République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunication

Spécialité : Réseau et télécommunication

Thème

Etude et mise en place d'un serveur supervision zabbix. Cas EPB

Préparé par :

- **M elle BENABAS Djamila**
- **M elle BENZEMMA Djedjiga**

Dirigé par :

Mr BERRAH Smail

Mr IMLOUL Fatah

Examiné par :

Présidente : M me OUALI Kahina

Examinatrice : M me GHANNEM Souhila

Année Universitaire : 2023-2024

Remerciements

D'abord au bon dieu ALLAH, le grand et l'infini et le tout puissant de nous avoir illuminées et ouvert les portes du savoir et nous avoir données la volonté, la santé et le courage pour effectuer ce travail.

Nous remercions notre encadrant, Mr BERRAH Smail, pour ses précieux conseils, orientations, disponibilité, sympathie et le temps qu'il nous a accordé tout au long de notre projet.

Nous remercions également tout le personnel d'entreprise Portuaire de Bejaïa en particulier Mr IMLOUL Fatah, pour les informations et leur contribution et pour mise à notre disposition.

Nous tenons également à exprimer notre reconnaissance à l'ensemble des membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous remercions tous les professeurs qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous a aidés à mener à terme notre projet.

- B.Djamila & B.Djedjiga -

Dédicaces

Je remercie Allah de m'avoir donné la force et le courage pour pouvoir réaliser ce modeste travail.

Avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce

Modeste travail :

À mes très chers parents « Nacira et Omar que j'aime énormément », pour leur

Patience, leur amour, leur encouragement et leur sacrifice tout au long de mon

Parcours et que dieux vous garde en bonne santé pour nous ;

À ma cher et petite sœur, ma meilleure amie « Thanina » ; que le bon dieu te garde pour nous, ma lumière ;

À mon seul et petit frère « Walid » ; tu resteras mon petit pour toujours et je te souhaite réussir dans ta vie ;

À ma chère tante et grande sœur « Zahira » ; merci pour ta présence et ton

Soutien ma belle ;

Et surtout à Ma Grand-mère « Mamah » que le bon dieu garde pour nous et

L'accueille dans son vaste paradis

À toute la famille BENABAS et MAOUCHI

À ma cher binôme Djedjiga ainsi qu'à sa famille ;

À tous mes amis(es)surtout ;

Et à tous ceux qui m'ont aidé de près ou de loin à l'élaboration de ce travail.

B.Djamila -

Dédicaces

Je remercie Allah de m'avoir donné la force et le courage pour pouvoir réaliser ce modeste travail.

Avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce modeste travail :

À mes très chers parents « Messad et Lounis que j'aime énormément », pour leur patience, leur amour, leur encouragement et leur sacrifice tout au long de mon Parcours et que dieux vous garde en bonne santé pour nous ;

A mes chers frères « Soufiane et Haman »merci pourleur amour, encouragement, leur accompagne ;

A mes chers sœurs« Lynda, Nassima, Lamia » pour leur grand amour et leur soutien ;

Et surtout à Ma Grand-mère« Nouara » que le bon dieu garde pour nous ;

À toute la famille Benzemma

À ma cher binôme Djamila ainsi qu'à sa famille ;

À tous mes amis(es)surtout ;

Et à tous ceux qui m'ont aidé de près ou de loin à l'élaboration de ce travail.

- B.Djedjiga -

Sommaire

Sommaire

Liste d'abréviation

ACL Liste de Contrôle d'Accès

ARP L'Address Resolution Protocol

ASN Abstract Syntax Notation One

CPU Cenral Process Unit

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DSI Direction des Systèmes d'Information

FTP File Transfert Protocol

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IGMP Internet Group Management Protocol

IP protocole Internet

LAN Local Area Network

LLC limited liability company

MAN Métropolitain Area Network

MIB Management Information Base

OID Object Identifier

OSI Open Systems Interconnection

PAN personals Area Network

PHP Hypertext Preprocessor

POP Post Office Protocol

RARP Reverse Address Resolution Protocol

SI système informatique

SMI Système de Management Intégré

SMTP Simple Mail Transport Protocol

SNMP Simple Network Management Protocol

SO International Organization for Standardization

SSMTP Simple Mail Transfer Protocol

TCP IP Transmission Control Protocol

TELNET Telle communication Network

UDP User Datagram Protocol

USM User-based Security Model

VLAN Virtual Local Area Network

VPN Virtual Private Network

VTP VLAN Trunking Protocol

WAN Wide Area Network

YAML YAML Ain't Markup Language

Liste des tableaux

Liste des figures

Liste des figures

Liste des figures

Introduction Générale

Les entreprises, quel que soit leur secteur d'activité, s'efforcent toujours de rester compétitives sur le plan économique tout en préservant leur réputation. Elles accordent ainsi une grande importance à leur infrastructure informatique dans sa globalité, car le système d'information et de communication est désormais l'élément essentiel de toute entreprise. Ce système permet de collecter, de traiter et de communiquer toutes les données cruciales pour son fonctionnement, représentant ainsi son histoire et son expertise.

Étant au cœur des opérations commerciales, la gestion efficace du système informatique devient donc primordiale pour assurer sa fiabilité et son efficacité. Parallèlement, les incidents tels que les défaillances, les pannes, les coupures et les différents problèmes techniques doivent être réduits, du fait qu'une indisponibilité du système ou du réseau peut causer des pertes considérables, Ainsi, la mise en place d'une surveillance et d'un contrôle rigoureux, sous la forme de la "supervision informatique".

La supervision revêt une importance cruciale dans la surveillance et le contrôle en temps réel des systèmes informatiques et des réseaux d'une entreprise. Grâce à l'utilisation d'outils de supervision avancés, les équipes informatiques peuvent collecter et analyser en continu des données, ce qui leur permet de repérer les problèmes potentiels et d'intervenir avant qu'ils ne deviennent des incidents majeurs. La supervision permet de suivre de près les performances du réseau, les temps de réponse, les niveaux de charge, la sécurité et divers autres paramètres critiques. Cette approche proactive aide les équipes informatiques à repérer les problèmes naissants, à identifier leurs causes profondes et à prendre des mesures correctives avant qu'ils ne s'aggravent**.**

L'objectif de ce projet est de mettre en place un outil de supervision basé sur le logiciel Zabbix, que nous allons configurer sur une machine virtuelle utilisant le système d'exploitation Linux. Pour bien comprendre le travail et bien cerner les problèmes techniques, nous avons réalisé un stage au niveau de l'EPB, qui se charge de la promotion immobilière. Ceci nous a permis d'établir la problématique qui consiste en la détection de pannes.

Afin d'atteindre les objectifs visés, notre mémoire sera structuré sur quatre parties, comme suite :

✓ Dans le premier chapitre, nous procéderons à la présentation générale de l'organisme d'accueil EPB et sa structure organisationnelle, ceci afin de tirer une problématique à traiter dans le cadre de notre projet et énumérer les différentes solutions.

- ✓ Le deuxième chapitre aborde des généralités sur les réseaux et sécurité informatique.
- ✓ Le troisième chapitre portera sur la description du concept de supervision, ainsi que le protocole qui permet la supervision d'infrastructures réseaux et la présentation des différents outils de supervision.
- ✓ En dernier chapitre, nous illustrerons les étapes de notre travail et nous réaliserons quelques tests
- ✓ Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire.

Chapitre I

Présentation et organisme d'accueil

Introduction

Dans cette partie, nous allons vous présenter l'EPB (Entreprise Portuaire de Bejaïa), où nous avons effectué notre stage pour ce projet. Nous commencerons par vous donner un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Ensuite, nous analyserons le réseau informatique et les composants qui ont mis en place dans l'entreprise.

1. Présentation et organisme d'accueil

Le port de Bejaia est un port algérien situé dans la région de Kabylie dans le nord du pays. Il est notamment consacré au commerce international et aux hydrocarbures .il joue un rôle très important dans les transactions internationales vu sa place et sa position géographique.

Aujourd'hui, il est classé 2`eme port d'Algérie en marchandises générales, et 3`eme port Pétrolier. Il est ´également le 1er port du bassin m´méditerranéen certifié ISO 9001.2000 pour L'ensemble de ses prestations, et à avoir installé un système de management de qualité.

Figure 1 : Le port de Bejaia.

1.1. Historique

Présentant des sites de mouillage naturels, Bejaia a toujours attiré les navires qui y trouvaient dans la baie un refuge sûr, la réalisation du port dans la composante actuelle débuta en 1834, elle fut achevée en 1987. C'est en 1960 qu'a été charge le premier pétrolier d'Algérie, et ce depuis le port de Bejaia.

Le port de Bejaïa aujourd'hui est mi réputé mixte ; hydrocarbures et marchandises générale y sont traités. L'aménagement moderne des superstructures, le développement des infrastructures, l'utilisation des moyens de manutention et de techniques adapte à l'évolution de la technologie des navires et enfin ses outils des gestions modernes, ont fait évoluer le port de Bejaïa depuis le milieu des années.

En 2014, un port sec a été construit dans la ville de Tixter, à l'est de la wilaya de Bordj Bou Arreridj permettant de transférer directement les cargaisons vers les haut-plateaux, Cette zone extra-portuaire affectée au port de Bejaia permettra de le désengorger. La zone aura une superficie de 20 hectares et sera reliée par chemin de fer au Port de Bejaia, via Bordj Bou Arreridj. Le port sec a une capacité de 500 000 conteneurs par an et de 20 millions de tonnes de fret non-conteneurisables.(1)

1.2. Position géographique

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Il est délimité par (1) :

- Au nord par la route nationale N°9.
- Au sud par les jetées de fermeture et du large sur une largeur de 2 750m.
- A l'est par la jetée Est.
- A l'ouest par la zone industrielle de Bejaia.

2. Les missions et activités de l'EPB

L'entreprise portuaire de Bejaia a plusieurs missions et activités pour promouvoir les échanges extérieurs, gérer le port, exporter des marchandises et développer les infrastructures portuaires. Elle assure également le contrôle et la sécurité des opérations portuaires.

2.1. Les Missions de l'entreprise

L'entreprise Portuaire de Bejaia a pour missions :

– La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de la gestion de l'EPB, c'est dans le but de promouvoir les échanges extérieurs du pays. Elle se doit d'assumer la police et la sécurité au sein du pays.
– Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures.

2.2. Les Activités de l'entreprise

Les principales activités de l'entreprise sont :

– L'exploitation de l'outillage et des installations portuaires.
– L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la Super structure portuaire.
– L'exercice du monopole des opérations d'acconage et de manutention portuaire.
– L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
– La police et la sécurité portuaire dans la limite géographique du domaine public Portuaire.

3. Présentation des différentes structures de l'EPB

L'entreprise portuaire de Bejaia (EPB) est structurée en différentes directions, chacune dirigée par une Direction Générale qui se charge des actions liées à la gestion et au développement de l'entreprise. Chaque partie prenante de l'organisation joue un rôle extrêmement important. Cependant, dans le cadre de cette mémère, nous allons nous Intéresser en exclusivité à la Direction des Systèmes d'Information (DSI).

4. Direction des Systèmes d'Information (DSI)

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. La DSI est une direction de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information.

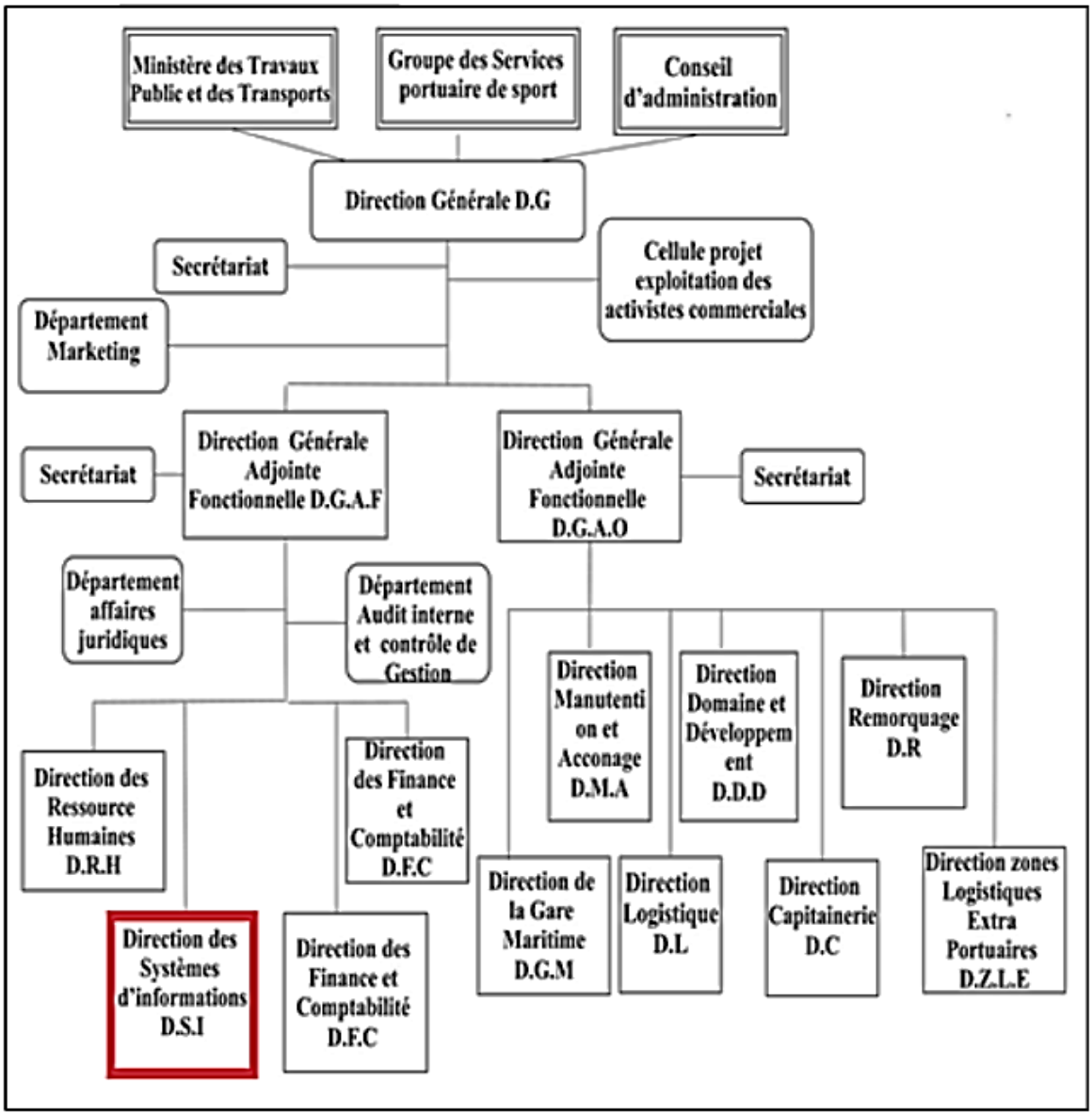


Figure 2 : La structure générale de l'EPB*(1)*

5. Infrastructures Informatique

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 18 (parc à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par fibres optiques de type 4, et 12 brins. Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.(1)

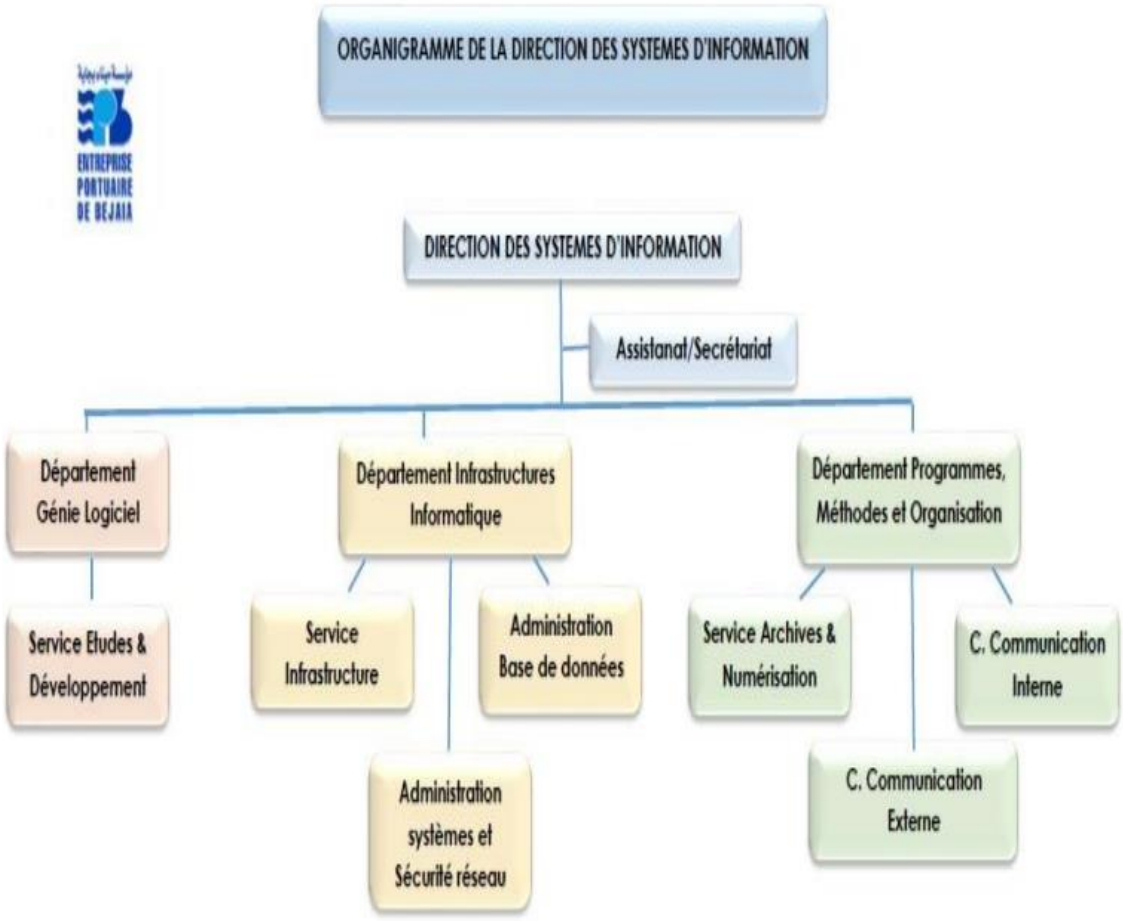


Figure 3 : Organigramme de la Direction des Systèmes(1)

5.1. Le réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail d'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergères en interne nécessaire à l'exécution des tâches quotidiennes des employés. Le réseau du port de Bejaïa s'étend du port pétrolier (N16) aux ports 13 et 18 (port à bois).(1)

5.2. Architecture du réseau local de l'entreprise

L'architecture du réseau LAN de l'entreprise est représentée dans la figure ci-dessous(1) :

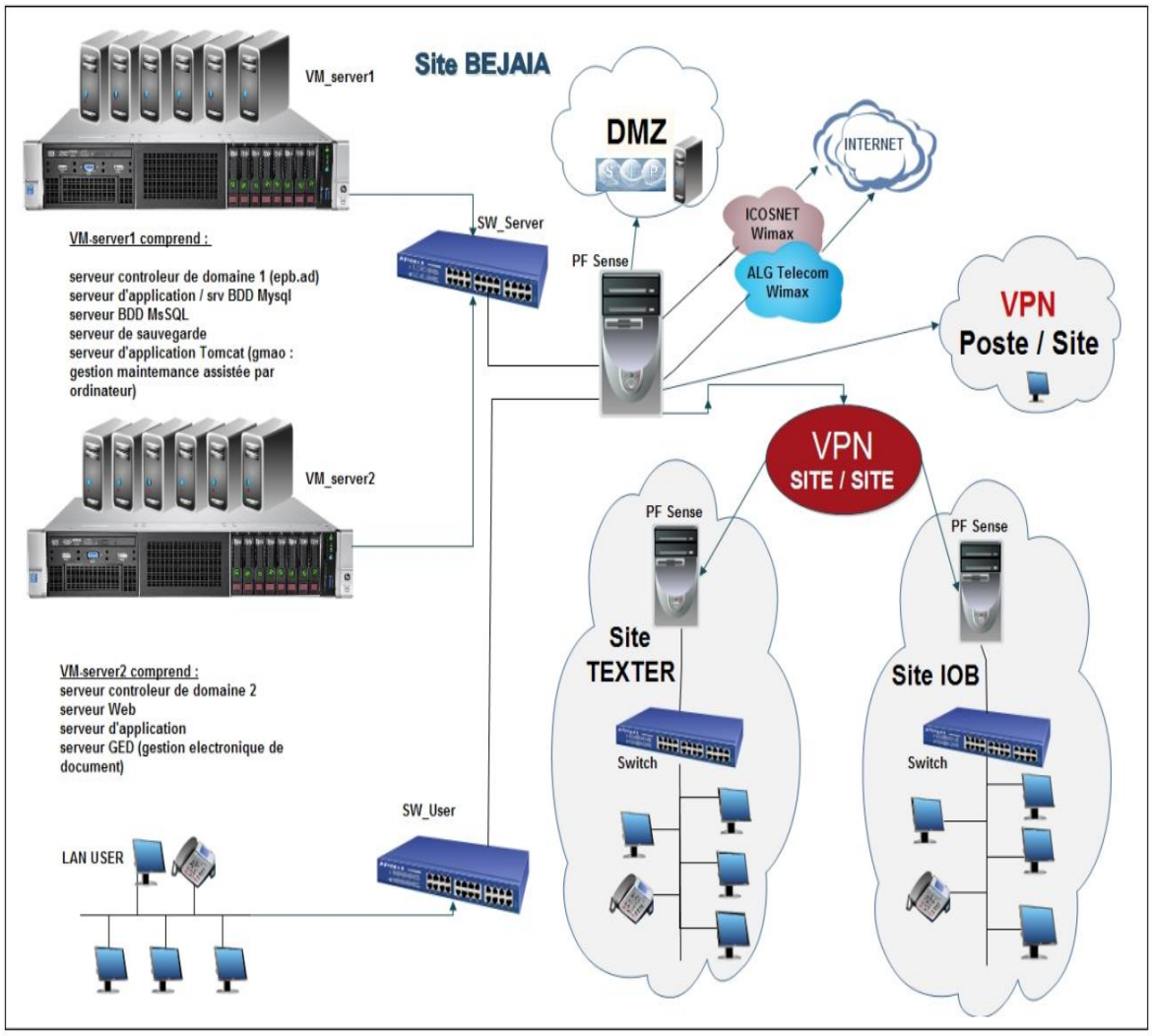


Figure 4 : L'architecture du réseau LAN de l'entreprise EPB.*(1)*

6. Problématique

L'entreprise EPB se trouve confrontée à plusieurs problématiques essentielles dans son fonctionnement quotidien. Parmi celles-ci, la gestion efficace de ses infrastructures informatiques représente un enjeu majeur et la protection contre les cyber menaces et les violations de données est cruciale pour préserver la confidentialité et l'intégrité des informations sensibles de l'entreprise et de ses clients. De plus, la conformité aux réglementations en matière de protection des données, telles que le RGPD, peut représenter un défi supplémentaire nécessitant une surveillance constante et des mesures de sécurité

renforcées. EPB doit assurer la disponibilité et les performances de ses services critiques, tout en minimisant les risques de temps d'arrêt et en optimisant l'utilisation de ses ressources.

7. Solution proposée

La surveillance centralisée du réseau, des serveurs et des différentes applications devient alors cruciale pour détecter rapidement les problèmes potentiels, prévenir les incidents et garantir la continuité de ses activités. En intégrant Zabbix dans son arsenal technologique, EPB peut renforcer sa posture de sécurité en détectant les activités suspectes, en surveillant les vulnérabilités du réseau et en garantissant le respect des normes de conformité, contribuant ainsi à prévenir les risques potentiels pour ses opérations et sa réputation, par exemples :

- **Supervision du réseau et des systèmes :** Zabbix permet de surveiller en temps réel l'état du réseau informatique, des serveurs, des applications et des Gestion des performances : En surveillant les performances des différents éléments du système informatique, Zabbix peut aider à identifier les goulets d'étranglement, les goulots d'étranglement ou les problèmes de performances qui affectent les opérations.
- **Alertes et notifications** : Zabbix peut être configuré pour envoyer des alertes et des notifications en cas de problèmes ou d'événements importants, ce qui permet aux équipes informatiques d'intervenir rapidement pour résoudre les problèmes.
- **Analyse des tendances :** En collectant des données sur les performances du système sur une période de temps prolongée, Zabbix permet d'analyser les tendances et de prévoir les besoins futurs en matière de capacité et de ressources.
- **Sécurité :** Zabbix peut également être utilisé pour surveiller les journaux d'événements et détecter les activités suspectes ou les violations de sécurité potentielles.
- **Conformité et rapports :** Zabbix offre des fonctionnalités de reporting qui peuvent être utilisées pour générer des rapports sur la performance du système, la disponibilité des services, etc., ce qui peut être utile pour répondre aux exigences de conformité ou pour évaluer les performances globales du système.
- **Centralisation de la surveillance :** Dans l'entreprise avec un grand nombre de systèmes et d'applications, Zabbix offre la possibilité de centraliser la surveillance de l'ensemble du parc informatique, ce qui facilite la gestion et la maintenance.

En résumé, Zabbix est souvent utilisé dans les entreprises publiques pour résoudre des problèmes liés à la supervision, à la gestion des performances, à la sécurité et à la conformité,

en offrant des fonctionnalités de surveillance avancées et une capacité de personnalisation étendue.

8. Le parc informatique de l'EPB

L'EPB dispose de 250 PC HP et ACER répartis à travers les différentes directions de l'entreprise et interconnecté à un réseau informatique interconnecté par fibre optique et de câbles à paires torsadés (1)

- Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distributions.
- La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).
- Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.
- Tous les PC sont dotés d'un anti-virus ESET END point.
- Tous les PC sont connectés à l'internet.

Conclusion

À travers ce chapitre, nous avons présenté la structure d'accueil et l'architecture réseau dont elle dispose. Après une étude de l'existant et sa critique, nous avons soulevé quelques problèmes rencontrés par la société ce qui nous a permis de cerner la problématique de notre projet.

Chapitre II
Généralités sur le réseau et la sécurité informatique

Introduction

Les réseaux se développent en fonction de leurs caractéristiques et besoins, ils deviennent aujourd'hui une infrastructure indispensable dans tous les domaines de la vie, Cependant, les menaces et les attaques sur les réseaux prennent de nouvelles mises à jour représentant les pires ennemis de cette évolution. Pour cela, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

Dans ce chapitre, nous allons définir quelques notions fondamentales sur les réseaux informatiques, les types et les différentes topologies ainsi le modèle OSI et TCP/IP pour terminer le chapitre avec une présentation générale de la sécurité informatique.

1. La définition d'un réseau informatique

Un réseau informatique est un ensemble matérielles et logicielles interconnecté via un support physique tels que des ordinateurs, des imprimantes, des scanners, des modems, des routeurs, des commutateurs, etc. Via des ondes radio.

L'objectif principal d'un réseau informatique est de permettre l'échange d'informations, que ce soit par le biais de messageries, de transferts de fichiers, d'interrogations de bases de données, etc. Cela permet aux utilisateurs de partager des données et des applications, de les sécuriser, de communiquer entre eux et d'accéder à Internet.

2. Les différentes types des réseaux informatiques

Il existe différents types de réseaux qui sont classés en fonction de nombre d'utilisateur, de leur vitesse de transfert de données :

Figure 5: Le réseau informatique

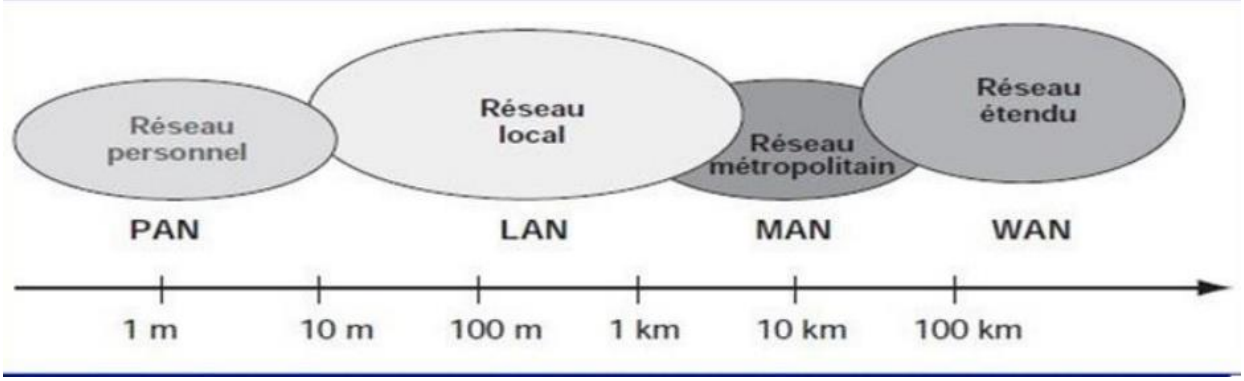


Figure 6: La taille des différentes catégories de réseaux informatiques.*(2)*

2.1. Les réseaux personnels

2.1.1. PAN (personnels Area Network)

Il est un petit réseau permet d'échange des données entre des appareils proche (généralement dans la même pièce) tels que : ordinateurs portable, des téléphones mobiles, des agendas électronique …etc. Ils couvrent une distance de quelques mètres.

2.1.2. Les réseaux locaux : LAN (Local Area Network)

Il un réseau qui se trouve sur une zone géographique limité, telle qu'un bureau, une maison et un campus (donc il est utilisé dans les environnements de travail et domestique pour faciliter la collaboration et l'accès aux ressources partagées).

Le LAN permet de transmettre une grande quantité rapidement, celui-ci vous permet de partager des serveurs, de fichier, impriment ou encore des applications, il est généralement basé sur des technologies des câbles telles que l'Ethernet ou des réseaux son fil comme le Wi-Fi.

2.1.3. Les réseaux métropolitains : MAN (Métropolitain Area Network)

Il est un réseau qui s'étend sur une région de la taille d'une zone métropolitaine. Le MAN permet de relie plusieurs LAN proches. Celui-ci permet d'échange très rapidement des données entre différents branches d'une société par exemple. En utilisent la fibre optique et des routeurs assez puissants, l'échange de données est plus rapide que via l'internet. Un MAN permet la communication entre des nœuds distants sur une distance maximale de quelques kilomètres à des débits élevés.

2.1.4. Les réseaux étendus : WAN (Wide Area Network)

Il connecte des dispositifs sur de vastes distances géographiques, couvrant souvent des régions étendues, des villes, des pays ou même des continents. Contrairement aux réseaux LAN qui opèrent localement, les réseaux WAN utilisent généralement des liaisons de communication longue distance, telles que des lignes de télécommunication louées, des liaisons par satellite ou des connexions via Internet, pour connecter des sites distants. Les réseaux WAN sont couramment utilisés par les organisations pour relier leurs bureaux régionaux et leurs centres de données répartis géographiquement. Ils permettent le partage de ressources, la communication entre les sites et l'accès aux services centralisés. Internet est l'un des plus grands exemples de WAN, permettant la communication et le partage de données à l'échelle mondiale.(2)

3. Les Topologies des réseaux

La topologie d'un réseau fait référence à la façon dont les équipements sont interconnectés entre eux, à savoir :

3.1. La Topologie en bus

C'est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire des câbles, généralement de type coaxial tel qu'il est illustré dans la figure 7. Une seule station émet en même temps. À chaque extrémité, le réseau est terminé par un bouchon, qui empêche l'apparition de signaux parasites. Cette topologie a pour avantage d'être facile à mettre en

œuvre et de posséder un fonctionnement simple. En revanche, si l'une des connexions est défectueuse, l'ensemble du réseau est affecté.

Figure 7 : La topologie en bus.

3.2. La Topologie en étoile

Dans une topologie en étoile les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles nous pouvons connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

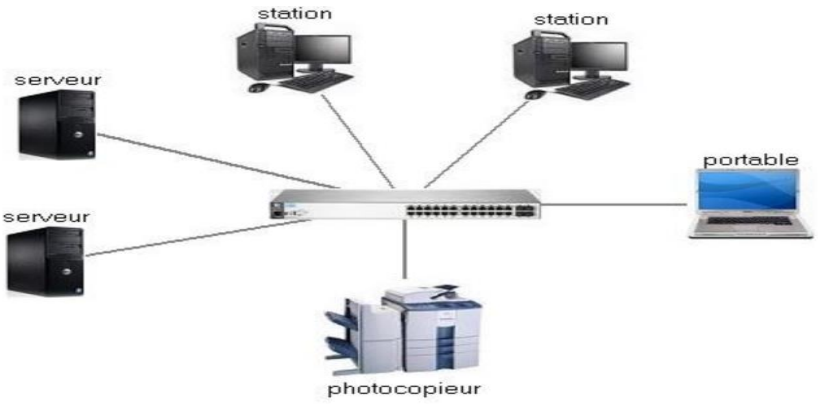


Figure 8: La topologie en étoile.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux à topologie en étoile sont beaucoup moins vulnérables car nous pouvons aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau. En revanche, un réseau à topologie en étoile est plus coûteux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire à savoir le hub.

3.3. La Topologie en anneau

La topologie d'anneau est un type de configuration de réseau où les périphériques sont connectés de manière circulaire, formant ainsi une boucle fermée. Dans cette configuration, chaque appareil est connecté à exactement deux autres appareils, ce qui crée une voie continue pour la transmission de données. Cela signifie que les données voyagent dans une seule direction autour de l'anneau, en passant par chaque appareil jusqu'à ce qu'elles atteignent leur destination.

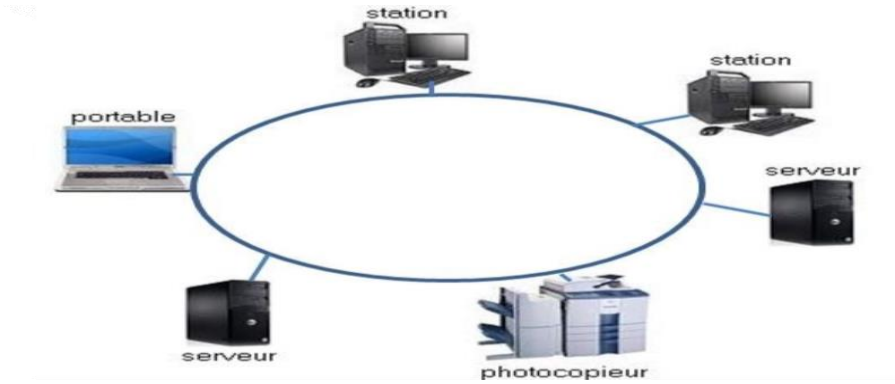


Figure 9 : Topologie en anneau

4. Le Modèle OSI et TCP/IP des réseaux informatiques

4.1. Modèle OSI

Le modèle OSI (open system interconnexion) est un modèle conceptuel créé par l'Organisation internationale de normalisation qui permet à divers systèmes de communication de communiquer à l'aide de protocoles standard. En clair, l'OSI fournit une norme pour que différents systèmes informatiques communiquent entre eux.

Le modèle OSI peut être considéré comme un langage universel pour les réseaux informatiques Il est basé sur un concept consistant à organiser un système de communication en sept couches abstraites, empilées les unes sur les autres, comme indiquer dans la figure 10.(3)

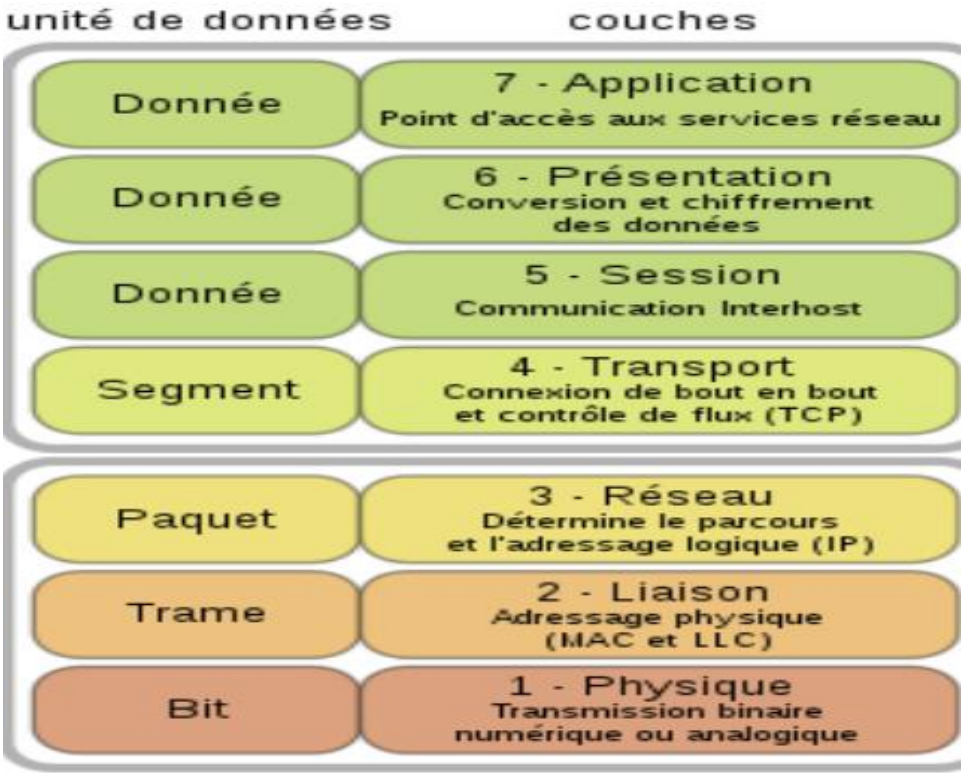


Figure 10 : Le modèle OSI

Les 7 couches du modèle OSI :

– **La couche « physique » :** Cette couche comprend les équipements physiques impliqués dans le transfert de données, tels que les câbles et les commutateurs. C'est à son niveau où les données sont converties en un flux de bits, c'est-à-dire une chaîne de 1 et de 0.

– **La couche « liaison de données » :** Elle assure un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l´établissement, le maintien et la libération du lien logique entre les entités. Elle permet en outre, de détecter les erreurs incohérentes aux supports physiques, Elle est divisée en deux sous-couches :

– La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.

– La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.

– **La couche « réseau » :** Elle permet de gérer le routage des données à travers le réseau en choisissant les chemins les plus efficaces, évitant la congestion et assurant la qualité de service. Elle divise les données en paquets, les dirige vers leur destination et surveille le trafic pour maintenir une communication fluide.

– **La couche « transport » :** Elle est la couche pivot du modèle OSI., elle assure le contrôle du transfert de bout en bout (end to end) lors du transfert des informations (messages) entre les deux extrémités communicantes donc elle est également responsable du contrôle de flux, du contrôle d'erreurs et du contrôle de congestion. La couche transport segment les données envoyées par la machine source en paquet et les ressemble en flux de donnée sur la machine destinatrice. Exemple : protocoles TCP, UDP

– **La couche « session » :** Elle gère l'´échange de données entre les applications distantes. La couche session fournit des services a la couche présentation. La fonction essentielle de cette couche est la synchronisation des ´échanges et la d´finition de points de reprise.

– **La couche « présentation » :** Elle convertit les données en informations compréhensibles par les applications et les utilisateurs ; syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.

– **La couche « application » :** Cette couche est responsable des services et des protocoles qui permettent aux applications de communiquer entre elles en utilisent des protocoles tel que HTTP qui utilisé pour le transfert de donnes sur le web, FTP pour transfert de fichier et SMTP pour l'envoi de courriers électronique

4.2. Modèle TCP/IP

Le modèle de référence TCP/IP est une suite de protocoles de communication a quatre couches utilisées pour interconnecter des périphériques réseaux sur Internet qui a été développé par la DARPA (Defense Advanced Research Project Agency USA).

Le protocole Internet (IP) est le système d'adressage de l'Internet et a pour fonction principale de transmettre des paquets d'informations d'un dispositif source à un dispositif cible. L'IP est le principal moyen d'établir des connexions réseau et constitue la base de l'Internet. Ces fonctionnalités nécessitent un autre protocole, généralement c'est le TCP.(4)

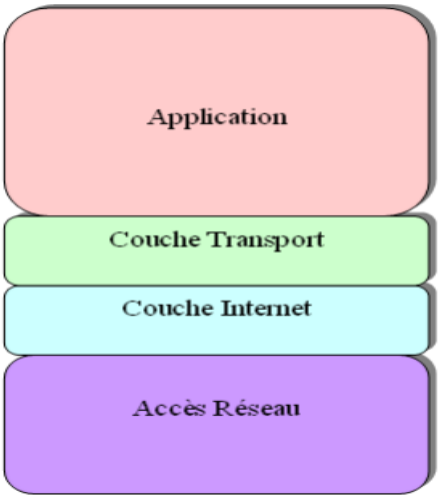


Figure 11 : Le modèle TCP/IP

Les quatre couches du modèle TCP /IP sont :

– **Couche Accès Réseau :** C'est la couche la plus basse de la pile TCP/IP. Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique. Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé et permet la conversion des signaux analogiques/numériques. Elle est composée de deux niveaux MAC et LLC.

– **Couche Internet :** Elle est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recomposition des segments. La couche Internet utilise les cinq protocoles suivants : IP (Internet Protocol), ARP (Adresse Resolution Protocol), ICMP (Internet Control Message Protocol), RARP (Reverse Address Resolution Protocol), IGMP (Internet Group Management Protocol).

– **Couche transport :** La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles TCP fournit d'excellents moyens de créer avec souplesse des communications réseau fiables.

– **Couche application :** Elle reprend les applications standards en réseau informatique et Internet. Elle dispose des protocoles suivants : SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), TELNET (Telle communication Network), FTP (File Transfert Protocol).

5. Les réseaux d'entreprises

Le réseau d'entreprise permet de relier chaque ordinateur entre eux via un serveur qui va gérer l'accès à Internet, les e-mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers. Le réseau d'entreprise permet de centraliser les données de l'entreprise, les sécurisés et de travailler en équipe.(5)

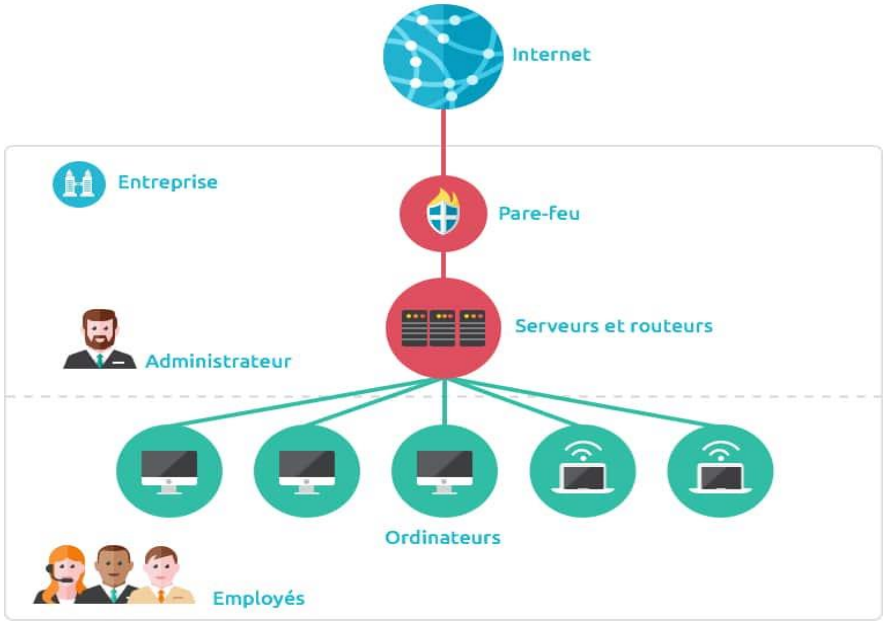


Figure 12 : Le schéma d'un réseau d'entreprise

6. Sécurité informatique

6.1. Définition de sécurité

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité.(6)

6.2. Les Critères de sécurité

La sécurité informatique vise cinq principaux critères. Comme illustré dans la figure 13:

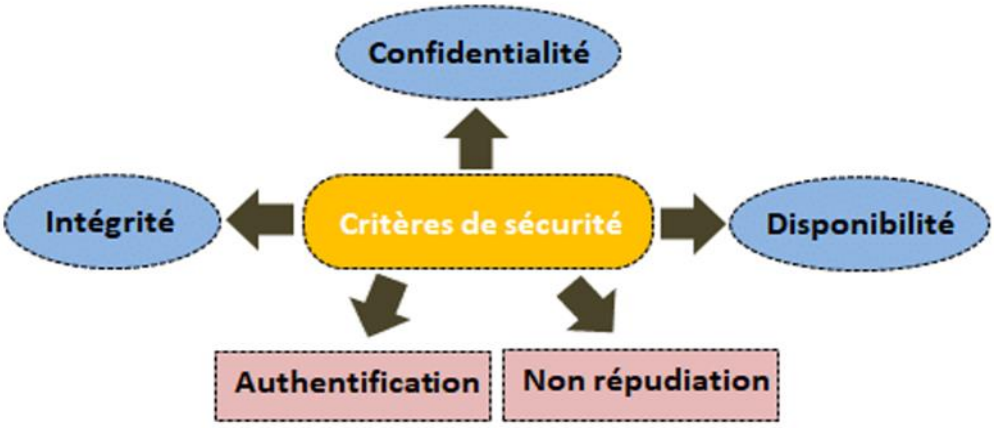


Figure 13 : Les cinq dimensions de la sécurité informatique.

– **La confidentialité :** C'est un ensemble de mécanismes permettant à une communication de données de rester privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.

– **L'authentification :** Est un processus qui permet comment vérifier l'identité d'une personne ou d'une entité. Son but est de s'assurer que seules les personnes autorisées peuvent accéder aux ressources. En d'autres termes, l'authentification garantit que seules les personnes légitimes ont accès aux informations et aux fonctionnalités qui leur sont autorisées.

– **L'intégrité :** C'est un ensemble des mécanismes permet d'assurer la fiabilité des données. Les données reçues par le destinataire doivent être les mêmes que les données envoyées par le récepteur.

– **La disponibilité :** La disponibilité de l'information consiste à s'assurer qu'elle est toujours accessible pour les utilisateurs finaux et les applications, quels que soient les événements (forte charge du réseau, panne d'équipement, etc.).

– **Non répudiation :** C'est un mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

6.3. Terminologie de sécurité

La sécurité informatique utilise un langage spécifique pour mieux comprendre les risques liés aux attaques informatiques. Cela permet de définir clairement certains termes importants pour mieux se protéger :

– **Vulnérabilité :** Une vulnérabilité est une faille de sécurité, souvent cachée, qui affecte une infrastructure informatique. Ce terme est généralement associé aux logiciels, mais il englobe également toutes les faiblesses, quelles qu'elles soient. Par exemple, une mauvaise configuration d'un équipement réseau ou l'utilisation d'un mot de passe vide ou trivial peuvent constituer des vulnérabilités.

– **Menace :** Les menaces sont des actions potentiellement nuisibles pour un système informatique. Elles peuvent provenir de différentes sources.

– **Risque :** Le risque représente la probabilité d'un événement dommageable et les coûts qui en découlent. Il dépend également de la valeur des éléments à protéger.

– **Attaque :** Une attaque est une méthode utilisée pour exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité, mais toutes les vulnérabilités ne sont pas exploitables.

– **Contre-mesures :** sont des procédures ou techniques utilisées pour remédier à une vulnérabilité ou contrer une attaque spécifique. Il est important de noter qu'il peut y avoir d'autres attaques exploitant la même vulnérabilité.

6.4. Les différents types d'attaque

Les attaques peuvent être regroupées en trois familles différentes : (6)

- **Les attaques directes**

C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

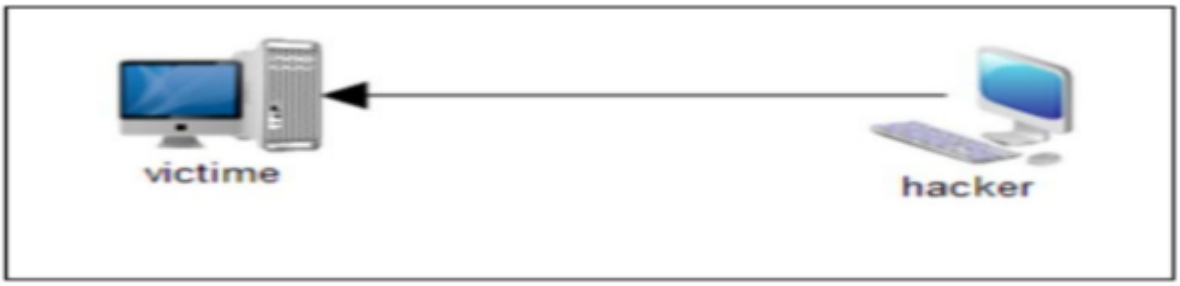


Figure 14: Attaque directe*(6)*

- **Les attaques indirectes par rebond :**

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

– Masquer l'identité (l'adresse IP) de l'hacker.

– Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour réaliser son attaque.

Le principe en lui-même, est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

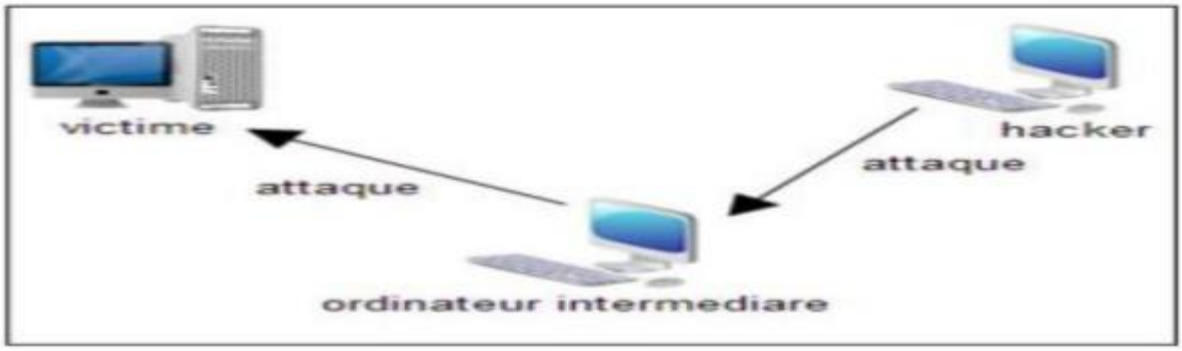


Figure 15: Les attaques indirectes par rebond*(6)*

- **Les attaques indirectes par réponse :**

Cette attaque est un dérivé par rebond. Elle offre les mêmes avantages, du point de vue de l'hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête et c'est cette réponse à la requête qui va être envoyé à l'ordinateur victime.

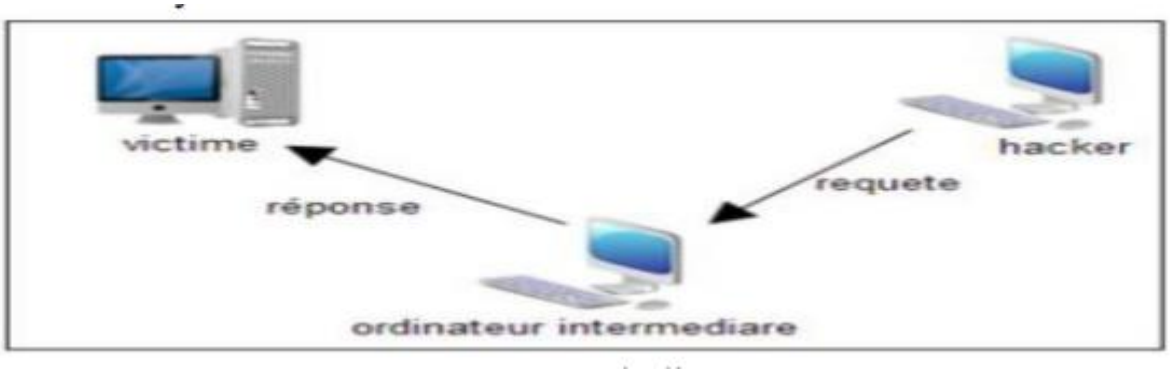


Figure 16: Les attaques indirectes par réponse (6)

6.5. Les dispositifs de protection

6.5.1. Firewall (pare-feu)

Le pare-feu est un dispositif matériel ou logiciel qui permet de contrôler le trafic réseau entrant et sortant d'un système ou d'un réseau informatique. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau (7).

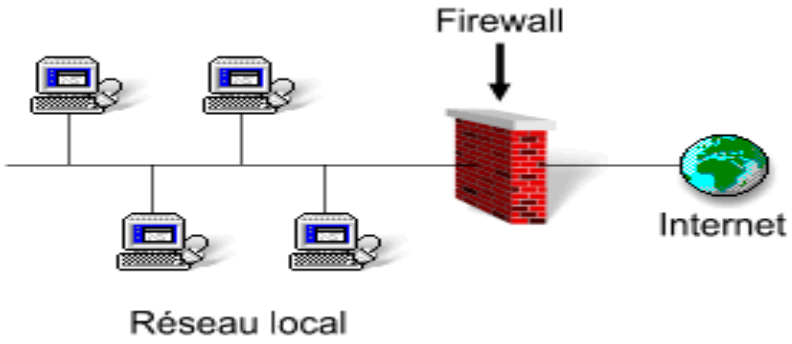


Figure 17 : Le pare-feu.

6.5.2. Proxy

Un serveur proxy se place entre le réseau local et l'extérieur : il peut être vu comme une porte sur l'extérieur. Un serveur proxy est souvent utilisé pour permettre à un réseau local d'accéder de manière transparente à l'Internet, aux sites d'Internet : on parle alors de proxy HTTP mais il peut aussi autoriser l'accès à des serveurs FTP : nous aurons un proxy FTP, il peut exister des serveurs proxy pour chaque protocole applicatif.

Son fonctionnement est simple : il s'agit d'un serveur mandataire par une application pour effectuer ses requêtes sur Internet a sa place. Un serveur proxy est parfois appelé serveur mandataire pour cette raison. Lorsqu'un poste client désire se connecter à l'Internet l'aide d'une application configurée pour se servir d'un serveur proxy. Cette dernière va tout d'abord se connecter au serveur proxy et lui envoyer ses requêtes. Ensuite, le serveur proxy se connectera au serveur distant sur l'Internet et lui on verra ses requêtes. Les réponses de ce serveur seront alors renvoyer au serveur proxy qui les transmettra à l'application du poste client(8).

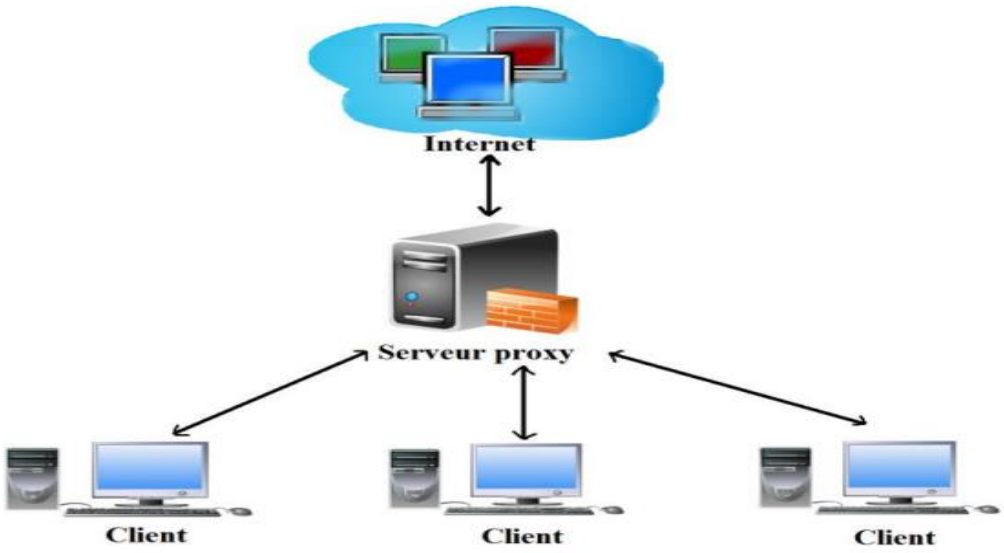


Figure 18 : Le serveur proxy

6.5.3. VLAN (Virtual Local Area Network)

Les entreprises à recourir à la technologie VLAN, afin d'améliorer la sécurité et les performances de leurs réseaux locaux.

Un Vlan est un regroupement de stations de travails indépendamment de la localisation géographique sur le réseau, ces dernières pourront communiquer comme si elles étaient sur le même segment. Il permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.

6.5.4. Les listes de contrôles d'accès (ACL)

Les listes de contrôle d'accès (Access Control List) ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau]. Ils semblent à avoir toujours existé sur les routeurs et rares sont les configurations où elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques (9).

6.5.5. Virtual Private Network (VPN)

VPN est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

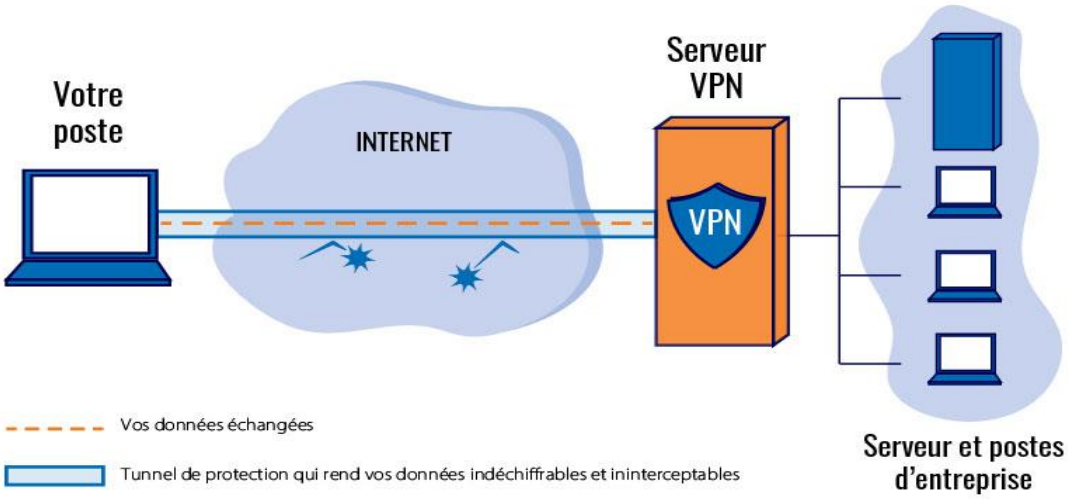


Figure 19 : VPN

Un réseau VPN repose sur le protocole de tunneling. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise. Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.

6.5.6. Zone démilitarisée (DMZ)

Les entreprises disposant d'un site Web public que les clients utilisent doivent rendre leur serveur Web accessible à Internet. Pour protéger le réseau local de l'entreprise, le serveur Web est installé sur un ordinateur distinct des ressources internes. La DMZ permet la communication entre les ressources commerciales protégées, telles que les bases de données internes, et le trafic qualifié d'Internet.

Une DMZ est une zone tampon d'un réseau d'entreprise, située entre le réseau local et internet, derrière le pare-feu. Il a pour fonction principale de permettre aux ordinateurs ou aux hôtes de fournir des services au réseau externe et de fonctionner comme un filtre de

protection pour le réseau interne, agissant comme un « pare-feu » et le protégeant des intrusions malveillantes qui pourraient compromettre la sécurité.

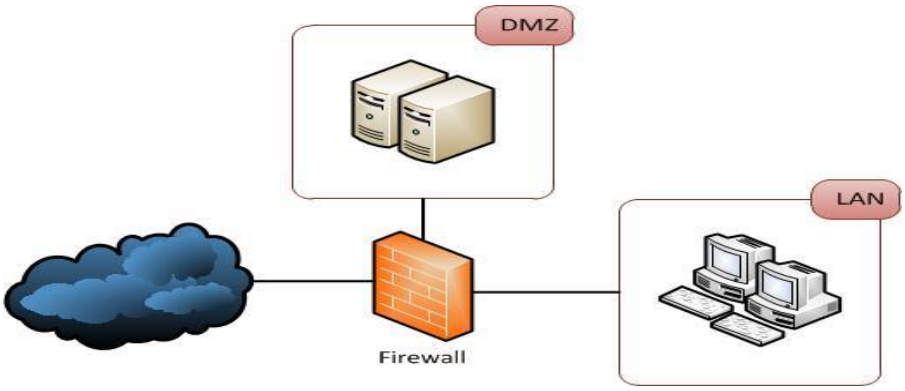


Figure 20 : La DMZ.

Conclusion

Dans ce chapitre, nous avons défini quelques notions fondamentales concernant les réseaux et la sécurité informatique, Le prochain chapitre sera entièrement dédié aux principes et aux concepts de supervision dans un réseau informatique.

.

Chapitre III

Principe et concept de la supervision

Introduction

Les entreprises quel que soit leur domaine d'activité, attachent une grande importance à leur système informatique. C'est ce système qui assure le bon fonctionnement de leurs activités et contribue à maintenir leur réputation et leur compétitivité sur le marché. Il est crucial de surveiller et de superviser l'ensemble du système pour éviter les erreurs et les pannes qui pourraient affecter la performance du réseau et de l'entreprise dans son ensemble. Cela permet à l'administrateur de pouvoir analyser et gérer le système en tout temps. Dans ce chapitre, nous allons donc aborder les différents concepts liés à la supervision. C'est une étape essentielle pour assurer le bon fonctionnement et la stabilité du système informatique d'une entreprise.

1. Monitoring

Le monitoring (ou monitorage en français), désigne le fait de « surveiller ». Cependant, le fait de surveiller quelque chose revient à connaître son état actuel mais aussi l'historique de ses états passés, par l'intermédiaire de valeurs (UP/DOWN) et de données chiffrées (des pourcentages par exemple). C'est ici que l'on retrouve une distinction entre deux notions que sont la supervision et la métrologie(10).

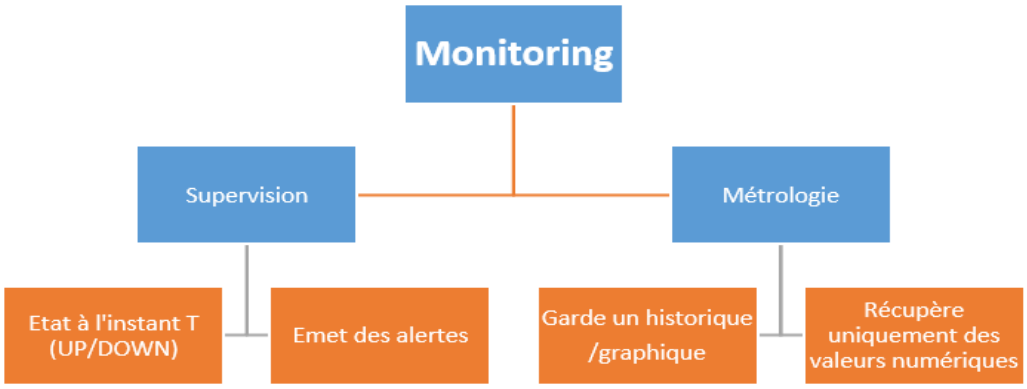


Figure 21 : Organigramme présentant le concept de monitoring

1.1. La supervision

La supervision est la surveillance du bon fonctionnement d'un système ou d'une activité. Elle permet la surveillance du bon fonctionnement des systèmes d'informations et aux administrateurs réseau de surveiller les différents composants matériels et Logiciels, les visualiser, et analyser les différentes informations et données fournies sur eux. L'administrateur peut donc vérifier le fonctionnement normal ou anormal du système informatique et agir pour résoudre ses problèmes. La supervision réseau comprend un

ensemble de protocoles, matériels et logiciels informatiques dont la majorité est basée sur le protocole SNMP permettant de suivre à distance l'activité d'un réseau informatique.

Autour de la supervision, plusieurs modules coexistent :

– La supervision réseau porte à son tour sur la supervision de manière continue de la disponibilité des services en ligne, du fonctionnement du réseau, des débits et bande passante, de la sécurité, etc.

– La supervision système c'est la vérification de la santé des ressources matérielles (la mémoire, le CPU, le disque dur, etc.)

– La notification permet l'envoi d'alertes par email, par sms, par téléphone, par avertissement sonore...

– L'exécution de commandes permet de relancer une application qui fait d´défaut ;

– La retranscription d'état du système permet de voir à tout moment l'état de tous les composants et applications supervisés sous forme d'un graphique, d'une carte ou d'un tableau. Son but est de rendre les résultats plus lisibles ;

– La cartographie visualise le réseau supervisé par l'intermédiaire de cartes, de graphique, de tableau...

– Le « reporting » consiste en un historique complet de la supervision.

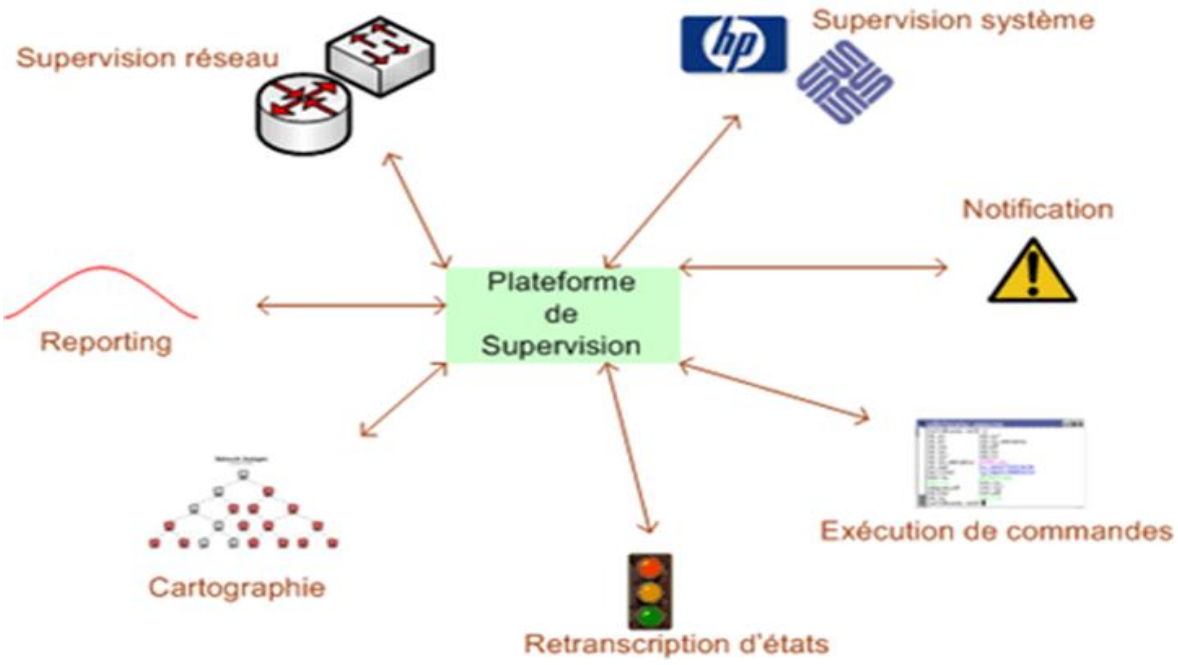


Figure 22 : Les modules de supervision

1.1.1. Le rôle de supervision

Deux phases essentielles permettent aux administrateurs d'atteindre les objectifs de supervision: surveiller le système et garantir sa disponibilité en cas d'anomalie. Nous pouvons citer les rôles suivants :

– Prévenir les problèmes potentiels tels que les pannes matérielles ou les interruptions de service, et assurer une notification rapide des incidents.
– Automatiser la récupération des applications et des services en mettant en place des mécanismes de redondance pour réduire au minimum le temps d'intervention, par

Exemple : redémarrage des services interrompus, gestion de la charge CPU (Cenral Process Unit) pour éviter les surcharges, mise en place de sauvegardes miroir pour prévenir la perte de données, etc.

1.1.2. Le principe de supervision

La supervision réseau peut être mise en œuvre sur la base d'analyse de logs, de Résultats de commandes et de scripts locaux mais c'est surtout sur la base de protocoles Standards comme le protocole SNMP pour que le monitoring des réseaux informatiques Fonctionne. De nombreux logiciels existent pour ce fait La communauté du libre (Open Source) est particulièrement active dans le monitoring. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

– Surveillance du réseau
– Visualisation des composantes du système
– Analyser les problèmes
– Déclencher des alertes en cas de problèmes
– Effectuer des actions en fonction des alertes

Le travail de l'administrateur est alors simplifié. Les outils de supervision lui donnent un schéma généralisé du système d'information pour surveiller ses différentes fonctionnalités en temps réel.

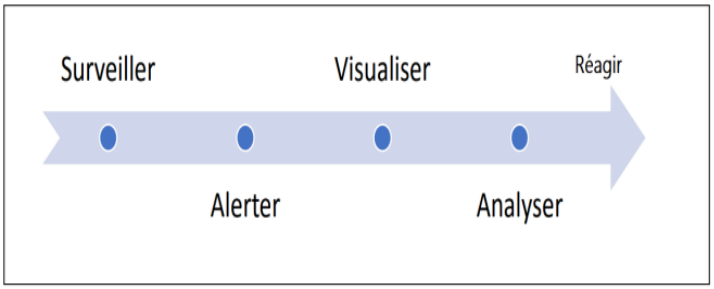


Figure 23 : Principe de supervision

1.1.3. Méthode de supervision

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes :

A. Supervision active

La supervision active est la plus classique. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision.

Cette m´méthode est composée de trois étapes

- Le serveur envoie une requête vers la ressource supervisée.
- La ressource répond à la requête du serveur.
- Le serveur analyse l'information et détermine un état pour la ressource.

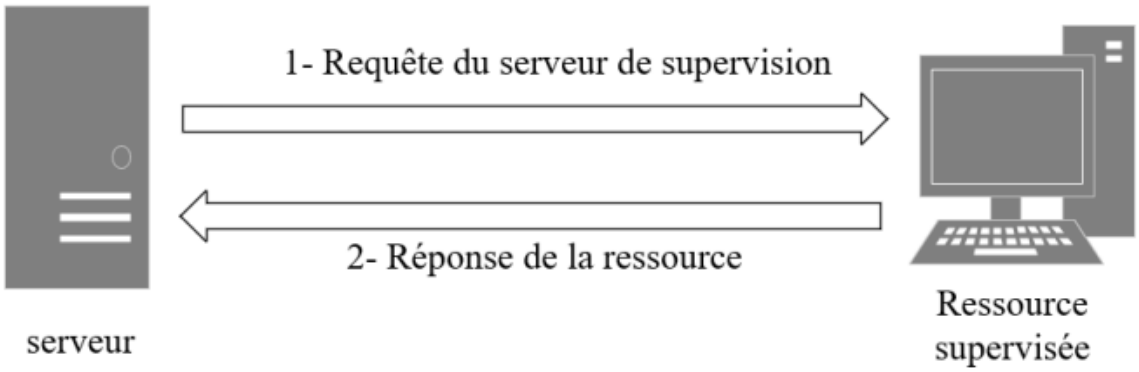


Figure 24 : Echange de messages dans une supervision active.

Le protocole le plus utilisé par les outils de supervision, SNMP utilise la méthode active.

B. Supervision passive

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

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

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

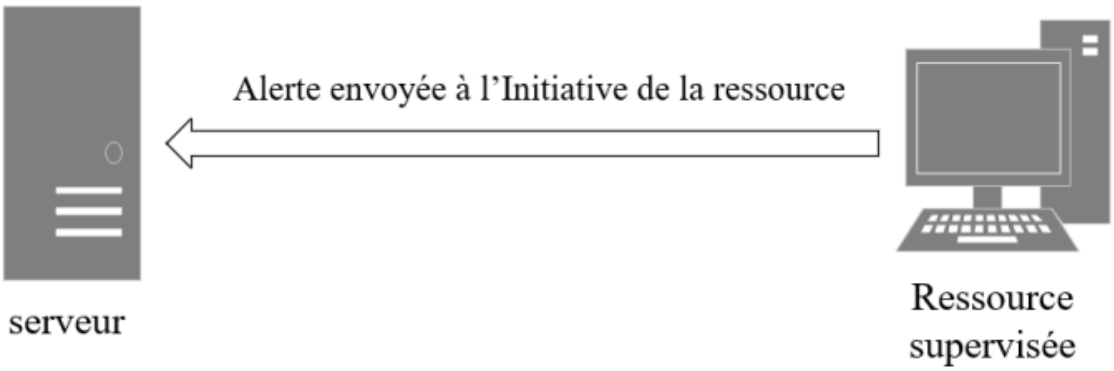


Figure 25 : Echange de messages dans une supervision passive

Le protocole standardisé et privilégié pour la supervision passive est aussi SNMP avec le mécanisme de trappes.

1.2. La métrologie

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

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

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

Les termes supervision et métrologie sont encore parfois distingues même si les frontières tendent à se dissiper : la supervision s'attache aux alertes alors que la métrologie se rapporte davantage aux mesures (11).

1.3. Monitoring un outil indispensable en entreprise

La sécurisation des systèmes informatiques en entreprise est une priorité fondamentale. Par conséquent, la surveillance des systèmes d'information et des infrastructures informatiques revêt une importance cruciale pour garantir la disponibilité continue des services.

La surveillance en temps réel, via des protocoles et des formats de données tels que SNMP, ainsi que l'utilisation d'outils de monitoring réseau et de solutions de supervision, permet de détecter rapidement les pertes de capacité du système d'information de l'entreprise. Les responsables ou les opérateurs réseau reçoivent alors des alertes (souvent par e-mail ou SMS) en cas de surcharges, leur permettant d'intervenir directement via l'interface du système monitor.

En tant qu'outil de visualisation complet, le monitoring permet la détection des anomalies sur l'ensemble du système informatique, interne de l'entreprise, les serveurs, les disponibilités réseaux, les imprimantes, les applications, ainsi que tous les autres éléments actifs en contact avec le réseau (routeurs, switches, hubs, etc.). Une telle solution de supervision et de monitoring permet ainsi à l'administrateur de bien monitorer chaque point du réseau et à distance lorsqu'il n'est pas sur place.

2. Le protocole SNMP

2.1. Définition de SNMP

SNMP qui signifie « Simple Network Management Protocol », qui veut dire protocole simple de gestion de réseau en français. Est un protocole de couche applicative. Il offre aux administrateurs réseau la possibilité de gérer les équipements du réseau, de surveiller et de diagnostiquer les problèmes, ainsi que de superviser les systèmes d'exploitation, entre autres. L'environnement de gestion SNMP se compose de plusieurs éléments, tels que la station de supervision et les éléments actifs du réseau.

2.1.1. Le fonctionnement de SNMP

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager.

SNMP utilise le protocole UDP. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents (12).

2.1.2. Les requêtes SNMP

Il existe quatre types de requêtes :

- Get-Request : Permet la rechercher d'une variable sur un agent.
- Get-Next-Request : Sert à obtenir la valeur de la variable suivante.
- Set-Request : permet de changer la valeur d'une variable sur un agent.
- Get-Bulk : Permet la recherche d'un ensemble de variables regroupées.

2.1.3. Les réponses de SNMP

- Get-Response : L'information a bien été transmise.
- NoSuchObject : Aucune variable n'a été trouvée.
- NoAccess : Les droits d'accès ne sont pas attribués.
- NoWritable : La variable ne peut être écrite.

À la suite de requêtes, l'agent répond toujours par GetResponse. Toutefois si la variable demandée n'est pas disponible, le GetResponse sera accompagné d'une erreur noSuchObject.

2.1.4. Les alertes

- **Trap : L'agent SNMP envoie une alerte au Manager.**

Les alertes (Traps, Notifications) Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap.

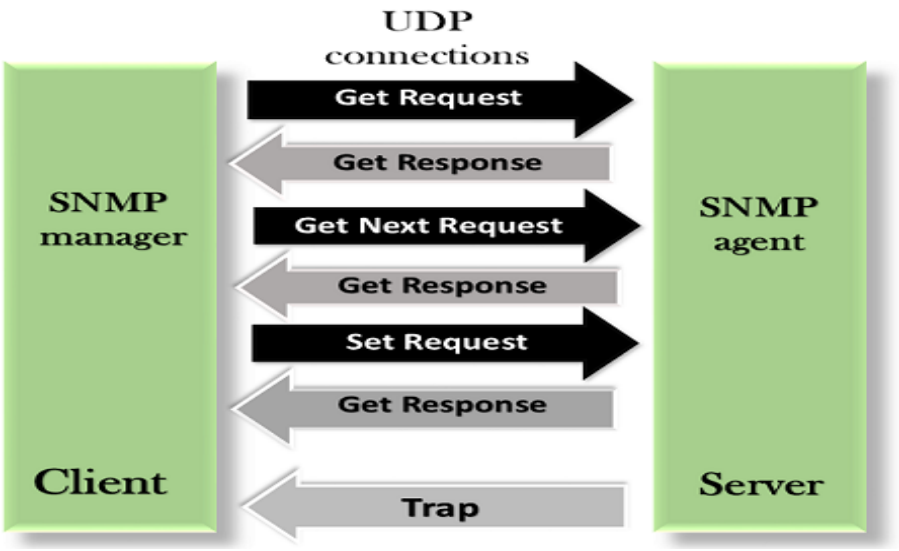


Figure 26 : Les types de message SNMP.

2.2. Les différentes versions de SNMP

Ce protocole d'administration, très répandu dans les réseaux locaux, est basé sur l'échange de messages entre les périphériques administrables et une station d'administration.

Il existe actuellement 3 versions différentes du protocole SNMP :

– **SNMP V1 :** première version standard mais La sécurité de cette version est minimale car elle basée uniquement sur la chaîne de caractère appelée "communauté".
– **SNMP V2c :** avec une amélioration de la sécurité mais jamais unifiée.
– **SNMP V3 :** permet de disposer des avantages de la version 2 sans en présenter les inconvénients. Elle définit un nouveau modèle de sécurité USM (User-base Security Model) évitant le décryptage des messages de commande qui transitent sur le réseau et autorise des droits différents en fonction des utilisateurs.

2.3. L'architecture de SNMP

Le système de gestion SNMP se compose de divers éléments, notamment la station de supervision (Manager), les équipements actifs du réseau, les variables MIB et les agents SNMP.

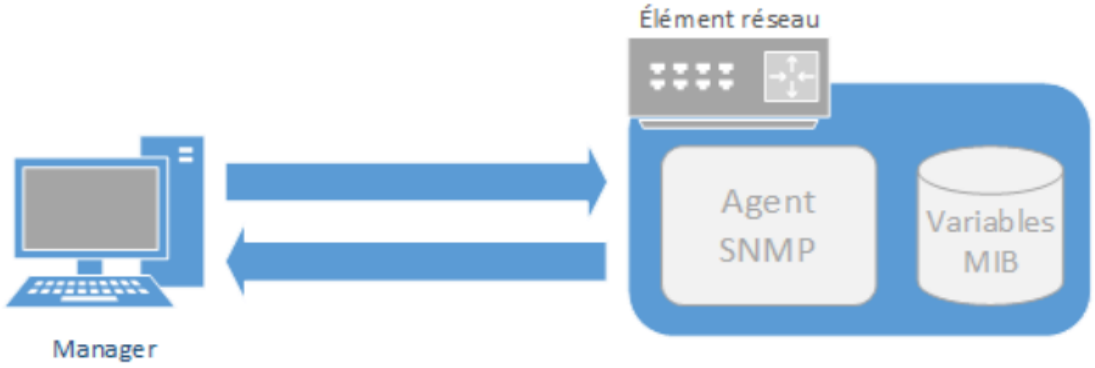


Figure 27 : Architecture SNMP (12)

Les différentes composantes du protocole SNMP sont les suivantes :

– **Les agents SNMP :** ce sont les équipements (réseau ou serveur) qu'il faut superviser.

– **Elément du réseau :** Ce sont les équipements (Ex : Routeur, Switch, Poste de travail, Imprimante, …) que l'on cherche à gérer. Chaque élément réseau est composé d'un Agent SNMP et d'un

– **Manager :** Il exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail. Le manager va aller récupérer les Informations auprès des agents et les centraliser variable MIB.

– **La MIB** : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur.

SNMP fonctionne au niveau 7 du modèle OSI mais s'appuie directement sur le protocole UDP il a donc besoin d'un numéro de port pour communiquer. Du fait qu'il utilise UDP, SNMP fonctionne en mode non connecté sans contrôle des données transmises.

2.3.1. Le manager

Rappelons que le Manager se trouvera sur une machine d'administration (un poste de travail en général). Il reste un client avant tout, étant donné que c'est lui qui envoie les différentes requêtes aux agents. Il devra disposer d'une fonction serveur, car il doit également rester à l'écoute des alertes que les différents équipements sont susceptibles d'émettre à tout moment. Le Manager dispose d'un serveur qui reste à l'écoute sur le port UDP 162 ainsi que d'éventuels signaux d'alarme appelés des "traps". Le Manager peut tout autant être installé sur une machine.

2.3.2. L'agent SNMP

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent Permet de recueillir la base de données d'informations et la rend disponible aux interrogations. Les principales fonctions d'un agent SNMP :

- Collecter des informations de gestion sur son environnement local.
- Récupérer des informations de gestion telle que déni dans la MIB propriétaire.
- Signaler un évènement au gestionnaire.

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'alerter le manager en cas de problème, s'il a été configuré.

2.3.3. MIB

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

Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actifs du réseau.

Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle SMI (Structure of Management Information), basée sur ASN.1 (Abstract Syntaxe Notation 1) qui décrit les variables, les tables et les larmes gérer au sein d'une MIB.

La MIB est une structure arborescente dont chaque nœud est défini par un nombre ou OID (Object Identifier). Cette OID est très utile car il permet d'accéder à une information grâce à la suite de tous les index

Voici un exemple de la structure de table MIB :

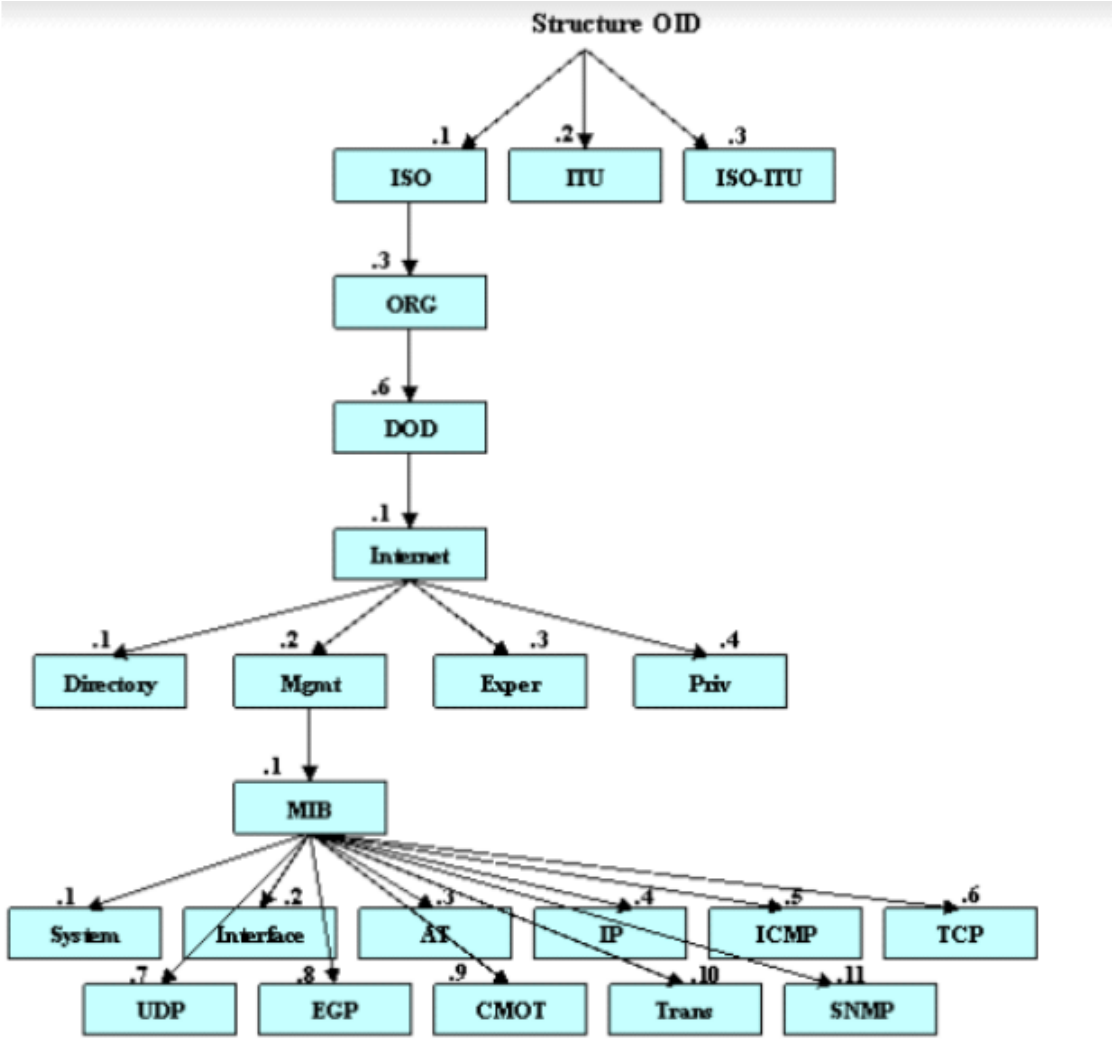


Figure 28 : Exemple de structure d'un MIB.

En fin, Pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne L'emplacement de la variable à consulter dans la MIB.

3. Open source

L'open source est une approche d'ingénierie logicielle qui consiste à développer des logiciels ou des composants logiciels et à rendre le code source résultant librement accessible, qui peut ensuite être exploité par les développeurs et les entreprises souhaitant l'adapter à leurs besoins métiers ou affiner son intégration. Avec leurs systèmes d'information.

3.1. Outils de monitoring open source existants

Les outils monitoring du réseau sont utilisés pour surveiller et alerter sur les problèmes de réseau susceptibles de provoquer des pannes ou des coupures. Ces outils mesurent l'état

de différents éléments du réseau, tels que les commutateurs ou les routeurs, ainsi que la manière dont ils interagissent. Ils peuvent également suivre les VPN et les interfaces réseau. La plupart de ces outils permettent aux utilisateurs de visualiser les informations liées au réseau concerné sous forme de graphiques et de tableaux, ce qui facilite l'identification des problèmes potentiels et la résolution de ceux existants pour éviter les coupures et les pannes de réseau.

Il existe de différents outils de supervision utilisés dans les entreprises. Nous allons Voir les différents outils qui existent

3.1.1. Zabbix

Zabbix a été créé par Alexei Vladishev, et est actuellement activement développé et maintenu par ZABBIX SIA. Zabbix est une solution de supervision professionnelle libre de droit. Zabbix est un logiciel qui permet de superviser de nombreux paramètres d'un réseau ainsi que la santé et l'intégrité des serveurs, des machines virtuelles, des applications, des services, des bases de données, des sites web, du cloud et plus encore. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer une alerte e-mail pour possiblement tout événement. Ceci permet une réponse rapide aux problèmes serveurs (13).

3.1.1.1. Fonctionnalités de Zabbix

Zabbix offre à l'administrateur réseau plusieurs possibilités pour lui faciliter la tâche et garantir le bon fonctionnement du réseau :

- Découverte automatique des serveurs et périphériques réseaux.
- Configuration facile (ajout des équipements à superviser, sélection des déclencheurs
- D'alarmes, etc.).
- Notification d'alerte par e-mail, sms etc.
- Agent local hautes performances (sur les systèmes Linux, Windows, Solaris etc.).
- Vue globale des équipements à superviser.
- Authentification d'agent sécurisée.
- Supervision sans agent.
- Interface web flexible.

3.1.1.2. Architectures de Zabbix

Zabbix se compose de plusieurs composants logiciels majeurs. Leurs responsabilités sont décrites ci-dessous :

– **Serveur :** Le serveur Zabbix est le composant central auquel les agents envoient leur disponibilité, les informations d'intégrité et les statistiques. Le serveur est le 43 Mémoire de Master 2 : Sécurité et supervision de réseaux référentiel central dans lequel toutes les données de configuration, statistiques et données opérationnelles sont stockées.

– **Stockage de base de données :** Toutes les informations de configuration ainsi que les données recueillies par Zabbix sont stockées dans une base de données.

– **L'interface Web :** pour permettre un accès facile à Zabbix de n'importe où et de n'importe quelle plate-forme. L'interface fait partie du serveur Zabbix et fonctionne généralement (mais pas nécessairement) sur la même machine physique que celle qui exécute le serveur.

– **Procuration :** Le Proxy Zabbix peut collecter des données de performance et de disponibilité au nom du serveur Zabbix. Un proxy est un composant facultatif du déploiement de Zabbix. Cependant, il peut être très bénéfique de distribuer la charge d'un seul serveur Zabbix.

– **Agent :** Les Agents Zabbix sont déployés sur des cibles de surveillance pour superviser activement les ressources locales et les applications, et envoyer les données collectées au serveur Zabbix.

Ce qui suit est la représentation du principe de fonctionnement de Zabbix (son architecture) :

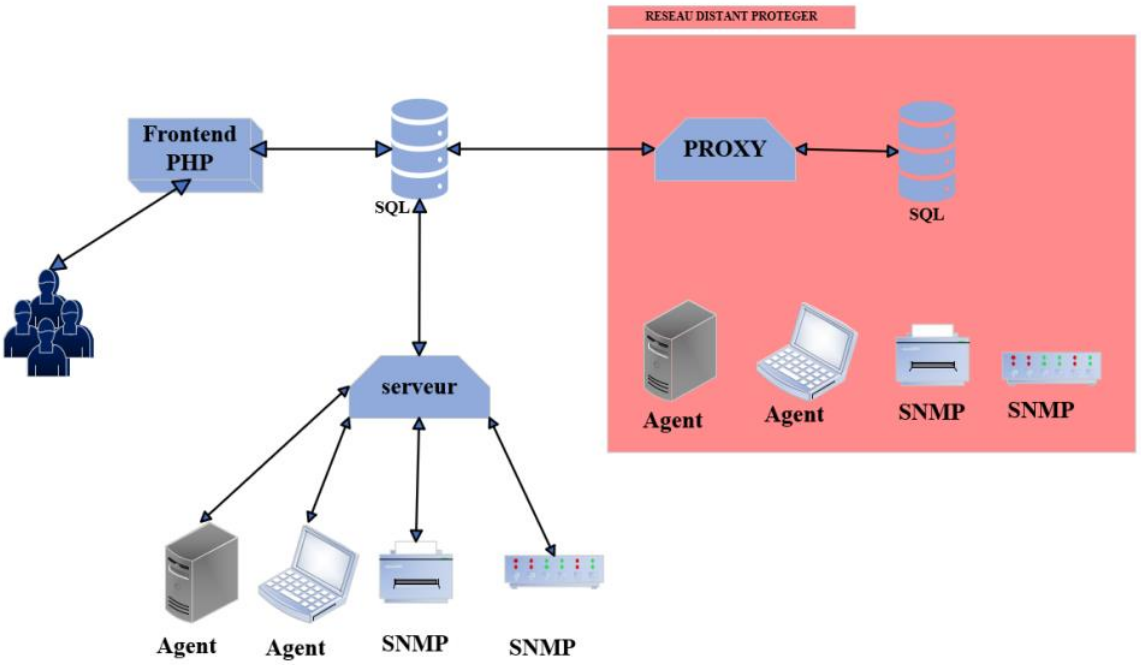


Figure 29 : Architecture globale de zabbix.

3.1.1.3. Avantages et inconvénients de Zabbix

Avantages

Voici quelques avantages de l'outil de supervision Zabbix :

– Solution Open Source.
– Réalisation de graphiques, cartes ou screens.
– Facilité d'installation.
– Affichage clair des erreurs sur le Dashboard.
– Serveur Proxy Zabbix. Surveillances des sites web : temps de réponse, vitesse de transfert.
– Mise à jour de la configuration via l'interface Web de Zabbix.

Inconvénients :

Parmi les inconvénients de Zabbix on distingue :

– Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire.
– L'agent Zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple).

- Limité au ping sans le client.
- Problème de configuration sur le switch.

3.1.2. Nagios

Nagios (Net Saint) a été le premier outil de monitoring IT open source à se positionner en 1999 par Ethan Galstad. Derrière le logiciel, une véritable communauté s'est créée avec plus d'un million d'utilisateurs à travers le monde. Nagios est un logiciel ordonnanceur qui surveille les systèmes, les réseaux et l'infrastructure. Il offre des services de surveillance et d'alerte pour les serveurs, les commutateurs, les applications et les services. Il alerte les utilisateurs en cas d'incidents et les avertit une deuxième fois lorsque le problème a été résolu. Nagios a été conçu à l'origine pour fonctionner sous Linux, mais il fonctionne aussi bien sur d'autres variantes d'Unix (10). Il permet :

- La surveillance des équipements et systèmes cibles, à travers notamment des protocoles.
- La surveillance des réseaux, systèmes d'exploitation et tous types de matériel (comme les sondes de température, les alarmes, etc.) via des scripts communément appelé plugins de supervision.
- L'alerte en cas de de dépassement de seuil ou panne via un système de notification qui prévient l'exploitant du SI ou l'administrateur.

3.1.2.1. Avantages et inconvénients de Nagios

Avantages

Les principaux avantages de Nagios sont :

- Très puissant et modulaire
- Surveillance des ressources des équipements (serveur, routeur, etc.) comme la charge du processeur, des informations sur l'utilisation des disques durs, les processus en cours.
- Disponible en open source.
- Surveillance des services réseaux (SMTP, POP, HTTP, PING, etc.
- Surveillance des données environnementales comme par exemple la température.

Inconvénients :

Parmi ses inconvénients nous citons :

- Difficile à installer et à configurer
- Dispose d'une interface compliquée

- Ne permet pas d'ajouter des hosts via Web
- Besoin d'un autre outil comme CACTI pour faciliter sa configuration
- Pas de représentations graphiques.

3.1.3. Centreon

Créé en 2003 par des français souhaitant améliorer Nagios, il a été repris par une nouvelle entreprise nommée Merethis il se présente comme une évolution de celui-ci pour tout d'abord son interface mais aussi ses fonctionnalités. Il s'appuie également sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision (14).

Centreon possède sa propre version de chaque fichier de configuration de Nagios. Lorsque l'utilisateur modifie un paramètre par l'interface Centreon, ce changement est d'abord répercuté sur les fichiers « de copies » de Centreon pour que les modifications soient prises en compte par Nagios.

3.1.3.1. Avantages et inconvénients de Centreon

Avantages

On en cite quelques avantages :

- Facilite la configuration de Nagios.
- Une découverte automatique du réseau via NMAP.
- Graphe le résultat des alertes, système de reporting.

Inconvénients :

Et quelques inconvénients :

- Risque de problèmes de compatibilité ou de complexité accrue (Personnalisation excessive).
- Exige plus d'efforts pour les mises à jour et la sécurité (Maintenance).
- Configuration peut être difficile pour les débutants (Complexité initiale).
- Limité par rapport aux solutions propriétaires (Support technique).

3.1.4. Cacti

Cacti est une application open source de gestion graphique de réseau et de surveillance basée sur le langage de programmation PHP. Elle est conçue pour permettre aux administrateurs système de surveiller et de visualiser les performances réseau en utilisant des graphiques générés à partir de données recueillies à intervalles réguliers.

Il utilise le protocole SNMP pour collecter des données à partir de périphériques réseau tels que des routeurs, commutateurs et serveurs, puis les stocke dans une base de données MySQL. Les utilisateurs peuvent ensuite créer des graphiques personnalisés pour analyser et surveiller les tendances de performance du réseau.

3.1.4.1. Avantages et inconvénients de cacti

Avantages

Ses avantages sont :

- Facilité d'installation.
- Facilité de configuration.
- Affichage clair des graphs sur plusieurs périodes.
- Peut-être amélioré grâce à des plugins.
- Gestion des utilisateurs

Inconvénients :

Il a aussi des limites :

- Limité de base.
- Peut mettre un certain temps à générer les graphs.
- Pas de gestion d'alertes.

4. Choix de l'outil

Comme nous voulons un logiciel plus adapté à notre travail, nous avons donc choisi les logiciels de supervision car ils nous permettent de vérifier la disponibilité des services et des ressources, réagir aux alertes en notifiant l'administrateur ou en redémarrant des services, synthétiser l'état du système d'information sur une page web. Ces logiciels permettent aussi de créer des graphiques avec les données obtenues. Disons tout ce dont on a besoin pour la bonne supervision d'un réseau.

Sur les quatre logiciels, on n'a décidé de ne pas choisir nagios à cause des difficultés à installer et à configurer et il dispose d'une interface compliquée. Centreon est un bon logiciel de supervision mais il est Limité par rapport aux solutions propriétaires. Aussi Cacti est la perte de sa flexibilité et de ses capacités de sa personnalisation poussée pour la surveillance des performances réseau, Donc notre choix s'est porté sur zabbix qui est un bon logiciel de supervision réseau.

En effet, zabbix est une solution de surveillance open source puissante qui offre de nombreux avantages pour la gestion des infrastructures informatiques.il propose une surveillance en temps réel via des protocoles standards et des agents personnalisés, une interface utilisateur intuitive, des alertes personnalisables, des rapports détailles et des visualisations dynamiques. De plus il bénéficie d'une communauté active et d'un support professionnel optionnelle pour une assistance continue et des mises à jour régulière.

Conclusion

Dans ce chapitre, nous avons exploré les principes fondamentaux de la supervision et du monitoring. Nous avons décrit trois outils utilisés dans le domaine de la supervision des réseaux informatiques, à savoir : Zabbix, Nagios, Centreon, Cacti.

Le chapitre suivant, nous mettrons en place une architecture de réseau informatique, en intégrant zabbix pour assurer une supervision efficace et une gestion optimale des ressources.

Chapitre IV

La mise en place d'un serveur supervision Zabbix

Introduction

Dans ce chapitre, nous procédons à la mise en place initiale de la solution développée dans le cadre de notre projet, mettant l'accent sur l'installation des logiciels et outils nécessaires à notre infrastructure. Nous aborderons également en détail notre exploration de la supervision à l'aide de l'outil Zabbix.

1. Environnement du travail

1.1. Installation de GNS3 sous Windows

GNS3 (Graphical Network Simulator) est un simulateur de réseau gratuit, open source, multiplateforme qui permet d'émuler des réseaux complexes. Il utilise des logiciels tels que VMware ou Virtual Box pour émuler différents systèmes d'exploitation dans un environnement virtuel.

La figure ci-dessous représente le logo de GNS3.

Figure 30: Logo GNS3

Afin d'installer GNS3, il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les instructions d'installation jusqu'à leur terme. Enfin, il suffit de cliquer sur le bouton "Finish" pour finaliser le processus.

La capture d'écran ci-dessous illustre l'interface de GNS3.

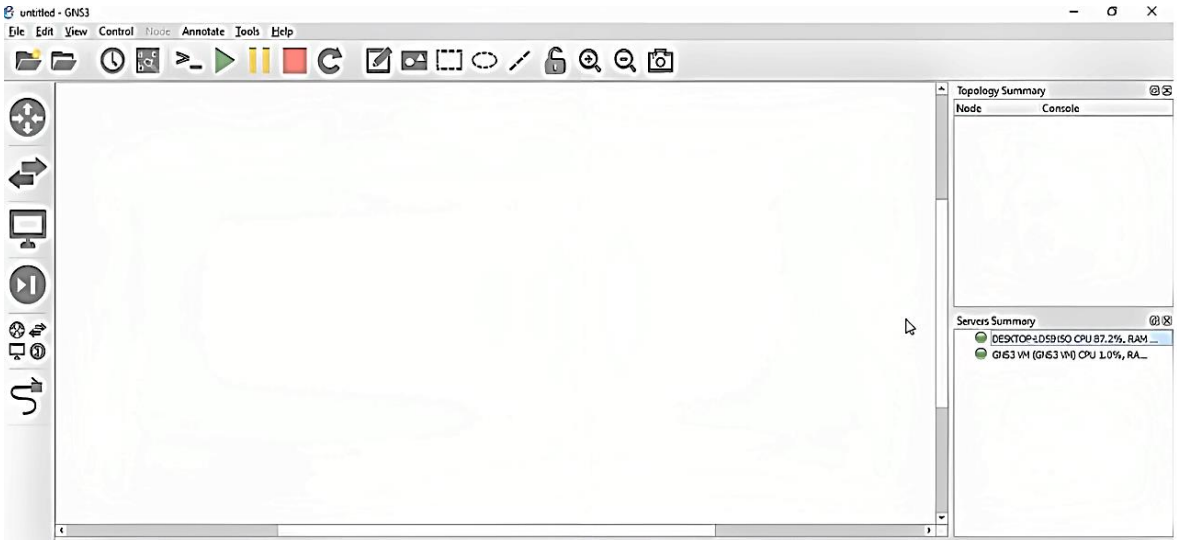


Figure 31 : Interface d'accueil de GNS3

1.2. Installation de VMware Workstation version 17 pro

VMware Workstation Pro est l'hyperviseur de bureau standard de l'industrie pour l'exécution de machines virtuelles sur des PC Linux ou Windows, il peut être utilisé pour mettre la mise en place d'un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique.

Figure 32: Logo VMware

Afin d'installer VMware Workstation 17 pro, il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les étapes de la figure ci-dessous :

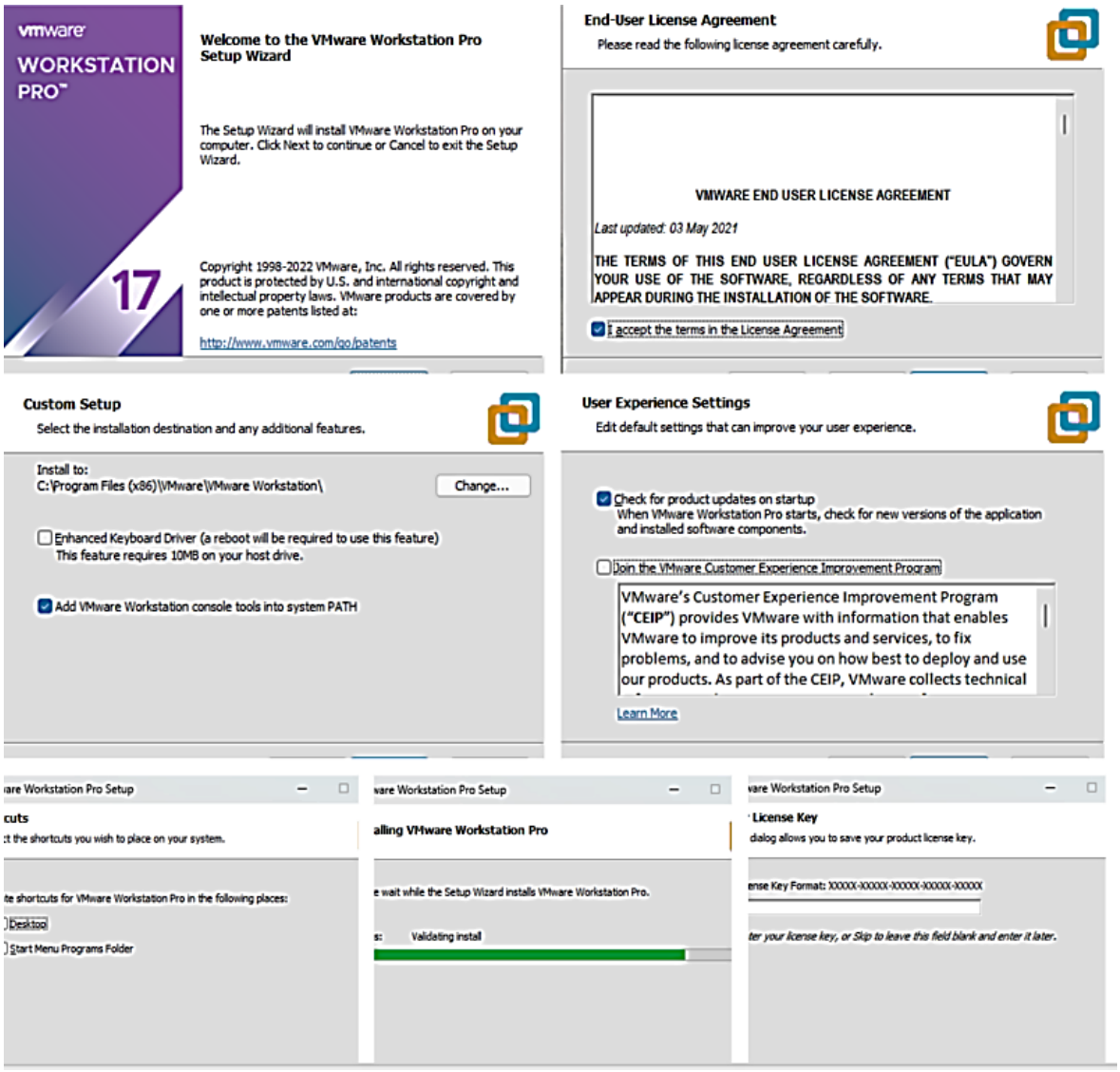


Figure 33 : Installation de VMware Workstation

Après avoir installé VMware, vous serez accueilli par une page d'accueil. Cette page d'accueil peut fournir diverses options et fonctionnalités pour vous permettre de gérer vos machines virtuelles

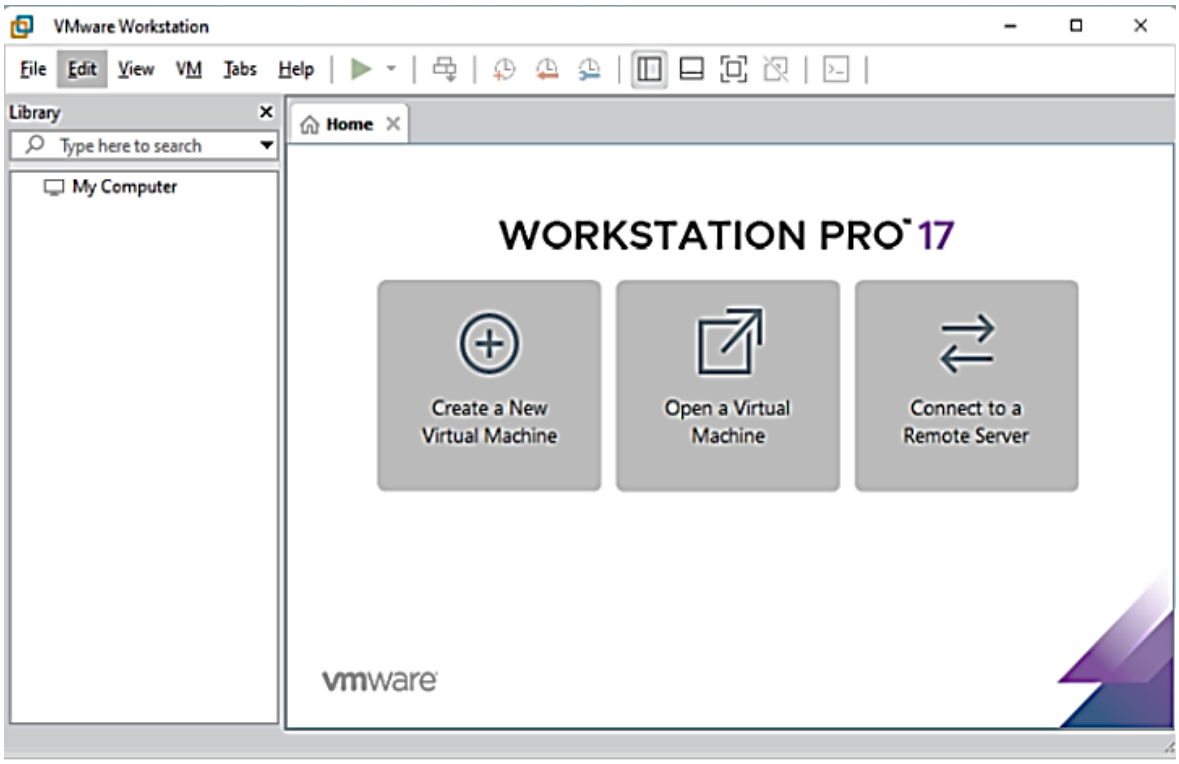


Figure 34 : Page d'accueil de VMware Workstation

1.3. Installation des serveurs

- **Installation du Windows server 2022**

Dans cette partie nous allons voir les différentes étapes d'installations du Windows Server 2022, voir la figure ci-dessous.

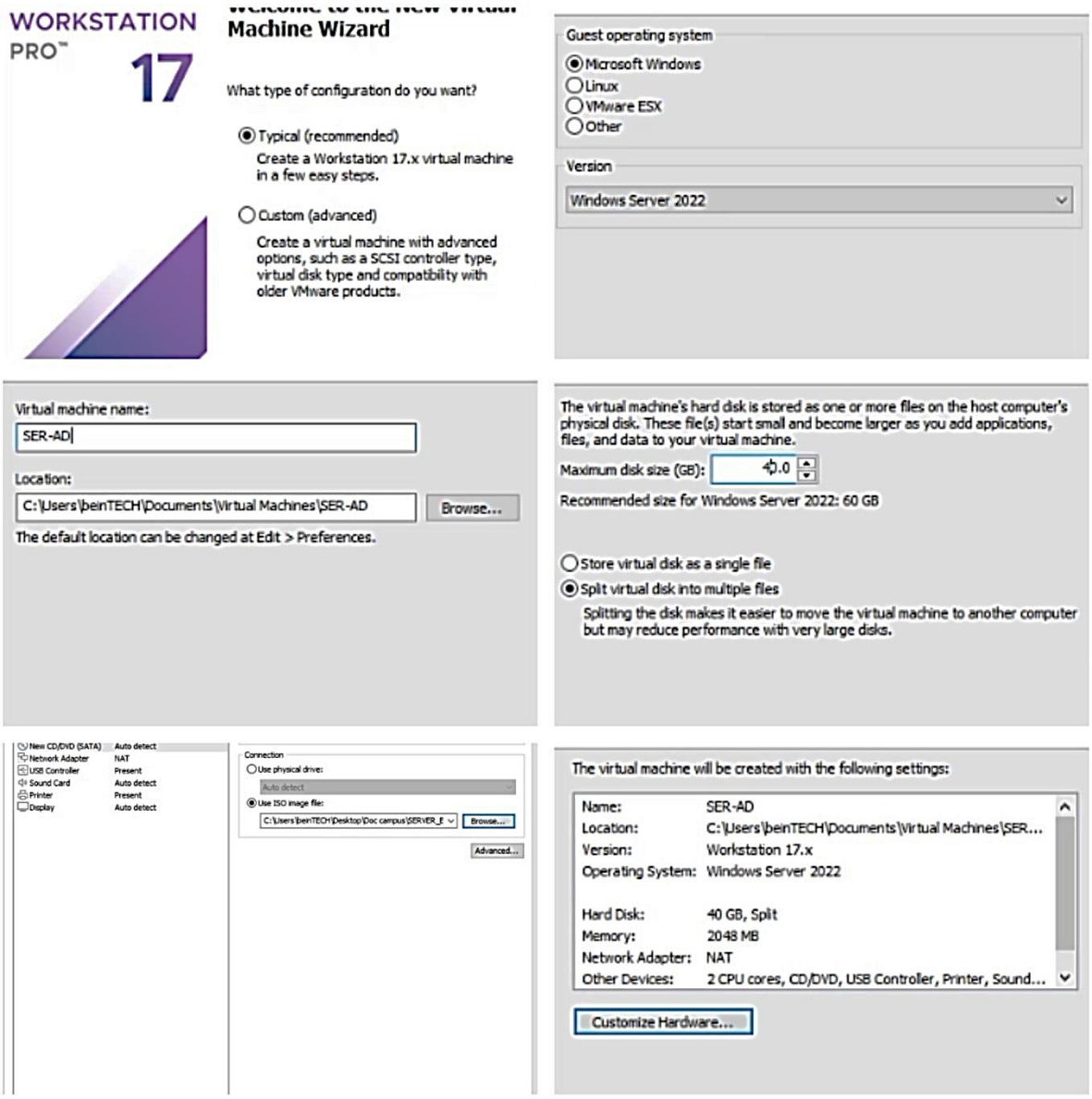


Figure 35 : Les étapes installation Windows server 2022

- **Installation du Linux server " Debian 11.X 64 bit"**

Dans cette partie nous allons voir les différentes étapes d'installations du Linux server " Debian 11.X64bit ».

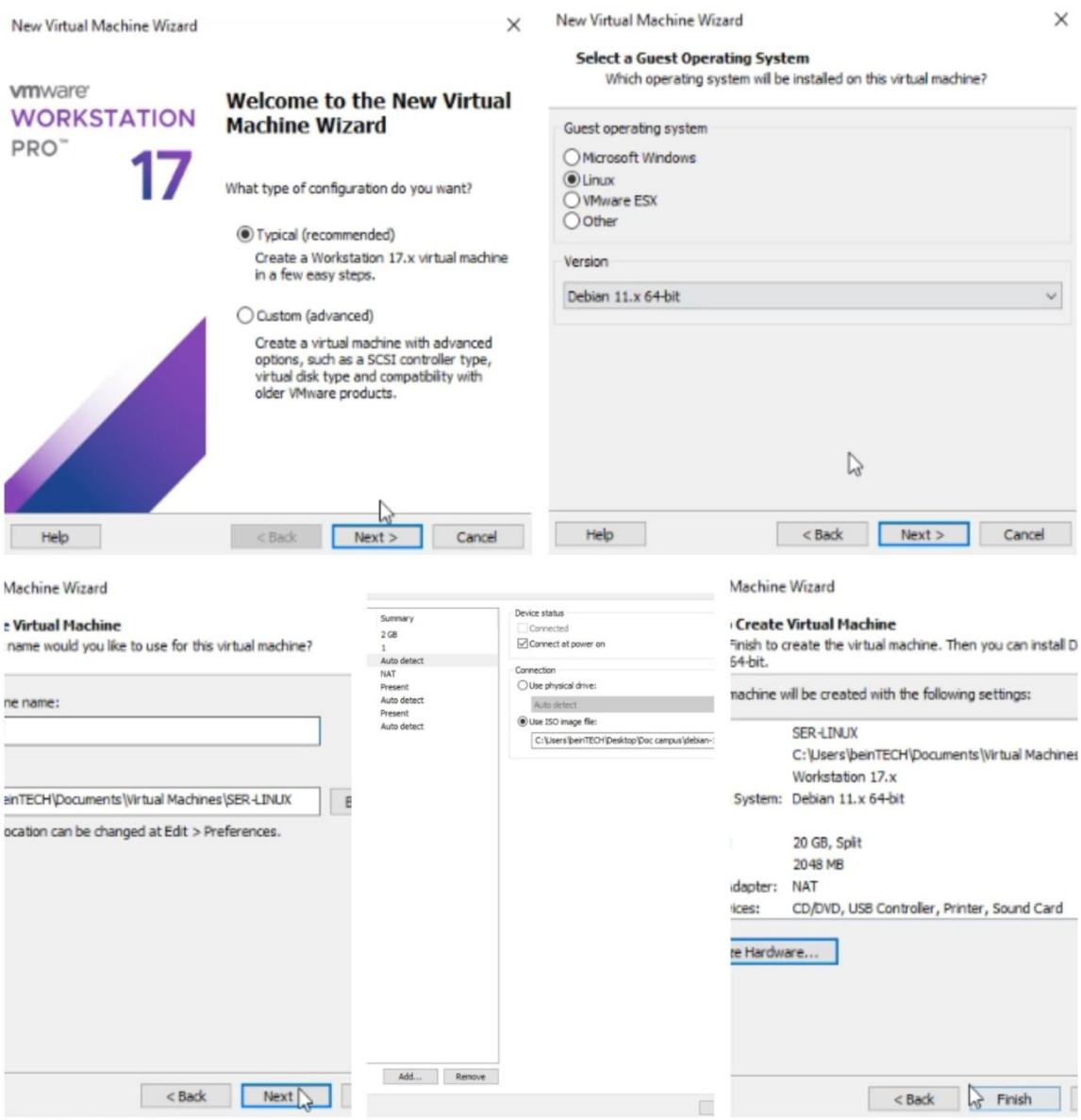


Figure 36 : Les étapes d'installation Linux server " Debian 11.X 64 bit"

2. Architecture proposée

A fin de permettre une meilleur supervision du réseau de l'entreprise, nous avons proposé une architecture basée sur le serveur Zabbix et qui permet de surveiller les équipements à savoir : le routeur, le switch, le pfsense….

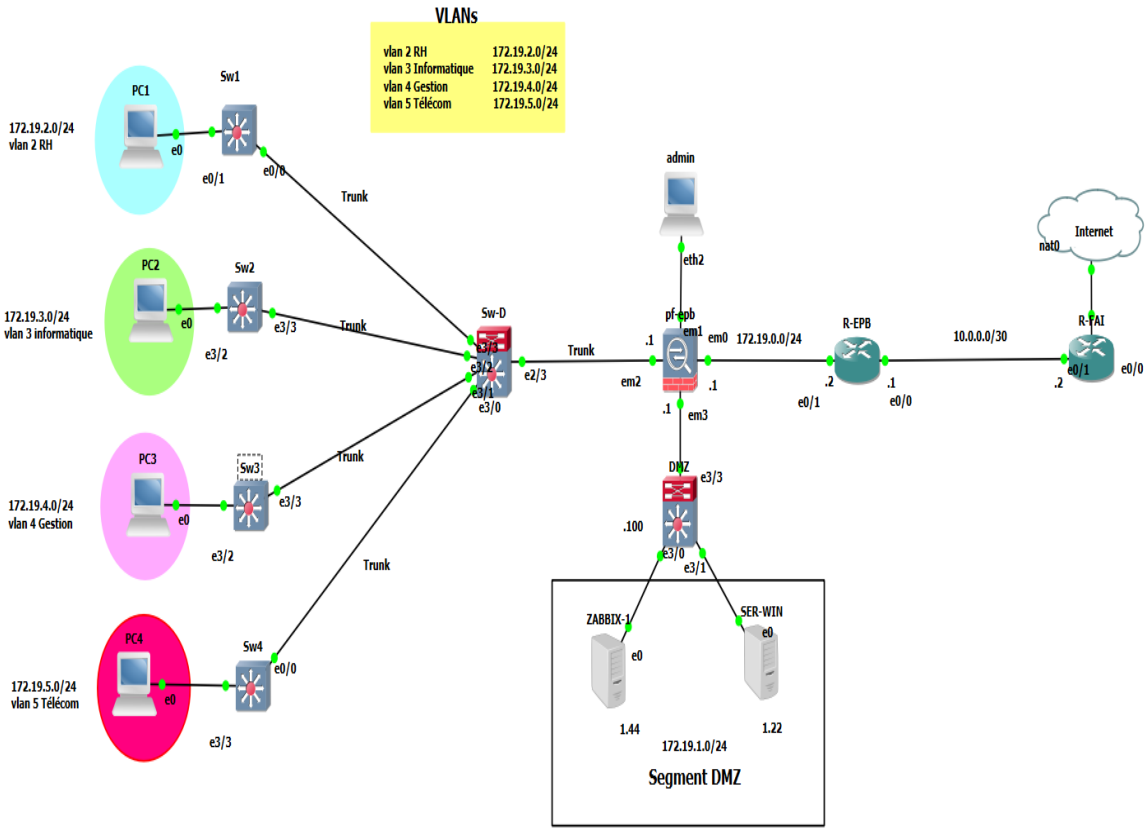


Figure 37 : Architecture proposée

3. Configuration des équipements

Dans cette partie, nous allons présenter la configuration en générale des équipements qui vont nous permettre de mettre en place la nouvelle architecture proposée

3.1. Le plan d'adressage des VLANs

Nom de Vlans	Id vlan	Adresse sous réseau	Passerelle de sous réseau
RH	2	172.19.2.0	172.19.2.1
Informatique	3	172.19.3.0	172.19.3.1
Gestion	4	172.19.4.0	172.19.4.1
Télécom	5	172.19.5.0	172.19.5.1

Tableau 1 : Plan d'adressage des VLANS

3.2. Le plan d'adressage des équipements

Le tableau ci-dessous représente le plan d'adressage des équipements.

Équipements	Interfaces	Adressage
R-FAI	e0/0 e0/1	Connexion internet obtenue par DHCP 10.0.0.2
R-EPB	e0/0 e0/1	10.0.0.1 172.19.0.2
Pf-epb	Port 0 Port 1 Port 2 Port 3	172.19.0.1 192.168.1.1 Trunk 172.19.1.1
Sw-DMZ	Vlan 1	172.19.1.100
SW1	Vlan 2	172.19.2.0
SW2	Vlan 3	172.19.3.0
SW3	Vlan 4	172.19.4.0
SW4	Vlan 5	172.19.5.0

Tableau 2 : Plan d'adressage des équipements

4. Méthodologie de configuration de GNS3

Le schéma de la figure ci-dessous montre les étapes suivies pour la configuration de la topologie.

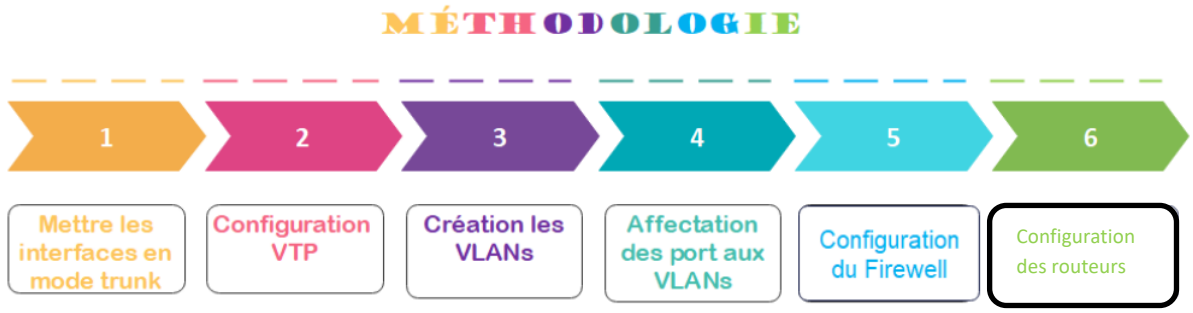


Figure 38 : Les étapes de la méthodologie de GNS3

4.1. Mettre les interfaces en mode Trunk

Mettre le switch distribution en mode Trunk :

Premièrement, nous avons affiché les voisins du switch distribution.

```
Sw1#show  cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Sw4              Eth 3/0           141             R S I  Linux Uni Eth 0/0
Sw1              Eth 3/1           145             R S I  Linux Uni Eth 3/3
Sw2              Eth 3/2           133             R S I  Linux Uni Eth 3/3
Sw3              Eth 3/3           140             R S I  Linux Uni Eth 0/0

Total cdp entries displayed : 4
```

Figure 39 : Afficher les voisins du switch distribution

Deuxièmement, nous avons mis le switch distribution en mode trunk.

```
Sw1(config)#in
Sw1(config)#interface  r
Sw1(config)#interface  range eth
Sw1(config)#interface  range ethernet 3/0-3
Sw1(config-if-range)#sw
Sw1(config-if-range)#switchport t
Sw1(config-if-range)#switchport trunk en
Sw1(config-if-range)#switchport trunk encapsulation do
Sw1(config-if-range)#switchport trunk encapsulation dot1q
Sw1(config-if-range)#sw
Sw1(config-if-range)#switchport mo
Sw1(config-if-range)#switchport mode tr
Sw1(config-if-range)#switchport mode trunk
Sw1(config-if-range)#end
Sw1#
Sw1#
Sw1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
```

Figure 40 : Mettre le switch distribution en mode Trunk

Mettre les switches d'accès en mode Trunk :

La figure ci-dessous montre les étapes nécessaires pour mettre le switch d'accès 1 en mode Trunk. Nous allons effectuer les mêmes étapes avec les trois autres switches d'accès.

```
Sw1#show  cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Sw4              Eth 3/0           141             R S I  Linux Uni Eth 0/0
Sw1              Eth 3/1           145             R S I  Linux Uni Eth 3/3
Sw2              Eth 3/2           133             R S I  Linux Uni Eth 3/3
Sw3              Eth 3/3           140             R S I  Linux Uni Eth 0/0

Total cdp entries displayed : 4
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#in
Sw1(config)#interface  r
Sw1(config)#interface  range eth
Sw1(config)#interface  range ethernet 3/0-3
Sw1(config-if-range)#sw
Sw1(config-if-range)#switchport t
Sw1(config-if-range)#switchport trunk en
Sw1(config-if-range)#switchport trunk encapsulation do
Sw1(config-if-range)#switchport trunk encapsulation dot1q
Sw1(config-if-range)#sw
Sw1(config-if-range)#switchport mo
Sw1(config-if-range)#switchport mode tr
Sw1(config-if-range)#switchport mode trunk
Sw1(config-if-range)#end
Sw1#
Sw1#
Sw1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
```

Figure 41 : Mettre le switch d'accès 1 en mode Trunk

Afin de vérifier cette configuration, on affiche l'état des interfaces avec la commande : "show interfaces trunk" ou bien la commande "show interfaces status"

```
Sw1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    1            auto   auto unknown
Et0/2                        connected    1            auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    4            auto   auto unknown
Et3/3                        connected    trunk        auto   auto unknown
Sw1#
```

Figure 42 : afficher l'état des interfaces

4.2. Configuration VTP

Afin de profiter des services VTP, nous avons configuré le switch distribution en mode serveur et le reste des switches d'accès en mode client. Cela a permis la propagation des VLANs du switch-D vers les autres switches d'accès.

- **Configuration VTP du switch distribution**

En configurant le switch distribution en tant que serveur VTP, les VLANs pourront être propagés vers les switches d'accès. Nous avons utilisé la commande "vtp pruning" sur le switch distribution pour activer la fonction de pruning VTP.

Cela nous a permis de restreindre la propagation des informations de VLAN uniquement aux liens trunks nécessaires, réduisant ainsi le trafic inutile sur le réseau. L'activation du pruning VTP sur le switch distribution a contribué à optimiser l'utilisation de la bande passante en éliminant les VLANs non nécessaires sur les trunks et à améliorer les performances du Réseau.

```
Sw1(config)#vtp mode  server
Device mode already VTP Server for VLANS.
Sw1(config)#vtp dom
Sw1(config)#vtp domain epb.vtp
Changing VTP domain name from NULL to epb.vtp
Sw1(config)#vtp pass
Sw1(config)#vtp password cisco
Setting device VTP password to cisco
Sw1(config)#vtp mo
Sw1(config)#vtp pru
Sw1(config)#vtp pruning
Pruning switched on
Sw1(config)#vtp ver
Sw1(config)#vtp version 2
Sw1(config)#end
```

Figure 43 : Configuration VTP du switch Distribution

- **Configuration VTP des switches d'accès**

En configurant les switches d'accès en tant que clients VTP, ils pourront recevoir les mises à jour des VLANs provenant du switch distribution.

```
Sw1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
Sw1(config)#vtp domain epb.vtp
Changing VTP domain name from NULL to epb.vtp
Sw1(config)#vtp password cisco
Setting device VTP password to cisco
Sw1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Sw1(config)#end
Sw1#wr
```

Figure 44 : Configuration VTP de switch d'accès 1

Afin de vérifier la configuration et le fonctionnement du protocole VTP , nous allons utiliser la commande : "show vtp status"

```
Sw1#show vtp st
Sw1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : epb.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 5-22-24 12:49:39
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0xA9 0xFC 0x52 0x66 0x38 0xD8 0x27 0x1D
                                  0xFA 0x50 0x06 0x08 0x3F 0x02 0x1A 0xB3
Sw1#
```

Figure 45 : vérifier la configuration et le fonctionnement du protocole VTP

4.3. Création des VLANs

Pour créer les VLANs sur le switch distribution en utilisant la commande "vlan" dans le mode de configuration, puis leur donner des noms à l'aide de la commande "name" dans le même mode comme suit :

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vlan 2
Sw1(config-vlan)#name RH
Sw1(config-vlan)#vlan 3
Sw1(config-vlan)#name informatique
Sw1(config-vlan)#vlan 4
Sw1(config-vlan)#name gestion
Sw1(config-vlan)#vlan 5
Sw1(config-vlan)#name telecom
Sw1(config-vlan)#end
```

Figure 46 : Création des VLANs

Pour vérifier la création des VLANs sur le switch distribution, nous allons utiliser la commande "show vlan brief"

```
Sw1#show  vl
Sw1#show  vlan br
Sw1#show  vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
2    RH                               active
3    informatique                     active
4    gestion                          active
5    telecom                          active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
Sw1#
```

Figure 47 : vérifier la création des VLANs

4.4. Affectation des ports aux VLANs

Dans cette étape, nous allons assigner des ports aux VLANs au niveau des switches d'accès avec les commandes montrées dans la figure ci-dessous :

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#in
Sw1(config)#interface  eth
Sw1(config)#interface  ethernet 3/2
Sw1(config-if)#sw
Sw1(config-if)#switchport mo
Sw1(config-if)#switchport mode  acc
Sw1(config-if)#switchport mode  access
Sw1(config-if)#
Sw1(config-if)#sw
Sw1(config-if)#switchport  acc
Sw1(config-if)#switchport  access vl
Sw1(config-if)#switchport  access vlan  4
Sw1(config-if)#end
```

Figure 48 : Affectation des ports aux VLANs

4.5. Configuration du Firewell

- **Installation de PfSense**

En commençant par l'installation de pfsense sur GNS3 comme la figure ci-dessous montre :

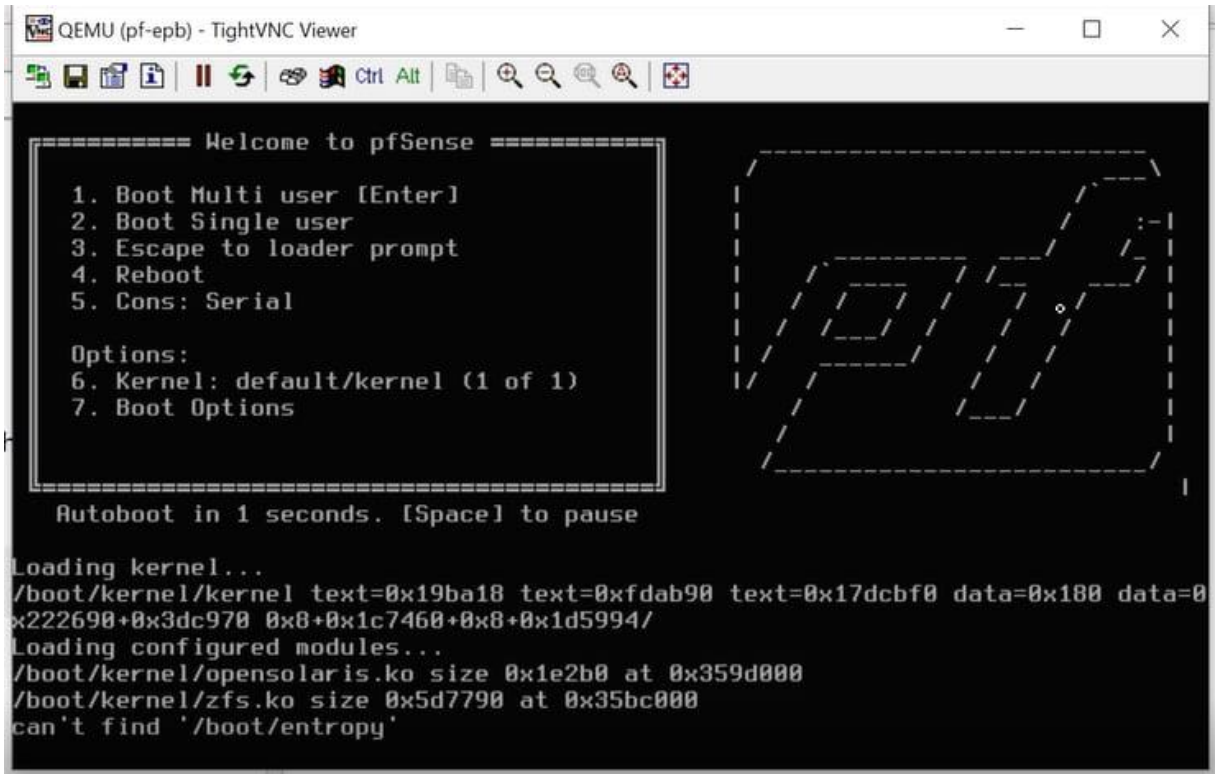


Figure 49 : Ecran de démarrage de l'installation de Pfsense.

On laisse le système démarrer de lui-même et après quelques secondes, on arrive à l'écran suivant :

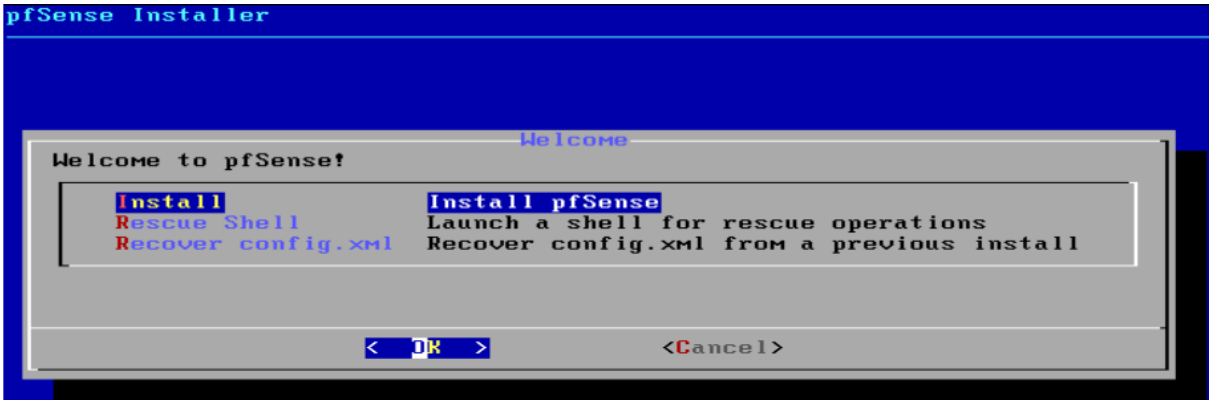


Figure 50 : Début de l'installation de Pfsense.

On accepte le type d'installation puis en validant par la touche « Entrée ». Après quelque étape préliminaire, on procède maintenant au redémarrage du système pour que ça prenne en compte toutes nos manipulations

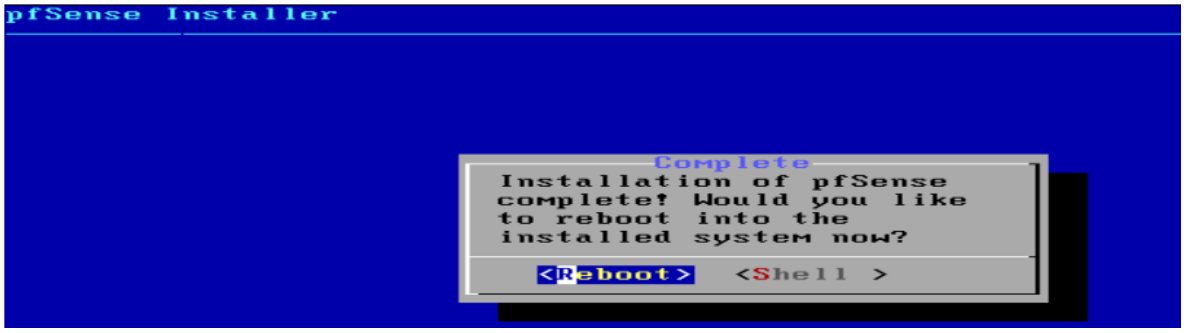


Figure 51 : Fin de l'installation de Pfsense

- **Configuration des interfaces :**

PfSense demande d'affecter chaque interface (ici em0, em1, em2, em3) à une interface WAN ou bien à un LAN ou la DMZ. Une fois les affectations son faite, PfSense détecte automatiquement les cartes réseaux disponibles, puis on attribue pour chaque interface une adresse IP qui sont attribué par nous-mêmes par le choix de l'option 2, sauf l'interface WAN qui reçoit une adresse IP par DHCP

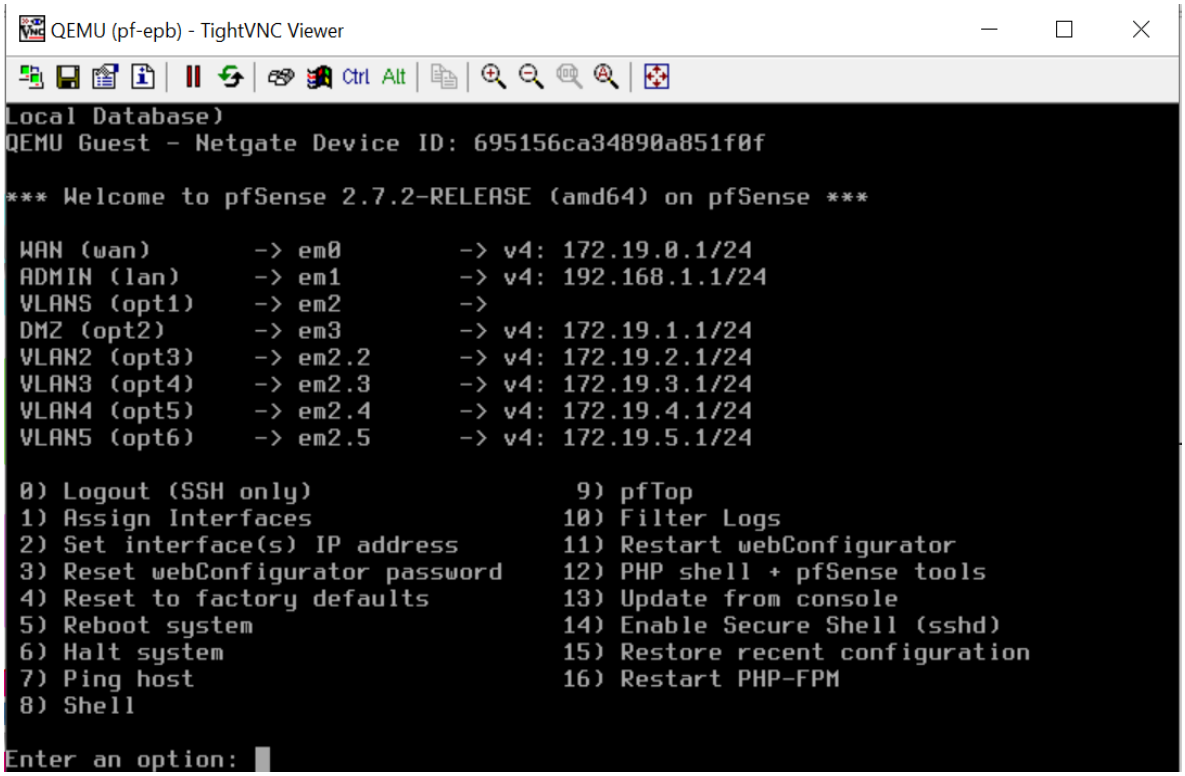


Figure 52: Configuration des interfaces

➢ **Configuration de Pfsense**

Nous accédons à l'interface web en entrant l'adresse IP du LAN : http: //192.168.1.1/ dans un navigateur. C'est à partir de cette adresse que toutes les manipulations vont se dérouler.

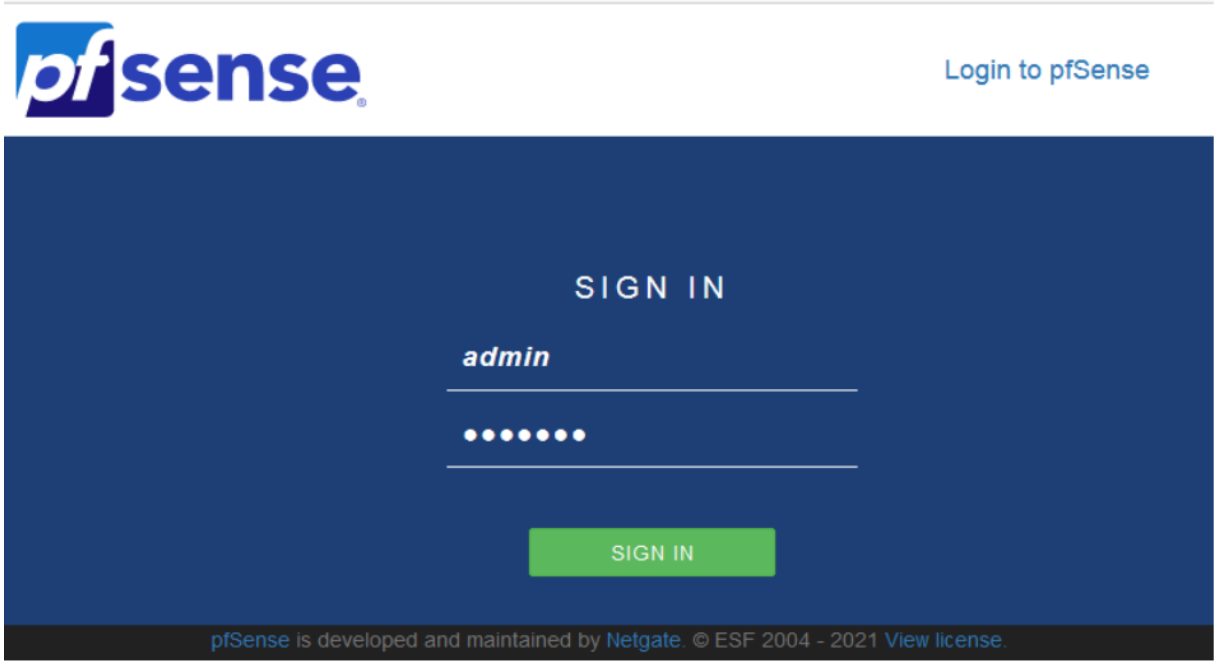


Figure 53 : Page d'identification de PfSense

Le couple <User Name/Password> par défaut est <admin/ PfSense>.

Une fois connecté avec succès, il est possible d'accéder à l'interface web d'accueil de pfSense après la configuration.

Les différents onglets de Pfsense :

Nous avons des onglets qui fournissent plusieurs services :

– **System :** Permet de faire l'ensemble des réglages concernant le système en lui-même.
– **Interfaces :** Permet la gestion des interfaces réseau (Lan et Wan).
– Firewall : Permet de mettre en place toute les règles servant de Firewall.
– **Services :** Permet d'activer de nombreux service faisant de PfSense un firewall multifonction pouvant se transformer en serveur/relai DHCP ou bien encore en portail captif.
– **VPN** : Permet d'activer/désactiver le VPN, de mettre en place une sécurité via IP Sec.
– **Status :** Permet de voir le statut de l'ensemble des configurations.
– **Diagnostics :** Permet de donner des outils permettant le diagnostic d'un quelconque bug

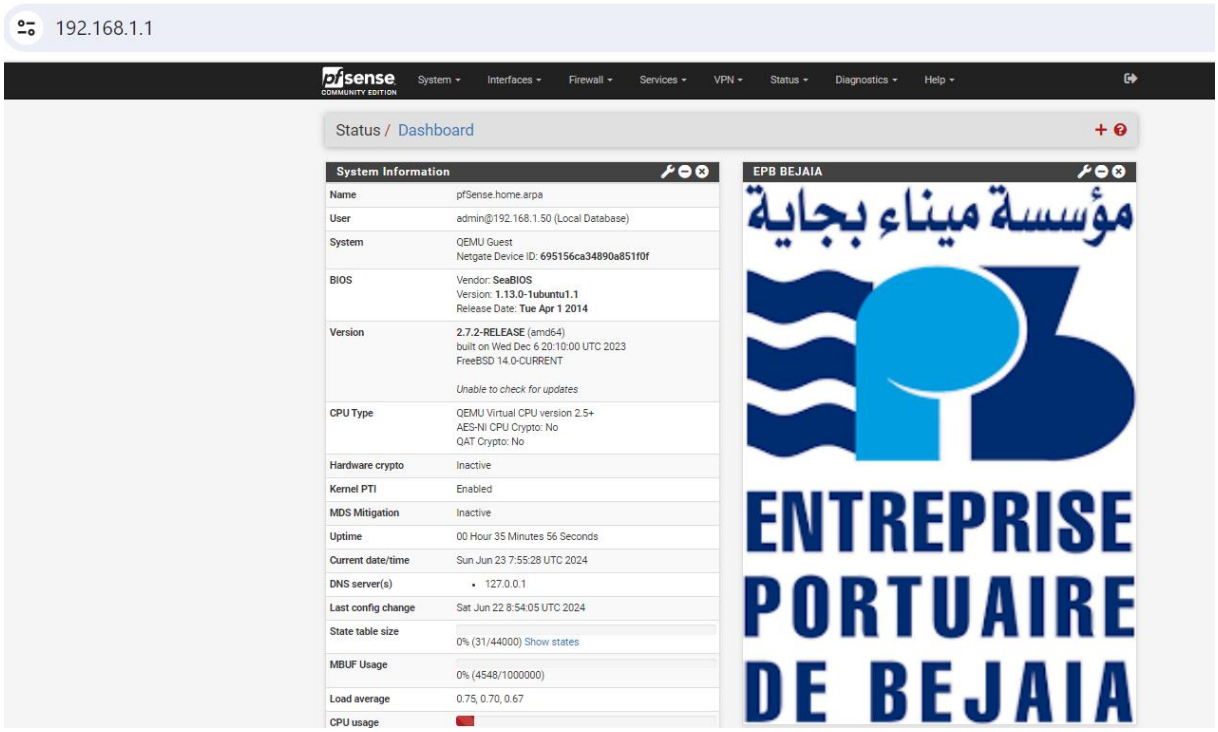


Figure 54: La page d'accueil de Pfsense

Configuration des Règles du pare-feu

Après s'être connecté à l'interface web de configuration de pfSense, on passe à la configuration des règles du pare-feu pour les 3 réseaux (LAN, WAN et DMZ). Pour cela on va dans l'onglet "Firewall" Rules comme ceci :

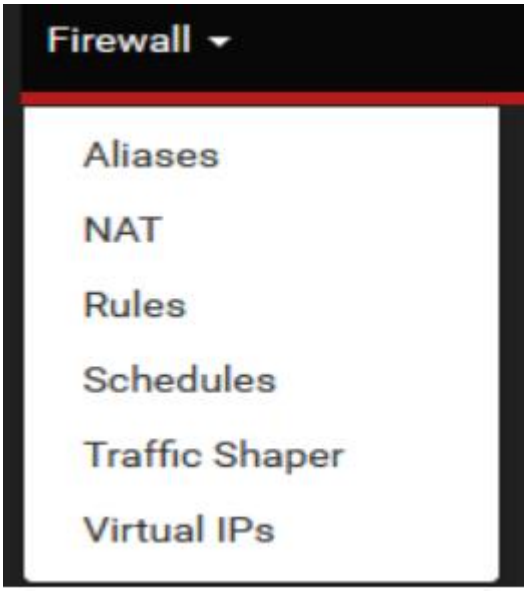


Figure 55: Onglet Firewall.

- **Pour la configuration des interfaces**

Pour configurer une interface WAN sur pfSense, commencez par accéder à l'interface Web., allez dans le menu Interfaces et sélectionnez Assignments. Dans cette section, vous pouvez attribuer une interface WAN en sélectionnant l'interface physique appropriée (comme em0 ou re0) dans le menu déroulant et en cliquant sur Add.

Après avoir ajouté l'interface, cliquez sur le nom de l'interface WAN pour accéder à ses paramètres de configuration. Donnez une description à l'interface, par exemple WAN Interface, pour une identification facile. Ensuite, activez l'interface en cochant la case Enable Interface. Pour configurer l'adresse IP, choisissez le type de connexion approprié : DHCP pour obtenir une adresse IP automatiquement du fournisseur d'accès, ou Static IPv4 si vous avez une adresse IP statique. Si vous sélectionnez Static IPv4, entrez l'adresse IP, le masque de sous-réseau et la passerelle.

Une fois ces paramètres configurés, cliquez sur Save pour sauvegarder les modifications. Enfin, cliquez sur Apply Changes pour appliquer les nouvelles configurations.

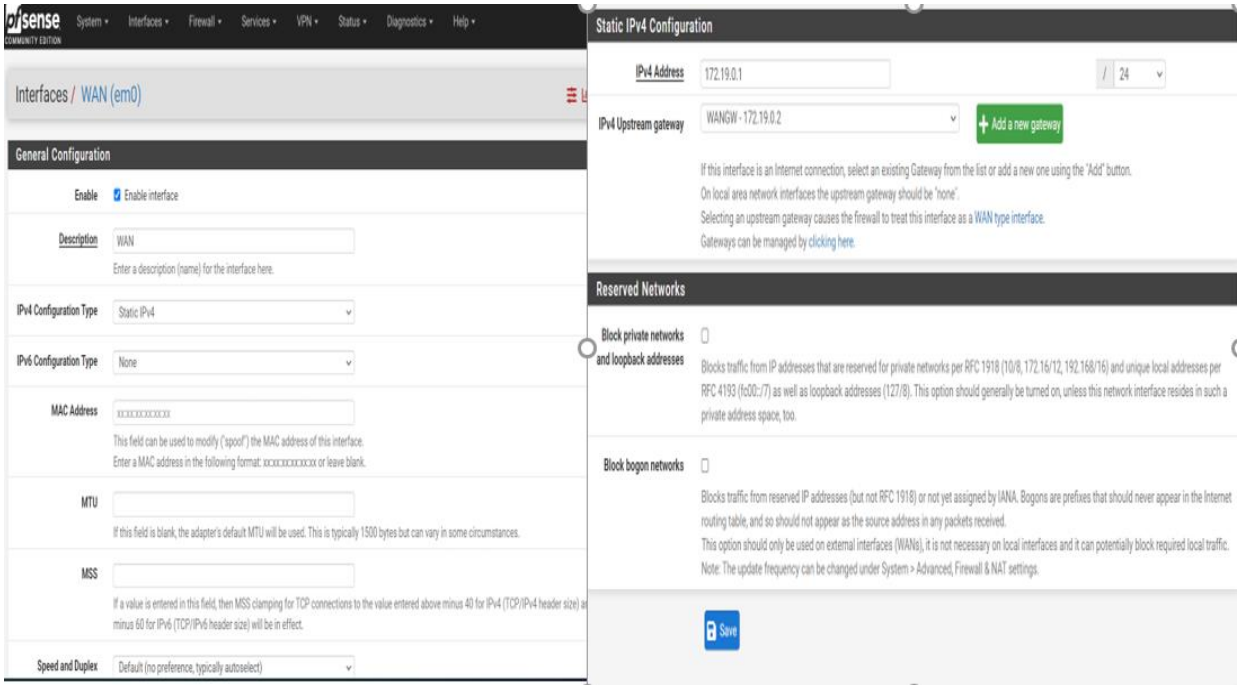


Figure 56 : Configuration de interface WAN

Vérifiez ensuite le statut de l'interface sous Status > Interfaces pour s'assurer qu'elle est correctement configurée et connectée.

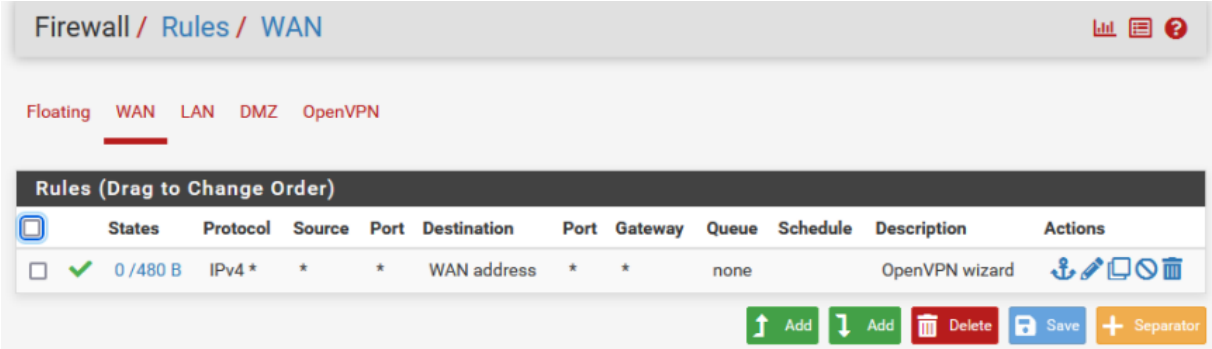


Figure 57 : Le status de l'interface WAN

Après avoir ajouté les interfaces Admin, DMZ, VLAN1, VLAN2, etc., en suivant les mêmes étapes que pour l'interface WAN, voici leur statut, comme illustré sur la figure ci-dessous ;

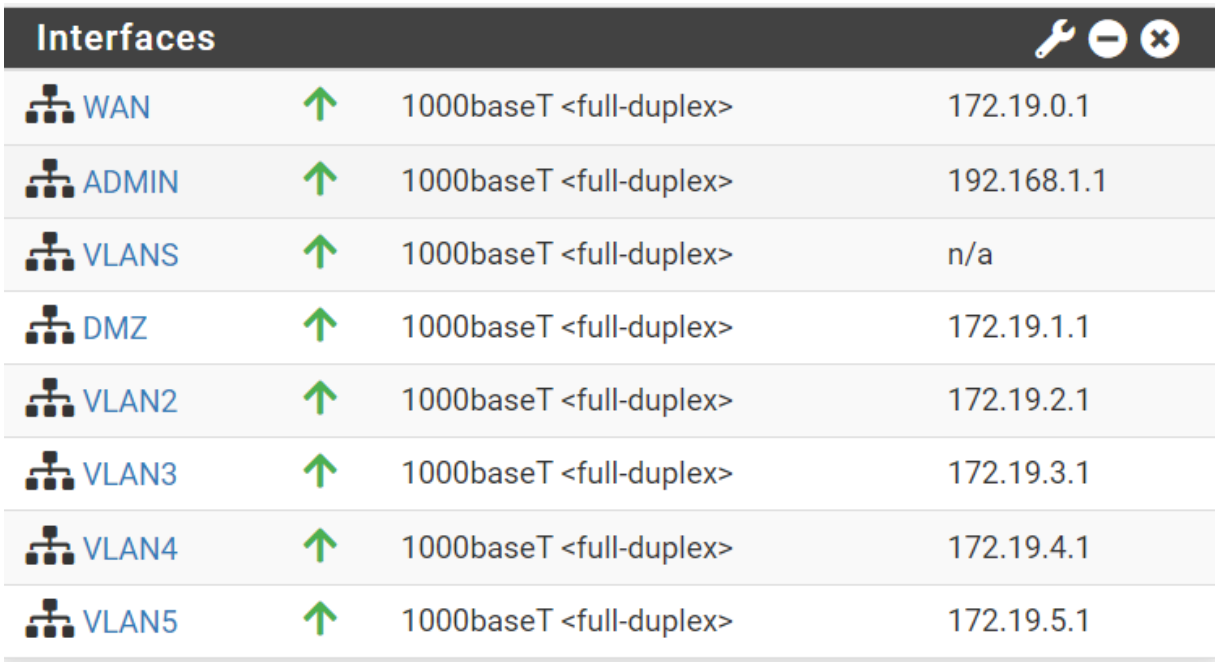


Figure 58 : La configuration des interfaces sur pfesens

4.6. Configuration des routeurs

- **Configuration du routeur R-EPB**

Premièrement, nous allons configurer les interfaces Ethernet 0/0 et 0/1

```
R1(config)#interface  ethernet 0/0
R1(config-if)#ip add
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#no shutdown
*May 22 13:26:08.570: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May 22 13:26:09.574: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#
R1(config-if)#
R1(config-if)#shu
R1(config-if)#shutdown
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#end
*May 22 13:26:16.542: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
R1(config-if)#end
```

Figure 59 : Configuration du l'interface Ethernet 0/0 de R-EPB

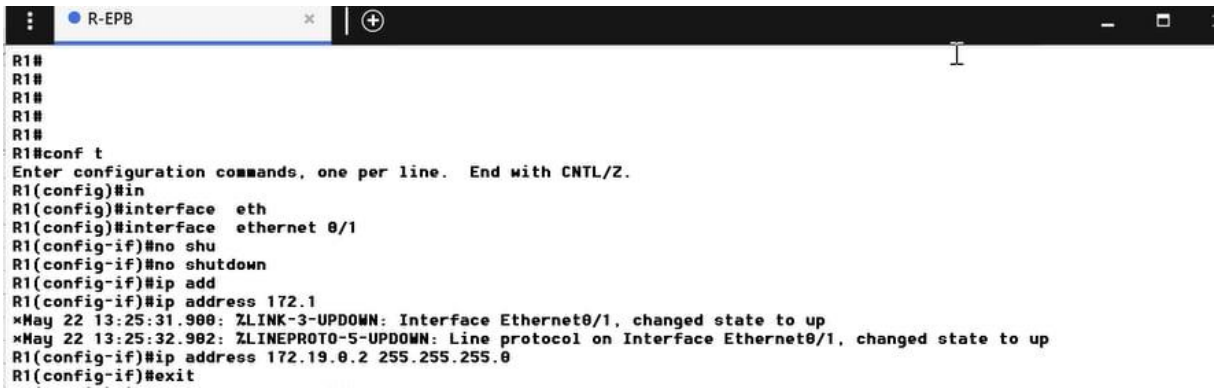


Figure 60 : Configuration du l'interface Ethernet 0/1 de R-EPB

- **Configuration du routeur R-FAI**

Premièrement, nous allons configurer les interfaces Ethernet 0/0 et 0/1.

```
R-FAI(config)#interface  ethernet 0/0
R-FAI(config-if)#ip add
R-FAI(config-if)#ip address  dhc
R-FAI(config-if)#ip address  dhcp
R-FAI(config-if)#no shu
R-FAI(config-if)#no shutdown
R-FAI(config-if)#end
```

Figure 61 : Configuration du l'interface Ethernet 0/0 de R-FAI

```
R-FAI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-FAI(config)#in
R-FAI(config)#interface  eth
R-FAI(config)#interface  ethernet 0/1
R-FAI(config-if)#no shu
R-FAI(config-if)#no shutdown
R-FAI(config-if)#ip add
R-FAI(config-if)#ip address 10.0.
*May 22 13:27:23.161: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*May 22 13:27:24.167: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
R-FAI(config-if)#ip address 10.0.0.2 255.255.255.252
```

Figure 62 : Configuration du l'interface Ethernet 0/1 de R-FAI

5. Méthodologie de La supervision "Monitoring"

Le schéma de la figure ci-dessous montre les étapes suivies pour la configuration de la supervision.

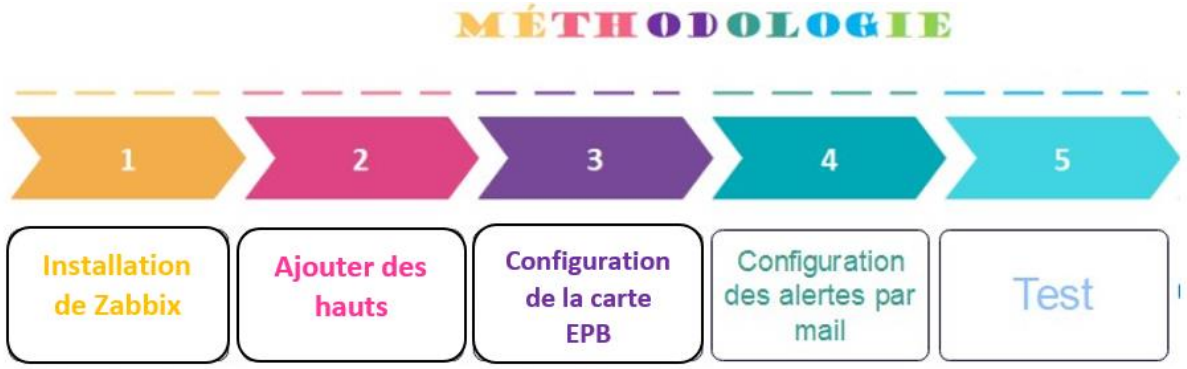


Figure 63 : Les étapes de la méthodologie de supervision

5.1. Installation de Zabbix

Étape 1 : Installation du serveur Web Apache et des paquets PHP 1.

Mettre d'abord le système d'exploitation à jour, comme illustré dans la figure ci-dessous :

```
root@zabbix:/home/zabbix# apt update && apt upgrade
```

Figure 64 : Commande de mise à jour du système d'exploitation.

Téléchargement et installation d'Apache, PHP et certains modules PHP requis, comme illustré dans la figure ci-dessous ;

```
root@zabbix:/home/zabbix# apt install apache2 apache2-bin apache2-data apache2-u
tils libapache2-mod-php libapache2-mod-php7.4 libapr1 libaprutil1 libaprutil1-db
d-sqlite3 libaprutil1-ldap libcurl4 libgd3 liblua5.3-0 libonig5 libsodium23 libx
pm4 libxslt1.1 php php-bcmath php-common php-gd php-ldap php-mbstring php-mysql
php-xml php7.4 php7.4-bcmath php7.4-cli php7.4-common php7.4-gd php7.4-json php7
.4-ldap php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml s
sl-cert
Lecture des listes de paquets... Fait
```

Figure 65 : Commande d'installation des dépendances et des packages requis.

Une fois l'installation terminée, vérifier si le service Apache2 est en cours d'exécution, comme illustré dans la figure ci-dessous :

```
root@zabbix:/home/zabbix# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-05-05 14:15:30 CEST; 14s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 33777 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 33781 (apache2)
      Tasks: 6 (limit: 2278)
     Memory: 15.6M
        CPU: 39ms
     CGroup: /system.slice/apache2.service
             ├─33781 /usr/sbin/apache2 -k start
             ├─33785 /usr/sbin/apache2 -k start
             ├─33786 /usr/sbin/apache2 -k start
             ├─33788 /usr/sbin/apache2 -k start
             ├─33789 /usr/sbin/apache2 -k start
             └─33790 /usr/sbin/apache2 -k start

mai 05 14:15:30 zabbix systemd[1]: Starting The Apache HTTP Server...
mai 05 14:15:30 zabbix apachectl[33780]: AH00558: apache2: Could not reliably determine the se
mai 05 14:15:30 zabbix systemd[1]: Started The Apache HTTP Server.
```

Figure 66 : Commande de vérification si Apache2 est en cours d'exécution

Arrêter et démarrer Apache pendant que le système est en cours d'exécution, comme illustré dans la figure ci-dessous;

```
root@zabbix:/home/zabbix# systemctl start apache2
root@zabbix:/home/zabbix# systemctl stop apache2
root@zabbix:/home/zabbix# systemctl restart apache2
```

Figure 67 : Commande d'arrêt et de démarrage d'Apache2

Étape 2 : Installation du serveur et du client Maria DB

Télécharger et installer Maria DB,cette dernière remplace MySQL dans les distributions Debian actuelles, pour stocker toutes les données Zabbix., comme illustré dans la figure ci-dessous;

```
root@zabbix:/home/zabbix# apt install mariadb-server mariadb-client
```

Figure 68 : Commande d'installation de la base de données MariaDB.

Vérifier quel service est en cours d'exécution, comme illustré dans la figure ci-dessous;

```
root@zabbix:/etc/apt# sudo service mysql status
● mariadb.service - MariaDB 10.11.6 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-06-12 19:47:50 CEST; 23min ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
   Main PID: 834 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 10 (limit: 2244)
     Memory: 126.1M
        CPU: 1.297s
     CGroup: /system.slice/mariadb.service
             └─834 /usr/sbin/mariadbd
```

Figure 69 : Commande de vérification si Maria DB est activée

Sécuriser l'installation de Maria DB. Le paquet Debian fournit un script qu'il faut exécuter, comme illustré dans la figure ci-dessous :

```
root@zabbix:/home/zabbix# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Figure 70 : Commande de sécurisation de Maria DB.

Le paquet Debian fournit un script qu'il faut exécuter. Il faut ensuite appliquer les paramètres appropriés pour chaque environnement. Ce script vous invitera à effectuer des actions, telles que la suppression d'utilisateurs anonymes, la désactivation de l'accès root du réseau et la suppression de la base de données de test. Une fois toutes les modifications appliquées et l'installation MariaDB sécurisée, il faut procéder à la création d'une base de données Zabbix, comme illustré dans la figure ci-dessous ;

```
root@zabbix:/home/zabbix# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.5.19-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost identified by 'mypassword';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> quit;
Bye
```

Figure 71 : Commande de configuration de la base de données Maria DB.

Étape 3 : Installation de Zabbix sous Debian

Télécharger les packages DEB du serveur Zabbix, comme illustré dans la figure ci-dessous ;

```
root@zabbix:/home/zabbix# wget https://repo.zabbix.com/zabbix/6.3/debian/pool/main/z/zabbix-release/zabbi
x-release_6.3-1+debian11_all.deb
--2023-05-05 14:23:31--  https://repo.zabbix.com/zabbix/6.3/debian/pool/main/z/zabbix-release/zabbix-rele
ase_6.3-1+debian11_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)… 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3672 (3,6K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.3-1+debian11_all.deb »

zabbix-release_6.3-1+debia 100%[=====================================>]   3,59K  --.-KB/s    ds 0s

2023-05-05 14:23:32 (58,6 MB/s) – « zabbix-release_6.3-1+debian11_all.deb » sauvegardé [3672/3672]
```

Figure 72 : Commandes de téléchargement des packages DEB du serveur Zabbix.

Installer les packages DEB à l'aide de la commande dpkg, comme illustré dans la figure ci-dessous ;

```
root@zabbix:/home/zabbix# dpkg -i zabbix-release_6.3-1+debian11_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 151250 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.3-1+debian11_all.deb ...
Dépaquetage de zabbix-release (1:6.3-1+debian11) ...
Paramétrage de zabbix-release (1:6.3-1+debian11) ...
```

Figure 73 : Commande d'installation des packages DEB du serveur Zabbix.

Mettre à jour les packages du serveur Zabbix, comme illustré dans la figure ci-dessous;

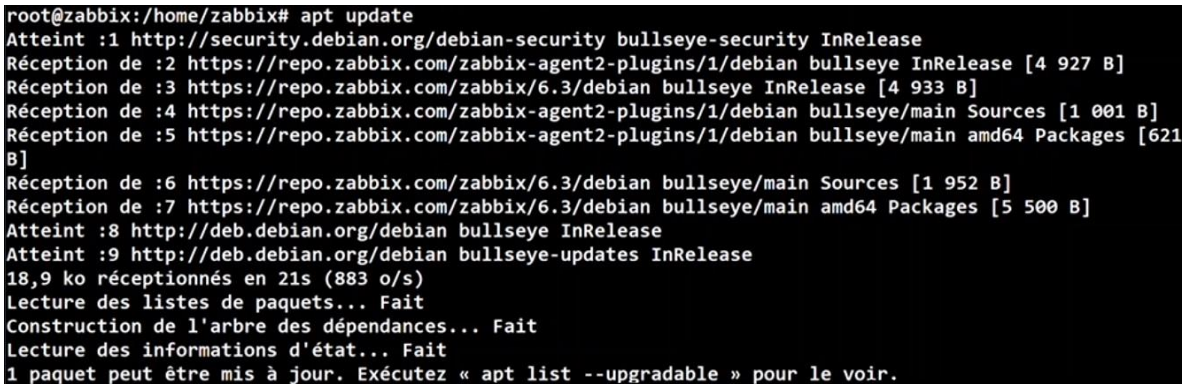


Figure 74 : Commande de mise à jour des packages DEB du serveur Zabbix.

Installer le serveur Zabbix, l'interface Web (GUI) et les agents, comme illustré dans la figure ci-dessous ;

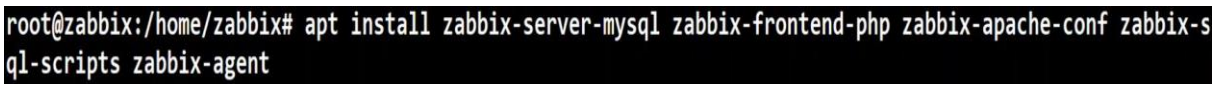


Figure 75 : Commande d'installation du serveur Zabbix.

Importer le schéma et les données dans la nouvelle base de données Zabbix créée, comme illustré dans la figure ci-dessous ;

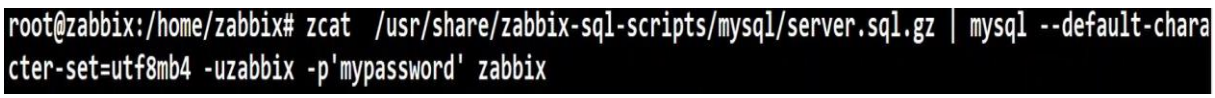


Figure 76 : Commande permettant d'apporter des modifications au serveur Zabbix.

Configurer le serveur Zabbix pour utiliser la nouvelle base de données dans laquelle on vient d'importer les données, puis modifier le fichier comme illustré dans la figure ci-dessous ;

Figure 77 : Commande permettant d'ouvrir le fichier de configuration du serveur Zabbix.

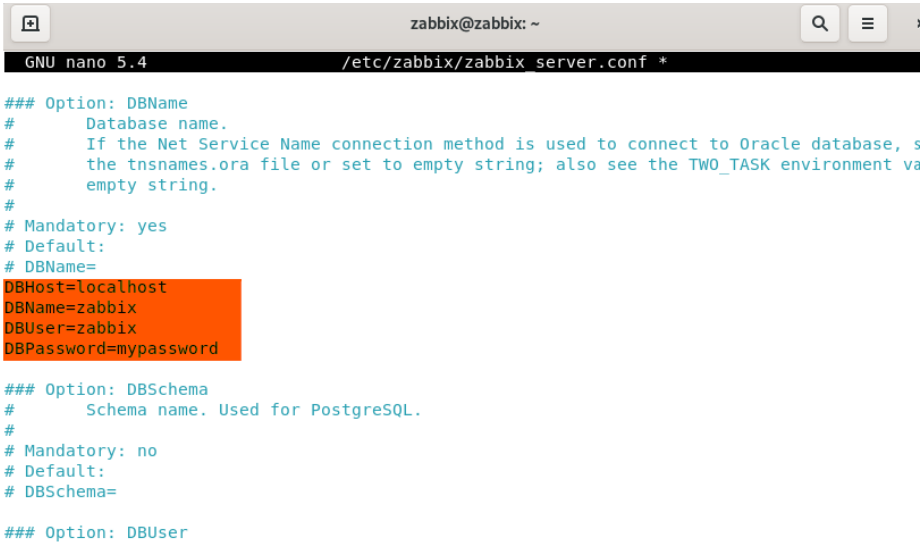


Figure 78 : Le fichier de configuration du serveur Zabbix.

Redémarrez maintenant le serveur Apache pour appliquer les nouvelles modifications, comme illustré dans la figure ci-dessous ;

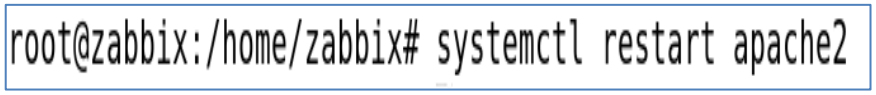


Figure 79 : Commande de redémarrage de Appache2.

Démarrer le serveur Zabbix les services doivent déjà être configurés pour démarrer automatiquement au redémarrage, comme illustré dans la figure ci-dessous ;

Figure 80 : Commande de démarrage du serveur Zabbix.

S'assurer que le serveur Zabbix est activé, comme illustré dans la figure ci-dessous ;

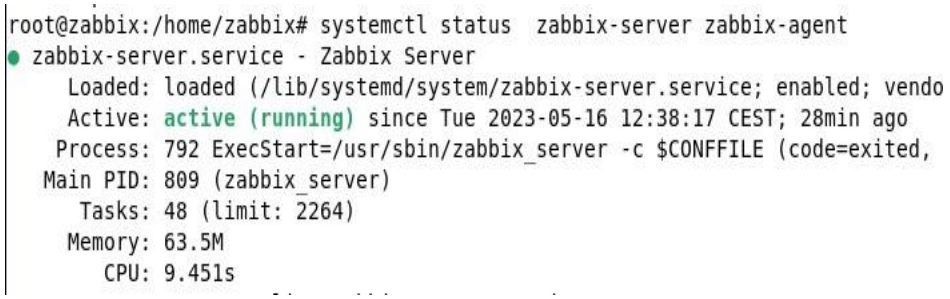


Figure 81 : Commande de vérification si le serveur Zabbix est opérationnel.

Étape 4 : Terminer l'installation de Zabbix via l'assistant web

Vous pouvez maintenant vous connecter à l'interface Zabbix et terminer le processus d'installation. Il suffit pour cela de pointer votre navigateur vers l'adresse indiquée ci-dessous. Pour accéder à l'assistant d'installation de la console, il faut d'abord exécuter la commande « ifconfig » afin de récupérer votre adresse IP.

Figure 82 : Lien de navigateur vers le serveur Zabbix.

Sur le premier écran de l'assistant d'installation frontale, utiliser le menu déroulant ''Langue par défaut'' pour choisir la langue que vous voulez, comme illustré dans la figure ci-dessous ;

Figure 83 : Choix de la langue pour continuer l'installation.

Vérifier les prérequis. S'assurer que toutes les conditions logicielles préalables sont remplies, comme illustré dans la figure ci-dessous ;

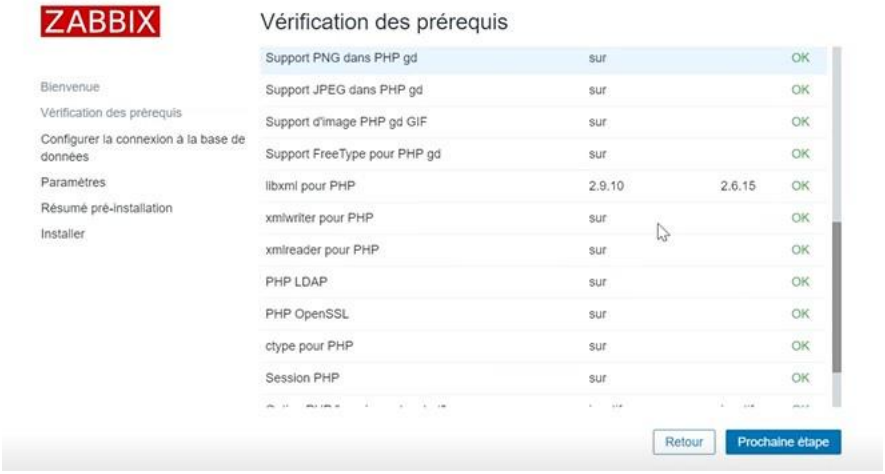


Figure 84 : Les conditions logicielles préalables de Zabbix.

Configurer la connexion à la base de données et y entrer ses détails de connexion. La base de données Zabbix devrait déjà être créée, comme illustré dans la figure ci-dessous ;

Figure 85 : Configuration de la base de données de Zabbix

Saisir les paramètres, à savoir le nom du serveur Zabbix, le fuseau horaire et le thème par défaut pour l'interface frontale, comme illustré dans la figure ci-dessous ;

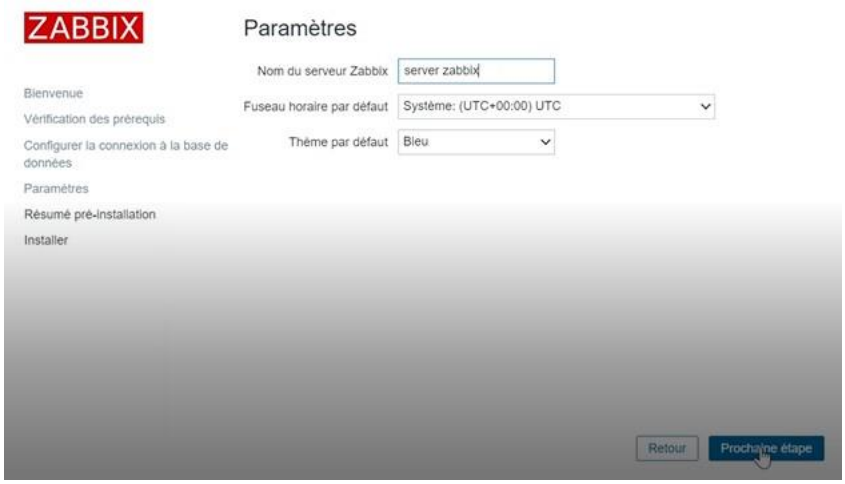


Figure 86 : Paramètre de saisie du nom de Zabbix.

S'assurer d'avoir terminé toutes les étapes d'installation, comme illustré dans la figure ci-dessous ;

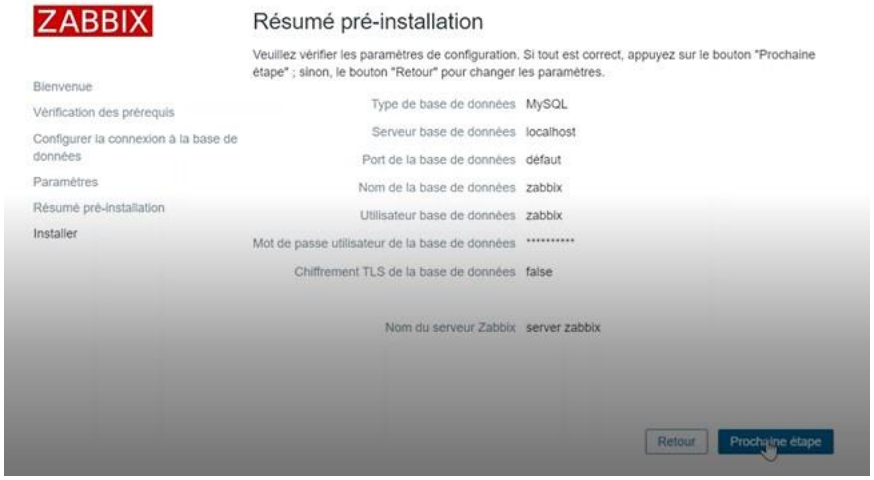


Figure 87 : Installation complète de Zabbix.

Vous pouvez désormais commencer à utiliser le logiciel Zabbix, la figure ci-dessous montre la fin de l'installation ;

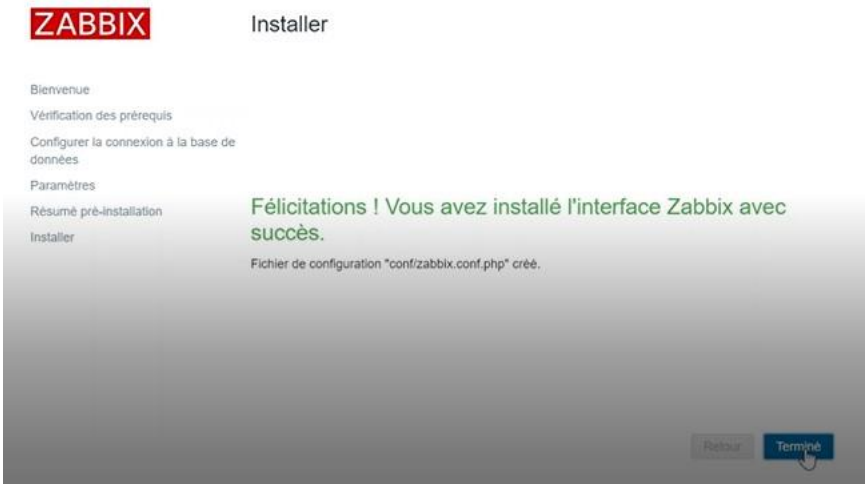


Figure 88 : Zabbix prêt à être utilisé

Sur la page de connexion, utiliser les informations de connexion par défaut pour se connecter (Nom d'utilisateur = Admin, Mot de passe = zabbix) comme illustré dans la figure ci-dessous. Une fois authentifié, il est recommandé de sécuriser le compte de l'administrateur Zabbix en remplaçant le mot de passe par défaut par un mot de passe plus puissant ;

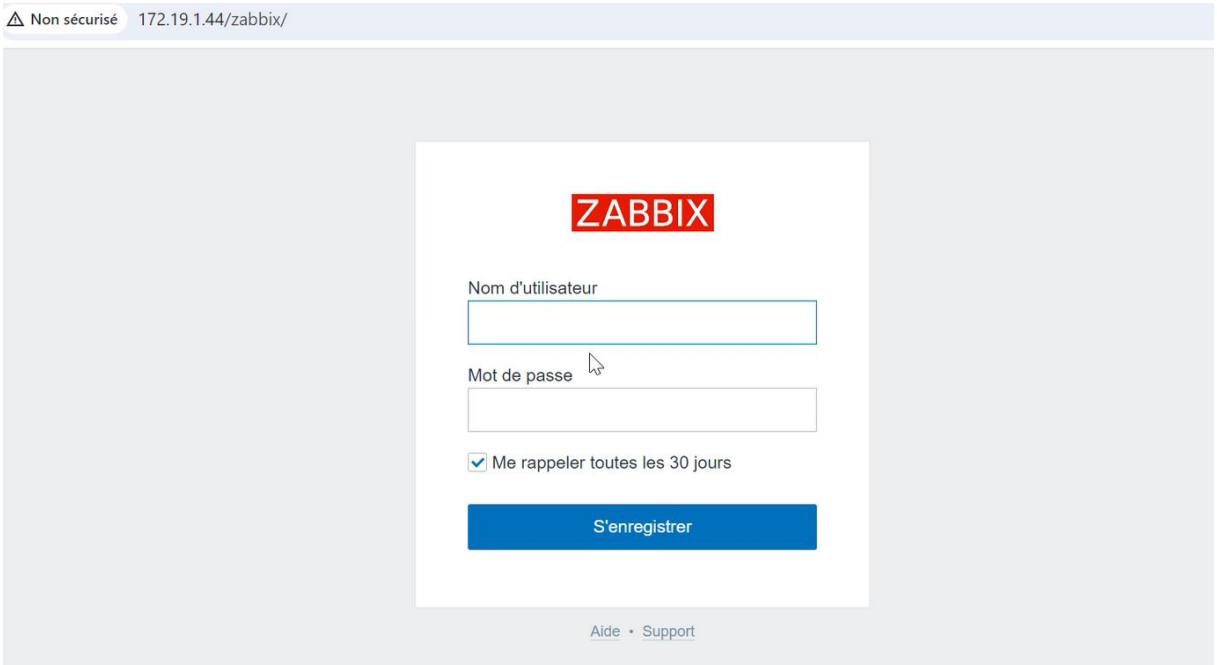


Figure 89 : Page de connexion de Zabbix

La figure ci-dessous montre la page d'accueil de Zabbix ;

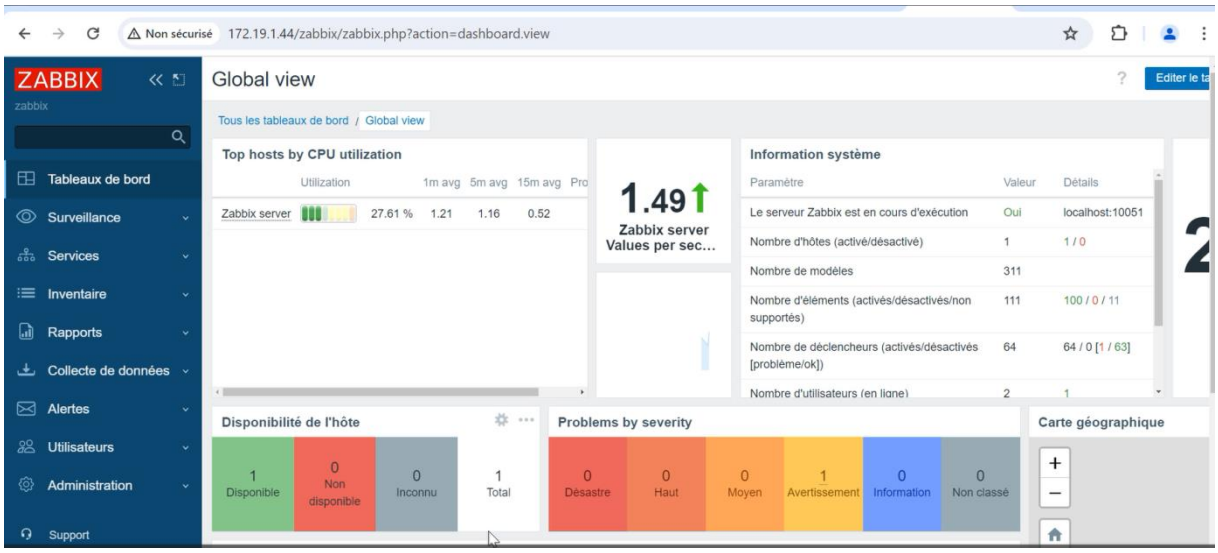


Figure 90 : Page d'accueil de Zabbix.

5.2. Ajouter des hauts

Avant de créer des hôtes dans Zabbix, il convient de noter que le serveur Zabbix lui-même est déjà considéré comme un hôte. En effet, Zabbix surveille ses propres composants pour s'assurer qu'ils fonctionnent correctement et pour identifier tout éventuel problème de performance ou de configuration. Cette surveillance des composants internes de Zabbix permet d'obtenir une vue complète de l'état de l'environnement de surveillance.

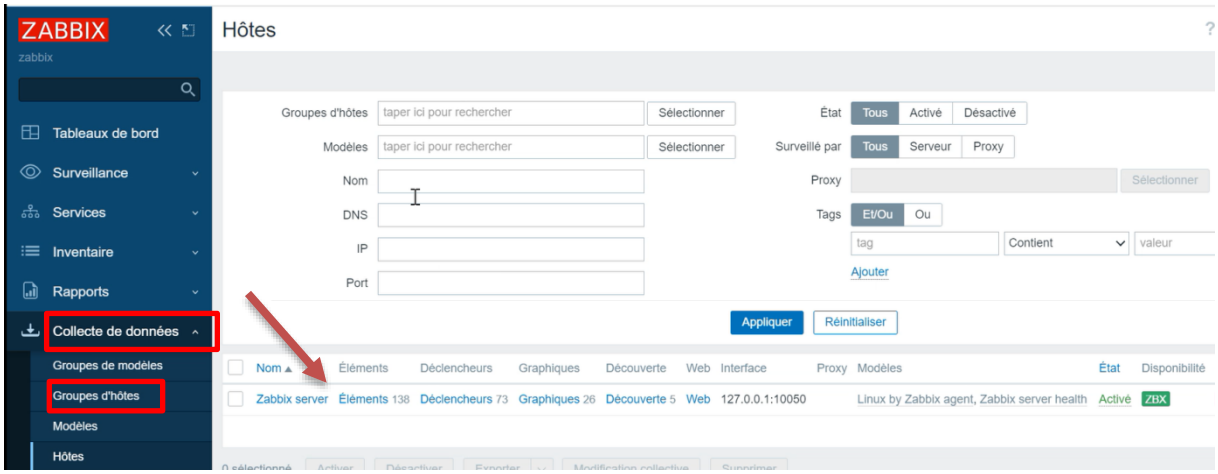


Figure 91 : Supervision du serveur zabbix

- **Ajouter un commutateur**

Pour ajouter un commutateur dans Zabbix, il est nécessaire de suivre les étapes illustrées dans les figures suivantes :

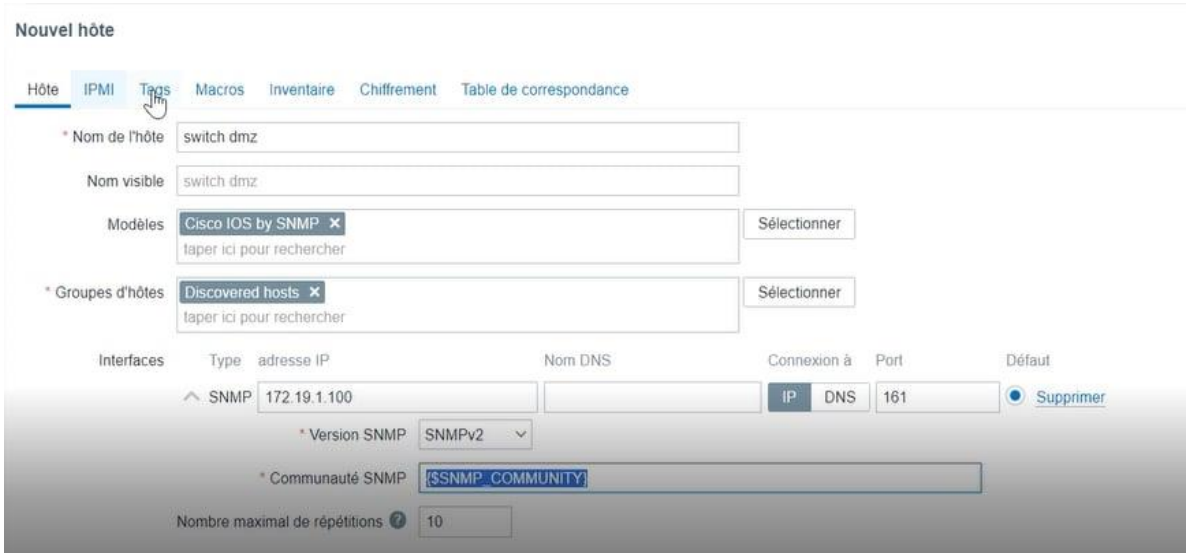


Figure 92 : Configuration d'un nouvel hôte

Tout d'abord, il faut remplir le nom de l'hôte, puis sélectionner le modèle approprié afin que Zabbix puisse choisir une Template spécifique pour l'équipement. Dans notre cas, il s'agit d'un équipement Cisco avec un agent SNMP. Ensuite, il est important de choisir les groupes d'hôtes correspondants pour regrouper des hôtes similaires et faciliter la gestion de la surveillance, la configuration des paramètres de surveillance de manière centralisée, la génération de rapports et de tableaux de bord pour chaque groupe d'hôtes, et la définition des permissions d'accès pour les utilisateurs de Zabbix.

Enfin, il est essentiel de configurer le protocole SNMP en indiquant l'adresse IP de l'équipement, la version du protocole et la communauté SNMP. Cette communauté est déjà configurée par défaut, il suffit donc simplement de la copier pour l'utiliser à l'étape suivante.

- **Remarque :**

Les templates Zabbix sont des modèles de configuration prédéfinis écrits en YAML, un format de représentation de données textuelles facilement lisible par les humains et les machines. Ils peuvent être utilisés pour surveiller différents types de services et d'applications, car ils contiennent des éléments de surveillance tels que des seuils de déclenchement, des graphiques et des alertes.

En utilisant les templates Zabbix, les utilisateurs peuvent gagner du temps et simplifier la configuration de la surveillance de leurs hôtes. Les utilisateurs peuvent également créer leurs propres templates personnalisés pour répondre à leurs besoins spécifiques et les partager avec la communauté.

La prochaine étape consiste à configurer une macro avec sa valeur. Cette valeur sera utilisée lors de la configuration du protocole SNMP au niveau des commutateurs. Il s'agit en quelque sorte d'un mot de passe partagé entre le serveur Zabbix et le commutateur DMZ.

- **Définition d'une Macro :**

Les macros dans Zabbix sont des variables qui permettent de stocker des valeurs dynamiques ou statiques, utilisées pour personnaliser et adapter le comportement du système de surveillance. Elles sont principalement utilisées pour paramétrer des objets tels que les hôtes, les éléments, les déclencheurs, les actions, les graphiques, les modèles, etc. Une macro dans Zabbix est représentée par une chaîne de caractères encadrée par des accolades, par exemple {$MACRO}. Voir ça configuration dans la figure ci-dessous ;

Figure 93 : Configuration d'une Macro

- **Configuration du protocol SNMP au niveau des Commutateurs (DMZ)**

La configuration du SNMP sur un commutateur implique plusieurs étapes :

– Activation du SNMP : Le service SNMP est activé sur le commutateur en utilisant la commande « snmp-server ».

– Communautés SNMP : Les communautés SNMP sont configurées pour permettre l'accès au commutateur avec une valeur (mot de passe partagé). On définit une communauté en lecture seule (read-only) ou une communauté en lecture/écriture (read-write). Dans notre cas, nous utilisons le mot de passe partagé « swdmzsnmp » entre le serveur et le commutateur DMZ.

– Niveaux d'accès SNMP : Les niveaux d'accès SNMP sont définis pour spécifier les permissions. Nous configurons la communauté SNMP en mode « RO » (read-only) pour permettre uniquement la récupération d'informations.

– Adresses IP autorisées : Les adresses IP autorisées à accéder au commutateur via SNMP sont spécifiées pour des raisons de sécurité. Dans notre cas, nous autorisons l'adresse IP de notre serveur de supervision Zabbix, avec l'adresse IP 172.19.1.100

```
DMZ(config)#snmp-server community swdmzsnmp ro
DMZ(config)#end
```

Figure 94 : Configuration du protocol SNMP sur le commutateur DMZ

Après avoir configuré le commutateur et le serveur Zabbix, on peut observer dans la figure ci-dessous que le commutateur DMZ est ajouté au serveur Zabbix. Il est important de noter que le commutateur doit être ajouté au serveur avant d'activer le protocole SNMP sur celui-ci.

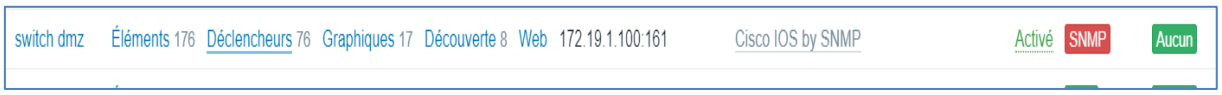


Figure 95 : Surveillance de switch DMZ

Cependant, on peut remarquer que la disponibilité du SNMP sur le commutateur est affichée en rouge, ce qui indique qu'il y a un problème. Il est probable que cela soit dû au fait que le serveur Zabbix n'est pas encore connecté à la topologie sur GNS3.

Lorsque nous cliquons sur le problème, nous constatons que les requêtes ping échouent Figure ci-dessous. Cela confirme notre hypothèse précédente selon laquelle le serveur n'est pas connecté à la topologie sur GNS3.

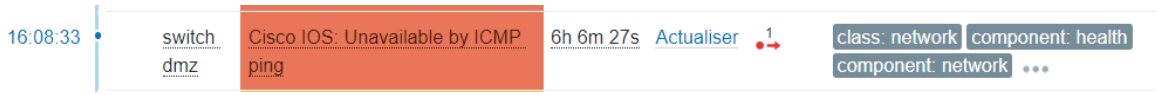


Figure 96 : Problème des requêtes ICMP

Pour résoudre ce problème, il est nécessaire de connecter le serveur Zabbix à la topologie réseau sur GNS3.

Après avoir résolu le problème et connecté le serveur Zabbix à la topologie sur GNS3, nous pouvons effectuer un test de ping depuis le serveur Zabbix vers le commutateur distribution et également vers Internet en passant par la topologie pour s'assurer que tout est correctement connecté.

```
zabbix@zabbix:~$ ping 172.19.1.100
PING 172.19.1.100 (172.19.1.100) 56(84) bytes of data.
64 bytes from 172.19.1.100: icmp_seq=1 ttl=255 time=1.59 ms
64 bytes from 172.19.1.100: icmp_seq=2 ttl=255 time=1.51 ms
64 bytes from 172.19.1.100: icmp_seq=3 ttl=255 time=1.85 ms
64 bytes from 172.19.1.100: icmp_seq=4 ttl=255 time=2.03 ms
64 bytes from 172.19.1.100: icmp_seq=5 ttl=255 time=1.72 ms
64 bytes from 172.19.1.100: icmp_seq=6 ttl=255 time=1.07 ms
```

Figure 97 : Test Ping du serveur Zabbix ver le commutateur DMZ

```
DMZ#ping 172.19.1.44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.19.1.44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

Figure 98 : Test ping du commutateur DMZ ver le serveur Zabbix

```
root@zabbix:/home/zabbix# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=124 time=33.8 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=124 time=34.7 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=124 time=29.9 ms
```

Figure 99 : Test Ping du serveur zabbix ver Internet

Après avoir effectué les tests de ping, nous constatons que les résultats sont positifs et que la connectivité fonctionne correctement. Cela est illustré dans les figures précédents où les tests de ping ont été exécutés avec succès.

Et après quelques minutes, nous constatons que le problème est résolu et que le commutateur DMZ est ajouté avec succès, sans aucun problème. Voir la figure ci-dessous.

Cela signifie que le protocole SNMP fonctionne correctement et que le serveur Zabbix peut maintenant surveiller et gérer le commutateur DMZ grâce à la configuration adéquate du SNMP.

Figure 100 : Etat du switch DMZ après avoir résolu le problème de connectivité

- **Ajout du routeur**

Le routeur est également un équipement Cisco, tout comme les commutateurs précédents. Par conséquent, sa configuration sur Zabbix est similaire à celle des commutateurs.

Après avoir configuré le routeur EPB et suivi les mêmes étapes de configuration des commutateurs, Zabbix a détecté un problème (voir la figure ci-dessous) : les deux interfaces eth0/0 et eth0/1 sont configurées en mode Half-Duplex.

Figure 101 : Problème du routeur EPB détecté par Zabbix

Pour résoudre ce problème, nous allons configurer ces deux interfaces en mode FullDuplex. Les configurations requises sont illustrées dans la Figure ci-dessous ;

```
R1(config)#interface  range ethernet 0/0-1
R1(config-if-range)#du
R1(config-if-range)#duplex fu
R1(config-if-range)#duplex full
R1(config-if-range)#
R1(config-if-range)#end
R1#
R1#
R1#
R1#wr
Building configuration...
[OK]
```

Figure 102 : Résoudre le problème du routeur

Après avoir configuré les interfaces eth0/0 et eth0/1 en mode Full-Duplex, nous constatons que le problème a été résolu, comme le montre la Figure ci-dessous ;

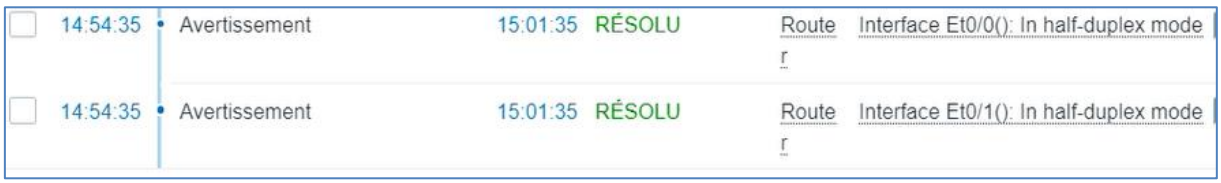


Figure 103 : Résolution de problème du routeur

- **Ajouter serveur Windows**

Tout d'abord, télécharger la dernière version de l'agent Zabbix sur le site officiel de Zabbix. Exécuter le programme d'installation de l'agent Zabbix sur le serveur Windows que vous souhaitez superviser. Suivez les instructions pour terminer l'installation. Ouvrez le fichier de configuration de l'agent Zabbix (zabbix_agentd. Conf) situé généralement dans le répertoire d'installation de l'agent. Configurez les paramètres tels que l'adresse du serveur Zabbix, le port, etc.

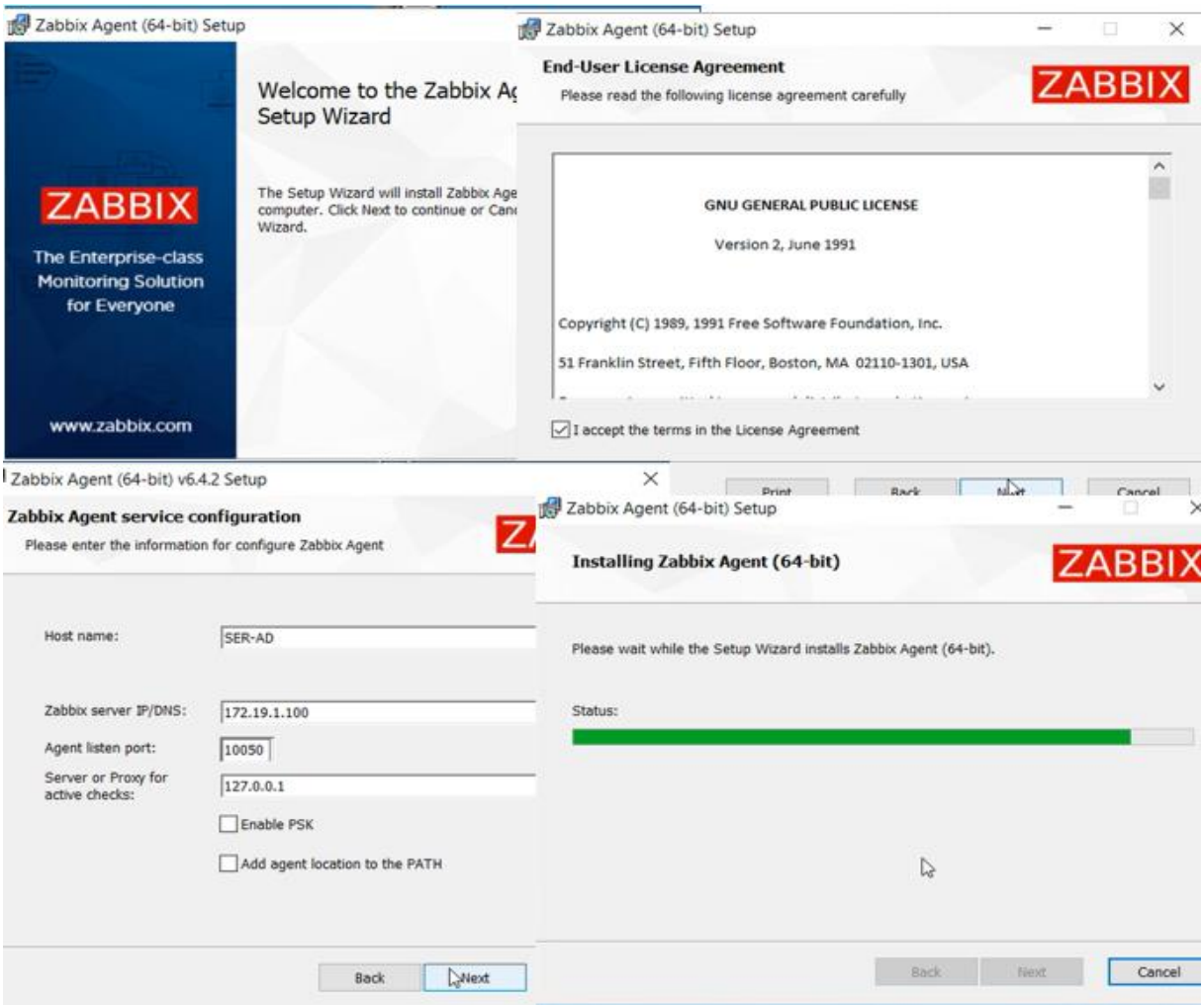


Figure 104 : Etapes d'installation de l'agent Zabbix pour Windows

Ensuite ajouter de l'hôte sur le serveur Zabbix, Connecter à l'interface web Zabbix, accédez à la section "Configuration", puis "Hôtes". Cliquer sur "Créer un hôte" et saisir les détails de l'hôte Windows à surveiller.

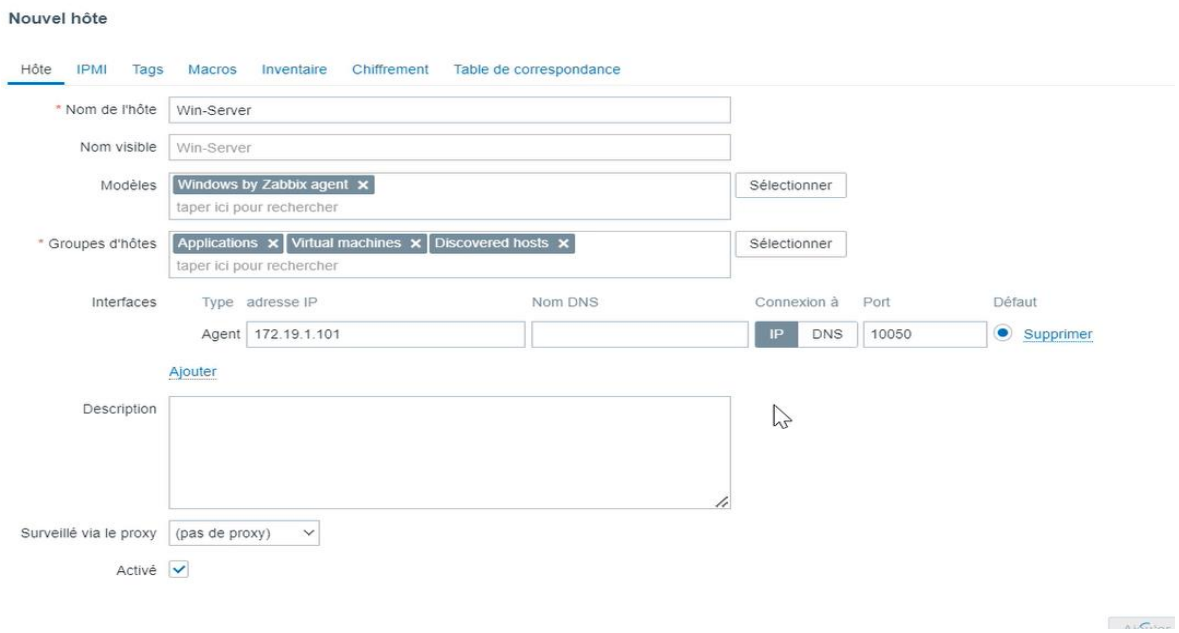


Figure 105 : Configuration de serveur Windows sur zabbix

Après avoir configuré les éléments de surveillance, surveillez les données collectées par l'agent Zabbix pour vous assurer que la supervision fonctionne correctement.

Figure 106 : Etat de serveur Windows sur Zabbix

- **Ajouter pfsense**

Créer un nouvel hôte (pfsense) en suivant la même procédure que pour les équipements précédents. Ensuite, dans la configuration de l'hôte, nous sélectionnons le modèle (la Template importée) comme illustré dans la figure ci-dessous, nous cliquons sur le bouton "Ajouter". Cela permettra de surveiller et d'analyser les performances du pare-feu pfsense à l'aide des paramètres prédéfinis dans la Template importée.

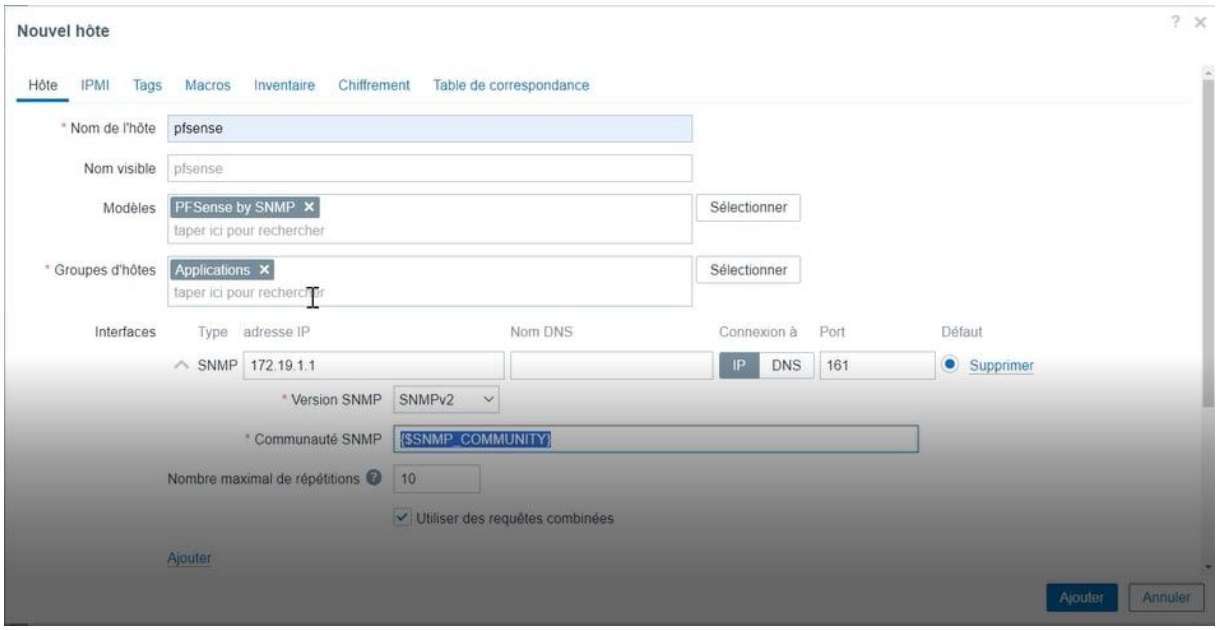


Figure 107 : Ajouter le pare-feu pfsense

Configuration du protocole SNMP au niveau du pare-feu pfsense

Pour configurer SNMP ajouter la communauté SNMP sur pfSense, accédez à l'interface Web de pfSense et allez dans Services > SNMP. Dans cette section, cochez la case pour activer le service SNMP. Ensuite, dans le champ Community, entrez le nom de la communauté, par exemple public. Assurez-vous que le port est défini par défaut sur 161, sauf si vous devez utiliser un port différent. Enfin, cliquez sur Save pour enregistrer les modifications.

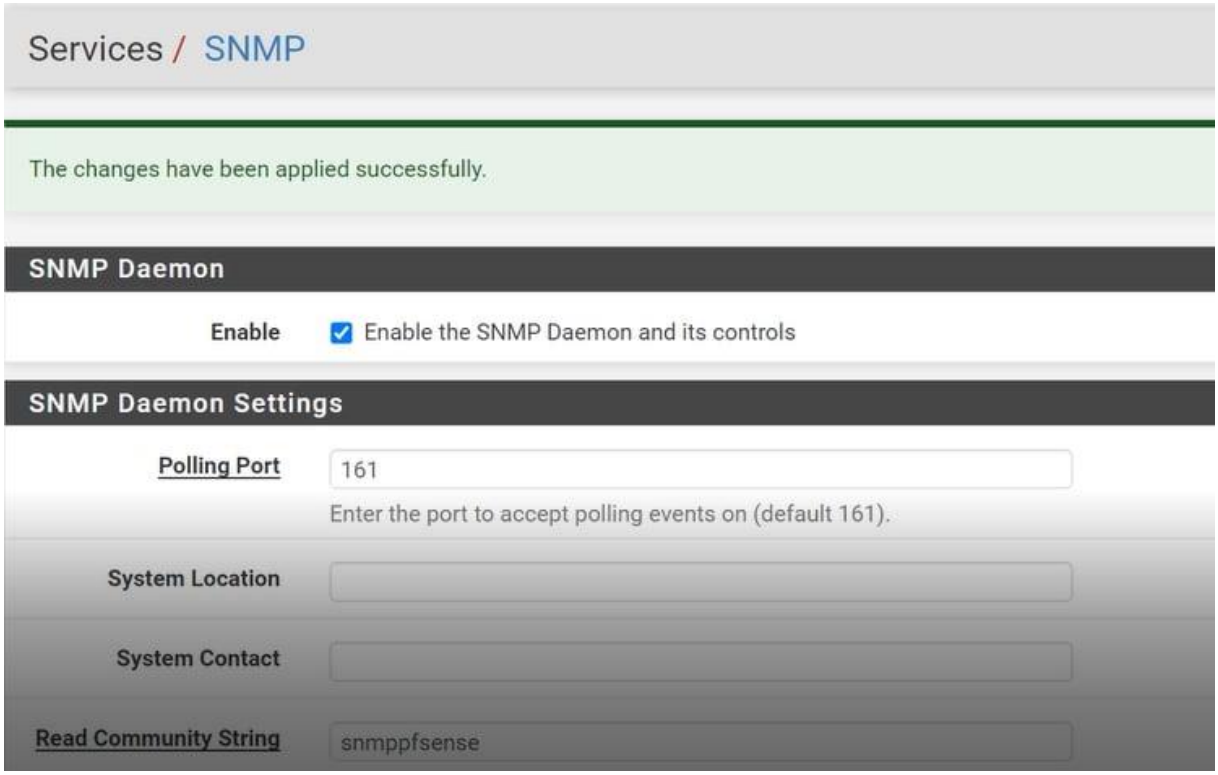
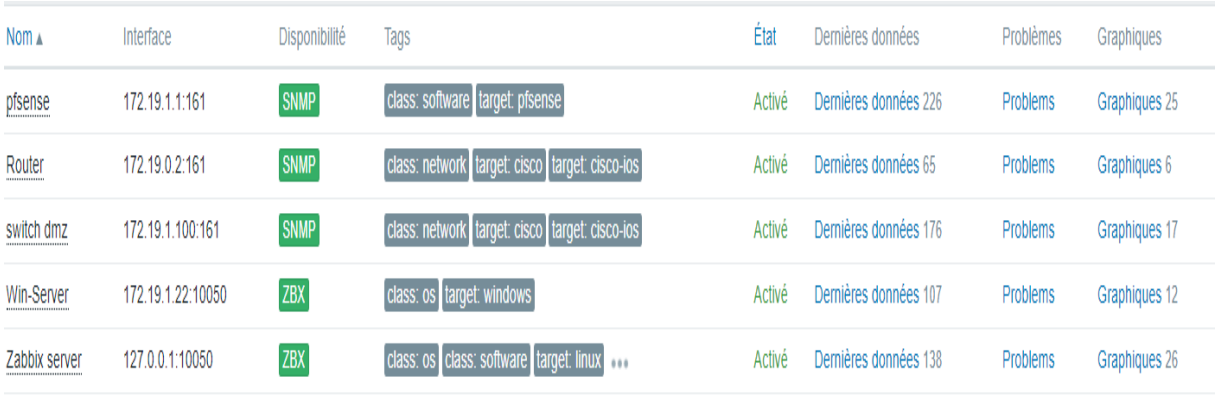


Figure 108 : Configuration de SNMP au niveau du pare-feu

Après avoir configuré le protocole SNMP sur Zabbix et sur le pare-feu, on constate que le pare-feu a été ajouté avec succès à Zabbix, sans aucun problème, voir la figure ci-dessous ;

Figure 109 : Etat du pare-feu pfsense

Après avoir configuré avec succès tous les équipements et les avoir ajoutés à Zabbix, nous pouvons confirmer que la surveillance est opérationnelle. Dans la suivant, nous pouvons voir que tous les équipements sont présents dans Zabbix, prêts à être surveillés et à détecter d'éventuels problèmes.



Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
pfsense	172.19.1.1:161	SNMP	class: software target: pfsense	Activé	Dernières données 226	Problems	Graphiques 25
Router	172.19.0.2:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 65	Problems	Graphiques 6
switch dmz	172.19.1.100:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 176	Problems	Graphiques 17
Win-Server	172.19.1.22:10050	ZBX	class: os target: windows	Activé	Dernières données 107	Problems	Graphiques 12
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 138	Problems	Graphiques 26

Figure 110 : Vue d'ensemble de la surveillance des équipements sur Zabbix

Zabbix permet de visualiser un enregistrement en temps réel de tous les événements qui se passent dans nos systèmes surveillés.

Pour assurer la surveillance de notre machine, nous allons superviser les paramètres systèmes tels que le CPU, le Traffic réseau ainsi que la mémoire afin de réaliser cette surveillance de manière efficace. Cela nous permettra de déterminer l'état du module surveillé et de diagnostiquer les éventuels problèmes en temps opportun, Alors Pour visualiser les graphes d'une machine sur Zabbix, allez directement dans l'onglet "Équipements", sélectionnez la machine souhaitée, puis cliquez sur "Graphes". Les graphes disponibles pour cette machine s'afficheront, Dans notre exemple illustré dans la figure ci-dessous Le module CPU, Traffic réseau et la mémoire renvoie les informations et pourcentages en usage.

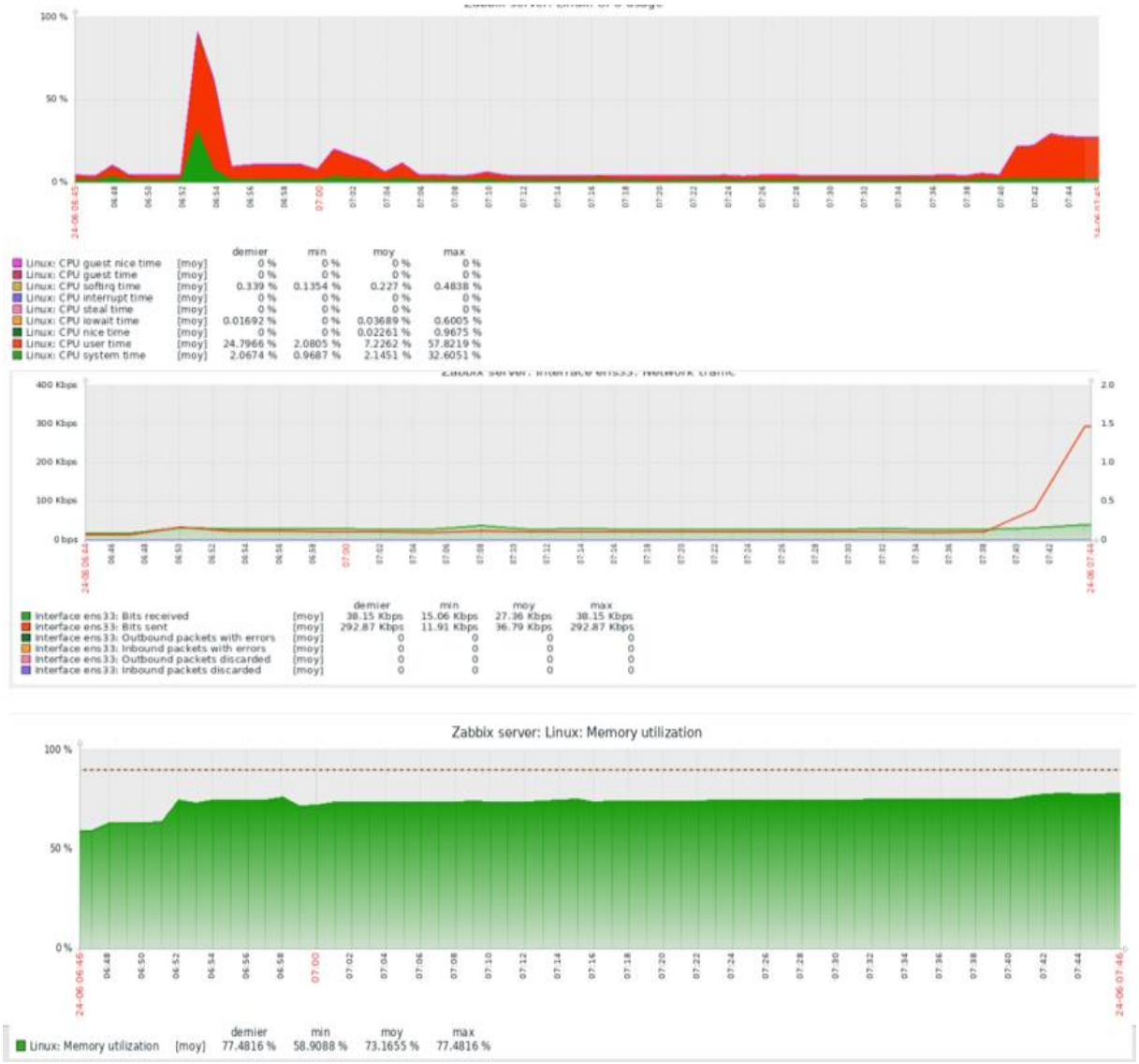


Figure 111 : Graphe des différents paramètres system de notre machine de supervision.

5.3. Ajouter une carte sur Zabbix

Ajouter une carte sur Zabbix offre une représentation visuelle de la topologie réseau ou système surveillée, permettant ainsi de visualiser les éléments surveillés et leurs performances de manière graphique.

Pour ajouter une carte sur Zabbix, ensuite les étapes illustrées dans les figures suivantes :

D'abord, on commence par cliquer sur l'onglet "Surveillance" dans Zabbix. Ensuite, on sélectionne l'option "Cartes" dans le menu. Pour créer une nouvelle carte, on clique sur le bouton "Créer une carte". On peut se référer à la figure ci-dessous pour voir à quoi cela ressemble.

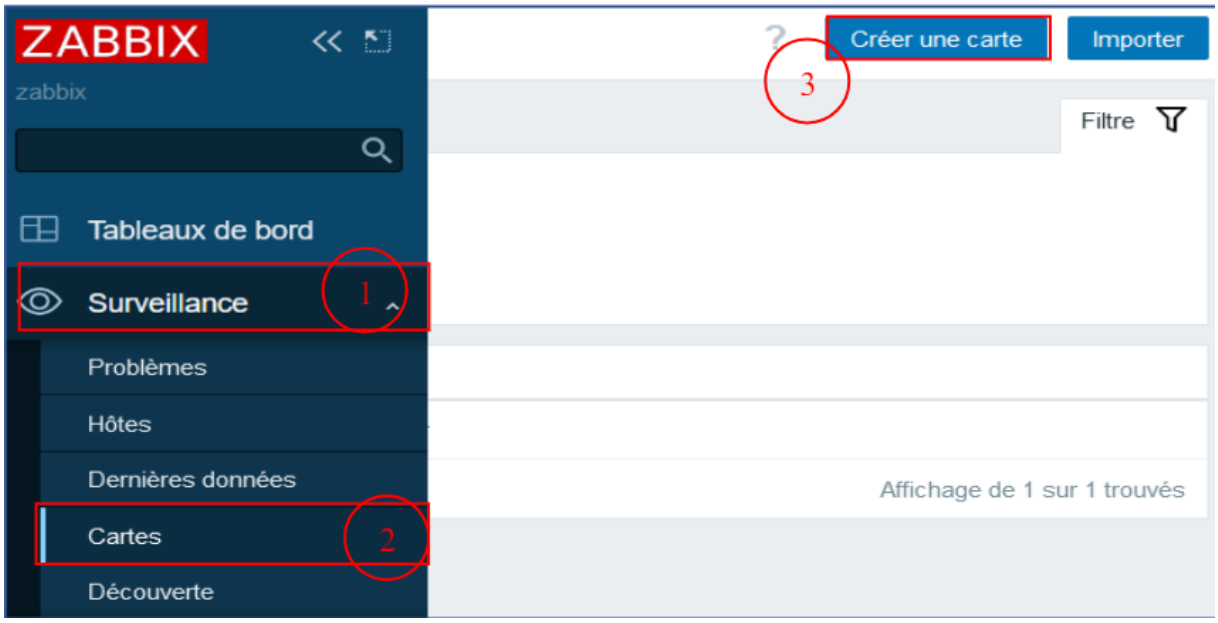


Figure 112 : Création d'une nouvelle carte

Ensuite, il faut remplir les informations de la carte telles que le Propriétaire, le Nom, la Largeur, etc. Une fois toutes les informations remplies, on clique sur le bouton "Ajouter" pour ajouter cette carte.

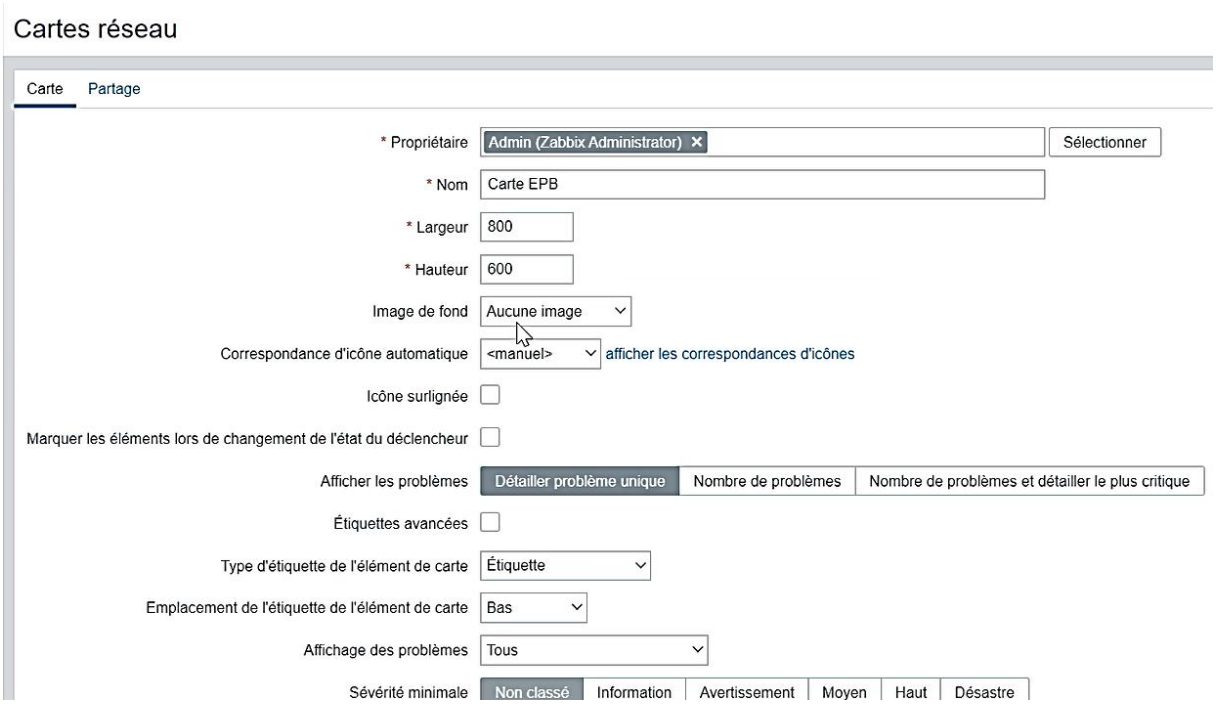


Figure 113 : Remplissage des informations de la carte sur Zabbix

Après avoir créé cette carte, on clique sur le bouton "Ajouter" pour ajouter un équipement à la carte. Ensuite, on remplit les différents éléments à l'intérieur tels que le

Type, l'Étiquette, la Sélection de l'icône, etc. On peut se référer à la figure ci-dessous pour visualiser cette étape. Le champ le plus important est le champ "Hôte", où il faut sélectionner l'équipement physique correspondant à ajouter à la carte. Une fois toutes les informations remplies, on clique sur le bouton "Appliquer" pour valider les modifications.

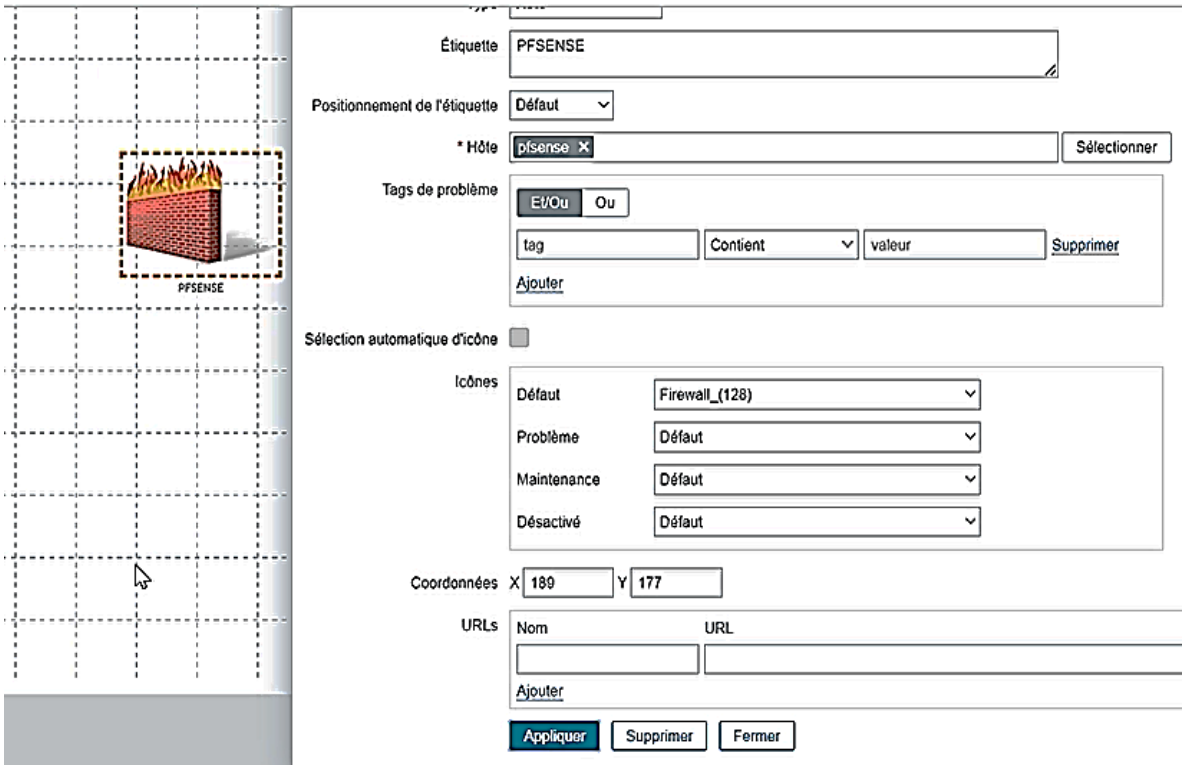


Figure 114 : Ajout d'un équipement à la carte et configuration des éléments

Le même principe est appliqué pour ajouter les autres équipements sur la carte. Il suffit de modifier l'hôte et l'icône de l'hôte pour obtenir le résultat illustré dans la figure ci-dessous ;

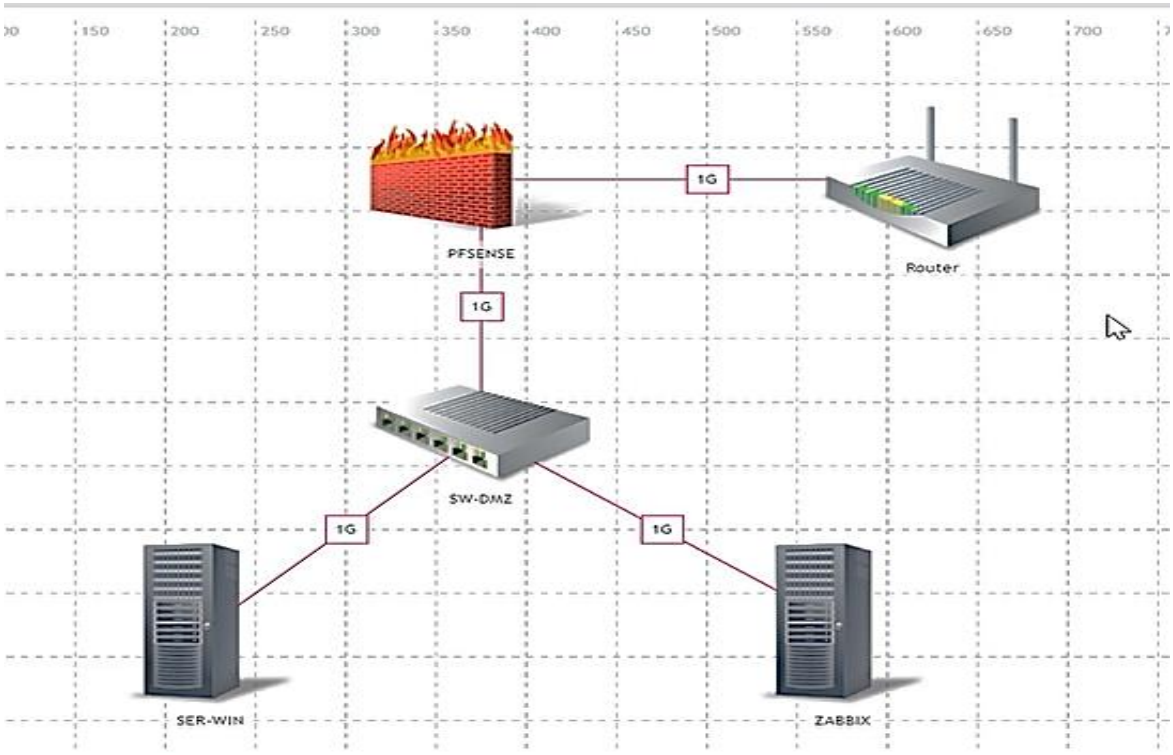


Figure 115 : Vue finale de la carte avec les équipements ajoutés

Maintenant, nous allons ajouter cette carte au tableau de bord Zabbix afin de visualiser les problèmes détectés par Zabbix. Pour effectuer cette tâche, on se rend sur la barre de navigation de Zabbix, puis on clique sur "Tableau de bord". Ensuite, on clique sur "Éditer le tableau de bord".

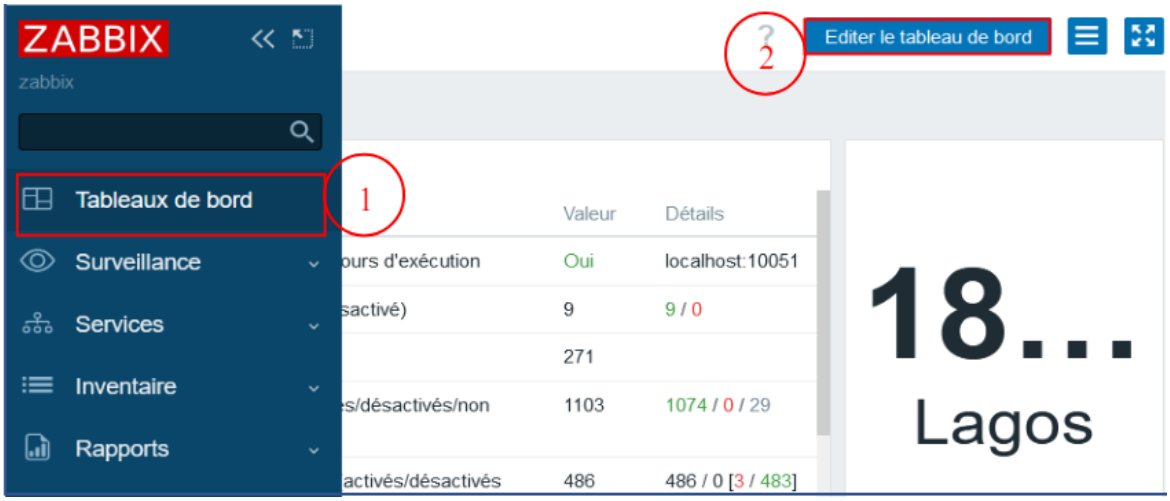


Figure 116 : Édition du tableau de bord Zabbix

Une fois que nous avons cliqué sur le bouton "Éditer le tableau de bord", nous cliquons sur un endroit vide du tableau de bord. Cela ouvrira la fenêtre "Ajouter un widget", comme

illustré dans la Figure ci-dessous. Dans la section "Type", nous sélectionnons "Carte", puis nous cliquons sur "Ajouter" pour l'ajouter au tableau de bord.

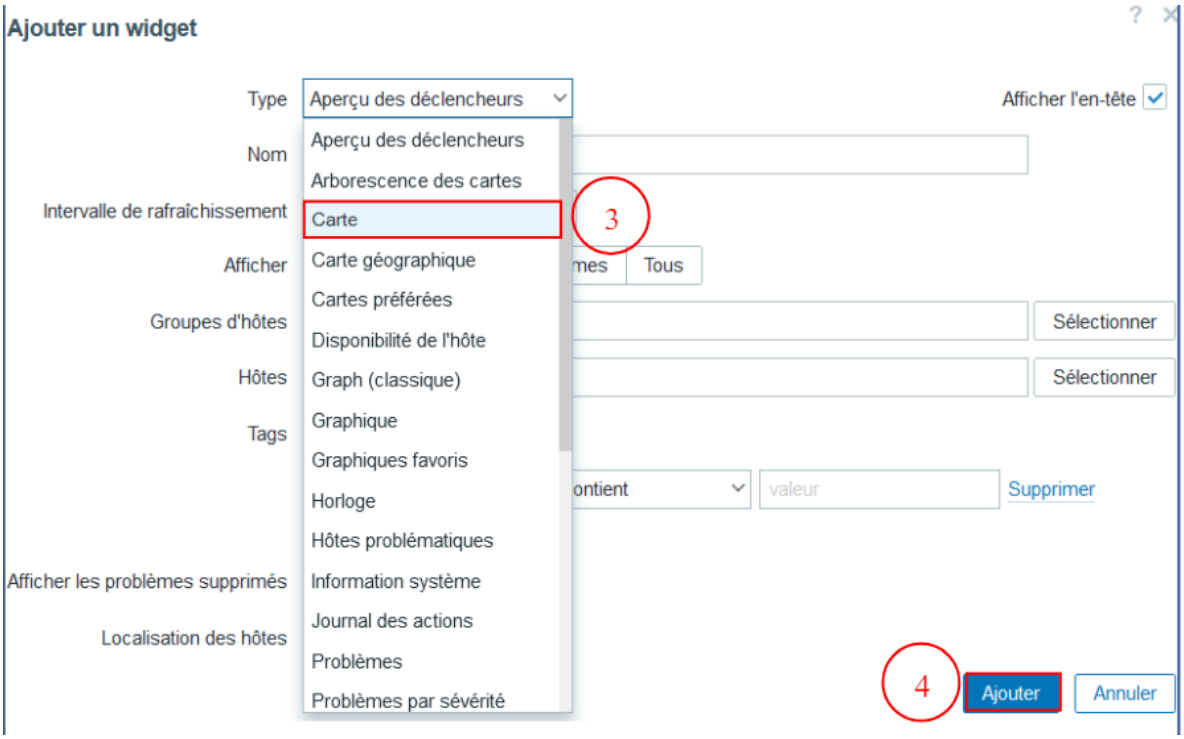


Figure 117 : Ajout d'un widget de carte sur le tableau de bord Zabbix

On peut observer que la carte a été ajoutée et qu'il n'y a aucun problème dans la topologie du réseau pour le moment.

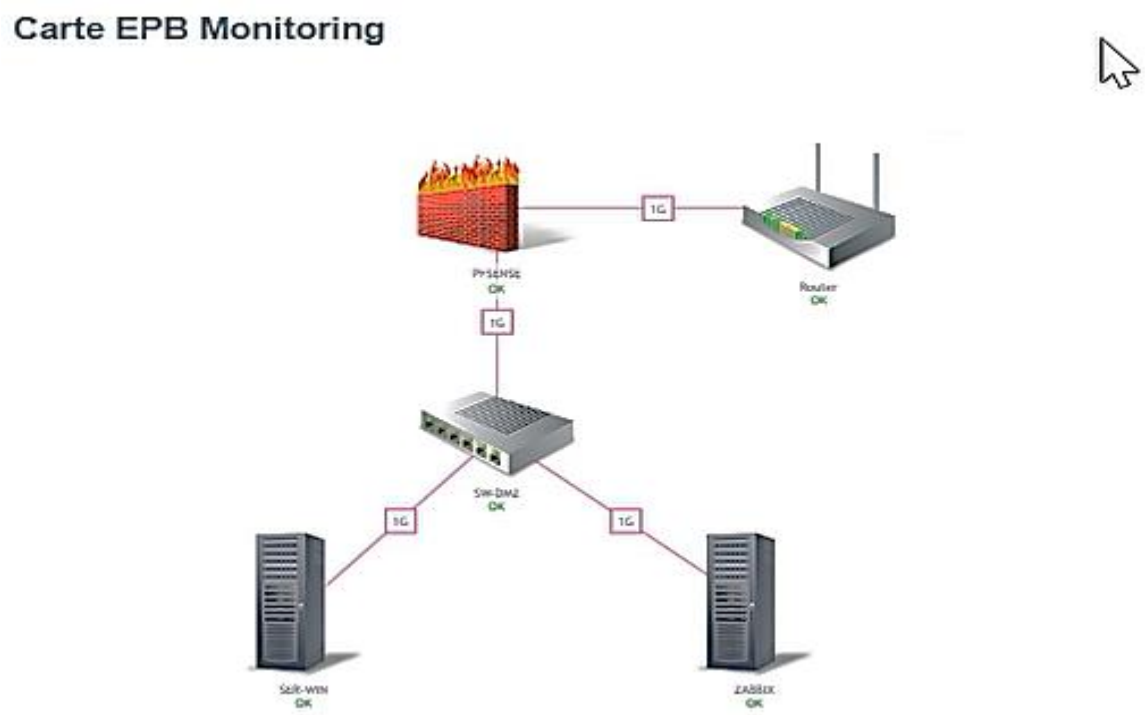


Figure 118 : Carte ajoutée sur le tableau de bord Zabbix

5.4. Configuration des alertes Zabbix avec le service Gmail

Dans Zabbix, la méthode la plus simple est d'assigner une alerte d'avertissement. Notre première alerte consiste simplement à envoyer un e-mail lorsqu'une des machines se trouve dans un état critique. Pour configurer Zabbix afin d'envoyer des alertes via Gmail, nous avons installé et configuré le protocole SMTP.

- **Installation et configuration du service SSMTP sur le serveur Debian**

L'objectif de l'installation de SSMTP sur le serveur Debian est de configurer un serveur SMTP local qui agira comme un relais pour les e-mails sortants depuis le serveur Debian vers le serveur SMTP de Gmail.

```
root@zabbix:/home/zabbix# apt install ssmtp
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libgnutls-openssl27
```

Figure 119 : Installation du service SSMTP

Cette étape consiste à modifier le fichier de configuration de SSMTP afin que notre service SSMTP puisse se connecter à Gmail et envoyer des e-mails. Pour effectuer des modifications dans le fichier de configuration SSMTP.

Figure 120 : Configuration du service SSMTP

Maintenant nous devons fournir des informations d'authentification, telles que le nom d'utilisateur (dans notre cas, "djamila.djedjiga@gmail.com") et le mot de passe généré par Gmail. De plus, nous devons spécifier le "mailhub" comme étant "smtp.gmail.com" et modifier le port pour le configurer sur "465".

Figure 121 : modification du fichier de configuration SSMTP

Le "mail hub" représente l'adresse du serveur SMTP vers lequel SSMTP enverra les e-mails sortants. Quant au port, il s'agit du canal de communication utilisé pour établir la connexion avec le serveur SMTP. En configurant correctement ces paramètres dans le fichier

de configuration de SSMTP, nous permettons à SSMTP d'établir une connexion sécurisée avec le serveur SMTP de Gmail et d'envoyer les e-mails avec succès.

Maintenant que nous avons configuré SSMTP sur le serveur Debian, nous allons effectuer un test en envoyant un e-mail via SSMTP. Pour cela, nous allons utiliser la commande illustrée dans la Figure ci-dessous pour envoyer un message contenant le texte "Test". Cette commande permettra de vérifier si la configuration de SSMTP fonctionne correctement en envoyant un e-mail de test.

```
root@zabbix:/home/zabbix#
echo "test zabbix" | ssmtp djamila.djedjiga@gmail.com
```

Figure 122 : Envoi d'un message de test avec SSMTP

Apres utilisation de la commande le message a été envoyée, Cela confirme que la configuration de SSMTP sur le serveur Debian est fonctionnelle. Comme illustré dans la figure ci-dessous ;

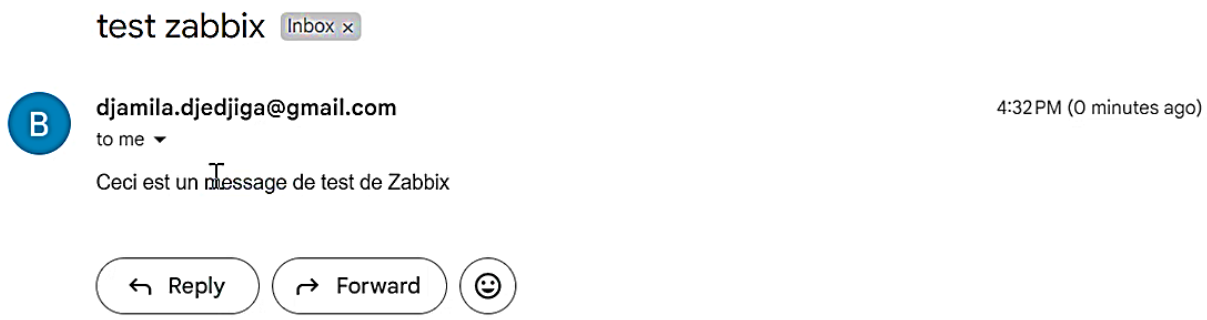


Figure 123 : Capture d'écran de confirmation d'envoi de l'e-mail via SSMTP.

- **Configuration et activation du service SMTP sur Zabbix**

Dans cette étape, nous allons configurer Zabbix pour qu'il utilise le serveur SMTP local configuré via SSMTP. Cela permettra de faire transiter les e-mails sortants de Zabbix par le biais du serveur SMTP local, qui se chargera ensuite de les envoyer à Gmail. Le service SSMTP installé sur Debian agit en tant qu'interface pour l'envoi des e-mails vers un serveur SMTP distant.

Tout d'abord, nous cliquons sur l'onglet "Alertes" dans le menu principal de Zabbix. Ensuite, nous sélectionnons "Types de média" dans la section des alertes. Une fois dans la liste des types de média, nous repérons l'option "Gmail" et cliquons sur le bouton "Activer"

correspondant. Cette étape permet d'activer le support de Gmail en tant que type de média pour les alertes par e-mail dans Zabbix.

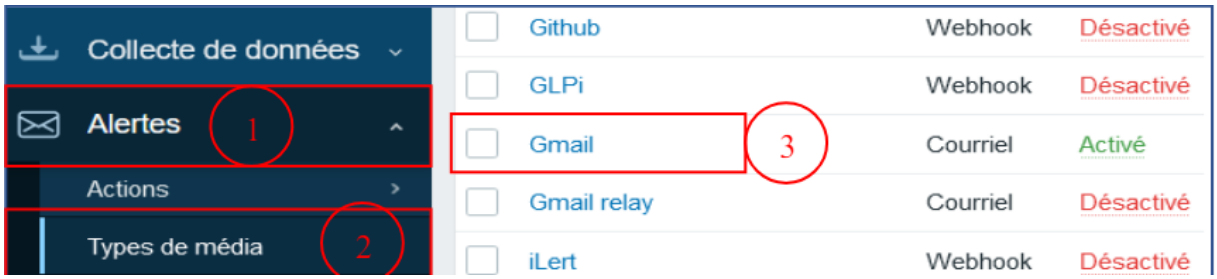


Figure 124 : Capture d'écran de l'activation du type de média Gmail dans Zabbix

Pour configurer l'e-mail comme type de média (les médias sont les canaux de diffusion utilisés pour envoyer des notifications et des alertes depuis Zabbix) : Accédez à Alertes → Types de médias. Cliquez sur Créer un type de média. Ce dernier contient les attributs généraux qu'il faut remplir obligatoirement comme illustré dans la figure ci-dessous ;

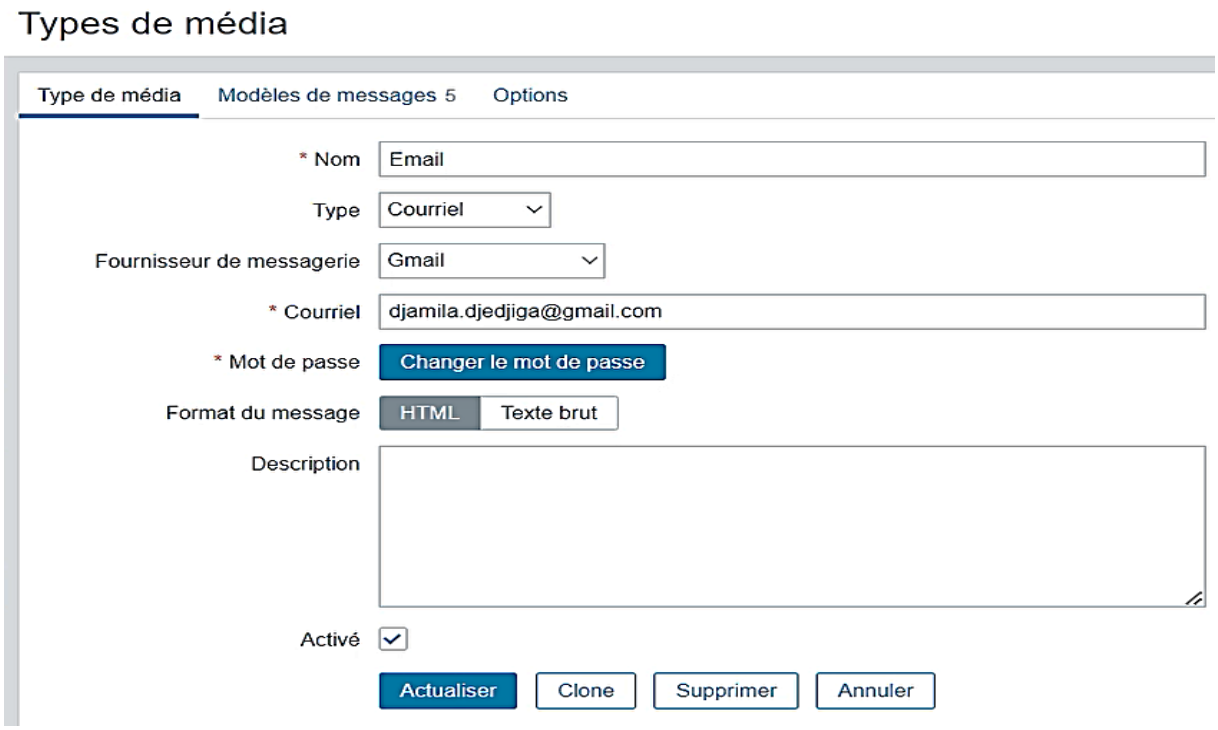


Figure 125 : Configuration l'e-mail comme type de média

Enfin, pour tester si un type de média, par exemple e-mail une fois configuré, fonctionne correctement, un message de réussite ou d'échec du test s'affiche dans la fenêtre comme illustré dans la figure ci-dessous ;

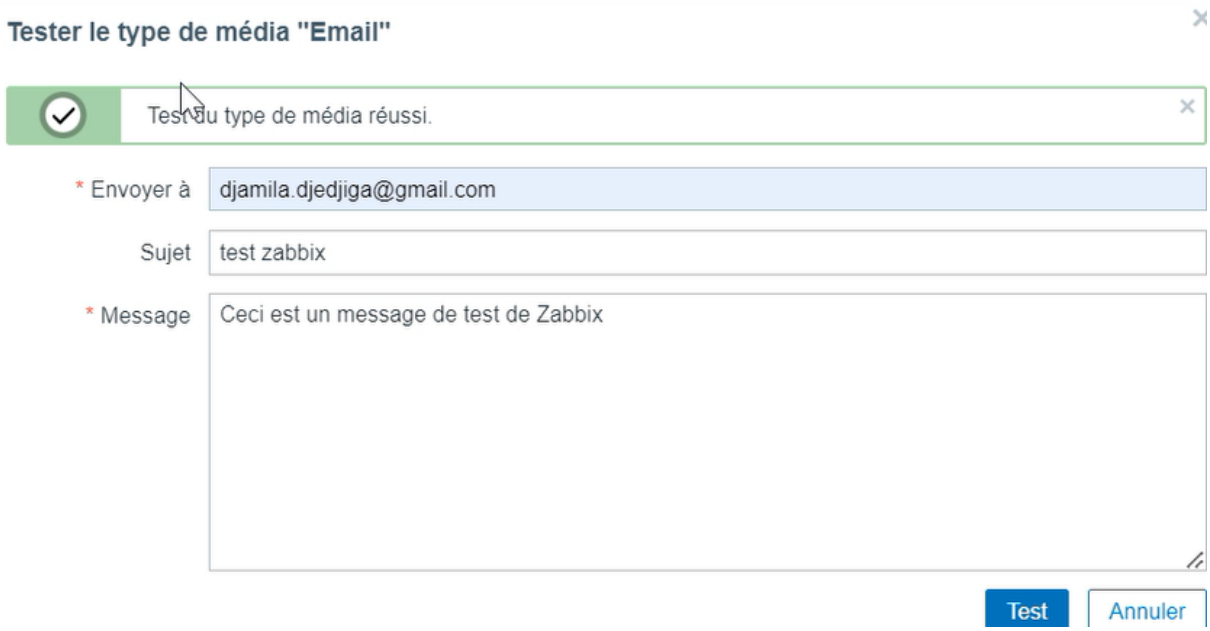


Figure 126 : Capture d'écran du test d'envoi d'e-mail depuis Zabbix

Pour configurer les groupes d'utilisateurs afin qu'ils puissent recevoir les alertes, nous allons suivre les étapes présentées dans les figures suivantes : D'abord nous commençons par accéder à la barre de navigation de Zabbix. Ensuite, nous cliquons sur l'option "Utilisateurs". Dans le menu déroulant qui apparaît, nous sélectionnons "utilisateurs". Une liste des utilisateurs disponibles s'affiche. Nous recherchons et cliquons sur le groupe spécifique auquel nous souhaitons apporter des modifications, dans notre cas c'est "Zabbix administrateur". En cliquant sur ce groupe, nous accédons à la page de configuration du groupe d'utilisateurs.

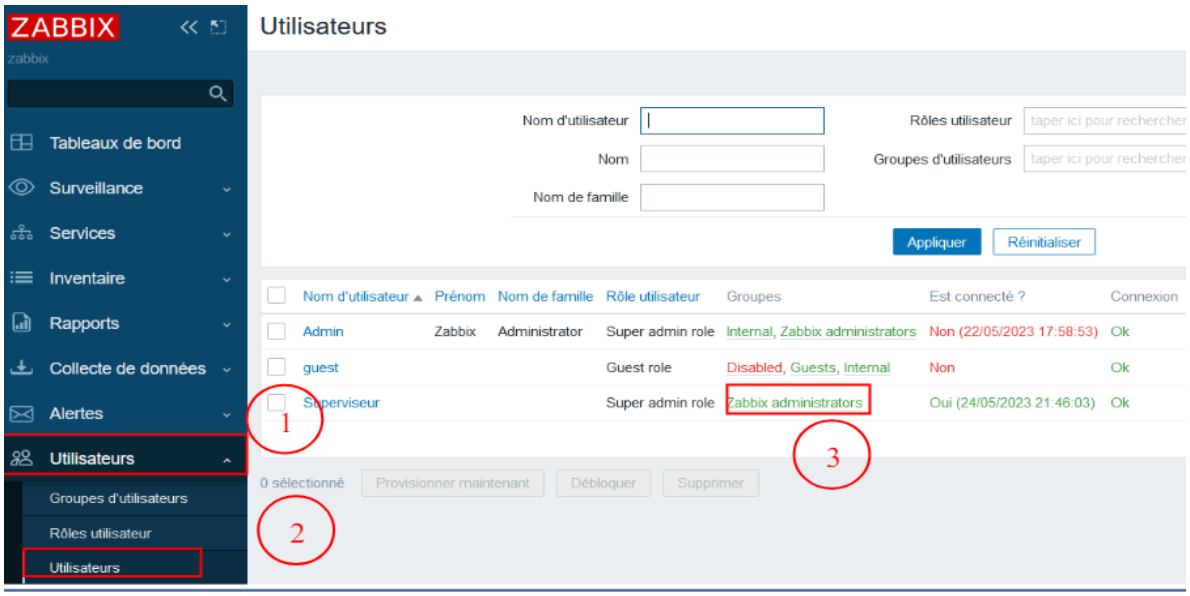


Figure 127 : Accéder au groupe Zabbix administrateurs

Une fois que nous accédons à la page de configuration du groupe d'utilisateurs, nous naviguons vers l'onglet "Média". Là, nous cliquons sur le bouton "Ajouter" pour ajouter un nouveau média. Cela nous redirige vers la page de configuration du média. Nous sélectionnons le type de média approprié pour notre configuration, à savoir "Gmail". Ensuite, nous saisissons les adresses e-mail du groupe "Zabbix administrateur" dans les champs correspondants. Nous cocherons également la case "Activer" pour activer ce média. Une fois que nous avons rempli toutes les informations nécessaires, nous cliquons sur le bouton "Ajouter" pour ajouter le média. Ensuite, nous pouvons cliquer sur le bouton "Actualiser" pour mettre à jour les paramètres.

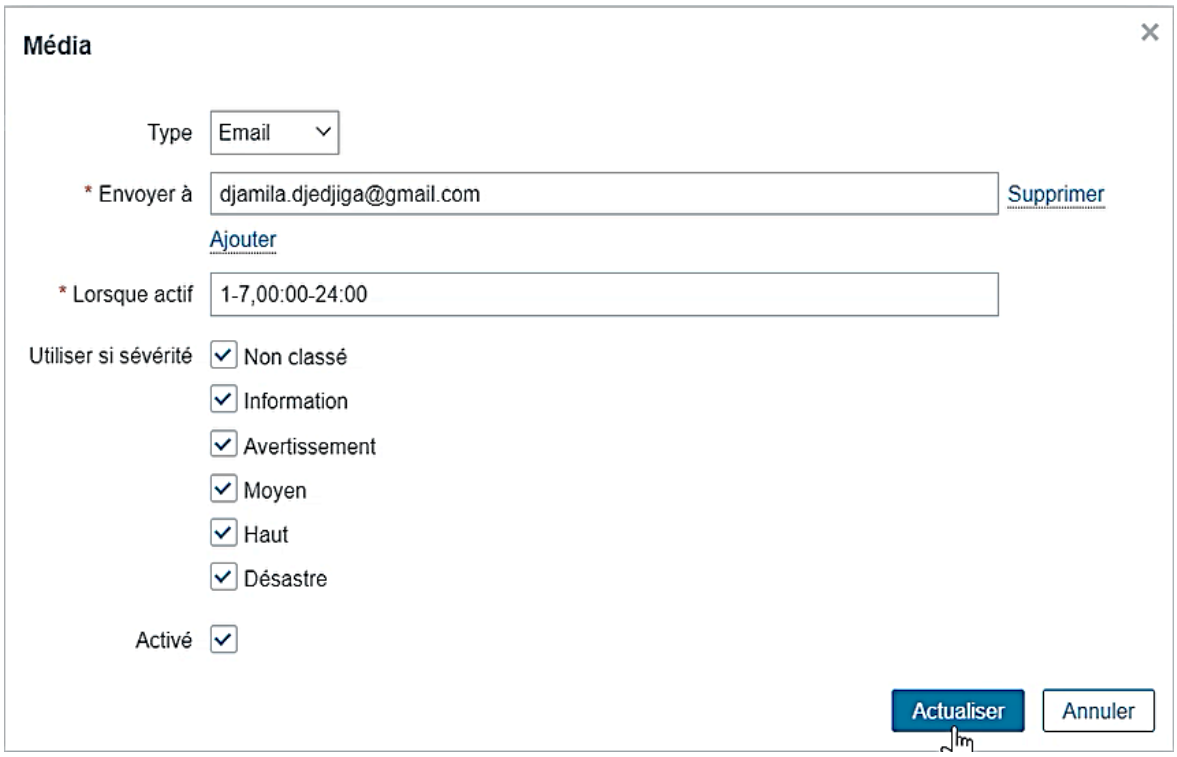


Figure 128 : Configuration du Média

Après avoir effectué la configuration du média pour le groupe d'utilisateurs "Zabbix administrateur", nous pouvons observer dans la figure ci-dessous que le média a été correctement configuré et activé. Cela signifie que les utilisateurs appartenant à ce groupe seront en mesure de recevoir les alertes via ce média spécifié.

Figure 129 : Confirmation de l'activation du média pour le groupe Zabbix administrateur

5.5. Exécution des tests de surveillance avec Zabbix

Pour valider notre configuration et s'assurer du bon fonctionnement de Zabbix, nous allons effectuer une série de tests sur les hôtes que nous avons ajoutés. Ensuite, nous allons consulter les résultats de ces tests à travers : Gmail.

- **Tester Zabbix à travers de routeur**

Pour tester la surveillance d'un routeur sur Zabbix, vous pouvez simuler une panne en utilisant GNS3. Lorsque le routeur est éteint dans GNS3, Zabbix détectera ce problème et affichera probablement une alerte en rouge pour signaler une indisponibilité.

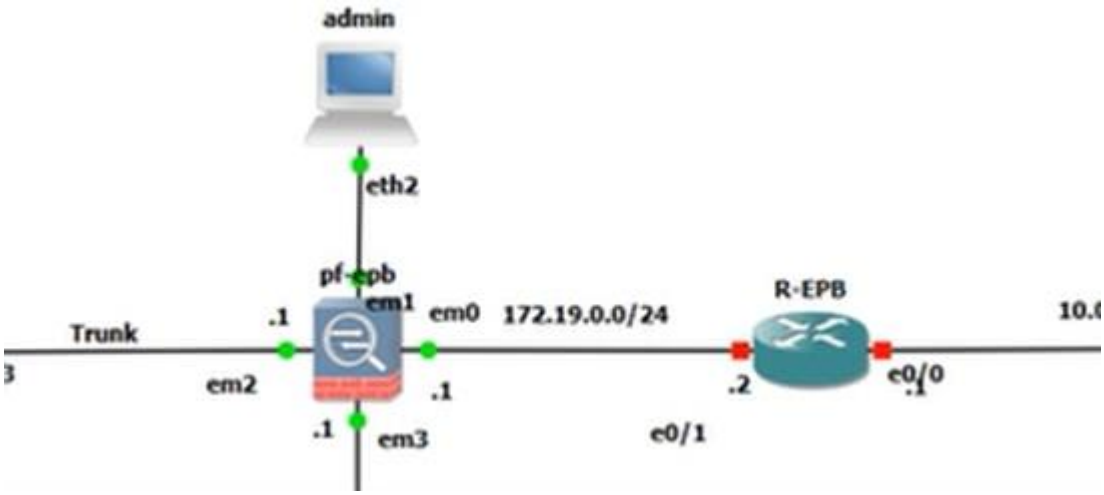


Figure 130 : Eteindre le routeur R-EPB

Figure 131 : Problème t de routeur sur zabbix

- **Les alertes affichés sur le tableau de bord :**

Lorsque le routeur est éteint, cela peut entraîner un problème de connectivité détecté par Zabbix à travers la surveillance du ping ICMP. Zabbix envoie régulièrement des requêtes ICMP (ping) au routeur pour vérifier sa disponibilité.

Si le routeur est hors ligne ou non accessible, Zabbix ne recevra pas de réponse aux requêtes ICMP. Dans ce cas, Zabbix génère une alerte sur le tableau de bord pour signaler que le ping ICMP a échoué, indiquant ainsi un problème potentiel avec la connectivité ou l'état du routeur. Cette alerte permet aux administrateurs réseau d'être rapidement informés de la situation, facilitant ainsi une intervention immédiate pour résoudre le problème et restaurer la connectivité réseau normale.

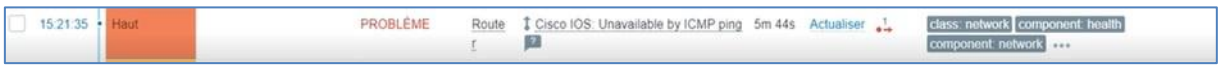


Figure 132 : Alerte affiché sur tableau de bord

- **Les alertes reçus par E-mail (notification) :**

Les administrateurs système reçoivent des emails d'alerte de Zabbix comme la figure ci-dessous montre ;

Figure 133 : Alerte envoyées par e-mail

Conclusion

La supervision joue un rôle crucial dans la gestion efficace de notre environnement informatique en nous permettant de surveiller en temps réel les performances, la disponibilité et la sécurité de nos systèmes critiques. Dans ce chapitre, nous avons présente les éléments clés de notre partie pratique. Ou nous avons décrire les étapes d'installation et de configuration de déférentes processus suivi, Par la suite nous aborderons également en détail notre exploration de la supervision à l'aide de l'outil Zabbix.

Conclusion Générale

En conclusion, notre mémoire met en évidence l'importance cruciale d'un système de supervision efficace pour les administrateurs dans la gestion de leur réseau. Notre projet nous a permis de définir l'objectif de la supervision et son influence sur le système informatique et sur le fonctionnement performant des entreprises.

À mesure que le nombre d'équipements et de services informatiques augmente, les tâches des administrateurs deviennent de plus en plus complexes, ce qui entraîne des difficultés à les assurer, aboutissant ainsi à une perte de temps et à un travail incomplet.

Notre projet consistait à mettre en place un outil de supervision système et réseau. Les grandes entreprises disposent d'un vaste parc matériel qui doit être géré par les administrateurs. Cette gestion devient ardue lorsque les détails sur l'ensemble du parc informatique ne sont pas disponibles en temps réel. C'est là qu'un logiciel de supervision efficace intervient en simplifiant le travail de l'administrateur, le réduisant à des vérifications simples ou à des actions correctives pour résoudre les problèmes. Une surveillance continue permet à l'entreprise d'éviter les erreurs et les pannes, réduisant ainsi les interruptions qui pourraient compromettre ses opérations et sa réputation.

Notre contribution a donc consisté à fournir toutes les étapes nécessaires à mettre en place d'un service de supervision Zabbix.

Dans notre étude initiale, nous avons d'abord effectué une étude sur les réseaux informatiques et de la supervision, en analysant les outils disponibles et en examinant l'architecture des entreprises. Nous avons identifié les défis majeurs rencontrés par les administrateurs réseau dans la gestion de ces environnements complexes.

Dans la partie réalisation, nous avons mis en œuvre notre projet en configurant l'outil Zabbix sur les différentes machines de l'entreprise. Cette mise en œuvre nous a permis de surveiller efficacement le réseau et les systèmes, tout en assurant une réactivité rapide grâce aux alertes par e-mail en cas de défaillance.

Enfin, on ce qui concerne l'implémentation pratique et selon les experts de l'entreprise, le travail réalisé et très intéressant et ils ont déjà entamé l'installation des différents outils matériels et logiciels pour une meilleure supervision de leur réseau.

Références bibliographiques

1. Présentation de l'Entreprise Portuaire de Béjaïa. *Documents internes de l'EPB.*

2. Salvatori. *Initiation aux réseaux.* Éditions Eyrolles. p. 448, 2001.

3. G.pujolle. *Les reseaux* . EYROLLES,Paris : 8 éme édition , 2014.

4. https: //www.samomoi.com/reseauxinformatiques/modele_DOD.php . [Citation : 07 juin 2022.]

5. Réseau d'entreprise. *https: //cours-informaique-gratuit.fr.*

6. ACISSIé. *sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre.* s.l. : 3e édition, 2012.

7. Kanneganti, R. *« sécurité des réseaux ».* 1ere édition. 1 juin 2008.

8. Pirio, Mikael. *Installation, administration, et sécurisation.* France : s.n., Janvier 2004.

9. M, Bruno. *la sécurité informatique CERAM, << Fondamentaux des sciences de l'information >>.*

10. GABES, J. Nagios 3 pour la supervision et la métrologie : D´eploiement. 2009.

11. CABANTOUS, T. *Les réseaux informatiques : informatiques Guide pratique pour l'administration et la supervision.* paris , 2019.

12. *https: //philpetitpa.pagesperso orange.fr/adminsupervis/SNMP.pdf.*

13. Qu'est-ce que Zabbix? https: //www.zabbix.com.

14. *Centreon Community'GUIDE PRATIQUE de la Communauté Centreon'. PDF*

.

Etude et mise en place d'un serveur supervision zabbix. Cas EPB

Résume

Ce mémoire traite de la mise en place d'un système de supervision pour l'entreprise EPB. L'objectif principal était de proposé une architecture réseau pour EPB. Nous avons d'abord étudié le réseau actuel, ce qui nous a permis d'identifier les faiblesses et de proposer des solutions pour concevoir une nouvelle architecture. La configuration du réseau proposé a été réalisée à l'aide du simulateur GNS3.

Pour la supervision du réseau, nous avons déployé et configuré une station de surveillance Zabbix. Cette station est chargée d'alerter l'administrateur en cas de pannes ou de surcharges sur le réseau. Des agents Zabbix et le protocole SNMP ont été utilisés pour surveiller les machines sous Linux et Windows. Toutes les configurations ont été effectuées sur des machines virtuelles VMware utilisant le système d'exploitation Linux, garantissant une surveillance efficace et en temps réel. Toutes les étapes d'installation, de configuration et de test sont présentées et expliquées dans ce mémoire.

Mots clés : Supervision, GNS3, VMware, Zabbix, Agent-Zabbix, SNMP.

Abstract

This thesis addresses the implementation of a supervision system for the company EPB. The main objective was to propose a network architecture for EPB. We first studied the current network, which allowed us to identify weaknesses and propose solutions to design a new architecture. The configuration of the proposed network was carried out using the GNS3 simulator.

For network supervision, we deployed and configured a Zabbix monitoring station. This station is responsible for alerting the administrator in case of network failures or overloads. Zabbix agents and the SNMP protocol were used to monitor machines running Linux and Windows. All configurations were performed on VMware virtual machines using the Linux operating system, ensuring effective and real-time monitoring. All installation, configuration, and testing steps are presented and explained in this thesis.

Keywords: Supervision, GNS3, VMware, Zabbix, SNMP, Zabbix Agent.