République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaïa

Faculté des Sciences Exactes
Département Informatique

Mémoire de Fin d'études

En vue de l'obtention du diplôme de Master 2 en informatique
Option : Administration et Sécurité des Réseaux

Thème :

ÉTUDE ET MISE EN PLACE D'UNE SOLUTION MONITORING : PROMETHEUS

CAS D'ÉTUDE : EPB

Présenté par :

HAMMICHE Laldja & HAOUCHINE Rania

Défendu le 04/07/2024, devant le jury composé de :

M^{r} N. SALHI	Professeur	Président de jury	UAMB - Bejaia
M^{me} N. SAAD	M.C.B	Examinatrice	UAMB - Bejaia
M^{r} D. TOUAZI	M.C.B	Promoteur	UAMB - Bejaia

Année Universitaire 2023 – 2024

REMERCIMENTS

Tout d'abord, Nous tenons à remercier « **Allah** », le clément et le miséricordieux de nous avoir donné la force et le courage de mener à bien ce modeste travail.

Nous remercions également à exprimer notre gratitude envers **nos familles** pour leurs soutiens et leurs encouragements constants tout au long de ce projet, leur patience et leur compréhension ont été des piliers essentiels dans la réalisation de ce travail.

Notre cher promoteur, **Monsieur D.TOUAZI** a généreusement accepté de nous encadrer pour ses conseils avisés, ses orientations précieuses et sa disponibilité tout au long de ce travail ont grandement contribué à sa réussite.

Nous tenons à remercier également les membres de jury **Monsieur N.SALHI** et **Madame N.SAAD** d'avoir accepté de juger et d'évaluer ce mémoire.

Nous exprimons une reconnaissance particulière **l'Organisme d'Accueil EPB**, ainsi que **Monsieur IMLOUL Fatah**, notre encadrant sur le lieu de stage, pour son encadrement attentif, ses suggestions pertinentes et le partage de ses connaissances. Sa présence et son suivi ont été essentiels pour enrichir notre expérience professionnelle.

Enfin, nous n'oublions pas nos amis et collègues qui ont partagé leurs idées et leur expérience, contribuant ainsi à l'amélioration de notre projet.

DÉDICACE

Le devoir de reconnaissance m'oblige à dédier ce modeste mémoire à tous ceux qui me sont chers, ceux à qui je dois mon succès.

À notre « Seigneur, Dieu Tout-Puissant »,

Merci de m'avoir accordé tes bénédictions et exaucé mes prières, me permettant ainsi d'atteindre cet accomplissement.

A mes chers parents,

Vous avez été les piliers de ma vie, m'offrant un amour inconditionnel et un soutien sans faille à chaque étape de mon parcours. Vos sacrifices, votre patience et vos conseils avisés m'ont permis de traverser les moments les plus difficiles et de rester motivée jusqu'à la fin. C'est grâce à vos encouragements que j'ai pu surmonter les obstacles et atteindre mes objectifs. Je vous en serai éternellement reconnaissante.

A ma chère sœur Assia,

Ton affection et tes encouragements ont été une source inépuisable de motivation. Merci pour ta patience et ta compréhension. Je suis profondément reconnaissante de t'avoir à mes côtés.

A ma chère binôme,

T'es plus qu'une binôme t'es une sœur, sans ton soutien et tes encouragements, nous ne serions pas arrivées jusqu'q ici. Travailler ensemble a été une expérience précieuse, et je suis reconnaissante pour chaque moment partagé avec toi. Ta présence amicale et professionnelle a été d'une valeur inestimable tout au long de ce parcours. Merci pour tout.

Merci à toute personne qui nous a soutenue de pré et de loin.

Laldja

DÉDICACE

Le devoir de reconnaissance m'oblige à dédier ce modeste mémoire à tous ceux qui me sont chers, ceux à qui je dois mon succès.

À notre « Seigneur, Dieu Tout-Puissant »,

Merci de m'avoir accordé tes bénédictions et exaucé mes prières, me permettant ainsi d'atteindre cet accomplissement.

À mon cher père,

Je te remercie pour ton soutien et tes encouragements constants. Tu as toujours cru en moi. Ton amour et ta patience m'ont guidé tout au long de ce parcours. Merci pour tous tes sacrifices et pour être un modèle d'inspiration. Ton rôle dans ma réussite est inestimable.

À ma chère mère,

Je te remercie pour ton amour inconditionnel et ta douceur sans pareille. Tu as su m'encourager et m'apaiser, même dans les moments les plus difficiles. Ton soutien moral et ta tendresse m'ont été indispensables. Merci pour ta présence réconfortante et pour avoir toujours été là pour moi. Ta force ma porté jusqu'à la réalisation de ce projet.

À mes adorables sœurs, Chaima, Nour El Houda, et Malak,

Vous avez été une source inestimable de soutien et de réconfort. Votre amour, vos rires et vos encouragements m'ont accompagné tout au long de ce parcours. Merci d'avoir été mes piliers et de m'avoir toujours poussé à donner le meilleur de moi-même.

À ma chère Binôme,

Je te remercie pour ta présence, ton soutien inconditionnel t ton amour. Tu es ma meilleure amie et bien plus encore, ma soeur. Ensemble nous avons accompli un travail exéptionnel sur notre projet de fin d'études,démontrant notre complicité et notre capacité à surmonter tous les défis. Je suis reconnaissante de t'avoir à mes cotés dans cette aventure.

Merci à toute personne qui nous soutenue de pré et de loin.

Rania

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ACRONYMES

A	**ARP**	Address Resolution Protocol
	ASCII	American Standard Code for Information Interchange
	ASN.1	Abstract Syntax Notation 1
B	**BDD**	Base de Données
C	**CD**	Content Delivery
	CNAN	Compagnie Nationale Algérienne de Navigation
	CNCF	Cloud Native Computing Foundation
	CPU	Central Processing Unit
D	**DA**	Direction Achats
	DC	Direction Capitainerie
	DDD	Direction Domaine et Développement
	DDN	Direction Digitalisation et Numérique
	DE	Direction Exploitation
	DG	Direction Générale
	DGA	Direction Générale Adjointe
	DFC	Direction Finances et Comptabilité
	DM	Direction Maintenance
	DMZ	Demilitarized Zone
	DNS	Domain Name System
	DRH	Direction Ressources Humaines
	DSCI	Direction du Système de Contrôle Interne
E	**EPB**	Entreprise Portuaire de Bejaia
F	**FDDI**	Fiber Distributed Data Interface
	FreeBSD	Free Berkeley Software Distribution
	FTP	File Transfer Protocol
G	**GED**	Gestion Électronique de Document
	GMAO	Gestion de Maintenance Assistée par Ordinateur
	GNS3	Graphic Network Simulator 3
H	**HTTP**	Hypertext Transfer Protocol
I	**ICMP**	Internet Control Message Protocol
	IETF	Internet Engineering Task Force
	IP	Internet Protocol
	IPMI	Intelligent Platform Management Interface
	IR	Infra Rouge

	ISO	International Standardization Organisation
	IT	Information Technology
J	**JMX**	Java Management Extensions
	JPEG	Joint Photographic Experts Group
L	**LAN**	Local Area Network
M	**MAN**	Metropolitan Area Network
	MIB	Management Information Base
	MPEG	Moving Picture Experts Group
	MySQL	My Structured Query Language
N	**NMS**	Network Management Station
O	**OID**	Object Identifier
	ONP	Office National des Ports
	OSI	Open Systems Interconnection
P	**PAN**	Personal Area Network
	Pfsense	Pare-feu Sense
	PPP	Point-to-Point Protocol
	PromQL	Prometheus Query Language
R	**RFC**	Request For Comments
	RPC	Remote Procedure Call
	RRD	Round Robin Database
	RRDTool	Round Robin Database Tool
S	**SI**	Systèmes d'Information
	SMS	Short Message Service
	SNMP	Simple Network Management Protocol
	SMTP	Simple Mail Transfer Protocol
	SO.NA.MA	Société Nationale de Manutention
	SQL	Structured Query Language
	SSH	Secure Shell
	SSL	Secure Sockets Layer
	Syslog	System Logging Protocol
T	**TCP**	Transmission Control Protocol
	Telnet	Telecommunication Network
	TLS	Transport Layer Security
	TSDB	Time Series Database
U	**UDP**	User Datagram Protocol
	USB	Universal Serial Bus
	UI	User Interface
V	**VPN**	Virtual Private Network
W	**WAN**	Wide Area Network
	WiMax	Worldwide Interoperability for Microwave Access
	WMI	Windows Management Instrumentation
V	**VMware**	Virtual Machine Software

INTRODUCTION GÉNÉRALE

L'évolution des entreprises dans le monde numérique a entraîné une augmentation exponentielle de la complexité des systèmes informatiques. Désormais, les entreprises modernes dépendent fortement de ces systèmes pour gérer leurs activités quotidiennes, ce qui rend la disponibilité, la performance et la sécurité essentielles à leur succès.

Cependant, l'adoption croissante d'infrastructures distribuées et d'applications cloud expose les entreprises à des nouveaux défis majeurs, parmi ceux-ci les risques de panne système, les menaces de cyberattaques compromettant la sécurité des données sensibles, ainsi que la difficulté de maintenir une performance optimale dans des environnements complexes et distribués. La gestion de ces défis nécessite souvent des investissements importants en termes de technologie et de compétences spécialisées, ce qui peut être un défi supplémentaire pour les organisations.

De ce fait, les administrateurs réseau recours à des logiciels de surveillance et de supervision de réseaux afin de vérifier en temps réel l'état de l'ensemble du parc informatique, ce qui leur permet de maintenir la performance et la disponibilité sous leur responsabilité pour éviter les défis majeurs.

Ce mémoire a pour objectif de proposer Prometheus comme un outil de supervision très puissant pour garantir la fiabilité et la qualité de service de l'Entreprise Portuaire Bejaia. Pour réaliser cette étude de manière efficace, nous avons structuré notre mémoire en quatre chapitres :

Chapitre1 : Le premier chapitre se focalise sur une analyse détailléé de l'Entreprise Portuaire de Bejaia (EPB). Par la suite, nous avons repéré et présenté la problématique particulière à laquelle cette entreprise fait face en examinant ses causes et ses conséquences. Finalement, nous avons suggéré une solution appropriée.

Chapitre2 : Le deuxième chapitre traite les concepts fondamentaux de la sécurité informatique ainsi que du monitoring et des protocoles associés, détaillant les différentes méthodes et technologies utilisées pour surveiller les performances, la disponibilité et la sécurité des systèmes informatiques.

Chapitre3 : Le troisième chapitre se concentre sur les outils de supervision, mettant en avant notre solution choisie, Prometheus. En fournissant une analyse approfondie de ses caractéristiques, son architecture et son fonctionnement.

Chapitre4 : Le quatrième chapitre décrit la partie pratique de notre mémoire, dont laquelle nous avons présenté l'environnement de travail ainsi que l'installation et la configuration de la solution Prometheus.

CHAPITRE 1

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Introduction

Dans ce chapitre, nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage pour la réalisation de notre projet de fin d'étude. Nous commencerons d'abord par une brève présentation de l'Entreprise Portuaire Bejaia (EPB). Ensuite, nous introduirons la structure générale de son organisation avec ses différentes directions et en particulier sa direction informatique, ainsi que ses objectifs. Pour finir, nous ferons le point sur la problématique posée et la solution proposée.

1.1 Présentation générale de l'EPB

L'entreprise portuaire de Bejaïa est une entité majeure dans le secteur maritime en Algérie. Avec ses installations modernes et son emplacement stratégique, elle joue un rôle capital dans le développement économique régional et le commerce international. Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN) [10].

FIGURE 1.1 – Entreprise Portuaire Bejaia

1.2 Création et évolution

1.2.1 Création

L'Entreprise Portuaire de Bejaïa a été créée le 14 août 1982 suite au décret n°82-285 [9].

1.2.2 Evolution

Depuis sa création, l'entreprise portuaire de Bejaïa a connu une évolution significative, tant sur le plan des infrastructures que des services offerts. Elle s'est diversifiée pour accueillir une gamme

plus large de cargaisons. D'importants investissements ont été faits pour moderniser les installations portuaires, augmenter les capacités de manutention et améliorer l'efficacité opérationnelle. Elle est notamment certifiée à la norme ISO 14001 :2004.

1.3 Situation géographique de l'EPB

L'entreprise portuaire de Bejaïa est située dans la ville de Bejaïa, en Algérie, plus précisément sur la côte sud de la région de Bejaïa. Cette position lui offre un accès direct à la mer Méditerranée, en faisant un port important pour le commerce maritime avec l'Algérie et d'autres pays méditerranéens. Grâce à cette situation favorable, le port de Bejaïa est une région centrale dans les affaires et la logistique, contribuant significativement à l'économie de la région et du pays.

FIGURE 1.2 – Port de Bejaia

1.4 La structure de l'entreprise

L'EPB est structurée en différentes directions, sous la supervision d'une Direction Générale chargée de la gestion et du développement de l'entreprise. Chaque partie prenante de l'organisation remplit un rôle important. Dans le cadre de ce mémoire, notre attention se portera exclusivement sur **la Direction Digitalisation et Numérique**.

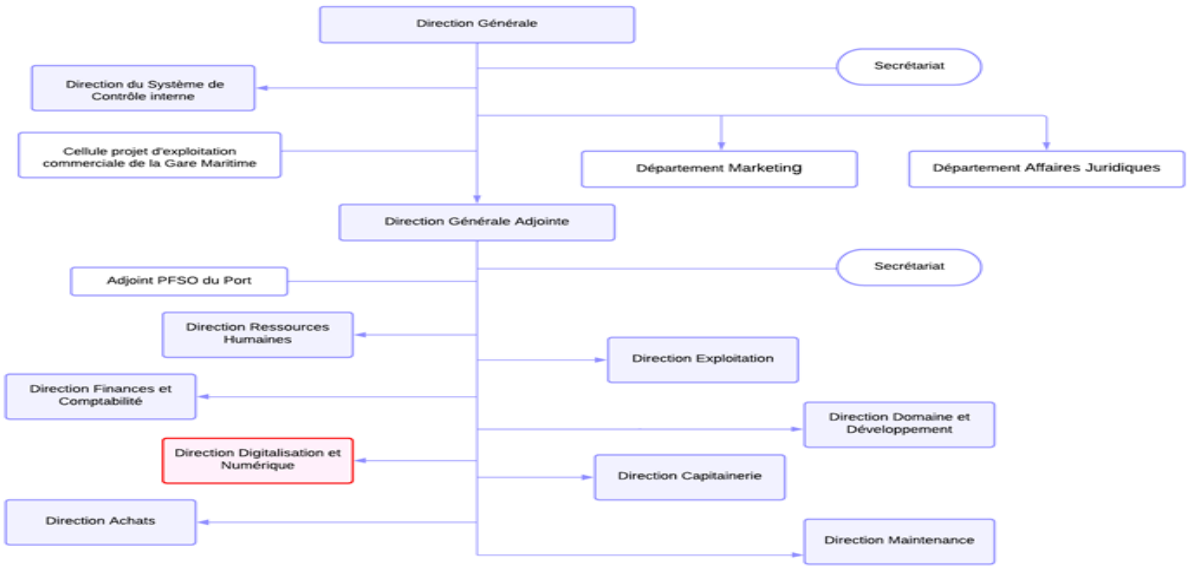

FIGURE 1.3 – Organigramme de l'Entreprise Portuaire Bejaia

1.4.1 Direction Générale(DG)

Elle est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise.

Les structures rattachées directement à la Direction Générale sont :

- Direction du Système de Contrôle Interne (DSCI).
- Département Marketing.
- Département Affaires Juridiques.

1.4.2 Direction Générale Adjointe (DGA)

Est organisée en directions opérationnelles et fonctionnelles :

1.4.2.1 Directions opérationnelles

Il s'agit des structures qui prennent en charge les activités sur le terrain et qui ont une relation directe avec les clients.

- Direction Exploitation (DE).
- Direction Maintenance (DM).
- Direction Domaine et Développement (DDD).
- Direction Capitainerie (DC).

1.4.2.2 Directions fonctionnelles

Il s'agit des structures de soutien aux structures opérationnelles.

- Direction Finances et Comptabilité (DFC).
- Direction Ressources Humaines (DRH).
- Direction Achats (DA).
- Direction Digitalisation et Numérique (DDN).

1.5 Activités et les missions d'EPB

1.5.1 Ses Missions

Les principales missions de l'EPB sont :

- La gestion, l'exploitation et le développement du domaine portuaire.
- L'aide à la navigation.
- La police et la sécurité dans le port.
- Le traitement des passagers et des marchandises transitant par le port.

1.5.2 Ses Activités

Les principales activités de l'entreprise sont :

- L'exploitation de l'outillage et des installations portuaires.
- L'exercice des opérations d'acconage et de manutention portuaire.
- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- L'exercice des opérations de remorquage, de pilotage et d'amarrage.

1.6 Les objectifs de l'EPB

- Maintenir la position de leader dans le domaine de l'activité portuaire.
- Développer la culture d'entreprise pour une gestion optimale des ressources.
- Participer au développement socio-économique.
- Pérenniser et créer des emplois.
- Crée la valeur ajoutée en matière de logistique et de transport.

1.7 Présentation de la Direction Digitalisation et Numérique

La Direction Digitalisation numérique de l'EPB est une direction rattachée à la direction générale adjointe, est un ensemble de personnes chargées de la gouvernance des SI (système d'information) de l'organisation.

1.7.1 Missions

- La réalisation du schéma directeur par la conduite des projets d'informatisation en veillant à la cohérence fonctionnelle et technique ainsi qu'à la qualité et la sécurité des systèmes d'information.
- La mise en oeuvre des systèmes d'information à la fois flexibles et fiables.
- Le management des évolutions des systèmes d'information et des projets informatiques.
- La mise en place et la gestion de l'infrastructure informatique.

1.7.2 Stratégies

Pour une vue d'ensemble des stratégies de l'EPB, voici un schéma résumant leurs principales approches :

FIGURE 1.4 – Les Stratégies de DDN

1.8 Organisations de la DDN

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

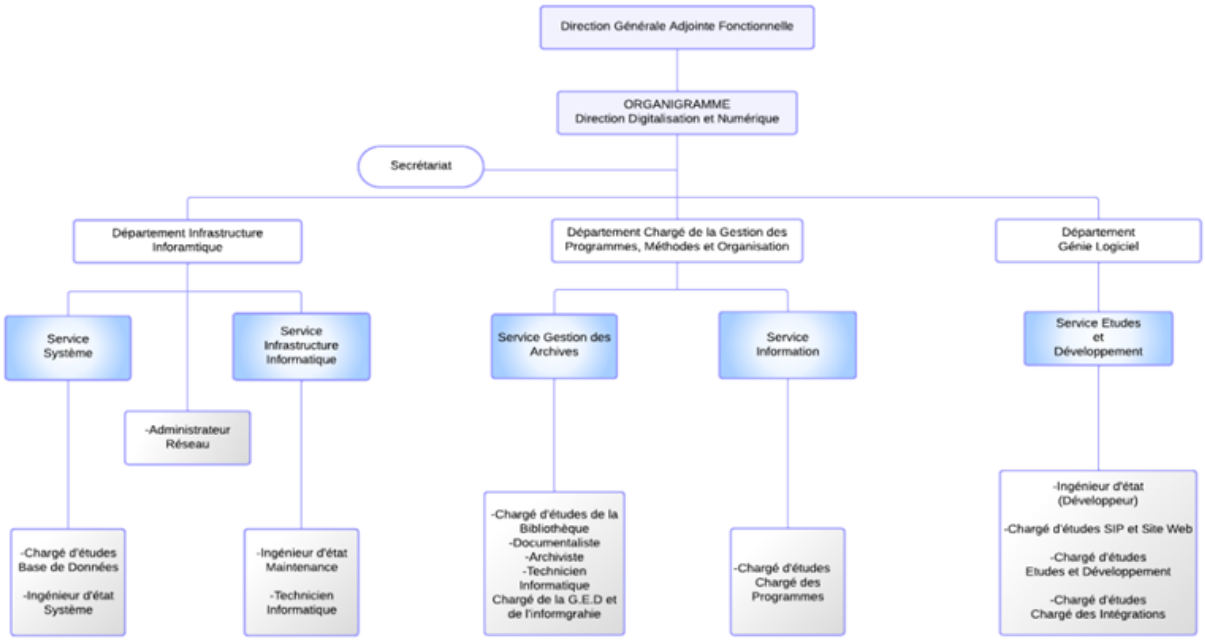

FIGURE 1.5 – Organigramme de la Direction Digitalisation et Numérique

1.8.1 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. Il s'occupe également du déploiement et de l'assistance chez les utilisateurs finaux.

1.8.2 Département chargé de la gestion des programmes, méthodes et organisations

Se compose en deux services :

- **Le service d'information :** chargé d'études des programmes.
- **Le service de gestion des archives :** qui se compose d'un documentaliste, bibliothécaire, archiviste et technicien informatique ce service est chargé de la GED et de l'infographie.

1.8.3 Département de l'infrastructure informatique

Possède un administrateur réseau et se divise en deux services :

- **Le service des infrastructures informatiques :** qui se compose d'ingénieurs d'état maintenance et de technicien informatique.
- **Le service des systèmes :** qui se compose d'ingénieurs d'état système et se charge d'étude des bases de données.

1.9 Etude de l'existant

1.9.1 Infrastructure informatique : Présentation du Réseau de l'EPB

Le réseau portuaire de Bejaia s'étend du port pétrolier au port à bois. La salle informatique 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 DDN 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).

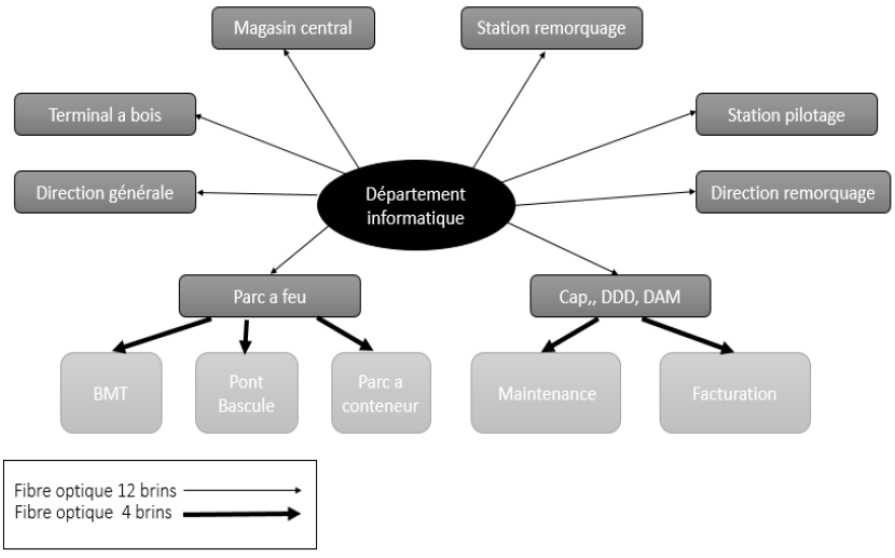

FIGURE 1.6 – Réseau Informatique de l'EPB

1.9.2 Vue globale du Data Center

- Le data center est muni de deux armoires de brassage, dont l'une d'entre elles est l'armoire cœur du réseau du port.

- L'onduleur central gère tous les équipements et les armoires (armoire optique et câble normale).

- A l'intérieur de l'armoire optique on trouve des switchs Cisco référence Catalyst 2960, des switchs D-link, un support de transmission optique équipement Huawei OSN 500 Optique X qui est alimenté par deux connexions optiques hauts-débits (Connexion 10 mega/b et 30 mega/b) et des switchs optiques D-Link xStack. Le switch Cisco Catalyst 2960 fait la translation de l'optique vers le switch Ethernet, l'internet passe par le switch optique vers le switch Ethernet puis vers le switch serveur lié aux serveurs.

- Coté serveurs on retrouve des hyperviseurs qui contiennent des machines virtuels (VMwares), ces machines virtuelles sont des serveurs parmi eux on retrouve des serveurs Windows (Active Directory), serveurs EZet (serveur anti-virus), serveur BDD (MySQL et MariaDB) et un serveur SIP qui est un serveur local (site internet en intranet) les utilisateurs peuvent consulter le site à travers ce serveur. Pour accéder aux hyperviseurs on utilise les switchs KVM en effectuant des modifications au niveau de sa console et on les chapote à travers un soft VSphereClient.

- Il existe deux baies de stockages une en mode NAS et l'autre en mode SAN. Toutes les données sont stockées dans la baie de stockage à travers les disques durs qui sont reliés au réseau NAS. Pour envoyer les données on sollicite la couche cœur qui distribue vers la couche distribution puis vers la couche accès qui contient deux switchs Catalyst Cisco 2960, qui permettent l'accès au réseau global.

FIGURE 1.7 – Data Center

1.9.3 Architecture du département informatique de l'EPB

Dans cette partie nous allons décrire l'architecture du réseau informatique de L'EPB qui dispose de deux machines serveur.

La première comprend :

- Serveur contrôleur de domaine 1.
- Serveur d'application/serveur BDD MySQL.
- Serveur d'application tomac (gmao : gestion maintenance assistée par ordinateur).

Et la deuxième comprend :

- Serveur contrôleur de domaine 2 (serveur web, serveur d'applications).
- Serveur GED (gestion électronique de document).

La sécurité est assurée par des Pare Feu (pfSense), qui bloquent les accès au réseau local à partir de la DMZ (un sous-réseau séparé et isolé du réseau local et d'internet par le pare-feu), ces derniers sont associés aux SW-servers (Switch) qui diffuse les informations à un réseau LAN (LAN USER).

L'EPB est dotée de deux connexions WiMax à savoir : icosnet WiMax, Alg télécom WiMax.

Elle dispose de deux réseaux VPN qui sont :

- **VPN (post/site) :** il correspond aux serveurs qui fournissent des services à un ou plusieurs machines.
- **VPN (site/site) :** représente la liaison de ce réseau au réseau de deux ports secs (site Texter à Bordj Bou Arreridj, site Ighil Ouberouak à Bejaia).

C'est ce qui est regroupé dans la figure suivante :

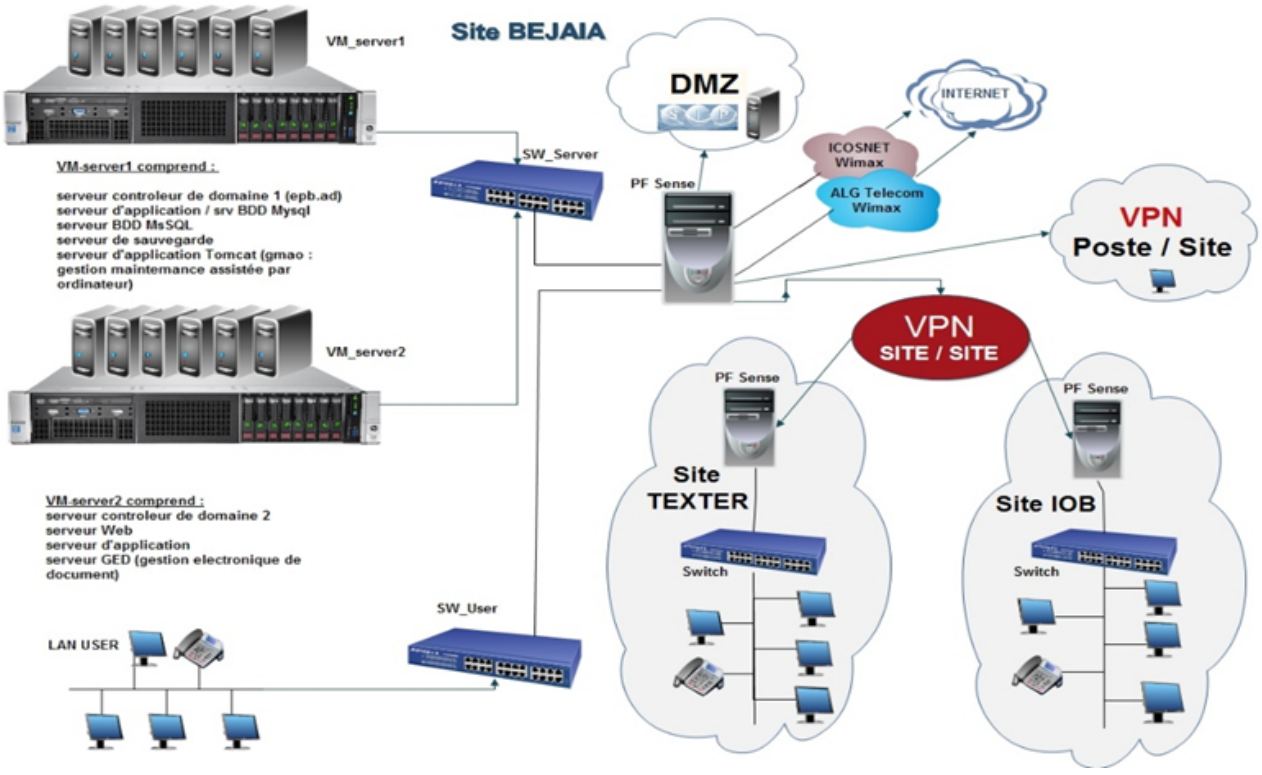

FIGURE 1.8 – Architecture de Réseaux Informatique de l'EPB

1.9.4 Services Intranet et internet de l'EPB

1.9.4.1 Services Intranet

Les services intranet existant à l'EPB sont les suivants :

- Le courrier électronique.
- L'accès à l'internet public.
- L'accès aux données de l'entreprise.
- La distribution et la publication d'informations.
- La gestion des documents.

1.9.4.2 Services Internet

Internet offre une variété de fonctionnalités et d'avantages aux utilisateurs comme :

- La messagerie électronique(E-mail).
- Le transfert des fichiers FTP.
- Le World Wide Web.

1.10 Problématique

Le réseau EPB comme n'importe quel autre réseau n'est pas sans faille en termes de sécurité et réseau, notamment en raison du nombre élevé de ses utilisateurs.

Au cours de nos visites au sein de l'entreprise, nous avons constaté que le manque de supervision réseau et système peut entraîner plusieurs problèmes, notamment :

- Indisponibilité des services.
- Risques de sécurité accrus.
- Incapacité à détecter les problèmes.
- Difficultés à diagnostiquer les problèmes.
- Surutilisation des ressources.

1.11 Solution

Afin de résoudre ces problèmes, il est essentiel de mettre en place une supervision du réseau et un système efficace. Cela en utilisant des outils appropriés et en définissant des processus clairs pour la surveillance et la gestion des infrastructures informatiques. Dans ce contexte, notre choix s'est porté sur l'outil Prometheus car il est open source est le résultat d'une analyse approfondie de ses caractéristiques et fonctionnalités. Il est considéré comme le plus adapté à notre cas, offrant une supervision en temps réel, une facilité d'utilisation et une large gamme de fonctionnalités avancées.

Conclusion

Ce chapitre nous a permis de présenter l'organisme d'accueil, EPB, en détaillant sa structure organisationnelle ainsi que le rôle et les missions du département informatique. Nous avons également identifié les failles et proposé une solution pour améliorer la situation. Dans le chapitre suivant, nous exposerons quelques généralités sur les réseaux et sécurités. Ensuite, nous présenterons le monitoring et les protocoles utilisés pour la supervision.

CHAPITRE 2

SÉCURITÉ INFORMATIQUE ET MONITORING

Introduction

Le deuxième chapitre aborde les concepts fondamentaux de la sécurité informatique ainsi que du monitoring. Nous commençons par définir le concept essentiel de ce dernier pour le bon fonctionnement des entreprises et des administrations, puis nous détaillons son architecture générale. Ensuite, nous explorons les différents niveaux de surveillance, la structure de gestion des réseaux et les protocoles employés.

2.1 Sécurité Informatique

2.1.1 Définition

Ensemble des techniques, moyens et procédés utilisés afin de protéger les systèmes informatiques, les réseaux et les données contre les accès non autorisés, attaques, les dommages et les perturbations [8].

2.1.2 Objectifs

La sécurité informatique est fondée sur cinq principaux objectifs :

- **Confidentialité :** garantir que seules les personnes autorisées peuvent accéder et visualiser les données confidentielles.
- **Intégrité :** s'assurer que les données restent telles qu'elles sont et ne subissent aucune modification non autorisée.
- **Disponibilité :** assure que les systèmes, les applications et les données sont accessibles en cas de besoin par les utilisateurs autorisés.
- **Authenticité :** réfère aux caractéristiques d'une communication, garantissant que les données sont authentiquées à l'original et non modifiées ou falsifiées.

- **Non répudiation :** garantir qu'une tâche ou une transaction ne peut pas être niée par l'utilisateur qui l'a réalisée.

2.1.3 Politique de sécurité

Ensemble de lois et de consignes destiné à protéger les ressources et les informations contre tout préjudice à leur confidentialité, leur intégrité et leur disponibilité. La politique rédigée sous forme de règles définit les sujets et les objets, ainsi que les activités et opérations autorisées et interdites [11].

2.1.3.1 Les attaques informatiques

Une attaque informatique est toute tentative d'accès non autorisé à un ordinateur, un système ou un réseau informatique dans le but de causer des dommages. Ces attaques visent à perturber ou contrôler des systèmes ou encore voler ou modifier les données [19].

2.1.3.2 Catégories des attaques

- **Attaques passives :** est une tentative d'obtenir des informations ou de surveiller des systèmes informatiques sans modifier le contenu des données. L'objectif est de recueillir des informations sensibles sans être détecté.

    - **Interception des communications :** capturer et analyser les données en transit sur un réseau.
    - **Analyse de trafic :** observer les modèles de trafic pour déduire des informations.
    - **Collecte de métadonnées :** récupérer des informations sur les communications sans accéder aux données elles-mêmes.

- **Attaques actives :** les attaques actives consistent à modifier les ressources et les données d'un système afin de perturber son fonctionnement normal.

    - **Déni de service (DoS/DDoS) :** submerger un service avec des requêtes pour le rendre indisponible.
    - **Malware :** inclut virus, vers, chevaux de Troie, pour infecter et contrôler les systèmes.
    - **Exploitation des vulnérabilités :** utiliser des failles pour obtenir un accès non autorisé.
    - **Force brute :** Deviner des mots de passe par essais successifs.
    - **Attaques sur les réseaux sans fil :** Rechercher des réseaux Wi-Fi vulnérables (wardriving) ou créer de faux points d'accès (evil twin).

2.1.3.3 Mécanismes de sécurité

Les mécanismes de sécurité sont des outils qui servent à protéger les systèmes informatiques contre les attaques. Voici quelques outils :

- **Pare-feu :** équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement [5].

- **VPN (réseau privé virtuel) :** permet de créer un tunnel sécurisé entre deux réseaux distants, permettant ainsi à l'utilisateur une connexion sécurisée au réseau distant [5].

- **Vlan (Virtual Local Area Networks) :** permet de segmenter un réseau physique en plusieurs réseaux logiques, renforçant ainsi la sécurité en isolant les différents segments de trafic [5].

- **DMZ (Demilitarized Zone) :** zone réseau intermédiaire qui protège le réseau interne en isolant les services accessibles depuis l'extérieur [5].
- **Cryptographie :** mécanisme permettant d'implémenter du chiffrement et des signatures électroniques [5].

- **Antivirus et antimalware :** des programmes utilisés pour détecter et éliminer les logiciels malveillants et les virus qui ont déjà été identifiés par la communauté sécurité [5].

- **Contrôle d'accès :** authentification des utilisateurs via nom d'utilisateur et mot de passe [5].

- **Surveillance du réseau :** les outils de surveillance réseau peuvent alerter en cas d'activité malveillante et permettent d'agir rapidement pour contrer les menaces [5].

2.2 Monitoring

2.2.1 Définition

Le monitoring informatique, également connu sous le nom de surveillance informatique, permet d'analyser, de surveiller, de gérer, d'agir et alerter les fonctionnements anormaux des logiciels et des équipements qui constituent l'infrastructure informatique d'une entreprise, dans le but de fournir une vision précise sur le réseau et d'alerte l'administration suite à une détection d'un évènement indésirable ou des failles du réseau afin d'éviter la détérioration des données [14].

2.2.2 Principe de fonctionnement

La supervision informatique est une méthode essentielle pour surveiller à distance les activités d'un réseau informatique afin d'assurer sa stabilité, ses performances et sa sécurité. Ce processus se déroule en plusieurs étapes :

- La station de supervision envoie des requêtes à l'agent, qui renvoie ensuite des réponses.

- Lorsqu'un événement anormal est détecté, l'agent déclenche une alerte vers la station de supervision, également connue sous le nom de manager.

- Cette dernière est capable de résoudre automatiquement les problèmes ou d'alerter les administrateurs via des systèmes d'alerte tels que les e-mails ou les SMS.

Garantissant ainsi une gestion efficace du réseau informatique.

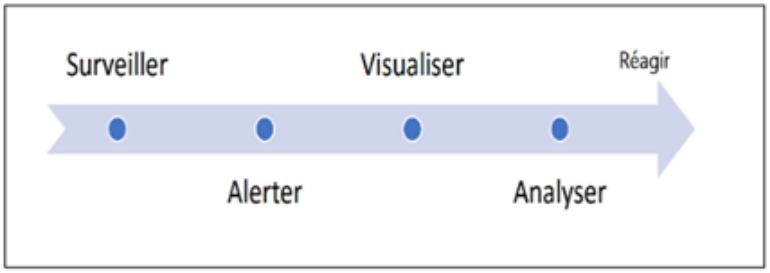

FIGURE 2.1 – Principe de Supervision

2.2.3 Architecture Générale

L'architecture de la supervision désigne la planification et la mise en place des divers éléments et systèmes utilisés pour superviser les différents processus, systèmes ou infrastructures. Voici un aperçu de cette architecture :

- **Agents :** sont des programmes ou des dispositifs installés sur les périphériques, les applications ou les serveurs à surveiller, ils collectent des données locales sur les performances et l'état des systèmes.
- **Collecteurs de données :** ils assurent la réception des données provenant des agents et stockent et traitent les informations collectées.
- **Base de données de stockage des données :** stocke les données de surveillance collectées par les agents et aussi permet de conserver un historique des performances et des événements sur une période définie.
- **Moteur de traitement et d'analyse :** chargé du traitement et de l'analyse des données collectées pour en extraire des informations significatives. Il peut comprendre des algorithmes d'analyse de données, des règles d'alerte, la corrélation d'événements.
- **Interface utilisateur :** est une interface graphique ou d'une application web permettant aux utilisateurs d'interagir avec le système de surveillance. Elle inclue des tableaux de bord, des rapports, des outils de requête pour prendre des mesures en cas d'alerte.
- **Système d'alerte :** chargé d'informer les administrateurs des problèmes détectés. Il a la possibilité d'envoyer des alertes.
- **Sécurité et authentification :** assure la sécurité des données collectées et la confidentialité des utilisateurs, en mettant en place des mécanismes d'authentification des utilisateurs, le chiffrement des données et des audits d'accès.

2.2.4 Différents niveaux de supervision

- **La supervision réseau :** consiste à surveiller un réseau informatique pour s'assurer qu'il n'y a pas de perturbations ou de défaillances au niveau de ses composants. Les administrateurs sont avertis lorsqu'un problème est suspecté, afin de pouvoir le diagnostiquer et le résoudre [6].

- **La supervision des systèmes :** se focalise essentiellement sur le contrôle et la surveillance des ressources clés du système, à savoir le processeur, la mémoire et le stockage.

- **La supervision des applications (Applicative) :** permet d'évaluer la disponibilité des machines en termes de services offerts, en testant les applications hébergées par les serveurs, telles que les bases de données, les serveurs de messagerie et autres serveurs web.

- **La supervision sécurité :** surveiller les attaques contre le système d'information de l'entreprise, en mettant en œuvre toutes les mesures de précaution en examinant, analysant les diverses entrées et en permettant de repérer les tentatives d'intrusion.

2.2.5 Méthodes de la supervision

2.2.5.1 Supervision active

La supervision active est la plus utilisée elle a l'avantage d'être fiable, cette méthode se compose de trois étapes :

- **Interrogation :** la plateforme de supervision envoie des requêtes SNMP, ICMP (ping) aux équipements du réseau pour obtenir des informations sur leur état et leur performance.

- **Mesure :** cette plateforme mesure les réponses reçues pour évaluer l'état et la performance des équipements surveillés.

- **Analyse et Rapport :** enfin l'analyse des données collectées et génération des rapports ou des alertes pour maintenir et optimiser les performances du réseau.

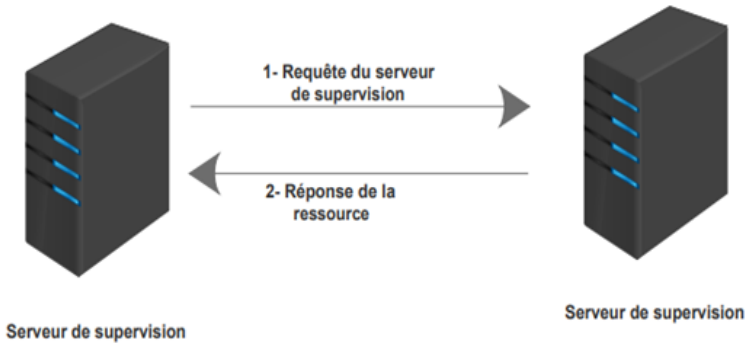

FIGURE 2.2 – Supervision Active

2.2.5.2 Supervision passive

Est une méthode où les systèmes surveillés envoient automatiquement des données sur leurs états, voici ses étapes :

- La ressource supervisée est équipée de capteurs ou de mécanismes internes qui lui permettent de surveiller son propre état et transmet le résultat au serveur de supervision.

- Le serveur de supervision reçoit les alertes provenant des ressources supervisées et de les traiter en conséquence.

- L'échange d'informations entre la ressource supervisée et le serveur de supervision est unidirectionnel, ce qui signifie que la ressource envoie des données au serveur mais ne reçoit pas de commandes ou d'instructions en retour.

FIGURE 2.3 – Supervision Passive

2.2.6 Avantages et Inconvénients

2.2.6.1 Avantage

- Surveillance complète et la notification en temps réel.

- Garantir la sécurité et identifier plus rapidement les menaces.

- Une meilleure utilisation des ressources informatique.

- Permet d'anticiper les pannes et défaillances tôt pour les résoudre plus vite.

2.2.6.2 Inconvénients

- Mettre en place et maintenir des outils de supervision peut être cher.

- Configurer et gérer ces outils peut nécessiter des compétences spécifiques.

- La qualité de la supervision dépend de la connexion Internet.

2.2.7 Structure de gestion des réseaux

2.2.7.1 Manageur

Est un logiciel installé sur un système puissant connecté au réseau, chargé de collecter des informations sur des périphériques surveillés, en envoyant des demandes aux agents pour avoir l'état de la machine.

Ensuite la présentation des informations analysées sous forme de tableaux, graphiques ou jauges faciles à comprendre.

2.2.7.2 Agent

Est un programme qui permet de surveiller en temps réel leur état, leurs performances et leur utilisation des ressources en effectuant les tâches suivantes :

- Il analyse les données collectées sur les performances des équipements pour repérer les problèmes.
- Il signale l'évènement détecté au manager en envoyant des notifications aux gestionnaires.
- Les agents traitent les demandes du manageur tout on renvoyant les renseignements en réponse.
- L'agent peut également résoudre les problèmes détectés.

2.2.7.3 La MIB (Management Information Base)

Est une structure arborescente qui organise les informations réseau.

- Chaque agent dispose de sa propre MIB qui définit les données qu'il peut fournir au manager pour surveiller et gérer les équipements.
- Chaque objet est identifié par un numéro unique appelé OID (Object Identifier), qui représente le chemin parcouru.
- Lorsqu'un un OID est interrogé, la valeur de retour est une séquence de chiffres séparés par des points.

La MIB peut contenir des milliers d'OID, formant un arbre dense avec des nœuds racine appelé "root-node", des branches et des feuilles.

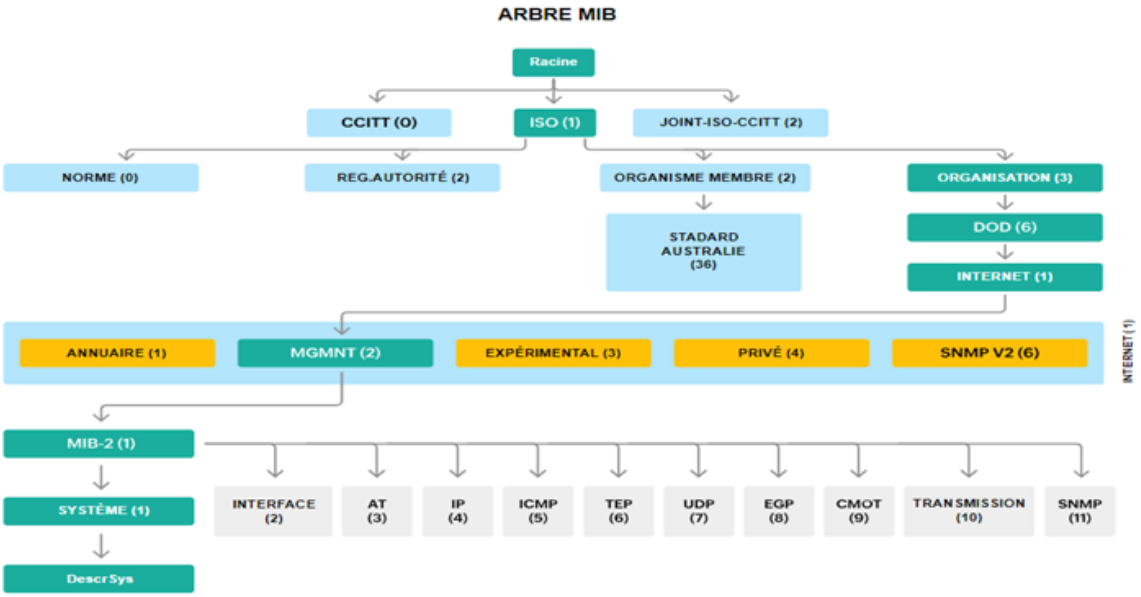

FIGURE 2.4 – Arbre MIB

2.2.8 Protocoles de supervision

2.2.8.1 IPMI (Intelligent Platform Management Interface)

Est une interface de gestion à distance des serveurs et des systèmes informatiques, généralement utilisé dans les environnements informatiques d'entreprise et de centre de données.

2.2.8.2 ICMP (Internet Control Message Protocol)

Est un protocole qui permet de vérifier la connectivité entre les périphériques réseau, mesurer le temps de réponse, détecter les pertes de paquets et générer des messages d'erreur en cas de défaillance.

2.2.8.3 HTTP (HyperText Transfer Protocol)

Est un protocole utilisé pour les communications Web et la transmission de données entre un navigateur web (client) et un serveur web. Il permet de surveiller la performance des sites web et collecter des informations.

2.2.8.4 WMI (Windows Management Instrumentation)

Est un outil de gestion des éléments logiques et physique des systèmes Microsoft Windows, utilisé dans l'administration système, la surveillance des performances et la création de scripts pour automatiser les tâches de gestion ces systèmes.

2.2.8.5 Syslog (System Logging Protocol)

C'est un protocole qui permet la transmission d'évènements de chaque équipement et les centralisés dans une seule machine dans le but d'archivage, d'analyse et la production d'alerte [18].

2.2.9 Protocole SNMP (Simple Network Management Protocol)

2.2.9.1 Présentation

SNMP est un protocole de gestion de réseaux proposé par l'IETF [1] (Internet Engineering Task-Force). Il est actuellement le plus utilisé pour la gestion des équipements de réseaux [13] et des serveurs ou même des périphériques. Il permet de :

- Connaître l'état global d'un équipement.
- Gérer les évènements exceptionnels.
- Analyser les différentes métriques afin d'anticiper les futurs problèmes.

2.2.9.2 Les versions du protocole SNMP

Plusieurs versions du protocole sont disponibles mais les plus utilises sont : SNMPv1, SNMPLv2c et SNMPv3.

1. L'IETF (Internet Engineering Task Force) est une organisation qui développe les normes pour assurer le bon fonctionnement et l'évolution de l'Internet.

- **SNMPv1 :** est la première version du protocole qui est définie dans le RFC (Request For Comments) 1157 [1].
  La sécurité de cette version est minimale car elle est basée uniquement sur la chaîne de caractère appelé « communauté ».

- **SNMPv2c :** elle assure une sécurité renforcée, des messages d'erreurs plus précis, autorise l'usage d'un Manager central.

- **SNMPv3 :** est la version la plus récente et la plus sécurisés, offrant une authentification robuste, un cryptage des données et un contrôle d'accès.

2.2.9.3 Architecture du protocole SNMP

SNMP facilite la communication entre le gestionnaire et les agents pour collecter les éléments spécifiques de la MIB. Elle repose sur un modèle client-serveur et se compose de trois principaux éléments :

a- Manager (Station de supervision)

Le manager NMS (Network Management Station) est un logiciel essentiel utilisé pour superviser et gérer les réseaux informatiques, en collectant des données sur les performances, l'état et l'utilisation des ressources des périphériques.

En utilisant ces informations, le NMS peut :

- Générer des rapports détaillés.
- Identifier les problèmes potentiels.
- Envoie des alertes en cas d'événements critiques.
- Accède aux informations de gestion de la MIB locale via un protocole d'administration.
- Centralise les données et les met en forme pour l'affichage et la sauvegarde.
- Réceptionne les alertes et agit en réaction.
- Ecoute sur le port UDP 162.

b- Agent SNMP

Est un logiciel implanté sur un équipement à superviser. Il s'agit souvent d'un équipement réseau, mais on trouve aussi des agents sur des serveurs. Il doit rester à l'écoute d'un port particulier, le port UDP 161.

Le rôle d'un agent SNMP est [12] :

- Créez différentes variables pour les différents composants MIB de cet équipement.
- Changez les valeurs de ces variables qui sont dynamiques.
- Émulez le comportement des messages SNMP « Trap » ou « Inform » sur le port UDP 162 pour signaler un événement extraordinaire.
- Assurer la sécurité de l'accès aux variables MIB conformément au modèle de sécurité établi.

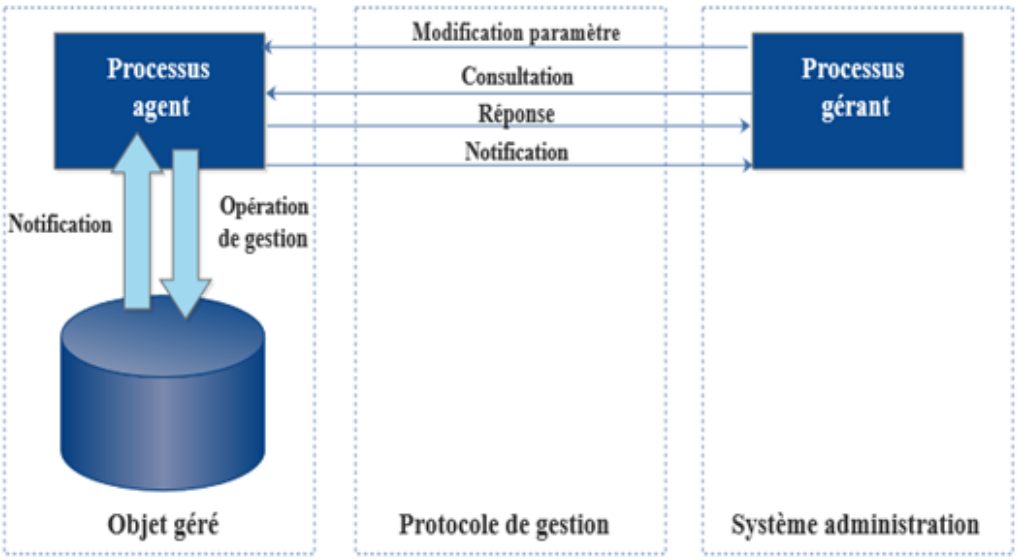

FIGURE 2.5 – Agent SNMP

c- La MIB

— **Management Information Base :** est un composant fondamental du protocole SNMP utilisé pour la gestion des réseaux informatiques, 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 [2] (Abstract Syntax Notation 1) sont l'ensemble des requêtes effectuer du manager vers l'agent ce dernier collecte ces données localement et les stocke tel que défini dans la MIB [12].

— **Structure d'une MIB et Object Identifier :** la structure d'une MIB est organisée de manière hiérarchique et est représentée par des OID uniques.

- Les OIDs sont des séquences de nombres qui représentent les chemins dans cet arbre, par exemple : « 1.3.6.1.2.1.1.3 » pourrait être l'OID pour l'objet « sysUpTime », qui indique le temps écoulé depuis le démarrage du périphérique.

- Les OIDs permettent aux systèmes de gestion réseau (NMS) de trouver et de comprendre les informations spécifiques sur les équipements, ce qui facilite la surveillance.

En résumé, la MIB offre une structure organisée pour représenter les données de gestion réseau, ce qui est essentiel pour la supervision et la gestion efficaces des infrastructures informatiques.

2. ASN.1 est un langage utilisé pour décrire et échanger des structures de données dans les communications réseau.

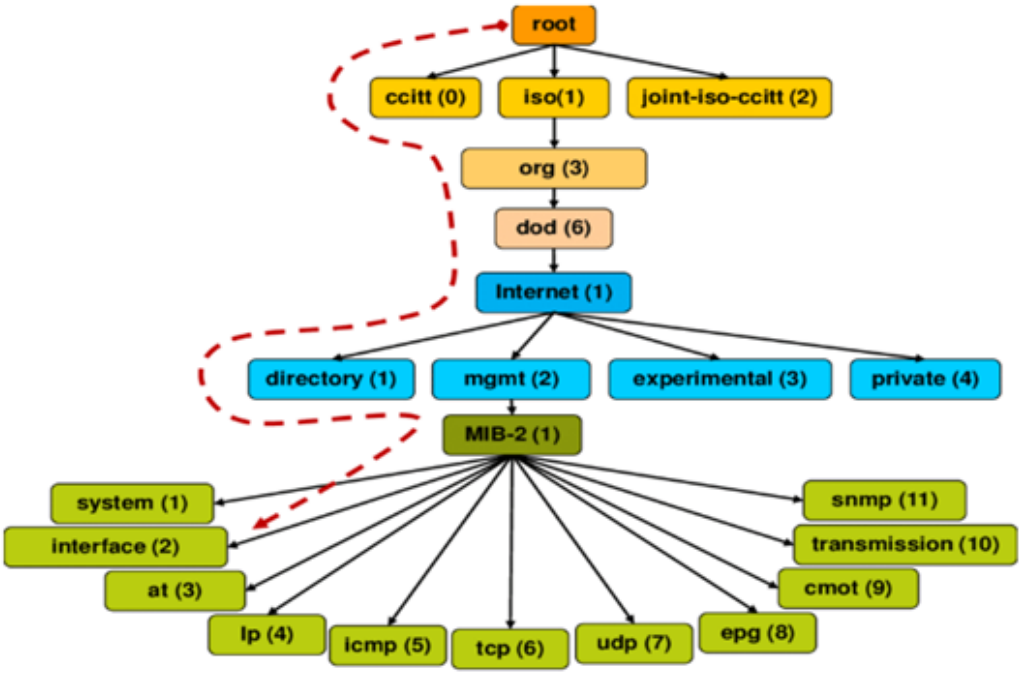

FIGURE 2.6 – Arbre MIB SNMP

2.2.9.4 Fonctionnement du protocole SNMP (Commandes SNMP)

a- Les types de requêtes du manager SNMP vers l'agent SNMP

Une requête :

Émise du manager vers un agent via le port 161 UDP, s'il veut demander ou imposer quelque chose à cet agent. La requête peut être de quatre types :

- **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 pour récupérer un nombre défini de données en une seule opération. Elle équivaut à plusieurs requêtes GET-NEXT consécutives.
- **Set Request :** le Manager SNMP met à jour une information sur un agent SNMP.

b- Les Réponses ou Alerte de l'agent vers le manager

L'agent traite la requête et émettre une réponse via le même port, si la requête est traitée avec succès, l'agent répond un **GetResponse** accompagné de la valeur demandée.

- **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.

Mais dans le cas contraire l'agent ajoutera un code d'erreur en réponse qui est l'alarme.

c- Gestion des Alarmes et Notifications

Une alarme :

Créée par un agent en cas d'événement et utilise un message transite via le port 162 UDP pour prévenir le manager, ce message peut être de type :

- **Trap :** permet à un agent de notifier un évènement. Elle est envoyée lors de la détection d'une anomalie par l'agent.

- **Inform :** assure la même fonction que les TRAPS SNMP. Contrairement à ces dernières, les paquets INFORM se démarquent par l'envoi d'un accusé de réception par le manager.

Les formes d'alarmes [14] :

- **ColdStart(0) :** redémarrage à froid du système.
- **WarmStart(1) :** redémarrage à chaud du système.
- **LinkDown(2) :** le lien réseau n'est plus opérationnel.
- **LinkUp(3) :** le lien réseau est opérationnel.
- **AuthentificationFailure(4) :** tentative d'accès à l'agent avec un mauvais nom de communauté.
- **EGPNeighboorLoss(5) :** la passerelle adjacente ne répond plus.
- **EntrepriseSpecific(6) :** alarme propre aux constructeurs.

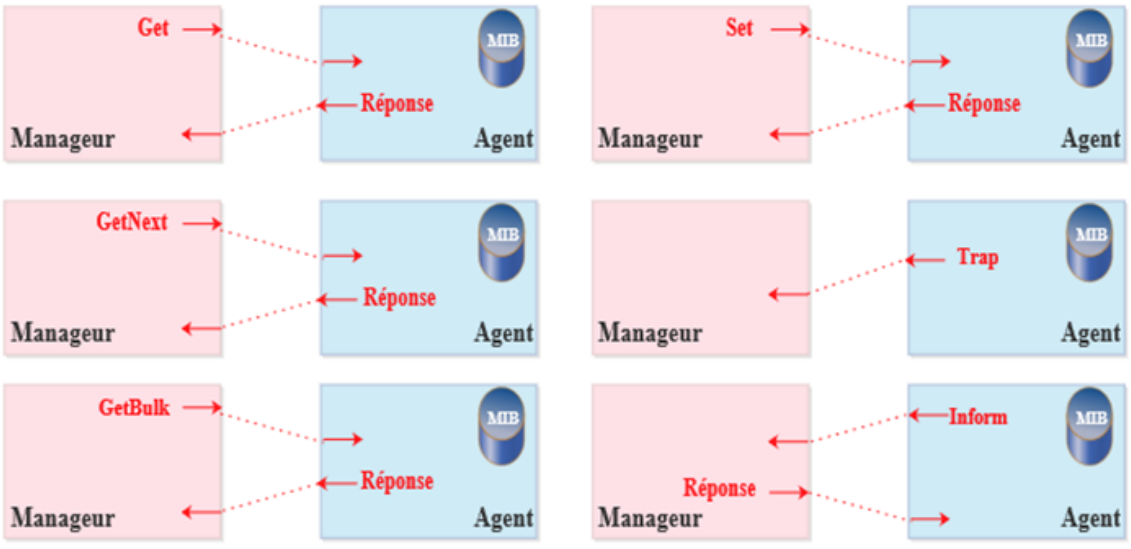

FIGURE 2.7 – Fonctionnement du Protocole SNMP

Conclusion

Pour conclure, ce chapitre nous a permis d'avoir une vue d'ensemble des réseaux informatiques et de leur sécurité, ainsi l'importance d'une gestion efficace et d'une supervision continue pour assurer la performance et la sécurité des réseaux. Dans le chapitre suivant nous allons voir les outils de supervision disponibles et les critères à suivre pour faire le bon choix.

CHAPITRE 3

CHOIX DE L'OUTIL

Introduction

Dans le domaine de la surveillance informatique, le choix de l'outil est essentiel pour garantir le bon fonctionnement et la disponibilité des systèmes et des applications.

Dans ce chapitre, nous examinerons les principales solutions disponibles, en mettant en évidence leurs caractéristiques, afin d'orienter le choix vers l'outil le plus adapté aux besoins spécifiques de surveillance.

3.1 Solutions disponibles

3.1.1 Solutions propriétaires

Les logiciels propriétaires [1] ont un support présent et réactif grâce au contrat mis en place entre le propriétaire et le client.

3.1.1.1 HP OpenView HP

C'est un logiciel de supervision. Il permet de gérer des composants d'une infrastructure informatique d'une manière standardisée.

Il est principalement utilisé pour la surveillance de serveurs, réseaux, bases de données et applications pour assurer que les défauts sont détectés et alertés dans les meilleurs délais [18].

Avantage :

- Surveillance en temps réel.
- Détection proactive des problèmes avant qu'ils n'affectent les opérations.
- Évaluer les résultats et produire des rapports afin d'améliorer la prise de décision.

1. Propriétaire : Signifie que le code source est détenu par une seule entité qui limite l'accès et la modification à ceux qui ont été autorisés, souvent par des licences payantes.

Inconvénients :

- Les coûts d'acquisition de mise à niveau et de maintenance sont assez élevés.
- La mise en place et sa gestion nécessitent une expertise.
- Avoir des problèmes de compatibilité avec d'autres systèmes de surveillance.

3.1.1.2 CiscoWorks

C'est un outil de surveillance développé par CiscoSystems, conçu pour surveiller et gérer les équipements réseau Cisco. Il est prêt à localiser les problèmes de connectivité en temps réel et à identifier leurs répercussions. L'intelligence de connectivité de CiscoWorks peut également être appliquée à d'autres systèmes de gestion des événements multi périphérique et multifournisseurs installés sur le réseau [7].

Avantage :

- Analyse automatique de la connectivité du réseau et de l'impact sur les réseaux composés [7].
- Consolidation et intégration de l'analyse de panne et de l'état opérationnel [7].
- Intégration facile avec des outils déjà utilisés par les utilisateurs [7].

Inconvénients :

- La non disponibilité des codes sources, présente un inconvénient pour la mise à jour des applications.
- Contraintes liées à la politique de licence et aux coûts associés.

3.1.2 Solution Open source

3.1.2.1 Zabbix

Solution open source [2] de supervision réseau, qui permet de surveiller en temps réel les performances et la disponibilité des systèmes informatiques.
Zabbix collecte des informations à partir d'agents installés sur les systèmes surveillés ou via des protocoles standards comme SNMP, IPMI ou JMX, puis il utilise ces données pour détecter les problèmes et envoyer des alertes [4].

2. Open source : signifie que le code source d'un logiciel est accessible à tous , et peut être utilisé, modifié et distribué librement par toute personne.

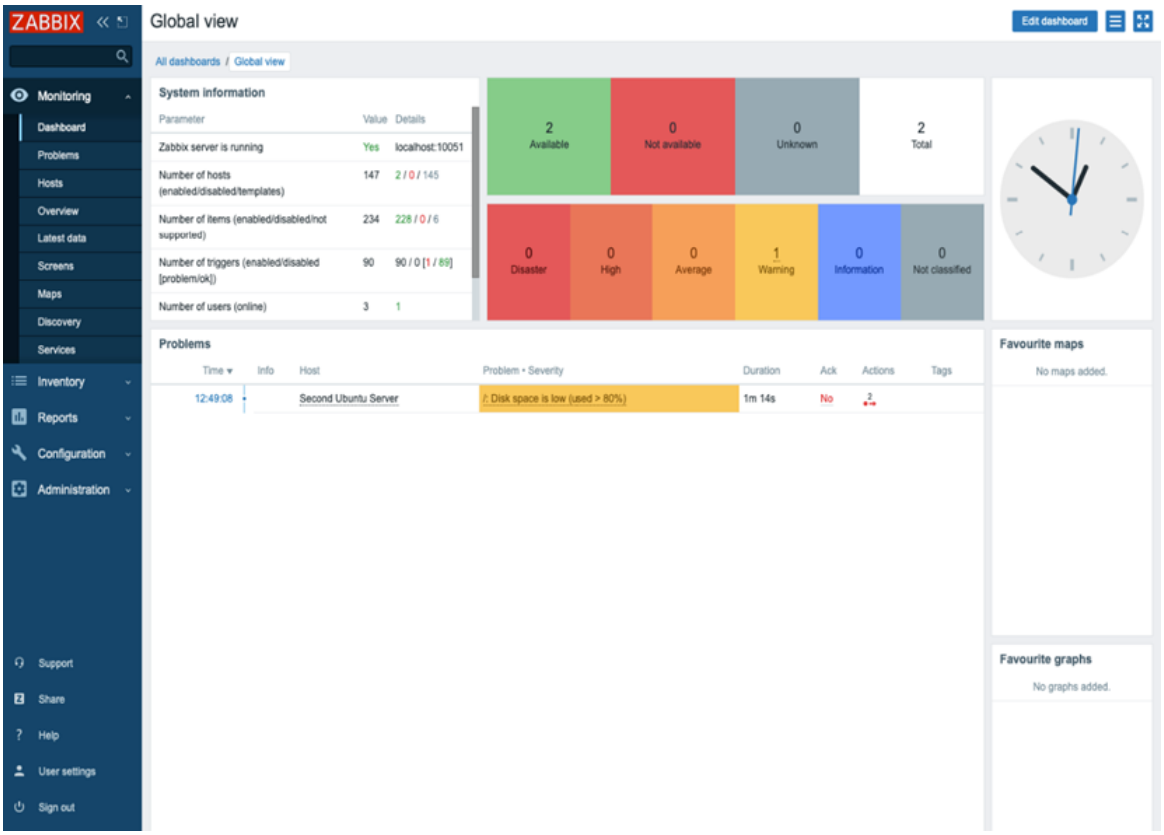

FIGURE 3.1 – Interface de Zabbix

Avantage :

- Collecte de données polyvalente.
- Alertes personnalisables.
- Ses agents sont assez légers (écrits en langage C).

Inconvénients :

- Configuration initiale complexe.
- Consommation de ressources système élevée.
- L'agent Zabbix communique par défaut en clair les informations.

3.1.2.2 Nagios

Ce logiciel de supervision open source a été créé en 1999 par Ethan Galstad. Il permet de visualiser et surveiller les équipements et leurs états, et de produire des rapports d'activité. En intégrant différentes fonctionnalités, Nagios facilite une gestion efficace des opérations informatiques, assurant ainsi la fiabilité et les performances de l'infrastructure [17].

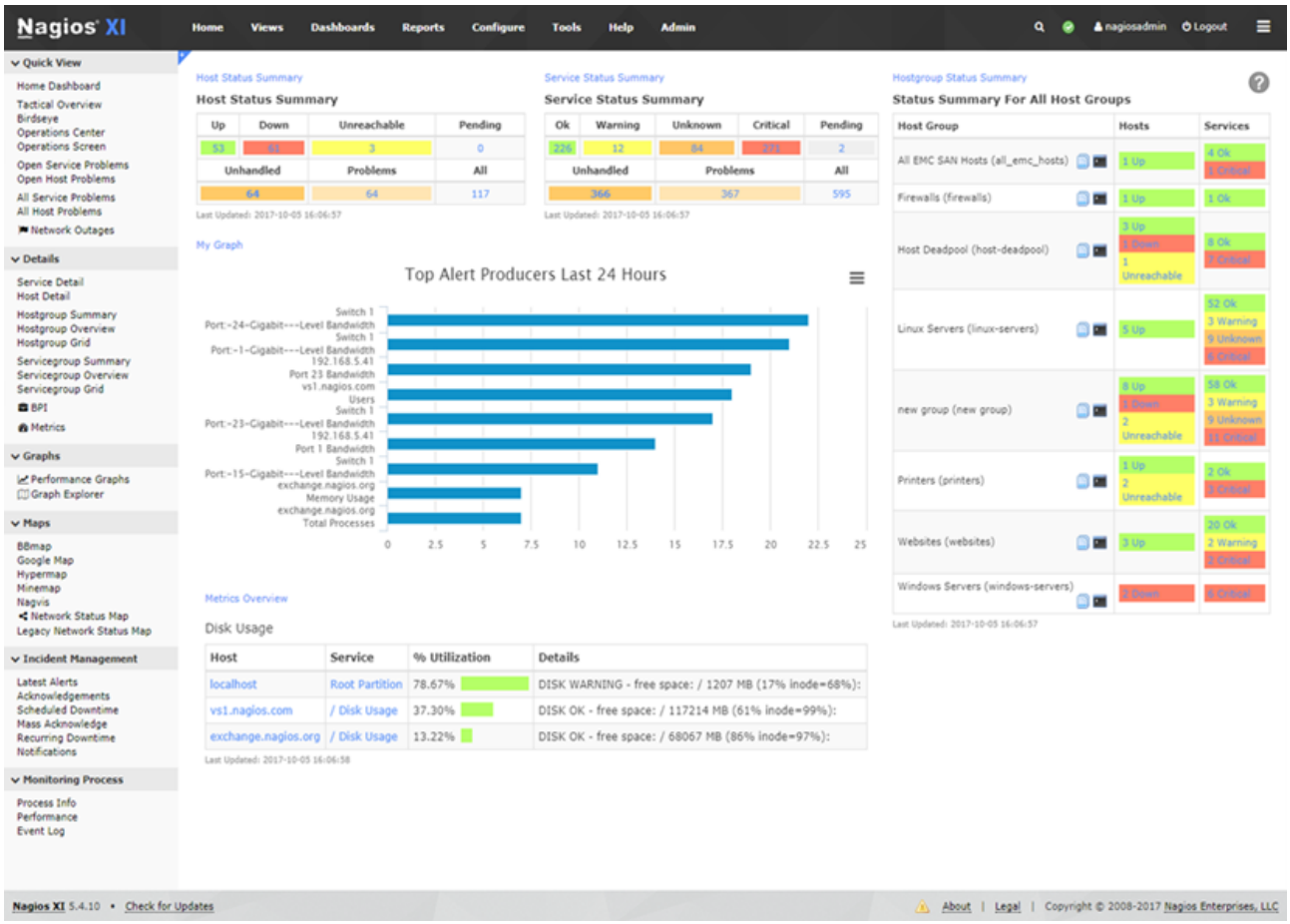

FIGURE 3.2 – Interface de Nagios

Avantage :

- La supervision à distance peut utiliser SSH.
- Offre des notifications personnalisables.
- Performances du moteur.

Inconvénients :

- Interface non ergonomique et peu intuitive.
- Ne permet pas d'ajouter des hosts via Web.
- Pour avoir toutes les fonctionnalités il faut installer des plugins [3], d'une base assez limitée.

3.1.2.3 Centreon

C'est une solution open source de supervision informatique basée sur Nagios, qui utilise les protocoles SNMP, WMI et SSH pour collecter des données de performance à partir d'équipements.

3. Plugin : est un petit programme qui apporte des fonctionnalités supplémentaires à un logiciel existant, permettant ainsi à l'utilisateur d'étendre ses capacités selon ses besoins spécifiques.

Cet outil offre des fonctionnalités avancées de visualisation, de tableau de bord et de reporting pour surveiller et gérer efficacement les infrastructures IT (Information Technology) [3].

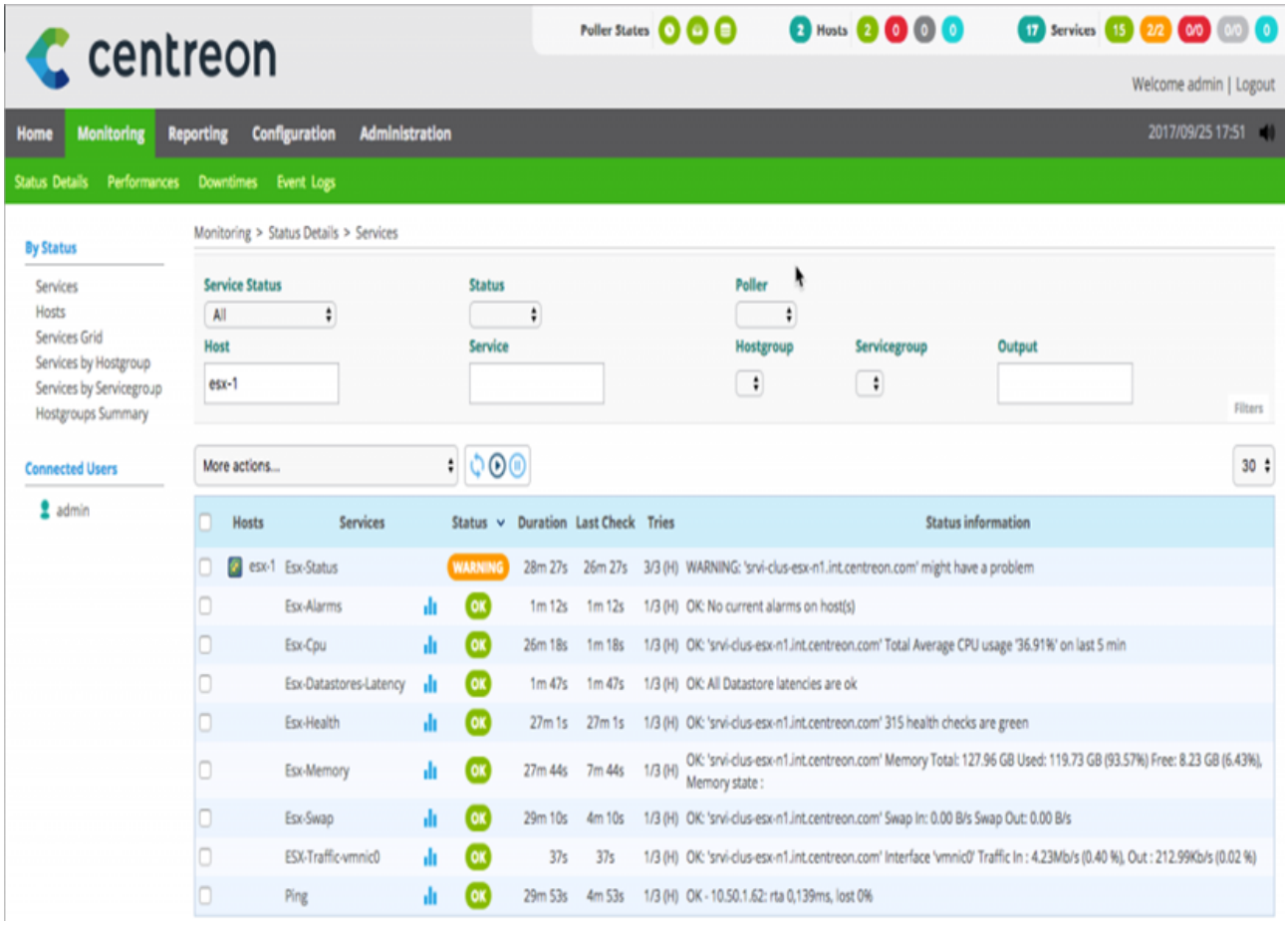

FIGURE 3.3 – Interface de Centreon

Avantage :

- Interface conviviale.
- Surveillance multi-plateforme.
- Reporting et analyse intégrés.

Inconvénients :

- Configuration complexe pour des environnements très hétérogènes.
- Dépendance à Nagios pour certaines fonctionnalités.
- Besoin de maintenir et de mettre à jour régulièrement la solution.

3.1.2.4 Prometheus

Un outil open-source de surveillance et d'alerte pour les applications et systèmes informatiques, conçu pour collecter, stocker et analyser des données de performance en temps réel [16].

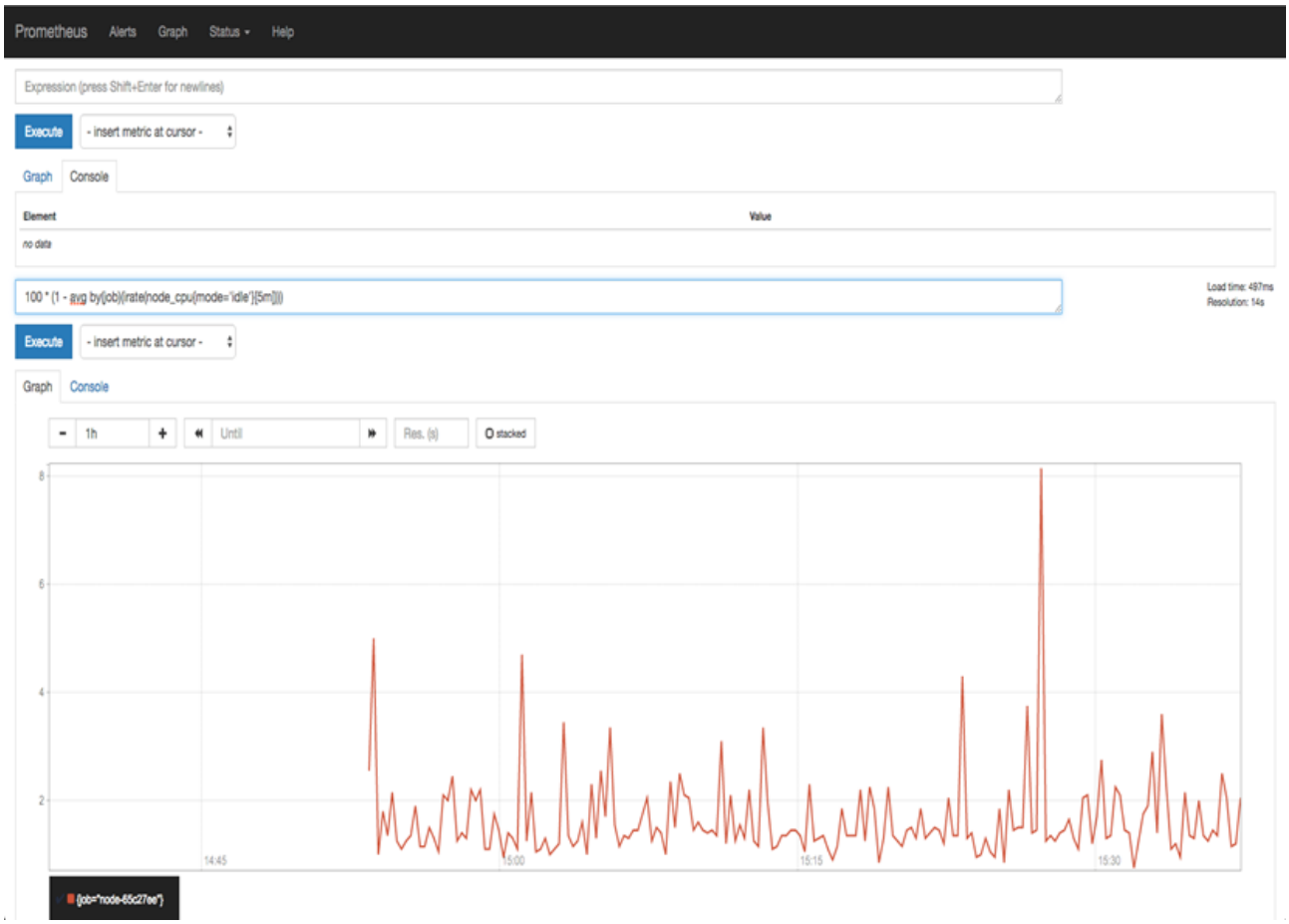

FIGURE 3.4 – Interface de Prometheus

Avantage :

- Il s'intègre à de nombreuses solutions grâce aux exportateurs tiers.
- Conçu pour des configurations de haute disponibilité.
- Détection proactive des problèmes.
- Sécurisé et extensible.

Inconvénients :

- Courbe d'apprentissage de PromQL.
- Stockage à court terme.

3.2 Tableau comparatif

Voici un tableau comparatif des outils de surveillances :

Caractéristique	Prometheus	Zabbix	Centreon	Nagios
Environnement	Linux, Windows, macOS.	Linux, Windows.	Linux.	Linux, Windows.
Capacité	Haute (TSDB pour stockage).	Bonne, divers types de métriques.	Bonne, nécessite modules supplémentaires.	Moyenne, nécessite plus de ressources.
Installation et configuration	Simple.	Moyenne.	Complexe.	Moyenne.
Langage de requête	PromQL (puissant et flexible).	SQL-like.	SQL-like.	Pas de langage spécifique.
Alerting	Intégré (Alertmanager)	Intégré (avancé)	Intégré (avancé)	Intégré (basique)
Visualisation	Intégré (via Grafana souvent)	Intégré (graphiques de base)	Intégré (graphiques de base)	Intégré (graphiques de base)
Utilisation de ressource	Efficace.	Peut devenir lourd	Peut devenir lourd	Peut devenir lourd
Sécurité	Très élevé	Élevé	Élevé	Moyen
Extension	Large (via Exporters)	Large, nombreux plugins	Large, nombreux plugins	Large, nombreux plugins

TABLE 3.1 – Comparaison entre les outils

3.3 Choix de l'outil

3.3.1 Pourquoi Utiliser Prometheus

D'après la comparaison entre les différents outils, Prometheus est le choix le plus efficace pour la surveillance des divers systèmes. De par sa flexibilité il offre une grande capacité, un langage de requêtes puissant PromQL et un système d'alertes intégré permettant une gestion proactive.

De plus, son intégration avec Grafana permet des visualisations avancées tandis que ses fonctionnalités de sécurité robustes garantissent la confidentialité et la préservation des données surveillées.

3.3.2 Présentation du Prometheus

Cet outil de surveillance et d'alerte open source est initialement développé chez SoundCloud, lancé en 2012. Il bénéficie d'une communauté de développeurs et d'utilisateurs très active. C'est pourquoi de nombreuses entreprises et organisations l'ont adopté. Pour clarifier la structure de gouvernance du projet, Prometheus a rejoint la Cloud Native Computing Foundation (CNCF) en 2016.

Prometheus est basé sur des métriques monitorsystème de gestion. Il collecte des données auprès des services et des hôtes en envoyant des requêtes HTTP aux points de terminaison de métriques. Ensuite, il stocke les résultats dans une base de données de séries chronologiques et les rend disponibles pour l'analyse et l'alerte [16].

3.3.3 Fonctionnalités de Prometheus

Les principales fonctionnalités de Prometheus sont les suivantes :

FIGURE 3.5 – Logo de Prometheus

- Un modèle de données multidimensionnel avec des données de séries temporelles identifiées par le nom de la métrique et des paires clé/valeur [16].
- PromQL, un langage de requête flexible pour exploiter cette dimensionnalité [16].
- Aucune dépendance sur un stockage distribué, les nœuds de serveur individuels sont autonomes [16].
- La collecte des séries temporelles se fait via un modèle de pull sur HTTP [16].
- La transmission de séries temporelles est prise en charge via une passerelle intermédiaire [16].
- Les cibles sont découvertes via le Service Discovery [4] ou une configuration statique [16].
- Prise en charge de plusieurs modes de graphiques et de tableaux de bord [16].

3.3.4 Métriques de Prometheus

Les métriques jouent un rôle d'une grande importance dans le bon fonctionnement de Prometheus, car elles permettent de collecter et de surveiller des données sur les performances et le comportement des systèmes et des applications. Chaque métrique est une série temporelle identifiée par un nom unique et des labels, offrant ainsi un contexte bien précis [16].

Il existe quatre types de métriques :

- **Compteur :** est utile pour les valeurs uniquement croissantes ou les valeurs peuvent être remises à zéro au redémarrage. Utilisés pour suivre le nombre d'événements (nombre total de requêtes http).
- **Jauge :** valeur numérique unique utilisées pour mesurer des valeurs qui peuvent augmenter ou diminuer, comme la charge CPU ou la mémoire utilisée.
- **Histogramme :** échantillonne les observations, telles que la durée des demandes ou la taille des réponses. Il les compte dans des compartiments configurables, tout en offrant la somme de toutes les valeurs observées.

4. Service Discovery : processus automatique de localisation et de configuration des cibles à surveiller sans avoir à les spécifier manuellement.

- **Résumé :** tout comme un histogramme, un résumé d'échantillons d'observations offre un décompte total des observations et la somme des valeurs observées, tout en calculant des quantiles configurables sur une fenêtre temporelle glissante.

3.3.5 Composants de Prometheus

Le système de Prometheus est constitué de plusieurs composants :

- **Serveur Prometheus :** est le serveur principal, qui récupère et stocke les données de séries temporelles [16].

- **Agent d'exposition (Exporter) :** ce sont des processus ou des bibliothèques intégrés aux applications ou aux systèmes pour exposer leurs métriques au format Prometheuse. Ils peuvent être spécifiques à une application (Exporter pour MySQL, Node Exporter pour les serveurs Linux, etc.) ou généraux (Exporter SNMP, Exporter JMX, etc.) [16].

- **Passerelle de push :** il prend en charge les tâches de courte durée [16].

- **Base de données de séries temporelles (Time Series Database :** stocke les métriques collectées de manière efficace pour un accès rapide [16].

- **Langage de requête PromQL (Prometheus Query Language) :** est un langage de requête pour interroger les données de surveillance stockées dans Prometheus [16].

- **Interface utilisateur (Prometheus Web UI) :** est une interface utilisateur Web qui permet aux utilisateurs d'explorer les métriques collectées, de construire et d'exécuter des requêtes PromQL, et de visualiser les résultats [16].

- **Gestionnaire d'alerte (Alertmanager) :** gère les alertes générées, définit des règles et de router les alertes vers différents canaux de notification [16].

3.3.6 Intégration de Grafana avec Prometheus

3.3.6.1 Définition

Grafana est un logiciel open-source créé en 2014 par Torkel Ödegaard, conçu pour la surveillance et l'analyse en temps réel des données provenant de diverses sources. Comme des bases de données de séries temporelles, des services de monitoring comme Prometheus. Cette solution offre la possibilité de concevoir des tableaux de bord personnalisés, incluant des graphiques et des diagrammes, ainsi que la configuration d'alertes personnalisées afin de répondre efficacement à des besoins spécifiques d'analyse de données [2].

3.3.6.2 Avantages d'intégration

L'intégration de Prometheus avec Grafana est une combinaison puissante pour la surveillance et la visualisation des métriques de performance des systèmes et applications. Voici les avantages de cette intégration :

- Il permet la collecte et le stockage des métriques pour une analyse ultérieure.
- Grafana offre une variété d'options de visualisation pour afficher les métriques collectées en créant des tableaux de bord personnalisés avec des graphiques interactifs, des diagrammes à barres.
- Prometheus peut être configuré pour envoyer des alertes, et Grafana peut les gérer et les intégrer avec des services tiers.
- Grafana permet de sécuriser l'accès aux données de Prometheus en mettant en place des mécanismes d'authentification et d'autorisation.
- Grafana offre une capacité robuste, permettant de gérer efficacement des charges de travail croissantes grâce à une architecture évolutive et à une utilisation efficace des ressources.

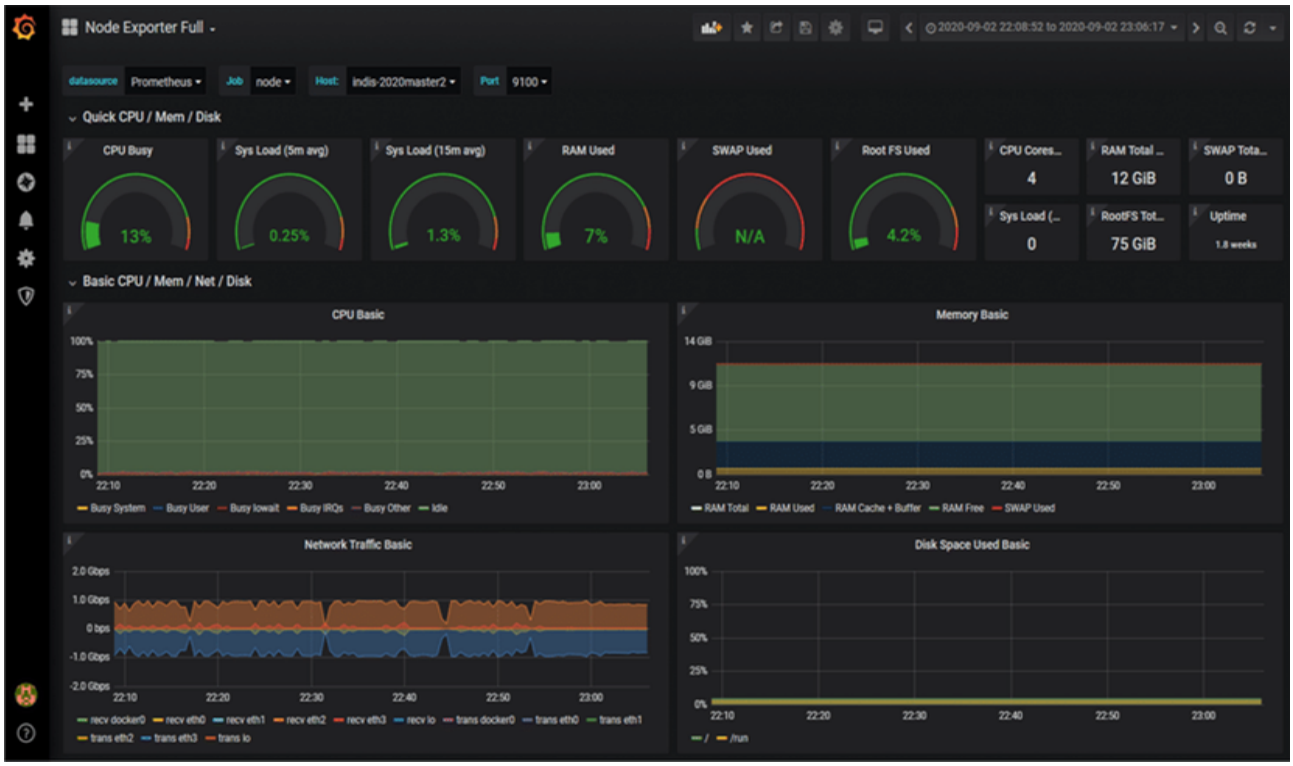

FIGURE 3.6 – Interface de Grafana

3.3.7 Architecture de Prometheus

Ce diagramme illustre l'architecture de Prometheus et certains de ses composants d'écosystème [16] :

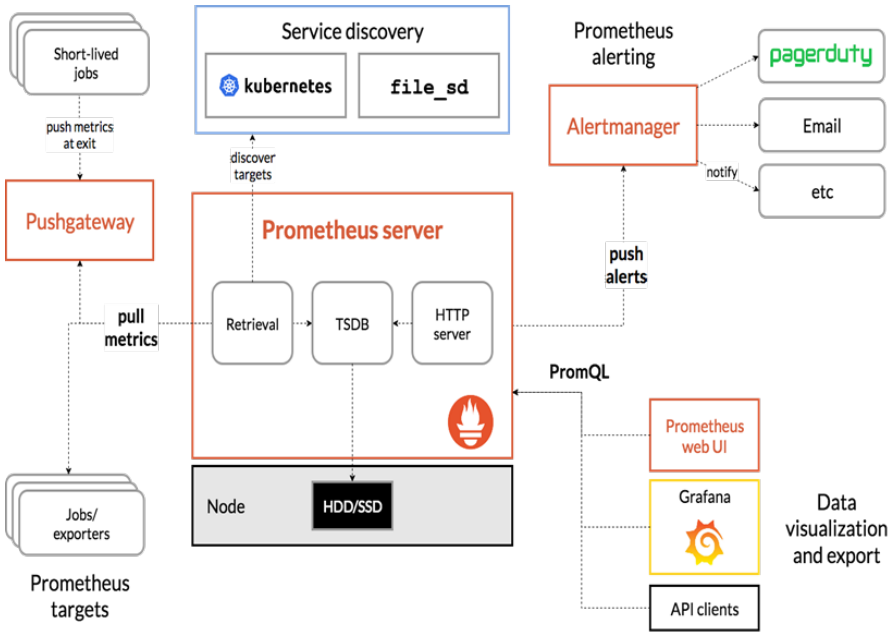

FIGURE 3.7 – Architecture de Prometheus

3.3.8 Fonctionnement de Prometheus

- **Collecte de métriques :** prometheus collecte régulièrement les métriques des cibles configurées (Applications, Serveurs, Conteneurs Docker et Bases de Données) en utilisant un point de terminaison HTTP fourni par ces cibles, où les métriques sont disponibles en format texte ou en format Prometheus.

  Cette collecte se fait en deux méthodes :

  Pull : c'est la méthode principale où le serveur récupère activement les métriques.
  Push : les cibles envoient leurs métriques au serveur via un intermédiaire appelé "push gateway".

  Ces métriques collectées sont stockées dans une base de données de séries temporelles.

- **Interrogation des métriques :** les utilisateurs peuvent interroger les données de métriques en utilisant langage de requête PromQL (Prometheus Query Language) qui permet de les sélectionner, agréger et manipuler.

  Les résultats des requêtes peuvent être visualisés dans l'interface ou exportés vers Grafana.

- **Moteur d'alerte intégré :** prometheus génère des règles d'alerte qui se déclenchent en cas de conditions anormales, envoyant ensuite des notifications via divers canaux tels que l'e-mail.

Conclusion

Après avoir étudié les différentes solutions de surveillance informatique, nous avons conclu que Prometheus est l'outil le plus adapté à nos besoins spécifiques.

Dans le chapitre suivant, nous aborderons la mise en place de Prometheus en décrivant les étapes d'installation, configuration et de son utilisation.

CHAPITRE 4

RÉALISATION ET ÉMULATION

4.1 Introduction

Dans ce chapitre, nous exposerons l'environnement de travail nécessaire pour la simulation et la mise en place d'une solution de supervision avec Prometheus. Nous aborderons l'installation des outils de simulation et des machines virtuelles, ainsi que les équipements matériels et logiciels essentiels. Ensuite, nous présenterons l'architecture du réseau et la méthode de configuration. Enfin, nous expliquerons comment installer Prometheus et son intégration avec Grafana afin de garantir un suivi efficace des performances et une gestion optimale des infrastructures réseau.

4.2 Présentation de l'environnement de travail

4.2.1 Outils de simulation

4.2.1.1 Définition GNS3 sous Windows

Graphic Network Simulator est un logiciel open source utilisé en informatique réseau pour concevoir, tester et dépanner des réseaux virtuels et réels. Il permet de créer des topologies réseau complexes en simulant divers équipements, tels que des routeurs et des commutateurs, et en intégrant des machines virtuelles.

FIGURE 4.1 – Logo GNS3.

4.2.1.2 Définition VMware Workstation pro

C'est un logiciel de virtualisation complet qui permet de créer et de gérer des machines virtuelles sur un seul ordinateur. Il offre un environnement puissant et flexible pour exécuter plusieurs systèmes d'exploitation simultanément, ce qui facilite le test d'applications, la configuration d'environnements de développement et le déploiement de solutions logicielles.

FIGURE 4.2 – Logo VMware.

4.2.2 Equipements hardware et software

— Routeur : C'est un équipement informatique qui permet de diriger le trafic des données entre différents réseaux ou sous-réseaux. Il fonctionne à la couche réseau du modèle OSI et utilise des tables de routage pour déterminer le chemin optimal pour transférer les paquets de données vers leur destination.

— Switch : ou commutateur, est un dispositif de réseau qui relie plusieurs appareils au sein d'un réseau local (LAN). Il reçoit des données d'un appareil et les envoie uniquement à l'appareil destinataire. Cela favorise une communication efficace et rapide entre les dispositifs du réseau.

— Pfsense : C'est un logiciel open-source qui fonctionne à la fois comme un pare-feu et un routeur afin de gérer et de sécuriser les réseaux. Il est basé sur le système d'exploitation FreeBSD (Free Berkeley Software Distribution) et peut être installé sur du matériel informatique ou des machines virtuelles.

— Ubuntu Desktop : la version conviviale du système d'exploitation Ubuntu. Elle propose une interface utilisateur basée sur GNOME ainsi qu'une sélection complète de logiciels préinstallés, couvrant les besoins courants comme la navigation web, la gestion de fichiers et la création de documents.

— Serveur ESXi : Un hyperviseur de type 1 de VMware permettant de créer et gérer des machines virtuelles directement sur le matériel d'un serveur, optimisant ainsi les ressources et simplifiant la gestion des infrastructures informatiques.

— VMware VSphere : plateforme de virtualisation de data center qui simplifie la gestion des infrastructures IT en permettant la création, la gestion et la migration des machines virtuelles sur des serveurs physiques.

4.2.3 Description des équipements

Équipements	Fournisseur	Nom de l'équipement	Système	Caractéristiques
Routeur L3	Cisco	R1	IOS	Routage entre réseaux
Switch L2	Cisco	SWD	IOS	Transfert local,VLANs
Switch catalyst 2960	Cisco	USER et SW_SER	IOS	VLANs
Pare-feu	Netgate	Pfsense	FreeBSD	Contrôle de trafic

TABLE 4.1 – Tables des équipements.

4.2.4 Architecure proposée

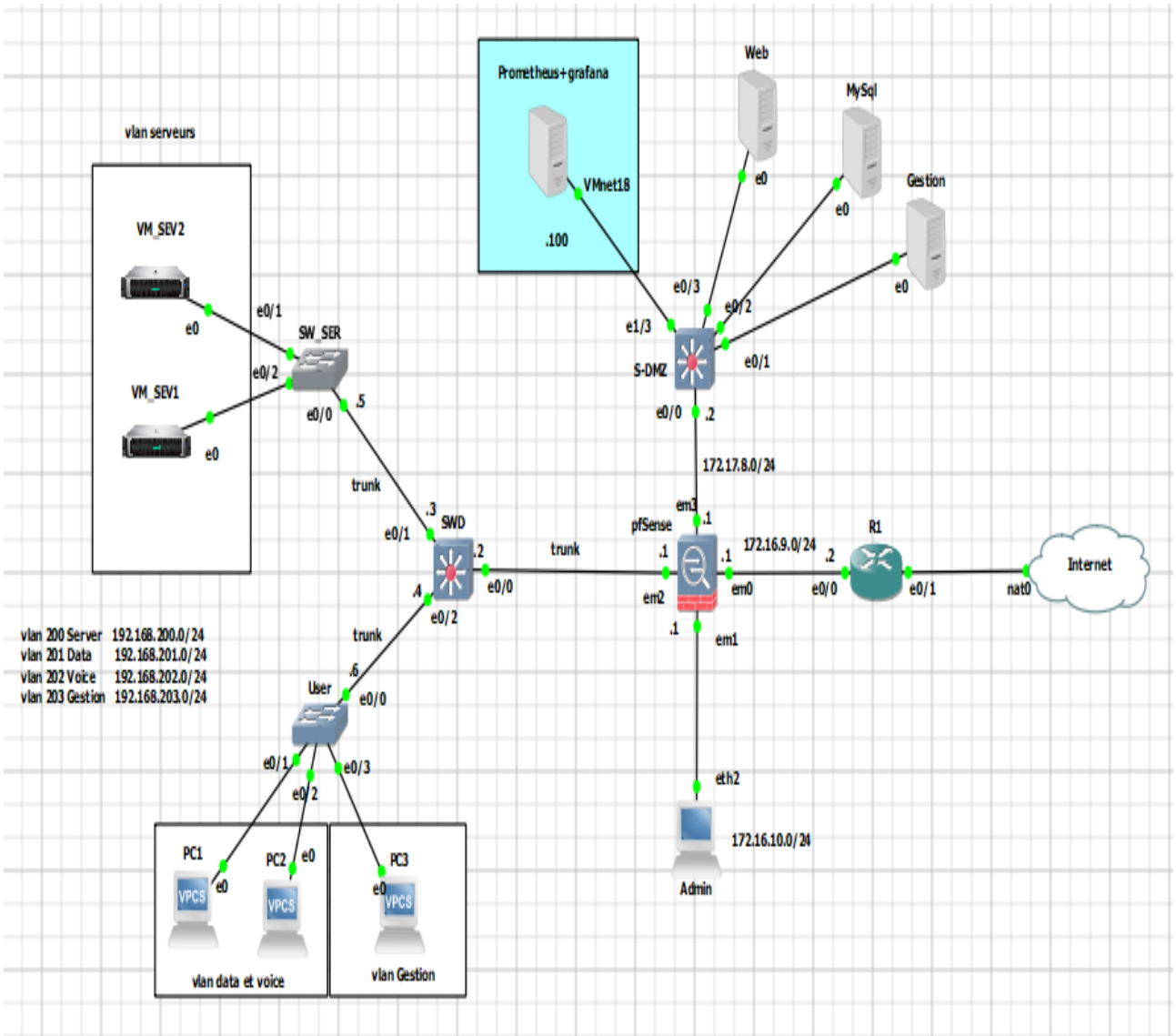

FIGURE 4.3 – Architecture du réseau proposée.

4.3 Méthodologie de configuration

4.3.1 Tableau d'adressage

Nom d'équipement	Interfaces	Adresse IP	Description
Routeur	E0/0	172.16.9.2/24	Connecté au Pfsense
	E0/1	Nat	Connecté à l'internet
Pfsense	em0	172.16.9.1/24	Connecté au Routeur
	em1	172.16.10.1/24	Connecté à l'administration
	em2	En mode Trunk	Connecté au SWD
	em3	172.17.8.1/24	Connecté à la DMZ
Admin	eth2	172.16.10.2/24	Connecté au Pfsense
S-DMZ	E0/0	172.17.8.2/24	Connecté au Pfsense
	E0/1	En mode Access	Connecté au Gestion
	E0/2	En mode Access	Connecté au MySql
	E0/3	En mode Access	Connecté au Web
	E1/3	En mode Access	Connecté au Prometheus+Grafana
Prometheus+Grafana	VMnet18	172.17.8.100/24	Connecté à la DMZ
SWD	E0/0	En mode Trunk	Connecté au Pfsense
	E0/1	En mode Trunk	Connecté au SW_SER
	E0/2	En mode Trunk	Connecté au User
SW_SER	E0/0	En mode Trunk	Connecté au SWD
	E0/1	En mode Access	Connecté au VM_SER2 (VLAN200 Serveur)
	E0/2	En mode Access	Connecté au VM_SER1 (VLAN200 Serveur)
User	E0/0	En mode Trunk	Connecté au SWD
	E0/1	En mode Access	Connecté au Vlan201 Data
	E0/2	En mode Access	Connecté au Vlan202 Voice
	E0/3	En mode Access	Connecté au Vlan203 Gestion

TABLE 4.2 – L'adressage.

4.3.2 Tableau d'adressage des Vlans et routage inter Vlan

Nom de Vlan	Id du Vlan	L'adresse IP	gateway
Vlan Server	200	192.168.200.0/24	192.168.200.1
Vlan Data	201	192.168.201.0/24	192.168.201.1
Vlan Voice	202	192.168.202.0/24	192.168.202.1
Vlan Gestion	203	192.168.203.0/24	192.168.203.1

TABLE 4.3 – Tableau d'adressage des Vlans et routage inter Vlan.

Phase 1 : Les installations

4.4 Installation des outils logiciels

4.4.1 Installation Prometheus

Étape 01 : Mettre à jour la liste des paquets

Pour mettre à jour la liste des paquets disponibles et installer les mises à jour des paquets déjà présents sur le système afin d'assurer que le logiciel reste à jour et sécurisé, nous utilisons les commandes illustrées dans la figure suivante :

```
monitor@monitor-prometheus:~$ sudo apt update
[sudo] Mot de passe de monitor :
Atteint :1 http://fr.archive.ubuntu.com/ubuntu focal InRelease
Atteint :2 http://security.ubuntu.com/ubuntu focal-security InRelease
Réception de :3 http://fr.archive.ubuntu.com/ubuntu focal-updates InRelease [128
 kB]
Atteint :4 http://fr.archive.ubuntu.com/ubuntu focal-backports InRelease
128 ko réceptionnés en 12s (11,0 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
monitor@monitor-prometheus:~$ sudo apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

FIGURE 4.4 – Mise à jour des paquets

Pour créer un utilisateur, un groupe et un répertoire appelés Prometheus, nous devons exécuter les commandes illustrées dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ sudo useradd --no-create-home --shell /bin/false p
rometheus
monitor@monitor-prometheus:~$ sudo mkdir /etc/prometheus
monitor@monitor-prometheus:~$ sudo mkdir /var/lib/prometheus
monitor@monitor-prometheus:~$ sudo chown prometheus:prometheus /etc/prometheus
monitor@monitor-prometheus:~$ sudo chown prometheus:prometheus /var/lib/promethe
us
```

FIGURE 4.5 – Création de l'utilisateur et des répertoires pour Prometheus

Étape 02 : Télécharger Prometheus

Nous téléchargeons le fichier d'archive prometheus-2.27.1.linux-amd64.tar.gz depuis le site GitHub de Prometheus. La commande exacte est comme dans la figure :

```
monitor@monitor-prometheus:~$ wget https://github.com/prometheus/prometheus/rele
ases/download/v2.27.1/prometheus-2.27.1.linux-amd64.tar.gz
```

FIGURE 4.6 – Téléchargement de Prometheus v2.27.1

Après avoir exécuté la commande précédente, nous nous assurons que notre fichier est authentique et non corrompu. Ensuite, nous extrayons le contenu de l'archive comme illustré dans la figure suivante :

```
monitor@monitor-prometheus:~$ tar -xvf prometheus-2.27.1.linux-amd64.tar.gz
prometheus-2.27.1.linux-amd64/
prometheus-2.27.1.linux-amd64/consoles/
prometheus-2.27.1.linux-amd64/consoles/index.html.example
prometheus-2.27.1.linux-amd64/consoles/node-cpu.html
prometheus-2.27.1.linux-amd64/consoles/node-disk.html
prometheus-2.27.1.linux-amd64/consoles/node-overview.html
prometheus-2.27.1.linux-amd64/consoles/node.html
prometheus-2.27.1.linux-amd64/consoles/prometheus-overview.html
prometheus-2.27.1.linux-amd64/consoles/prometheus.html
prometheus-2.27.1.linux-amd64/console_libraries/
prometheus-2.27.1.linux-amd64/console_libraries/menu.lib
prometheus-2.27.1.linux-amd64/console_libraries/prom.lib
prometheus-2.27.1.linux-amd64/prometheus.yml
prometheus-2.27.1.linux-amd64/LICENSE
prometheus-2.27.1.linux-amd64/NOTICE
prometheus-2.27.1.linux-amd64/prometheus
prometheus-2.27.1.linux-amd64/promtool
```

FIGURE 4.7 – Extraction du contenu de l'archive prometheus-2.27.1

La commande « ls » est utilisée pour lister le contenu d'un répertoire dans un système de fichiers. Elle affiche les fichiers et sous-répertoires présents dans le répertoire courant ou dans un répertoire spécifié comme c'est illustré dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ ls
Bureau     Modèles                                Public
Documents  Musique                                Téléchargements
Images     prometheus-2.27.1.linux-amd64.tar.gz   Vidéos
monitor@monitor-prometheus:~$
```

FIGURE 4.8 – Affichage du contenu du répertoire avec la commande `ls`

Nous accédons au dossier Prometheus avec la commande « cd » et utilisons « ls » pour voir le contenu du dossier. Nous voyons deux fichiers binaires (prometheus et promtool) comme indiqué dans la figure ci-dessous.

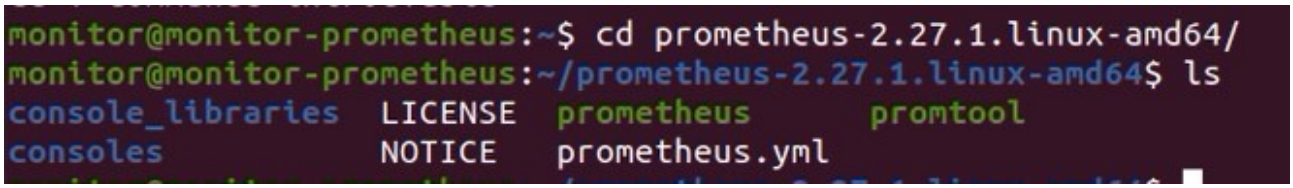

FIGURE 4.9 – Affichage des fichiers binaires

Étape 03 : Copier les fichiers binaires de Prometheus

Cette commande est utilisée pour déplacer des fichiers et des répertoires vers des emplacements spécifiques avec des privilèges administratifs (sudo). Comme dans la figure suivante :

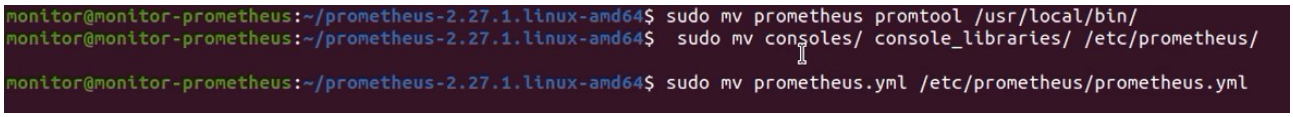

FIGURE 4.10 – Déplacement des fichiers

Prometheus a été installé avec succès sur le système. Nous confirmons la version installée en utilisant les commandes dans la figure suivante :

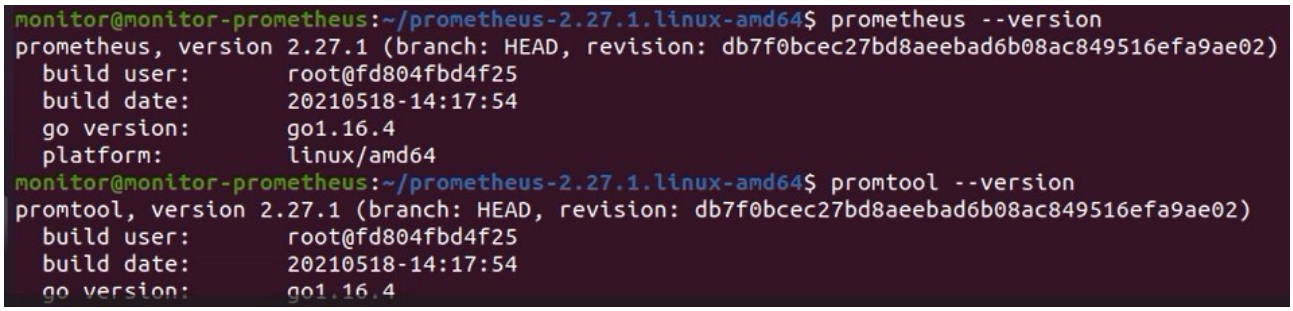

FIGURE 4.11 – Affichage de la version Prometheus

Enfin, nous démarrons et activons le service Prometheus. Comme c'est illustré dans la figure ci-dessous :

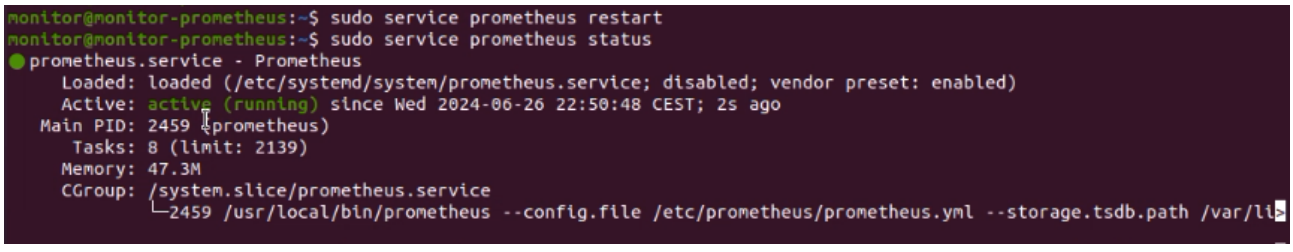

FIGURE 4.12 – Activation du service Prometheus

Après l'installation et la configuration, nous avons accédé à l'interface via un navigateur web en utilisant l'adresse IP. Voici l'interface qui s'est affichée :

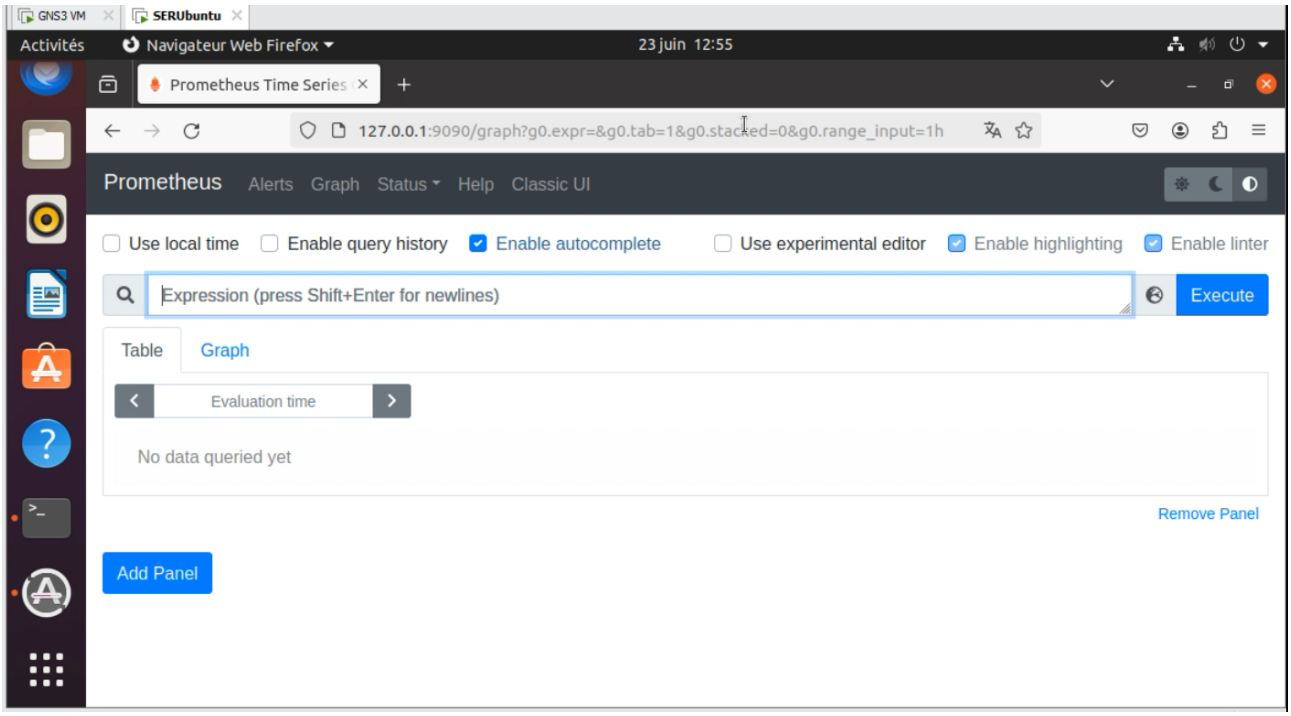

FIGURE 4.13 – Interface de Prometheus

4.4.2 Installation Grafana

Étape 01 : Installer les paquets prérequis

Ces paquets sont indispensables pour faciliter l'installation et la gestion de logiciels supplémentaires, ainsi que pour assurer le téléchargement sécurisé des paquets via http. Les étapes sont illustrées dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ sudo apt-get install -y apt-transport-https software-properties-common wget
[sudo] Mot de passe de monitor :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
software-properties-common est déjà la version la plus récente (0.99.9.12).
software-properties-common passé en « installé manuellement ».
wget est déjà la version la plus récente (1.20.3-1ubuntu2).
wget passé en « installé manuellement ».
Les NOUVEAUX paquets suivants seront installés :
  apt-transport-https
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1 704 o dans les archives.
Après cette opération, 162 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://fr.archive.ubuntu.com/ubuntu focal-updates/universe amd64 apt-transport-https all 2.0.10 [1 704
B]
1 704 o réceptionnés en 0s (5 417 o/s)
Sélection du paquet apt-transport-https précédemment désélectionné.
(Lecture de la base de données... 184257 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../apt-transport-https_2.0.10_all.deb ...
Dépaquetage de apt-transport-https (2.0.10) ...
Paramétrage de apt-transport-https (2.0.10) ...
```

FIGURE 4.14 – Installation des paquets

Étape 02 : Importer la clé GPG

Afin de créer un répertoire et de télécharger la clé GPG du référentiel Grafana, nous tapons les commandes dans la figure suivante :

```
monitor@monitor-prometheus:~$ sudo mkdir -p /etc/apt/keyrings/
monitor@monitor-prometheus:~$ wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings
/grafana.gpg > /dev/null
```

FIGURE 4.15 – Téléchargement de la Clé GPG

Étape 03 : Ajouter des Dépôts

Pour ajouter des dépôts pour les versions stables, bêta et mettre à jour la liste des paquets disponibles, nous suivons les étapes dans la figure :

```
monitor@monitor-prometheus:~$ echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main"
| sudo tee -a /etc/apt/sources.list.d/grafana.list
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main
monitor@monitor-prometheus:~$ echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com beta main" |
sudo tee -a /etc/apt/sources.list.d/grafana.list
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com beta main
monitor@monitor-prometheus:~$ sudo apt-get update
```

FIGURE 4.16 – Ajout des dépôts

Étape 04 : Installer Grafana

La figure ci-dessous illustre le processus d'installation de Grafana sur un système Linux en utilisant la commande `apt-get` :

```
monitor@monitor-prometheus:~$ sudo apt-get install grafana
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  musl
Les NOUVEAUX paquets suivants seront installés :
  grafana musl
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 115 Mo/115 Mo dans les archives.
Après cette opération, 428 Mo d'espace disque supplémentaires seront util
```

FIGURE 4.17 – Installation de Grafana

Enfin, nous démarrons et activons le service Grafana. Comme c'est illustré dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ grafana-server -v
Version 11.0.0 (commit: 277ef258d4b9a5acdf2932347c6a4ca72d739b28, branch: HEAD)
monitor@monitor-prometheus:~$ sudo systemctl start grafana-server
monitor@monitor-prometheus:~$ sudo systemctl enable grafana-server
Synchronizing state of grafana-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /lib/systemd/system/grafana-server
.service.
monitor@monitor-prometheus:~$ sudo systemctl status grafana-server
● grafana-server.service - Grafana instance
     Loaded: loaded (/lib/systemd/system/grafana-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-06-23 14:12:13 CEST; 15s ago
       Docs: http://docs.grafana.org
   Main PID: 5067 (grafana)
      Tasks: 15 (limit: 2139)
     Memory: 49.6M
     CGroup: /system.slice/grafana-server.service
             └─5067 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/gra
```

FIGURE 4.18 – Activation du service Grafana

Après l'installation et la configuration, nous avons accédé à l'interface via un navigateur web en utilisant l'adresse IP. Voici un aperçu de l'interface qui s'est affichée :

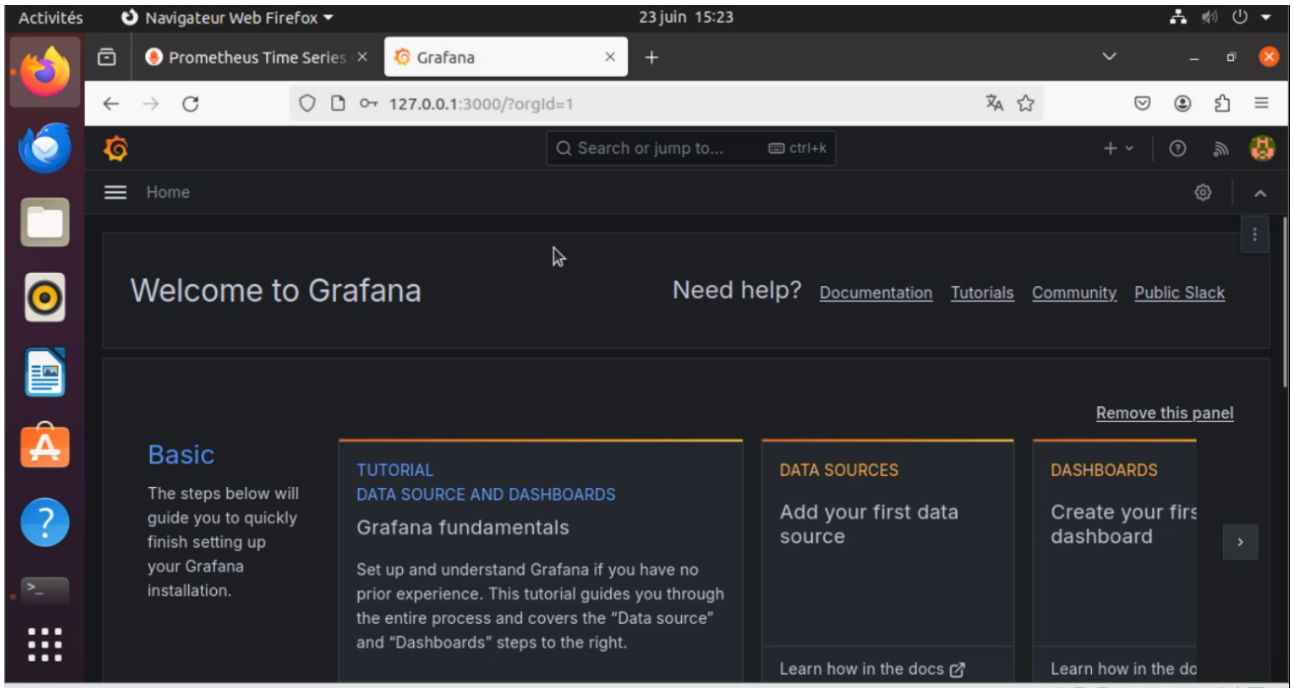

FIGURE 4.19 – Interface de Grafana

4.4.3 Installation AlertManager

Étape 01 : Création d'un User

Pour créer un utilisateur système nommé alertmanager sans répertoire personnel et sans accès au shell, nous exécutons la commande dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ sudo useradd --no-create-home --shell /bin/false a
lertmanager
[sudo] Mot de passe de monitor :
monitor@monitor-prometheus:~$
```

FIGURE 4.20 – Création d'un User

Étape 02 : Création d'un répertoire de conf et datas

```
monitor@monitor-prometheus:~$ sudo mkdir /etc/alertmanager
monitor@monitor-prometheus:~$ sudo mkdir -p /var/lib//alertmanager/data
monitor@monitor-prometheus:~$ sudo chown alertmanager:alertmanager /var/lib/alertmanager/data
monitor@monitor-prometheus:~$
```

FIGURE 4.21 – Création d'un répertoire

Étape 03 : Téléchargement et installation

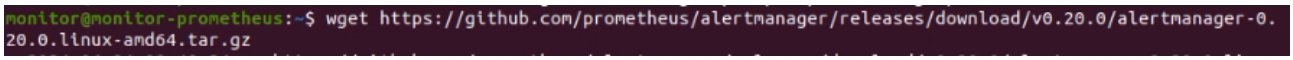

FIGURE 4.22 – Installation d'AlertManager

Ces commandes : ls, tar -xzvf, et cd alertmanager sont utilisées pour lister le contenu d'un répertoire, extraire les fichiers d'une archive compressée, et changer le répertoire courant vers alertmanager, respectivement :

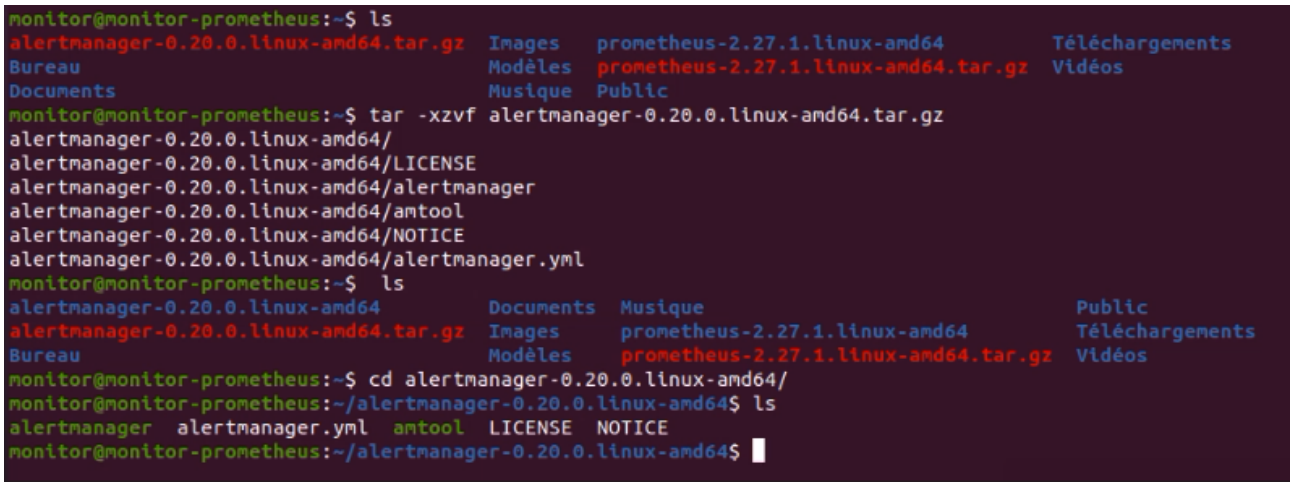

FIGURE 4.23 – Gestion des fichiers et répertoires

Étape 04 : Placer les binaires dans le chemin

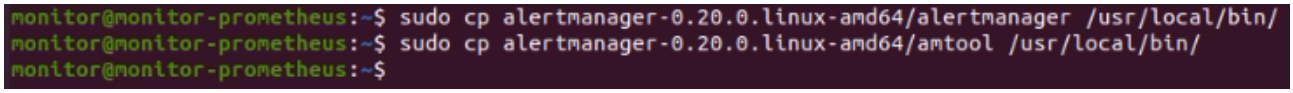

FIGURE 4.24 – Commande CP

Étape 05 : Changement des droits

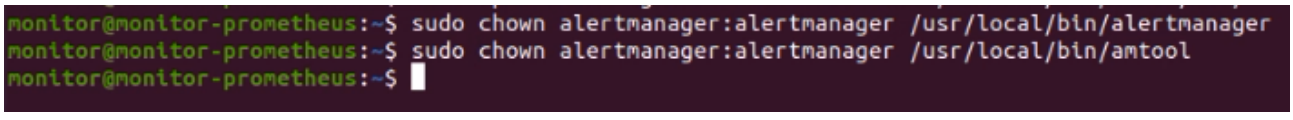

FIGURE 4.25 – Commande chown

Après l'installation et configuration d'AlertManager, ainsi que l'activation du port 9093 dans le fichier prometheus.yml, nous pouvons accéder à son interface via un navigateur en effectuant l'adresse avec le port comme c'est illustré dans la figure suivante :

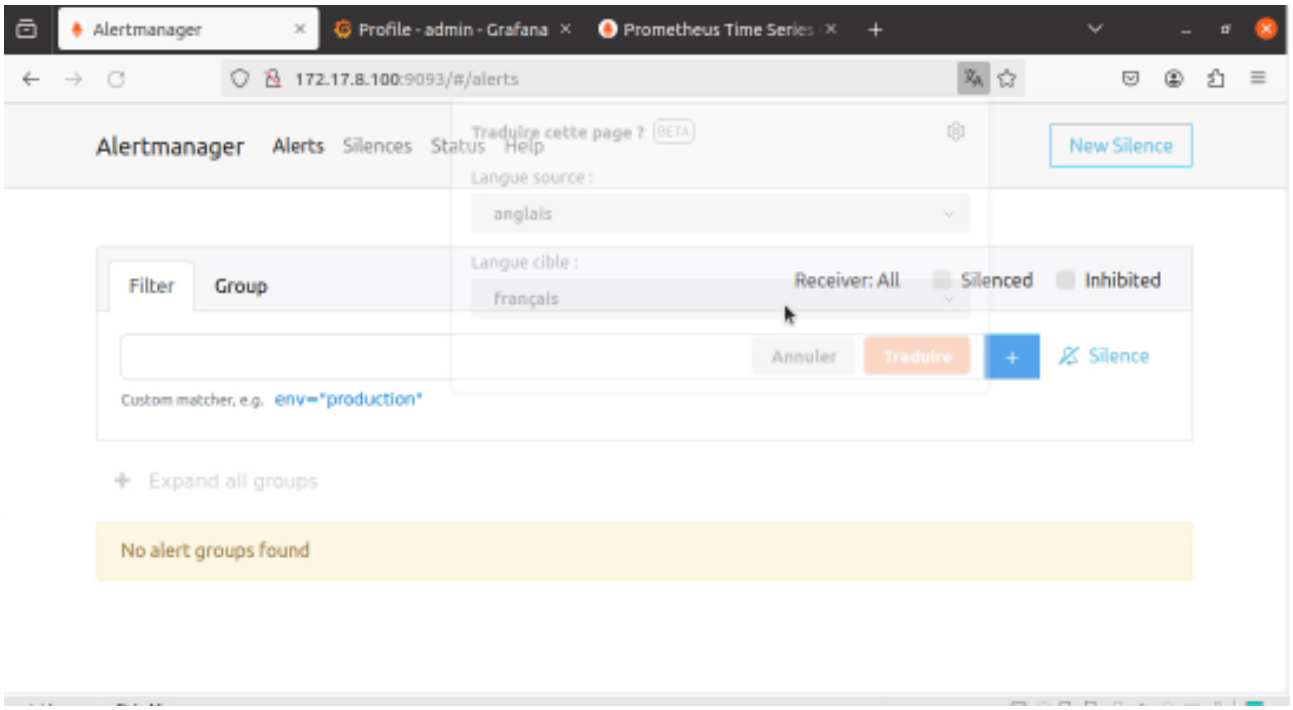

FIGURE 4.26 – Interface AlertManager

4.4.4 Installation SNMP Exporter

Pour installer SNMP Exporter, nous exécutons la commande illustrée dans la figure suivante :

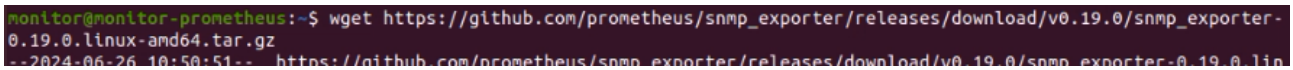

FIGURE 4.27 – Installation du SNMP Exporter

Après avoir exécuté la commande précédente, nous extrayons le contenu de l'archive en exécutant les commandes dans la figure suivante :

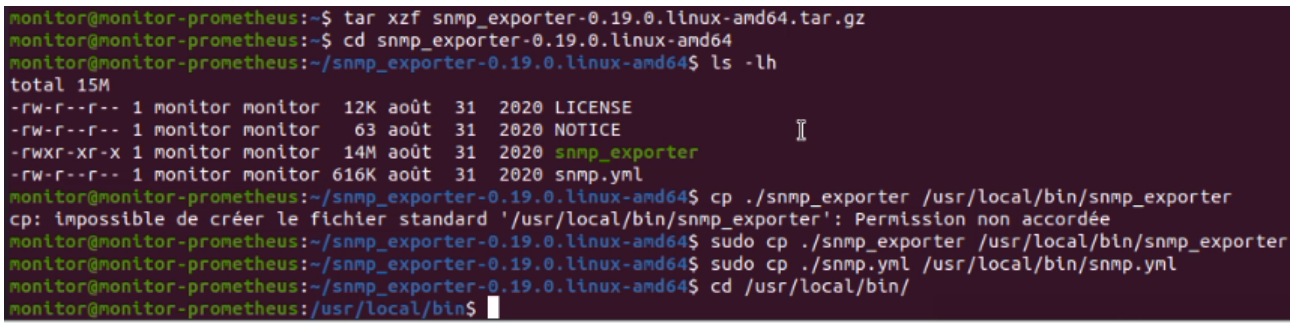

FIGURE 4.28 – Extraction du contenu de l'archive Snmp Exporter

Pour ouvrir et modifier le fichier snmp-exporter.service avec l'éditeur de texte, nous exécutons la commande illustrée dans la figure suivante :

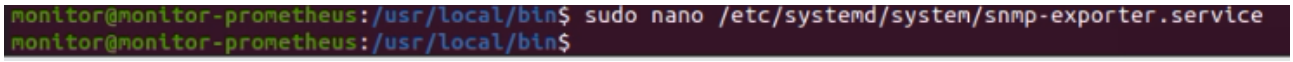

Figure 4.29 – Accès au fichier snmp-exporter.service

Après l'ouverture du fichier, nous établissons des modifications, comme c'est illustré dans la figure suivante :

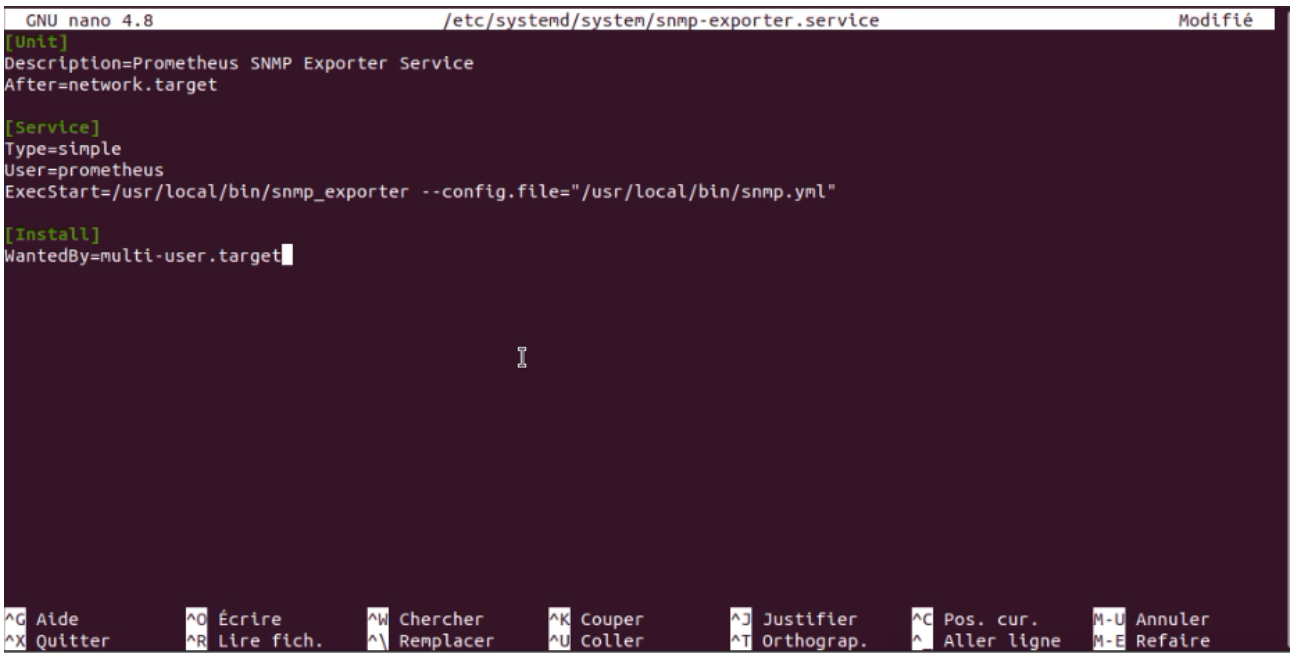

Figure 4.30 – Fichier snmp-exporter.service

Enfin, nous démarrons et activons le service SNMP Exporter. Comme c'est illustré dans la figure ci-dessous :

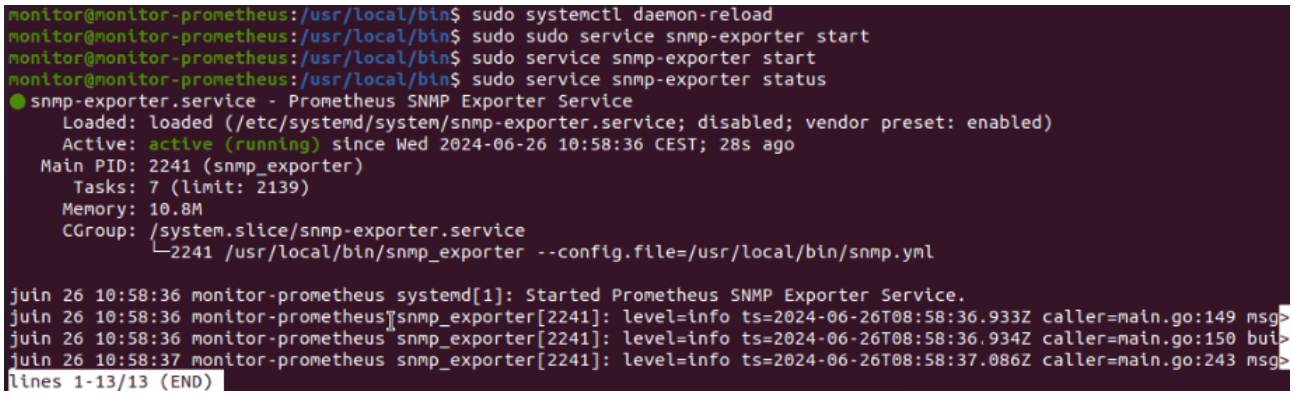

Figure 4.31 – Activation du SNMP Exporter

Après l'activation du SNMP Exporter, voici l'interface qui s'affiche :

FIGURE 4.32 – Interface SNMP Exporter

Phase 2 : Configurations

4.5 Configuration de base

4.5.1 Routeur

Pour la configuration du routeur Cisco, nous commençons par configurer l'interface Ethernet0/0, l'activons, et attribuons une adresse IP via DHCP. Ensuite, nous configurons l'interface Ethernet0/1, attribuons une adresse IP statique, puis activons l'interface. Ensuite, nous passons à la configuration de la NAT, attribuons les interfaces internes et externes, et appliquons les règles de surcharge NAT.

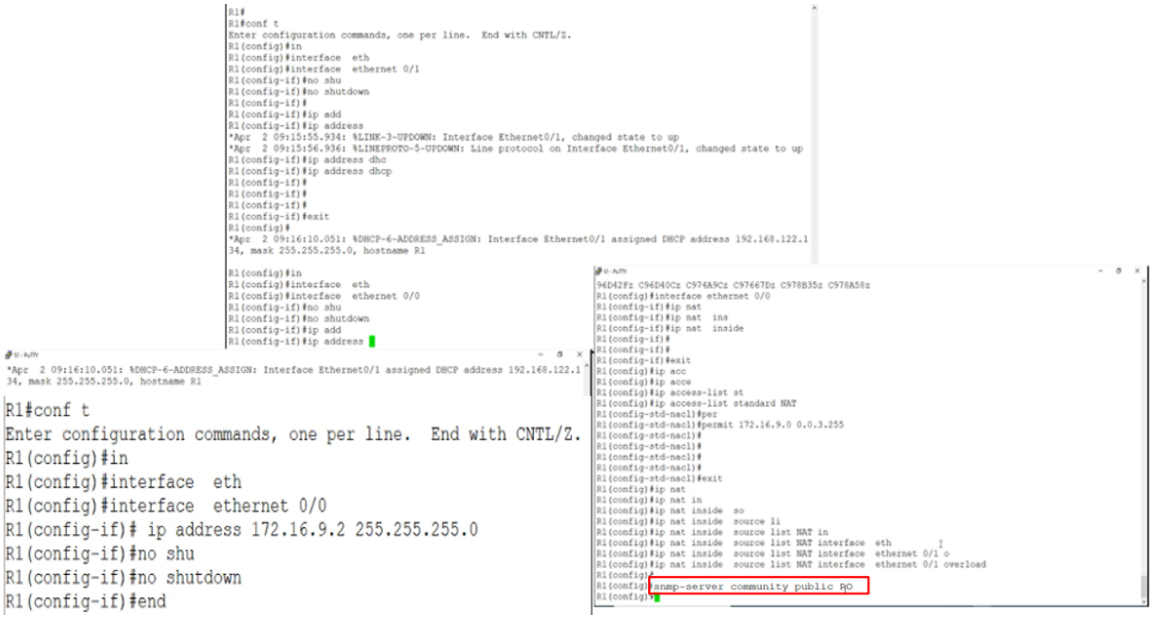

FIGURE 4.33 – Configuration du Routeur (R1)

4.5.2 SWD

Pour la configuration du SWD, configurez une plage d'interfaces Ethernet, et aussi l'interface Ethernet0/0 en mode trunk. Après, passez à la configuration du Protocole VTP, incluant le mode serveur, le domaine, le mot de passe, la version et l'activation du pruning. Puis, la création de plusieurs VLANs avec des identifiants et des noms spécifiques.

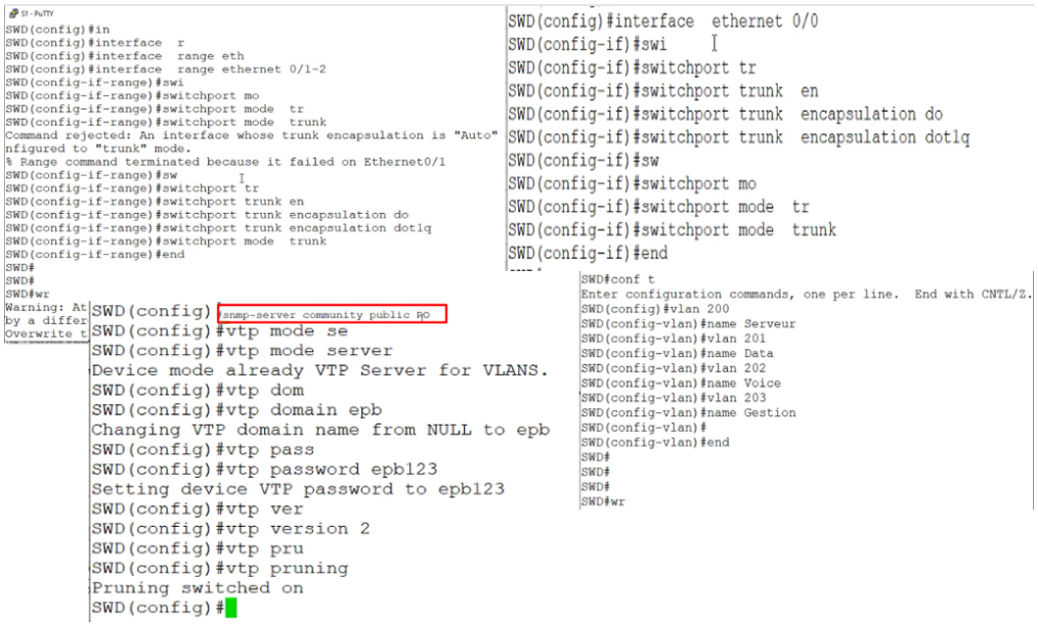

FIGURE 4.34 – Configuration SWD

4.5.3 S-DMZ

Commencez par configurer l'interface VLAN 1, en l'activant et en lui assignant une adresse IP (172.17.8.200 255.255.255.0). Ensuite, configurez une communauté SNMP en lecture seule (RO) avec le nom "public".

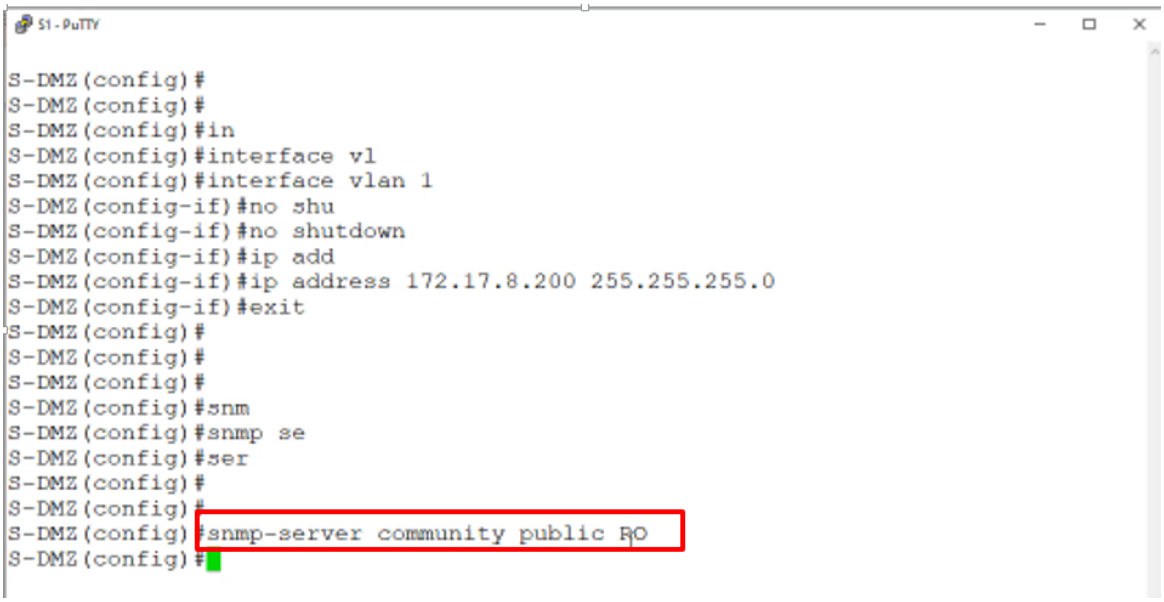

FIGURE 4.35 – Configuration de la DMZ

4.5.4 User

Commencez par la configuration de l'interface Ethernet 0/0 en mode trunk. Ensuite, passez à la configuration de la plage d'interfaces Ethernet 0/1-2 en mode accès avec des VLANs spécifiques assignés (VLAN 101, VLAN voice 202). Après, la configuration de l'interface Ethernet 0/3 en mode accès et assignée au VLAN 203. Ensuite, configurations pour les paramètres VTP, notamment le mode client.

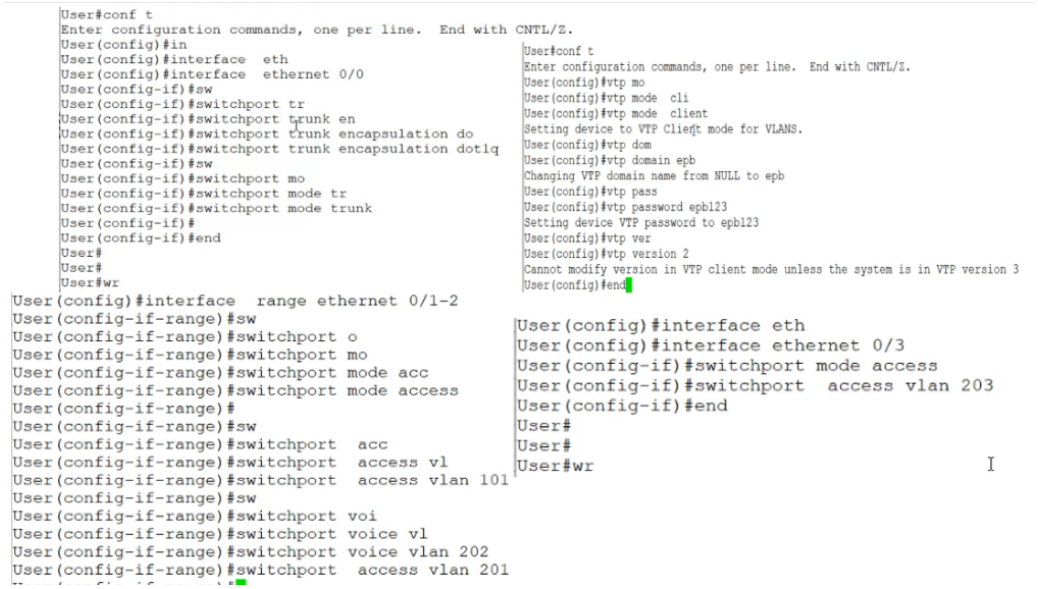

FIGURE 4.36 – Configuration User

4.5.5 SW_SER

Commencez par configurer l'interface Ethernet 0/0 en mode trunk. Puis, configurez une plage d'interfaces Ethernet 0/1-3 en mode accès en assignant le VLAN 200. Ensuite, activez le mode client VTP.

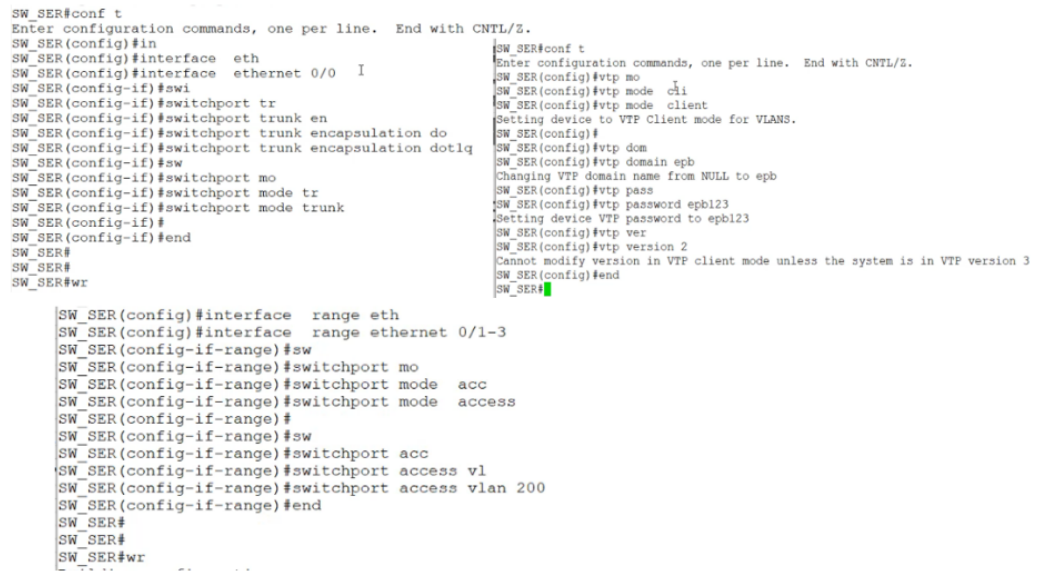

FIGURE 4.37 – Configuration SW_SER

4.6 Configuration Pfsense

Pour la configuration de l'interface LAN du pfSense, sélectionnez l'interface à configurer (option 2) et saisissez l'adresse : 172.16.10.20 avec le masque /24, et suivez les étapes illustrées dans la figure ci-dessous :

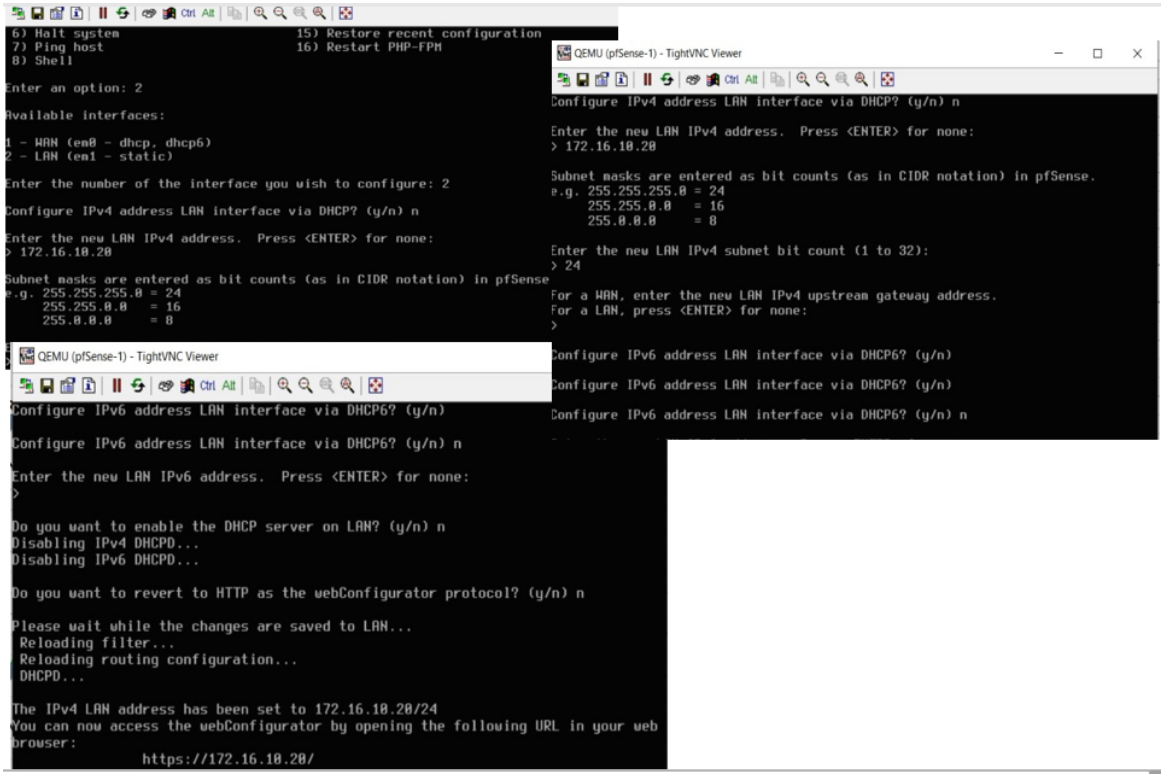

FIGURE 4.38 – Configuration Pfsense

4.6.1 Interface de Pfsense

Après la configuration du Pfsense, voici l'interface qui s'affiche :

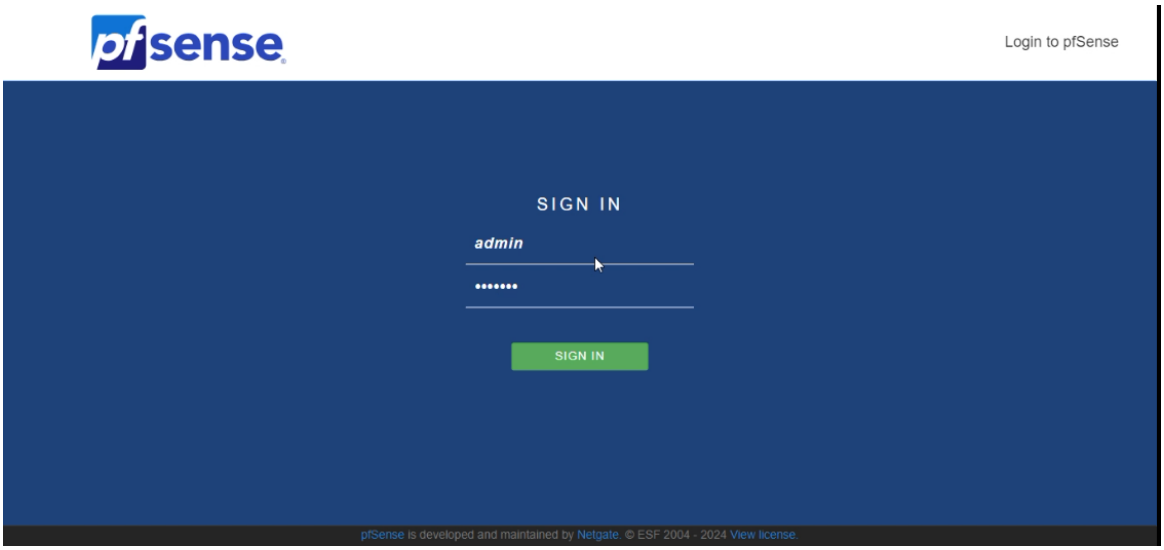

FIGURE 4.39 – Interface de Pfsense

4.6.2 Ajout des Interfaces

Afin d'ajouter des interfaces, suivez les étapes illustrées dans la figure suivante :

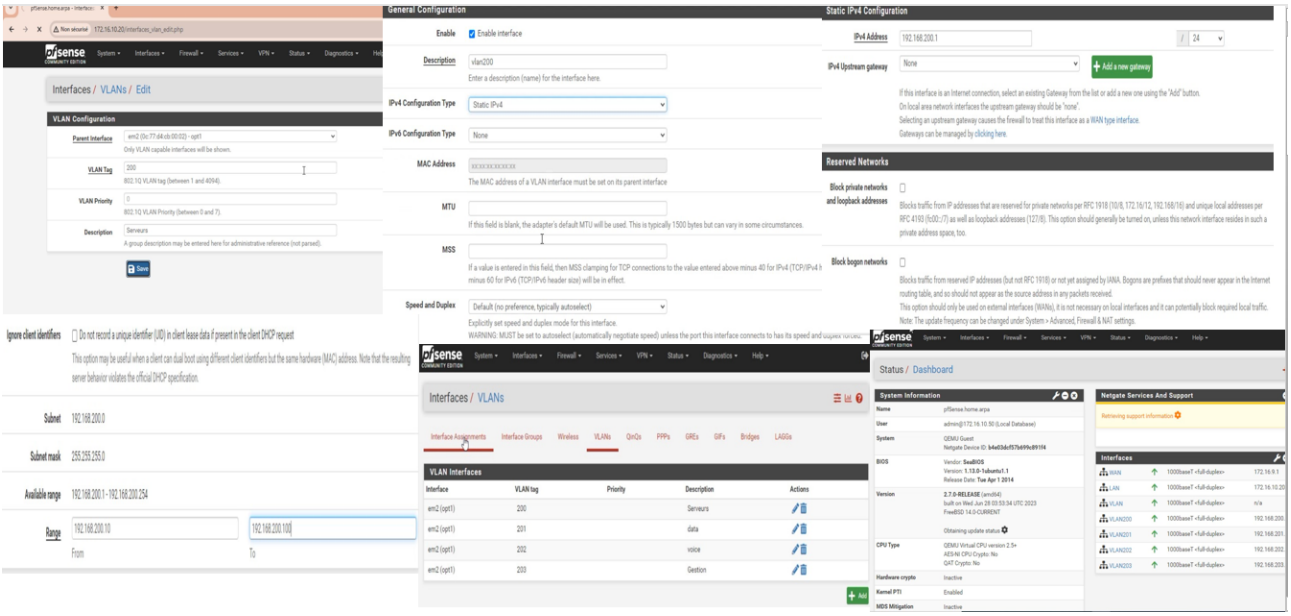

FIGURE 4.40 – Ajout des interfaces

4.6.3 Activer port SNMP sur Pfsense

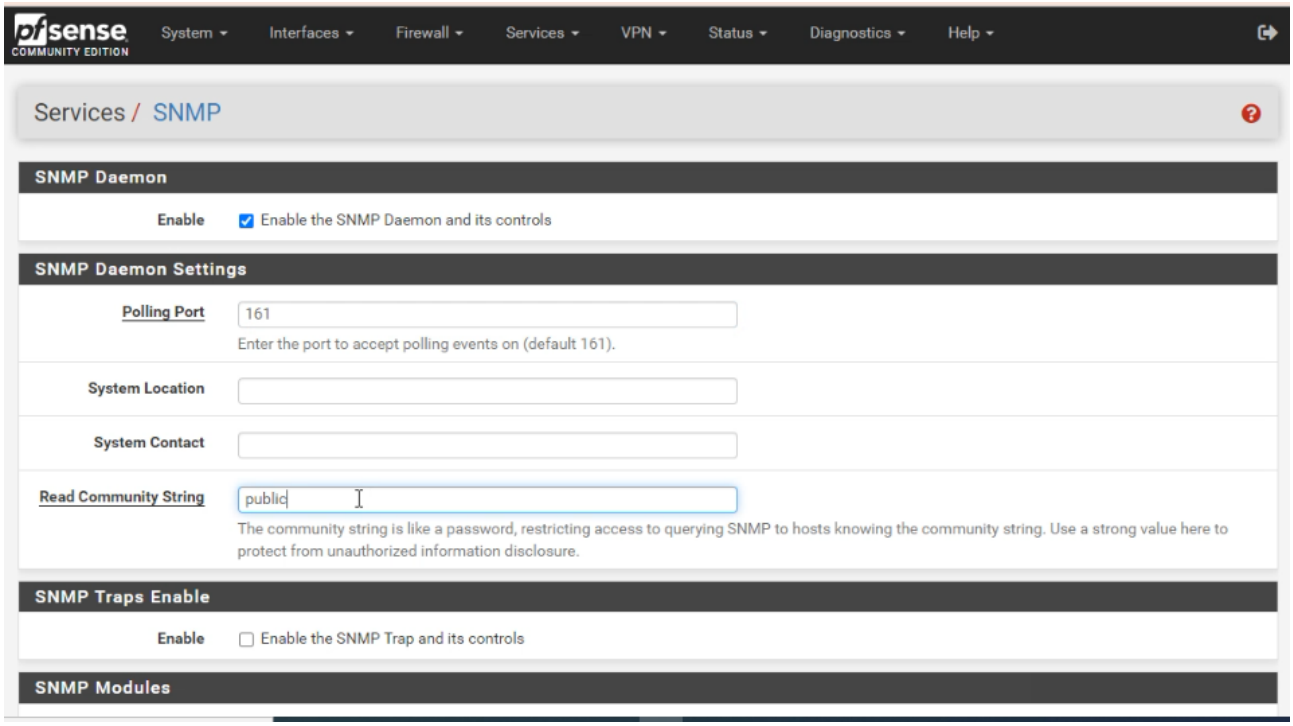

FIGURE 4.41 – Activation du port SNMP

4.7 Configuration ESXI

Pour configurer ESXI, suivez les étapes illustrées ci-dessous :

FIGURE 4.42 – Configuration ESXI

4.7.1 Interface ESXI

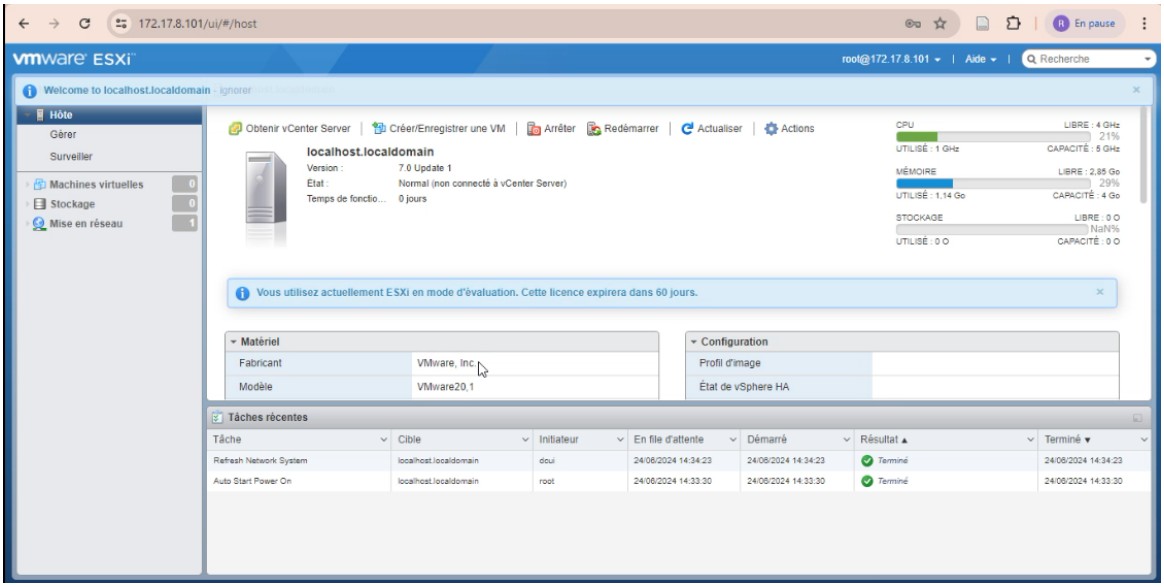

FIGURE 4.43 – Page d'accueil d'ESXI

4.8 Configuration SNMP sur VSphere

Afin de configurer SNMP sur VSphere, suivez les étapes indiquées ci-dessous :

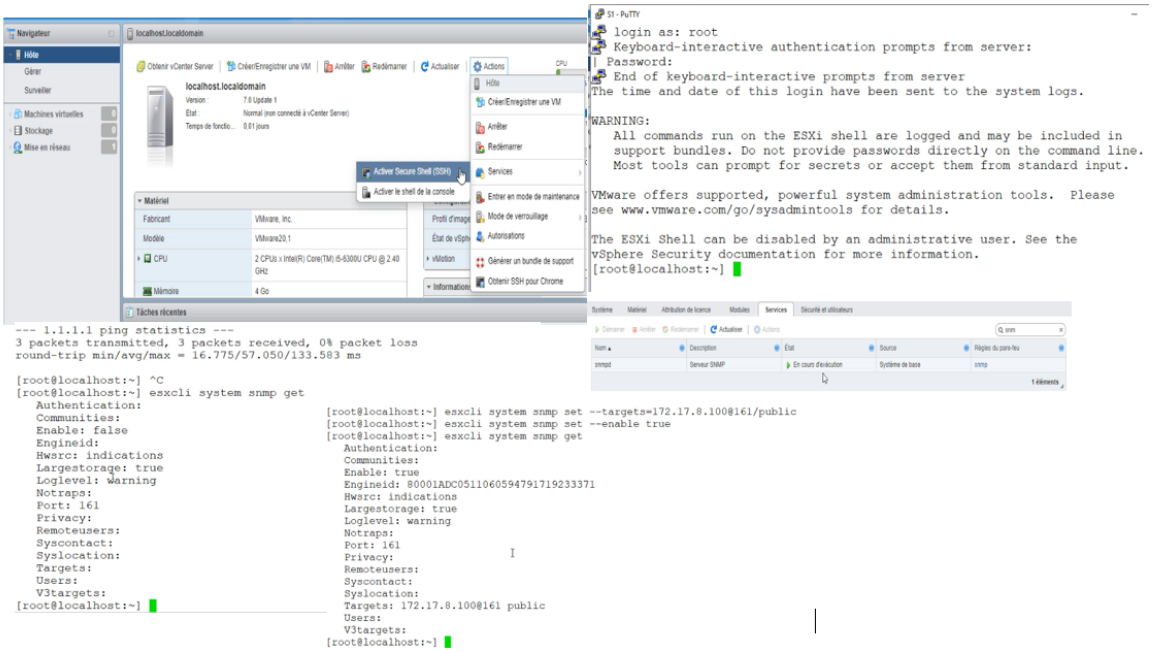

FIGURE 4.44 – Configuration SNMP sur VSphere

4.9 Configuration Prometheus

Pour l'affichage du contenu du fichier de configuration 'prometheus.yml' qui se trouve dans le répertoire '/etc/prometheus/', nous avons exécuté la commande 'cat /etc/prometheus/prometheus.yml'. Comme illustré ci-dessous :

```
cat /etc/prometheus/prometheus.yml
```

FIGURE 4.45 – Affichage du fichier prometheus.yml avec « cat »

Après l'exécution de la commande précédente, le fichier 'prometheus.yml' s'affichera et des modifications peuvent être effectuées selon les besoins. Comme illustré dans la figure ci-dessous :

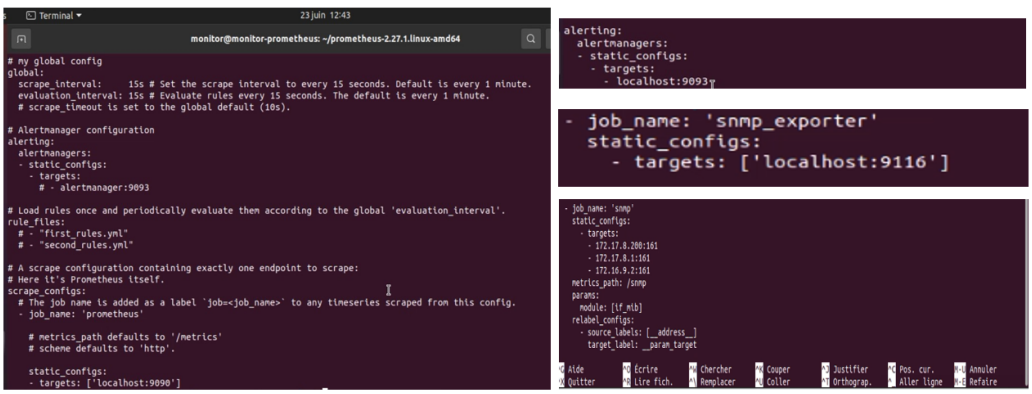

FIGURE 4.46 – Fichier prometheus.yml

Pour ouvrir et modifier le fichier ‘prometheus.service‘ avec l’éditeur de texte ‘nano‘, nous utilisons la commande exacte illustrée dans la figure suivante :

FIGURE 4.47 – Commande nano

Après avoir créé le fichier avec succès, nous avons effectué des modifications dans le fichier puis enregistré ces modifications. Comme illustré dans la figure suivante :

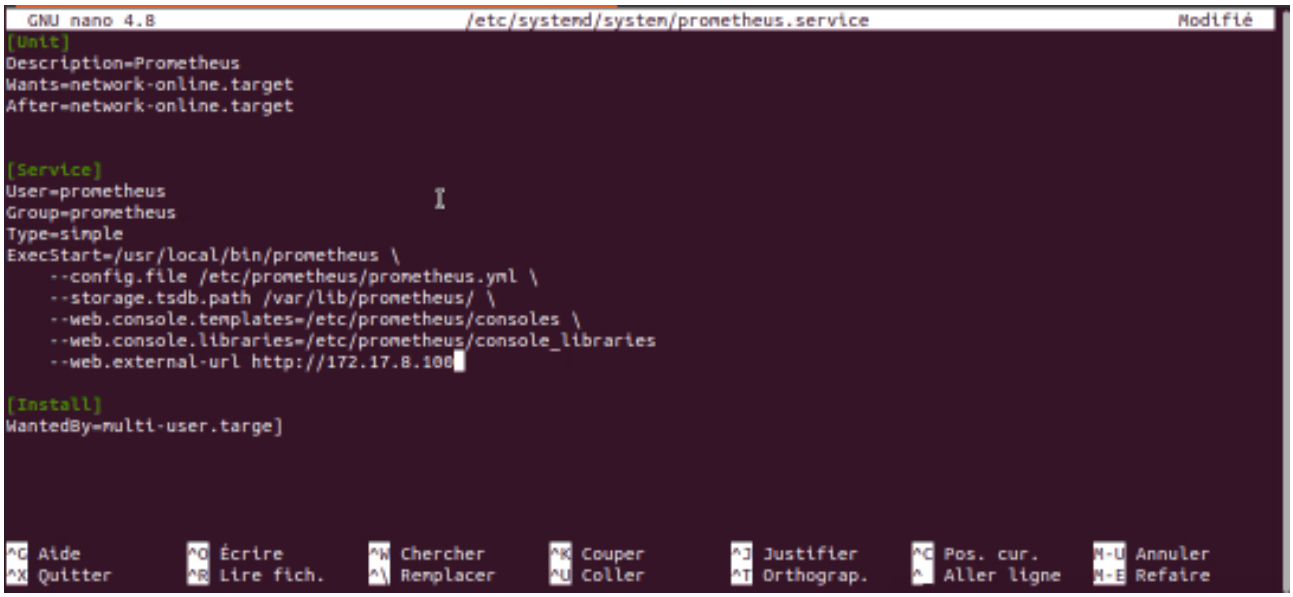

FIGURE 4.48 – Fichier prometheus.service

Pour utiliser le nouveau service créé, nous avons rechargé les services du démon en utilisant la commande ci-dessous :

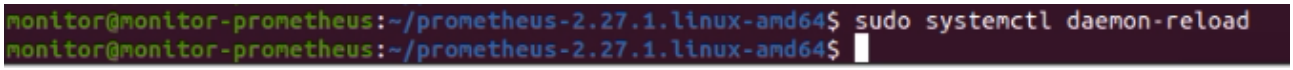

FIGURE 4.49 – Commande systemctl daemon-reload

Pour autoriser le service Prometheus dans le pare-feu, nous avons activé le port 9090. La commande exacte est illustrée dans la figure ci-dessous :

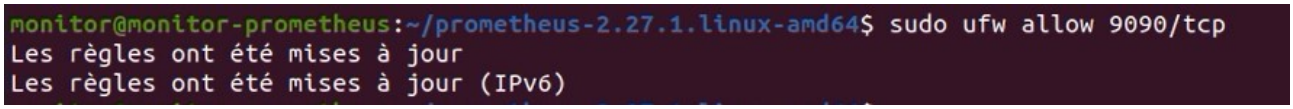

FIGURE 4.50 – Activation du port 9090

4.10 Configuration Grafana

Afin d'afficher le contenu du fichier de configuration `sources.list` qui se trouve dans le répertoire `/etc/apt/`, nous avons exécuté les commandes indiquées dans la figure suivante :

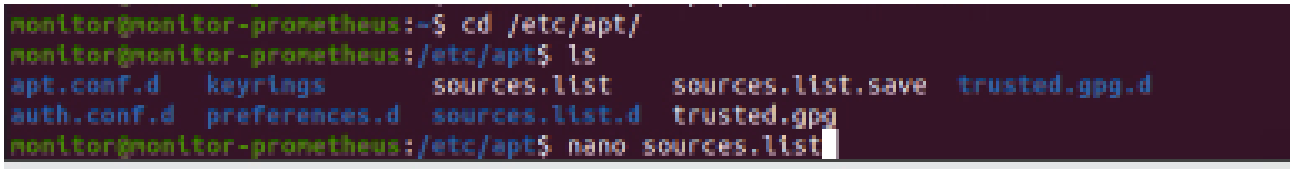

FIGURE 4.51 – Affichage du contenu du fichier sources.list

Après l'exécution des commandes précédentes, le fichier s'affiche et des modifications peuvent se faire selon les besoins. Comme c'est indiqué dans la figure ci-dessous :

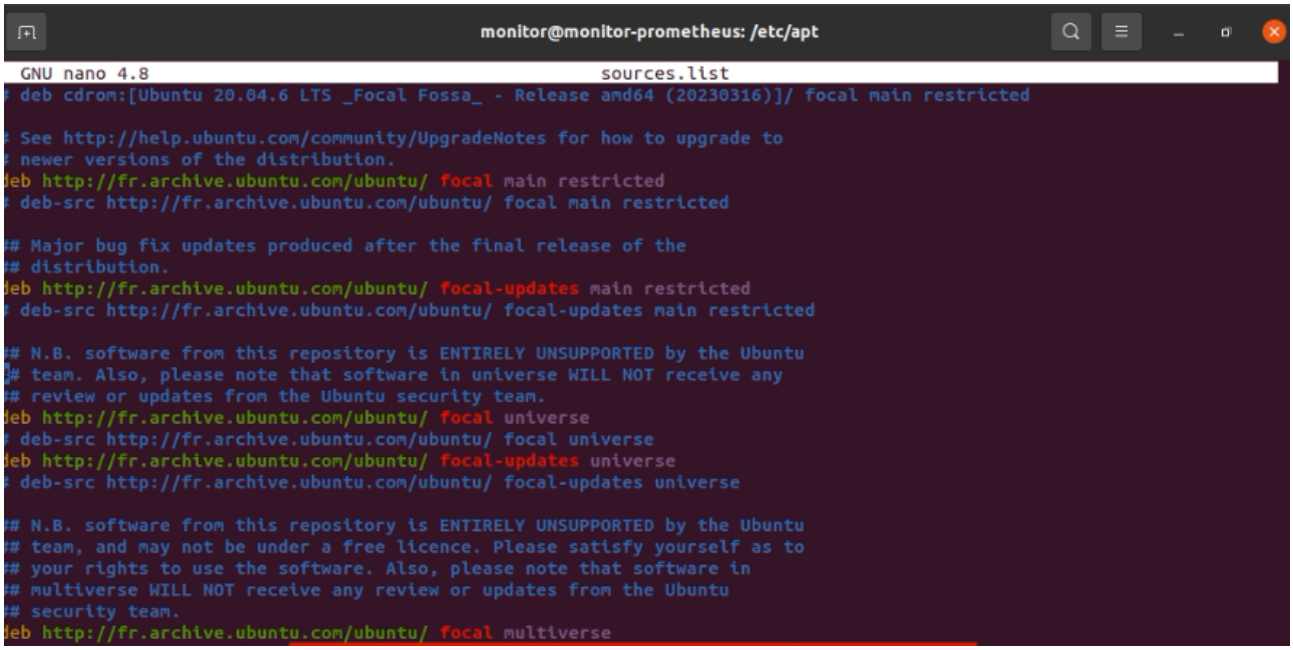

FIGURE 4.52 – Affichage détaillé du fichier sources.list

Pour autoriser le service Grafana dans le pare-feu, nous avons activé le port 3000 en suivant les commandes illustrées dans la figure suivante :

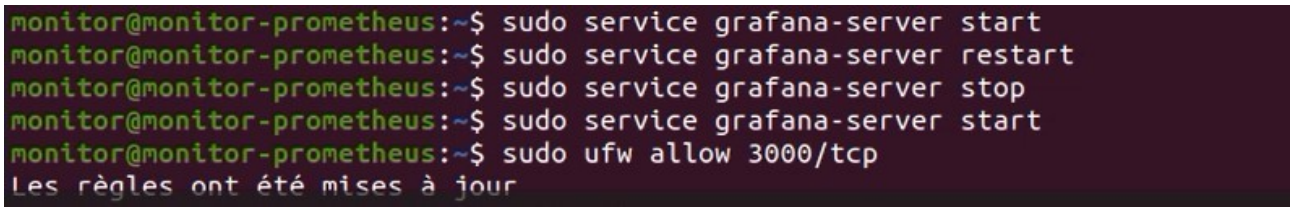

FIGURE 4.53 – Activation du port 3000

Ensuite, nous avons démarré et activé le service Grafana. Comme c'est illustré dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ grafana-server -v
Version 11.0.0 (commit: 277ef258d4b9a5acdf2932347c6a4ca72d739b28, branch: HEAD)
monitor@monitor-prometheus:~$ sudo systemctl start grafana-server
monitor@monitor-prometheus:~$ sudo systemctl enable grafana-server
Synchronizing state of grafana-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /lib/systemd/system/grafana-server
.service.
monitor@monitor-prometheus:~$ sudo systemctl status grafana-server
● grafana-server.service - Grafana instance
     Loaded: loaded (/lib/systemd/system/grafana-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-06-23 14:12:13 CEST; 15s ago
       Docs: http://docs.grafana.org
   Main PID: 5067 (grafana)
      Tasks: 15 (limit: 2139)
     Memory: 49.6M
     CGroup: /system.slice/grafana-server.service
             └─5067 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/gra
```

FIGURE 4.54 – Activation du service Grafana

4.11 Intégration Prometheus avec Grafana

Afin d'intégrer Prometheus avec Grafana, allons dans source de données dans l'interface d'accueil de Grafana, ensuite sur connexion attribuons l'adresse IP de Prometheus ainsi que son port. Après la sauvegarde, un message « successfully queried the prometheus API » s'affiche.

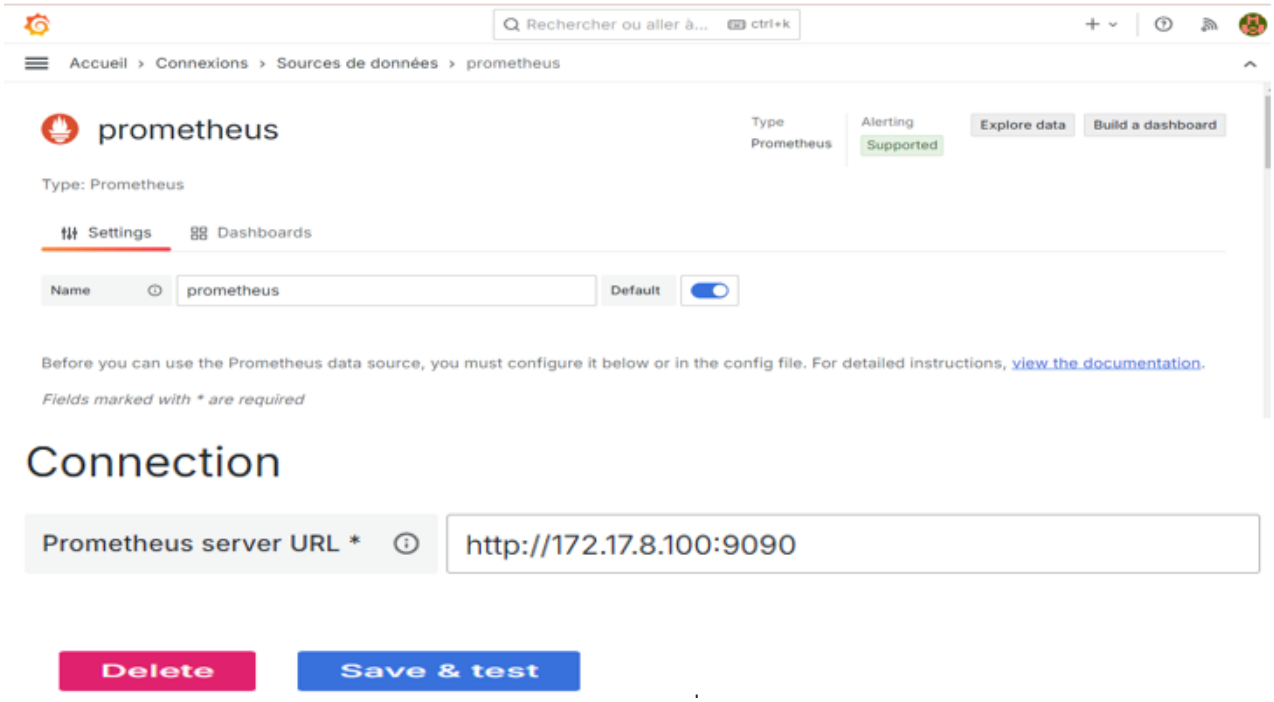

FIGURE 4.55 – Connexion Grafana avec Prometheus

L'interface d'intégration s'affiche comme dans la figure suivante :

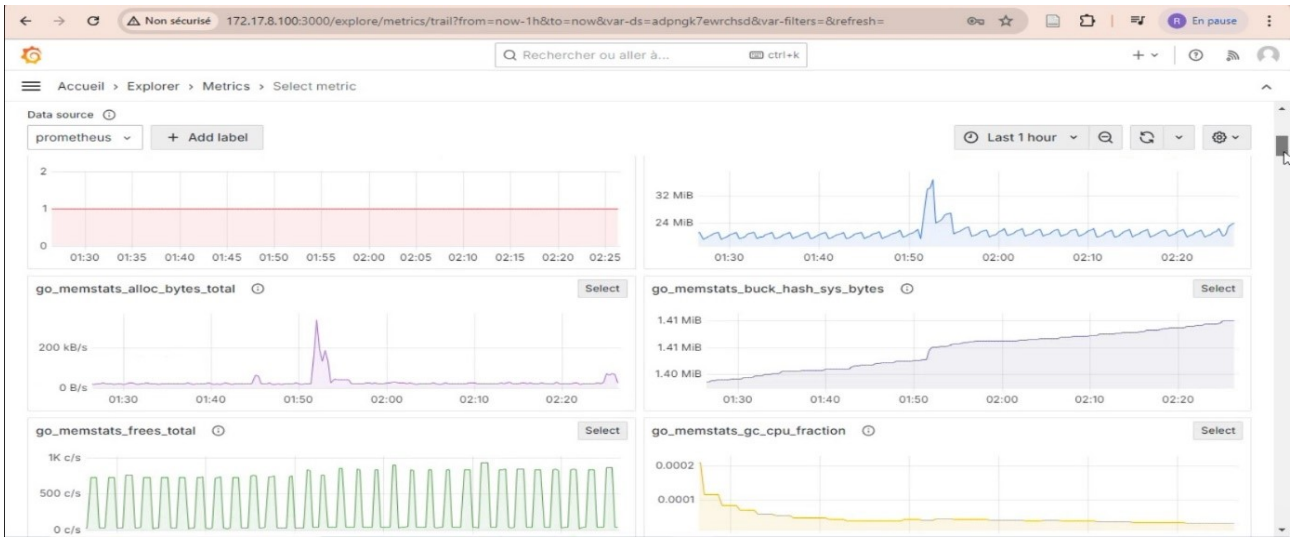

FIGURE 4.56 – Interface Grafana avec Prometheus

4.12 Configuration AlertManager

Afin d'ouvrir et modifier le fichier `alertmanager.yml` avec l'éditeur de texte, exécutons la commande ci-dessous :

```
monitor@monitor-prometheus:~$ sudo nano /etc/alertmanager/alertmanager.yml
```

FIGURE 4.57 – Accès au fichier alertmanager.yml

Après l'exécution de la commande précédente, voici le fichier `alertmanager.yml`. Des modifications peuvent se faire selon nos besoins :

```
 GNU nano 4.8                    /etc/alertmanager/alertmanager.yml                    Modifié
global:
  resolve_timeout: 2m
  smtp_require_tls: false

route:
  group_by: ['alertname']
  # Send all notifications to me.
  group_wait: 30s
  group_interval: 1m
  repeat_interval: 5s
  receiver: 'email-me'

receivers:
- name: 'email-me'
  email_configs:
  - to: "laldjarania@gmail.com"
    from: "laldjarania@gmail.com"
    smarthost: "smtp.gmail.com:465"
    auth_username: "laldjarania@gmail.com"
    auth_identity: "laldjarania@gmail.com"
    auth_password: "l[redacted]1"
```

FIGURE 4.58 – Fichier alertmanager.yml

Pour ouvrir et modifier le fichier `alertmanager.service` avec l'éditeur de texte Nano, exécutons les commandes indiquées dans la figure ci-dessous :

```
monitor@monitor-prometheus:~$ sudo chown alertmanager:alertmanager -R /etc/alertmanager
monitor@monitor-prometheus:~$ sudo nano /etc/systemd/system/alertmanager.service
monitor@monitor-prometheus:~$ sudo nano /etc/systemd/system/alertmanager.service
monitor@monitor-prometheus:~$
```

FIGURE 4.59 – Accès au fichier alertmanager.service

Après avoir créé le fichier et l'avoir modifié avec succès, enregistrons-le.

```
 GNU nano 4.8                    /etc/systemd/system/alertmanager.service                    Modifié
[Unit]
Description=Alertmanager
Wants=network-online.target
After=network-online.target

[Service]
User=alertmanager
Group=alertmanager
Type=simple
WorkingDirectory=/etc/alertmanager/
ExecStart=/usr/local/bin/alertmanager --config.file=/etc/alertmanager/alertmanager.yml --web.external-url http://0.0.0

[Install]
WantedBy=multi-user.target

^G Aide      ^O Écrire      ^W Chercher    ^K Couper      ^J Justifier   ^C Pos. cur.   M-U Annuler
^X Quitter   ^R Lire fich.  ^\ Remplacer   ^U Coller      ^T Orthograp.  ^_ Aller ligne M-E Refaire
```

FIGURE 4.60 – Fichier alertmanager.service

Pour utiliser le nouveau service créé, rechargeons les services du démon et redémarrons Prometheus et Alertmanager comme indiqué ci-dessous.

```
monitor@monitor-prometheus:~$ systemctl daemon-reload
monitor@monitor-prometheus:~$ systemctl restart prometheus
monitor@monitor-prometheus:~$ systemctl restart alertmanager
```

FIGURE 4.61 – Redémarrage des systèmes

4.13 Configuration SNMP Exporter

Pour configurer SNMP Exporter, nous avons ajouté les adresses ip des équipements cibles dans les targets dans le fichier prometheus.yml comme s'est illustre dans la figure ci-dessous, afin que SNMP récupère des informations des cibles :

```
- job_name: 'snmp'
  static_configs:
    - targets:
      - 172.17.8.200:161
      - 172.17.8.1:161
      - 172.16.9.2:161
  metrics_path: /snmp
  params:
    module: [if_mib]
  relabel_configs:
    - source_labels: [__address__]
      target_label: __param_target
```

FIGURE 4.62 – Configuration du SNMP Exporter.

Ensuite, nous avons redémarré les deux services snmp-exporter et prometheus :

```
monitor@monitor-prometheus:~$ sudo service snmp-exporter start
monitor@monitor-prometheus:~$ sudo service snmp-exporter restart
monitor@monitor-prometheus:~$ sudo service prometheus restart
monitor@monitor-prometheus:~$
```

FIGURE 4.63 – Redémarrage des services.

4.14 Attribution du mot de passe pour Prometheus

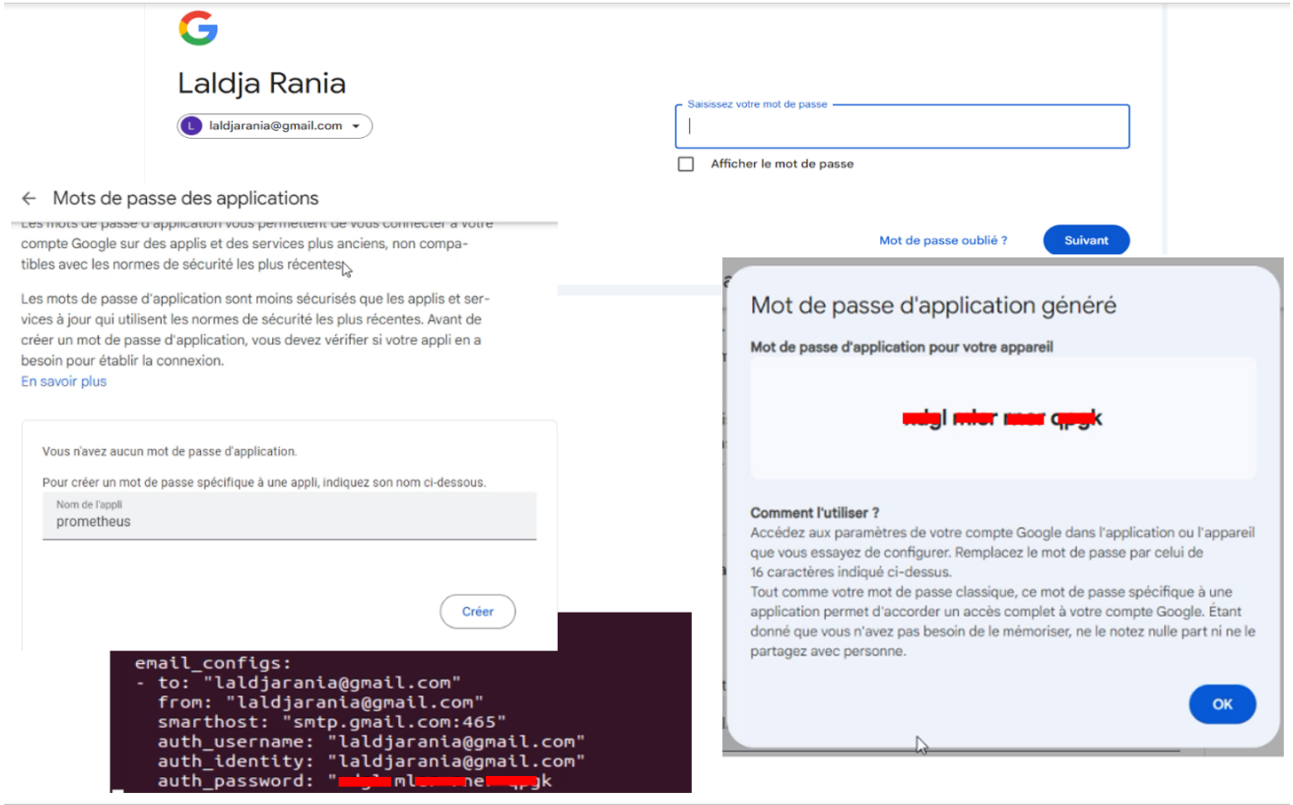

FIGURE 4.64 – Attribution du mot de passe.

Phase 3 : Tests et validations

4.15 État des cibles surveillées par Prometheus

Apres la configuration du SNMP , prometheus affiche l'état des cibles surveillées avec les points de terminaison associés qui sont en état de fonctionnement, comme s'est illustre dans la figure ci-dessous :

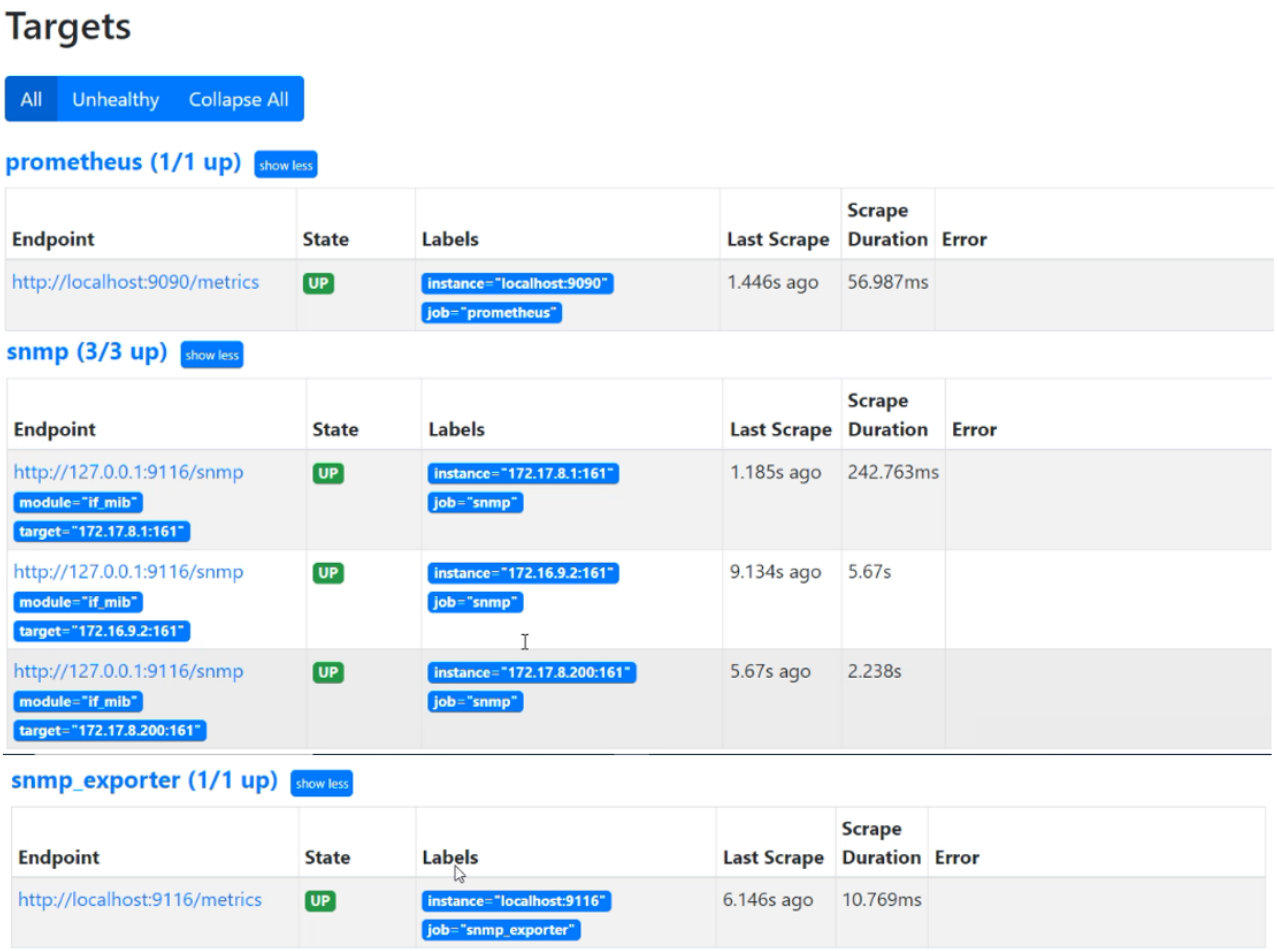

FIGURE 4.65 – Information sur les cibles surveillées.

4.16 Tests d'alertes

Après avoir mis en place la surveillance de notre architecture, les alertes d'anomalies sont reçues. Voici des exemples d'alertes recus :

— **Alert sur prometheus**

FIGURE 4.66 – Alerte reçue sur prometheus.

— **Alerte sur alertmanager**

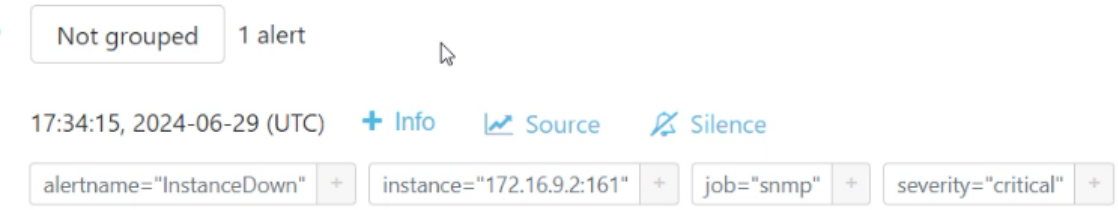

FIGURE 4.67 – Alerte reçue sur alertemanager.

— **Alerte sur email**

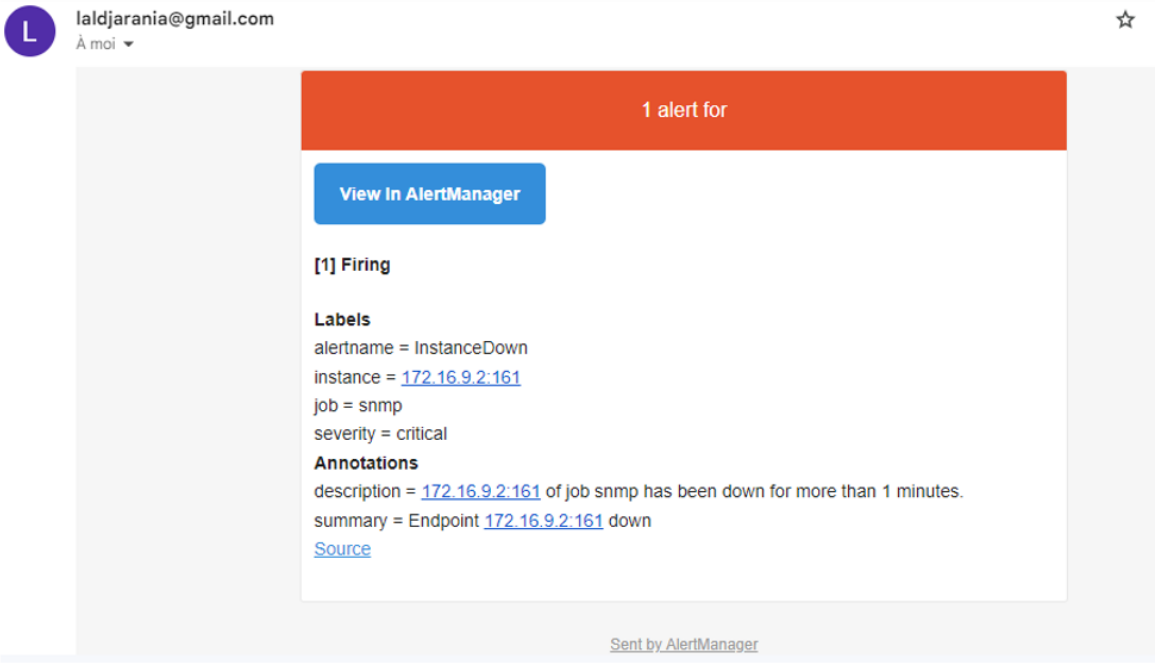

FIGURE 4.68 – Alerte reçue d'un problème.

Après la résolution du problème :

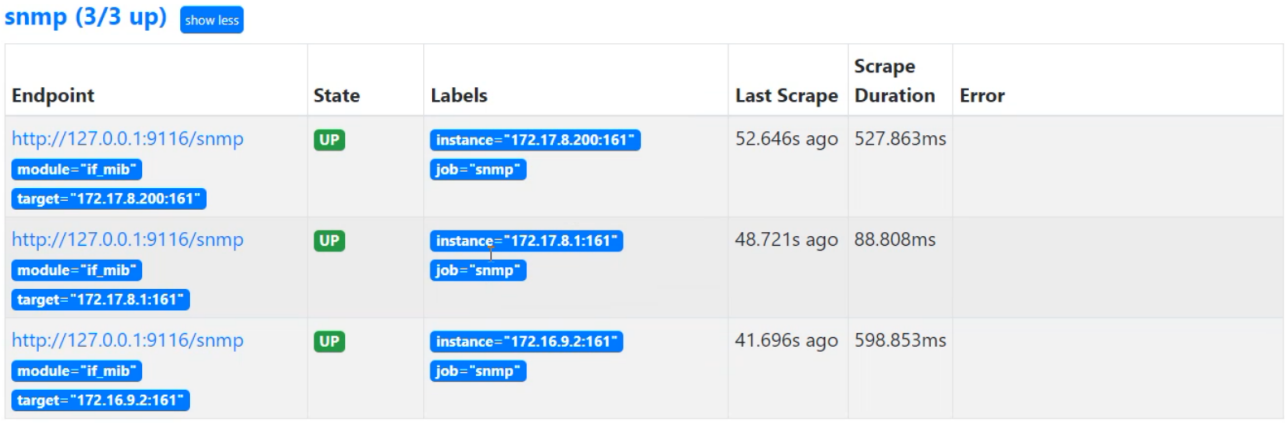

FIGURE 4.69 – Problème résolu.

4.17 Conclusion

Pour conclure, dans ce chapitre nous avons détaillé l'ensemble des procédures et des outils nécessaires pour réaliser notre projet. Il met en évidence l'importance d'une bonne planification et d'une exécution précise afin de garantir le succès de l'implémentation et la performance optimale de l'infrastructure créée.

CONCLUSION GÉNÉRALE

L'objectif de notre projet est de répondre aux défis croissants rencontrés par l'Entreprise Portuaire Bejaia dans la gestion de leurs infrastructures informatiques, en mettant en place l'outil Prometheus, une solution de monitoring moderne reconnue par sa robustesse et son efficacité, et de montrer comment elle peut permettre aux entreprises de relever ces défis de manière proactive et de renforcer la sécurité des données.

Afin d'atteindre cet objectif, nous avons d'abord approfondi nos connaissances dans les réseaux et sécurités, ainsi dans le domaine de supervision.

Ensuite, nous avons étudié en détail l'architecture réseau de l'entreprise, ce qui nous a permis d'identifier la problématique principale ainsi que la solution appropriée.

À la suite de notre étude comparative des outils de supervision disponibles, nous avons choisi Prometheus comme solution optimale en raison de sa capacité à assurer une surveillance complète et à répondre aux besoins spécifiques de l'Entreprise Portuaire Bejaia.

La mise en place de la solution nous a confirmé que la supervision joue un rôle crucial dans la gestion proactive des infrastructures informatiques, en améliorant la disponibilité, la performance et la sécurité des systèmes.

Enfin, ce projet a été bénéfique pour nous, car il nous a permis d'appliquer nos connaissances en administration sécurité des réseaux et de découvrir le domaine de la supervision.

À l'avenir, plusieurs améliorations et développements peuvent être envisagées, tels que le développement de scripts et d'algorithmes pour automatiser les réponses aux incidents détectés, la création de métriques et de tableaux de bord spécifiques pour évaluer la performance des applications, ainsi que l'intégration avec d'autres outils complémentaires.

BIBLIOGRAPHIE

[1] Abbou, M., and Abacherif, M. a. Mise en place d'une solution de supervision cacti cas d'étude : Cevital. Mémoire de master, Université Abderrahmane Mira – Bejaia, 2021.

[2] Alphorm. Formation en ligne - apprendre prometheus et grafana : Présenter grafana (tuto vidéo), 2024. https://www.alphorm.com/tutoriel/formation-en-ligne-apprendre-prometheus-et-grafana/tuto-video-presenter-grafana (Consulté le 3 mars 2024).

[3] Alphorm. Formation en ligne - centreon : Superviser un système d'information, 2024. https://www.alphorm.com/tutoriel/formation-en-ligne-centreon-superviser-un-systeme-dinformation (Consulté le 2 mars 2024).

[4] Alphorm. Formation en ligne zabbix : Supervision avancée, 2024. https://www.alphorm.com/tutoriel/formation-en-ligne-zabbixsupervision-avancee (Consulté le 2 mars 2024).

[5] Bloch, L., and Wolfhugel, C. *Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs*, 4th ed. Groupe Eyrolles, Paris, 2013.

[6] Centreon. Définition de la supervision réseau, 2024. https://www.centreon.com/fr/glossary/definition-supervision-reseau/ (Consulté le 28 février 2024).

[7] Cisco. Network connectivity (document pdf), 2024. https://www.cisco.com/web/FR/documents/pdfs/datasheet/ios/NETWORKCONNECTIVITY.pdf (Consulté le 1er mars 2024).

[8] de Batna, U. Sécurité des réseaux - partie 1 (document pdf), 2024. https://cs.univ-batna2.dz/sites/default/files/web/files/securite_des_reseaux_partie_1.pdf (Consulté le 22 février 2024).

[9] de Bejaia, P. Histoire du port de bejaia (document pdf), 2020. https://www.portdebejaia.dz/wp-content/uploads/dlmuploads/2020/03/01-histoire-compressed.pdf (Consulté le 18 février 2024).

[10] de Bejaia, P. Historique du port de bejaia, 2024. https://www.portdebejaia.dz/historique/ (Consulté le 18 février 2024).

[11] de Tlemcen, U. Sécurité - chapitre 1 (document pdf), 2020. https://elearn.univtlemcen.dz/pluginfile.php/115080/mod_resource/content/0/M1%20S%C3%A9curit%C3%A9%20Chapitre1%202020.pdf (Consulté le 22 février 2024).

[12] DJENNANE, L., and KASSA, R. Etude et proposition d'une solution de supervision réseau basée sur pandora fms au profit de l'epb. Mémoire de master, Université Abderrahmane Mira – Bejaia, 2020.

[13] FrameIP. Snmp - simple network management protocol, 2024. https://www.frameip.com/snmp/ (Consulté le 5 mars 2024).

[14] Lydia, S. Mise en place d'une solution supervision au sein campus nts bejaia. Mémoire de master, Université Mouloud MAMMERI De Tizi-Ouzou, 2023.

[15] Oran, E. E. Support khatir 2021 (document pdf), 2024. https://elearning.esgee-oran.dz/pluginfile.php/16193/mod_page/content/44/Support-KHATIR2021.pdf (Consulté le 20 février 2024).

[16] Prometheus. Prometheus overview, 2024. https://prometheus.io/docs/introduction/overview/ (Consulté le 3 mars 2024).

[17] Rima, A. La mise en place d'un système de supervision réseau cas : Insim bejaia. Mémoire de master, Université A.MIRA-BEJAIA, 2021.

[18] Saida, W. Mise en place d'un outil de monitoring de réseau à base de logiciel libre. Mémoire de master, Université virtuelle de Tunis.

[19] University, C. Attaque informatique : en quoi ça consiste ?, 2024. https://www.cyberuniversity.com/post/attaque-informatique-en-quoi-ca-consiste (Consulté le 23 février 2024).

ANNEXES

Annexe 1

Installation GNS3

Pour installer GNS3, lançons le fichier et suivons les instructions d'installation illustrées dans les figures ci-dessous :

Etape1 :

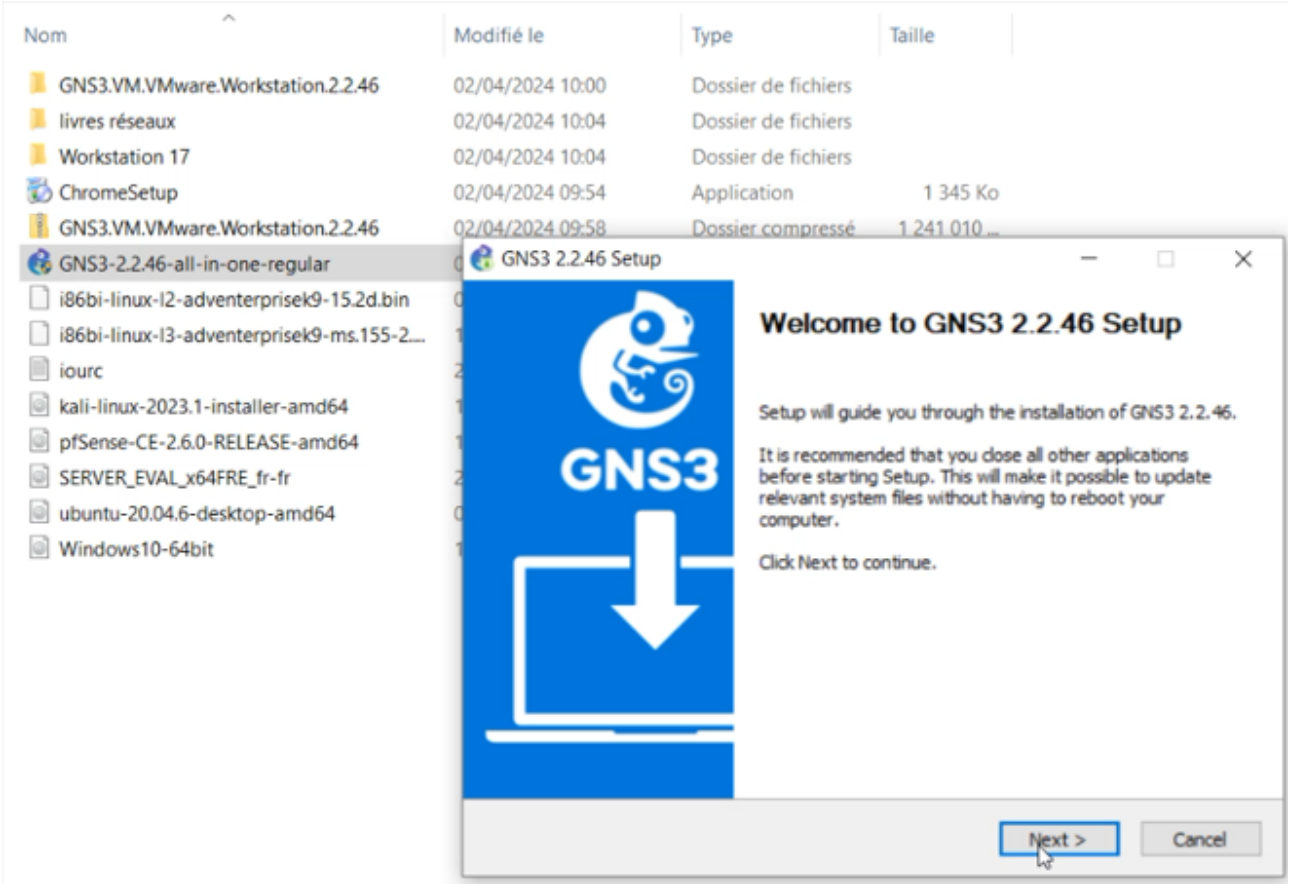

FIGURE 1 – Installation de GNS3 version 2.2.46

Etape2 :

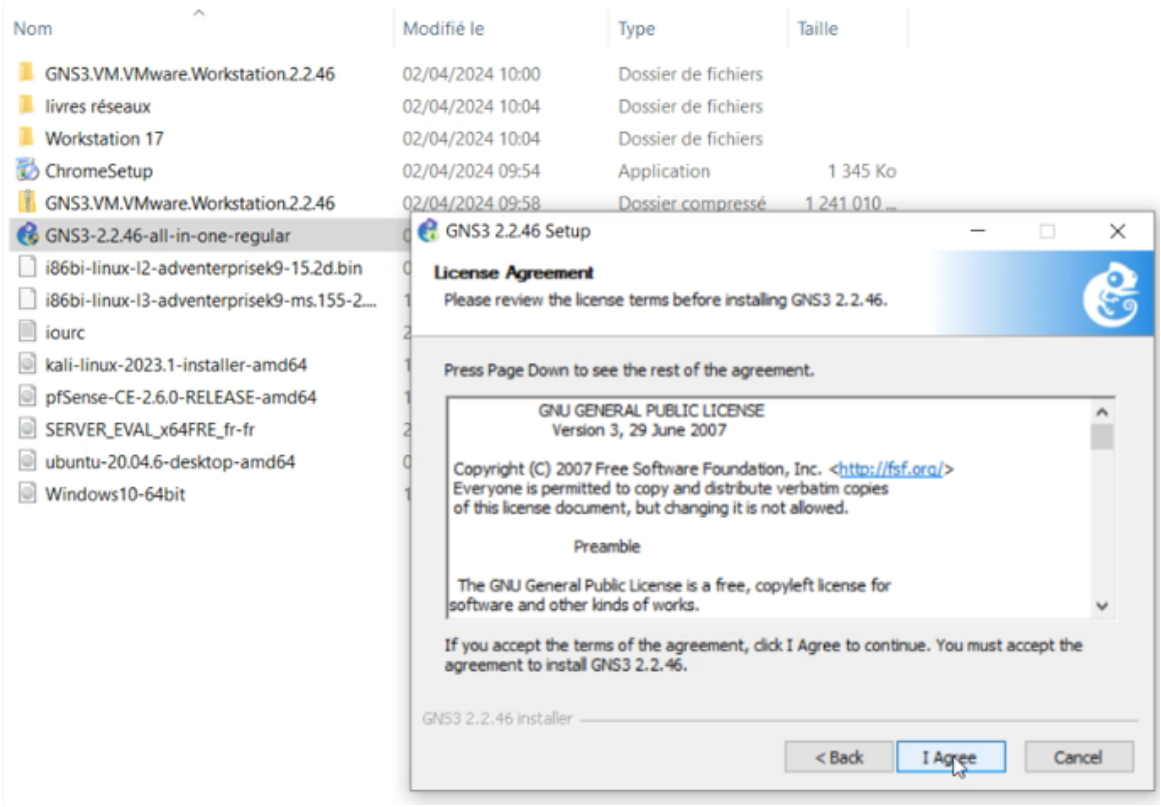

FIGURE 2 – Accord de licence pour l'installation de GNS3

Etape3 :

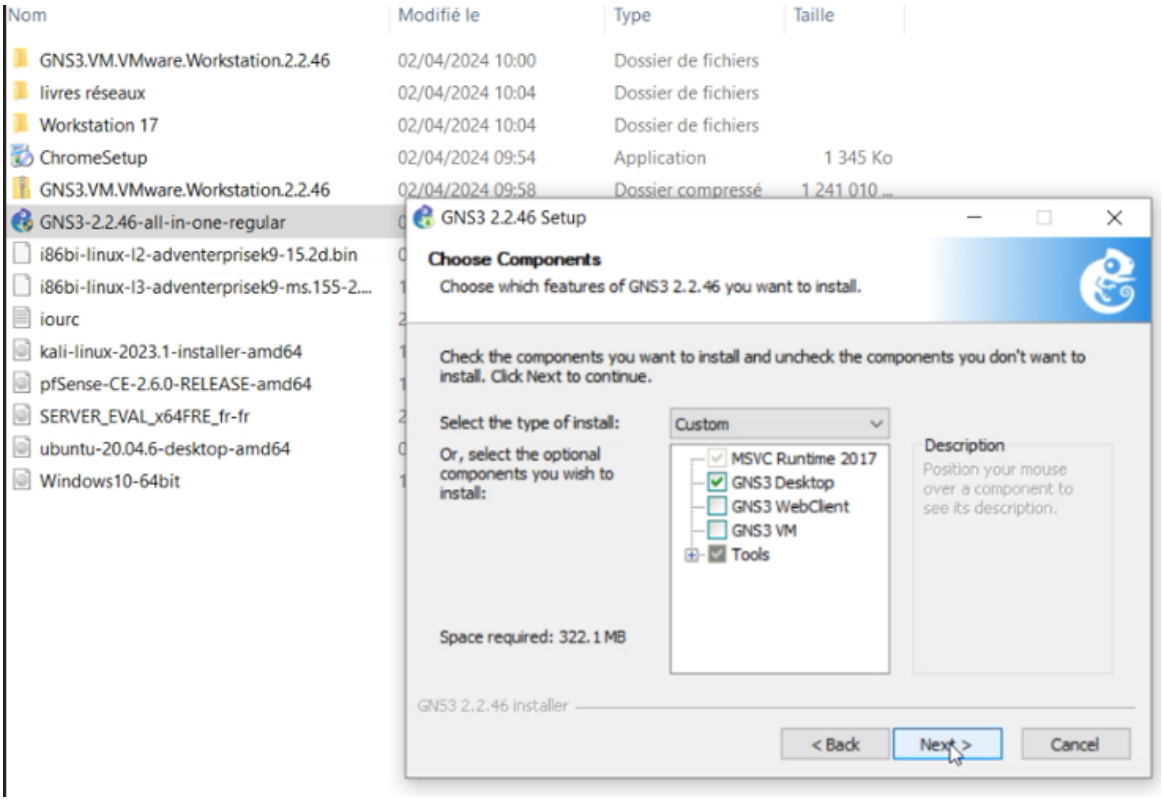

FIGURE 3 – Sélection des composants à installer pour GNS3

Etape4 :

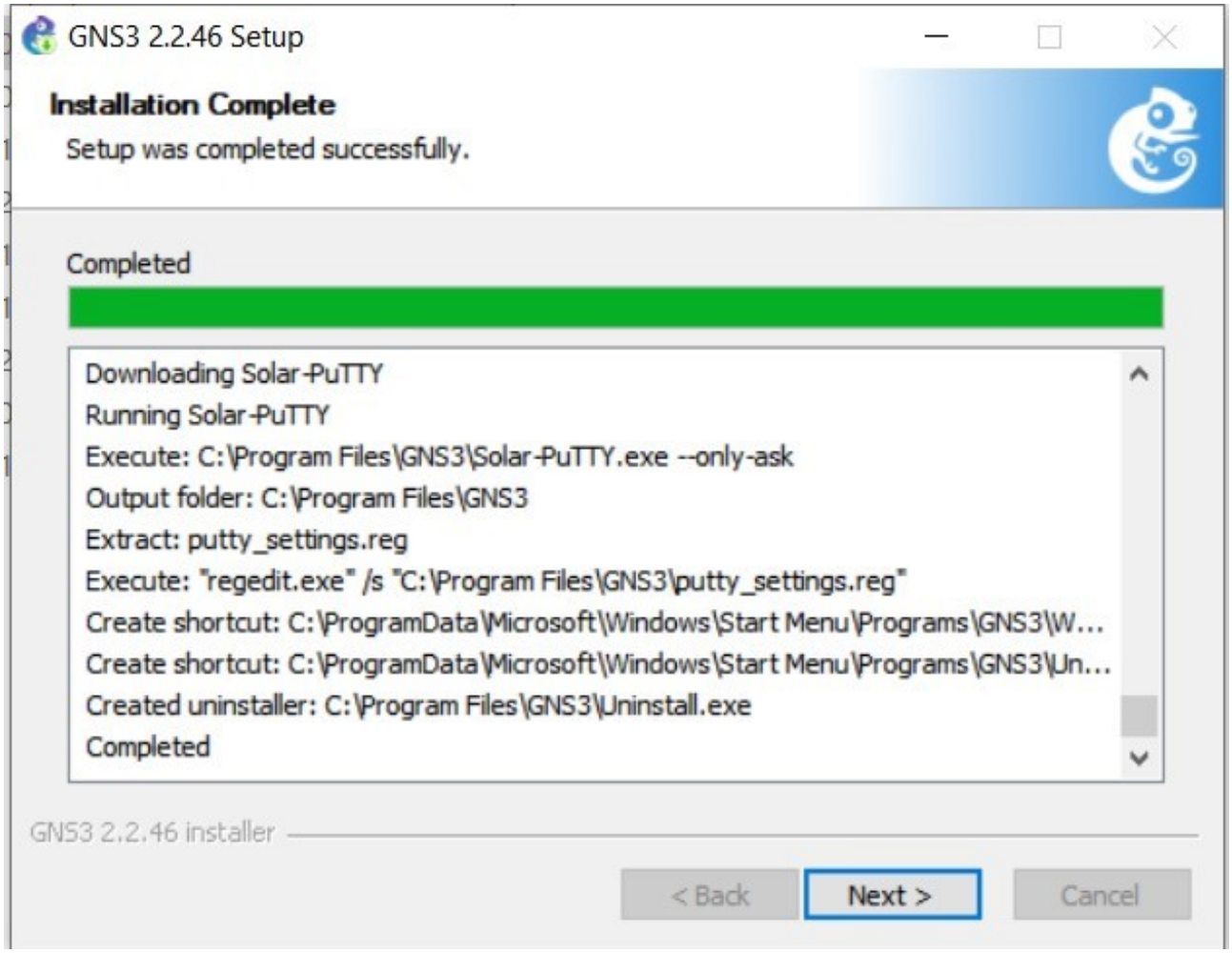

FIGURE 4 – Installation terminée

Annexe 2

Installation VMware

Pour installer VMware Workstation 17 Pro, nous avons suivi ces étapes : nous avons commencé par télécharger le fichier exécutable, puis nous l'avons lancé et suivi les instructions illustrées dans la figure ci-dessous :

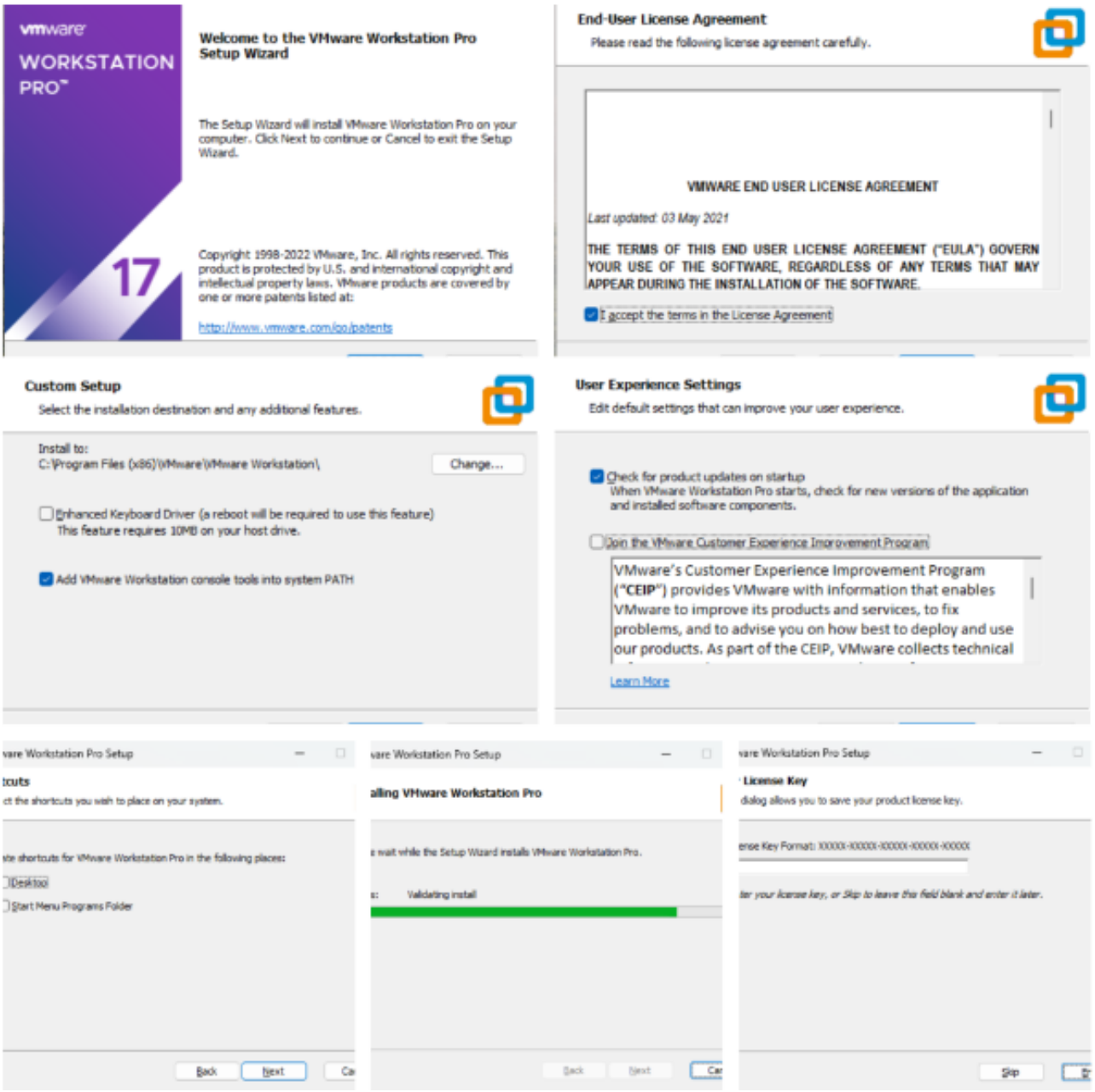

FIGURE 5 – Installation de VMware workstation

Annexe 3

GNS3 VM

Etape1 :

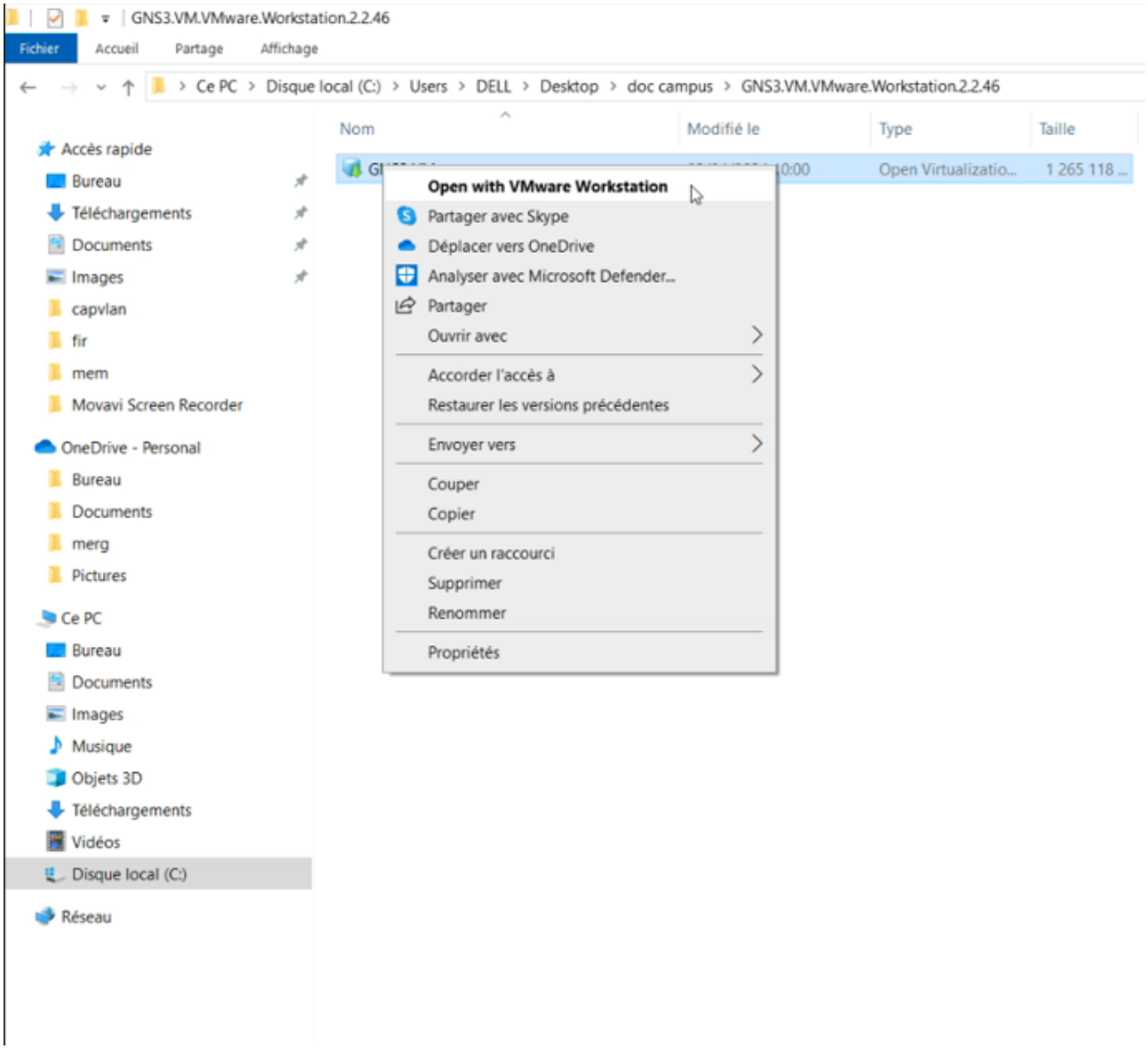

FIGURE 6 – Ouverture du fichier GNS3.VM dans VMware Workstation

Etape2 :

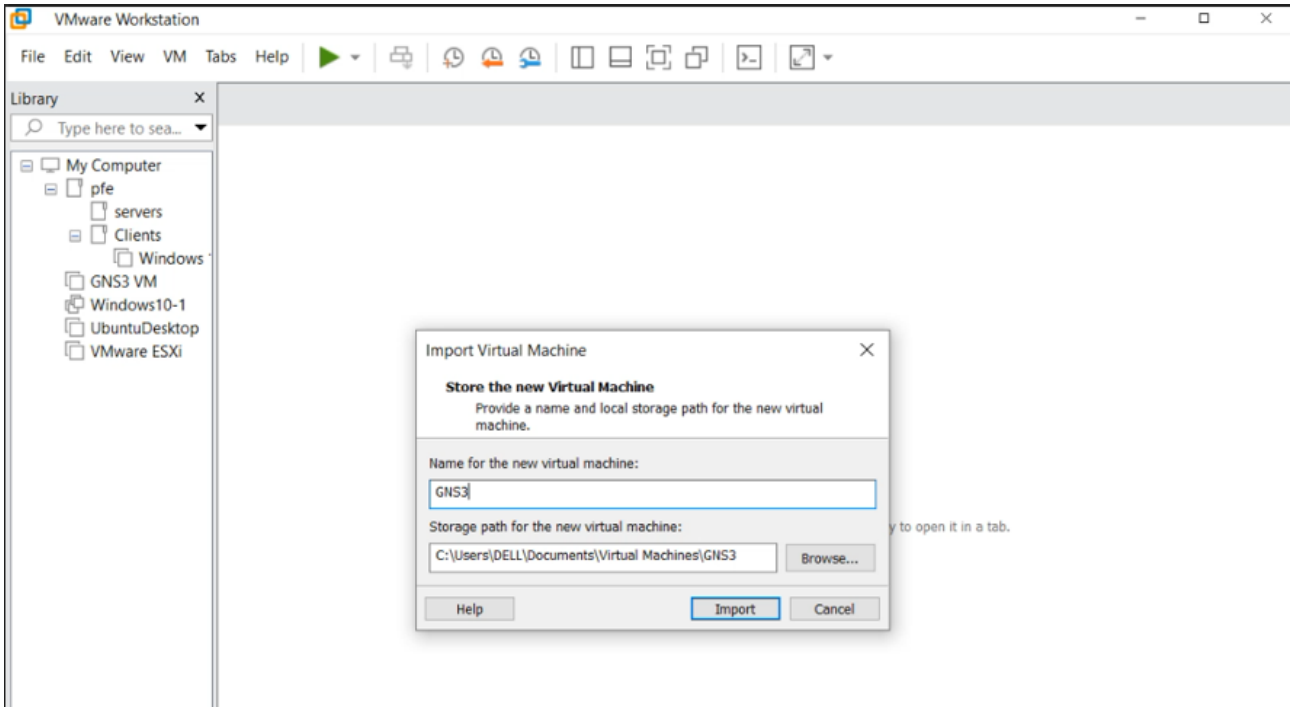

FIGURE 7 – Importation de la machine virtuelle GNS3 dans VMware Workstation

Annexe 4

Ubuntu Desktop

Etape1 :

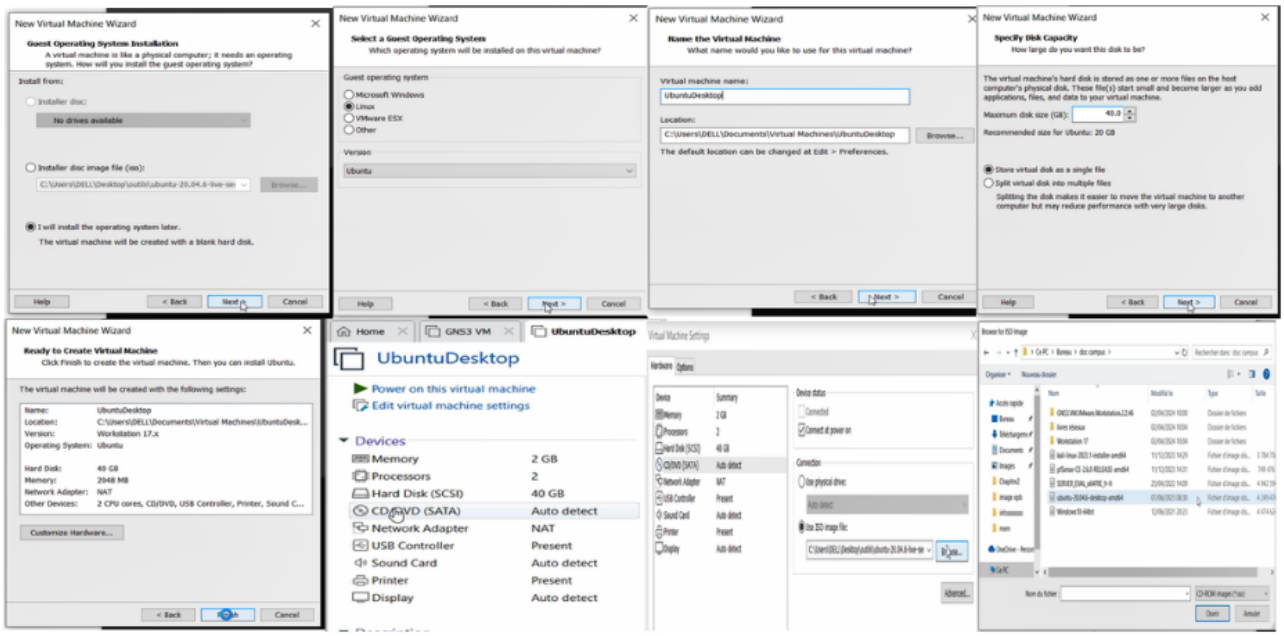

FIGURE 8 – Clonage de la machine virtuelle UbuntuDesktop

Etape2 :

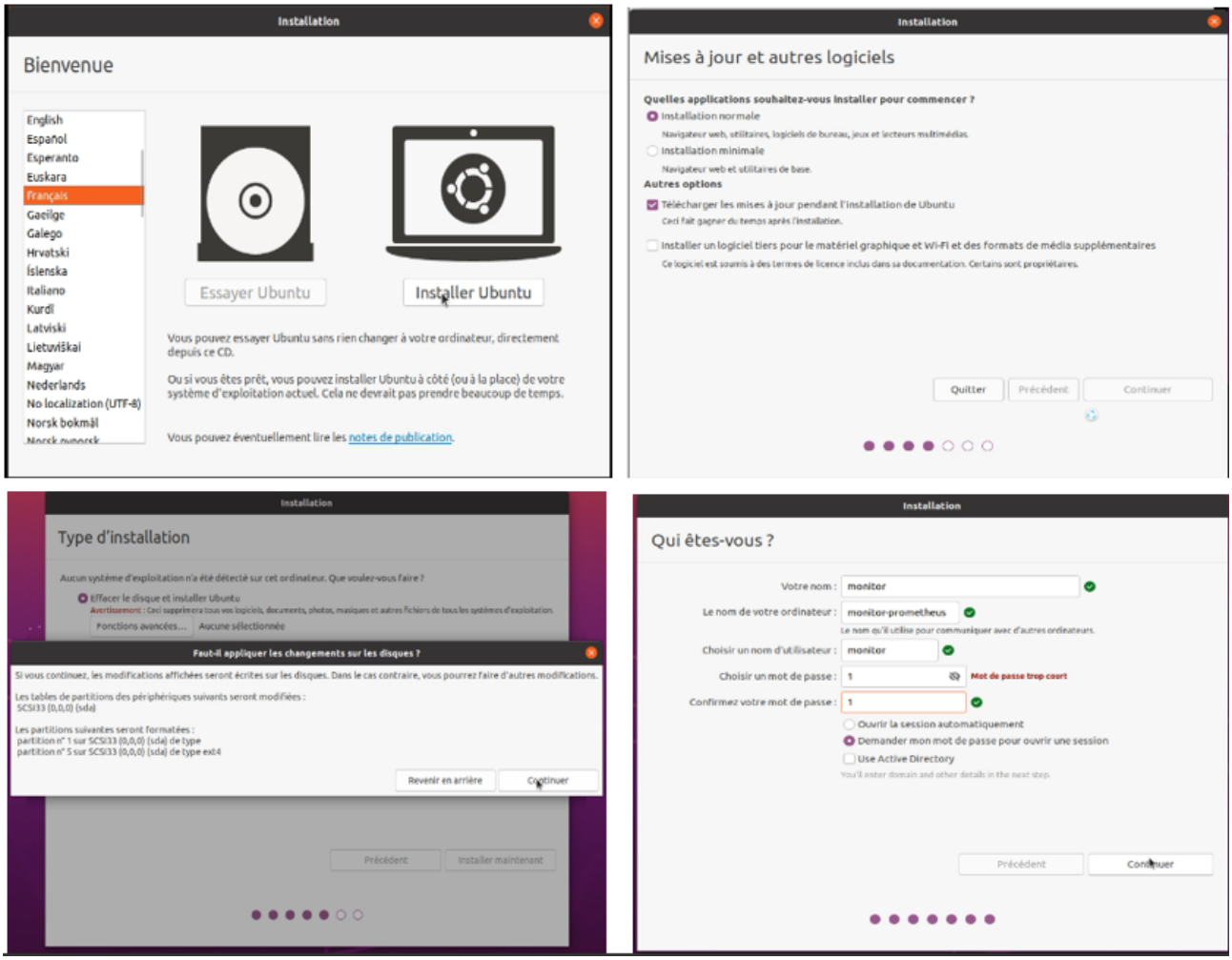

FIGURE 9 – L'instalation de Ubuntu Desktop

Etape3 :

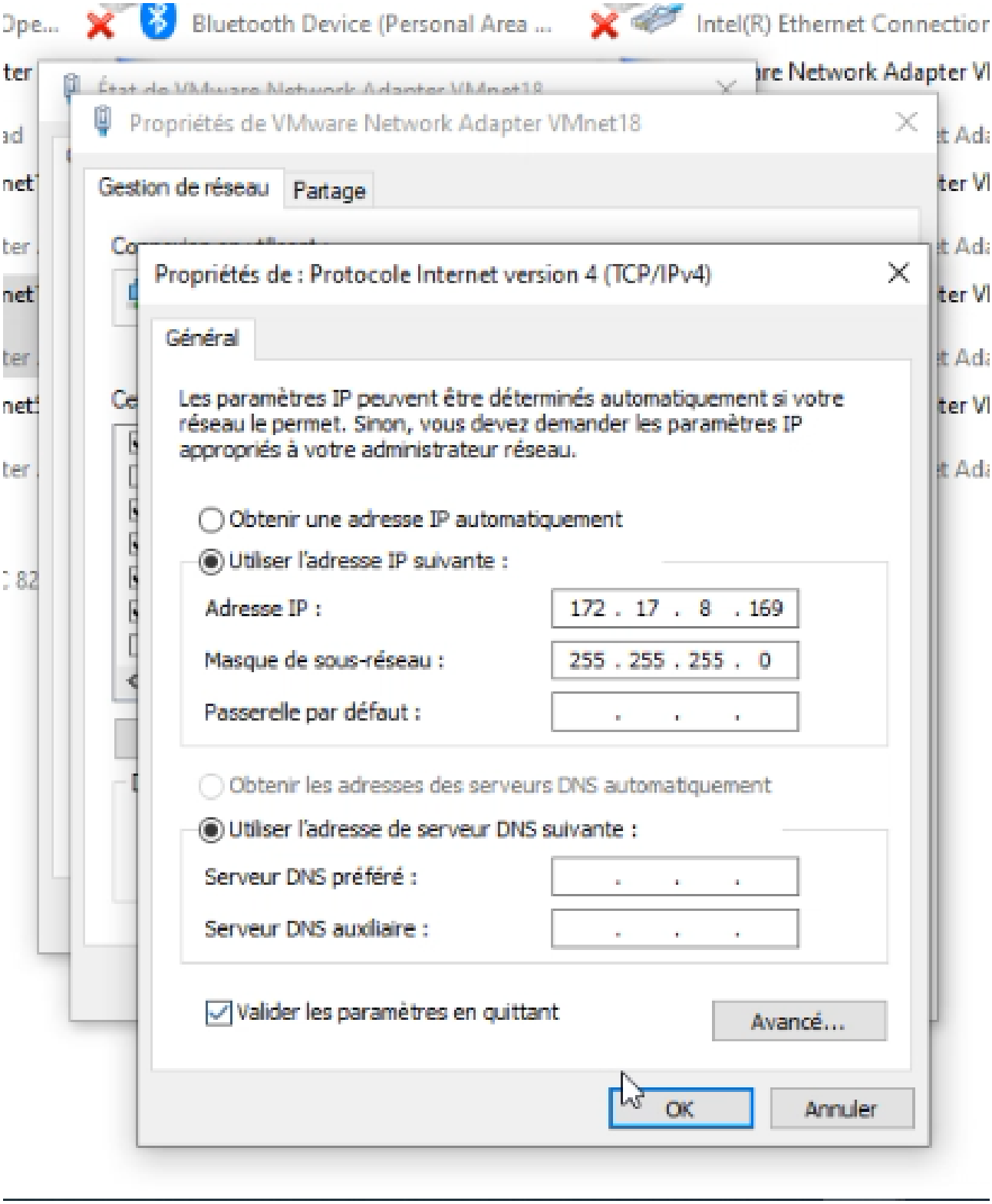

FIGURE 10 – Attribution d'une adresse ip au vmnet 18

Etape4 :

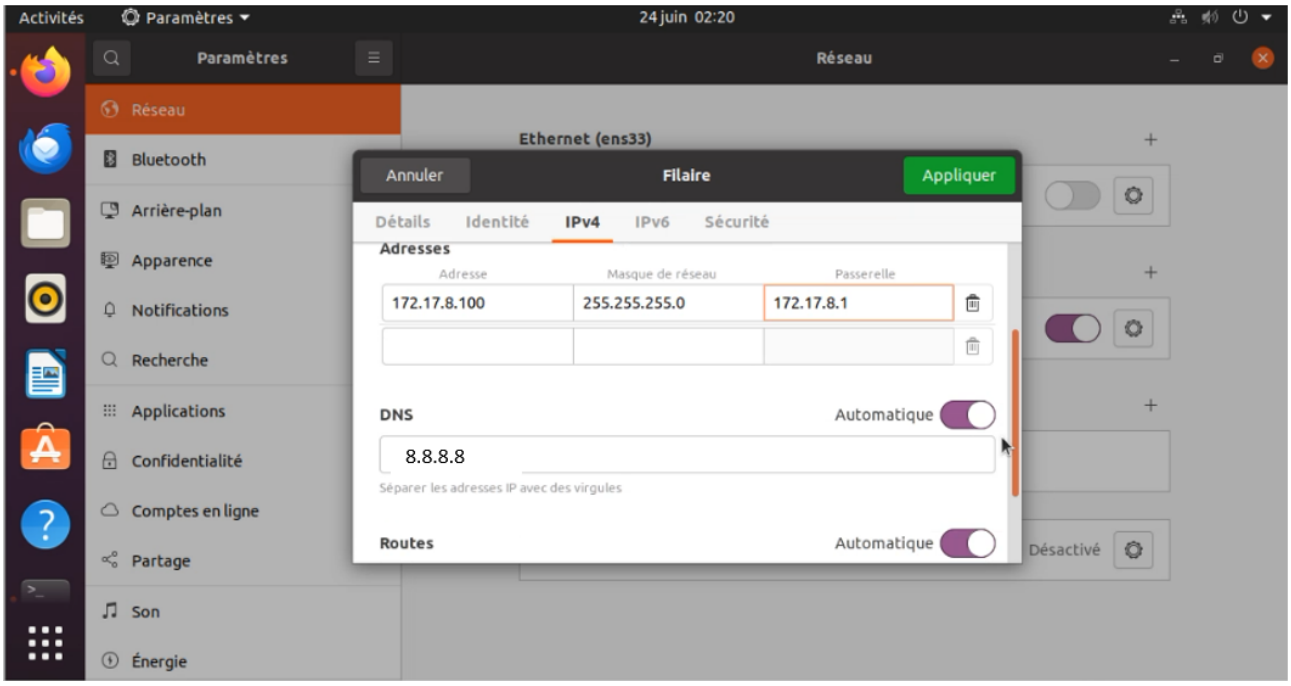

FIGURE 11 – Attribution de l'adresse

Annexe 5

ESXI

Etape1 :

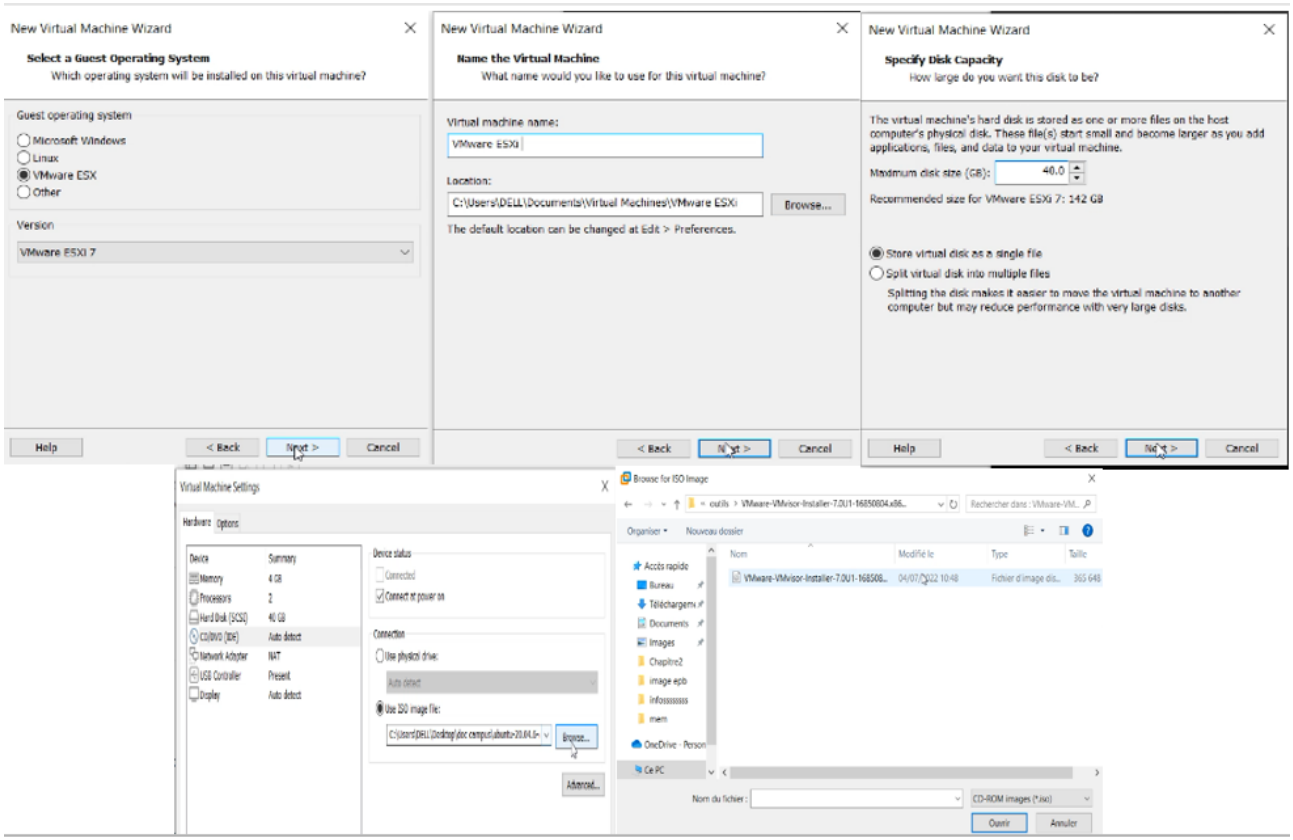

FIGURE 12 – Clonage de la machine virtuelle ESXI

Etape2 :

FIGURE 13 – Installation ESXI

Etape3 :

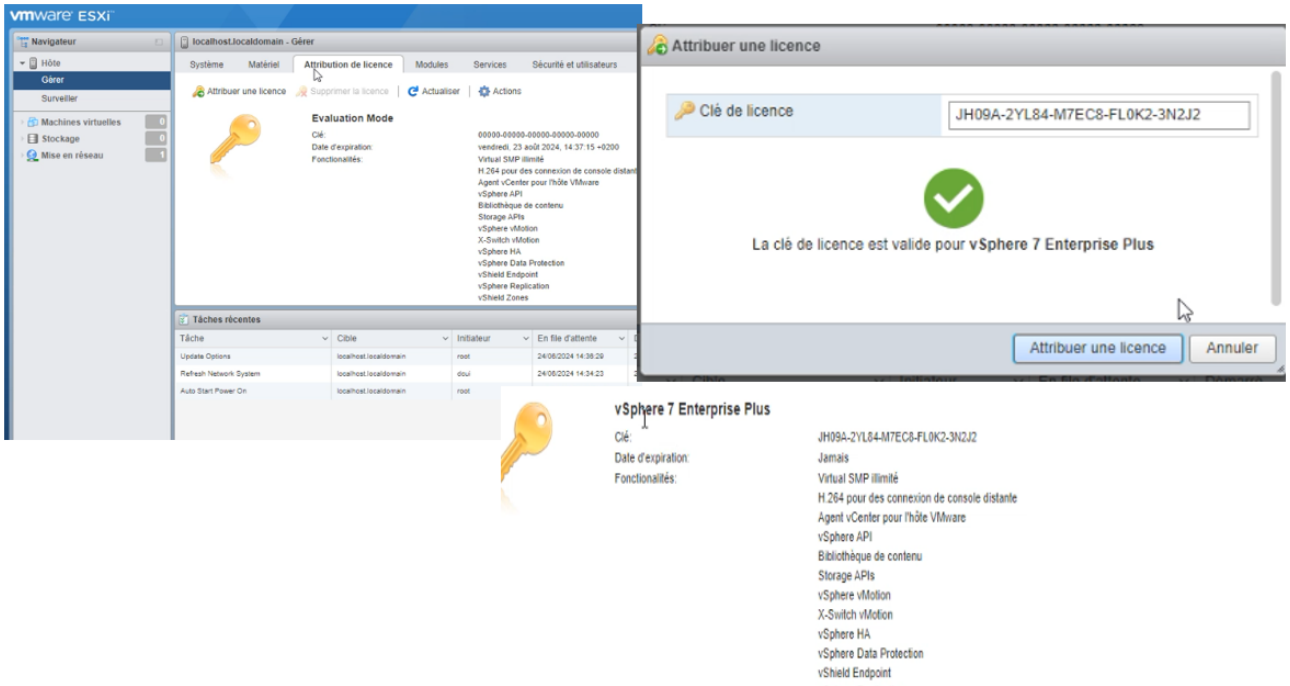

FIGURE 14 – Activation du VSphere.

Annexe 6

Pfsense

Etape1 :

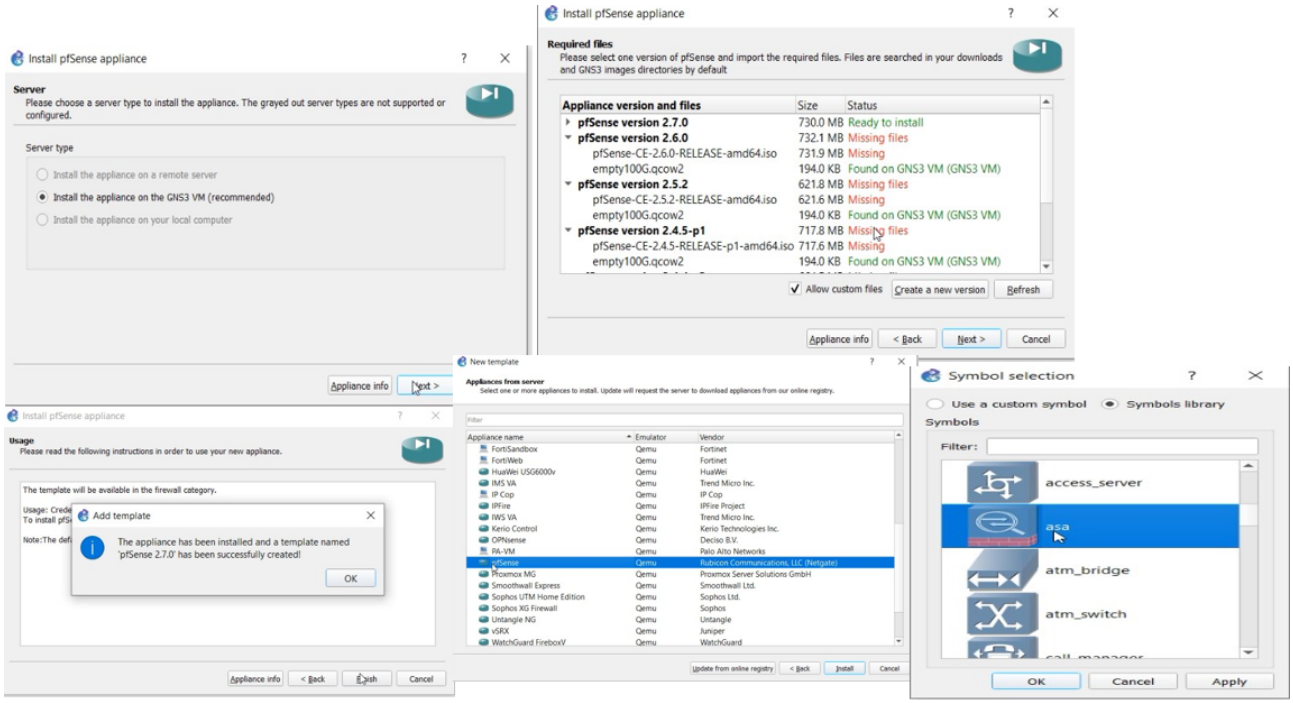

FIGURE 15 – Importation du Pfsense sur Gns3

Etape2 :

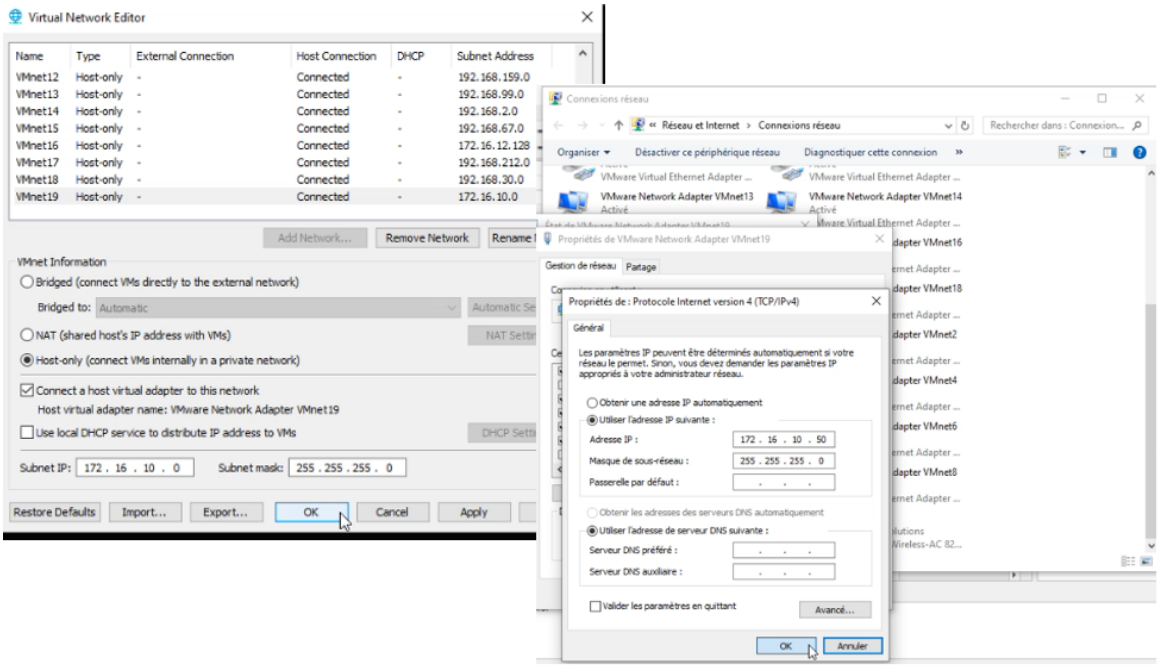

FIGURE 16 – Activation du Network Adapter sur vmnet19

Résumé

Les réseaux informatiques jouent un rôle crucial dans le fonctionnement des entreprises, facilitant la communication et la coordination des opérations. Cependant, ces réseaux sont confrontés à divers problèmes tels que les pannes, la congestion et les attaques de sécurité, ce qui rend la surveillance continue essentielle pour assurer leur fiabilité et leur performance. Ce mémoire se concentre sur l'étude et la mise en place de l'outil Prometheus comme solution de monitoring au sein de l'entreprise portuaire de Bejaïa. Après une analyse approfondie des besoins spécifiques de l'entreprise, Prometheus a été choisi pour ses capacités de supervision en temps réel, sa flexibilité et son extensibilité. La mise en œuvre a inclus la configuration des métriques, des alertes et des tableaux de bord, permettant une gestion optimale des ressources et une détection proactive des anomalies. Cela a conduit à une amélioration significative de la surveillance et de la performance des systèmes informatiques de l'entreprise, assurant ainsi une meilleure continuité des opérations.

Mots-clés : Prometheus, Monitoring, Supervision, Métriques, Alertes, Tableaux de bord

Abstract

Computer networks play a crucial role in the functioning of businesses, facilitating communication and coordination of operations. However, these networks face various issues such as outages, congestion, and security attacks, making continuous monitoring essential to ensure their reliability and performance. This thesis focuses on the study and implementation of the Prometheus tool as a monitoring solution within the port company of Bejaïa. After an in-depth analysis of the company's specific needs, Prometheus was chosen for its real-time supervision capabilities, flexibility, and extensibility. The implementation included the configuration of metrics, alerts, and dashboards, enabling optimal resource management and proactive anomaly detection. This led to a significant improvement in the monitoring and performance of the company's IT systems, thus ensuring better continuity of operations.

Keywords : Monitoring, Prometheus, Supervision, Metrics, Alerts, Dashboards