans la zone de couverture d'une BS pour pouvoir communiquer avec cette dernière [27].

#### 1.4.1.2 Domaines d'application WiMAX

Un des usages possibles du WiMax consiste à couvrir la zone dite du dernier kilomètre, encore appelée boucle locale radio, c'est-à-dire fournir un accès à internet haut débit, aux zones non couvertes par les technologies filaires classiques (telle que l'ADSL) [22].
Le WiMAX couvre les domaines suivants :

- Zones isolées (sites ruraux, montagnes, désert, engins mobiles...) ;
- Zones démunies d'infrastructures de télécommunications au sol (zones non équipées, sinistrées) ;
- Zone stratégique (Banques et assurances, administrations publiques, télémaintenance).

#### 1.4.1.3 Évolution de la technologie WiMAX

Les normes du WIMAX sont en évolution continue. Le tableau 1.5 présente les trois standards 802.16 les plus importants :

| **Norme** | **Description** |
|---|---|
| **IEEE 802.16d (IEEE 802.16 2004)** | Révise et corrige quelques erreurs détectées dans les standards 802.16 et 802.16a et apporte des améliorations. C'est le standard que suivent les produits WiMAX fixe [34]. |
| **IEEE 802.16e (IEEE 802.16 2005)** | Définit la mobilité jusqu'à des vitesses de l'ordre de 100 km/h [37]. |
| **IEEE 802.16m (IEEE 802.16 2009)** | Définit la nouvelle génération du WiMAX (WiMAX phase 2), Elle offre des débits en nomade ou stationnaire jusqu'à 1 Gbit/s et 100 Mbit/s en mobilité à grande vitesse [37]. |

TABLE 1.5 – Évolution de la technologie WiMAX

#### 1.4.1.4 Avantages et inconvénients de la technologie WiMAX

Le tableau 1.6 présente les avantages et inconvénients de la technologie WiMAX :

| **Avantages** | **Inconvenients** |
|---|---|
| • Facilité d'installation dans les zones difficiles à câbler ;<br>• Une Connexion internet à haut débit symétrique sans support filaire ;<br>• Une Connexion illimitée gérée par une plate-forme sécurisée et redondante ;<br>• Service internet plus rapide que l'ADSL ;<br>• Permet la connectivité internet sans fil à haut débit sur de longues distances. | • Pour avoir des distances et des débits optimaux, l'émetteur et le récepteur doivent être en «ligne de vue . Hors «ligne de vue», les débits chutent rapidement ;<br>• Le débit est partagé entre les usagers d'une même antenne centrale ;<br>• Nécessite de disposer d'un point haut : afin d'assurer la meilleure couverture possible, l'émetteur doit être placé sur un point haut (pylône, château d'eau, etc.) ;<br>• Existence d'obstacle physique. |

TABLE 1.6 – Avantages et inconvénients de la technologie WiMAX.

## 1.5 Réseaux WAN d'entreprise

Un réseau étendu, appelé aussi réseau WAN d'entreprise encore appelé réseau longue distance, couvre de vastes zones géographiques à l'échelle d'un pays, et relie plusieurs réseaux plus petits comme des LAN ou des MAN.

Les fournisseurs de services internet utilisent des WAN pour connecter les réseaux locaux d'entreprise et les clients à internet [10].

Si un réseau étendu est implémenté par radio, on le nomme WWAN (Wireless Wide Area Network) ou réseau étendu sans fil.

On distingue généralement quatre technologies qui sont déployées dans les entreprises :

- Le WAN filaire qui est basé sur la technologie XDSL (Digital Suscriber Line, ligne d'abonné numérique) et XPON (Passive Optical Network) ;
- Le WAN sans fil qui est basé sur la technologie 4G et 5G.

### 1.5.1 Technologie XDSL

La technologie DSL (Digital Suscriber Line, ligne d'abonné numérique) permet d'assurer des transmissions numériques haut débit, sur de la paire torsadée classique. On distingue généralement deux canaux : une voie montante allant de l'abonné vers le réseau et une voie descendante allant du réseau vers l'abonné. Voie montante et voie descendante ont un débit différent dans les techniques asymétriques et un même débit dans les techniques symétriques. Ce débit théorique chute généralement en fonction de la distance et n'est donc effectif que dans les premières centaines de mètres de la voie [18].

#### 1.5.1.1 Architecture XDSL

La figure 1.5 présente l'architecture XDSL :

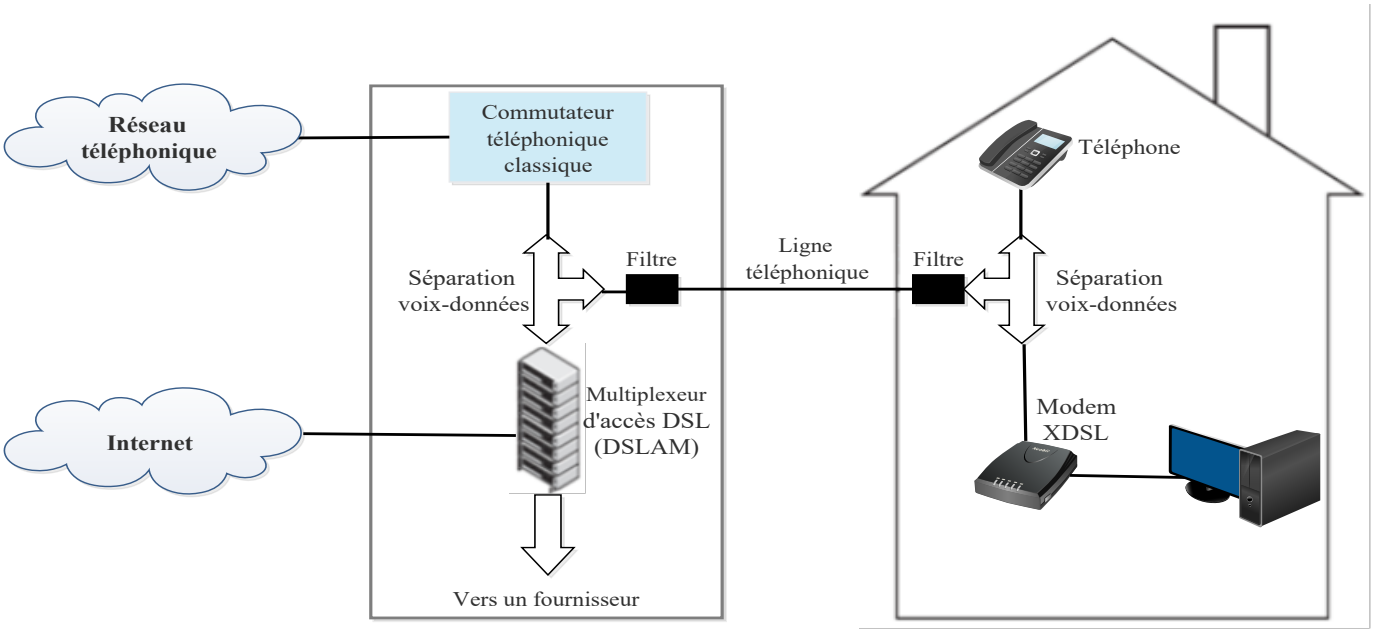


FIGURE 1.5 – Architecture XDSL.

- ✓ **DSLAM (DSL Access Module) :** les DSLAM forment l'autre extrémité de la liaison, chez l'opérateur. Ce sont des équipements dont le rôle est de récupérer les données émises par l'utilisateur depuis son équipement terminal au travers de son modem XDSL. Ces équipements intègrent des modems situés à la frontière de la boucle locale et du réseau de l'opérateur [34].
- ✓ **Filtre :** est responsable de l'éclatement et de la recombinaison des deux types de signaux dans le central et chez l'abonné (indispensable chez ce dernier uniquement lorsque celui-

ci utilise un téléphone numérique ; il sert alors à séparer les canaux utilisés pour la téléphonie de ceux employés pour la transmission des données) [14].

#### 1.5.1.2 Domaines d'application XDSL

Les technologies XDSL couvrent les domaines suivants :

- Les entreprises ;
- Services résidentiels : téléphone, télévision, connexion à l'internet...etc ;
- Interconnexion des réseaux locaux ;
- Téléconférence ;
- Réseaux haut débit ATM (Asynchrounous Transfer Method).

#### 1.5.1.3 Évolution de la technologie XDSL

Le tableau 1.7 présente l'évolution de la technologie XDSL [18] :

| **Appellation** | **Description** | **Débit descendant** | **Débit ascendant** | **Distance** |
|---|---|---|---|---|
| IDSL (Integrated Service Digital Network DSL) | Ligne d'abonnée numérique RNIS(réseau numérique à intégration de service) | 144 kbit/s | 144 kbit/s | 5 km |
| ADSL (Asymetric DSL) | Ligne d'abonnée numérique asymétrique | 8 Mbit/s | 2 Mbit/s | 5,5 km |
| ADSL2+ | Ligne d'abonnée numérique asymétrique (sans filtre) | 25 Mbit/s | 1,2 Mbit/s | 3 km |
| HDSL(High bit rate DSL) | Ligne d'abonnée numérique symétrique à haut débit | 2 Mbit/s | 2 Mbit/s | 3,6 km |

| | | | | |
|---|---|---|---|---|
| SDSL (Symetric DSL ou Single line DSL) | Ligne d'abonnée numérique symétrique | 2 Mbits/s | 2 Mbits/s | 3 km |
| SHDSL (Single-pair High-speed Digital Subscriber Line) | Ligne d'abonnée numérique symétrique à haut débit | 2,3 Mbit/s | 2,3 Mbit/s | 5,4 km |
| VDSL (Very high speed ou Very high bit rate DSL) | Ligne d'abonnée numérique asymétrique à très haut débit | 52 Mbit/s | 6,4 Mbit/s | 300 m à 1,5 km |
| VDSL 2 | Ligne d'abonnée numérique asymétrique à très haut débit | 92 Mbits/s | 36 Mbits/s | 300 m à 1,5 km |

TABLE 1.7 – Évolution de la technologie XDSL.

#### 1.5.1.4 Avantages et inconvénients de la technologie XDSL

Le tableau 1.8 présente les avantages et inconvénients de la technologie XDSL :

| **Avantages** | **Inconvenients** |
|---|---|
| • Conservation de l'installation existante (la paire de cuivre) ;<br>• Un accès à internet haut débit permanent ;<br>• La possibilité (comme avec le câble) de téléphoner tout en surfant sur le Web ;<br>• La vidéoconférence avec une grande qualité d'images, améliore les communications. | • D'une part, l'abonné ne doit pas être éloigné de plus de 5,4 Km de son central téléphonique de rattachement. Cette technologie est donc réservée de fait à des zones d'habitat dense ;<br>• D'autre part le débit est directement dépendant du trafic de la ligne, ce qui fait que les débits sont très variables. |

TABLE 1.8 – Avantages et inconvénients de la technologie XDSL.

### 1.5.2 Technologie XPON

PON (Passive Optical Network) Signifie « réseau optique passif », est un réseau de télécommunication qui transmet des données sur des lignes à fibres optiques. Il est utilisé dans les réseaux de desserte optique. Le PON est caractérisé par une architecture fibre Point-Multipoint passive. La ligne de transport principale peut être divisée en 32 lignes distinctes, ce qui nécessite beaucoup moins d'infrastructures que la construction de lignes directes vers chaque destination [20].

Un PON est parfois présenté comme le «dernier tronçon» entre le fournisseur et l'utilisateur ou entre la fibre optique et le X (FTTX), le «X» pouvant faire référence au [34] :

- **FTTC (Fiber-To-The-Curb) :** on câble jusqu'à un point assez proche de l'immeuble ou de la maison qui doit être desservi, le reste du câblage étant effectué par l'utilisateur final ;
- **FTTN (Fiber-To-The-Node) :** on câble jusqu'à un répartiteur dans l'immeuble lui-même ;
- **FTTH (Fiber-To-The-Home) :** on câble jusqu'à la porte de l'utilisateur ;
- **FTTT (Fiber-To-The-Terminal) :** on câble jusqu'à la prise de l'utilisateur, à côté de son terminal.

#### 1.5.2.1 Architecture XPON

L'architecture d'un réseau optique passif PON est basée sur 3 éléments essentiels [35] :

- **OLT (Optical Line Terminal) :** est l'équipement maître d'accès optique pour des clients connectés au FTTx, un lieu de collecte permet de distribuer des services tel que : l'internet, la téléphonie et la vidéo, cet équipement est actif, placé au central, envoie et reçoit des signaux lumineux porteurs des données.
- **ONU/ONT (Optical Network Unit / Optical Network Terminal) :** L'ONT peut-être considéré comme un modem optique auquel le client vient connecter sa passerelle d'accès au haut débit. C'est un élément terminal du réseau optique. L'ONT est l'interlocuteur direct de L'OLT.
- **Coupleur optique (splitter) :** Le coupleur optique «ou splitter» est un équipement passif installé sur le cheminement de la fibre optique entre l'OLT et les ONU, assure la fonction diviseur ou concentrateur de la transmission. Il ne nécessite aucune alimentation électrique, son fonctionnement est basé sur la seule propagation de la lumière à l'intérieur de la fibre. Dans le sens montant le coupleur permet de combiner par addition les signaux optiques, dans le sens inverse il divise le signal optique qui vient de L'OLT.

La figure 1.6 suivante présente les composantes principales d'une architecture XPON :

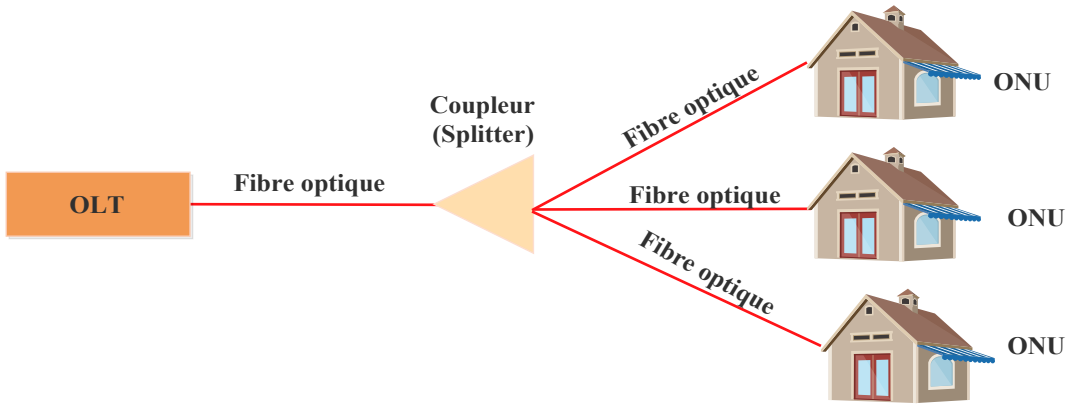


FIGURE 1.6 – Architecture XPON.

.

#### 1.5.2.2 Domaines d'application XPON

Les technologies XPON couvrent les domaines suivants :

- Les campus universitaires ;
- Les environnements d'entreprises ;

- Les réseaux de desserte optique (par exemple le FTTH) ;
- Les réseaux de transmission de données et les réseaux d'accès à internet à très haut débit.

#### 1.5.2.3 Évolution de la technologie XPON

Les technologies XPON se résument dans le tableau 1.9 [34] :

| Technologie | Description |
|---|---|
| **A-PON (ATM Over PON)** | C'est un système point multipoint sur fibre optique qui utilise l'ATM comme protocole de transmission. Avec l'APON, les données à haut débit, la voix et la vidéo peuvent être acheminées jusqu'aux abonnés sur une seule fibre. Un système APON peut relier jusqu'à 32 abonnés au PON et leur fournit un système d'accès flexible et un débit élevé (622 Mbit/s ou 155 Mbit/s dans le sens descendant, 155 Mbit/s dans le sens montant). |
| **E-PON (Ethernet Passive Optical Network** | Lorsque les trames qui sont émises sur le PON sont de type Ethernet, on parle d'EPON. L'objectif était de remplacer la technologie ATM, très coûteuse à mettre en œuvre sur une technologie multipoint, par la technologie Ethernet. |
| **G-PON (Giga Passive Optical Network)** | Les GPON ont pour objectif d'augmenter encore les débits pour suivre les progrès technologiques et atteindre 10 puis 40 Gbit/s. |

TABLE 1.9 – Évolution de la technologie XPON.

#### 1.5.2.4 Avantages et inconvénients de la technologie XPON

Le tableau 1.10 présente les avantages et inconvénients de la technologie XPON :

| **Avantages** | **Inconvenients** |
|---|---|
| • Peu de fibres optiques sont employées dans le réseau PON ;<br>• Aucun local alimenté en énergie n'est nécessaire dans ce type de réseau, ce qui entraîne des économies d'investissement, d'exploitation et de maintenance ;<br>• Au niveau de la centrale, le PON permet d'économiser de l'espace grâce au partage des ports des équipements actifs entre plusieurs abonnés. | • Budget optique limité par le coupleur, donc portée réduite ;<br>• Débit partagé et limité à la capacité de la fibre commune ;<br>• Les flux étant reçus par tout le monde, le tri se faisant au niveau des ONT. |

TABLE 1.10 – Avantages et inconvénients de la technologie XPON.

### 1.5.3 4G et 5G

Les communications entre utilisateurs mobiles se développent rapidement et représentent un marché qui est devenu énorme. Cinq générations de réseaux de mobiles se sont succédé. Dans cette partie, on va s'intéresser aux réseaux de mobile 4G et 5G.

#### 1.5.3.1 4G

4G est la quatrième génération des standards pour la téléphonie mobile correspondant au LTE (Long Term Evolution)-Advanced . Succédant à la 2G, la 3G et 3.5G (HSPA, High Speed Packet Access ), cette technologie permet le très haut débit mobile (débit théorique 150 Mbit/s, par cellule, voir plus) et permet également l'accès à plusieurs réseaux simultanément. L'une des caractéristiques de la 4G est d'avoir un réseau cœur basé que sur l'IP (Internet Protocol). Les objectifs de débit maximal définis pour le LTE sont les suivants : 100 Mbit/s en voie descendante pour une largeur de bande allouée de 20 MHz ; 50 Mbit/s en voie montante pour une largeur de bande allouée de 20 MHz [11].

**Avantages et inconvénients de la 4G :**

Le tableau 1.11 présente les avantages et inconvénients de la 4G :

| **Avantages** | **Inconvenients** |
|---|---|
| • Les téléchargements se font beaucoup plus rapidement (applications, photos...etc.) ;<br>• Très haut débit : son débit de transmission de données est largement supérieur à celui de l'ADSL ;<br>• Visionner des vidéos en HD (High-definition) et écouter des musiques en streaming sans aucune difficulté ;<br>• Partager et envoyer des pièces «lourdes» (sons, photos, vidéos) et permet la visioconférence ;<br>• La mobilité. | • Consommation de batterie ;<br>• Fournit un service pour une zone géographique limitée ;<br>• Des coûts d'abonnement généralement plus élevé que l'ADSL classique ;<br>• Il est compatible qu'avec certains modèles de tablettes et de téléphones portables. |

TABLE 1.11 – Avantages et inconvénients de la 4G.

#### 1.5.3.2 5G

5G est la cinquième génération des standards pour la téléphonie mobile. Elle permet des débits plus importants, le débit maximum devrait se situer entre 1 et 100 Gbit/s soit 100 à 1000 fois plus rapides que celui de la 4G avec des temps de latence très courts et une haute fiabilité ; elle permettra aussi d'augmenter le nombre de connexions simultanées par surface couverte. L'une des caractéristiques principales concerne l'internet des objets (IoT, Internet of things), les applications IoT couvriront plus le domaine médical, le domicile (application domotique) et d'autres domaines [34].

**Avantages et inconvénients de la 5G :**

Le tableau 1.12 présente les avantages et inconvénients de la 5G :

| **Avantages** | **Inconvenients** |
|---|---|
| • Une augmentation des débits ;<br>• Une réactivité accrue grâce à un temps de latence divisé par dix ;<br>• Une amélioration des capacités de connectivité avec beaucoup plus d'utilisateurs qui pourront se connecter en même temps, tout en conservant une connexion de qualité. | • Le développement des infrastructures nécessite un coût élevé ;<br>• La vitesse que revendique cette technologie semble difficile à atteindre (dans le futur, ce sera peut-être le cas) en raison du soutien technologique incompétent dans la plupart des régions du monde ;<br>• Gourmande en électricité. |

TABLE 1.12 – Avantages et inconvénients de la 5G.

## 1.6 Architecture d'un réseau d'entreprise

La conception d'une topologie de réseau est la première étape de la phase de conception logique de la méthodologie de conception de réseau descendante. Pour atteindre les objectifs d'évolutivité et d'adaptabilité d'un client, il est important de concevoir une topologie logique avant de sélectionner des produits ou des technologies physiques [30].

### 1.6.1 Architecture plate (topologie plate)

Une topologie de réseau plate convient aux petits réseaux. Avec une conception de réseau plate, il n'y a pas de hiérarchie. Chaque périphérique réseau a essentiellement le même travail et le réseau n'est pas divisé en couches ou modules. Une topologie de réseau plate est facile à concevoir et à implémenter, et elle est facile à entretenir, tant que le réseau reste petit. Cependant, lorsque le réseau se développe, un réseau plat n'est pas souhaitable. L'absence de hiérarchie rend le dépannage difficile. Plutôt que de pouvoir concentrer les efforts de dépannage sur une seule zone du réseau, vous devrez peut-être inspecter l'ensemble du réseau [30].

### 1.6.2 Conception de réseau hiérarchique

Plus généralement nommé par sa version anglaise, «three-layers hierarchical internetworking design/model», ce modèle a été inventé et diffusé par Cisco. Le principe est simple : créer un

design réseau structuré en trois couches (layers), chacune ayant un rôle précis impliquant des différences de matériel, performances et outils.

Ces trois couches sont [3] :

- La couche cœur, «Core layer» ;
- La couche distribution, «Distribution layer» ;
- La couche accès, «Access layer».

✠ **Couche d'accès :** constitue la périphérie du réseau, où le trafic entre dans le réseau de campus et en sort. Traditionnellement, un commutateur de couche d'accès a pour fonction principale de fournir à l'utilisateur un accès au réseau. Les commutateurs de couche d'accès se connectent aux commutateurs de la couche de distribution. Ceux-ci implémentent des technologies de fondation de réseau telles que le routage, la qualité de service et la sécurité.

✠ **Couche distribution :** établit l'interface entre la couche d'accès et la couche cœur de réseau pour fournir de nombreuses fonctions importantes, notamment :

- Regroupement de réseaux étendus d'armoires de câblage ;
- Regroupement des domaines de diffusion de couche 2 et des limites de routage de couche 3 ;
- Fonctions intelligentes de commutation, de routage et de règles d'accès au réseau, pour l'accès au reste du réseau ;
- Haute disponibilité pour l'utilisateur final et chemins à coût égal vers le cœur de réseau au moyen de commutateurs redondants dans la couche de distribution ;
- Services différenciés, pour différentes classes d'applications de services à la périphérie du réseau.

✠ **Couche cœur de réseau :** elle sert de réseau fédérateur. Elle connecte plusieurs couches du réseau de campus. La couche cœur de réseau sert d'agrégateur pour tous les autres blocs de campus et joint le campus au reste du réseau. La couche cœur de réseau a pour objectif principal d'assurer l'isolation des défaillances et la connectivité haut débit du réseau fédérateur.

Le modèle à trois couches présenté dans la figure 1.7 est un cadre conceptuel. Il s'agit d'une image abstraite d'un réseau similaire au concept du modèle de référence Open System Interconnexion (OSI).

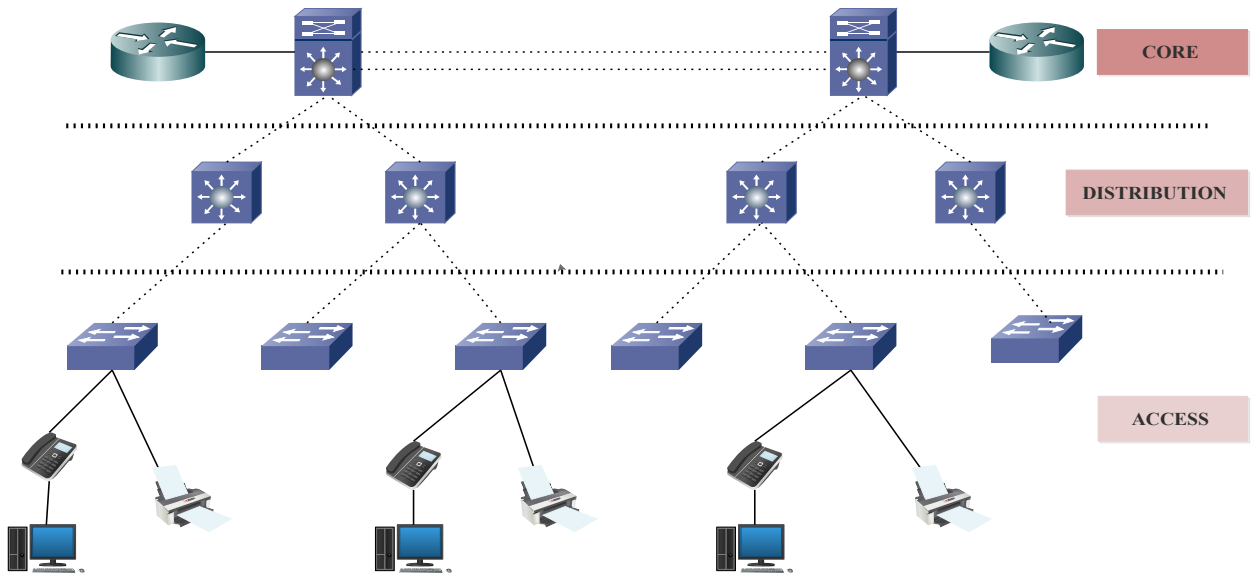


FIGURE 1.7 – Modèle hiérarchique à trois couches.

#### 1.6.2.1 Avantage d'un réseau hiérarchique

Les avantages sont [19] :

- **Evolutif :** ces réseaux peuvent s'étendre plus facilement ;
- **Redondant :** la redondance au niveau de la couche cœur de réseau et de la couche de distribution permet d'assurer une continuité de service pour la couche d'accès ;
- **Performant :** la mise en place d'agrégat de liens entre les commutateurs de la couche de distribution et ceux de la couche cœur du réseau permet d'augmenter la vitesse ;
- **Sécurité :** la sécurité du réseau peut être renforcée avec la mise en place de la sécurité des ports au niveau de la couche d'accès et la mise en place des stratégies de sécurité et/ou des listes de contrôle d'accès au niveau de la couche de distribution ;
- **Coût de gestion diminué :** la cohérence de paramétrage entre les différents commutateurs de même couche permet une simplification de la gestion ;
- **Maintenance :** la conception modulaire d'un réseau hiérarchique permet une mise à jour plus aisée.

## 1.7 Éléments actifs d'un réseau d'entreprise

### 1.7.1 Éléments d'interconnexion

Les éléments d'interconnexion assurent la connexion entre deux ou plusieurs équipements terminaux. On distingue :

- **Répéteur (Repeater) :** est un organe non intelligent, permet de fournir des fonctions de conversion de signaux et la régénération de ce dernier pour étendre la longueur maximale d'un segment, ou compenser l'affaiblissement pour résoudre le problème des bruits. Le répéteur agit au niveau de la couche physique du modèle de référence.
- **Commutateur(Switch) :** analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats. Le commutateur agit au niveau de la couche liaison de données du modèle de référence.
- **Routeur(Router) :** est destiné à relier plusieurs réseaux différents. Il opère au niveau de la couche 3 du modèle de référence.
- **Passerelle(Gateway) :** est un nœud qui joue le rôle d'intermédiaire, ce nœud intermédiaire peut-être plus ou moins complexe, suivant la ressemblance ou la dissemblance des deux réseaux à interconnecter [34].
- **PDU Zero-U (bandeau d'alimentation) :** est une multiprise qui sert à alimenter les actifs.

### 1.7.2 Éléments de sécurité

Les éléments de sécurité sont [29] :

- **L'onduleur (UPS en anglais, pour Uninterruptible Power Supply) :** est un équipement qui fournit une alimentation électrique de secours pendant quelques minutes (ou quelques heures selon les produits) pendant une coupure de courant et protège contre les surtensions (orages...).
- **Pare-feu (Firewall) :** est un moyen matériel (ou logiciel en couche basse) , permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu permet de filtrer les paquets de données échangés avec le réseau.
- **VPN (Virtual Private Network) :** est constitué d'un ensemble de LAN privés reliés à travers internet par un «tunnel» sécurisé dans lequel les données sont cryptées.

- **DMZ (DeMilitarized Zone) :** est un sous-réseau séparé du réseau local et isolé de celui-ci et d'internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis internet, et qui n'ont pas besoin d'accéder au réseau local.
- **VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau local virtuel) :** est un réseau local qui redéfinit les domaines de diffusion de façon à regrouper les utilisateurs de manière logique, il est implémenté sur un commutateur et réalise un domaine "logique" de diffusion.

### 1.7.3 Équipements terminaux

Ces éléments sont à portée immédiate des utilisateurs. Ils permettent à l'utilisateur d'accéder aux ressources du réseau.

- **Ordinateur :** c'est le principal élément d'un réseau. Pour être utilisé, il doit être équipé d'un équipement appelé carte réseau et d'un système d'exploitation.
- **Serveur :** est un ordinateur très puissant disposant d'une grande capacité mémoire et d'une vitesse de calcul élevée. Il partage ses ressources avec d'autres machines appelées clients.
- **Imprimante :** est un périphérique permettant de faire une sortie imprimée (sur papier) des données de l'ordinateur.
- **Console KVM :** signifie Keyboard, Video (monitor) and Mouse, est un périphérique qui permet de contrôler, et gérer plusieurs PC ou serveurs via un seul clavier, moniteur et souris.

## 1.8 Éléments passifs d'un réseau d'entreprise

### 1.8.1 Équipements d'une baie de brassage

La baie de brassage est une armoire contenant les équipements réseaux permettant aux employés d'une même entreprise d'accéder à internet et de faire de l'intranet. De plus de ces équipements réseau elle peut contenir les éléments suivants :

- **Panneau de brassage :** relie les ports des différents équipements réseau aux arrivées des câbles du réseau et à des connecteurs RJ45 (Registered Jack45) ;
- **Cordon de brassage :** est un câble RJ45 droit court, il permet de faire la liaison entre deux équipements ;

- **Tiroir optique :** c'est un rack où arrivent des liaisons fibres optiques. Il comporte un certain nombre de connecteurs fibres (souvent soit ST (Straight Tip) soit SC (Subscriber Connector) et il est relié aux équipements réseau via des jarretières fibre ;
- **Jarretière optique :** est un câble fibre optique qui permet de faire la liaison, sur une courte distance, entre deux équipements.

### 1.8.2 Câblages

On distingue trois types de câbles :

- **La paire torsadée :** est le support de transmission le plus simple. Elle est constituée d'une ou de plusieurs paires de fils électriques agencés en spirale pour limiter les phénomènes d'interférence [33]. La bande passante dépend du diamètre des fils de cuivre et de la distance à parcourir. Il est possible de transporter des informations à plusieurs Mbits/s sur de courtes distances (quelques kilomètres). Elle permet le transport des signaux analogiques et numériques [13].
- **Câble coaxial :** est constitué de deux conducteurs concentriques séparés par un isolant diélectrique. Le conducteur extérieur est une tresse de cuivre appelée blindage qui est relié à la terre, le tout est protégé par une gaine isolante. Ce câble est peu sensible aux perturbations électromagnétiques extérieures, et il autorise des débits plus élevés que la paire torsadée qui peuvent atteindre jusqu'à 10 Mbits sur des distances de l'ordre du kilomètre [13].
- **Fibre optique :** est un fil en verre très pur et transparent, à la fois flexible et très fin. Les bits sont codés sur la fibre sous forme d'impulsions lumineuses. Les câbles à fibre optique transmettent les données sur de plus longues distances et avec une bande passante plus large que n'importe quel autre support réseau. Contrairement aux fils de cuivre, les câbles à fibre optique peuvent transmettre des signaux avec moins d'atténuation et sont entièrement protégés des perturbations électromagnétiques et radioélectriques. Elle est par ailleurs de plus en plus déployée sur le réseau d'accès de l'utilisateur comme solution de remplacement de l'ADSL [1].

### 1.8.3 Chemin de câbles

Un chemin de câble c'est un dispositif permettant de protéger les câbles électriques, il évite de laisser traîner les fils et câbles au sein des bureaux (par exemple la goulotte).

## 1.9 Conclusion

Au fil de ce chapitre, nous avons défini un réseau d'entreprise et son intérêt, nous avons par la suite cité les différentes technologies utilisées dans chaque catégorie. Enfin nous avons présenté les équipements actifs et passifs d'un réseau d'entreprise. Dans le chapitre suivant, nous allons détailler l'administration et supervision des réseaux.

# CHAPITRE 2

# ADMINISTRATION ET SUPERVISION DES RÉSEAUX

## 2.1 Introduction

La gestion d'un système informatique est un travail permanent. Ainsi le service informatique ou l'administrateur réseau doit savoir à tout moment l'état des équipements et des services sur les réseaux. C'est pour cela qu'on a recours à une technique de suivi qui est la supervision, qui permet de surveiller, d'analyser, de rapporter et d'alerter les fonctionnements normaux et anormaux des systèmes informatiques. La supervision permet entre autres d'avoir une vue globale du fonctionnement et problème pouvant survenir sur un réseau, mais aussi d'avoir des indicateurs sur la performance de son architecture. De nombreux logiciels qu'ils soient libres ou propriétaires existent sur le marché. La plupart s'appuient sur le protocole SNMP (Simple Network Management Protocol).

Pour bien structurer notre chapitre, nous l'avons divisé en trois parties : La première partie sera consacrée à présenter l'administration des réseaux informatiques.

Dans la seconde partie, nous allons définir précisément le concept du monitoring.

Et quant à la troisième partie, nous verrons le fonctionnement du protocole le plus utilisé actuellement : le protocole SNMP.

## 2.2 Administration des réseaux

L'administration des réseaux est une fonction indispensable dont il faut tenir compte lorsqu'on décide de s'investir dans la conception d'un réseau. Cette fonction est tellement impor-

tante que l'ISO (International Standard Organization) a dû définir des directives pour spécifier l'étendue du travail d'administration.

### 2.2.1 Définition de l'administration des réseaux

L'administration de réseaux recouvre l'ensemble des activités de surveillance, d'analyse, de contrôle et de planification du fonctionnement des ressources d'un réseau de télécommunications dans le but de fournir des services de télécommunications à des usagers avec un certain niveau de qualité [38].

L'administration est la fonction principale d'un administrateur réseau. Elle consiste à mettre en place, maintenir et organiser l'infrastructure du réseau, mais aussi [39] :

- Installer et maintenir les services nécessaires au fonctionnement du réseau ;
- Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures) ;
- S'assurer que les utilisateurs "n'outrepassent" pas leurs droits ;
- Gérer les logins (noms d'utilisateurs, mots de passe, droits d'accès, permissions particulières . . .) ;
- Gérer les systèmes de fichiers partagés et les maintenir.

### 2.2.2 Normes d'administration réseau

#### 2.2.2.1 Administration vue par L'ISO

##### 2.2.2.1.1 Généralités

L'ISO ne spécifie aucun système d'administration de réseau, elle définit un cadre architectural général (ISO 7 498-4, OS/ Management Framework) et un aperçu général des opérations de gestion des systèmes (ISO 10040, OS/ System Management) [37]. Ces documents de base décrivent trois modèles [37] :

- Un modèle organisationnel ou architectural (MSA, Managed System and Agents) qui organise la gestion OSI et définit la notion de systèmes gérés et gérants (DMAP, Distributed Management Application Processus) ;
- Le modèle informationnel (MIB, Management Information Base) qui constitue la base de données des informations de gestion. La MIB énumère les objets gérés et les informations s'y rapportant (attributs) ;

- Le modèle fonctionnel (SMFA, Specific Management Function Area) qui répartit les fonctions d'administration en cinq domaines (aires) fonctionnels (figure 2.1).

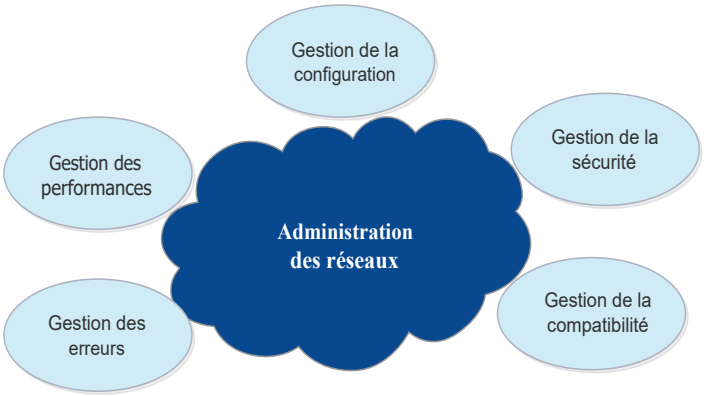


FIGURE 2.1 – Aires fonctionnelles de la gestion ISO.

#### 2.2.2.1.2 Différents modèles

✠ **Modèle architectural :** Le modèle architectural définit trois types d'activité : la gestion du système (System Management), la gestion de couche (Laver management) et les opérations de couche (Laver Operation).

- **La gestion du système (SMAE, System Management Application Entity)** met en relation deux processus : un processus gérant et un processus agent. L'agent gère localement un ensemble de ressources locales (équipements, protocoles. ..) sous le contrôle de l'agent gérant (figure 2.2) [37].

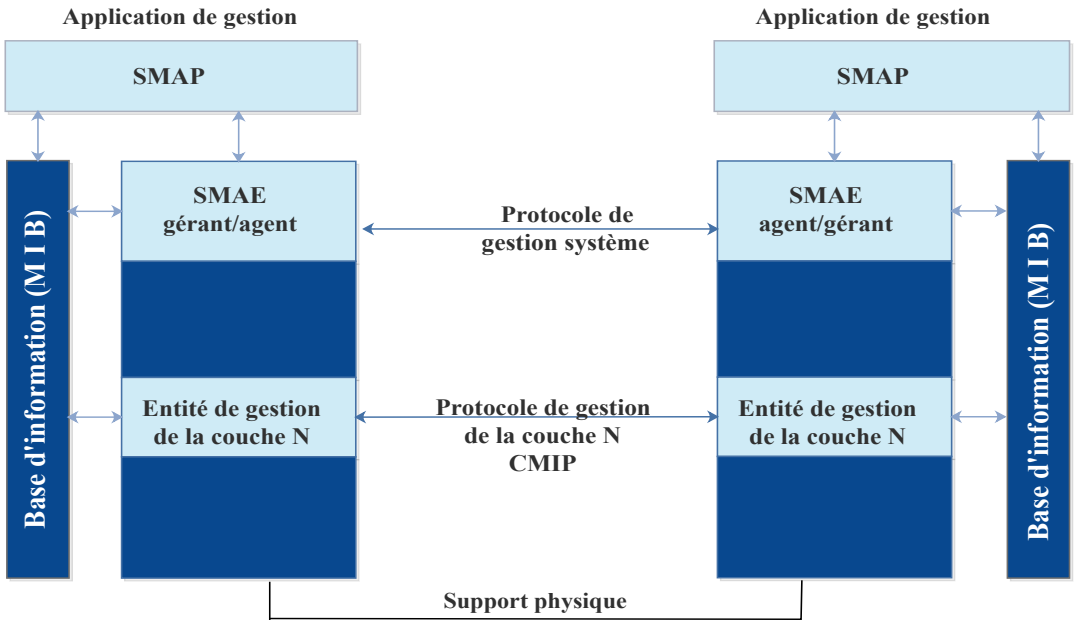


FIGURE 2.2 – Modèle architectural de l'ISO.

- **La gestion système** repose sur des échanges verticaux entre couches (CMIS, Common Management Information Service). CMIS (ISO 9595) définit les primitives d'accès aux informations. Ces primitives assurent le transfert d'information vers les applications de gestion (SMAP, System Management Application Process) non spécifiées par l'ISO [36].
- **La gestion de couche**, ou protocole de gestion de couche, fournit les moyens de transfert des informations de gestion entre les sites administrés, c'est un dialogue horizontal (CMIP, Common Management Information Protocol, ISO 9596). Les opérations de couche (N), ou protocole de couche (N), supervisent une connexion de niveau N. Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information [37].

✠ **Modèle Informationnel** : Le standard OSI décrit une méthode de description des données d'administration il modélise leur représentation et fournit un ensemble de directives pour garantir la cohérence de la base (SMI, Structure of Management Information). La représentation des éléments gérés (objets gérés) est orientée objet, les classes et occurrences d'objets sont représentées selon un arbre. Et pour que le protocole d'administration reste simple, SMI pose des restrictions sur les types de variables autorisées dans la MIB, et spécifie les règles de nommage de ces variables [36].

✠ **Modèle fonctionnel** : Ce modèle, plus concret que les précédents, définit des domaines

fonctionnels d'administration et leurs relations. Cinq domaines ou fonctions (aires fonctionnelles) y sont décrits (SMFA, Specific Management Function Area).

- **Gestion de la configuration** : consiste à maintenir un inventaire précis des ressources matérielles (type, équipement...) et logicielles (version, licences, fonctions ... ) et d'en préciser la localisation géographique. La gestion de la configuration associe, à chaque objet géré (chaque objet de l'inventaire), un nom qui l'identifie de manière unique [37].
- **Gestion des pannes** : est une fonction dominante. En effet, l'objectif essentiel d'une administration de réseaux est l'optimisation des ressources et des moyens. Il importe donc d'être en mesure d'anticiper et éventuellement de diagnostiquer rapidement toute défaillance du système, que celle-ci soit d'origine externe (ex. : coupure d'un lien public) ou interne au système (ex. : panne d'un routeur) [36].
- **Gestion des performances** : Elle doit pouvoir évaluer les performances des ressources du système et leur efficacité. Elle comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau. Les performances du réseau sont évaluées à partir de quatre paramètres : le temps de réponse, le débit, le taux d'erreur par bit, la disponibilité [37].
- **Gestion de la comptabilité** : Son rôle est de connaître les charges des objets gérés ainsi que leurs coûts de communication. Des quotas d'utilisation peuvent être fixés temporairement ou non sur chacune des ressources réseau. De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur [37].
- **Gestion de la sécurité :** La gestion de la sécurité est la collection des fonctions relatives à l'administration de réseaux et requises pour supporter les politiques de sécurité dans un réseau de télécommunication. Les fonctions essentielles de la gestion de sécurité comprennent la distribution des informations relatives à la sécurité, telles que les clés de cryptage et les privilèges d'accès, et le compte rendu des événements relatifs à la sécurité, tels que les intrusions dans un réseau, les tentatives d'accès à des informations ou à des services privilégiés par des processus non autorisés ou encore l'accès à des données et à des services protégés [38].

#### 2.2.2.2 Administration vue par L'U1T-T

L'UIT-T( Union internationale des Télécommunications-Telecommunication) (ex-CCITT, Comité Consultatif International Téléphonique et Télégraphique ) a élaboré le concept de Réseau de Gestion des Télécommunications (RGT ou TMN pour Telecommunications Management Network) [M.3010] pour définir une architecture fonctionnelle d'un système de gestion de réseaux souple, complet et évolutif. La notion de RGT est purement fonctionnelle. Elle ne préjuge en rien de la taille et des particularités des implantations physiques la réalisant. Il s'agit d'une architecture modulaire constituée de groupements fonctionnels dédiés à la réalisation de tâches particulières relatives au transport et au traitement des informations de gestion. Aussi, des points de référence ont été définis qui constituent des points de passage d'informations entre des groupements fonctionnels. L'UIT-T traite aussi de l'aspect informationnel avec la définition d'un modèle informationnel générique [M.3100] [38].

#### 2.2.2.3 Administration dans l'environnement TCP/IP

Le nombre important de réseaux TCP/IP (Transmission Control Protocol/Internet Protocol) ainsi que le besoin crucial de leur gestion a entraîné le développement d'un premier protocole de gestion, le protocole SGMP (Simple Gateway Monitoring Protocol) [RFC 1028], conçu à l'origine pour gérer les passerelles internet des réseaux grandes distance. Le protocole actuel SNMP (Simple Network Management Protocol) [RFC 1157] y trouve ses bases tout en intégrant certains concepts de gestion développés à l'ISO. En fait, les standards SNMP, établis depuis 1990, sont axés autour de deux aspects, la définition des protocoles d'échanges SNMP et la définition des informations d'administration des MIB [38].

Dans notre cas, nous étudions les réseaux d'entreprise basés sur les technologies TCP /IP plus exactement le protocole de gestion réseau SNMP.

### 2.2.3 La sécurité dans la gestion de réseaux

#### 2.2.3.1 Définition de la sécurité

La sécurité informatique c'est l'ensemble des moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

La sécurité vise à assurer les objectifs suivants :

- **La confidentialité :** C'est la propriété qui garantit que les informations transmises ne sont compréhensibles que par les entités autorisées ;

- **L'authentification** : C'est la propriété qui consiste à vérifier l'identité d'un utilisateur avant de lui donner l'accès à une ressource ;
- **L'intégrité :** C'est la propriété qui consiste à vérifier si les informations n'ont pas été modifiées durant la transmission ;
- **La disponibilité :** c'est la propriété qui permet de garantir l'accès aux données ;
- **La non-répudiation :** C'est la propriété qui permet d'empêcher l'utilisateur de nier l'envoi (ou réception) du message en question.

#### 2.2.3.2 Gestion de système et de réseau

Les activités de gestion de systèmes et de réseaux lorsqu'elles sont menées correctement, permettent d'offrir les niveaux de disponibilité et de performance nécessaires à la réalisation de la sécurité. De plus, elles intègrent les tâches de surveillance du réseau, de détection des anomalies d'intrusions ou d'incidents, qui sont nécessaires à la mise en œuvre de la sécurité et qui contribuent grandement à la sécurité globale du réseau et du système d'information qu'il dessert [16].

#### 2.2.3.3 Gestion de parc informatique

##### 2.2.3.3.1 Objectifs et fonctions

Les fonctions d'un système de gestion du parc informatique contribuent à la sécurité via les fonctions suivantes [16] :

- Gestion technique du parc ;
- Gestion du catalogue, codification des équipements, terminologie commune, repérage physique des matériels à des fins d'inventaires ;
- Inventaire initial et périodique de tous les composants du système d'information ;
- Gestion commerciale (administration des contrats, tarifs, commandes, acquittement des factures, gestion des délais de paiement, etc.) ;
- Gestion des incidents (réception automatique des incidents, description, etc.) ;
- Gestion physique du parc (définition des responsabilités pour l'entrée, le suivi de l'état, la localisation des équipements, identification de vols ou de destruction des équipements).

L'inventaire des ressources, des profils est primordiale pour identifier les valeurs à protéger et les critères de sécurités associés afin d'identifier les mesures de sécurité pour les satisfaire.

#### 2.2.3.3.2 Quelques recommandations

- La mise en oeuvre d'un service de gestion de parc s'inscrit dans une logique de qualité et doit s'interfacer et dialoguer harmonieusement avec les autres services de gestion de réseaux ;
- Une bonne gestion de parc informatique n'a de sens que si l'on sait également gérer correctement l'utilisation des ressources informatique et les fournisseurs dont l'entreprise dépend ;
- La mise en place d'une politique cohérente de remplacement des machines pour faire évoluer le parc informatique ;
- La dénomination des ressources ;
- Utiliser un outil logiciel de gestion des inventaires pour s'assurer de la cohérence, de la complétude et de l'exactitude des inventaires [16].

### 2.2.3.4 Gestion de qualité de service réseau

Dans le but d'assurer une bonne qualité de service réseau, il est nécessaire de respecter une bonne gestion quotidienne des ressources et des opérations de service [16].

#### 2.2.3.4.1 Indicateur de qualité

Les critères mesurables de la qualité de service réseau sont [16] :

- **La disponibilité :** est la période pendant laquelle le service est opérationnel ;
- **La capacité :** est le volume de travail susceptible d'être pris en charge durant la période de disponibilité du service réseau ;
- **L'accessibilité :** définit la façon dont la capacité est distribuée aux utilisateurs. Elle peut être vue comme étant le temps de réponse du réseau ;
- **La fiabilité :** est la probabilité, pour un utilisateur, de pouvoir mener correctement à terme une session de travail, elle exprime le niveau de confiance possible envers l'infrastructure de service ;
- **La qualité de service :** peut être surveillé tout au long du cycle de vie du réseau, et peut être surveillé par des mesures de performance qui peuvent vérifier la satisfaction des utilisateurs et garantir que les performances réelles du réseau sont compatibles avec la qualité attendue.

#### 2.2.3.4.2 Evaluation et efficacité

Un contrôle de la réalisation effective des améliorations par une étroite surveillance de l'évolution des indicateurs de performances est fondamental pour un bon suivi du réseau [16].

- Les évaluations du niveau de service ;
- Une politique de qualité de service ;
- Une observation suivie de la qualité de service ;
- La gestion du trafic (facteur de performance).

## 2.3 Monitoring

Le monitoring désigne le fait de "surveiller". Cependant, le fait de surveiller quelque chose revient à connaître son état actuel, mais aussi l'historique de ses états passés, par l'intermédiaire de valeurs (UP/DOWN) et de données chiffrées (des pourcentages par exemple). C'est ici que l'on retrouve une distinction entre deux notions que sont la supervision et la métrologie [15]. Les deux concepts sont présentés dans la figure 2.3 :

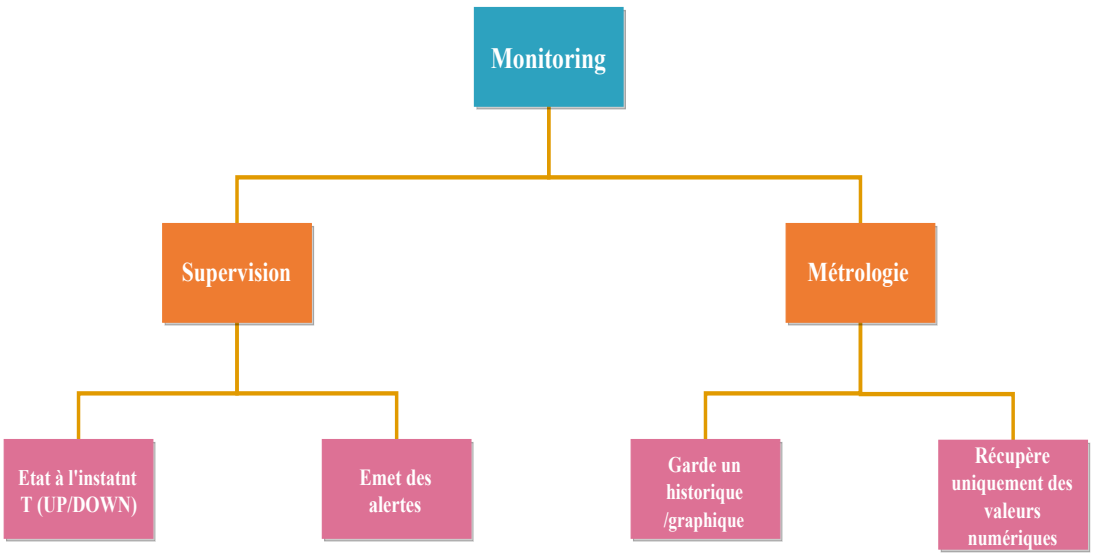


FIGURE 2.3 – Organigramme présentant le concept du monitoring.

### 2.3.1 Définition de la Supervision

La supervision est la surveillance du bon fonctionnement d'un système ou d'une activité. Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques. La supervision réseau comprend un ensemble de protocoles, matériels et logiciels informatiques dont la majorité est basée sur le protocole SNMP permettant de suivre à distance l'activité d'un réseau informatique. La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS par exemple) les administrateurs [31].

Autour de la supervision, plusieurs modules coexistent [25] :

- La supervision réseau ;
- La supervision système ;
- La notification permet l'envoi d'alertes par email, par sms, par téléphone, par avertissement sonore...
- L'exécution de commandes permet de relancer une application qui fait défaut ;
- La retranscription d'état du système permet de voir à tout moment l'état de tous les composants et applications supervisés sous forme d'un graphique, d'une carte ou d'un tableau. Son but est de rendre les résultats plus lisibles ;
- La cartographie visualise le réseau supervisé par l'intermédiaire de cartes, de graphique, de tableau...
- Le "reporting" consiste en un historique complet de la supervision.

La figure 2.4 présente les modules de la supervision :

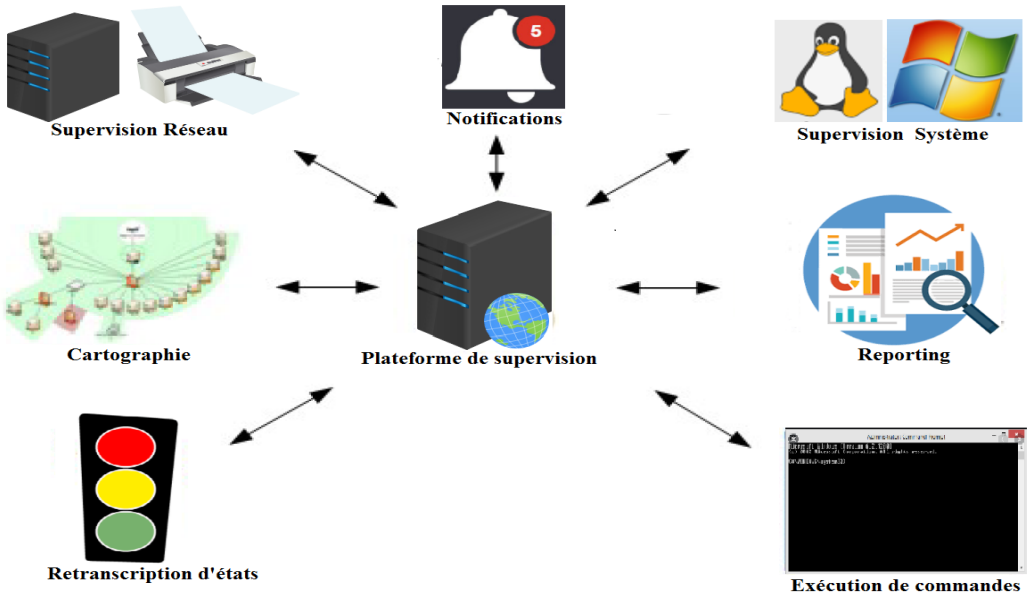


FIGURE 2.4 – Les modules de supervision.

#### 2.3.1.1 Que peut-on superviser ?

La supervision est un vaste domaine de l'informatique qui reprend plusieurs activités dont les principales sont [17].

- **La supervision réseau :** porte sur la surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité, mais également du contrôle des flux ;
- **La supervision système :** porte principalement sur les trois types principaux de ressources système : le processeur, la mémoire, le stockage ;
- **La supervision des applications(ou supervision applicative) :** permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs telles que les bases de données (Oracle, SQL (Structured Query Language Server), les serveurs de mails (Exchange, Notes) et autres serveurs Web.

#### 2.3.1.2 Moyens de supervision

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes [24] :

✠ **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.

La figure 2.5 illustre un échange de messages dans une supervision active :

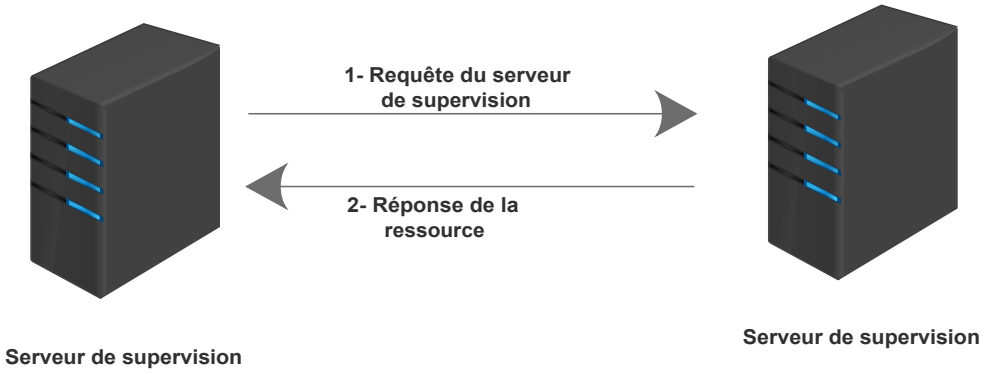


FIGURE 2.5 – Échange de messages dans une supervision active.

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.

Ces deux protocoles sont privilégiés, car ils sont non intrusifs : les agents sont natifs aux systèmes de supervision.

✠ **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.

La figure 2.6 illustre un échange de messages dans une supervision passive :


FIGURE 2.6 – Échange de messages dans une supervision passive.

La méthode passive possède plusieurs intérêts. D'abord elle est moins consommatrice de ressources du point de vue serveur de supervision et réseau. Le principal point noir de la supervision passive concerne la fraîcheur des informations : rien ne permet de garantir que la ressource supervisée est dans un état correct si aucune alerte n'est reçue. Les ressources n'envoient que très rarement des messages pour signaler un état correct. À cause de sa non-fiabilité, la supervision passive, en pratique, est surtout utilisée en complément de la supervision active pour la réception des traps SNMP.

### 2.3.2 Définition de la métrologie

La métrologie fait partie intégrante de la supervision. Elle désigne globalement la science de la mesure qui s'applique dans de nombreux domaines et notamment dans les réseaux informatiques.

La métrologie permet de créer des historiques de données, d'y appliquer un traitement (des filtres par exemple) afin d'extraire les données qui nous intéressent et de les présenter sous forme de graphiques ou de reporting. Cet historique des données permet si besoin d'apporter des correctifs au niveau des paramétrages des services, le juste pourcentage des ressources à utiliser...

Cet aspect du Monitoring est tout aussi important, car il va permettre d'améliorer le service, et donc ainsi le rendu de l'utilisateur.

Les termes supervision et métrologie sont encore parfois distingués même si les frontières tendent à se dissiper : la supervision s'attache aux alertes alors que la métrologie se rapporte davantage aux mesures [12].

### 2.3.3 Intérêts de la supervision et de la métrologie

La supervision et la métrologie se basent sur plusieurs points qui peuvent nous garantir ses services [15] :

- Être alerté en temps réel ;
- Pouvoir remonter à la source des problèmes ;
- Être proactif face aux problèmes ;
- Améliorer la disponibilité effective des applications ;
- Surveiller plus que le système d'information.

## 2.4 Protocole SNMP

Le protocole de communication SNMP permet aux administrateurs système et réseau de gérer tous les équipements du réseau informatique à distance afin de superviser et de contrôler les alarmes et alertes de tous leurs réseaux. Dans ce qui suit nous allons détailler le principe du fonctionnement de ce protocole.

### 2.4.1 Définition de SNMP

Le protocole SNMP (Simple Network Management Protocol ) a été standardisé par l'IETF (Internet Engineering Task Force) pour supporter les échanges d'informations de gestion pour gérer des systèmes distants via une infrastructure TCP/IP. S'appuyant sur UDP (User Datagram Protocol). Chaque système raccordé (poste de travail, serveur, routeur,etc.) qui doit être géré, intègre un module logiciel "agent de gestion" qui interagit à distance avec système gérant (le manager). SNMP est le protocole d'échange d'information entre des processus agents et gérant . Pour que ce protocole de gestion appréhende de façon universelle toutes les ressources à gérer , leur représentation a également été standardisée [16].

Il permet principalement de [18] :

- Connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...) ;
- Visualiser une quantité d'informations concernant le matériel, les connexions réseau, leur état de charge ; modifier le paramétrage de certains composants ;
- Alerter l'administrateur en cas d'événement considéré comme grave.

**Avantages**

Le protocole SNMP a de nombreux avantages en tant qu'outil de gestion réseau [28] :

- **Accès centralisé :** la gestion réseau s'effectue depuis une machine centrale sans soucis, et c'est même préférable pour la sécurité ;
- **Sécurité :** la sécurité s'est accrue au cours des différentes versions, jusqu'à respecter la plupart des contraintes imposées ;
- **Fiabilité :** le protocole utilisé permet de s'assurer que les requêtes sont bien arrivées à destination et qu'elles ont été correctement interprétées ;
- **Evolutivité :** l'utilisation d'une arborescence pour la gestion des variables permet d'avoir une évolution continuelle des capacités fonctionnelles accessibles via ce protocole.

### 2.4.2 Principaux éléments de SNMP

SNMP permet le dialogue entre le gestionnaire et les agents afin de recueillir les objets souhaités dans la MIB, ainsi une administration SNMP est composée de trois types d'éléments :

#### 2.4.2.1 Manager

Le Manager NMS (Network Management Station) ou «station de gestion de réseau», constitue le point central de l'architecture SNMP. Il se présente souvent sous la forme d'un poste et de logiciels d'administration, fournissant à l'administrateur une vue d'ensemble des équipements, il permet de [18] :

- Accède aux informations de gestion de la MIB locale via un protocole d'administration SNMP ce qui le met en relation avec les divers agents ;
- Centralise les données et les met en forme pour l'affichage et la sauvegarde ;
- Réceptionne les alertes et agit en réaction ;
- Écoute sur le port UDP 162.

#### 2.4.2.2 Agent

Un agent SNMP est un logiciel implanté sur un équipement à superviser. Il s'agit souvent d'un équipement réseau (switch, hub, routeur...), mais on trouve aussi des agents sur des serveurs. Cet agent doit rester à l'écoute d'un port particulier, le port UDP 161.

Le rôle d'un agent SNMP est [18] :

- D'instancier les différentes variables de la MIB spécifiques à cet équipement ;
- De mettre à jour les valeurs dynamiques de ces différentes variables ;
- De recevoir les requêtes SNMP envoyées par le superviseur SNMP et d'y répondre ;

- D'envoyer les messages SNMP "Trap" ou "Inform" au superviseur SNMP pour le prévenir d'un événement exceptionnel sur l'équipement ;
- Gérer la sécurité des accès aux variables de la MIB conformément au modèle de sécurité mis en place.

La figure 2.7 illustre les éléments principaux du protocole SNMP :

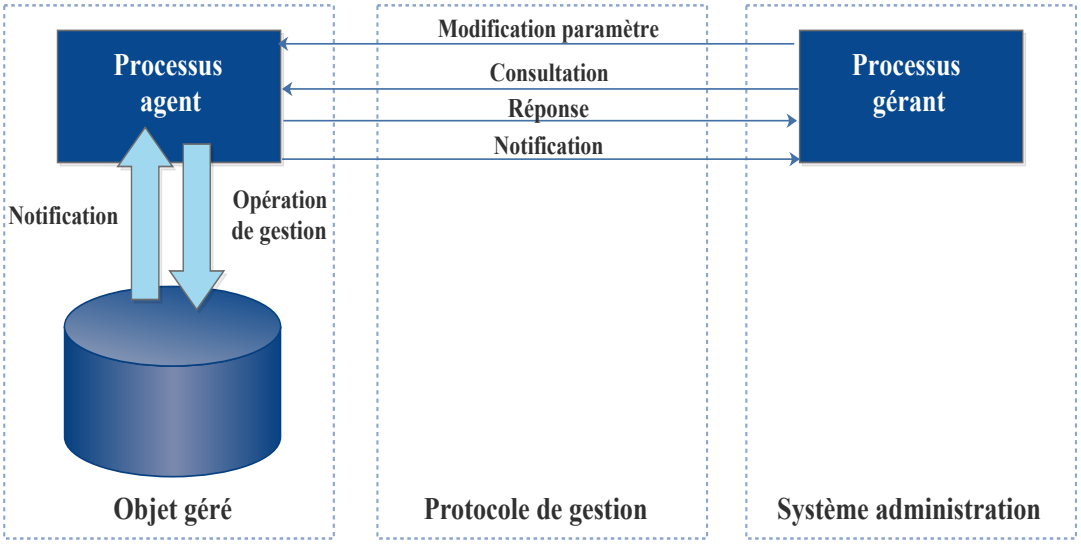


FIGURE 2.7 – Les éléments principaux du protocole SNMP.

### 2.4.2.3 MIB

#### 2.4.2.3.1 Management Information Base

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des N renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base (MIB).

Cette MIB contient toutes les informations administratives sur les objets gérés. Seul, le processus agent a accès à la MIB. Les fichiers MIB écrits en langage ASN.1 (Abstract Syntax Notation 1) sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB [37].

#### 2.4.2.3.2 Structure d'une MIB et Object Identifier

La MIB est une collection d'informations pour la gestion des éléments du réseau. Sa structure est une arborescence hiérarchique dont chaque nœud est défini par un nombre ou un Object

Identifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique (texte, entier, compteur, tableau...). Un OID est donc une séquence de chiffres séparés par des points [37].

La figure 2.8 montre la structure de la table MIB :

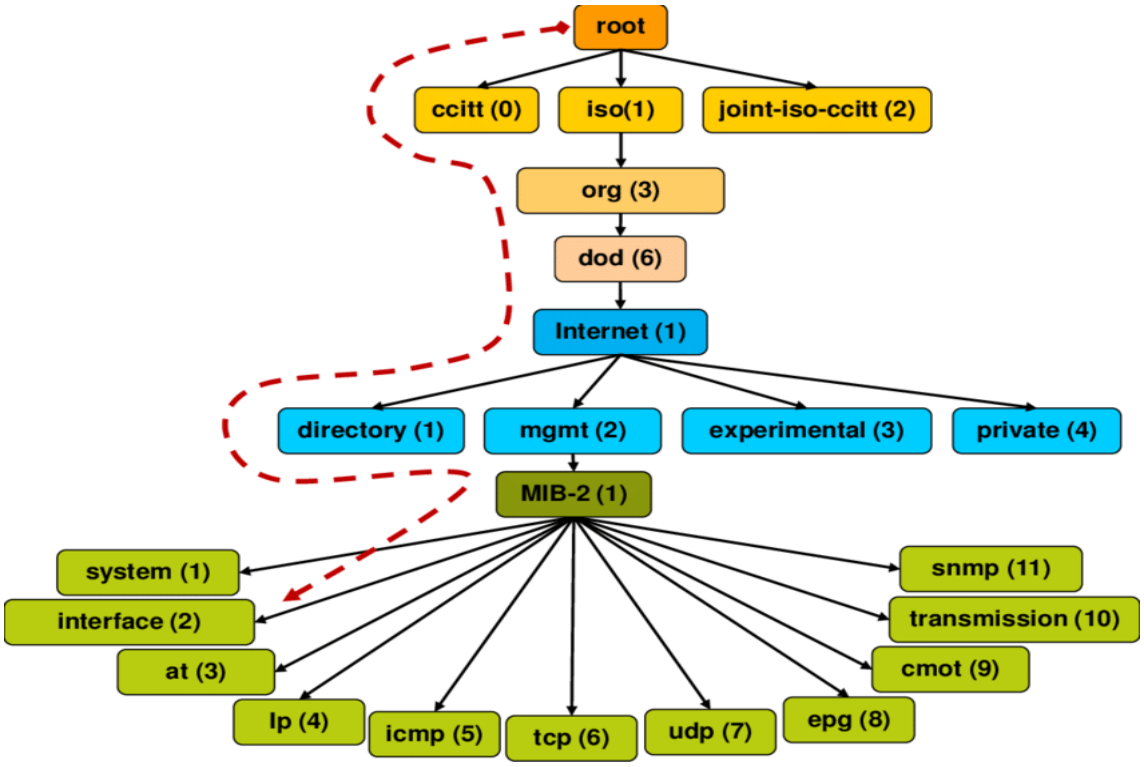


FIGURE 2.8 – Structure de l'arborescence d'une MIB.

### 2.4.3 RMON (Remote Network Monitoring)

La surveillance de réseau à distance, ou RMON, est une évolution logique de l'utilisation de SNMP. RMON a été ratifié par l'IETF en novembre 1991 (RFC 1271) pour combler les lacunes des MIB standard, qui n'avaient pas la capacité de fournir des statistiques sur la liaison de données et les paramètres de la couche physique. L'IETF a développé la RMON MIB pour fournir des statistiques de trafic Ethernet et un diagnostic de panne.

Les agents RMON collectent des statistiques sur les erreurs de contrôle de redondance cyclique (CRC, Cyclic Redundancy Check), les collisions Ethernet, la distribution de la taille des paquets, le nombre de paquets entrants et sortants et le taux de paquets diffusés. Le groupe d'alarmes RMON permet à un gestionnaire de réseau de définir des seuils pour les paramètres réseau et de configurer des agents pour envoyer automatiquement des alertes aux NMS. RMON prend également en charge la capture de paquets et l'envoi des paquets capturés à un NMS

pour l'analyse de protocole.

RMON fournit aux gestionnaires de réseau des informations sur l'intégrité et les performances du segment de réseau sur lequel réside l'agent RMON [30].

### 2.4.4 Les commandes SNMP

- **Les types de requêtes du manager SNMP vers l'agent SNMP sont :**
  - ✓ ***Get Request :*** le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB ;
  - ✓ ***Get Next Request :*** le manager interroge un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent ;
  - ✓ ***Get Bulk Request :*** l'application de gestion peut envoyer une requête GETBULK (à partir de la version SNMPv2) afin d'interroger un nombre défini d'ensembles de données avec une seule et même requête. Une requête GETBULK correspond à plusieurs requêtes GETNEXT consécutives ;
  - ✓ **Set Request** : le Manager SNMP met à jour une information sur un agent SNMP.
- **Les réponses ou informations de l'agent vers le manager sont :**
  - ✓ ***Get Response :*** la commande GET RESPONSE est le message retourné par les entités interrogées (agents) en réponse aux commandes de type GET REQUEST, GET NEXT REQUEST et SET REQUEST ;
  - ✓ ***Trap :*** la commande TRAP permet à un agent de notifier un événement. Cette alarme, envoyée lors de la détection d'une anomalie par l'agent (initialisation de l'agent, arrêt de l'agent, dépassement d'un seuil, etc.), cependant l'agent n'attend aucune réponse de la part du manager ;
  - ✓ ***Inform :*** les requêtes INFORM assurent généralement la même fonction que les traps SNMP. Contrairement à ces dernières, les paquets INFORM se démarquent toutefois par l'envoi d'un accusé de réception par le manager. Par conséquent, l'agent peut renvoyer le message si celui-ci n'a pas atteint le manager à la première tentative.

La figure 2.9 illustre les échanges entre le manager et l'agent :

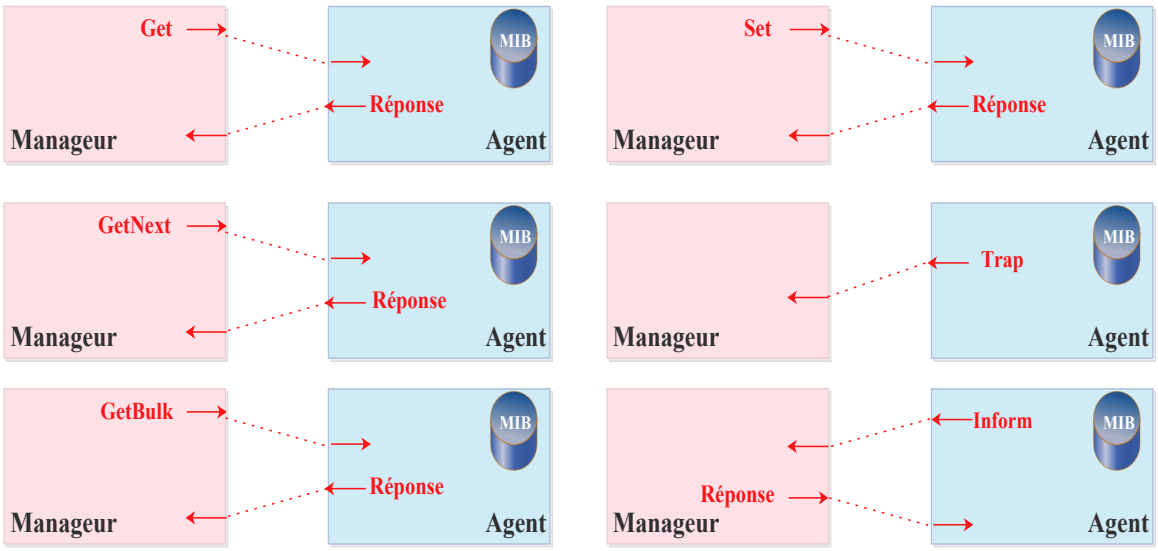


FIGURE 2.9 – Les échanges entre le manager et l'agent SNMP.

### 2.4.5 Les différentes versions de SNMP

Différentes versions de SNMP [18]. :

- **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 chaîne de caractère appelée "communauté" ;
- **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 ;
- **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.

## 2.5 Conclusion

À l'issue de ce chapitre nous avons présenté l'administration réseau, les différents modèles d'administration ainsi que les tâches de l'administrateur, nous avons par la suite défini l'aspect du monitoring et ces deux concepts à savoir la supervision et la métrologie, et nous avons fini par aborder le protocole SNMP. Le chapitre suivant va se porter sur la présentation de l'Entreprise Portuaire de Bejaia et l'étude de son architecture réseau.

# CHAPITRE 3

# PRÉSENTATION DE L'ORGANISME D'ACCUEIL ET DE PANDORA FMS

## 3.1 Introduction

Ce chapitre sera réservé à l'étude du réseau existant dans l'EPB (Entreprise Portuaire de Bejaia) et aux améliorations proposées. Dans un premier temps, nous donnerons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Ensuite, nous étudierons le réseau informatique et ses composants mis en place dans l'entreprise afin de pouvoir proposer d'éventuelles améliorations, et enfin nous présenterons le projet à mettre en œuvre.

## 3.2 Présentation de l'organisme d'accueil

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique.

L'EPB a été créé le 14 août 1982 suite au décret n 82-285, elle est l'une des entreprises socialistes à caractère économique ; elle est transformée en Entreprise Publique Économique, Société par Actions (EPE-SPA).

Aujourd'hui, il est classé 2ème port d'Algérie en marchandises générales, et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir installé un système de management de qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire de Bejaia a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS (Occupational Health

and Safety Assessment Series) 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

FIGURE 3.1 – Port de Bejaia.

## 3.3 Présentation des différentes structures de l'EPB

L'EPB est organisée selon de différentes directions, dirigées par une Direction Générale qui s'occupe des actions liées à la gestion et au développement de l'entreprise.

La figure 3.2 nous montre les différentes structures qui composent l'EPB :

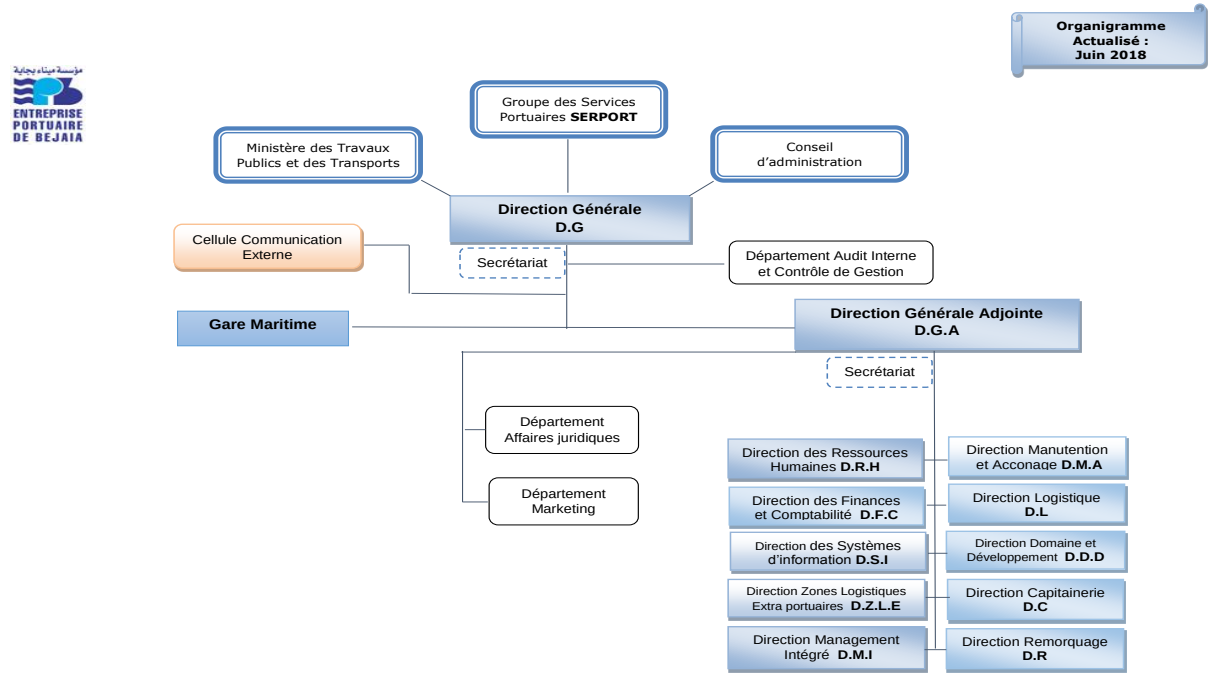


FIGURE 3.2 – Organigramme de l'Entreprise Portuaire Bejaia.

## 3.4 Présentation de la direction des systèmes d'information (DSI)

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

Le centre informatique est une structure de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaïa, et cela en mettant en place les logiciels et infrastructures nécessaires pour la gestion du système d'information.

L'EPB déploie des systèmes d'information pour accroître la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseur et clients.

### 3.4.1 Missions de la DSI

La figure 3.3 représente les missions visées par le système d'information de l'entreprise portuaire de Bejaïa :


FIGURE 3.3 – Missions du système d'information de l'EPB.

### 3.4.2 Organisation humain de la DSI

La DSI se compose de trois départements, chaque département est structuré en services comme le montre la figure 3.4 :

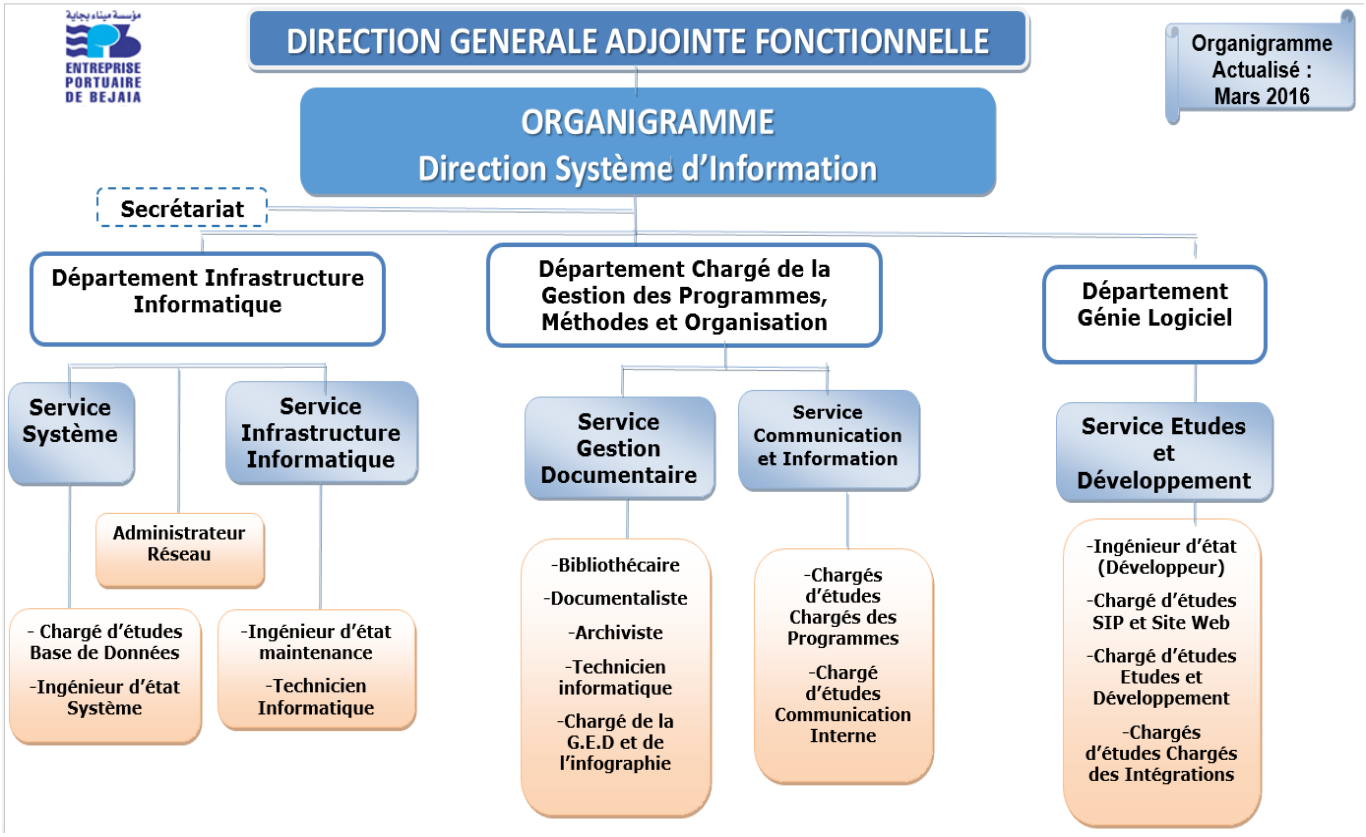


FIGURE 3.4 – L'organigramme de la structure informatique.

- **Département Infrastructure informatique** : chargé de l'administration et du déploiement du réseau, des systèmes, de la sécurité, des serveurs, des bases de données ; des équipements (dotation, suivi, maintenance et helpdesk . . . ).
- **Département Génie Logiciel** : c'est le département chargé de l'administration et du suivi des applications développées en interne ou acquises chez un fournisseur externe, dépoilement et assistance chez les utilisateurs finaux. Exemple d'applications existantes : GMAO (Gestion de Maintenance Assistée par Ordinateur), application ESCALE, GED (Gestion Électronique de Document), ERP (Enterprise Resource Planning), LOGIMAC, etc.
- **Département Programme Méthode et Organisation** : c'est une administration qui s'occupe des programmes méthode et organisations suivis des archives de l'affichage dynamique, communications internes . . . etc.

## 3.5 Infrastructure informatique

### 3.5.1 Réseau informatique de l'EPB

Le réseau du port de Bejaia s'étend du port pétrolier (n 16) aux ports 13 et 18 (port à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique éventuellement l'ensemble des serveurs, ces deux armoires servent à relier les différents sites de l'entreprise avec la DSI par fibres optiques. Chaque site a une armoire de brassage contenant un ou plusieurs convertisseur(s) média, un ou plusieurs Switchs (Cisco Catalyst 2960 24 ports, Micronet 16 ports) dans lesquels divers périphériques sont connectés via des câbles FTP (Foiled twisted pair).

### 3.5.2 Architecture réseau de l'entreprise

Le réseau de l'entreprise portuaire de Bejaïa est d'une architecture client/serveur. L'armoire de brassage constitue l'essence même du réseau de l'EPB, elle contient les équipements réseau permettant aux employés de l'entreprise d'accéder à Internet et de faire de l'intranet. On y distingue plusieurs switches où arrivent les câbles qui sont connectés aux différentes armoires de brassage de petite taille placées dans chaque étage des bâtiments, reliés aux prises murales où les employés connectent leurs ordinateurs. Les différents serveurs offrent des services aux différents postes clients.

La figure 3.5 représente l'architecture du réseau de l'Entreprise Portuaire de Bejaïa :

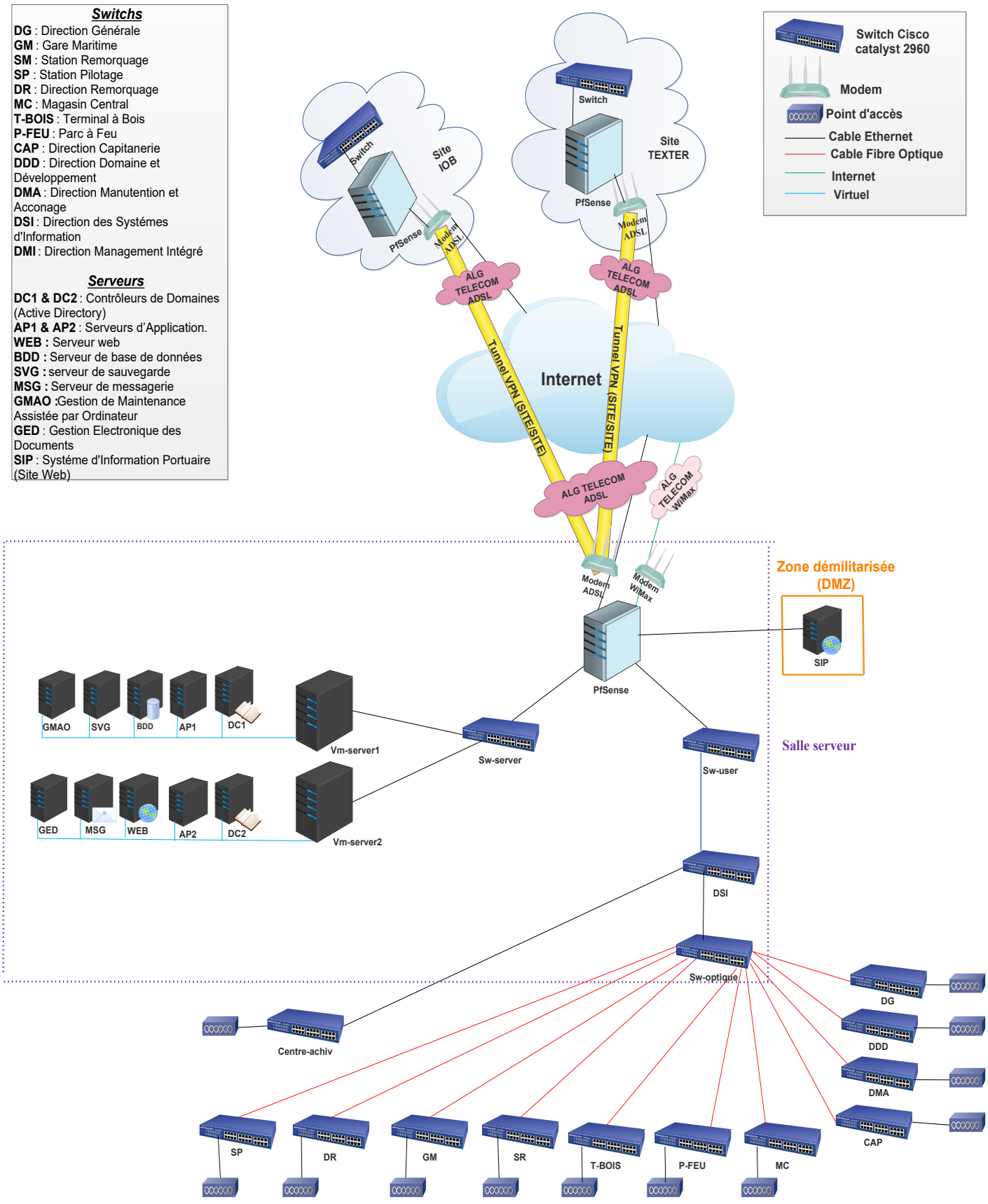


FIGURE 3.5 – Architecture actuelle du réseau de l'EPB.

#### 3.5.2.1 Étude de l'architecture

Notre étude est basée essentiellement sur un questionnaire effectué lors de nos différents entretiens qui ont eu lieu avec le personnel concerné de l'entreprise **(voir Annexe A)**.

$\alpha$ **Connexion Internet** : L'entreprise portuaire de Bejaïa s'est dotée de deux connexions fournies par ALG TELECOM : WiMAX et ADSL.

- La technologie ADSL permet d'assurer des transmissions numériques haut débit, sur de la paire torsadée classique ;
- La technologie WiMAX permet quant à elle de se connecter à internet haut débit grâce à une antenne Outdoor qui communique par ondes hertziennes via une station de base située au mont Gouraya respectivement, D'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

$\beta$ **Sécurité** :

- Les postes clients sont interconnectés avec les serveurs par des switches, sous contrôle d'un pare-feu pfSense pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet ;
- Une zone démilitarisée est utilisée pour avoir un accès au réseau local de manière privilégiée à partir de n'importe quel endroit ;
- Deux zones logistiques TEXTER et IGHIL OUBEROUAK qui sont reliées au réseau global via des tunnels VPN.

$\gamma$ **Salle serveur** : La salle serveur est le cœur du réseau, toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des switchs elle comporte les différents équipements :

- **Onduleur :** un onduleur afin de protéger les équipements réseau installés (switch, serveur...) ;
- **Armoire optique :** une armoire de fibre optique qui relie les câbles de fibre optique sortant elle contient des convertisseurs, des jarretières et des tiroirs optiques ;
- **Armoire de brassage :** contient une console KVM, des convertisseurs, des panneaux et cordons de brassage et deux serveurs physiques, contenant dedans d'autres serveurs virtuels tels que :
  - ✓ Deux contrôleurs de domaines DC1 et DC2 (Active Directory) sous Windows Serveur 2012 et également serveur DNS (Domain Name System) en plus l'infrastructure de clés publiques PKI (Public Key Infrastructure) hébergées dans DC1, DC2 hébergera un serveur DHCP (Dynamic Host Configuration Protocol)

et aussi un serveur WDS (Windows Déploiement Services) ;

- ✓ Serveur de base de données (SQL server and MARIA DB) ;
- ✓ Un serveur de sauvegarde en réseau NAS (Network-Attached Storage) intégrant le système RAID (Redundant Array of Independent Disks) en collaboration avec la baie de stockage ;
- ✓ Deux serveurs d'Applications ;
- ✓ Serveur web ;
- ✓ Serveur GMAO ;
- ✓ Serveur de messagerie Microsoft Outlook ;
- ✓ Serveur GED.

#### 3.5.2.2 Problématique

Aujourd'hui, la plupart des organisations et entreprises dépendent considérablement de leurs réseaux locaux pour leurs processus métier critiques. En d'autres termes, leur efficacité opérationnelle et l'amélioration continuelle de leur productivité et réactivité reposent en grande partie sur la qualité de leurs infrastructures réseau. Ceci a causé une véritable émergence de systèmes sophistiqués dédiés à la gestion de réseau, et grâce auxquels on gère très facilement des réseaux de plusieurs dizaines voire centaines d'équipements.

Après avoir étudié l'architecture réseau de l'EPB, cela nous a permis de soulever des faiblesses réseau existantes, qui peuvent se résumer globalement comme suit :

- Architecture plate : il n'y a pas de segmentation, il n'y a donc qu'un seul domaine de diffusion, ce qui signifie une charge énorme sur le réseau ;
- La sécurité est basée sur un pare-feu logiciel (pfSense), qui peut être facilement contourné et désactivé, laissant le système entier sans défense ;
- Les points d'accès sans fils ne sont pas protégés par un contrôleur WIFI contre les intrusions ;
- L'outil de supervision est très basique et présente de nombreuses lacunes :
  - Il ne permet pas de surveiller l'ensemble de l'infrastructure réseau et ces services ;
  - En cas de problème de fonctionnement anormal, l'administrateur ne sera pas alerté, ce qui entraînera une perte de temps importante lors du diagnostic des pannes, ce qui influe sur la qualité de service et donc sur le bon fonctionnement de l'entreprise ;
  - Incapacité de détecter la défaillance des équipements (charge CPU (Central Processing Unit), état mémoire, surcharge du disque...).

#### 3.5.2.3 Solutions proposées

Pour pallier aux problèmes énumérés dans la problématique, nous proposons les solutions suivantes :

- Mettre en place une architecture hiérarchique (switch accès/distribution/cœur) et segmenter le réseau en plusieurs VLAN, afin d'améliorer les performances du réseau et optimiser la bande passante en réponse aux surcharges rencontrées ;
- Mettre en place un pare-feu matériel, car il s'agit d'une solution de sécurité plus stable et performante, et elle est moins vulnérable aux attaques ;
- Remplacer la technologie ADSL par la fibre optique pour avoir une vitesse de connexion beaucoup plus élevée et une bande passante plus large ;
- Mettre en place un routeur avec deux cartes réseaux intégrées fibre optique et WiMAX ;
- Installer un contrôleur WIFI pour limiter l'accès, prévenir les intrusions, détecter et supprimer les interférences ;
- Placement d'un outil de supervision complet qui permet :
  - ✓ La surveillance réseau, système et applications ;
  - ✓ De détecter rapidement les pannes susceptibles d'affecter les équipements ;
  - ✓ D'alerter l'administrateur en temps réel par différents moyens (mail, sms) ;
  - ✓ La génération des rapports d'état et des graphes qui décrivent les états des composantes de chaque machine du parc.
  - ✓ Remplacer les onduleurs simples par des onduleurs UPS mangeables.

### 3.5.3 Architecture proposée pour le réseau de l'EPB

Nous pouvons regrouper les améliorations proposées dans l'architecture suivante (voir figure 3.6) :

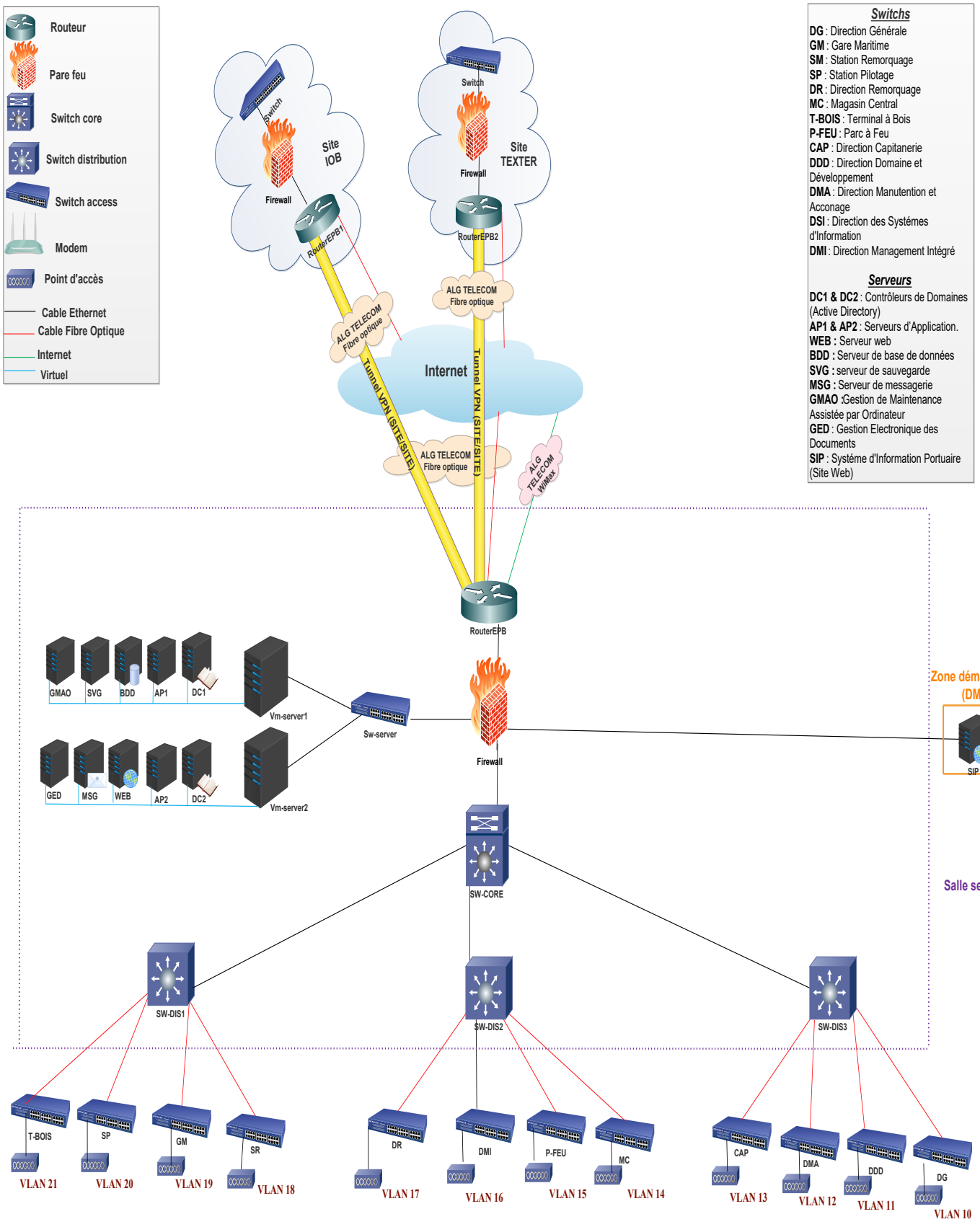


FIGURE 3.6 – Architecture proposée pour le réseau de l'EPB.

## 3.6 Présentation du projet à réaliser

Après avoir étudié les faiblesses et les améliorations de l'architecture réseau de l'EPB, nous serons en mesure d'utiliser un outil open source complet qui répond aux besoins de l'entreprise pour superviser l'ensemble de l'infrastructure réseau.

L'objectif principal de la supervision informatique est d'aider l'administrateur dans la gestion quotidienne du réseau et de lui permettre d'obtenir des informations précises sur l'état du réseau afin d'assurer la fiabilité et la crédibilité du service informatique. La solution permettra à l'entreprise d'augmenter son efficacité et sa productivité et offrira aux employés de meilleures conditions de travail.

### 3.6.1 Différents outils de supervision

Il existe plusieurs plateformes de supervision qui se veulent assez complètes, chacune d'entre elles propose des fonctionnalités différentes.

Cette partie comprendra une brève introduction de certaines solutions de supervision tout en expliquant leurs fonctionnalités, puis nous choisissons la solution la plus adaptée en fonction des besoins de l'entreprise.

#### 3.6.1.1 Outils de supervision propriétaires

Les logiciels de supervision dits « propriétaires » sont des logiciels caractérisés par l'appartenance à une personne ou à une société en particulier. Parmi ces logiciels on peut citer :

##### 3.6.1.1.1 WhatsUp Gold

WhatsUp Gold est un logiciel de supervision. Il propose un certain nombre de modules intégrés pour la gestion réseau. Les dernières nouveautés de la solution concernaient notamment l'ajout d'une rest API (Application Programming Interface) facilitant l'intégration. Aussi, les fonctionnalités de découverte ont été améliorées avec la possibilité de rafraîchir les liens sur les maps ou encore la création de listes d'exclusion [8].

##### 3.6.1.1.2 Cisco LMS

La solution de gestion de réseau local Cisco Prime LAN Management Solution (LMS) offre une gestion puissante du cycle de vie du réseau en simplifiant la configuration, la conformité, la surveillance, le dépannage et l'administration des réseaux Cisco. Cette solution innovante offre

une gestion de bout en bout des technologies et services critiques pour l'entreprise. Il aligne la fonctionnalité de gestion sur la façon dont les opérateurs de réseau font leur travail [9].

#### 3.6.1.1.3 PRTG Network Monitor

Le logiciel PRTG Network Monitor (Paessler Router Traffic Grapher), est un logiciel conçu par l'éditeur allemand Paessler spécialiste dans le domaine de la surveillance réseau. Cet outil permet de surveiller la bande passante des réseaux LAN, des serveurs et des sites Web. Il fournit ainsi les outils nécessaires pour surveiller le réseau, l'utilisation du disque, de mémoire ainsi que divers paramètres liés à l'infrastructure d'un réseau. Avec PRTG, tout est compris. Pas besoin d'installer de plug-ins supplémentaires ou de télécharger quoi que ce soit. PRTG est une solution puissante et intuitive convenant aux entreprises de toute taille [4].

### 3.6.1.2 Outils de supervision open Source

Plusieurs solutions existent pour résoudre les problématiques de la supervision. La plupart de ces solutions sont Open Source, c'est-à-dire que n'importe qui peut reprendre le code de l'application et le réadapter à sa manière ou bien pour ajouter de nouvelles fonctionnalités. Les logiciels de supervision dits « Open Source », les plus utilisées sont :

#### 3.6.1.2.1 Nagios

Nagios (anciennement Netsaint) est le logiciel libre le plus connu dans le milieu de la supervision réseau permettant de superviser le système et le réseau, C'est un outil très complet pouvant s'adapter à n'importe quel type d'utilisation avec des possibilités de configuration très poussées. Il reste l'outil de supervision le plus utilisé à l'heure actuelle.

L'architecture de Nagios est modulaire, il est composé par [6] :

- **Un moteur** : gérant l'ordonnancement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective) ;
- **L'interface web** : est la partie graphique visible, réalisée par php qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies ou (permettant de visualiser l'état du fonctionnement du système d'information) ;
- **Les plugins aussi appelées « sondes »** : permettant d'ajouter de nouvelles fonctionnalités au logiciel). Ces plugins peuvent être écrits dans de nombreux types de langages.

Le tableau 3.1 présente les avantages et inconvénients de Nagios :

| **Avantages** | **Inconvenients** |
|---|---|
| • Idéal pour une gestion de configuration centralisée ;<br>• Grosse communauté et bonne réputation ;<br>• Très puissant et modulaires ;<br>• Peut disposer d'une surcouche graphique (Centreon) ;<br>• Peut disposer de nombreux plugins. | • Difficile à installer et à configurer ;<br>• Dispose d'une interface compliquée ;<br>• Pas de représentations graphiques. |

TABLE 3.1 – Avantages et inconvénients de Nagios.

#### 3.6.1.2.2 Zabbix

Zabbix est une plateforme gratuite de supervision. Il propose une solution de supervision technique et applicative, offre des vues graphiques (générés par RRDtool (round-robin database tool)) et des alertes sur seuil. C'est une solution de monitoring complète embarquant un front-end web, un ou plusieurs serveurs distribués, et des agents multiplateformes précompilés (Windows, Linux, AIX (Advanced Interactive eXecutive), Solaris). Il est également capable de faire du monitoring SNMP et IPMI (Intelligent Platform Management Interface) ainsi que de la découverte de réseau. Il repose sur du C/C++, PHP (Hypertext Preprocessor) pour la partie front end et MySQL/PostgreSQL/Oracle pour la partie BDD (Base De Donnée) [7].

Le tableau 3.2 présente les avantages et inconvénients de Zabbix :

| **Avantages** | **Inconvenients** |
|---|---|
| • Des fonctionnalités très avancées permettant de gérer pratiquement tous les cas ;<br>• Facilité d'installation ;<br>• Ses agents sont assez légers (écrits en C) ;<br>• Solution très complète. | • Peu d'interfaçage avec d'autres solutions commerciales ;<br>• L'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple). |

TABLE 3.2 – Avantages et inconvénients de Zabbix.

#### 3.6.1.2.3 Pandora FMS

Pandora FMS (Flexible Monitoring System) est une solution complète qui a été conçue pour gérer et contrôler l'ensemble de l'infrastructure d'un réseau. C'est un système de surveillance à la fois flexible et hautement évolutif, destiné à être déployé dans des environnements de grande envergure.

Pandora FMS possède de nombreuses fonctionnalités, ce qui en fait une solution de nouvelle génération, qui couvre tous les problèmes de surveillance auxquels une organisation peut être confrontée. Il prend en charge les agents système Linux, Windows, AIX, HP-UX (Hewlett Packard Unix), Solaris et BSD (Berkeley Software Distribution). Il peut également être utilisé avec succès avec toutes sortes de dispositifs de réseau ; avec SNMP (versions 1,2,3) ou via des sondes de protocole TCP : SNMP, FTP (File Transfer Protocol), DNS, HTTP ( Hypertext Transfer Protocol ), ICMP (Internet Control Message Protocol) ou UDP. Il dispose d'une version commerciale qui permet de bénéficier de plus de fonctionnalités [5].

Le tableau 3.3 présente les avantages et inconvénients de Pandora FMS :

| **Avantages** | **Inconvenients** |
|---|---|
| • Grande variété de plugins ;<br>• Haute extensibilité ;<br>• Un grand nombre de fonctionnalités prêtes à l'emploi ;<br>• Compatible avec plusieurs OS ;<br>• Modulaire. | • Fonctionnalités supplémentaires sont dans la version payante. |

TABLE 3.3 – Avantages et inconvénients de Pandora FMS.

#### 3.6.1.3 Comparatif général des solutions Open Source

Le tableau 3.4 récapitule la comparaison des différents logiciels présentés :

| ***Critères fonctionnels*** | ***Nagios*** | ***Zabbix*** | ***Pandora FMS*** |
|---|---|---|---|
| **Environnement d'installation** | Linux | Linux | Windows/linux |
| **Installation et configuration simple** | Non | Oui | Oui |
| **Supervision systèmes/réseau /applicative** | Oui | Oui | Oui |
| **Génération de graphes** | Non | Oui | Oui |
| **Notification** | Oui | Oui | Oui |
| **Utilisation d'agents sur les machines cibles** | Oui | Oui | Oui |
| **Compatible SNMP** | Oui | Oui | Oui |
| **Découverte automatique** | Non | Oui | Oui |
| **Multiplateforme** | Non | Oui | Oui |
| **Rapports** | Oui | Oui | Oui |
| **Inventaire** | Non | Non | Oui |
| **Cartographie** | Non | Oui | Oui |
| **Action automatique** | Oui | Oui | Oui |
| **Logs et de gestion d'événements** | Oui | Oui | Oui |
| **Gestion d'ACL (Access Control List)** | Non | Oui | Oui |
| **Gestion des SLA (Service Level Agreement)** | Non | Oui | Oui |

TABLE 3.4 – Comparatif général des solutions Open Source.

### 3.6.2 Présentation de l'outil de supervision retenu

Pandora FMS est un logiciel de supervision on-prémisse orienté entreprise développée par la société espagnole Ártica en 2004 créée par Sancho Lerena. Pandora FMS recueille les données de n'importe quel système, génère des alertes basées sur ces données et affiche des graphiques, des rapports et des cartes de notre environnement. Il existe deux versions de Pandora FMS ; une version gratuite ou OpenSource et une version payante ou Entreprise.

Nous aurons la possibilité de surveiller des systèmes, des serveurs, des applications, des réseaux, des événements et une longue liste d'appareils. Pandora FMS collecte les informations que nous voulons surveiller, les compile et les enregistre pour les représenter visuellement, dans le but de réaliser les actions que nos systèmes nécessitent. Cet outil peut fonctionner sur différents systèmes d'exploitation, y compris Windows et Linux, ce dernier étant le système d'exploitation recommandé. L'une des caractéristiques principales de Pandora FMS est la flexibilité d'où son acronyme : F de "Flexibilité", M de "Monitoring" et S de "Software" [5].

Pandora FMS se compose de différents éléments pour son bon fonctionnement [5] :

- **Serveurs** : en charge de la collecte et du traitement des données ;
- **Base de données** : l'endroit où les serveurs stockent les informations collectées par les différents moniteurs, ainsi que la configuration de l'outil ;
- **Console** : c'est l'interface web chargée d'afficher les données collectées et la principale méthode d'interaction de l'utilisateur avec l'outil.

#### 3.6.2.1 Architecture de Pandora FMS

Pandora FMS se compose de plusieurs éléments, parmi lesquels les serveurs sont responsables de la collecte et du traitement des données. Les serveurs, avec les informations générées par eux ou par les agents, introduisent les données dans la base de données. La console est la partie chargée d'afficher les données présentes dans la base de données et d'interagir avec l'utilisateur final. Les agents logiciels sont des applications qui s'exécutent dans les systèmes surveillés et collectent les informations pour les envoyer aux serveurs Pandora FMS [5].

- **Serveurs :** les serveurs Pandora FMS sont les éléments chargés d'effectuer les contrôles existants. Ils les vérifient et modifient leur statut en fonction des résultats obtenus. Ils sont également chargés de déclencher les alertes qui sont établies pour contrôler l'état des données. Les serveurs Pandora FMS fonctionnent en permanence et vérifient en permanence si un élément a un problème et s'il est défini comme alerte.

  Il existe différents serveurs spécialisés dans différentes tâches de surveillance :

- ✓ ***Serveur de données :*** en charge du traitement des informations de surveillance locale collectées par les agents logiciels ;
- ✓ ***Serveur réseau :*** en charge de l'exécution des tâches de surveillance à distance via des contrôles réseau ;
- ✓ ***Serveur SNMP :*** en charge de la collecte et du traitement des traps SNMP ;
- ✓ ***Serveur WMI :*** en charge de la surveillance des environnements Windows ;
- ✓ ***Serveur de reconnaissance (Discovery) :*** chargé d'explorer le réseau et de détecter les nouveaux systèmes en fonctionnement ;
- ✓ ***Serveur de compléments (Plugins) :*** chargé de la surveillance à distance plus complexe à l'aide de scripts personnalisés ;
- ✓ ***Serveur de prédiction :*** chargé de savoir si une donnée, dans l'instant présent, est anormale ;
- ✓ ***Serveur WUX (WEB User eXperience) :*** en charge d'effectuer des transactions web complexes de manière distribuée.

- **Console web :** c'est l'interface utilisateur de Pandora FMS. Cette console d'administration et d'exploitation permet à différents utilisateurs, avec différents privilèges, de contrôler l'état des agents, de voir les informations statistiques, de générer des graphiques et des tableaux de données, ainsi que de gérer les incidents avec son système intégré. Il est également capable de générer des rapports et de définir de manière centralisée de nouveaux modules, agents, alertes et de créer d'autres utilisateurs et profils.
- **Base de données :** Pandora FMS utilise une base de données MySQL dans laquelle il stocke toutes les informations reçues en temps réel, en normalisant toutes les données provenant des différentes sources par exemple, toutes les données collectées par les agents, la configuration définie par l'administrateur, les événements, les incidents, les informations d'audit, etc. C'est le composant le plus important et le plus critique de toute installation Pandora FMS, contenant non seulement les informations et l'historique des données, mais aussi toutes les configurations effectuées au cours du temps. Actuellement, Pandora FMS ne supporte que MySQL/MariaDB/Percona.
- **Agents :** les agents définis dans la console Pandora FMS peuvent présenter des informations locales collectées par l'intermédiaire d'un agent logiciel, des informations à distance collectées par le biais de vérifications réseau, ou les deux. Il est important de distinguer entre ces deux concepts :
  - ✓ ***Agent logiciel :*** c'est un petit logiciel installé sur une machine et qui continue à s'exécuter, extrayant les informations à l'aide d'outils d'extraction locaux ou distants

et les envoyant régulièrement au serveur Pandora FMS. Cette installation est réalisée individuellement sur chaque machine, via un installateur ;

✓ ***Agent distant :*** Cet agent est installé à distance via la console Pandora FMS. En ciblant une adresse IP, il peut atteindre la machine sur laquelle le serveur Pandora FMS est installé. Dans cet agent, nous ne pouvons utiliser que des outils d'extraction distants.

Généralement, la surveillance des serveurs et de l'équipement sera effectuée à l'aide d'agents logiciels, tandis que la surveillance de l'équipement réseau sera effectuée à distance sans l'installation d'aucun logiciel.

La figure 3.7 présente l'architecture globale de pandora FMS :

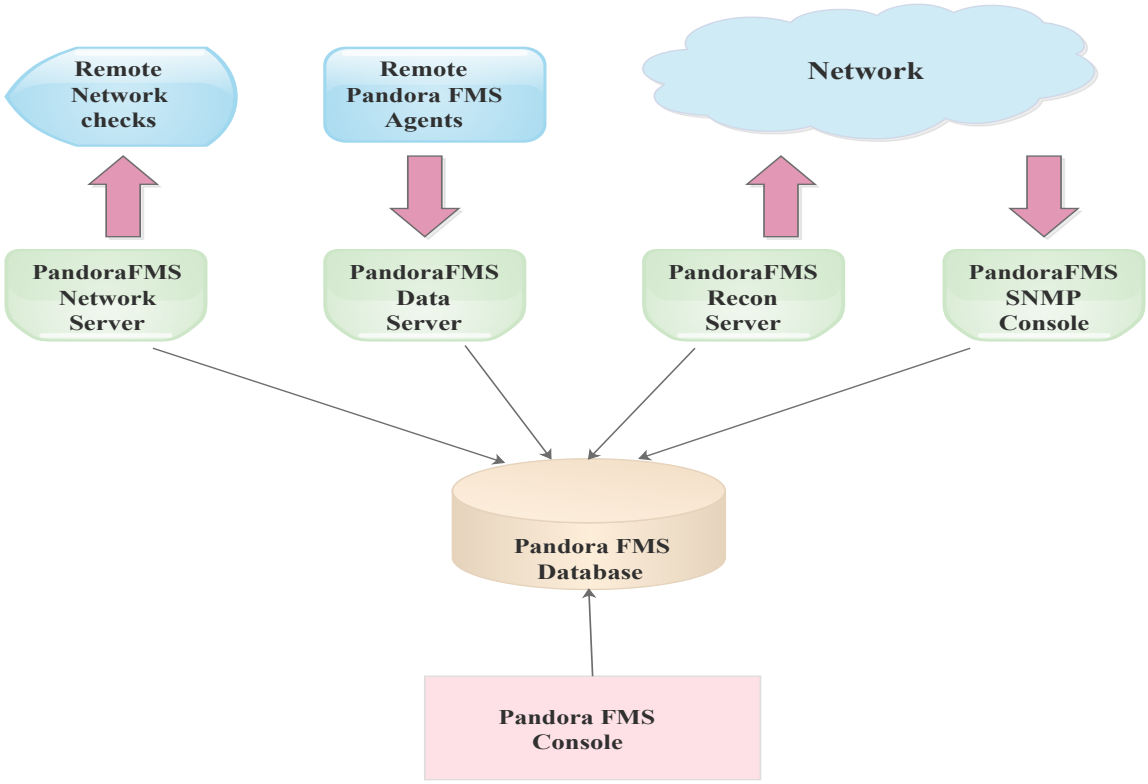


FIGURE 3.7 – Architecture globale de Pandora FMS.

#### 3.6.2.2 Les fichiers de configurations de Pandora FMS

Les fichiers principaux de configuration dont on a besoin de modifier/examiner sont [5] :

- **Pandora_server.conf :** situé par défaut dans le chemin */etc/pandora*, c'est un fichier de configuration principal du serveur de Pandora FMS qui contient toutes les directives globales de fonctionnement. En cas de modification d'une variable, on doit redémarrer le serveur Pandora FMS ;

- **config.php :** situé par défaut dans le chemin */var/www/html/pandora_console/include* contient un fichier de configuration de la console Pandora FMS généré automatiquement lors de l'installation ;
- **Pandora_agent.conf :** situé par défaut dans le chemin */etc/pandora*, c'est un fichier de configuration principal de l'agent software de Pandora FMS sur Unix. Tous les paramètres de configuration et de surveillance des agents logiciels se trouvent dans leur fichier de configuration. Celui-ci est stocké localement sur la machine où l'agent logiciel est installé, donc toute modification à apporter à l'agent doit être reflétée dans ce fichier ;
- **My.cnf :** situé dans le chemin */etc*, c'est une configuration principale de la base de donnée Pandora FMS (Mysql).

#### 3.6.2.3 Fonctionnalités de base de Pandora FMS

Les fonctionnalités de base de Pandora FMS sont [5] :

- Supervision système et applications ;
- La surveillance réseau (SNMP, WMI, TCP et ICMP...), IPv4 et IPv6 ;
- La surveillance de SNMP via scrutation et « traps » ;
- La surveillance de l'expérience d'utilisateur ;
- Surveillance des serveurs (Windows, Linux, Unix et MacOSX) : agent et sans agent ;
- Création de modules (module donnée /module réseau/module WMI) ;
- La gestion des événements et des échecs ;
- L'auto-découverte et la détection automatique de la topologie du réseau ;
- Console de visualisation personnalisable en fonction de niveaux de service ;
- Rapports d'inventaire ;
- Haute disponibilité ;
- Agents multiplateformes pour Windows, HP-UX, Solaris, BSD et Linux fournissent des informations sur le système dans lequel ils sont installés (CPU, utilisation de la mémoire, utilisation du disque, etc.) ;
- Gestion d'ACL : un utilisateur ne peut accéder qu'aux informations relatives au profil auquel il appartient ;
- Le SLA et l'élaboration des rapports ;
- La connexion SSH (Secure Shell) / Telnet (TELetype NETwork) aux périphériques depuis l'interface web ;
- Tableaux de bord et cartes topologiques de surveillance personnalisables ;

- La possibilité de développer ses propres plugins ;
- Génération et envoi d'alarmes (emails et SMS) ;
- Sauvegarde des journaux et logs.

#### 3.6.2.4 Pourquoi choisir Pandora FMS

- Simple à utiliser et facile à installer et à configurer ;
- Outil de surveillance open source pour la gestion de l'infrastructure informatique. Il se distingue comme l'une des solutions de surveillance les plus flexibles du marché, idéal pour la plupart des environnements de taille moyenne et grande (100 appareils ou plus) ;
- Il existe une version IOS basée sur Centos déjà préconfigurée ;
- C'est un outil très variable et modulaire, qui nous permet de travailler de différentes manières et avec la combinaison de différents types de surveillance ;
- Possède un grand nombre de fonctionnalités, ce qui en fait un logiciel de nouvelle génération qui couvre tous les problèmes de surveillance que votre organisation peut rencontrer ;
- La capacité de surveiller et de gérer de nombreuses facettes de votre infrastructure réseau, y compris l'utilisation de la bande passante / surveillance des commutateurs, routeurs, modems et autres passerelles et périphériques réseau ;
- L'interface web ergonomique et conviviale, pas trop de connaissances requises pour obtenir des rapports et des graphiques ;
- Évolutivité : Pandora FMS peut gérer jusqu'à 1000 agents par serveur ;
- Il offre non seulement aux administrateurs réseau et aux ingénieurs un tableau de bord informatif pour surveiller leurs applications et leurs serveurs de base de données, mais vous donne également la possibilité de présenter des informations critiques aux gestionnaires dans une mise en page graphique qui est présentée de manière facile à lire ;
- Offre un système d'alerte et de notification robuste. Les alertes et les notifications peuvent être configurées à l'aide de SMS, d'applications en ligne (y compris Slack, Jabber, etc.), d'e-mail, de Syslog et de scripts personnalisés ;
- Fonctionne en conjonction non seulement avec les systèmes d'exploitation Windows, mais également avec les systèmes d'exploitation Linux, ce qui le rend beaucoup plus robuste ;
- Unification des différents outils en un.

## 3.7 Conclusion

On a conçu ce chapitre pour nous familiariser avec l'entreprise d'accueil et l'architecture réseau dont elle dispose. Après avoir fait l'analyse du réseau de l'EPB, nous avons soulevé plusieurs faiblesses réseau existantes, ce qui nous a permis de cerner la problématique de notre projet et énumérer les différentes solutions. Ensuite, nous avons illustré certains outils de supervision, et ce pour but de faire une étude comparative. Enfin nous avons défini l'outil de supervision retenu « Pandora FMS » qui est le plus adapté dans notre cas par rapport aux caractéristiques qu'il offre et aux nombreuses fonctionnalités qui ne figurent pas dans d'autres logiciels.

Dans le chapitre suivant, nous présentons notre politique de supervision ainsi que les étapes d'implémentation.

# CHAPITRE 4

# IMPLÉMENTATION DE LA SOLUTION DE SUPERVISION PANDORA FMS

## 4.1 Introduction

Dans ce chapitre nous allons modéliser et implémenter notre politique de supervision.

## 4.2 Modélisation de la politique de supervision

Afin de mettre en œuvre notre projet, nous avons établi une politique de supervision basée sur un modèle de carte heuristique (Mind Map) présentée dans la figure 4.1.

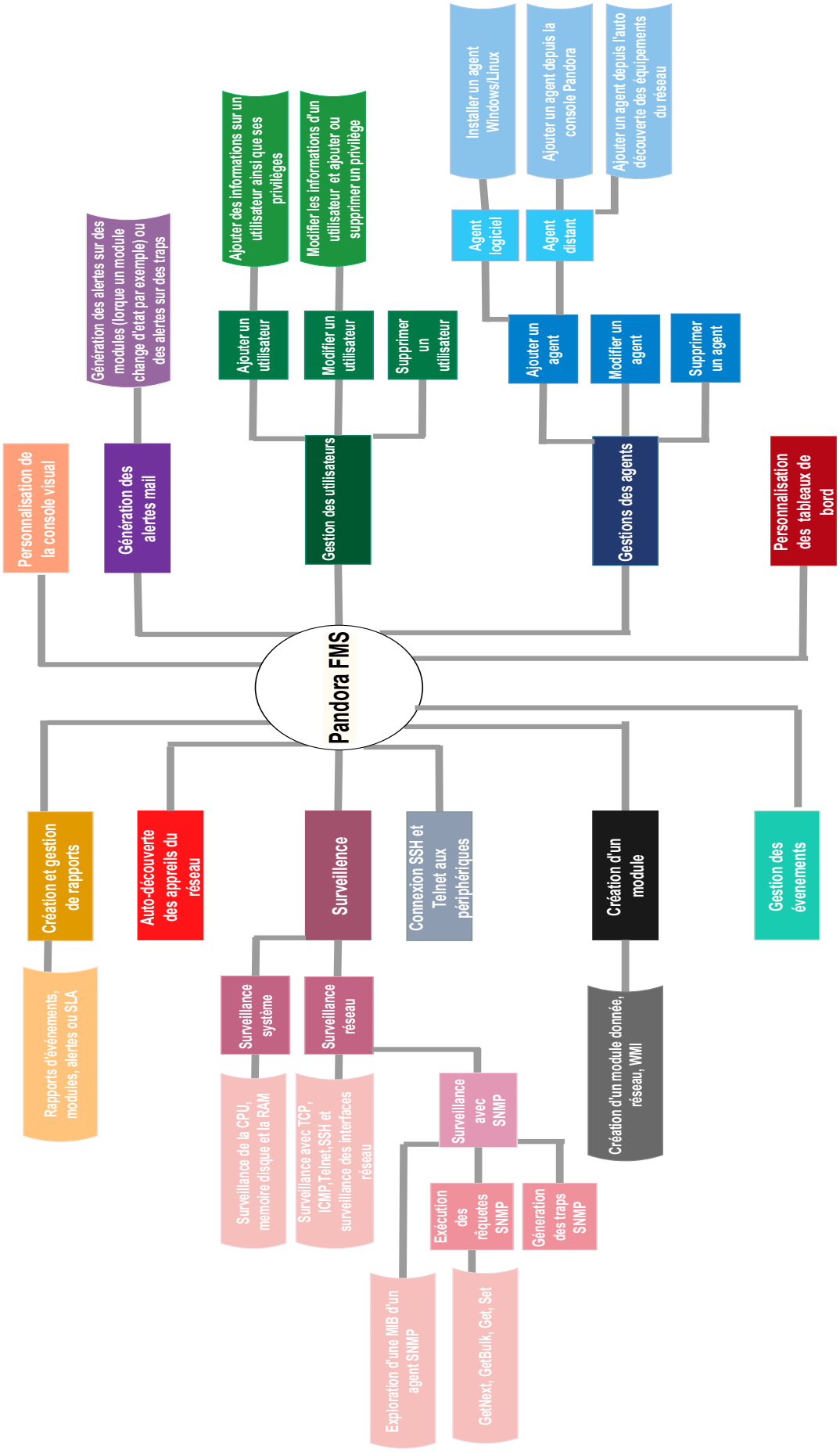


FIGURE 4.1 – Politique de supervision de Pandora fms.

## 4.3 Reproduction du réseau LAN de l'EPB

Afin de configurer et superviser le réseau LAN de l'EPB, nous allons le reproduire sous le simulateur GNS3 (Graphical Network Simulator-3).

### 4.3.1 Partie théorique

#### 4.3.1.1 Réseau à superviser

Le réseau que nous allons superviser est constitué de :

- Un routeur ;
- Sept switchs (un switch cœur, deux switchs distributions et quatre switchs accès) ;
- Des postes Linux et Windows ;
- Un serveur Pandora FMS qui s'occupera de la supervision et l'analyse des informations du réseau.

#### 4.3.1.2 Configuration des VLANs

Le tableau 4.1 suivant montre les noms des VLANs existant au niveau de l'entreprise ainsi que leurs adresses de sous réseau :

| **Nom VLAN** | **ID VLAN** | **Adresse de sous réseau** | **Description** |
|---|---|---|---|
| Administration | 1 | 192.168.100.0 /24 | VLAN pour la supervision des équipements |
| DG | 10 | 192.168.10.0/24 | VLAN des postes de travail de la direction Générale |
| DSI | 20 | 192.168.20.0/24 | VLAN des postes de travail de la direction des systèmes d'information |
| DFC | 30 | 192.168.30.0/24 | VLAN des postes de travail de la direction des finances et comptabilité |
| DRH | 40 | 192.168.40.0/24 | VLAN des postes de travail de la direction des ressources humaines |

Table 4.1 – Nom des VLANS.

#### 4.3.1.3 Configuration de VTP (Vlan Trunking Protocol)

Le protocole VTP est un protocole de couche 2, son principal avantage est sa capacité de propager automatiquement des VLANs configurés sur un commutateur en mode 'server' vers les autres commutateurs configurés en mode client.

Durant la phase de déploiement, nous allons configurer le switch cœur en mode 'VTP server' tandis que les autres switchs seront configurés en mode 'VTP client'.

Le tableau 4.2 montre comment le VTP sera configuré :

| **VTP** | **Domain** | **Mode** |
|---|---|---|
| SW-CORE | epb | Server |
| Tous les autres switchs | epb | Client |

TABLE 4.2 – Configuration de VTP.

#### 4.3.1.4 Configuration de STP (Spanning Tree Protocol)

STP est un protocole de couche 2 conçu pour les ponts et les commutateurs. Il apporte une solution au problème posé par la présence de boucles dans les réseaux commutés de type Ethernet.

#### 4.3.1.5 Classification des PC selon les VLANs

Les interfaces entre tous les switchs (switch accès, distribution, coeur) seront configurées en mode trunk pour qu'elles puissent transporter les informations des différents VLANs. Les interfaces qui seront connectées à des postes de travail seront configurées en mode access.

Le tableau 4.3 présente la classification des PC selon les VLANs :

| **Nom d'hôte** | **Port de switch** | **ID Vlan** | **Adresse IP du sous réseau** | **Passerelle** |
|---|---|---|---|---|
| PC1 | Port e2/1 SW-ACCESS1 | 10 | 192.168.10.0/24 | 192.168.10.10 |
| PC2 | Port e2/2 SW-ACCESS1 | 10 | 192.168.10.0/24 | 192.168.10.10 |
| PC3 | Port e2/1 SW-ACCESS2 | 20 | 192.168.20.0/24 | 192.168.20.10 |
| PC4 | Port e2/2 SW-ACCESS2 | 20 | 192.168.20.0/24 | 192.168.20.10 |
| PC5 | Port e2/1 SW-ACCESS3 | 30 | 192.168.30.0/24 | 192.168.30.10 |
| PC6 | Port e2/2 SW-ACCESS3 | 30 | 192.168.30.0/24 | 192.168.30.10 |
| PC7 | Port e2/1 SW-ACCESS4 | 40 | 192.168.40.0/24 | 192.168.40.10 |
| PC8 | Port e2/2 SW-ACCESS4 | 40 | 192.168.40.0/24 | 192.168.40.10 |

TABLE 4.3 – Classification des PC selon les VLANs.

### 4.3.2 Partie pratique

Afin de réaliser notre projet, nous allons procéder à la configuration des équipements sous GNS3, pour ensuite les superviser avec l'outil Pandora FMS.

La figure 4.2 présente l'architecture réseau LAN de l'EPB sous GNS3 :

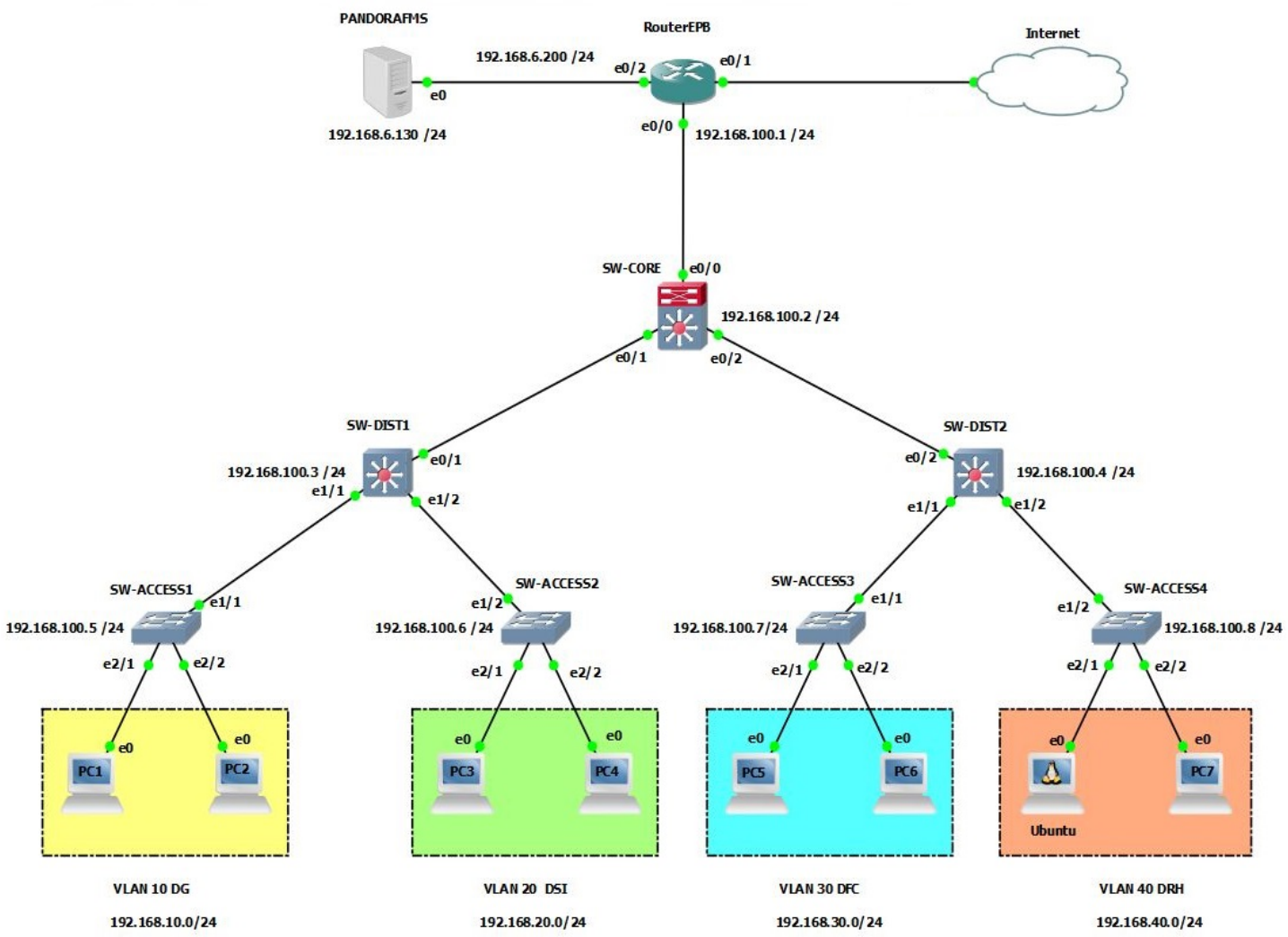


FIGURE 4.2 – Architecture réseau LAN de l'EPB sous GNS3.

#### 4.3.2.1 Configuration des équipements

Pour configurer les équipements, nous allons suivre les étapes ci-dessous, chaque exemple de configuration est illustré dans l'annexe **(Annexe B)** :

1. Configuration des noms des équipements ;
2. Configurations de mot de passe pour le mode privilégié, la ligne console et virtuelle (Telnet et SSH) ;
3. Configuration de la bannière de connexion ;
4. Création des Vlans et configuration de VTP ;
5. Configuration de STP ;
6. Configuration des interfaces ;
7. Configuration du routage inter-vlan ;
8. Configuration de DHCP.

## 4.4 Implémentation de la politique de supervision

Après avoir installé et configuré Pandora FMS (**voir Annexe C**) et modélisé notre politique de supervision, nous allons procéder à l'implémentation des fonctionnalités de Pandora FMS.

### 4.4.1 Gestion des agents

Nous pourrions diviser la surveillance en deux grands groupes, selon la façon dont l'information est recueillie : la surveillance fondée sur les agents logiciels et la surveillance à distance.

Les deux types d'agents partagent la même configuration générale et la même visualisation des données.

#### 4.4.1.1 Ajout d'un agent logiciel

La surveillance par agent logiciel consiste en l'installation d'un logiciel qui reste actif dans le système et en l'obtention d'informations "localement", par l'exécution de commandes et de scripts.

Nous avons illustré un exemple d'installation et de configuration d'un agent linux dans l'annexe (**Annexe C**).

#### 4.4.1.2 Ajout d'un agent distant

La surveillance à distance consiste à utiliser le réseau pour effectuer des contrôles à distance vers les systèmes, sans qu'il soit nécessaire d'installer un composant supplémentaire dans l'équipement à surveiller.

L'ajout d'un agent distant se fait de deux manières :

##### 4.4.1.2.1 Ajout d'un agent depuis la console Pandora FMS

1. Dans le menu latéral, accédez à Ressources → Gestion d'agents, Depuis l'écran présenté dans la figure 4.3, cliquez sur 'Créer un agent' pour définir un nouvel agent ;

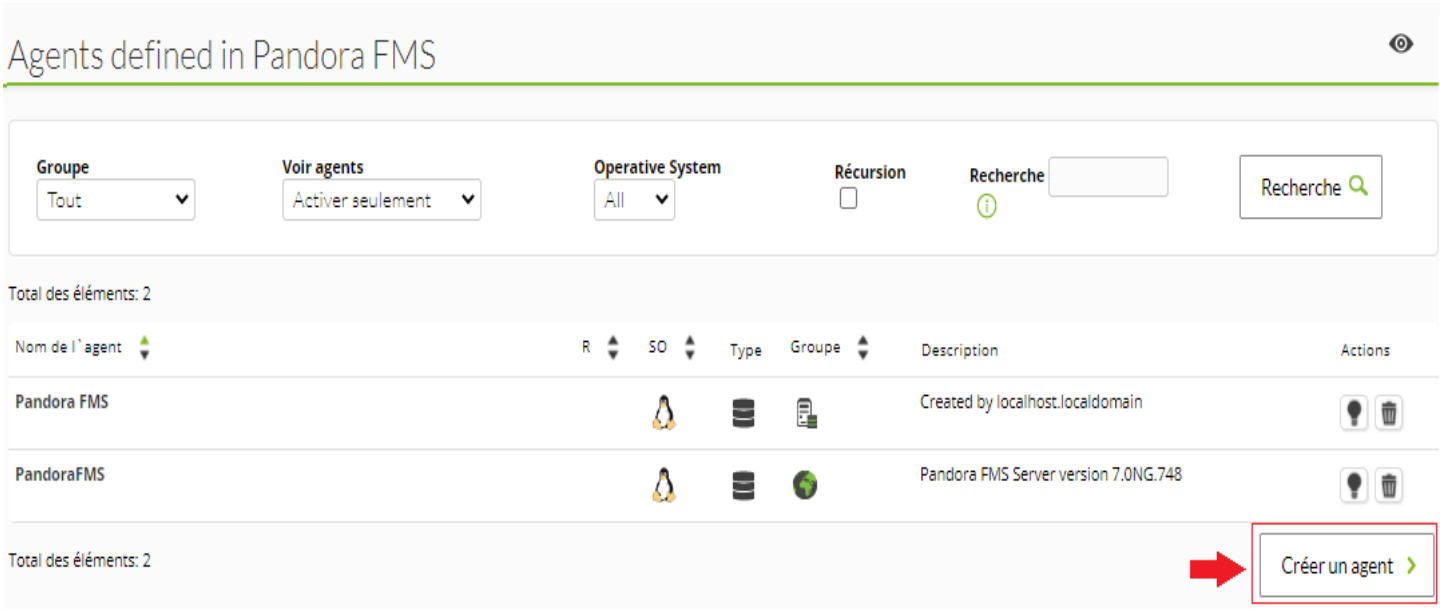


FIGURE 4.3 – Créer un nouvel agent dans Pandora FMS.

2. Sur la page Administrateur d'agents , définissez un nouvel agent en remplissant le formulaire. Une fois que vous avez terminé, cliquez sur 'Créer' comme illustré dans la figure 4.4 ;

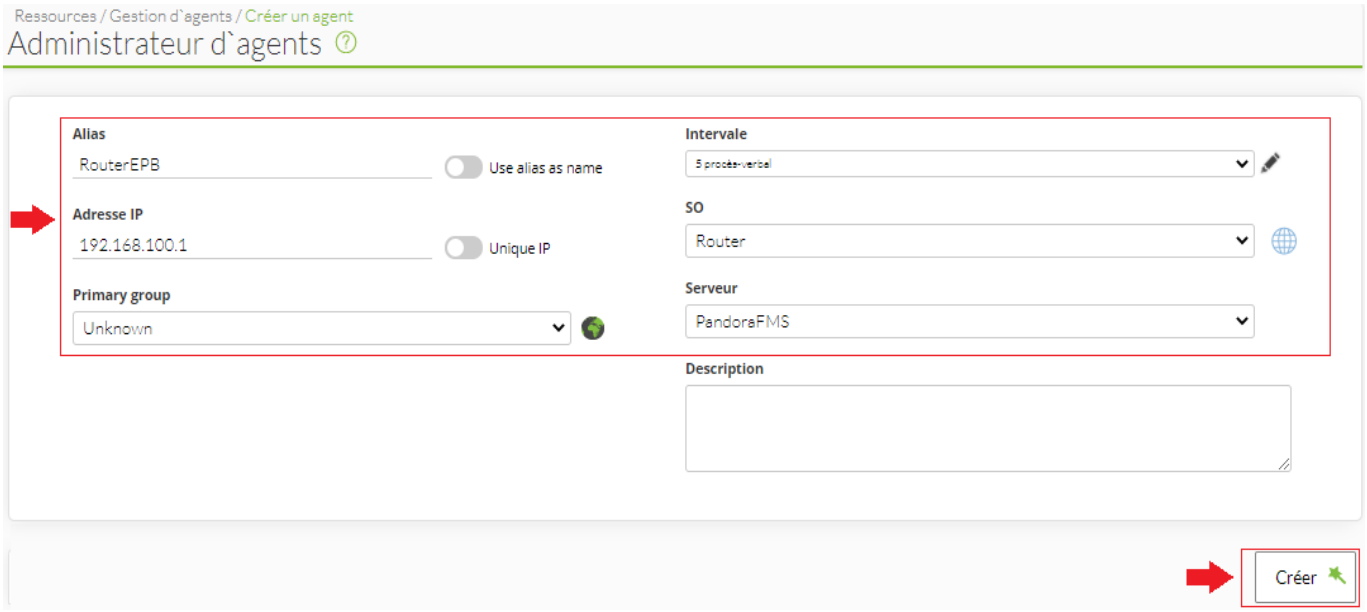


FIGURE 4.4 – Ajouter les détails de l'agent.

3. Après avoir ajouté l'agent, il doit se refléter dans la page Détail de l'agent (voir figure 4.5). Vous devez donc créer des modules pour surveiller l'hôte sur lequel l'agent s'exécute.

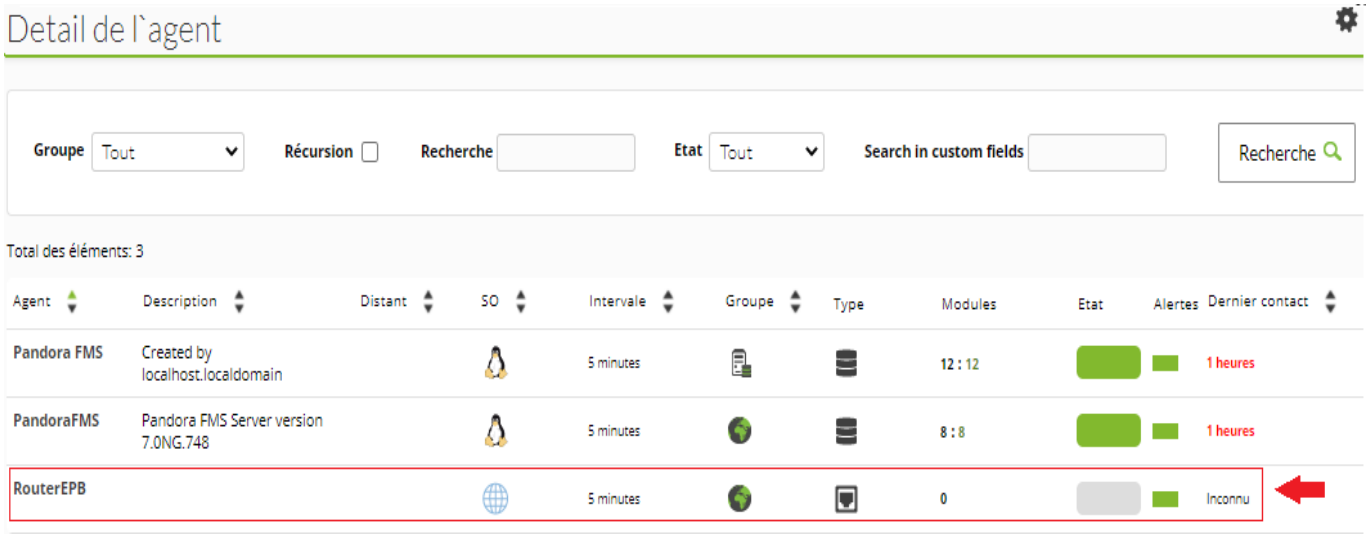


FIGURE 4.5 – Afficher les détails de l'agent Pandora FMS.

#### 4.4.1.2.2 Ajout d'un agent depuis l'auto découverte des équipements du réseau

1. Dans le menu latéral allez sur Discovery puis sur la page 'Network Scan', définissez une nouvelle tâche en remplissant le formulaire comme indiqué dans la figure 4.6. Une fois que vous avez terminé, cliquez sur suivant et sélectionnez le type Modèles réseau puis cliquez sur 'finir' ;

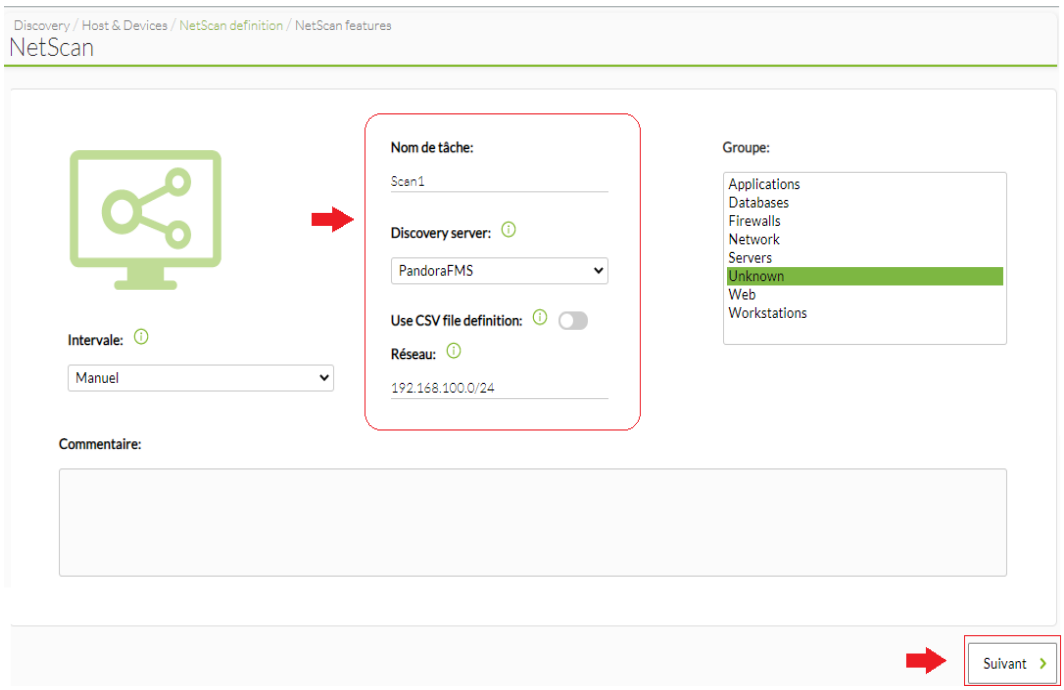


FIGURE 4.6 – Fenêtre Network Scan.

2. Une fois créée, une liste des agents découverts sera affichée, ensuite sélectionnez l'adresse de l'agent à superviser comme illustré dans la figure 4.7.

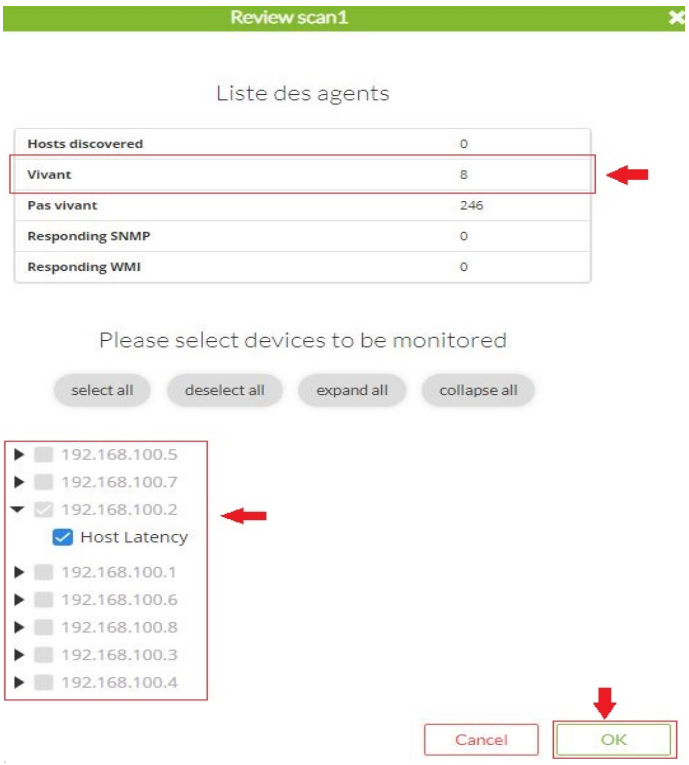


FIGURE 4.7 – Liste des agents découverts.

### 4.4.2 Création d'un module

Les modules sont des unités d'information stockées dans un agent. Il s'agit des éléments de surveillance avec lesquels l'information est extraite de l'appareil ou du serveur vers lequel l'agent pointe. Chaque module ne peut stocker qu'un seul type de métrique.

Tous les modules ont un état associé, qui peut être :

- **Non commencé (bleu) :** où aucune donnée n'a encore été reçue ;
- **Normal (vert) :** reçoit des données dont les valeurs se situent en dehors des seuils d'avertissement ou des seuils critiques ;
- **Avertissement (jaune) :** reçoit des données dont les valeurs se situent à l'intérieur du seuil d'avertissement ;
- **Critique (rouge) :** Les données sont reçues avec des valeurs inférieures au seuil critique ;
- **Inconnu (gris) :** le module a fonctionné et a cessé de recevoir des informations pendant un certain temps.

Pour créer un module :

1. Au niveau des agents définis dans l'écran Pandora FMS, cliquez sur le nom de l'agent (SW-ACCESS2) pour le modifier. Une fois chargée, cliquez sur l'onglet Modules ;
2. Sélectionnez ensuite le type de module (par exemple, Créer un nouveau module de

serveur réseau) et cliquez sur 'Créer', une fois créée et à partir de la fenêtre illustrée dans la figure 4.8 , sélectionnez le groupe de composants du module (par exemple, Gestion du réseau) et son type de contrôle réel (par exemple Host Alive ). Remplissez ensuite les autres champs et assurez-vous que l'adresse IP cible est celle de l'hôte à surveiller. Cliquez ensuite sur 'Créer'.

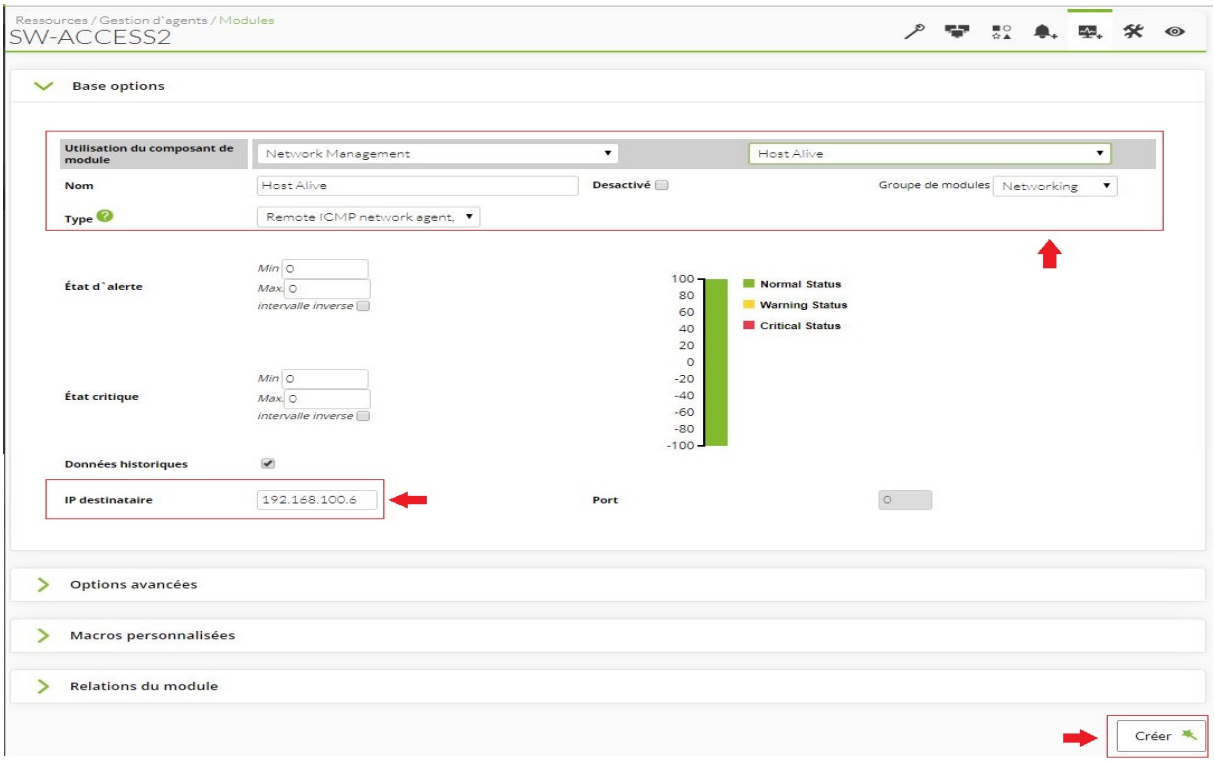


FIGURE 4.8 – Fenêtre créer module.

La fenêtre illustrée dans la figure 4.9 apparaît.

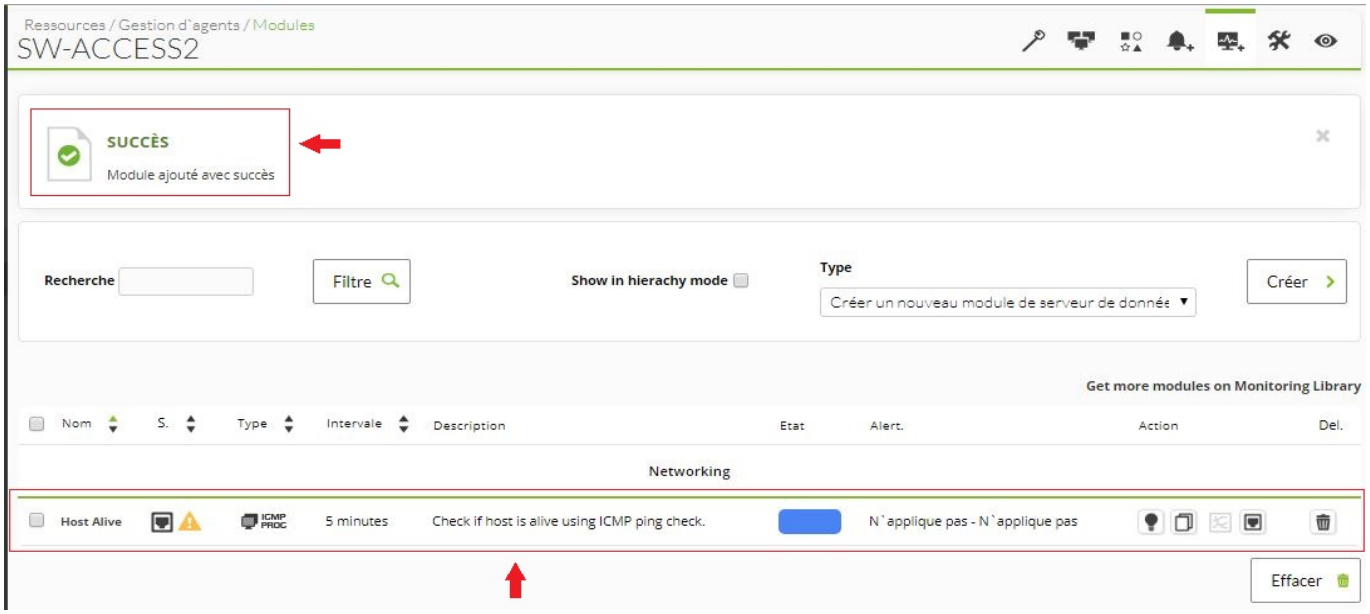


FIGURE 4.9 – Module de l'agent créé.

### 4.4.3 Connexion SSH et Telnet aux périphériques

La console Pandora FMS permet de se connecter via ssh ou telnet à n'importe quel agent avec une adresse IP configurée.

Pour accéder via Telnet/SSH :

1. Sélectionnez un agent depuis la liste des agents → cliquer sur le QuickShell, la fenêtre illustrée dans la figure 4.10 apparaît puis effectuer des actions telles que vous connecter par Telnet ou SSH ;

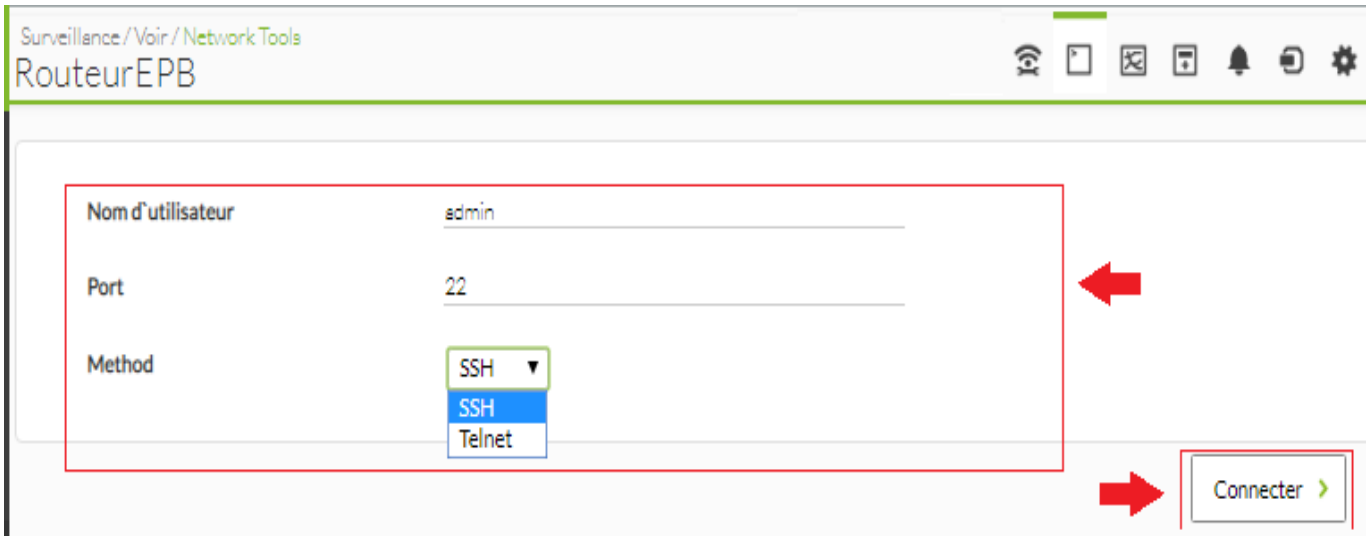


FIGURE 4.10 – Fenêtre QuickShell.

2. Une fois vous avez choisi le nom d'utilisateur et le protocole de connexion, lors de la

connexion, une interface s'ouvrira (voir figure 4.11), depuis cette interface, introduisez le mot de passe pour se connecter.

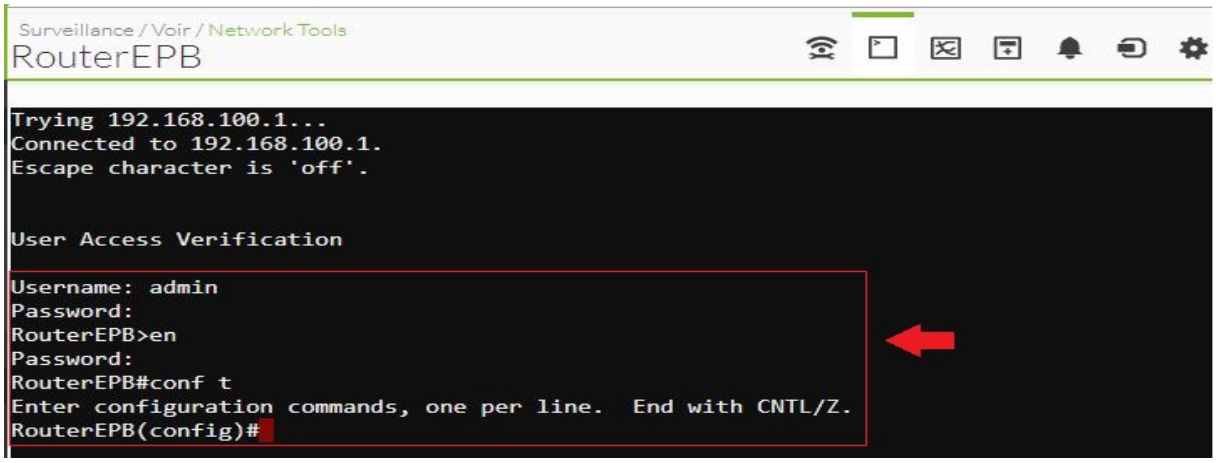


FIGURE 4.11 – Accès au RouterEPB via Telnet.

### 4.4.4 Personnalisation de la console visuelle

Pandora FMS permet de construire des cartes visuelles où chaque utilisateur définit sa propre façon de représenter visuellement la surveillance.

Pour créer une console visuelle :

1. Allez à carte de topologie → console visuelle. Une liste apparaît avec toutes les cartes créées ; pour en créer une nouvelle, cliquez sur 'Créer'. La Fenêtre 'Nouvelle console visuelle' apparaît ou vous devez remplir le formulaire et cliquer sur 'enregistrer' ;
2. Une fois enregistrée vous pouvez commencer à personnaliser votre console visuelle comme illustrée dans la figure 4.12.

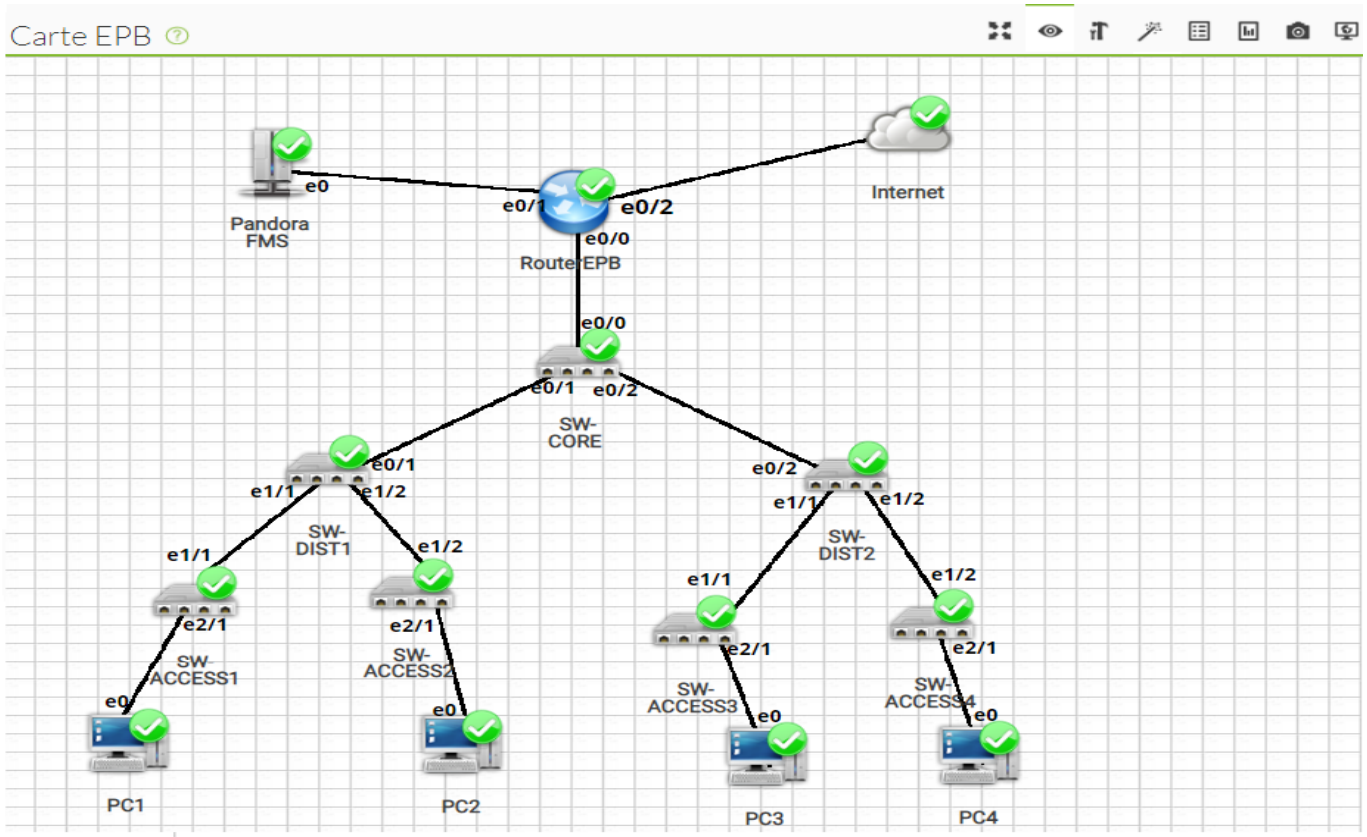


FIGURE 4.12 – Carte visuelle de l'EPB sous Pandora FMS.

### 4.4.5 Gestion des événements

Le système d'événements Pandora FMS permet de voir un enregistrement en temps réel de tous les événements qui se produisent dans nos systèmes surveillés.

Les événements sont classés en fonction de leur gravité :

- Maintenance (gris) ;
- Informatif (bleu) ;
- Normal (vert) ;
- Warning (jaune) ;
- Critique (rouge) ;
- Important (Marron) ;
- Minime (Rose).

Les événements sont gérés dans Événements → voir événements ", où le menu illustré dans la figure 4.13 est affiché, dans cette fenêtre vous pouvez valider, supprimer ou afficher les informations détaillées sur un événement.

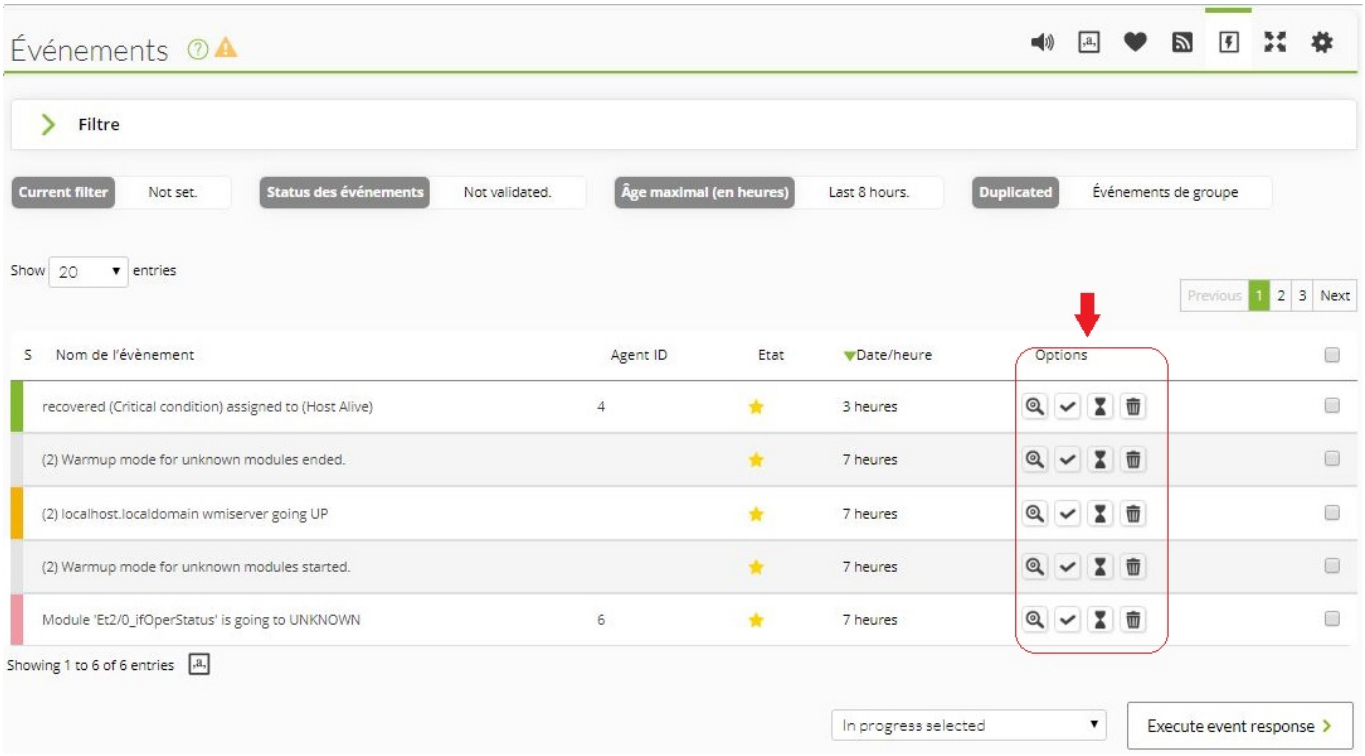


FIGURE 4.13 – Gestion des évènements.

### 4.4.6 Création et gestion des rapports

Pandora FMS nous offre la possibilité de présenter les données surveillées de manière ordonnée sous forme de rapports.

Dans un rapport, l'information à présenter est organisée en éléments du rapport. Il existe de nombreux types d'éléments différents, qui effectuent des calculs et présentent l'information de manières très différentes. Par exemple, un élément de type SLA qui permet de mesurer le niveau de réalisation d'un service (Service Level Agrement) d'un moniteur Pandora FMS.

La création d'un rapport se fait de la manière suivante :

1. Allez dans Rapports → Rapports personnalisés, Une liste de tous les rapports créés apparaîtra, pour créer un rapport, cliquez sur 'Créer un Rapport'.
2. Une fois le rapport créé, Nous pouvons ajouter différents types d'éléments au rapport (4.14).

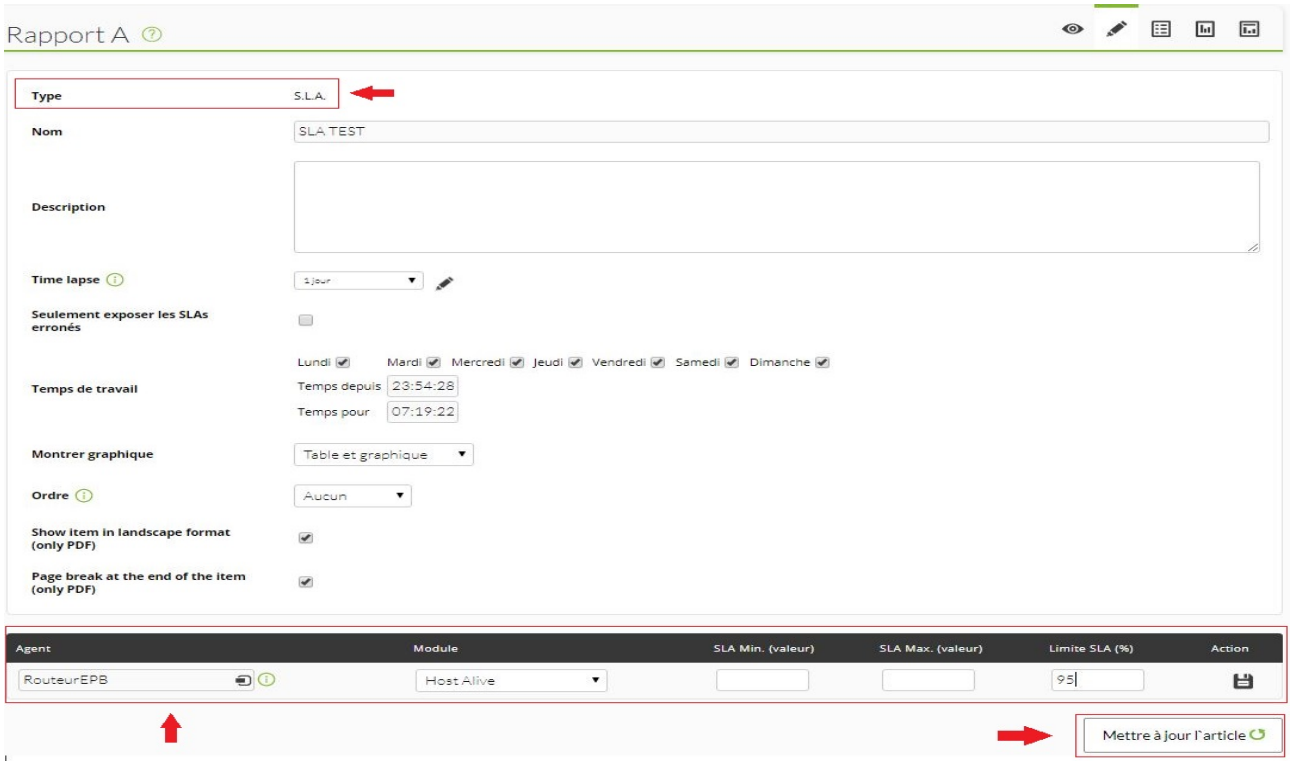


FIGURE 4.14 – Créer un rapport SLA.

Exemple de vue de ce type de rapport est illustré dans la figure 4.15 :

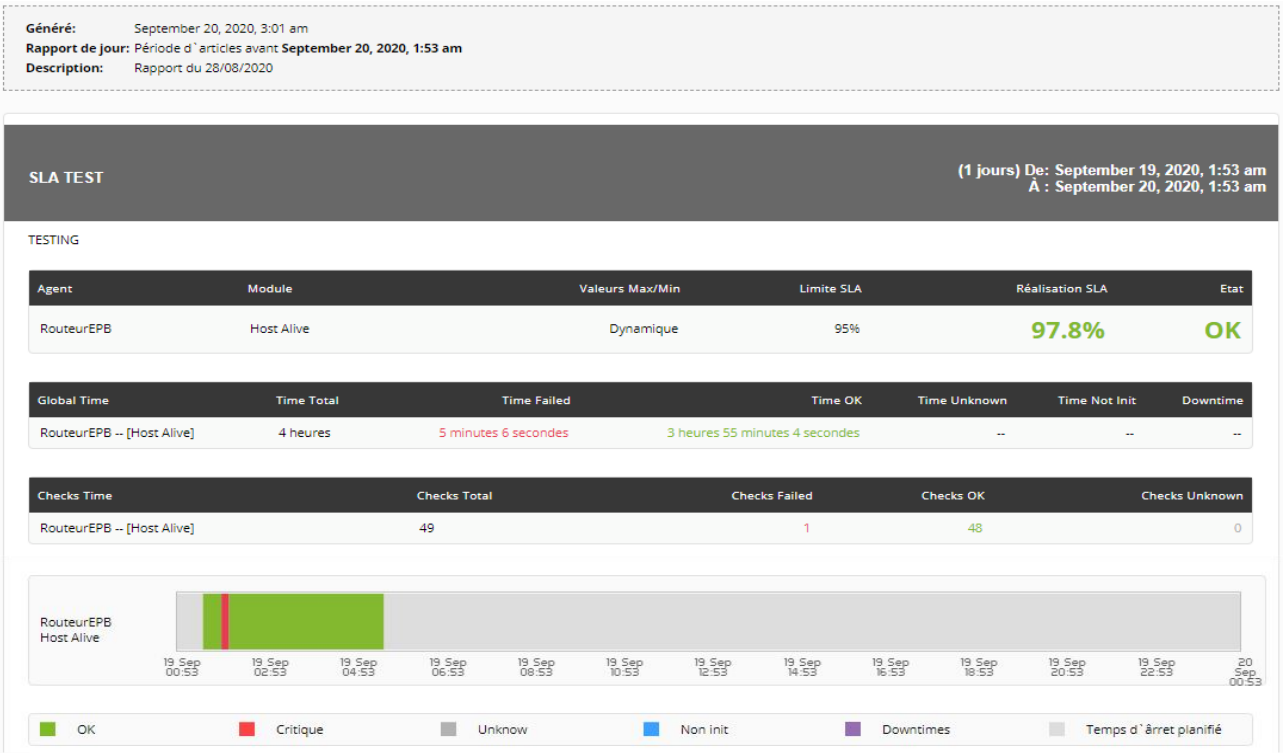


FIGURE 4.15 – Rapport SLA sur le module Host Alive.

### 4.4.7 Surveillance

#### 4.4.7.1 Surveillance système et réseau

Dans notre machine, nous souhaitons surveiller les paramètres systèmes (CPU) et réseaux (ICMP). Pour réaliser la surveillance, il est nécessaire de paramétrer les seuils 'warning' et 'critical' pour connaître l'état du module surveillé et diagnostiquer les éventuels problèmes dans le temps.

##### 4.4.7.1.1 Surveillance CPU de notre machine locale

Le module CPU Load renvoie le pourcentage de CPU en usage (voir figure 4.16).

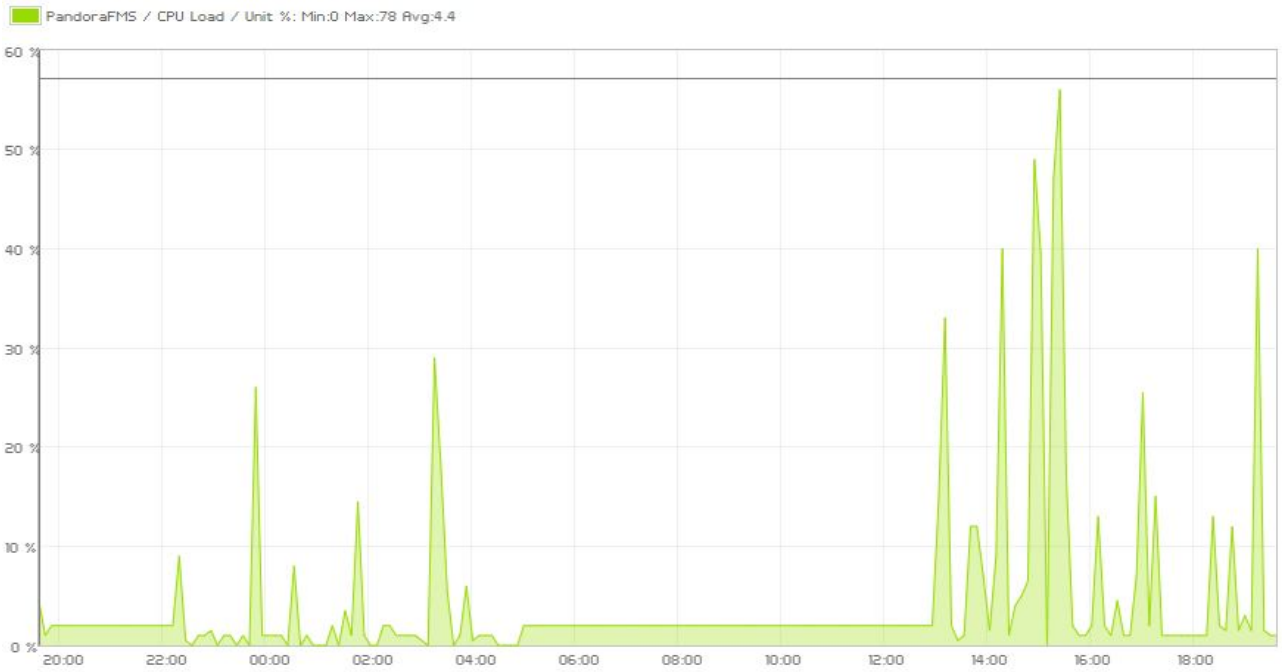


FIGURE 4.16 – Graphe du module CPU load.

##### 4.4.7.1.2 Surveillance ICMP de notre machine locale

Les tests ICMP ou ping sont très utiles pour savoir si une machine est connectée ou non à un réseau (voir figure 4.17).

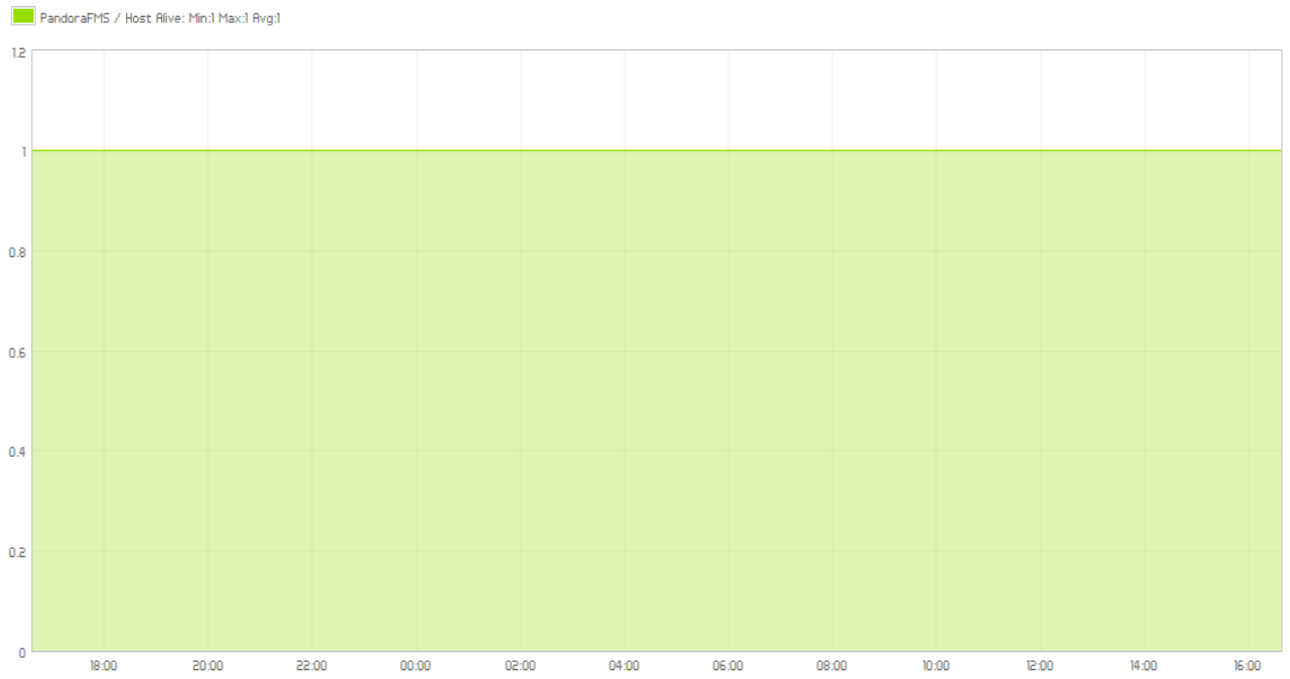


FIGURE 4.17 – Graphe du module Host Alive.

#### 4.4.7.2 Surveillance avec SNMP

Avant d'entamer la supervision des équipements (switchs et routeurs) nous devons d'abord configurer le service SNMP dans chaque équipement. Prenant comme exemple le SW-CORE (voir figure 4.18).

```
SW-CORE(config)#snmp-server community pandora rw ACL
SW-CORE(config)#snmp-server host 192.168.6.130 version 2c pandora
SW-CORE(config)#ip access-list standard ACL
SW-CORE(config-std-nacl)#permit 192.168.6.130
SW-CORE(config-std-nacl)#exit
SW-CORE(config)#
```

FIGURE 4.18 – Commandes de configuration de SNMP.

##### 4.4.7.2.1 Navigateur SNMP de Pandora FMS

Pour récupérer la MIB d'un équipement au niveau de la console Pandora FMS vous devez accéder à l'explorateur SNMP via le menu Surveillance → SNMP → SNMP Navigateur, puis introduire l'adresse IP ainsi que le nom de la communauté puis cliquer sur 'feuilleter' (voir figure 4.19).

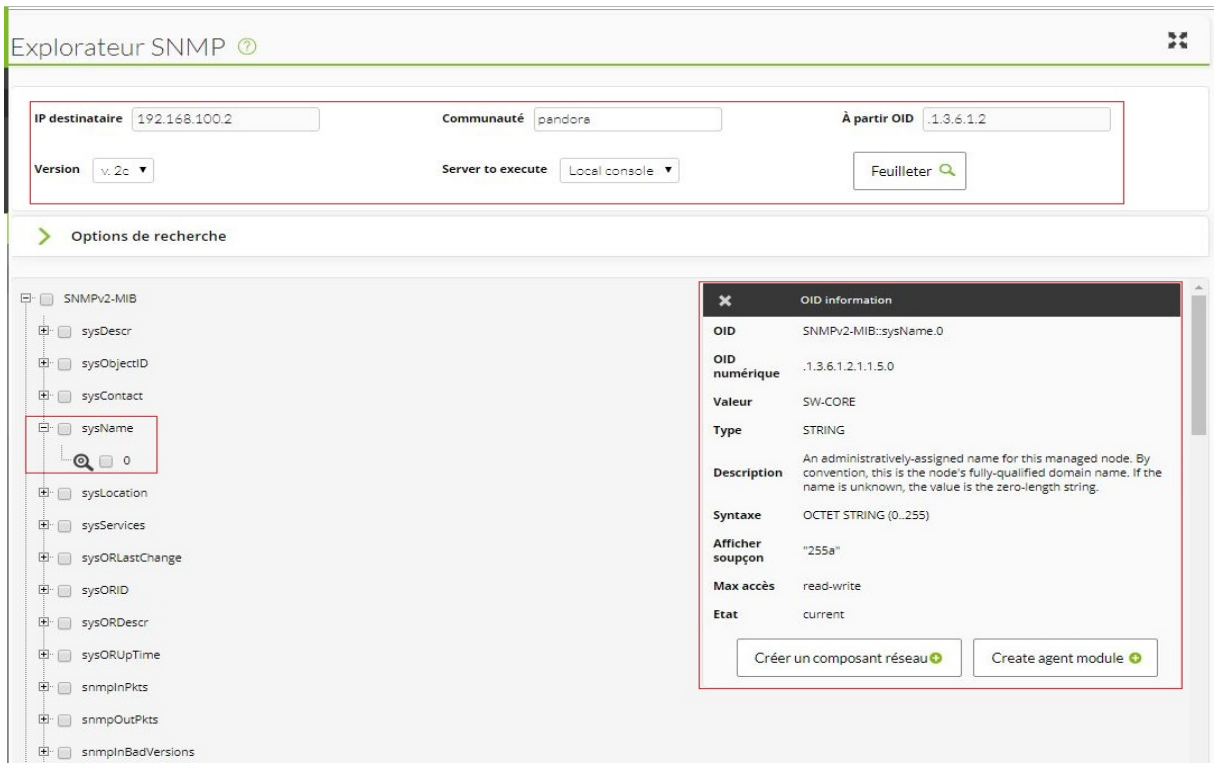


FIGURE 4.19 – Génération de la MIB du SW-CORE.

#### 4.4.7.2.2 Assistant SNMP de pandora FMS

Il existe un Assistant SNMP créé spécialement pour la navigation d'Interface. Ce Wizard navigue par la branche de SNMP IF-MIB : :interfaces, en offrant la possibilité de créer de multiples modules de différentes interfaces avec la sélection multiple.

Une fois l'adresse IP et la communauté introduites, Pandora FMS lance ainsi une découverte des interfaces (voir figure 4.20).

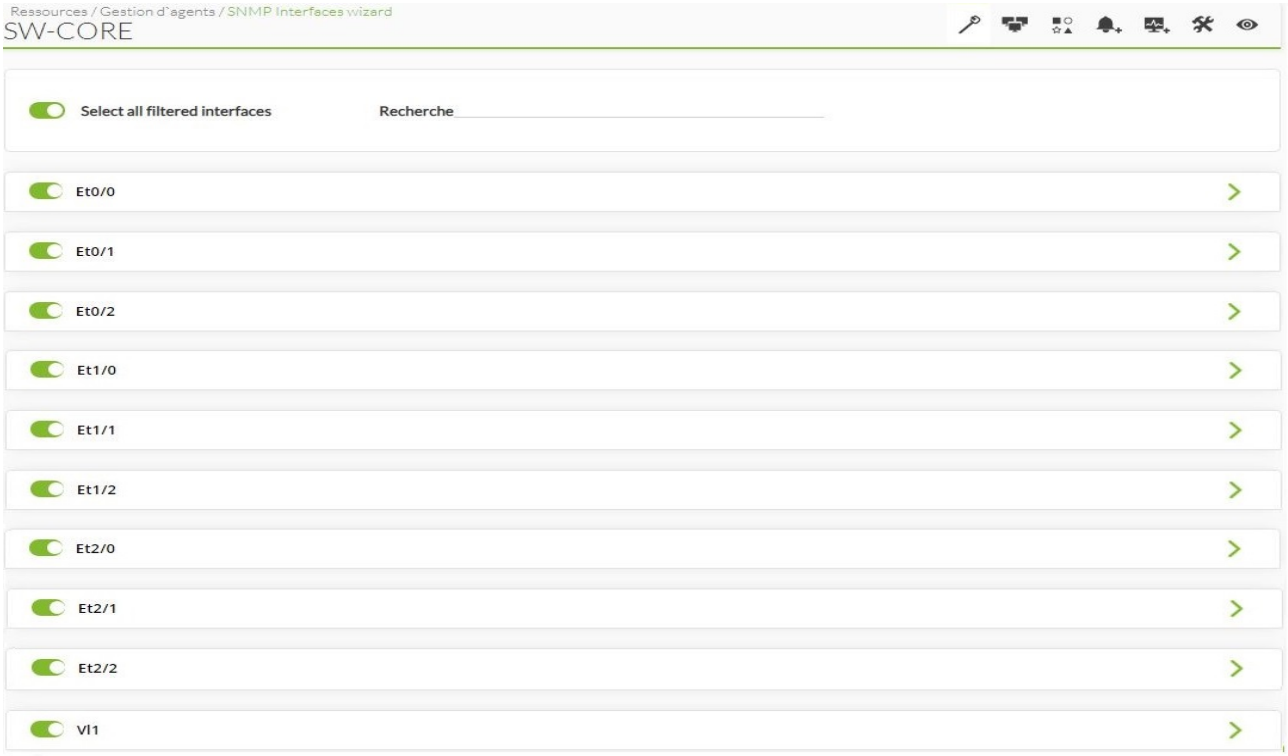


FIGURE 4.20 – Découverte des interfaces du SW-CORE.

#### 4.4.7.2.3 Traps SNMP

Pandora FMS dispose d'une console de réception des traps qui permet de visualiser les traps envoyés par les objets surveillés.

Afin de travailler avec des traps SNMP, vous devez passer par les configurations suivantes :

1. Modifiez tout d'abord le paramètre suivant dans */etc/pandora/pandora_server.conf* pour activer la console SNMP (voir figure 4.21) ;


FIGURE 4.21 – Configuration du fichier pandora_server pour la réception des traps SNMP.

2. Activez-les traps SNMP au niveau de l'équipement à superviser. Dans notre exemple nous avons décidé d'activer le traps SNMP sur le SW-CORE lors de la création ou la suppression d'un VLAN grâce aux commandes indiquées dans la figure 4.22 ;

```
SW-CORE(config)#snmp-server enable trap vlancreate
SW-CORE(config)#snmp-server enable trap vlandelete
SW-CORE(config)#
```

FIGURE 4.22 – Commandes d'activation des traps SNMP.

3. Pour accéder à la console de réception des traps dans pandora FMS, allez sur Surveillance → SNMP → SNMP Console où la liste des traps reçus apparaît (voir figure 4.23).


FIGURE 4.23 – Liste des traps SNMP reçus.

### 4.4.8 Génération des alertes mail

Dans Pandora FMS la façon la plus simple consiste à attribuer une alerte d'avertissement à un module spécifique. Notre première alerte sera tout simplement d'envoyer un mail lorsque l'une des machines est dans un état critique.

Afin de configurer Pandora FMS pour envoyer des alertes via Gmail, nous avons préalablement installé et configuré Postfix (**voir Annexe C**).

La configuration de l'alerte mail sur la console Pandora FMS se fait de la manière suivante :

1. Ouvrir le fichier de configuration du serveur */etc/pandora/pandora_server.conf* et documenter la ligne de configuration indiquée dans la figure 4.24 ;

```
# If not set, the MTA configuration specified in the Pandora FMS Console will be used.
mta_address localhost
```

FIGURE 4.24 – Configuration du fichier pandora_server pour les alertes mails.

Figure 4.24 :

2. Dans le menu latéral allez sur Alertes → Action, ajouter un destinataire d'e-mail auquel toutes les alertes seront envoyées( voir figure 4.25) ;

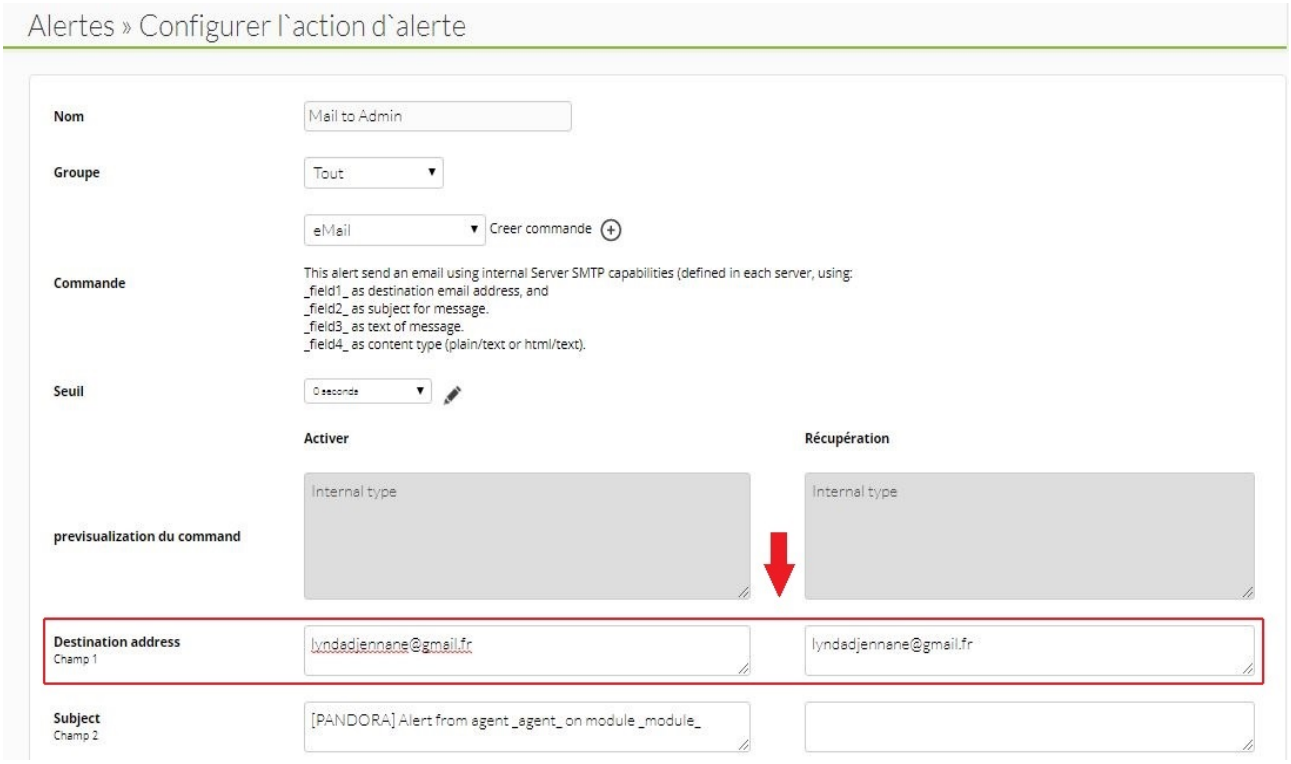


FIGURE 4.25 – Configuration de l'adresse mail.

3. La configuration d'une alerte au niveau du module d'un agent est illustrée dans la figure 4.26) ;

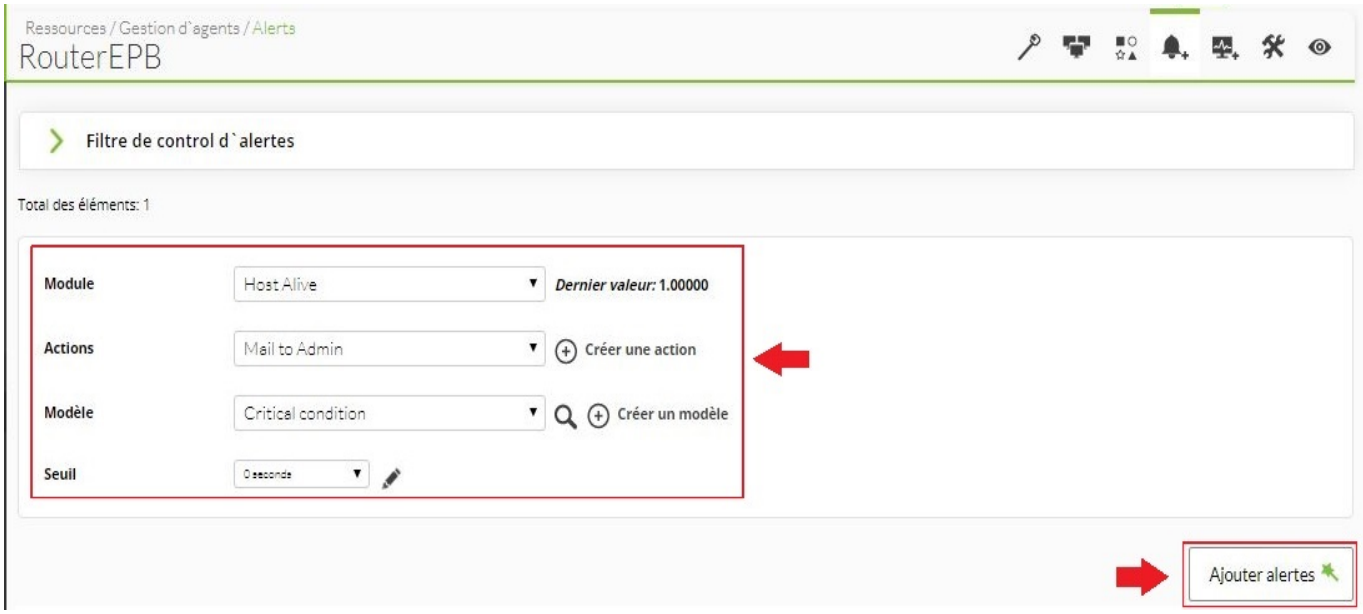


FIGURE 4.26 – Configuration de l'alerte.

4. Une fois l'alerte déclenchée, vous pouvez voir dans la figure 4.27 comment l'alerte atteint l'adresse e-mail attribuée.

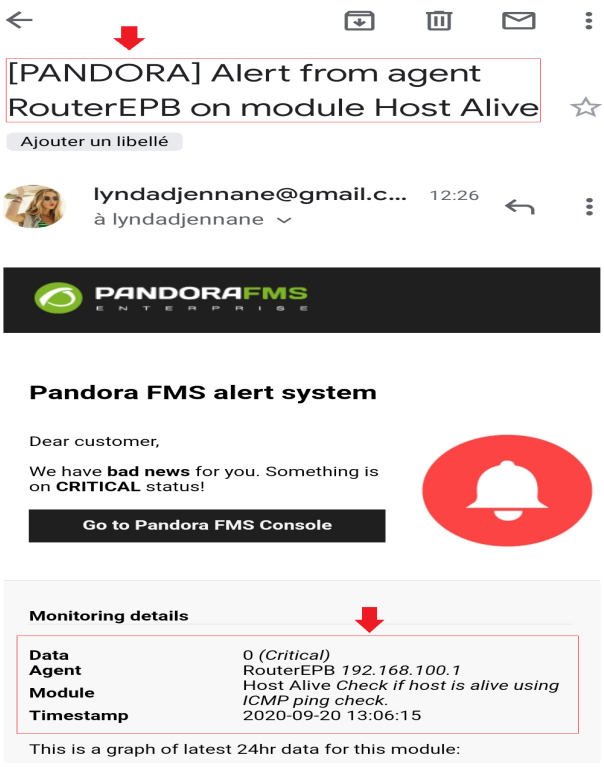


FIGURE 4.27 – Réception de l'alerte.

## 4.5 Conclusion

Dans ce chapitre, nous avons présenté les éléments clés de notre travail. Tout d'abord, nous avons modélisé notre politique de supervision pour mieux comprendre le fonctionnement de notre système. Par la suite, nous avons reproduit le réseau LAN de l'EPB sous GNS3 pour le superviser et enfin, nous avons décrit l'implémentation de certaines fonctionnalités de pandora FMS.

# CONCLUSION GÉNÉRALE ET PERSPECTIVES

L'objectif de notre projet est de mettre en place une solution de supervision informatique au sein de l'EPB permettant d'assurer la continuité opérationnelle de l'entreprise. En effet une solution de supervision permet de diminuer le taux lors de diagnostic des pannes et faciliter les tâches de l'administrateur réseau. Plus le nombre des équipements et des services informatiques augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement ce qui engendre une perte du temps.

Dans le but d'atteindre notre objectif, nous avons été amenés dans un premier lieu à perfectionner nos connaissances dans le domaine de l'administration et de la supervision réseau. Ensuite, nous avons fait une étude approfondie de l'architecture réseau de l'entreprise, nous avons posé la problématique ainsi que les solutions envisagées, par la suite nous avons fait une analyse de différents outils de supervisions, ou nous les avons présentés et déterminés les avantages et inconvénients de chacun et effectuer une comparaison entre ces outils open source, et c'est sur cette base que nous sommes arrivés au choix de la solution la plus complète qui est Pandora FMS. Pour finir, nous avons présenté Pandora FMS en détaillant ces fonctionnalités et en présentant son architecture. Puis nous avons procédé à son installation et sa configuration sur un serveur linux. Avec cette mise en œuvre, nous avons pu avoir un aperçu de l'étendue des possibilités qu'offre Pandora FMS.

La réalisation de ce projet a été bénéfique et fructueuse pour nous dans le sens ou il nous a permis d'une part de mettre en pratique les connaissances acquises durant le cycle de notre formation et d'autre part, de consolider nos connaissances en administration système et réseaux, et de faire une prospection dans le monde de la supervision.

De plus, nous avons eu l'opportunité de travailler dans une entreprise telle que l'EPB, cela nous a permis de manipuler de nouveaux concepts et de prendre conscience de la nécessité d'avoir un système informatique sans interruption.

Comme perspectives de ce travail, nous envisageons de développer nos propres plugins.

# BIBLIOGRAPHIE


[1] Cisco certification ccna1 : Introduction to networks. «chapitre 4 : Accès réseau, section 4.2 : Supports réseau».

[2] Cisco certification ccna1 : Routing and switching essentials. «chapitre 5 : Ethernet, section 5.1 : Protocole ethernet, rubrique 5.1.1 : Trame ethernet, page 5.1.1.3 : Evolution d'ethernet ».

[3] Cisco certification ccna2 : Introduction to networks. «chapitre 4 : Réseau commutés, section 4.1 : Conception d'un réseau local, rubrique 4.1.1 : Réseaux convergents, page 4.1.1.5 : Couches d'accès, de distribution et cœur d'un réseau ».

[4] https://www.paessler.com/, (Consulté le 07 Avril 2020).

[5] https://pandorafms.org/, (Consulté le 12 Juillet 2020).

[6] http://www.nagios.org/, (Consulté le 27 Mars 2020).

[7] http://www.zabbix.com/, (Consulté le 27 Mars 2020).

[8] https://www.whatsupgold.com/, (Consulté le 31 Août 2020).

[9] https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-lan-management-solution/index.html, (Consulté le 31 Août 2020).

[10] ATELIN, P. *Réseaux informatiques : notions fondamentales (normes, architecture, modèle OSI, TCP/IP, Ethernet, Wi-Fi,...)*, 3éme ed. ENI, Paris, 2009.

[11] BOUGUEN, Y., HARDOUIN, E., AND WOLFF, F.-X. *LTE et les réseaux 4G*, 5éme ed. EYROLLES, Paris, 2012.

[12] CABANTOUS, T. *Les réseaux informatiques : informatiques Guide pratique pour l'administration et la supervision.* ENI, Paris, 2019.

[13] CAZES, A., AND DELACROIX, J. *Architecture des machines et des systèmes informatiques : Cours et exercices corrigés*, 3éme ed. DUNOD, Paris, 2003.

[14] DROMARD, D., AND SERET, D. *Architecture des réseaux : Synthèse de cours et exercices corrigés*. Pearson Education France, Paris, 2009.

[15] GABES, J. *Nagios 3 pour la supervision et la métrologie :Déploiement, configuration et optimisation*. EYROLLES, Paris, 2009.

[16] GHERNAOUI, S. *Sécurité informatique et réseaux*, 4éme ed. DUNOD, août 2013.

[17] GHILI, A., AND MEZMAT, Y. *Etude et mise en place d'un outil de monitoring et de supervision des réseaux informatique : cas d'étude SONALGAZE*. Mémoire master, Université de Bejaïa, 2016.

[18] GOUPILLE, P.-A. *Technologie des ordinateurs et des réseaux : Cours et exercices corrigés*, 8éme ed. Dunod, Paris, 2008.

[19] GRELIER, F. *les principales commandes de commutation*. 'edition eni', Dépliant Cisco Certification CCNA.

[20] KOURAT, M., AND MOULAY, S. *Etude et simulation d'un réseau optique passif (PON)*. Mémoire master, Université Dr MOULAY Tahar de Saïda, 2019.

[21] LEMAINQUE, F. *Tout sur les réseaux sans fil*. Dunod, Paris, 2009.

[22] LEMAINQUE, F., AND PILLOU, J.-F. *Tout sur les réseaux et internet*, 4éme ed. Dunod, Paris, 2015.

[23] LOHIER, S., AND PRESENT, D. *Réseaux et transmissions : protocoles, infrastructures et services*, 6éme ed. Dunod, Paris, 2016.

[24] LOIC, F., AND BRUNO, L. *Centreon-maitriser la supervision de votre system informatique*. ENI, 2012.

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

[26] MELLOUK, S. *Etude et dimensionnement d'un réseau WiMAX fixe*. Mémoire master, UNIVERSITE ABOU-BEKR BELKAID TLEMCEN, 2014.

[27] MERAH, H. *Conception d'un MODEM de la quatrième génération (4G) des réseaux de mobiles à base de la technologie MC-CDMA*. Magister, UNIVERSITE FERHAT ABBAS – SETIF, 2012.

[28] MERE, A. La gestion réseau et le protocole snmp. http://kindman.amc-os.com/pub/rapport_fiifo4_snmp.pdf, (Consulté le 26 Mars 2020).

[29] MOUHLI, A. *Sécurité Du Périmètre Réseau : Bases de la sécurité réseau.* Edition Kindle, 2016.

[30] OPPENHEIMER, P. *Top-Down Network Design*, 3rd ed. Cisco Press, Indianapolis(USA), 2010.

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

[32] PUJOLLE, G. *Initiation aux réseaux : Cours et exercices.* Paris, 2001.

[33] PUJOLLE, G. *Les réseaux*, 6éme ed. EYROLLES, Paris, 2008.

[34] PUJOLLE, G. *Les réseaux*, 9éme ed. EYROLLES, Paris, 2018.

[35] SALIOUT, F. *Etude des solutions d'accès optique exploitant une extension de portée. Optique / photonique.* PhD thesis, Télécom ParisTech, 2010.

[36] SERVIN, C. *Réseaux et télécoms : Cours et exercices corrigés.* DUNOD, Paris, 2003.

[37] SERVIN, C. *Réseaux et télécoms*, 4éme ed. DUNOD, Paris, 2013.

[38] THAI, K.-L., ZNATY, S., AND VEQUE, V. *Architecture des réseaux haut débit : Cours, exercices et corrigés.* HERMES, Octobre 1995.

[39] YENDE, R. *Cours d'administration des réseaux informatique(Licence).* Congo-Kinshasa, 2019.

# ANNEXE A

# QUESTIONNAIRE ENTREPRISE EPB

***Partie 1 : Réseau LAN***

1. Disposez-vous d'un réseau local ?

   ☐ Oui

   ☐ Non

   Si OUI, citez les Éléments passifs et actifs.

2. Ce réseau couvre-t-il toute l'entreprise ?

   ☐ Oui

   ☐ Non

3. Quel est le type de votre architecture réseau (plate, hiérarchique...) ?

4. Citez les technologies utilisées (WiMax, Ethernet Wifi...) et pourquoi utilisez-vous cette technologie ?

5. Quel est le débit internet pour l'ADSL et le WiMax ?

6. Disposez-vous d'un réseau téléphonique ?

   ☐ Oui

   ☐ Non

   Si oui couvre-t-il tout le site ?

7. Avez-vous un schéma d'emplacement des prises RJ45 et de tout le câblage ?

   ☐ Oui

   ☐ Non

8. Vos ordinateurs et imprimantes sont-ils en réseau, c'est-à-dire connectés entre eux ?

   ☐ Oui

   ☐ Non

9. Votre entreprise utilise-t-elle les outils informatiques suivants ?

   a) Outils de travail collaboratifs (groupware, vidéoconférence...) ☐ Oui ☐ Non

   b) Outils de modélisation et d'automatisation (Workflow, BPMS...) ☐ Oui ☐ Non

10. Est-ce que vous disposez d'une pointeuse ?

    ☐ Oui

    ☐ Non

11. Avez-vous une connexion internet ?

    ☐ Oui

    ☐ Non

12. La connexion internet est-elle stable ?

    ☐ Oui

    ☐ Non

13. Disposez-vous des outils qui puissent tracer la stabilité d'internet ?

    ☐ Oui

☐ Non

Si oui, préciser lesquels.

14. Quels sont les fournisseurs d'accès à internet ?

15. Tous les ordinateurs de votre entreprise ont-ils accès à internet ?

☐ Oui

☐ Non

16. Est-ce que chaque service possède un point d'accès Wifi ?

☐ Oui

☐ Non

17. Avez-vous un contrôleur Wifi ?

☐ Oui

☐ Non

18. Votre entreprise dispose-t-elle d'un Intranet et/ou d'un extranet ?

☐ Oui

☐ Non

19. Citez les systèmes d'exploitation que vous utilisez (indiquer le nombre de postes par système d'exploitation).

20. Citez les ressources logicielles (applications) que vous exploitez.

21. Votre entreprise utilise-t-elle des solutions de virtualisation ?

## ***Partie 2 : Supervision***

1. Disposez-vous d'une solution de supervision réseau ?

   ☐ Oui

   ☐ Non

   Si oui, indiquez lequel et quels sont les équipements et les services manageables.

2. Avez-vous réalisé une étude comparative des diverses solutions de supervision ?

   ☐ Oui

   ☐ Non

## ***Partie 3 : Sécurité***

1. Où sont enregistrées vos données informatiques (courriers, devis, plans, ...) ?

   ☐ Sur chaque ordinateur

   ☐ Centralisées sur un ordinateur, un serveur

   ☐ Centralisées sur des disques NAS (disques de stockage)

   Autre, précisez.

2. Si vous effectuez des sauvegardes, à quelle fréquence ?

   ☐ Tous les jours

   ☐ Toutes les semaines

   ☐ Tous les mois

   ☐ De temps en temps

3. Quels sont les informations, services, équipements, etc. cruciaux qui sont dans l'existant et qui nécessitent une politique de sécurité ?

4. Citez les équipements, logiciels, méthodes et autres que vous exploitez dans votre politique de sécurité.

5. Avez-vous une solution antivirus installée sur chaque ordinateur ?

   ☐ Oui

   ☐ Non

   Si oui, quel est le type de l'antivirus que vous utilisez ?

6. Le réseau informatique dispose-t-il d'un équipement capable de filtrer les URL visitées (proxy ou firewall) ?

   ☐ Oui

   ☐ Non

   Si oui, quel est le type du par feu utilisé ?

7. Disposez-vous d'un VPN ?

   ☐ Oui

   ☐ Non

   Si oui, quel est le type de liaison et de cryptage VPN que vous utilisez ? Pourquoi ?

8. Avez-vous un serveur d'authentification Radius ?

   ☐ Oui

   ☐ Non

9. Disposez-vous des outils journalisation ?

   ☐ Oui

   ☐ Non

   Si oui, préciser lesquels ?

10. Quel degré d'importance attachez-vous à la sécurité informatique dans votre entreprise (Virus, pertes de données, vols, ...) ?

    ☐ Très importante

    ☐ Importante

    ☐ Peu importante

***Partie 4 : Autres informations***

1. Votre entreprise dispose-t-elle d'un site Web ?

   ☐ Oui

   ☐ Non

   Si OUI, précisez l'adresse de ce site, ainsi que les services proposés.

2. Disposez-vous d'autres structures dans la wilaya de Bejaia ou dans d'autres wilayas ?

   ☐ Oui

   ☐ Non

   Si oui, à quelle distance sont-elles implantées par rapport au port principal, et sont-elles reliées par une liaison (paire torsadée, fibre optique. . . ) ?

3. Les deux sites (Texter et IOB) ont-ils accès à internet, si oui quels sont les technologies utilisées (ADSL, WiMax, Fibre optique...) ?

4. Les deux ports secs (Texter et IOB) sont -il indépendant sous le plan informatique (utilisent-ils leurs propres logiciels métiers et serveurs) ?

5. Les utilisateurs doivent-ils demander d'autorisation avant d'installer des logiciels sur leurs ordinateurs ?

   ☐ Oui

   ☐ Non

6. Votre entreprise a-t-elle utilisé un progiciel de gestion intégré (PGI ou ERP) pour partager l'information entre les différents pôles de l'entreprise (comptabilité, finance, planning, production, marketing. . . ) ?

   ☐ Oui

   ☐ Non

7. Y a-t-il dans l'entreprise des personnes travaillant régulièrement en dehors des locaux de l'entreprise qui ont accès à distance au système informatique de l'entreprise par des réseaux électroniques (télétravail) ?

   ☐ Oui

   ☐ Non

8. Quel est le degré de dépendance de votre entreprise vis-à-vis de l'informatique ?

9. Aujourd'hui, pensez-vous être suffisamment protégé contre tous les risques liés à l'informatique et à Internet ?

   ☐ Oui, bien protégé

☐ Oui, suffisamment

☐ Non

☐ Ne sais pas

# ANNEXE B

# CONFIGURATION SOUS GNS3

GNS3 est un logiciel libre et disponible pour Windows, Linux et MacOS X, il permet de reproduire une architecture physique ou logique.

## B.1 Configuration des équipements

1. Configurez les noms des équipements, comme illustré dans la figure B.1 ;

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterEPB
RouterEPB(config)#
```

FIGURE B.1 – Commande de configuration du nom d'un équipement (RouterEPB).

2. Configurez le Mot de passe pour le mode privilégié, la ligne console et virtuelle (Telnet et SSH) pour chaque équipement, comme illustré dans la figure B.2 ;

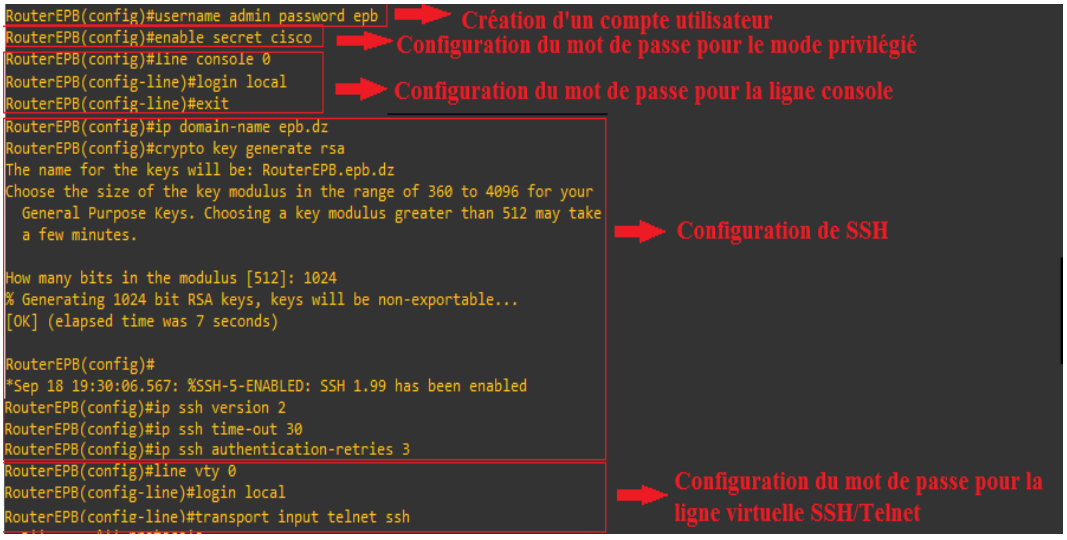


FIGURE B.2 – Commandes de configuration des différents mots de passe.

3. Configurez la bannière de connexion pour chaque équipement, comme illustré dans la figure B.3 ;


FIGURE B.3 – Commande de configuration de la bannière de connexion.

4. Créez des VLANs sur le SW-CORE comme illustré dans la figure B.4 ;

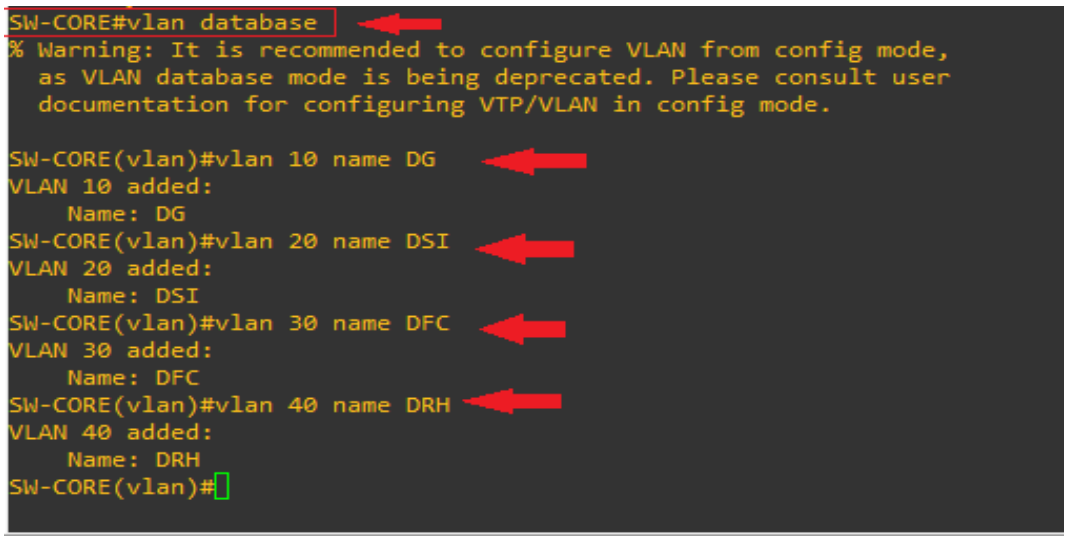


FIGURE B.4 – Commande de création des VLANs sur le SW-CORE.

Utilisez la commande 'show vlan' pour afficher la liste des VLANs crées, comme illustré dans la figure B.5 ;

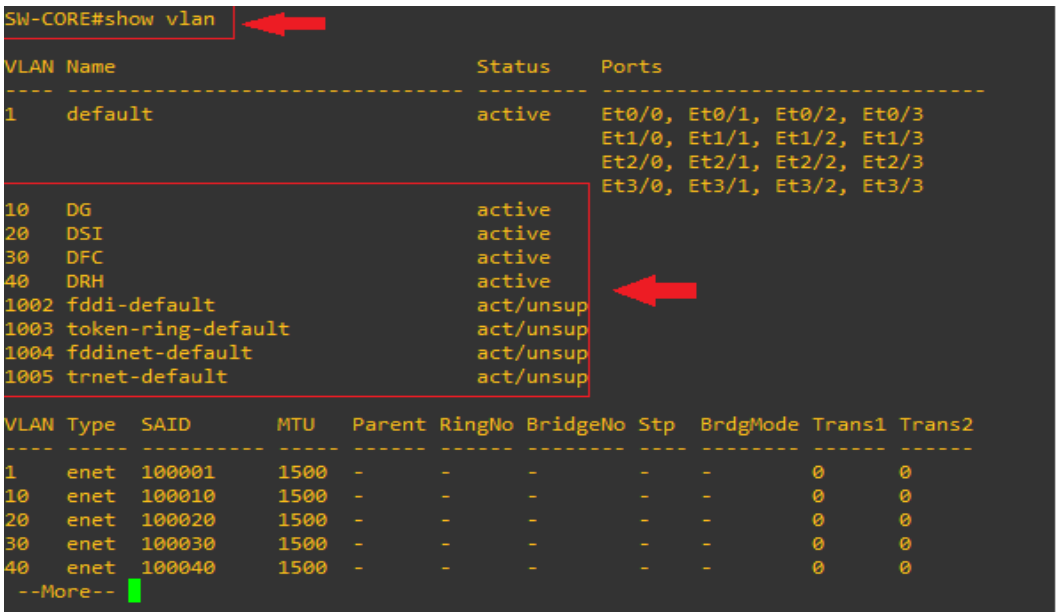


FIGURE B.5 – Commande d'affichage des VLANs crées.

5. Configurez le SW-CORE en mode vtp server (voir figure B.6) et les autres switchs en mode vtp client (voir figure B.7) et afficher sa configuration avec la commande 'show vtp status' comme illustré dans la figure B.8 ;

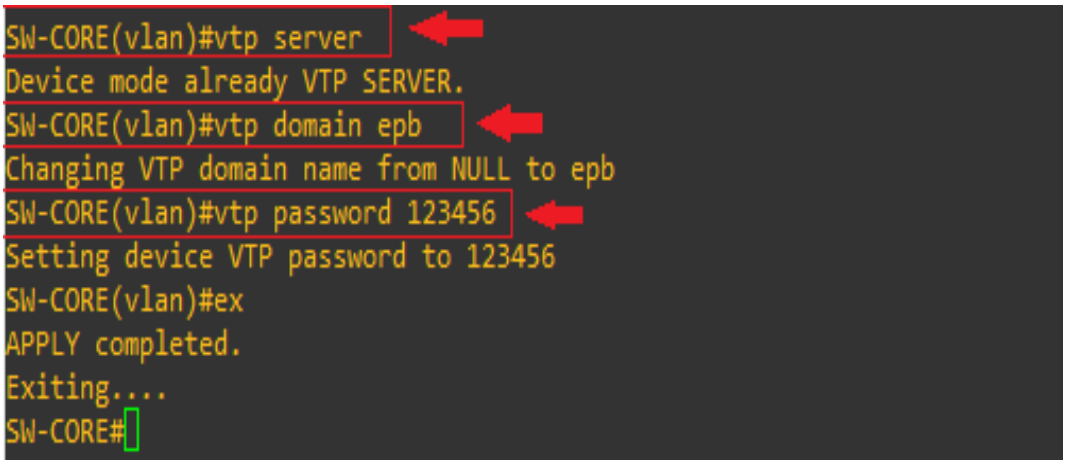


FIGURE B.6 – Commandes de configuration du switch en mode vtp server.

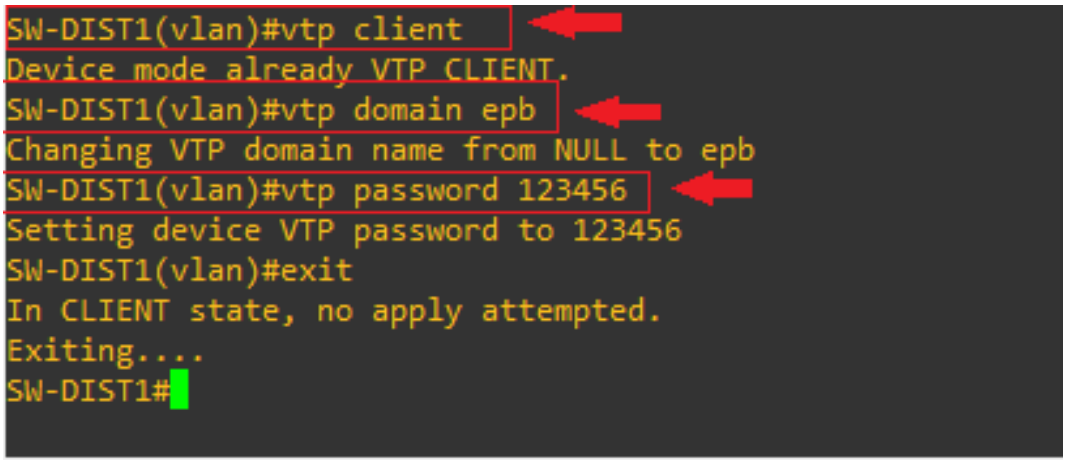


FIGURE B.7 – Commandes de configuration du switch en mode vtp client.


FIGURE B.8 – Commande d'affichage de la configuration vtp sur le SW-CORE.

6. Configurez les interfaces en mode trunk entre des commutateurs ou entre un commutateur et un routeur, comme illustré dans la figure B.9 ;

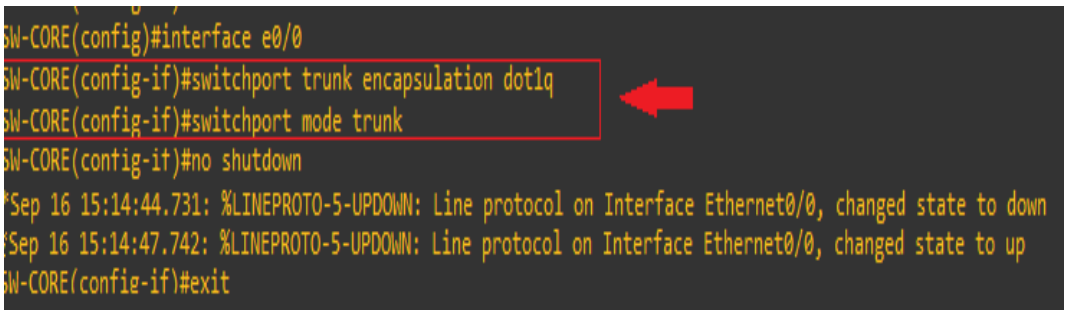


FIGURE B.9 – Commandes de configuration d'une interface en mode trunk (SW-CORE).

7. Configurez les interfaces en mode access entre un commutateur et un poste client, comme illustré dans la figure B.10 ;

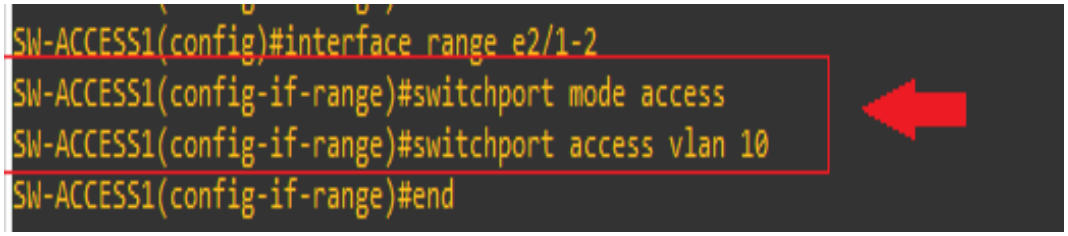


FIGURE B.10 – Commandes de configuration d'une interface en mode access (SW-ACCESS1).

8. Configurez le protocole STP sur le SW-CORE en lui attribuant la plus grande priorité (voir figure B.11), et sur les autres switchs comme SW-DIST2 en lui attribuant la priorité 0 (voir figure B.12) ;

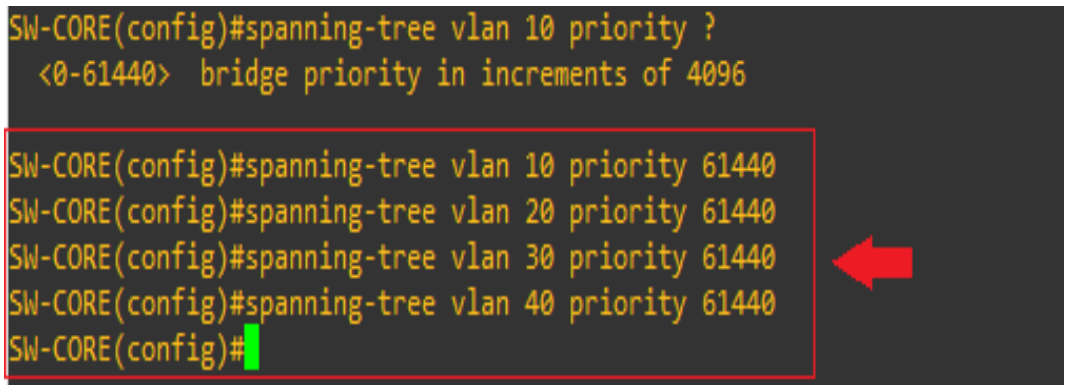


FIGURE B.11 – Commandes de configuration de STP sur le SW-CORE.

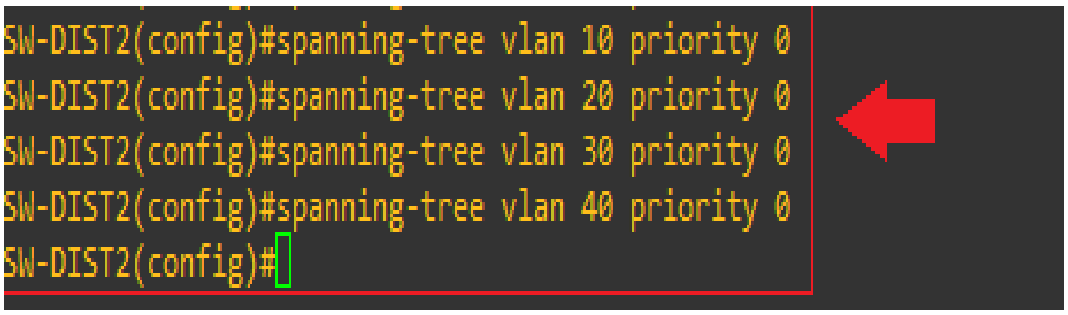


FIGURE B.12 – Commandes de configuration de STP sur le SW-DIST2.

9. Configurez les interfaces du routeur (voir figure B.13) ainsi que l'interface vlan 1 sur les switchs (voir figure B.14) pour les administrer à distance ;

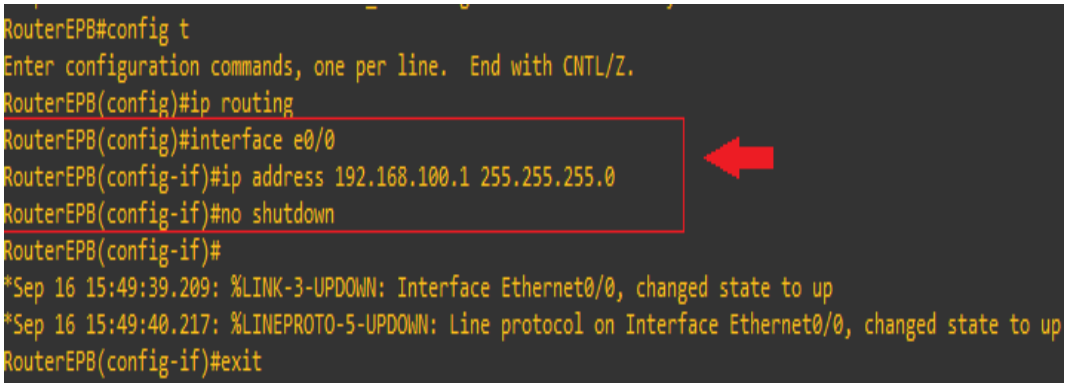


FIGURE B.13 – Commandes de configuration de l'interface du RouterEPB.

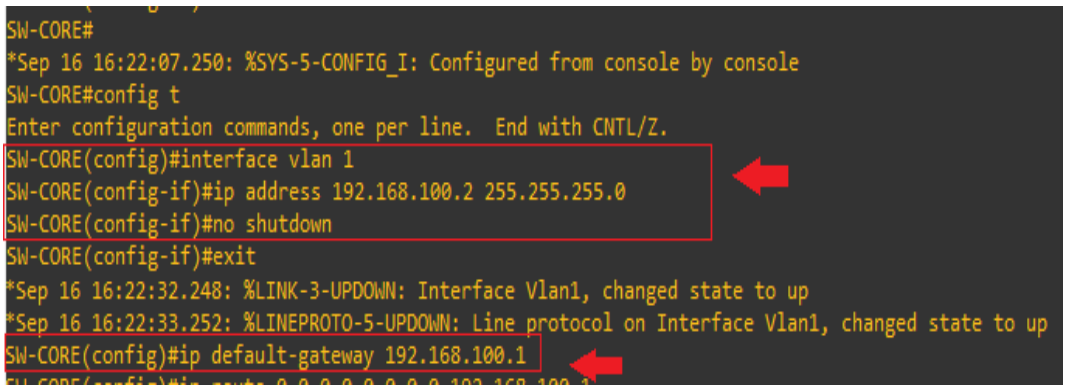


FIGURE B.14 – Commandes de configuration de l'interface vlan 1 sur SW-CORE.

10. . Configurez le routage inter-vlan sur le RouterEPB, comme illustré dans la figure B.15 ;

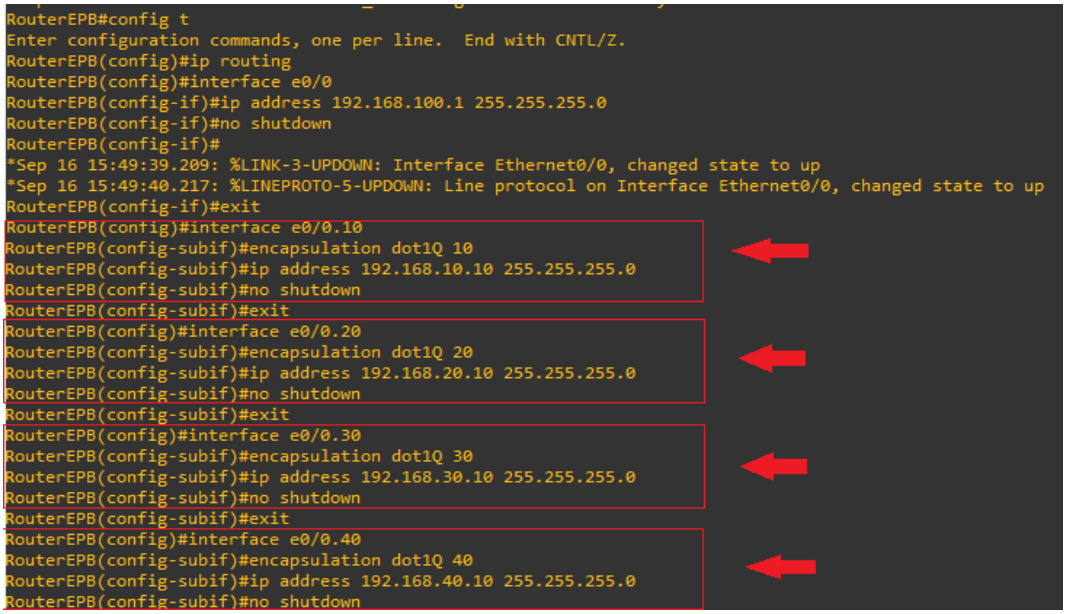


FIGURE B.15 – Commandes de configuration du routage inter-vlan.

11. Configurez le DHCP sur le RouterEPB (voir figure B.16) pour attribuer les adresses IP dynamiquement sur les postes client et tester la connectivité entre les différents équipements (voir figure B.17) ;

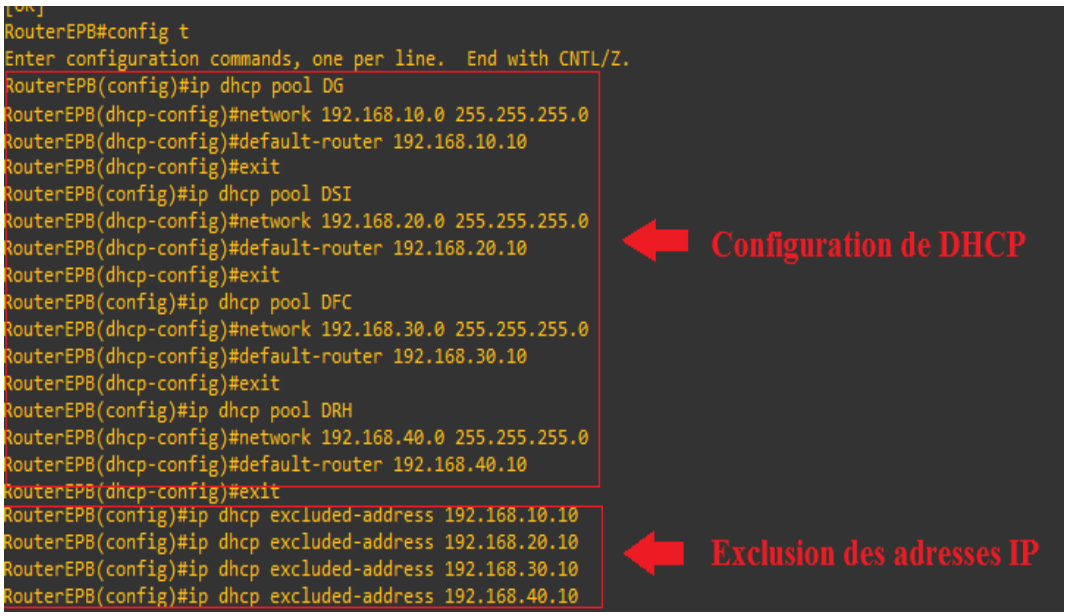


FIGURE B.16 – Commandes de configuration du service DHCP.

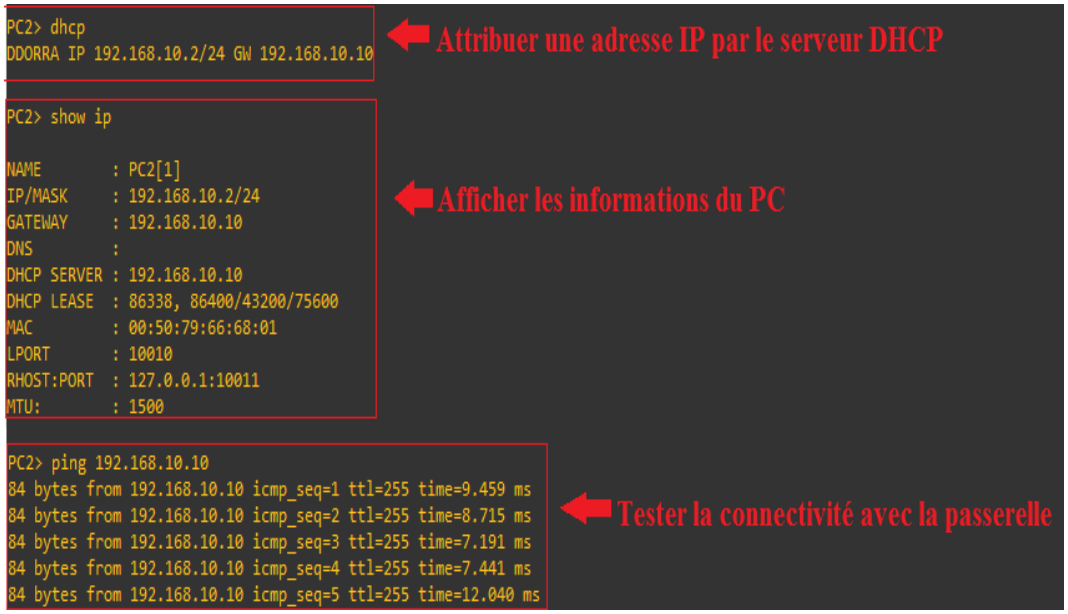


FIGURE B.17 – Vérification de la connectivité.

# ANNEXE C

# INSTALLATION ET CONFIGURATION DE PANDORA FMS

Afin de bien maitriser notre outil de supervision, nous avons effectué l'installation et la configuration de Pandora FMS avec deux façons : sous Ubuntu et sous CentOS.

## C.1 Sous Ubuntu

### C.1.1 Installation de Pandora FMS

**Étape 1 : Installation des dépendances et des packages requis**

1. Mettez à jour le cache de votre package APT comme illustré dans la figure C.1 ;


FIGURE C.1 – Commande de mise jour du paquet APT.

2. Installez toutes les dépendances requises pour le serveur Pandora qui comprend un certain nombre de modules Perl, le serveur HTTP Apache, PHP et ses modules, et le serveur de base de données MariaDB comme illustré dans la figure C.2 ;

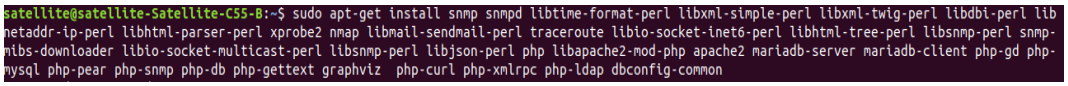


FIGURE C.2 – Commande d'installation des dépendances et des packages requis.

3. Une fois l'installation terminée, vérifiez si le service Apache2 est opérationnel (figure C.3). Vérifiez également s'il est activé (figure C.4) ;

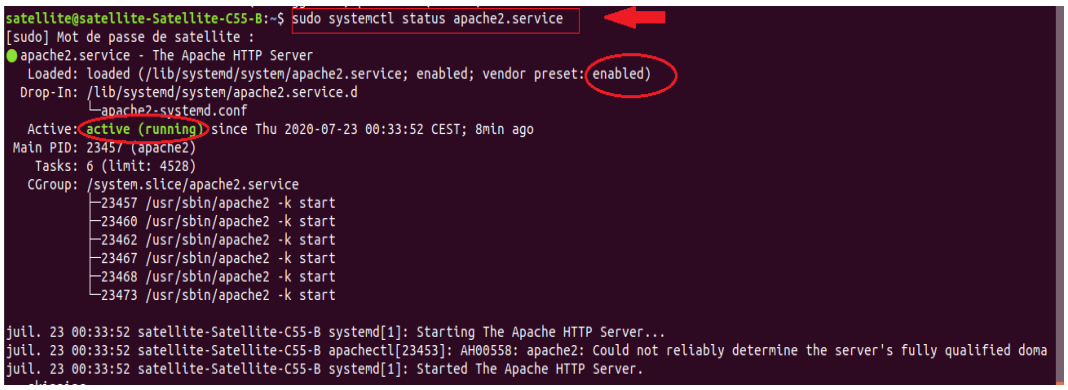


FIGURE C.3 – Commande de vérification si Apache2 est opérationnel.

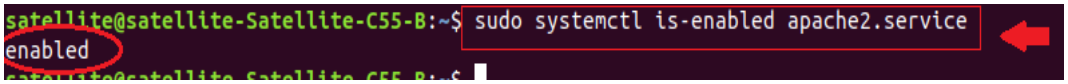


FIGURE C.4 – Commande de vérification si Apache2 est activé.

4. Vérifiez également si le service MariaDB est opérationnel et activé comme illustré dans la figure C.5 ;

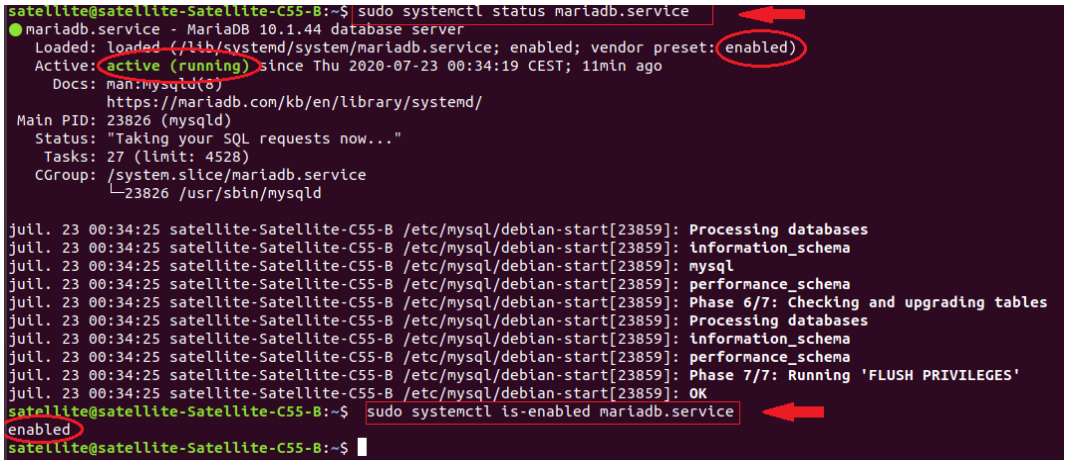


FIGURE C.5 – Commandes de vérification si MariaDB est opérationnel et activé.

5. Créez un mot de passe pour l'utilisateur root de la base de données MariaDB comme illustré dans la figure C.6 ;

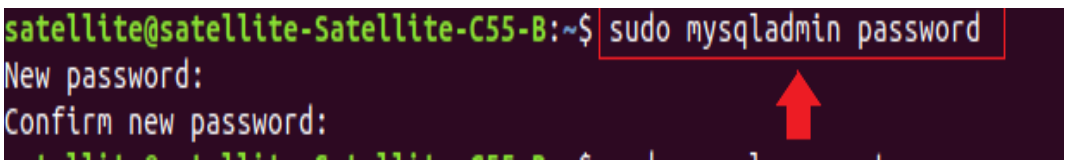


FIGURE C.6 – Commande de création d'un mot de passe pour la base de données MariaDB.

6. Par défaut sur Ubuntu, MySQL/MariaDB est configuré pour utiliser le plugin UNIX *auth_socket*. Cela empêche le script d'installation de la console de s'exécuter correc-

tement, en particulier au moment de la création de la base de données Pandora par l'utilisateur root. Vous devez donc mettre à jour le plugin d'authentification pour que l'utilisateur root utilise '*mysql_native_password*' comme illustré dans la figure C.7 ;

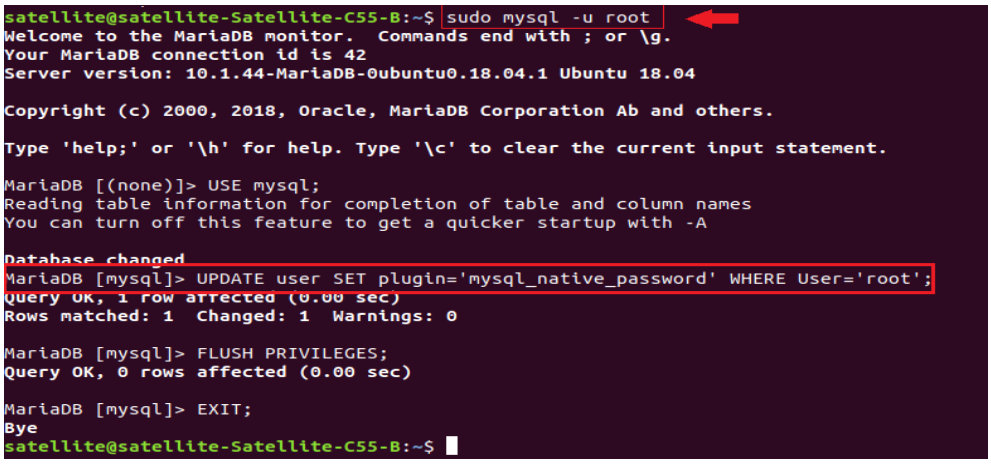


FIGURE C.7 – Commande de configuration de la base de données MariaDB.

7. Améliorez la sécurité de votre serveur MariaDB en exécutant le script shell '*mysql_secure_installation*' comme illustré dans la figure C.8 ;

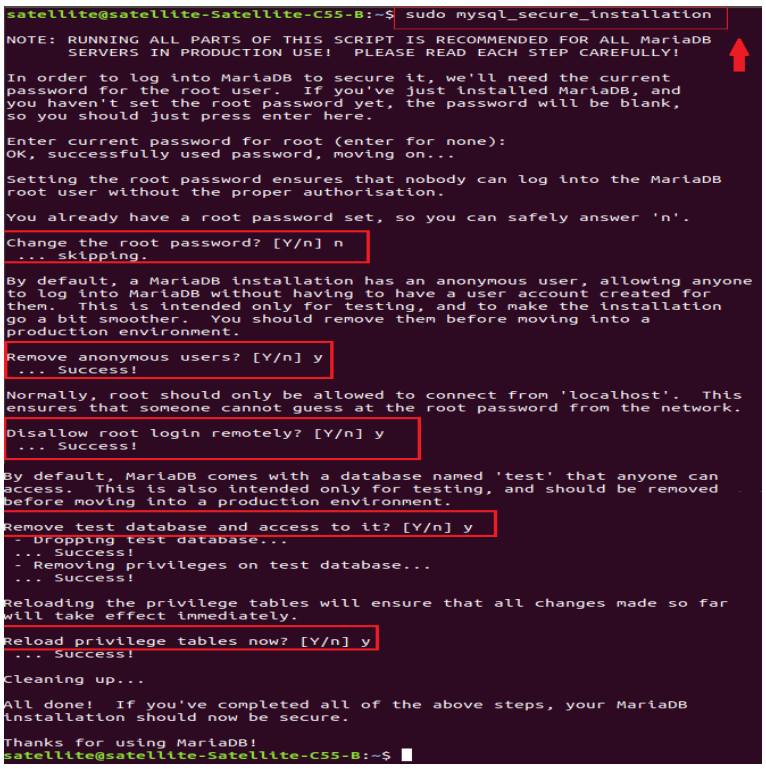


FIGURE C.8 – Commande d'amélioration de la sécurité du serveur MariaDB.

8. Une autre dépendance requise est le client WMI qui ne se trouve pas dans les référentiels Ubuntu. Vous devez le télécharger et l'installer à partir du référentiel Pandora sur SourceForge comme illustré dans la figure C.9.

```
satellite@satellite-Satellite-C55-B:~$ wget https://sourceforge.net/projects/pandora/files/Tools%20and%20dependencies%20%28All%20versions%29/DEB%20Debian%2C%20Ubuntu/wmi-client 0112-1 amd64.deb
satellite@satellite-Satellite-C55-B:~$ sudo dpkg -i wmi-client_0112-1_amd64.deb
```

FIGURE C.9 – Commandes d'installation du client WMI.

**Étape 2 : Installation du serveur et de la console Pandora FMS**

1. Téléchargez maintenant les packages DEB du serveur et de la console Pandora FMS comme illustré dans la figure C.10 ;

```
satellite@satellite-Satellite-C55-B:~$ wget https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/743/Debian_Ubuntu/pandorafms.console_7.0NG.743.deb
satellite@satellite-Satellite-C55-B:~$  wget https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/743/Debian_Ubuntu/pandorafms.server_7.0NG.743.deb
```

FIGURE C.10 – Commandes de téléchargement des packages DEB du serveur et de la console Pandora FMS.

2. Une fois que vous avez téléchargé les deux fichiers, installez-les à l'aide de la commande 'dpkg'. L'installation devrait échouer en raison de problèmes de dépendance, comme le montre la figure C.11. Pour résoudre les problèmes, passez à l'étape suivante ;

```
satellite@satellite-Satellite-C55-B:~$ sudo dpkg -i pandorafms.console_7.0NG.743.deb pandorafms.server_7.0NG.743.deb
Sélection du paquet pandorafms-console précédemment désélectionné.
(Lecture de la base de données... 140687 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de pandorafms.console_7.0NG.743.deb ...
Dépaquetage de pandorafms-console (7.0NG.743) ...
Sélection du paquet pandorafms-server précédemment désélectionné.
Préparation du dépaquetage de pandorafms.server_7.0NG.743.deb ...
Dépaquetage de pandorafms-server (7.0NG.743) ...
dpkg: des problèmes de dépendances empêchent la configuration de pandorafms-console :
 pandorafms-console dépend de php7.2-zip | php-zip ; cependant :
  Le paquet php7.2-zip n'est pas installé.
  Le paquet php-zip n'est pas installé.

dpkg: erreur de traitement du paquet pandorafms-console (--install) :
 problèmes de dépendances - laissé non configuré
dpkg: des problèmes de dépendances empêchent la configuration de pandorafms-server :
 pandorafms-server dépend de libnet-telnet-perl ; cependant :
  Le paquet libnet-telnet-perl n'est pas installé.
 pandorafms-server dépend de libgeo-ip-perl ; cependant :
  Le paquet libgeo-ip-perl n'est pas installé.

dpkg: erreur de traitement du paquet pandorafms-server (--install) :
 problèmes de dépendances - laissé non configuré
Traitement des actions différées (« triggers ») pour ureadahead (0.100.0-20) ...
Traitement des actions différées (« triggers ») pour systemd (237-3ubuntu10) ...
Traitement des actions différées (« triggers ») pour man-db (2.8.3-2) ...
Des erreurs ont été rencontrées pendant l'exécution :
 pandorafms-console
 pandorafms-server
satellite@satellite-Satellite-C55-B:~$
```

FIGURE C.11 – Commande d'installation du serveur et de la console Pandora FMS.

3. Exécutez la commande suivante pour résoudre automatiquement les problèmes de dépendance de l'étape précédente comme illustrés dans la figure C.12 ;

```
satellite@satellite-Satellite-C55-B:~$ sudo apt-get -f install
```

FIGURE C.12 – Commande de résolution de dépendance.

4. Une fois les packages installés, le programme d'installation redémarrera le service Apache2 et démarrera le moteur Pandora FMS Websocket comme illustré dans la figure C.13 ;

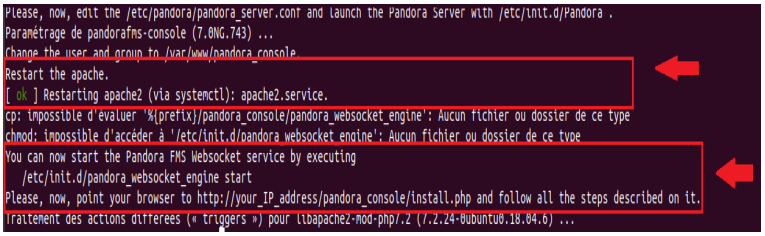


FIGURE C.13 – Résultat de la commande de résolution de dépendance.

5. La console Pandora est installée dans le chemin */var/www/html/pandora_console/*. Vous pouvez utiliser la commande 'ls' pour afficher le contenu du répertoire comme illustré dans la figure C.14 ;


FIGURE C.14 – Commande pour afficher le contenu du répertoire de la console Pandora FMS.

6. Si le service de pare-feu UFW est activé et en cours d'exécution, émettez les commandes illustrées dans la figure C.15 pour autoriser les requêtes HTTP et HTTPS via le pare-feu vers le serveur HTTP Apache2 avant d'accéder à la console Pandora.

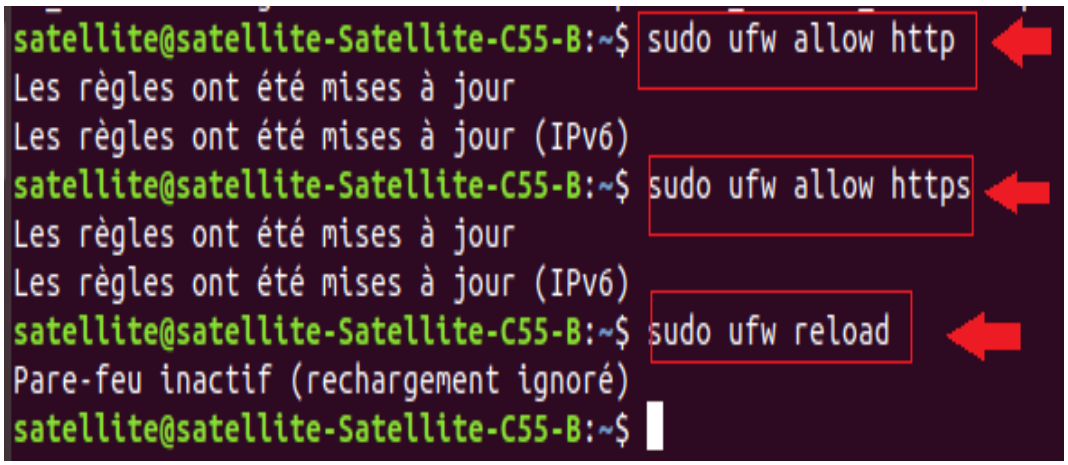


FIGURE C.15 – Commandes d'autorisation des requêtes via le pare-feu.

**Étape 3 : Terminer l'installation de Pandora FMS via l'assistant web**

1. Vous devez maintenant terminer l'installation de la console Pandora à partir d'un navigateur Web. Pointez votre navigateur vers l'adresse suivante comme le montre la figure C.16 pour accéder à l'assistant d'installation de la console. Vous devez d'abord exécuter la commande 'ifconfig' afin récupérer votre adresse IP ;


FIGURE C.16 – Lien de navigateur vers la console Pandora FMS.

2. Cliquez sur le bouton 'Yes, i accept licence terms' pour accepter les termes de la licence et poursuivre l'installation comme illustrée dans la figure C.17 ;

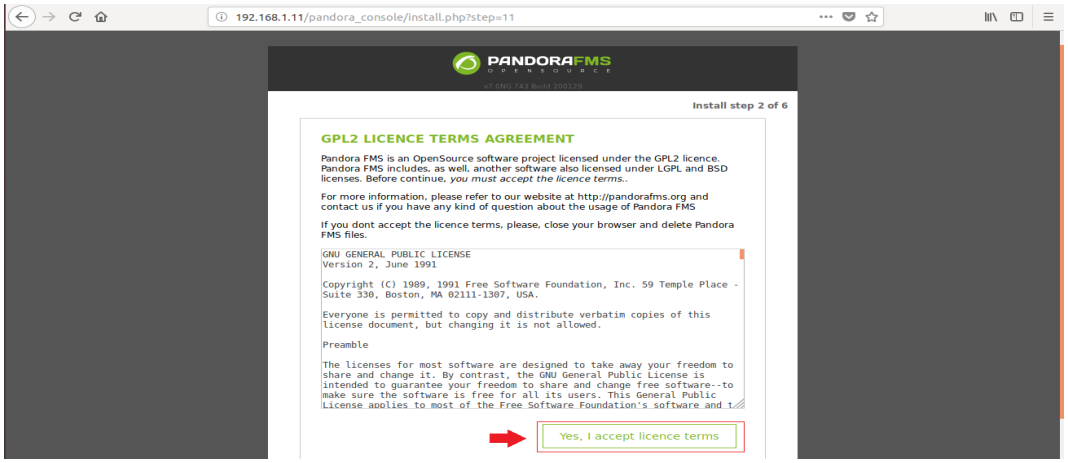


FIGURE C.17 – Acceptation de l'agrément pour l'installation de Pandora FMS.

3. L'installateur vérifiera les dépendances logicielles. Si tout va bien, vous pouvez cliquer sur le bouton 'Next' sinon vous devez installer les manques (voir figure C.18) ;

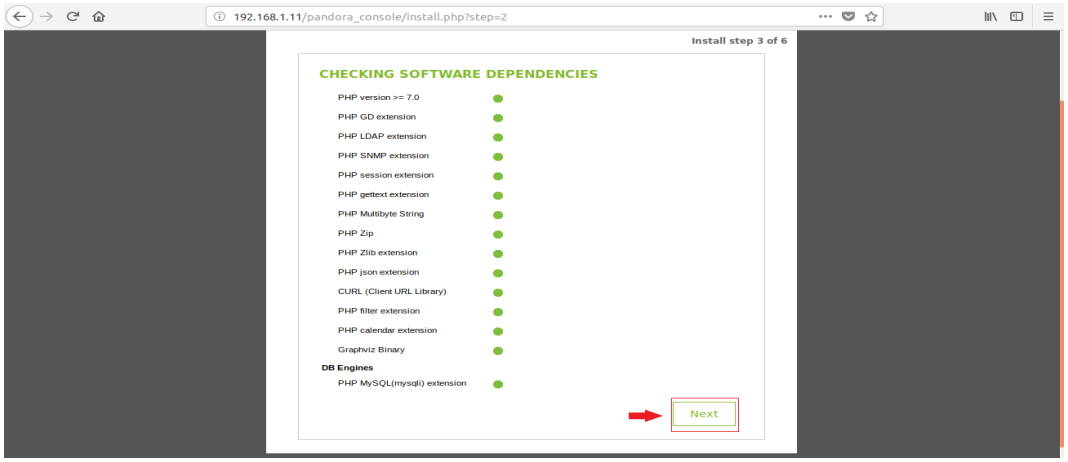


FIGURE C.18 – Dépendances logicielles de Pandora FMS.

4. Introduisez maintenant le mot de passe de l'utilisateur racine de la base de données MariaDB pour créer la base de données Pandora puis cliquez sur le bouton 'Next' comme illustré dans la figure C.19 ;

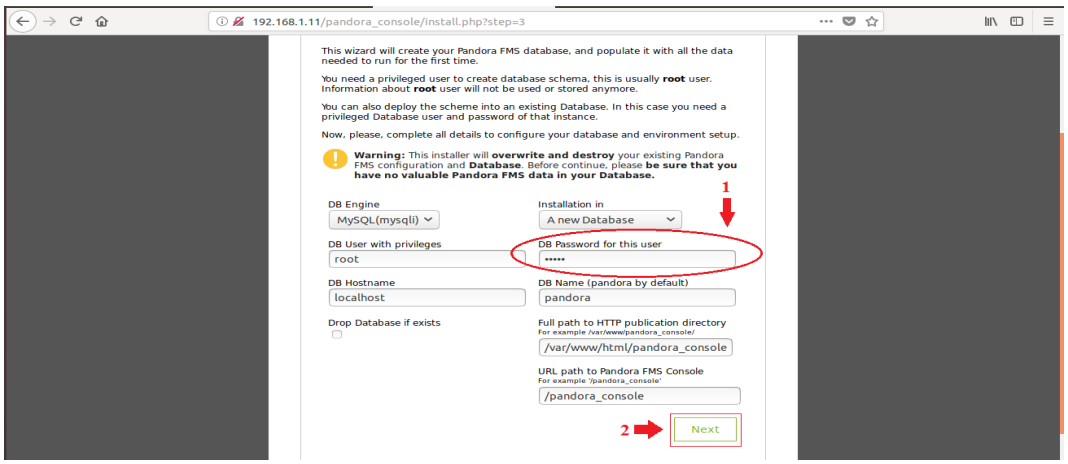


FIGURE C.19 – Configuration de la base de données Pandora FMS.

5. Ensuite, le programme d'installation créera la base de données Pandora et un utilisateur MySQL pour y accéder, et créera un mot de passe aléatoire pour l'utilisateur MySQL, prenez-en note (le mot de passe), vous devez le définir dans la configuration du serveur Pandora. En outre, il créera un nouveau fichier de configuration situé dans */var/www/html/pandora_console/include/config.php*. Cliquez sur le bouton 'Next ' pour terminer le processus d'installation comme illustré dans la figure C.20 ;

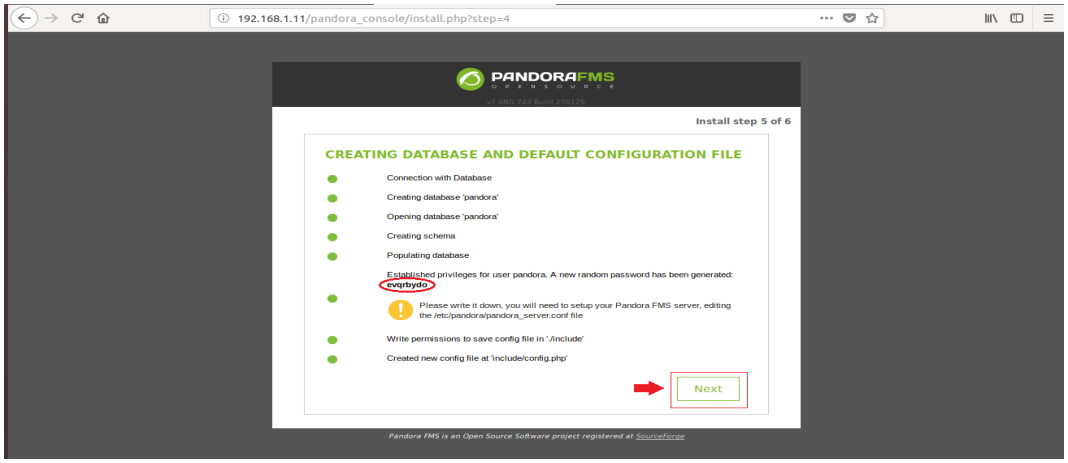


FIGURE C.20 – Création de la base de données Pandora FMS.

6. Lorsque l'installation est terminée, renommez le script d'installation en cliquant sur « Yes, rename the file » comme illustré dans la figure C.21 ;

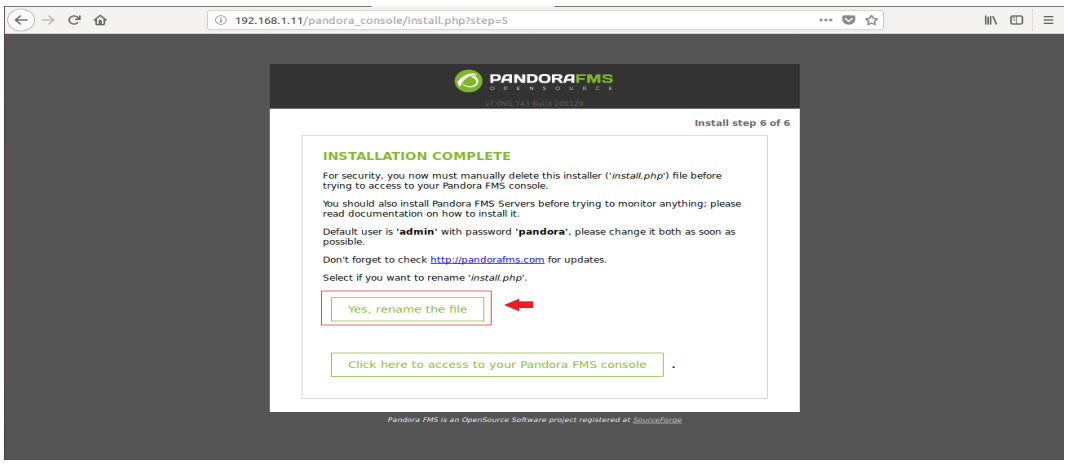


FIGURE C.21 – Installation complète de Pandora FMS.

7. Sur la page de connexion, utilisez les informations de connexion par défaut pour vous connecter (user = admin, Password = pandora) comme illustré dans la figure C.22. Une fois authentifiée vous pouvez sécuriser le compte de l'administrateur de la console Pandora, remplacez le mot de passe par défaut par un mot de passe fort et sécurisé ;

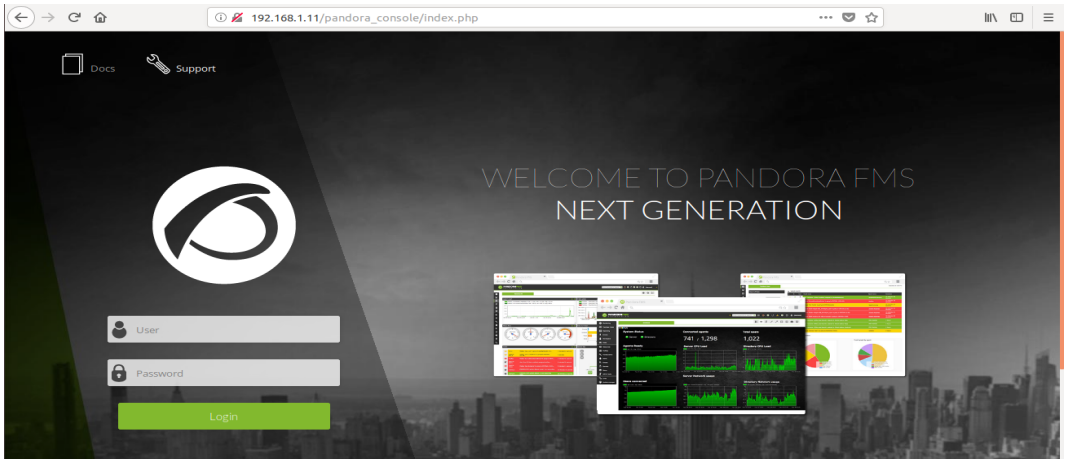


FIGURE C.22 – Page de connexion de Pandora FMS.

8. La figure C.23 montre la page d'accueil de Pandora FMS.

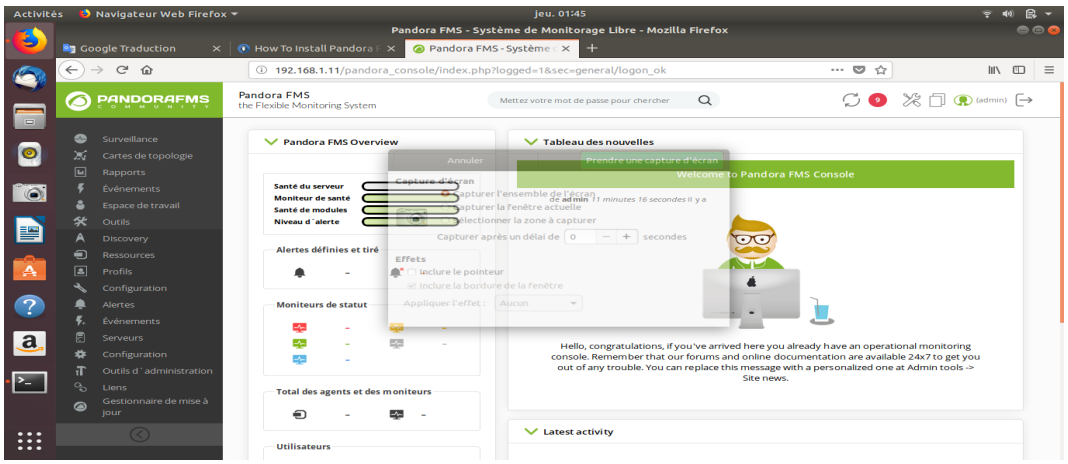


FIGURE C.23 – Page d'accueil de Pandora FMS sur Ubuntu.

### C.1.2 Configuration de Pandora FMS

1. Pour démarrer la surveillance, vous devez configurer le serveur Pandora FMS. Ouvrez le fichier nommé « */etc/pandora/pandora_server.conf* » (figure C.24) et modifiez-le ;

```
satellite@satellite-Satellite-C55-B:~$ sudo gedit /etc/pandora/pandora_server.conf
```

FIGURE C.24 – Commande pour éditer le fichier Pandora serveur.

2. Recherchez le paramètre 'dbpass' et définissez le mot de passe utilisateur MySQL généré précédemment lors de l'étape d'installation via l'assistant Web puis enregistrez le fichier comme illustré dans la figure C.25 ;

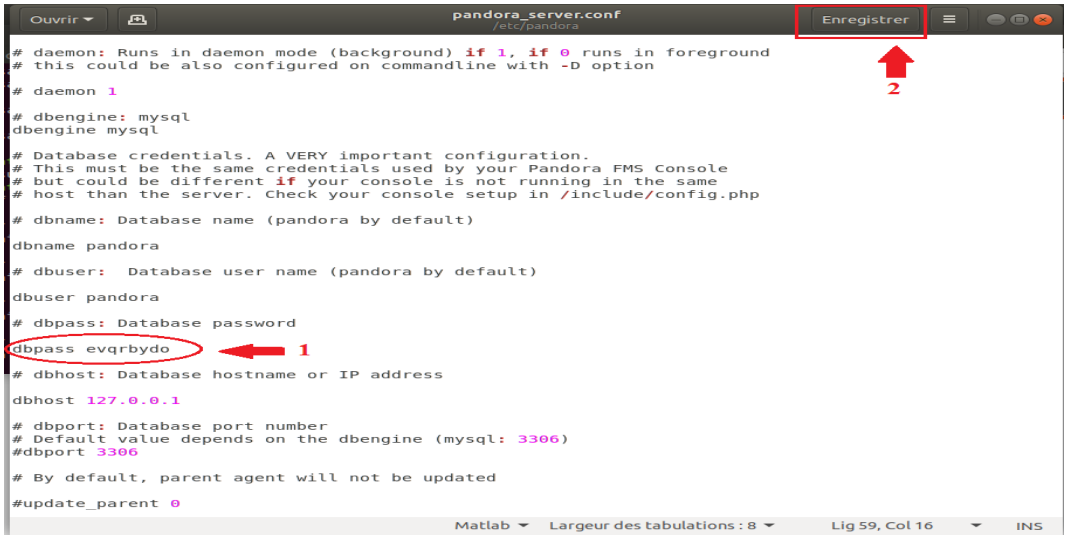


FIGURE C.25 – Modification du paramètre "dbpass" dans le fichier Pandora serveur.

3. Redémarrez le service Pandora et vérifiez s'il est opérationnel comme illustré dans la figure C.26 ;

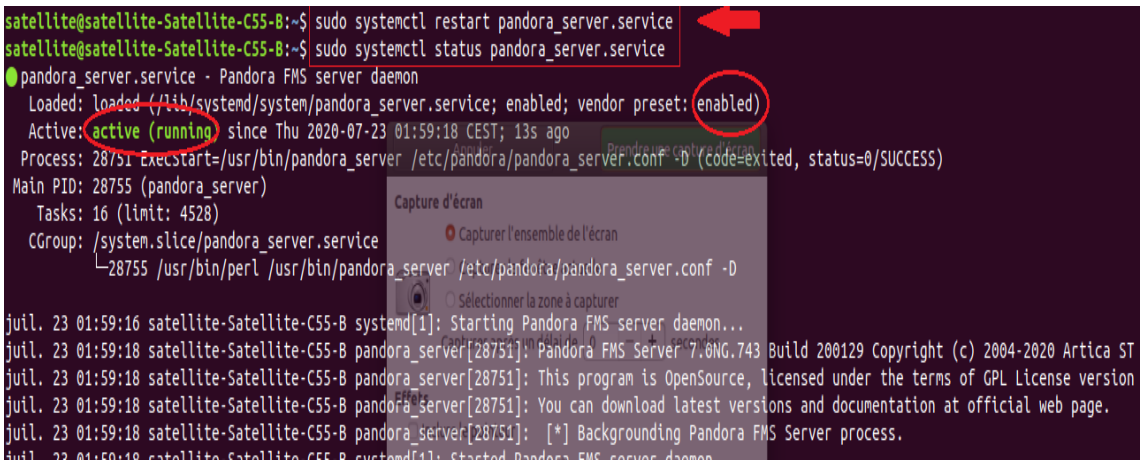


FIGURE C.26 – Commandes de vérification si le service Pandora FMS est opérationnel.

4. Assurez-vous également que le service Tentacle (un protocole de transfert de fichiers client / serveur) est opérationnel comme illustré dans la figure C.27 ;

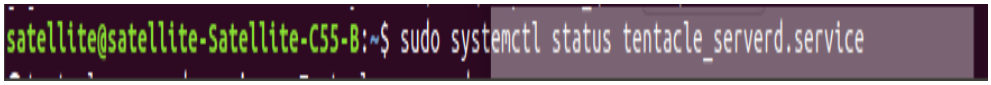


FIGURE C.27 – Commandes de vérification si le service Tentacle est opérationnel.

5. Enfin, revenez à la console Pandora et actualisez-la pour commencer à surveiller le serveur d'installation. Vous devriez pouvoir obtenir des informations sur l'hôte local sur le tableau de bord, comme indiqué dans la figure C.28.

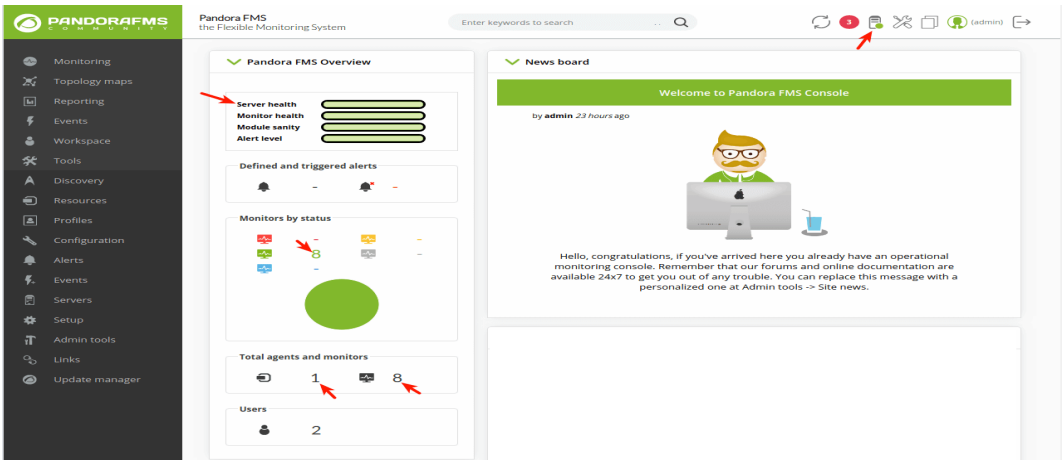


FIGURE C.28 – Console Pandora FMS

### C.1.3 Installation des agents Pandora FMS

1. Exécutez les commandes illustrées dans la figure C.29 pour télécharger le package DEB de l'agent et l'installer.

```
satellite@satellite-Satellite-C55-B:~$ wget https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/743/Debian_Ubuntu/pandorafms.
agent_unix_7.0NG.743.deb
satellite@satellite-Satellite-C55-B:~$ sudo dpkg -i pandorafms.agent_unix_7.0NG.743.deb
satellite@satellite-Satellite-C55-B:~$  sudo apt-get -f install
```

FIGURE C.29 – Commandes de téléchargement et l'installation du package DEB de l'agent Pandora.

### C.1.4 Configuration des agents Pandora FMS

1. Une fois le package de l'agent logiciel installé, configurez-le pour qu'il communique avec le serveur Pandora FMS, Ouvrez le fichier nommé «*/etc/pandora/pandora_agent.conf* » (figure C.30) et modifiez-le ;

```
satellite@satellite-Satellite-C55-B:~$ sudo gedit /etc/pandora/pandora_agent.conf
```

FIGURE C.30 – Commande pour éditer le fichier Pandora agent.

2. Recherchez le paramètre 'Server_ip' et définissez l'adresse du serveur Pandora FMS puis enregistrez le fichier comme illustré dans la figure C.31 ;

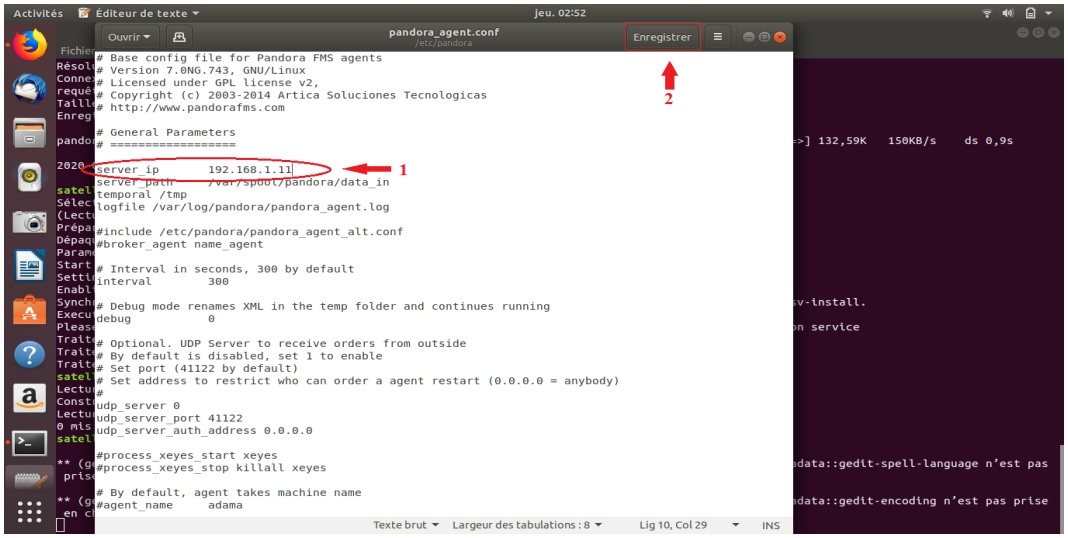


FIGURE C.31 – Modification du paramètre "Server_ip" paramètre dans le fichier Pandora agent.

3. Démarrez le service du démon de l'agent Pandora, activez-le pour démarrer automatiquement au démarrage du système et vérifiez que le service est opérationnel comme illustré dans la figure C.32.

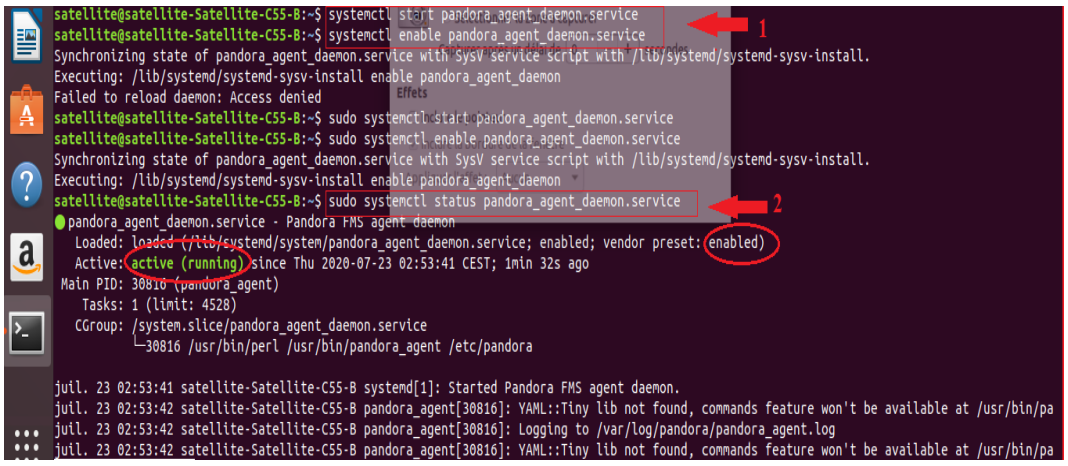


FIGURE C.32 – Commandes de démarrage et vérification si le service du démon de l'agent Pandora FMS est opérationnel.

## C.2 Sous CentOS

Dans la version 'Appliance CentOS ISO' tout est déjà installé et préconfiguré (vous n'aurez pas besoin de procéder à l'exécution des étapes précédentes utilisées lors de l'installation Pandora FMS sur Ubuntu), vous allez juste l'installer sur la VMware, c'est une installation minimale elle ne possède pas d'interface graphique, cette version possède juste un terminal pour exécuter les commandes.

**Étape 1 : Téléchargement de Appliance CentOS ISO**

1. Dans le site officiel de Pandora FMS : 'https ://pandorafms.org/features/free-download-monitoring-software/', cliquez sur 'CentOS Appliance ISO' pour télécharger l'image comme illustrée dans la figure C.33.

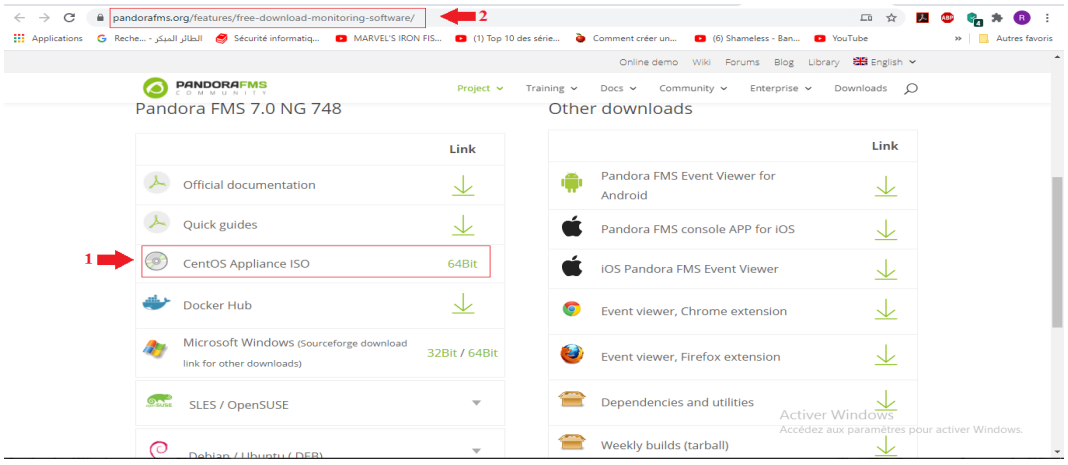


FIGURE C.33 – Site officiel de Pandora FMS.

## C.3 Installation et configuration de SNMP

**Étape 1 : Installation de SNMP**

1. Exécutez sous CentOS la commande illustrée dans la figure C.34, pour installer les packages SNMP.

```
[root@PandoraFMS ~]# yum install net-snmp net-snmp-utils_
```

FIGURE C.34 – Commande d'installation des packages SNMP.

**Étape 2 : Configuration de SNMP** Une fois l'installation terminée, procédez à la configuration de SNMP comme suit :

1. Le fichier de configuration par défaut pour SNMP est */etc/snmp/snmpd.conf*. Le fichier est fortement commenté et donc, nous n'apporterons que quelques modifications. Par conséquent, faites une copie du fichier original comme illustré dans la figure C.35 ;

```
Terminé !
[root@PandoraFMS ~]# ls /etc/snmp
snmpd.conf  snmptrapd.conf
[root@PandoraFMS ~]# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.org
```

FIGURE C.35 – Copie du fichier SNMP.

2. Editez le fichier snmpd.conf et changez le nom de la communauté comme illustré dans la figure C.36 ;

```
####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  default       test
```

FIGURE C.36 – Changement du nom de la communauté.

3. Activez et démarrez le service SNMP (voir figure C.37) ;

```
[root@PandoraFMS ~]# systemctl enable snmpd
Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to /usr/lib/systemd/s
ystem/snmpd.service.
[root@PandoraFMS ~]# systemctl start snmpd
[root@PandoraFMS ~]# service snmpd restart
Redirecting to /bin/systemctl restart snmpd.service
[root@PandoraFMS ~]#
```

FIGURE C.37 – Commandes d'activation et démarrage du service SNMP.

4. Testez pour vérifier que tout fonctionne comme prévu (voir figure C.38) ;

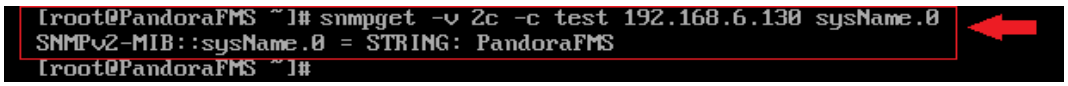


FIGURE C.38 – Commande de vérification du fonctionnement SNMP.

## C.4 Installation et configuration de POSTFIX

**Étape 1 : Installation de POSTFIX**

1. Installez les packages illustrés dans la figure C.39 sur le serveur Pandora pour que le serveur postfix fonctionne correctement avec un compte GMAIL.


FIGURE C.39 – Commande d'installation des packages pour le serveur postfix.

**Étape 2 : Configuration de POSTFIX** Une fois postfix installé sur le serveur et que tout fonctionne correctement, à l'exception de l'envoi d'e-mails via Gmail, procédez comme suit :

1. Vérifiez que l'option "moins sécurisée" est activée dans votre compte Gmail.
2. Editez le fichier */etc/postfix/main.cf* et ajoutez les lignes (voir figure C.40) à la fin du fichier ;

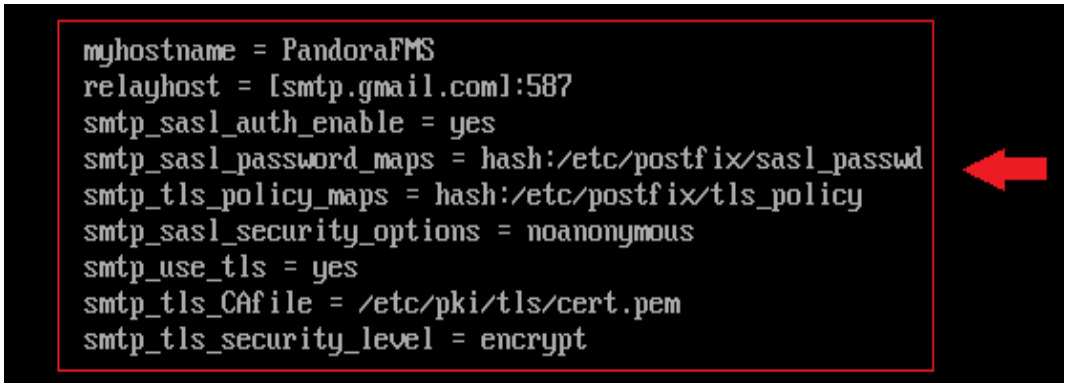


FIGURE C.40 – Edit du fichier postfix.

3. Créez le fichier */etc/postfix/sasl_passwd* et ajouter la ligne de configuration avec l'adresse Gmail et son mot de passe correspondant comme indiqué dans la figure C.41 ;


FIGURE C.41 – Aperçu du fichier sasl_passwd.

Sécurisez le fichier avec les commandes illustrées dans la figure C.42 ;

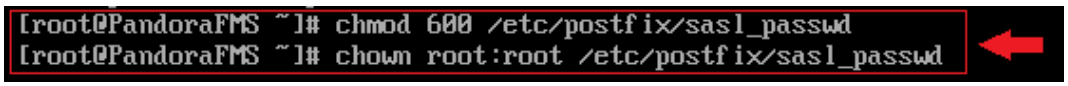


FIGURE C.42 – Commandes de sécurisation du fichier sasl_passwd.

4. Créez le fichier */etc/postfix/tls_policy* et ajoutez la ligne de configuration illustrée dans la figure C.43 ;

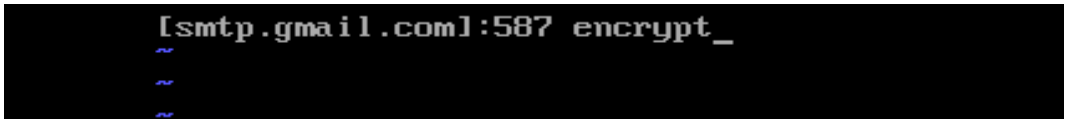


FIGURE C.43 – Aperçu du fichier tls_policy.

Sécurisez le fichier avec les commandes illustrées dans la figure C.44 ;


FIGURE C.44 – Commandes de sécurisation du fichier tls_policy.

5. Transformez */etc/postfix/sasl_passwd* et */etc/postfix/tls_policy* en un fichier indexé de type hachage via la commande illsutré dans la figure C.45. Il créera les fichiers */etc/postfix/sasl_passwd.db* et */etc/postfix/tls_policy.db* ;


FIGURE C.45 – Hachage des fichiers sasl_passwd et tls_policy.

6. Enfin, redémarrez postfix pour appliquer les modifications comme illustré dans la figure C.46 ;

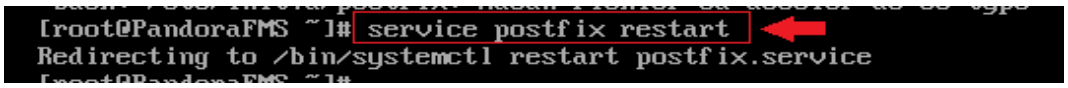


FIGURE C.46 – Redémarrage du service postfix.

7. Testez pour vérifier que postfix fonctionne, avec la commande illustrée dans la figure C.47 ;

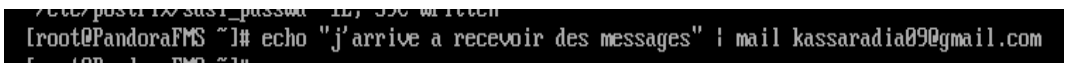


FIGURE C.47 – Test du fonctionnement du service postfix.

Réception du mail envoyé (voir figure C.48).

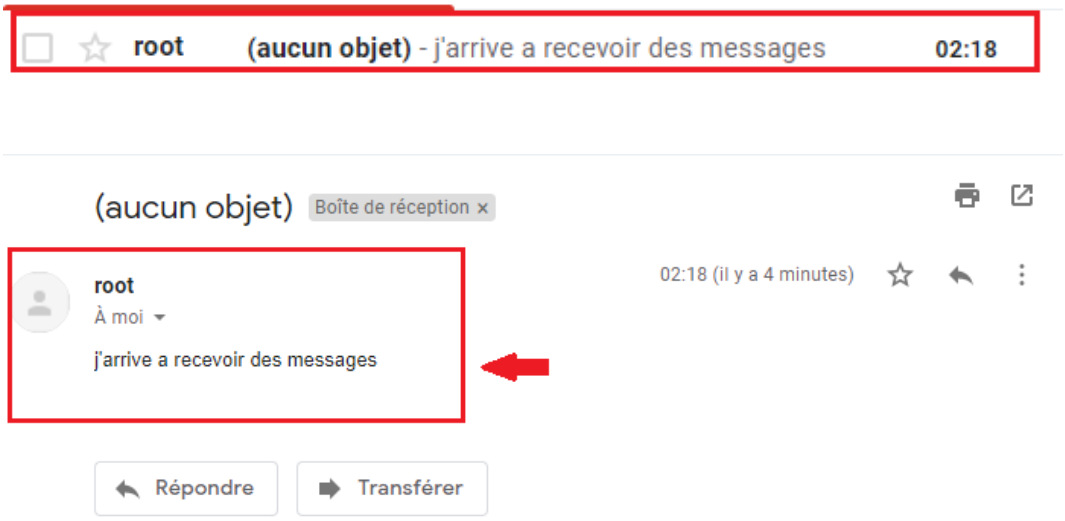


FIGURE C.48 – Réception du mail.

# Abstract

Since the emergence of new technologies, IT has established itself more than ever as a valuable tool needed by any company that wants to increase its productivity and remain competitive nationally and internationally. Indeed, any problem or failure related to IT must therefore be reduced to a minimum because it can have serious consequences, both financial and organizational. Network supervision is then necessary and essential to guarantee good activity of the networks and its equipment, by making it possible to have indicators on the performance of its architecture. In our project we proceeded to the implementation of a monitoring solution based on "Pandora FMS" for the administration of the IT park of the EPB. This tool relies on the SNMP protocol to manage network equipment and diagnose the system.



**Key words :** Network supervision, monitoring, Pandora FMS, administration, SNMP.



# Résumé

Depuis l'émergence des nouvelles technologies, l'informatique s'est imposée plus que jamais comme un outil précieux pour les entreprises qui souhaitent accroître sa productivité et rester compétitive au niveau national et international. En effet, tout problème ou panne liés à l'informatique doivent donc être réduits au minimum, car ils peuvent avoir de lourdes conséquences aussi bien financières qu' organisationnelles. La supervision des réseaux est alors nécessaire et indispensable pour garantir une bonne activité des réseaux ainsi que ses équipements et cela en permettant d'avoir des indicateurs sur la performance de son architecture. Dans notre projet nous avons procédé à la mise en œuvre d'une solution de supervision basée sur "Pandora FMS" pour l'administration du parc informatique de l'EPB. Cet outil s'appuie sur le protocole SNMP pour gérer les équipements du réseau et diagnostiquer le système.



**Mots clés :** Supervision des réseaux, monitoring, Pandora FMS, administration, SNMP.