

Projet de Fin d'Études

En vue de l'obtention du Diplôme de Licence en Informatique

Option : Administration Sécurité des Réseaux & Systèmes (ASRS)

**THÈME :**  
**ÉTUDE ET MISE EN PLACE D'UN OUTIL DE SUPERVISION OPEN SOURCE  
ZABBIX AVEC NOTIFICATION PAR MAIL : CAS D'ALBIDEYNET**

**Réalisé par :**

**ADAM MAHAMADENE LOUGOUMA**

**Sous la direction de :**

**M. MAHAMAT ISMAEL ABDELKERIM (encadrant)**

**M.GISCARD SIBEFO (Maître de stage)**

**Jury :**

**M. BRAHIM MOUSSA BECHIR (Président)**

**M. AHMAT BADAWI HAMIT (Rapporteur)**

Année académique : **2022-2023**

## **DEDICACE**

Au fond de mon cœur, je dédie ce travail à mon oncle paternel **BICHARA LOUGOUMA** pour son soutien inconditionnel, ses encouragements, pour m'avoir permis de réaliser mes études dans les meilleures conditions.

Pour m'avoir soutenu, accompagné et surtout encouragé tout au long de mon cursus.

## REMERCIEMENTS

Je souhaiterai d'abord remercier **Allah** le tout puissant de m'avoir donné la force, le courage et la patience de finir ce modeste travail.

Je remercie également tous les administrateurs de **l'ENASTIC** qui étaient et sont toujours debout et actifs pour la bonne marche de cette institution.

Je remercie également mes professeurs pour la qualité de l'enseignement qu'ils m'ont prodigué au cours de ces trois années passées à l'Ecole Nationale Supérieure des Technologies de l'Information et de la Communication (**ENASTIC**).

Je tiens à remercier particulièrement notre chef d'antenne **M.VOUNDAI VALAMDOU MAHAMAT**, le comptable, le chargé de matériel et toute l'équipe technique de la restauration pour l'effort fourni et leurs orientations.

Je remercie particulièrement mon Directeur de Mémoire **M. MAHAMAT ISMAEL ABDELKERIM** et mon Maître de Stage **M.GISCARD SIBEFO** pour leur précieuse assistance, leur disponibilité et l'intérêt qu'ils ont manifesté pour ce travail.

Mes remerciements à l'équipe d'**ALBIDEYNET** pour l'accueil chaleureux qui m'a été réservé, le temps que chacun de ses membres m'a accordé, et plus globalement pour toutes les informations que chacun m'a apporté.

Je remercie également mon cousin **OUMAR ALI FADOUL** pour ces précieux conseils et orientations contribuant à ce modeste travail.

Un grand merci à ma mère et mon père pour l'amour que vous portez, de vos conseils qui me guident et me donnent la force d'avancer. Longue et heureuse vie à vous **Incha'Allah**. Merci à mes frères et sœurs. Mes remerciements vont également à l'endroit de mes proches, de tous ceux qui ont contribué à ce travail.

Je tiens à remercier enfin l'ensemble de mes camarades de **l'ENASTIC D'AMDJARASS**, plus particulièrement ceux de L'Administration Sécurité des Réseaux & Systèmes (ASRS).

# TABLE DES MATIERES

DEDICACE.....	i
REMERCIEMENTS .....	ii
RESUME.....	vi
ABSTRACT .....	vii
LISTE DES FIGURES.....	viii
LISTE DES TABLEAUX.....	ix
SIGLES & ABREVIATIONS.....	x
Introduction Générale.....	1
Chapitre 1 : PRESENTATION DE LA STRUCTURE D'ACCUEIL : ALBIDEYNET .....	2
1.1 Introduction .....	3
1.2 Présentation d'Albideynet.....	3
1.3 Organigramme d'AlbideyNet.....	3
1.4 Les Missions d'AlbideyNet.....	4
1.5 Les visions d'AlbideyNet.....	5
1.6 Les Services de base.....	5
1.6.1 Fourniture d'accès Internet & Services à valeur ajoutée.....	5
1.7 Étude de l'existant.....	6
1.8 Critique de l'existant .....	6
1.9 Solution proposée.....	7
1.10 Architecture proposée .....	8
1.11 Conclusion.....	9
Chapitre 2 : PRINCIPE ET CONCEPT DE LA SUPERVISION .....	10
2.1 Introduction .....	11
2.2 Définition de la supervision .....	11
2.3 Principes de fonctionnement de la supervision.....	11
2.3.1 Fonctionnalités de la supervision .....	11
2.3.2 Principe de la supervision .....	12
2.4 Protocole SNMP.....	13
2.4.1 Présentation .....	13
2.4.2 Fonctionnement.....	14
2.4.2.1 Les agents.....	14
2.4.2.2 La MIB .....	14
2.4.2.3 Les commandes SNMP .....	15
2.5 Les méthodes de supervision .....	16
2.5.1 Mode actif .....	16

2.5.2 Mode passif .....	16
2.6 Solutions de la supervision.....	17
2.6.1 Solutions propriétaires .....	17
2.6.1.1 HP OpenView .....	18
2.6.1.2 IBM Tivoli Netview .....	18
2.6.2 Solutions Open Source .....	19
2.6.2.1 Zabbix .....	19
2.6.2.2 Nagios .....	21
2.6.2.3 Centreon .....	22
2.7 Comparaison entre open source ou propriétaire.....	23
2.7.1 Propriétaire.....	24
2.7.2 Open Source .....	24
2.8 Pourquoi choisir des solutions open sources ?.....	24
2.8.1 Contrainte des solutions open source .....	24
2.9 Tableaux comparatif entre les différents outils de supervision.....	25
2.10 La solution retenue : ZABBIX.....	26
2.11 Conclusion.....	27
Chapitre 3 : PRESENTATION DE L’OUTIL DE SUPERVISION ZABBIX.....	28
3.1 Introduction .....	29
3.2 Présentation de Zabbix .....	29
3.3 Qu'offre ZABBIX.....	29
3.4 Principe de fonctionnement de ZABBIX.....	30
3.4.1 Les composants de ZABBIX .....	30
3.4.1.1 Zabbix Server .....	30
3.4.1.2 ZABBIX Frontend .....	30
3.4.1.3 Zabbix Proxy .....	30
3.4.1.4 Zabbix Agent.....	31
3.5 Les fonctionnalités de Zabbix .....	31
3.6 Installation de Zabbix.....	32
3.7 Conclusion.....	42
Chapitre 4 : PROPOSITION DE LA SOLUTION ET MISE EN OEUVRE .....	43
4.1 Introduction .....	44
4.2 Environnement de travail .....	44
4.2.1 Environnement matériels .....	44
4.2.2 Environnement logiciels.....	44
4.3 Configurations de zabbix .....	45

4.3.1 Ajout d'hôte via agent ZABBIX .....	45
4.3.2 Ajout d'hôte via SNMP .....	45
4.3.3 Ajout d'un routeur MIKROTIK.....	47
4.4 Notification via email.....	50
4.4.1 Installation de postfixe .....	51
4.4.2 Configuration de postfixe.....	51
4.4.3 Teste de notification .....	55
4.5 Conclusion.....	56
Conclusion Générale .....	57
Bibliographie.....	58
ANNEXES .....	60
ANNEXES A : Installation Ubuntu 22.04 (jammy) .....	60
ANNEXE B : installation Vmware .....	65

## **RESUME**

Dans le monde de l'Internet et des réseaux, la sécurité est très importante. C'est pourquoi, en plus de mettre tous les mécanismes de sécurité pour une protection d'un réseau, pouvoir superviser le réseau est aussi très important. Elle nous permet de pouvoir surveiller des machines, des routeurs, des switches, des pare-feu, etc. Ainsi nous pouvons savoir, pour un réseau, l'état de chaque équipement et leurs services à temps réel. La supervision est possible grâce à des outils ou logiciels qui facilitent la surveillance des équipements et des services. Ces outils de supervision ont des interfaces Web pour visualiser ce que nous voulons superviser. C'est en ce sens que nous avons étudié des logiciels de supervision et ainsi que les protocoles utilisés par les outils pour leur faciliter les tâches. Nous avons choisi par la suite de travailler avec Zabbix, plus particulièrement Zabbix 6.4 (dernière version), qui est l'un des outils de supervision les plus utilisés dans le marché de l'entreprise actuellement et en même temps open source. Zabbix nous a permis de superviser notre réseau et peut superviser n'importe quel autre réseau d'entreprise. En plus des services, Zabbix peut alerter automatiquement l'administrateur en cas de dysfonctionnement via email, SMS, etc.

Mots clés : zabbix, supervision, notification, sécurité.

## **ABSTRACT**

In the world of the Internet and networks, security is very important. This is why, in addition to putting all the security mechanisms in place to protect a network, being able to supervise the network is also very important. It allows us to monitor machines, routers, switches, firewalls, etc. Thus we can know, for a network, the state of each piece of equipment and their services in real time. Supervision is possible thanks to tools or software that facilitate the monitoring of equipment and services. These monitoring tools have web interfaces to visualize what we want to monitor. It is in this sense that we studied supervision software and the protocols used by the tools to facilitate their tasks. We subsequently chose to work with Zabbix, more specifically Zabbix 6.4 (latest version), which is one of the most used monitoring tools in the enterprise market currently and at the same time open source. Zabbix allowed us to monitor our network and can monitor any other corporate network. In addition to the services, Zabbix can automatically alert the administrator in the event of a malfunction via email or SMS.

Key words : zabbix, supervision, notification, Security.



## LISTE DES FIGURES

Figure 1. 1 : Organigramme d'Albideynet.....	4
Figure 1. 2 : Ecran de supervision d'Albideynet .....	7
Figure 1. 3 : Architecture Proposée.....	8
Figure 2. 1 : Fonctionnement de SNMP.....	14
Figure 2. 2 : Les requêtes SNMP. ....	15
Figure 2. 3 : Mode Actif.....	16
Figure 2. 4 : Mode passif.....	17
Figure 2. 5 : Tableau de bord de Zabbix .....	21
Figure 2. 6 : Tableau de bord de Nagios .....	22
Figure 2. 7 : Tableau de bord de Centreon.....	23
Figure 3. 1 : Architecture de Zabbix .....	31
Figure 3. 2 : Les fonctionnalités de Zabbix.....	32
Figure 3. 3 : Téléchargement de Zabbix .....	33
Figure 3. 4 : Interface de navigateur de Firefox.....	36
Figure 3. 5 : Page de Bienvenue et choix de langues(Français) de Zabbix .....	37
Figure 3. 6 : Vérification des Prérequis .....	37
Figure 3. 7 : Connexion à la base de données .....	38
Figure 3. 8 : Changement de Paramètres .....	39
Figure 3. 9 : Résumé de Pré-Installation .....	40
Figure 3. 10 : Fin de l'installation avec succès.....	40
Figure 3. 11 : Page d'Authentification de Zabbix .....	41
Figure 3. 12 Page d'accueil de Zabbix .....	41
Figure 4. 1 : Installation de l'agent zabbix. ....	45
Figure 4. 2 : Choix de services SNMP .....	46
Figure 4. 3 : Insertion des informations SNMP .....	46
Figure 4. 4 : Interface de Winbox .....	47
Figure 4. 5 : Configuration de service SNMP dans Winbox.....	48
Figure 4. 6 : Configuration d'un hôte. ....	49
Figure 4. 7 : Ajout du routeur mikrotik.....	49
Figure 4. 8 : Vu des hôtes superviser (Zabbix Server, SNMP, agent) .....	50
Figure 4. 9 : Paramètre Google .....	52
Figure 4. 10 : Paramètres de messagerie Zabbix pour le serveur de messagerie Gmail .....	53
Figure 4. 11 : Image montrant comment tester le type de média « Email » via l'interface Zabbix...	54
Figure 4. 12 : Alerte d'indisponibilité d'une machine cliente.....	55

## LISTE DES TABLEAUX

Tableau 2. 1 Description des requêtes de la figure 2.2 .....	15
Tableau 2. 2 : Tableau comparatif des outils de supervision .....	25
Tableau 4. 1 : Environnement matériels .....	44
Tableau 4. 2 : environnement logiciels .....	44

## SIGLES & ABBREVIATIONS

- APT** : Advanced packaging tool
- BDD** : Base De Données
- BSD** : Berkeley Software Distribution
- CPU** : Central Processing Unit
- DB** : data base
- DHCP** : Dynamic Host Configuration Protocol
- DMZ** : Demilitarized zone
- DNS** : Domain Name System
- ENASTIC** : Ecole Nationale Supérieure des Technologies de l'Information et de la Communication
- FAI** : fournisseur d'accès à l'internet
- FTP** : File Transfert Protocol
- GNU** : GNU's not Unix
- HP-UX** : Hewlett Packard UniX
- HTTP** : hyper text Transfer Protocol
- ICMP** : internet Control Message Protocol
- IETF** : Internet Engineering Task Force
- IMAP** : Internet Message
- IP** : Internet Protocol
- IPMI** : intelligent Platform Management Interface
- IT** : Infrastructure Informatique
- JMX** : Java Management Extensions
- LTE** : long term Evolution
- MIB** : Management Information Base
- NNTP** : Network News Transfer Protocol
- OID** : Object Identifier
- PHP** : Hypertext Preprocessor
- PING** : Packet Internet Groper
- PoE** : Power over Ethernet
- POP3** : Post Office Protocol
- RAM** : random access memory
- SFP** : Small Form-Factor Pluggable
- SGBD** : système de gestion de base de données
- SMS** : Short Message Service

**SMTP** : simple mail Transfer Protocol

**SNMP**: Simple Network Management Protocol

**SSH** : Secure Shell

**SSL** : Secure Sockets Layer

**TCP**: Transmission Control Protocol

**TIC** : technologies de l'information et de la communication

**TLS** : Transport Layer Security

**UDP** : User Datagram Protocol

**USB** : Universal Serial Bus

**UTC** : Universal Time Coordinated

**VPN** : Virtual Private Network

**VSAT** : very Small Aperture Terminal

## **Introduction Générale**

Actuellement, les systèmes informatiques dans les entreprises deviennent de plus en plus importants. Le besoin de maintenance et de gestion de ces systèmes est rapidement devenu une priorité, d'autant plus qu'une panne ou une perte au niveau de ce système pourrait parfois avoir des conséquences catastrophiques.

Afin de minimiser le nombre de ces pertes, une surveillance et un contrôle permanent s'avèrent indispensables. La notion de « supervision informatique » est apparue et est devenue une tâche vitale pour tout système informatique ; c'est pourquoi les administrateurs systèmes et réseaux font appel à des logiciels de surveillance et de supervision. Ces logiciels vérifient l'état du système ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue globale en temps réel sur l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi alerté (par email, par SMS, etc.) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits, sans que les utilisateurs du système en question soient affectés ou se rendent compte des problèmes survenus.

Vu que le système informatique est au cœur des activités d'entreprise, sa maîtrise devient primordiale, puisqu'il doit fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées. D'autre part, les problèmes liés au système informatique 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 et même salir l'image de l'entreprise vis-à-vis des clients.

À cet effet, nous avons effectué un stage de deux mois à ALBIDEYNET. Notre objectif consiste à mettre en place une console d'administration réseaux dans le but de garantir le bon fonctionnement de leur infrastructure réseau.

De ce fait, nous avons organisé notre plan de projet en quatre (04) chapitres :

- Le premier chapitre est consacré à la structure d'accueil ;
- Le deuxième chapitre présente un aperçu général de la supervision ;
- Le troisième chapitre est consacré à la présentation de l'outil de supervision ZABBIX ;
- Le quatrième chapitre est consacré à la proposition de la solution et la mise en œuvre de ZABBIX.

Enfin, nous allons finir par une conclusion générale.

# **Chapitre 1 : PRESENTATION DE LA STRUCTURE D'ACCUEIL : ALBIDEYNET**

## 1.1 Introduction

Pour bien aborder le sujet, nous avons commencé dans cette partie par la présentation et l'organisation de la structure d'accueil. Dans ce chapitre, nous avons énuméré les missions et visions ainsi que les services de cette dernière. Pour finir, nous avons fait une conclusion.

## 1.2 Présentation d'Albideynet

AlbideyNet est une filiale d'Albidey Group Investissement qui est la représentation au Tchad de la multinationale Albidey Management Limited basée à Londres, Royaume-Uni. Elle a des branches au Soudan, au Sud Soudan, en Éthiopie et au Royaume-Uni. AlbideyNet est une société de technologie de pointe qui fournit des solutions de niveau entreprise à un prix très compétitif pour le gouvernement, les entreprises et les particuliers. AlbideyNet a été créée en 2007 comme une petite entreprise, mais a depuis gravité des échelons pour devenir un chef de file dans la fourniture d'Internet à haut débit et de services à valeur ajoutée au Tchad.

Elle possède deux licences (une première licence en tant que FAI obtenue en 2007 et une autre licence 4G obtenue en 2016). Depuis sa création, elle a mené à bien de nombreux projets dans ce domaine à travers tout le pays. Cette société, a pour slogan « Internet pour tous ! »[1].

## 1.3 Organigramme d'AlbideyNet

Pour assurer son bon fonctionnement et atteindre ses objectifs : AlbideyNet est structuré comme suit :

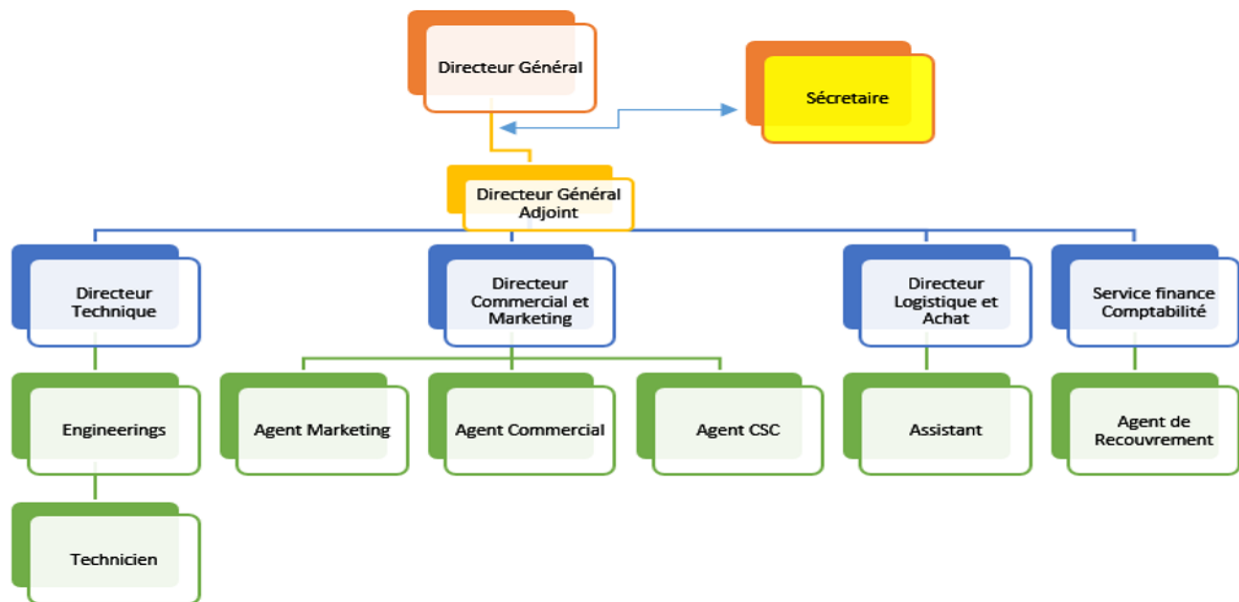
**Direction générale** : Administration/Ressources Humaines ;

**Direction Commerciale et Marketing** : vente/marketing/communication clientèle ;

**Direction logistique** : Achat et logistique ;

**Direction technique** : gestion, installation, maintenance du réseau, dépannage client, étude, coordination des activités et solution technique ;

**Service finance et comptabilité** : facturation, comptabilité et recouvrement [1].



**Figure 1. 1 : Organigramme d'Albideynet**

#### 1.4 Les Missions d’AlbideyNet

La croyance vers l’avenir et ils ont une grande vision pour les innovations et les technologies, leurs produits et services sont toujours en constante évolution pour répondre aux besoins de leurs clients.

Répondant à notre foi en l'avenir, AlbideyNet établit les principes suivants :

- Connaissance (Connaître tout et bien connaître) ;
- Service (Connaître les besoins de nos clients et les satisfaire) ;
- Crédibilité (Comprendre, réaliser nos engagements et être digne de confiance).

En outre, AlbideyNet fournit des solutions Internet et informatiques pour les entreprises clientes à des prix très concurrentiels. Nos services Internet et informatiques fonctionnent selon trois (03) principes :

1. Stabilité : Fournir des services Internet et des solutions informatiques à travers un système fiable et un réseau stable qui satisfait aux normes de sécurité ;
2. Flexibilité : Le développement de divers services et de solutions qui sont flexibles, pouvant être personnalisés pour répondre aux besoins opérationnels et sans limites, de tous nos clients d'entreprise ;
3. Dévouement : Se consacrer à fournir des services après-vente de qualité, des consultations et une résolution de problèmes rapide par une équipe d'experts qui sont disponibles 24 heures sur 24.



## **1.5 Les visions d'AlbideyNet**

En recherche constante d'innovations technologiques qui fourniront des performances, des solutions d'amélioration pour nos clients, et en luttant pour les plus hauts standards de service, nous allons continuer à promouvoir la fourniture d'un service Internet stable et des solutions de service au Tchad, en particulier dans les services destinés aux entreprises. Nous :

- Fournissons à nos clients des services abordables, évolutifs et pérennes avec des technologies de pointe et des solutions sans fil pour le haut débit ;
- Fournissons des solutions à haut débit et de haute qualité aux domiciles, aux bureaux, et sur les places publiques ;
- Assurons une connectivité fiable et robuste pour les marchés verticaux pour supporter leurs applications critiques ;
- Travaillons pour réduire la fracture numérique en couvrant les zones encore mal desservies et non desservies à travers le Tchad ;
- Permettre le e-commerce, la collaboration et l'accès illimité à l'information [1].

## **1.6 Les Services de base**

AlbideyNet offre un large éventail de services depuis la fourniture d'accès internet, de support informatique, des solutions de réseaux et télécommunications d'entreprise aux systèmes de sécurité d'entreprise.

### **1.6.1 Fourniture d'accès Internet & Services à valeur ajoutée**

Albideynet offre l'internet via les technologies suivantes :

Fibre optique ;

LTE 4G ;

VSAT ;

Wi-Fi ;

Microwave.

- Télécommunications : Équipements & Câblage ;
- Intégrateur de solutions informatiques ;
- Service & Support sur site ;
- Services Réseaux ;

- Hébergement de Serveur ;
- Solutions et systèmes de Téléphonie d'entreprise ;
- Installation et maintenance des systèmes de vidéosurveillance.

### **1.7 Étude de l'existant**

Après deux mois passés au sein d'Albideynet, nous avons vu que l'entreprise dispose d'un certains nombres d'équipements qui sont entre autres :

- Les routeurs ;
- Les commutateurs ;
- Un pare-feu matériel (FORTIGATE) ;
- Les imprimantes ;
- Les points d'accès ;
- Un central téléphonique de marque Panasonic ;

On a remarqué que le réseau de l'entreprise est supervisé à l'aide d'un outil de monitoring ZABBIX 4.2.

### **1.8 Critique de l'existant**

Après avoir mené un audit au sein de l'entreprise, nous avons relevé les problèmes suivants :

- l'outil de supervision utilisé est Zabbix 4.2 qui est une version ancienne et qui ne répond pas à certaines fonctionnalités telles que notifications par mail ;
- Pas d'alerte en cas de panne ou problème de fonctionnement sur le réseau ;
- Plus le nombre des équipements et des services augmente, plus il est difficile de détecter la défaillance des équipements (charge CPU, état mémoire, surcharge du disque...) ;
- Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des clients, ce qui rend les clients mécontents ;
- L'administrateur trouve des difficultés à vérifier la disponibilité des équipements, surtout pour les locaux distants ;
- Le diagnostic des pannes nécessite énormément de temps ;
- La taille de l'écran sur laquelle est déployé cet outil est défectueux et de petite taille. Comme le montre la figure 1.2.

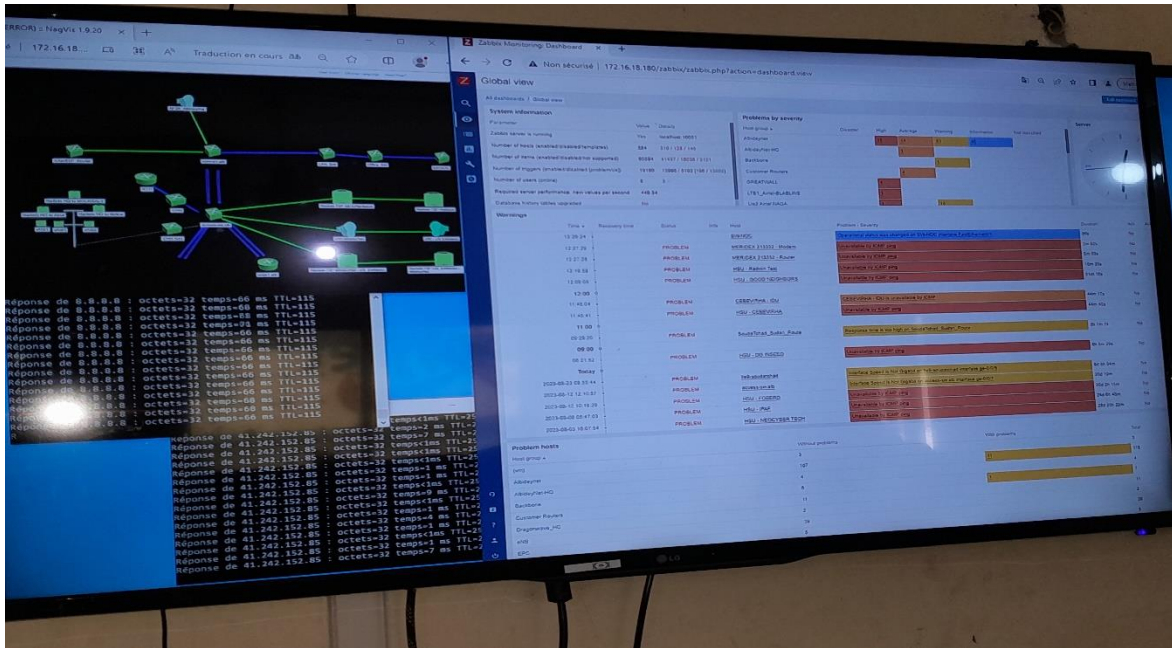


Figure 1. 2 : Ecran de supervision d'Albideynet

### 1.9 Solution proposée

Vu les inconvénients cités précédemment, nous proposons la mise en place d'un outil de supervision système et réseau open source (ZABBIX 6.4 dernière version) qui assure les tâches suivantes :

- Déclencher des alertes lors de la détection des pannes ;
- Offrir des renseignements supplémentaires : charge CPU, espace disque, mémoire disponible, etc ;
- Offrir à l'administrateur la possibilité de réagir le plus rapidement possible face aux pannes ;
- Avoir une interface graphique compréhensible pour l'interaction entre l'utilisateur et le logiciel ;
- Garantir la disponibilité des services ;
- Diagnostiquer l'état du réseau ;
- Avoir un grand écran mural pour la supervision.

### 1.10 Architecture proposée

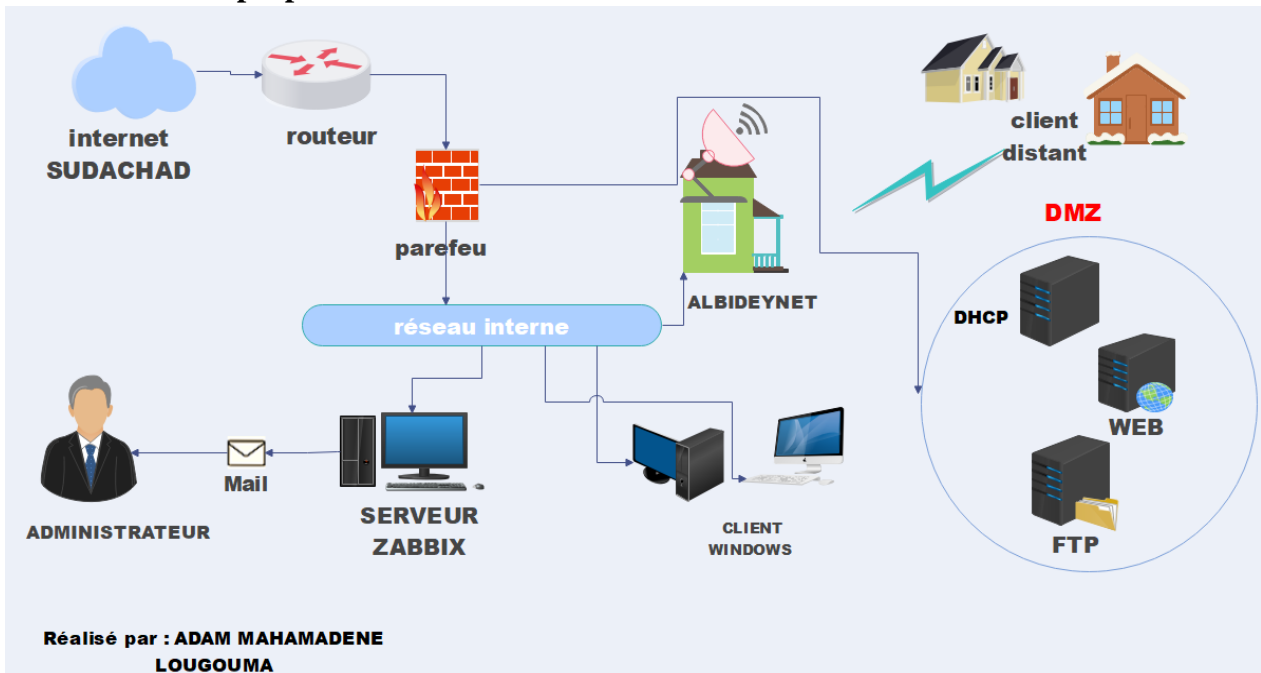


Figure 1. 3 : Architecture Proposée

L'objectif de cette architecture est donc de trouver une solution optimale pour la supervision de ses équipements, d'offrir la possibilité de devenir proactif face aux problèmes et de pouvoir détecter et interpréter les causes et origines des problèmes rencontrés et d'alerter automatiquement l'administrateur via mail.

## **1.11 Conclusion**

Dans ce chapitre, nous avons présenté l'entreprise d'accueil en général, dont les activités principales sont la connexion Internet, les services TIC, etc.

Et nous avons fait aussi une étude de l'existant, critique de l'existant, solution proposée et une architecture proposée.

Dans le chapitre suivant, nous allons parler de la généralité de la supervision.

## **Chapitre 2 : PRINCIPE ET CONCEPT DE LA SUPERVISION**

## **2.1 Introduction**

Les réseaux sont partout à l'heure actuelle. Ils sont devenus indispensables au bon fonctionnement de nombreuses entreprises et administrations. Tout problème ou panne peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. La supervision des réseaux est alors nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et problèmes pouvant survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture.

C'est pourquoi les administrateurs réseaux et systèmes font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Un tel système assure une gestion proactive du système et améliore la disponibilité effective des applications et des services opérant sur les serveurs.

## **2.2 Définition de la supervision**

La supervision informatique désigne l'ensemble des outils et ressources déployés pour veiller au bon fonctionnement de votre système d'information. Le but est de mettre en place une maintenance préventive afin d'éviter les interruptions de service et de détecter en amont les failles des infrastructures informatiques pour contrer les cyber-attaques. Le monitoring 7 J/7 permet de vérifier en permanence que les pare-feu et antivirus sont actifs et que les serveurs sur lesquels sont répliquées et sauvegardées vos données fonctionnent correctement.

Ainsi, un service de supervision informatique vous permettra d'avoir un système d'information opérationnel et disponible.

La surveillance de vos équipements informatiques permet de détecter toute anomalie en temps réel, et de pouvoir ainsi la traiter dans les meilleurs délais [2].

## **2.3 Principes de fonctionnement de la supervision**

Les principes de fonctionnement de la supervision peuvent être résumés en :

### **2.3.1 Fonctionnalités de la supervision**

On distingue quatre fonctionnalités de la supervision :

#### **A. La surveillance**

La surveillance informatique résulte de ce que l'on appelle monitoring qui est une activité de mesure d'une activité informatique. La surveillance des équipements d'une infrastructure est la fonctionnalité de base proposée par les différents outils de supervision du marché. Ils permettent de surveiller :

- Les ressources d'un équipement informatique ;

- Le trafic réseau ;
- Les attaques liées au réseau ;
- Les flux de données entre applications.

#### B. Les Notifications

La notification est employée pour décrire des fonctions d’alerte automatisées entre processus. Mais lorsqu’un incident est détecté, il faut autoriser la réception des notifications informant ainsi qu’un changement d’état vient d’avoir lieu. Ce genre d’événements est généralement distribué par messagerie ou par SMS. Il est même possible de distribuer sélectivement les notifications à un autre groupe d’utilisateurs bien défini en fonction des plages horaires programmées et de répéter cet envoi plusieurs fois lorsque la réparation ou l’acquittement n’est pas réalisé au bout d’un certain laps de temps.

#### C. Les sondes

Généralement, les outils de supervision n’effectuent pas eux-mêmes la surveillance de certaines composantes : mémoire, CPU, disques, etc.

Concrètement, les sondes sont des scripts, des programmes ou plus généralement du code, appelés scheduler, qui effectuent l’ensemble des traitements de vérification et envoient leurs résultats afin de centraliser les informations récoltées. On doit, donc, pouvoir ajouter facilement des sondes en s’appuyant sur les différentes extensions (ou plugins) disponibles.

#### D. Les dépendances

Il est primordial que les différents équipements conservent leur interdépendance au sein de l’outil de supervision. Si on prend l’exemple des bases de données, des switchs et des serveurs : le mode opérationnel est vérifié lorsque les bases de données hébergées sur les serveurs sont opérationnelles et que les switchs interconnectant les serveurs sont également en fonction. Ainsi, en précisant la dépendance des serveurs vis-à-vis des bases de données et des switchs vis-à-vis des serveurs, on peut alors notifier les cas de pannes. Et cela facilite la détection d’incidents en se concentrant sur l’essentiel de l’information, la panne de l’équipement interdépendant, plutôt que sur l’ensemble des machines en alerte. Cela permet de mieux mettre en évidence l’équipement ou le service en défaut et de faciliter le dépannage et la maintenance [3].

### 2.3.2 Principe de la supervision

Avant toute chose, le principe de la supervision est de s’assurer du bon fonctionnement d’un système. Il peut être appliqué sur plusieurs entités : serveurs, équipements réseaux, firewall, ...

Sa mise en place permet d’effectuer des actions proactives pour détecter un éventuel problème avant qu’il survienne. En général, lorsque l’on est en présence d’une grosse infrastructure, on délègue la gestion des alertes à des masters de supervision qui sont chargés de récolter les



informations venant des équipements. La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble des équipements supervisés, et ceci en temps réel. Elle permet de visualiser à tout moment l'état des différents équipements configurés. Les objectifs sont multiples :

- Éviter les arrêts de service ;
- Remonter les alertes ;
- Détecter et prévenir les pannes .

En configurant la solution de supervision, un utilisateur peut être informé à n'importe quel moment des problèmes qui peuvent survenir sur les équipements. On appelle ce type d'événement une alarme. Il s'agit d'un événement potentiellement problématique pouvant entraîner le mauvais fonctionnement du système. Par exemple, lorsqu'un disque dur atteint une occupation du disque de plus de 90 %, une alarme est générée afin de nous prévenir qu'il faut y remédier. L'alarme est alors visible sur l'interface de la solution de supervision, mais surtout elle peut être transmise via un e-mail ou un sms à un ou plusieurs destinataires afin de les tenir informés immédiatement.

"Mieux vaut prévenir que guérir" -- [Proverbe français] [4].

## **2.4 Protocole SNMP**

### **2.4.1 Présentation**

Créé en 1988 par l'IETF (Internet Engineering Task Force), SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau).

C'est un protocole qui permet de gérer les équipements réseaux ainsi que les machines informatiques, ce protocole étant utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau. Chaque machine, que ce soit sous Windows ou Linux possède de nombreuses informations capitales pour l'administrateur réseau. On retrouve

Des informations comme la quantité de RAM utilisée, l'utilisation du CPU, l'espace disque et encore bien d'autres indicateurs. SNMP va permettre de remonter ces informations à l'administrateur de façon centralisée pour pouvoir réagir au plus vite aux pannes éventuelles [5] [8].

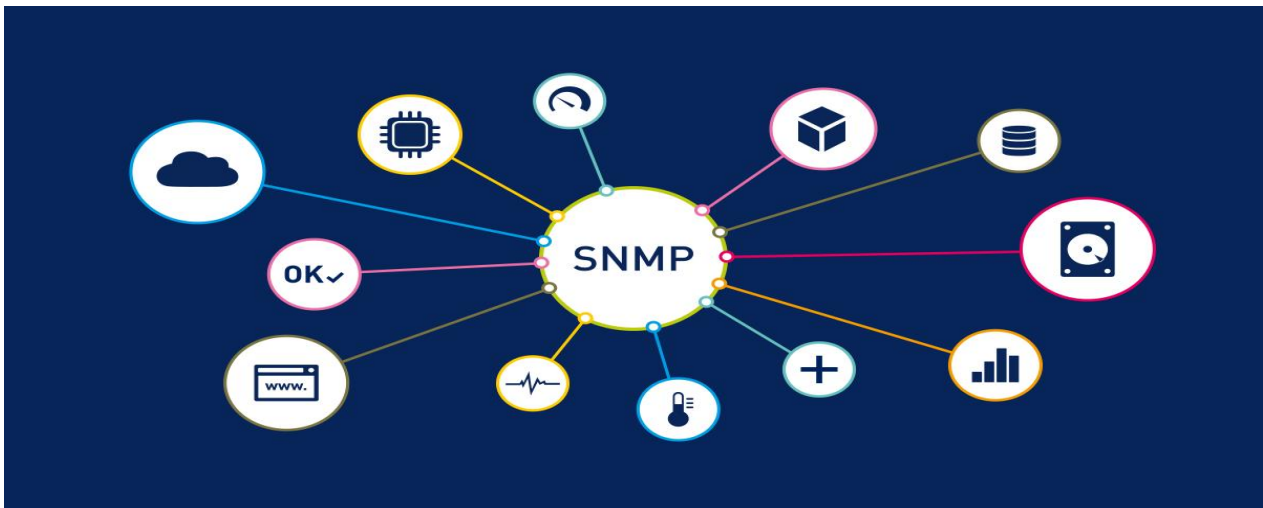


Figure 2. 1 : Fonctionnement de SNMP [8]

## 2.4.2 Fonctionnement

### 2.4.2.1 Les agents

Sur une machine à superviser, pour que SNMP envoie les informations que l'on souhaite, il faut qu'un agent soit installé sur celle-ci. Cet agent écoute sur le port 161 et attend que le serveur lui envoie des requêtes pour lui répondre.

L'agent pourra aussi envoyer des alertes lui-même si l'administrateur réseau les a configurées. Par exemple, pour surveiller l'occupation CPU d'une machine, l'administrateur définira une valeur critique à partir de laquelle une alerte doit lui être émise. Pour finir l'agent pourra aussi agir sur l'environnement local, c'est pourquoi ce protocole est critique car il peut servir à d'autres personnes mal intentionnées pour prendre le contrôle à distance de certains équipements.

Généralement, l'administrateur possède un outil permettant de centraliser ce que lui retournent tous les agents et c'est donc cet outil qui va interroger les équipements du réseau, afin de pouvoir gérer un réseau entier.

### 2.4.2.2 La MIB

Une MIB (Management Information Base, base d'information pour la gestion du réseau) est une base de données contenue sur chaque équipement où sont stockées l'ensemble des informations que l'équipement peut envoyer.

La MIB est présentée sous forme d'une arborescence où chaque nœud est un identifiant appelé OID (Object Identifier). L'OID est unique et universel. Il est représenté sous forme d'une énumération de nombres séparés par des ".".

### 2.4.2.3 Les commandes SNMP

Le protocole SNMP se base sur le fait qu'il existe une station de gestion réseau, le Manager, dont le rôle est de contrôler le réseau et de communiquer via ce protocole avec un agent. L'agent est de manière générale une interface SNMP embarquée sur le matériel destiné à être administré à distance [6]

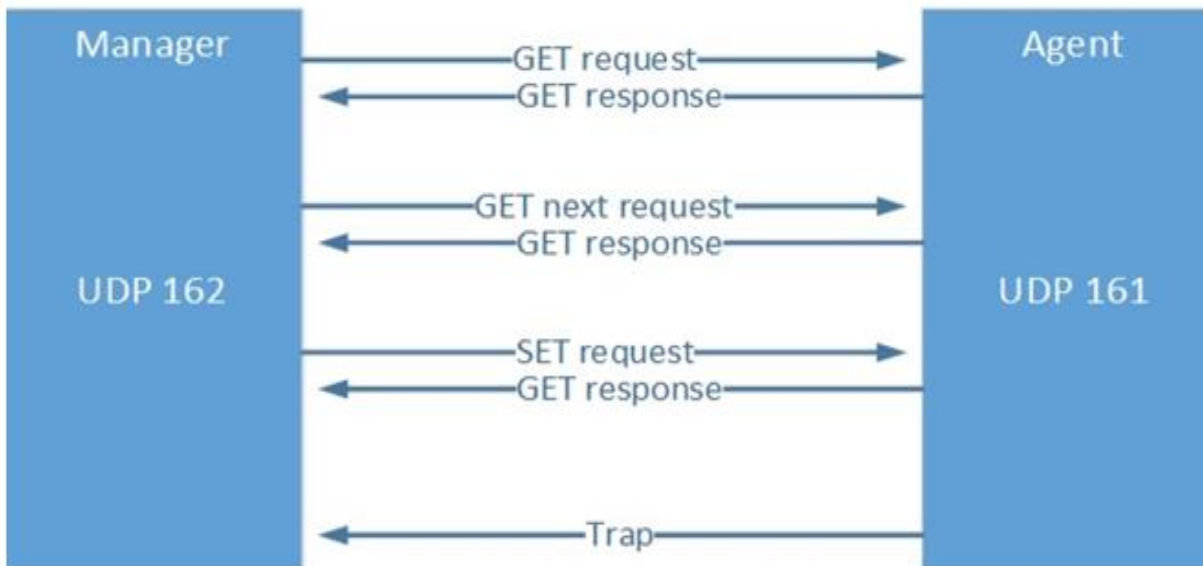


Figure 2. 2 : Les requêtes SNMP [7]

Tableau 2. 1 Description des requêtes de la figure 2.2

Commande	Action
get request	Le Manager SNMP demande une information à un agent SNMP
get next request	Le Manager SNMP demande l'information suivante à l'agent SNMP
set request	Le Manager SNMP met à jour une information sur un agent SNMP
get response	L'agent SNMP répond à un get-request ou à un set-request
trap	L'agent SNMP envoie une alarme au Manager

## 2.5 Les méthodes de supervision

Deux grandes méthodes s'opposent lorsqu'on parle de la supervision :

### 2.5.1 Mode actif

Le mode actif est une vérification réalisée à intervalles de temps réguliers par le serveur de monitoring, comme représenté sur la figure 2.3.

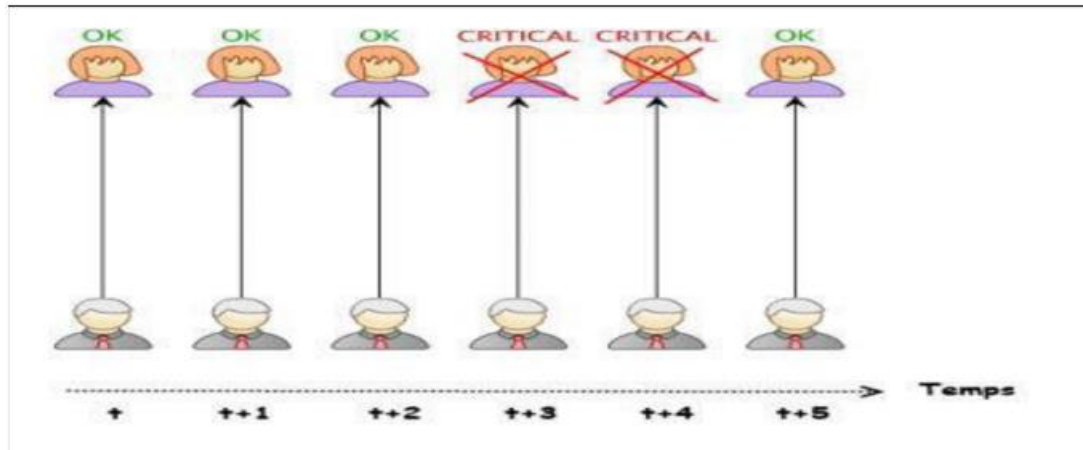


Figure 2. 3 : Mode Actif [9]

#### A. Les Avantages du mode actif

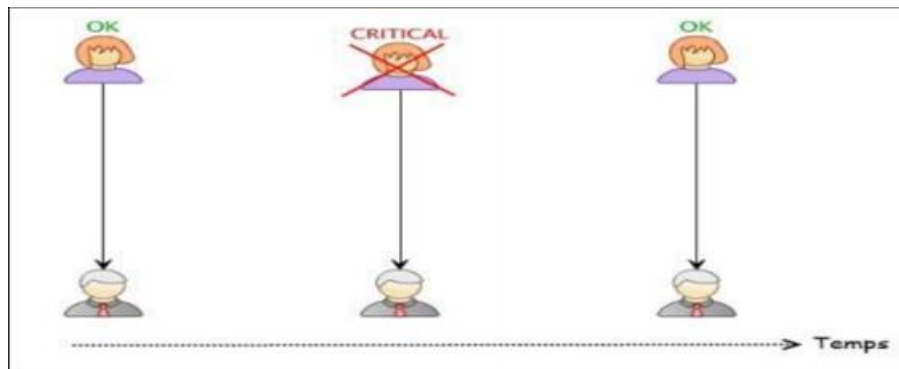
- Simple et rapide car c'est le serveur qui collecte les informations.
- Vérification réalisée en un laps de temps.

#### B. Les Inconvénient du mode actif

- Le temps de réaction est plus long car l'équipement est monitoré par le serveur de monitoring qui lui-même monitoré d'autres équipements.

### 2.5.2 Mode passif

Le mode passif est un signal émis par l'équipement monitoré à chaque changement d'état comme représenté sur la figure 2.4.



**Figure 2. 4 : Mode passif [9].**

**A. Les Avantages du mode passif :**

- Temps de réaction rapide car l'équipement se supervise lui-même ;
- Tous les changements d'états sont remontés par le client sans que le serveur le consulte.

**C. Les Inconvénients du mode passif :**

- si l'équipement ne fonctionne plus, aucune alerte ne sera remontée ;
- Surcharge du serveur de monitoring lors de l'envoi simultané d'alertes par plusieurs équipements.

Pour conclure, suite à une longue réflexion afin de déterminer lequel des deux concepts était le plus approprié pour notre projet, nous avons fini par conclure que celui-ci se rapprochait plus du mode actif.

Car le mode actif est :

- Simple et rapide à mettre en place ;
- Limiter les charges du serveur de monitoring (Vérification réalisée à intervalles de temps) ;
- Haute disponibilité sur la réception d'informations (en mode passif si l'équipement ne fonctionne plus, aucune alerte ne sera remontée) [9].

## **2.6 Solutions de la supervision**

Il existe deux solutions de la supervision :

### **2.6.1 Solutions propriétaires**

Parmi Les logiciels Nous allons maintenant voir quelques outils populaires de monitoring propriétaires tels que : HP OpenView et IBM Tivoli NetView.

### 2.6.1.1 HP OpenView

HP OpenView est, à l'heure actuelle, un des logiciels majeurs de la supervision. Il permet le management d'équipements réseaux. Une interface graphique permet un affichage de l'état courant des équipements. Il est basé sur SNMP pour dialoguer avec les différentes machines.

HP OpenView permet de gérer des composants d'une infrastructure informatique d'une manière standardisée. Il est principalement utilisé pour la surveillance de serveurs, périphériques, réseaux, bases de données et applications pour assurer que les défauts sont détectés et alertés dans les meilleurs délais. Il est composé de deux systèmes :

- Système de MAP : Une interface graphique appelée MAP permet un affichage de l'état courant des équipements. Les couleurs permettent de préciser l'état des différents périphériques ;
- Système d'alarme : HP OpenView intègre un système d'alarme. En effet, des requêtes SNMP sont régulièrement envoyées vers les agents. Si un état change ou une machine devient injoignable, une alarme est directement déclenchée et une action peut être entreprise (lancement d'un programme, envoi d'un mail, etc.).

#### 1. Les Avantages :

- Une vue globale du réseau ;
- Une vision des différents incidents.

#### 2. Les Inconvénients :

- Coût d'acquisition et de support [10].

### 2.6.1.2 IBM Tivoli Netview

Ce logiciel est né du rachat de l'entreprise Tivoli par IBM. C'est un des logiciels commerciaux les plus utilisés. Il s'agit d'une suite de logiciels comprenant notamment Tivoli Monitoring essentiellement dédié à la supervision de machines ou d'applications. L'architecture repose sur le protocole SNMP. Des agents sont en place sur chaque matériel et une application centrale permet d'effectuer diverses opérations :

- Définir les différentes règles de supervision ;
- Stocker les informations et les présenter sous la forme de pages web ;
- Générer différents graphiques sur l'état du réseau.

#### 1. Les Avantages :

- Découverte des réseaux TCP/IP ;
- Affichage des topologies réseaux ;
- Gestion des différents événements ;

- Affichage de la santé et de l'état du réseau ;
- Détection et prévention de problèmes.

## 2. Les Inconvénients :

- Coût d'acquisition et de support.

### 2.6.2 Solutions Open Source

Il faut savoir qu'il existe des dizaines de solutions Open Source dédiées au Monitoring, le principal critère de choix réside dans les différents cas d'utilisation. Dans cette partie, nous allons présenter quelques solutions de Monitoring, à savoir : ZABBIX, NAGIOS et CENTREON.

#### 2.6.2.1 Zabbix

Zabbix est une solution de supervision open source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de la supervision et créer une communauté autour de lui pour permettre une évolution plus rapide. À côté de cela, cette société propose un service de maintenance commercial.

Zabbix permet plusieurs moyens d'acquérir les données :

- Via SNMP : comme tous ses concurrents ;
- Via test de service : Il n'y a rien à installer sur l'équipement surveillé, mais les tests sont limités à des Ping ou tests de protocoles (SMTP, HTTP,...) ;
- Via l'agent Zabbix local : C'est une originalité : installer un agent permet d'obtenir toute information sur l'équipement sans utiliser le protocole SNMP.

L'architecture du logiciel est découpée en quatre (4) composants dans le but de faciliter le monitoring :

- Serveur : Le serveur est le cœur de l'application Zabbix. Il centralise les données et permet de les attendre (trapping) ou d'aller les chercher (polling). Il centralise aussi toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème ;
- Le proxy : Élément optionnel de l'architecture, il permet de placer les données reçues des différents sites dans le but de faciliter les traitements pour le serveur ;
- L'agent : Une fois installé sur un système, l'agent va collecter les données locales et les envoyer au serveur ;

- L'interface Web : Celle-ci est une partie du serveur bien qu'il n'est pas obligatoire qu'elle se trouve sur la même machine que le serveur. L'interface permet de configurer entièrement Zabbix, d'accéder aux statistiques ainsi qu'à d'autres informations ;

Tous ces composants sont écrits en C afin de garder de hautes performances, bien que l'interface Web soit développée en PHP.

L'interface est divisée en cinq parties :

- Monitoring : La partie affichage des statistiques, graphiques, alertes, cartographie, etc ;
- Inventory : L'inventaire des machines et équipements ;
- Report : Statistiques sur le serveur Zabbix et rapport de disponibilité des services sur les machines supervisées ;
- Configuration : Comme son nom l'indique, permet de configurer entièrement. Zabbix ;
- Administration : Permet de gérer les moyens d'alertes (SMS, Jabber, Email,...) et les utilisateurs ;

#### 1. Les Avantages :

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting ;
- Une entreprise qui pousse le développement, et une communauté croissante ;
- Une interface vaste mais claire ;
- Une gestion des templates poussée, avec import/export XML, modifications via l'interface ;
- Des performances au rendez-vous : l'application a été testée avec succès avec 10 000 équipements supervisés ;
- Compatible avec MySQL, PostgreSQL, Oracle, SQLite.

#### 2. Les Inconvénients :

- L'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, nécessitant de sécuriser ces données (via VPN par exemple) ;
- Commence à être connu, mais pas encore auprès des entreprises : Peu d'interfaçage avec d'autres solutions commerciales [20].



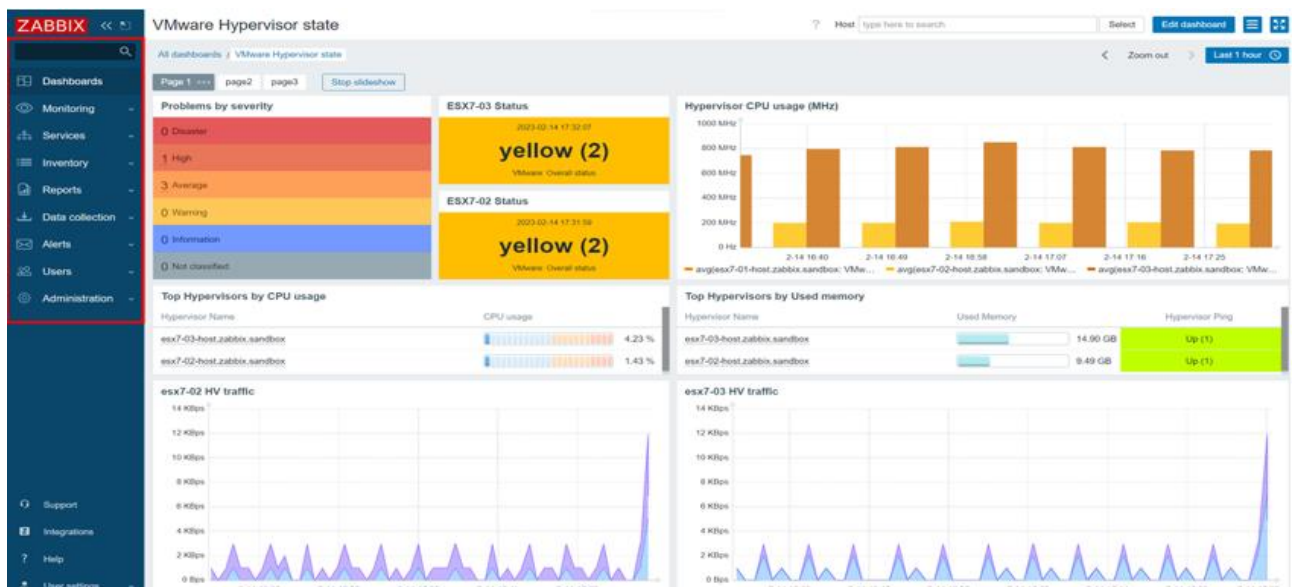


Figure 2. 5 : Tableau de bord de Zabbix [20]

### 2.6.2.2 Nagios

Successeur de NetSaint, Nagios est certainement le logiciel libre le plus connu dans le milieu de la supervision réseau. Appréciée par beaucoup d'entreprises ainsi que des particuliers.

L'architecture logicielle est modulaire comme chez ses concurrents.

L'interface est divisée en trois :

- Partie monitoring, qui permet plusieurs vues : vue globale, vue précise, vue de la carte du réseau, vue des problèmes, ... même une vue "3 D" ;
- Partie reporting regroupant les tendances des statistiques, les alertes et événements ainsi qu'un rapport de disponibilités des services ;
- Partie configuration classique permettant de tout configurer.

#### 1. Les Avantages :

- Reconnu auprès des entreprises, grande communauté ;
- des plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc.) ;
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, la gestion utilisateurs, ainsi que la cartographie des réseaux ;
- Beaucoup de documentations sur le Web ;
- Performances du moteur.

## 2. Les Inconvénients :

- Interface non ergonomique et peu intuitive ;
- Configuration fastidieuse via beaucoup de fichiers ;
- Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité [21].



Service	Check	Status	Time	Duration	Next Run	Output
webprod03	Check Users	OK	01-26-2007 14:58:59	0d 4h 53m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 4h 53m 23s	1/4	OK - load average: 0.21, 0.08, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 4h 53m 23s	1/4	OK - Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 4h 50m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 4h 50m 33s	1/4	DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 4h 50m 33s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 4h 50m 33s	1/4	OK - 95 processes running
Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	4/4	Critical Xen VMs Usage - Total NB: 0 - detected VMs:	
webprod04	Check Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4	USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4	OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:10	0d 0h 14m 13s	1/4	OK - Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 43s	1/4	DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4	OK - 250 processes running
Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	4/4	Warning Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4	
webprod05	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4	OK - Xen Hypervisor "webprod05" is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1	Check Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 3h 16m 21s	1/4	OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 3h 15m 41s	1/4	OK - Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 3h 15m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 3h 14m 51s	1/4	DISK OK [1196280 kB (9%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 3h 14m 1s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4	OK - 88 processes running
xen-vm2	Check Users	OK	01-26-2007 14:57:15	0d 3h 7m 41s	1/4	USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 3h 7m 1s	1/4	OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 3h 6m 21s	1/4	OK - Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 958 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 1h 15m 4s	1/4	DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 3h 9m 41s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 3h 9m 1s	1/4	OK - 52 processes running

Figure 2. 6 : Tableau de bord de Nagios [21]

### 2.6.2.3 Centreon

Centreon, basé sur Nagios, se présente comme une évolution de celui-ci pour tout d'abord son interface, mais aussi ses fonctionnalités. Créé en 2003 par des Français souhaitant améliorer Nagios et son interface très austère, Centreon a été repris par une nouvelle entreprise nommée Merethis. Centreon reprend donc les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes. Son interface reprend un découpage classique :

- Home : Page d'accueil avec Le "Tactical Overview" de Nagios permet un coup d'œil rapide aux problèmes survenus et accès aux statistiques des performances du moteur et de ses composants ;
- Monitoring : Possède plusieurs vues, mais reprend la grande idée de l'arbre des groupes d'équipements. Reprend également la vue Nagios ;
- Views : Permet d'accéder à tous les graphiques avec un menu arborescent. Accès à une cartographie du réseau en applet Java ;
- Reporting : Un Dashboard ressemblant à celui de Zabbix en ajoutant une frise chronologique de la disponibilité de l'équipement ;
- Configuration : Pour tout configurer de A à Z ;

- Administration : Configuration des accès utilisateurs.

### 1. Les Avantages :

- La robustesse et la renommée de Nagios ;
- Une interface beaucoup plus sympathique, permettant de tout configurer, de garder un œil sur tout le réseau en permanence ;
- Les utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios ;
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, la gestion utilisateurs, ainsi que la cartographie du réseau ;

### 2. Les Inconvénients :

- L'interface peut paraître complexe car il existe beaucoup d'options, de vues... Cela nécessite une petite formation ;
- Un développement qui n'est pas encore en phase avec celui de Nagios : Parfois des problèmes de compatibilité ;

Un peu plus lourd que du Nagios pur [22].



**Figure 2. 7 : Tableau de bord de Centreon [22]**

## 2.7 Comparaison entre open source ou propriétaire

Aujourd'hui plusieurs solutions de monitoring subsistent dans le monde de la supervision, open source ou propriétaires, mais chaque modèle de supervision a ses avantages et ses inconvénients.

## 2.7.1 Propriétaire

### 1. Les Avantages :

- Bénéficie d'une palette de fonctionnalités avancées et enrichies ;
- Solutions globales répondant à une large gamme de besoins.

### 1. Les inconvénients

- Développement additionnel restreint et coûteux ;
- Incompatibilités entre fournisseurs dues aux différents produits et protocoles ;
- Coût d'acquisition et de support pouvant être élevé selon la solution et les contrats.

## 2.7.2 Open Source

### 1. Les Avantages :

- Mises à jour fréquentes, notamment grâce à la communauté active soutenant le développement du produit ;
- Il est facile à administrer ;
- Respect des standards facilitant la compatibilité entre les différentes solutions ;
- Pas de coût d'acquisition : les solutions sont distribuées librement et restent accessibles à tous en tout temps.

### 2. Les inconvénients :

- Ce n'est pas totalement gratuit ;
- Le nombre de versions d'un logiciel est très nombreux : il est parfois difficile de trouver les dernières mises à jour [9].

## 2.8 Pourquoi choisir des solutions open sources ?

Pour des raisons financières, l'achat d'une ou plusieurs licences de logiciels propriétaires se voit écarté malgré les solutions confortables proposées.

Car il ne faut pas négliger que le principal atout de ces solutions open sources est certes la gratuité, mais aussi bel et bien les existantes communautés sur lesquelles s'appuient ces solutions.

### 2.8.1 Contrainte des solutions open source

En adoptant une telle solution, on ne distinguera qu'un seul et véridique obstacle, l'obligation constante de demeurer averti sur la technologie, il faudra régulièrement se rendre sur les forums, les blogs tout ce qui est capable de raisonner l'aspect communautaire, et ainsi d'ouvrir des réponses aux questions posées. Cet échange de bonne méthode permettra de mettre à jour fréquemment les solutions et de les adapter en fonction du besoin utilisateur [9].

## 2.9 Tableaux comparatif entre les différents outils de supervision

**Tableau 2. 2 : Tableau comparatif des outils de supervision**

Critères fonctionnels	Zabbix	Nagios	Centreon
Environnement d'installation	Unix, Windows	Unix	Unix
Base de données	PHP, C++, C	C++	PHP
Protocole	HTTP, FTP, SMTP, SSH, IMAP, SNMP	SNMP, SMTP, ICMP, NNTP, POP3	SNMP, SMTP, ICMP, NNTP, POP3
Gestion d'authentification	Oui	Oui	Oui
Création des graphes simples à partir des mesures	Oui	Non	Oui
Création des graphes complexe avec mise en relation des métriques des services supervisés	Oui	Non	Non
Utilisation d'agent sur machine cible	agent Unix/Windows	NSClient	NSClient
Installation et Configuration simple	Oui	Non	Oui
Intégration simple d'un nouvel hôte dans un système de centralisée	Oui	Non	Oui
Utilisation de gestion de base de données(RRD)	Non	Non	Oui

## **2.10 La solution retenue : ZABBIX**

Vu la popularité de Zabbix, ses mises à jour régulières et surtout sa volonté de rester gratuit, nous avons alors décidé de choisir ce dernier pour notre projet puisqu'il remplit toutes les prérogatives de la demande de l'entreprise car ils nous permettent de vérifier la disponibilité des services et des ressources, réagir aux alertes en notifiant l'administrateur via mail 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.

## **2.11 Conclusion**

Le présent chapitre a été consacré à la présentation détaillée de la notion de supervision de manière globale, ses enjeux et ses outils propriétaires et open sources afin de choisir le bon outil. Après avoir effectué le choix de l'outil de supervision open source convenable, dans le chapitre suivant nous verrons Présentation de l'outil de supervision Zabbix ainsi que son installation.

## **Chapitre 3 : PRESENTATION DE L'OUTIL DE SUPERVISION ZABBIX**



### 3.1 Introduction

Dans cette partie de notre rapport, nous commencerons par présenter l'outil de supervision Zabbix, son historique, ses composants, son principe de fonctionnement ainsi que son architecture.

### 3.2 Présentation de Zabbix

Zabbix a été créé par Alexeï Vladishev, et est actuellement activement développé et soutenu par ZABBIX SIA. C'est une "entreprise-class Open Source distributed monitoring solution".

Zabbix est un logiciel qui supervise de nombreux paramètres réseaux ainsi que la santé et l'intégrité des serveurs. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer une base d'alerte e-mail pour pratiquement tous les événements. Cela permet une réponse rapide aux problèmes serveurs. Zabbix offre un excellent reporting et des fonctionnalités de visualisation de données basées sur les données stockées. Cela rend Zabbix idéal "for Capacity Planning".

Zabbix supporte à la fois "polling et trapping". Tous les rapports et statistiques, comme la configuration de paramètres, sont accessibles par l'interface Web. L'interface Web veille à ce que le statut de votre réseau et de vos serveurs puisse être évalué depuis n'importe quel endroit. Correctement configuré, Zabbix peut jouer un rôle important dans la supervision de l'infrastructure IT. Ceci est également vrai pour les petites organisations avec peu de serveurs ainsi que pour les grandes entreprises avec une multitude de serveurs.

Zabbix est gratuit. Zabbix est écrit et distribué sous Licence publique générale GNU version 2. Cela signifie que son code source est librement distribué et disponible pour le public. Le support gratuit et commercial est disponible et fourni par Zabbix Company [5].

### 3.3 Qu'offre ZABBIX

Possibilités de Zabbix :

- Découverte automatique des serveurs et périphériques réseaux ;
- Supervision répartie sur une administration Web centralisée ;
- Support des mécanismes "polling and trapping" ;
- Logiciels serveurs pour Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X ;

- Agent haute performance en natif (Logiciel client pour Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista) ;
- Supervision sans agent ;
- Authentification d'agent sécurisée ;
- Permissions utilisateurs flexibles ;
- Interface Web ;
- Notification par e-mail d'événements prédéfinis ;
- Haut niveau (business) de visualisation des ressources supervisées ;
- Log d'audit [5].

### **3.4 Principe de fonctionnement de ZABBIX**

#### **3.4.1 Les composants de ZABBIX**

##### **3.4.1.1 Zabbix Server**

Permet une surveillance à distance (et en local) du bon fonctionnement de différents services systèmes et réseaux, tels que : les serveurs Web, les serveurs de courriers, ou bien encore les serveurs FTP, etc. Il gère la notification par mail, afin d'avertir les administrateurs de toute nouvelle alerte. Zabbix utilise le protocole SNMP pour superviser des hôtes. Il peut aussi avoir recours aux agents, mais dans ce cas, il ne remontera qu'une quantité limitée d'informations [12].

##### **3.4.1.2 ZABBIX Frontend**

Deuxième composant essentiel après Zabbix Server, Zabbix Frontend est tout simplement l'interface de visualisation des événements, mais aussi, et surtout l'interface d'administration et de configuration de Zabbix.

Zabbix Frontend, étant une interface Web (PHP), a l'avantage d'être accessible depuis n'importe quelle plate-forme possédant un navigateur Internet [12].

##### **3.4.1.3 Zabbix Proxy**

Permet de collecter des informations sur la performance et la disponibilité des données sur un hôte, avant de les transmettre au Zabbix Server. Zabbix Proxy offre la possibilité de réduire la charge d'un serveur Zabbix. En effet, toutes les informations collectées peuvent être traitées en local, avant leur transmission au serveur.

Le proxy Zabbix est idéal pour une surveillance centralisée de sites distants, fonctionnant comme un serveur intermédiaire, il remplit parfaitement son rôle de collecteur de données d'équipements variés. Distant d'un serveur Zabbix, il agit comme une sonde de collecte et de traitement des données [12].

### 3.4.1.4 Zabbix Agent

Même si le serveur Zabbix peut fonctionner sans agents, l'usage de ces derniers permet une meilleure surveillance des hôtes, et donc une supervision plus stable. L'installation d'un Zabbix Agent sur un hôte offre essentiellement une surveillance active des ressources locales, des applications, etc. L'agent envoie toutes les informations supervisées au Zabbix Server [12].

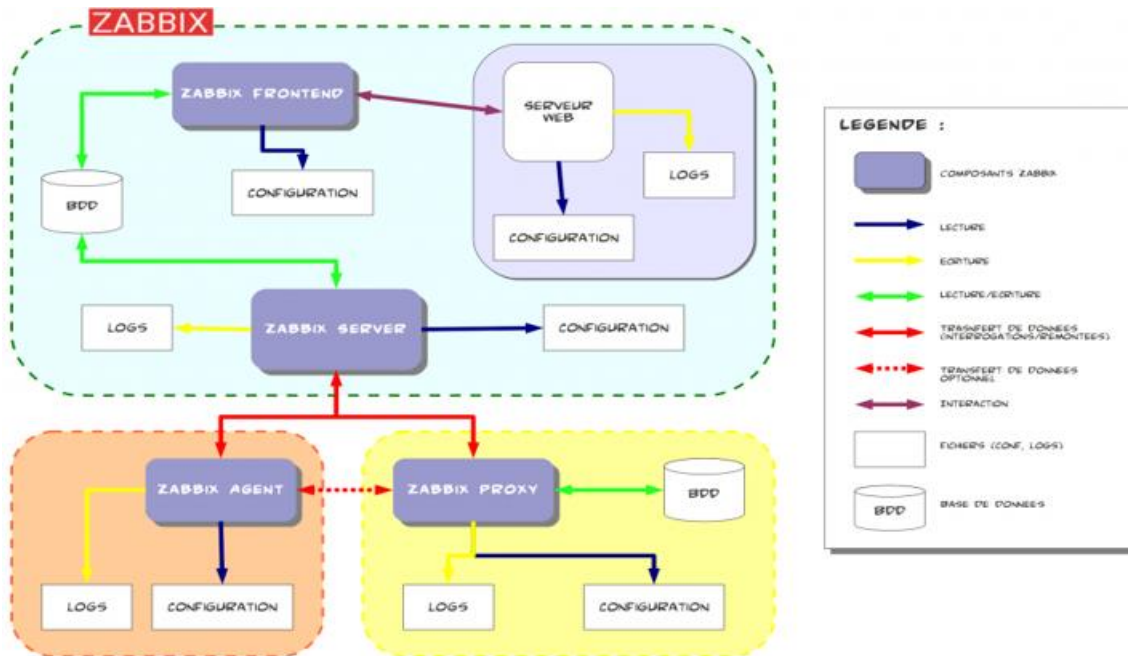


Figure 3. 1 : Architecture de Zabbix [12]

Dans ce schéma, les composants Zabbix sont regroupés en trois blocs, le premier représente la partie serveur de Zabbix, c'est-à-dire, les composants Server et Frontend, qui sont essentiels au fonctionnement et à l'administration d'un serveur Zabbix. Ces deux composants utilisent une base de données, servant à stocker les données de supervision, et également pour les afficher dans l'interface Web.

Quant aux deux autres blocs, ils représentent la partie Agent et Proxy de Zabbix. L'agent peut interagir avec le proxy, en transférant ses données non plus directement vers le serveur Zabbix, mais plutôt vers le proxy. Ce dernier agissant comme un serveur intermédiaire, c'est-à-dire un collecteur, il utilise donc comme pour Zabbix Server une base de données.

### 3.5 Les fonctionnalités de Zabbix

- Items (éléments) : Un item est un élément qui teste des services et collecte des données ; Exemple : Ping vers un serveur.
- Triggers (déclencheurs) : génèrent un événement en réaction à une certaine valeur ou donnée remontée par un item (déclencheurs d'alarmes) ;

Exemple : Serveur non disponible.

- Actions Envoi des alertes (notifications), en fonction d'événements précis générés par des triggers ;

Exemple : Envoi d'un mail.

Voici un schéma montrant les différentes relations entre les 3 éléments essentiels de Zabbix pour la génération d'une alerte, c'est-à-dire l'item, le trigger et l'action.

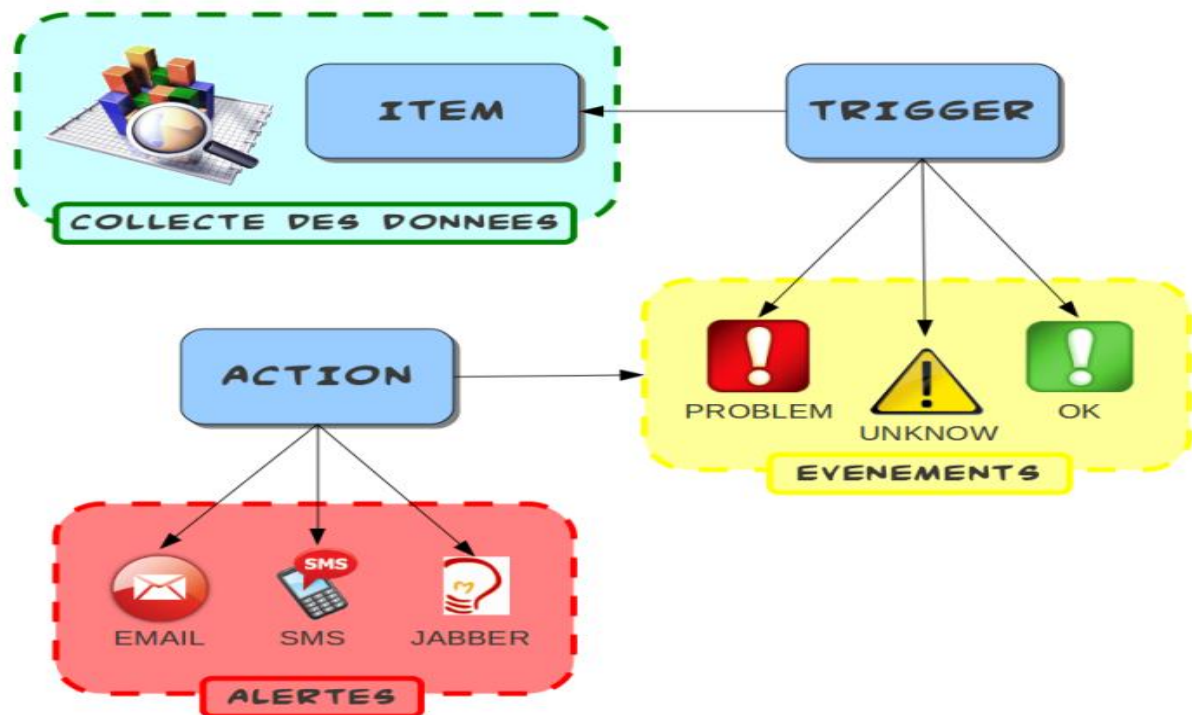


Figure 3. 2 : Les fonctionnalités de Zabbix [12]

### 3.6 Installation de Zabbix

Afin d'installer Zabbix sur notre machine, nous nous rendons dans le site officiel de Zabbix <https://www.zabbix.com/fr/download> pour l'installation de ce dernier comme le montre la figure.

Pour notre projet, nous avons choisi :

- La version de Zabbix 6.4 (dernière version) ;
- Distribution Ubuntu ;
- version du système d'exploitation 22.04 (JAMMY) ;
- Composant Zabbix (Serveur, Frontend, Agent) ;

- Base de données : MYSQL ;
- Serveur Web Apache.

Comme le montre la figure 3.3. [14].

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
6.4	Alma Linux	22.04 (Jammy)	Server, Frontend, Agent	MySQL	Apache
6.0 LTS	CentOS	20.04 (Focal)	Proxy	PostgreSQL	Nginx
5.0 LTS	Debian	18.04 (Bionic)	Agent		
4.0 LTS	OpenSUSE Leap	16.04 (Xenial)	Agent 2		
7.0 PRE-RELEASE	Oracle Linux	14.04 (Trusty)	Java Gateway		
	Raspberry Pi OS		Web Service		
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

**Figure 3. 3 : Téléchargement de Zabbix**

a) Installation de référentiel Zabbix [14].

Téléchargement des paquets zabbix depuis <https://www.zabbix.com/fr/download>.

```
root@asrs-virtual-machine:~# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.debs
```

Depaquage des fichiers zabbix

```
# dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
```

Mise à jour des paquets

```
# apt update
```

b) Installer le serveur, le frontend et l'agent Zabbix

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

c) Création d'une base donnée

```
root@asrs-virtual-machine:~# apt install mysql-server -y
```

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

NB : pour renforcer le niveau de la sécurité nous avons changé le mot de passe par Pa\$\$word123@@# dans le fichier de configuration

```
# Zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz |
mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Désactivez l'option `log_bin_trust_function_creators` après l'importation du schéma de base de données.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

d) Configurer la base de données pour le serveur Zabbix

Pour la configuration de la base de données du serveur, nous allons modifier le fichier `/etc/zabbix/zabbix_server.conf`.

```

DBName=zabbix
### Option: DBSchema
#   Schema name. Used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=

### Option: DBUser
#   Database user.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
#   Database password.
#   Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=
DBPassword=Pa$$word123@@#

```

Description du fichier de configuration /etc/zabbix/zabbix\_server.conf :

DBName=zabbix ;

DBUser=zabbix ;

DBpassword=Pa\$\$word123@@#.

e) Démarrage du processus du serveur et de l'agent Zabbix

Démarrez les processus du serveur et de l'agent Zabbix avec les commandes suivantes :

```

# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2

```

f) Ouverture d'un navigateur web (firefox)

Pour accéder à l'interface web de zabbix il nous faut une adresse ip et pour avoir une adresse ip on tape la commande ifconfig dans un terminal en mode root pour télécharger les paquets net-tools comme montre la capture suivante.

```

root@asrs-virtual-machine:~# apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
net-tools is already the newest version (1.60+git20181103.0eebece-1ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@asrs-virtual-machine:~# █

```

Après avoir téléchargé les paquets net-tools pour l'installation de ifconfig on peut maintenant voir notre adresse ip comme montre la capture suivante :

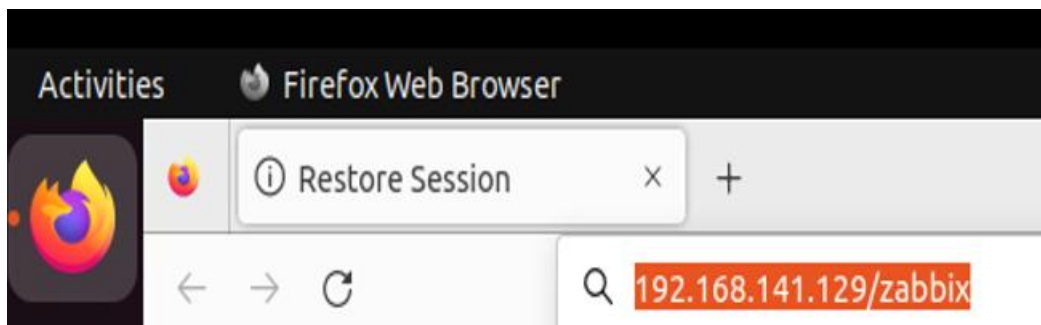
```
asrs@enatic:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.141.129 netmask 255.255.255.0 broadcast 192.168.141.255
    inet6 fe80::10bf:62e3:b628:44e prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a5:65:f7 txqueuelen 1000 (Ethernet)
    RX packets 2861 bytes 627895 (627.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2862 bytes 333679 (333.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 27406 bytes 2396212 (2.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27406 bytes 2396212 (2.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Les informations d'ifconfig sont :

- Adresse ip 192.168.141.129 ;
- Masque du réseau 255.255.255.0 ;
- Adresse de diffusion 192.168.141.255 ;

On ouvre le navigateur firefox avec l'adresse ip 192.168.141.129/zabbix comme montre la figure 3.4.



**Figure 3. 4 : Interface de navigateur de Firefox**

Mozilla Firefox est un navigateur Web gratuit et open-source développé par la Mozilla Foundation et sa filiale, la Mozilla Corporation. Il est disponible pour les systèmes d'exploitation Windows, macOS, Linux et Android. Vous pouvez télécharger Firefox pour votre ordinateur depuis le site officiel de Mozilla.

Après avoir entré l'adresse IP au navigateur on se retrouve sur la fenêtre suivante.

En cliquant sur prochaine étape on se retrouve sur la figure 3.5 Sur l'écran suivant, vous verrez le tableau qui énumère toutes les conditions préalables à l'exécution de Zabbix.





**Figure 3. 5 : Page de Bienvenue et choix de langues(Français) de Zabbix**

Toutes les valeurs de ce tableau doivent être correctes (OK), vérifiez donc qu'elles le sont. N'oubliez pas de faire défiler vers le bas et d'examiner toutes les conditions préalables. Une fois que vous avez vérifié que tout est OK comme montre la figure 3.6, cliquez sur prochaine étape pour continuer.



**Figure 3. 6 : Vérification des Prérequis**

L'écran suivant demande des informations sur la connexion à la base de données. Comme le montre la figure 3.7.

**Figure 3. 7 : Connexion à la base de données**

Description des paramètres de la base de données :

- Type de base de données : il y a deux types de SGBD dont MySQL et PostgreSQL.

Le choix de SGBD dépend des besoins spécifiques de l'utilisateur. Cependant, selon une comparaison générale entre MySQL et PostgreSQL, MySQL est plus adapté aux applications simples et aux requêtes simples, tandis que PostgreSQL est plus adapté aux applications complexes et aux requêtes complexes ;

Notre repose sur MySQL comme la plupart des utilisateurs choisissent MySQL pour se connecter à la base de données de Zabbix en raison de sa simplicité d'utilisation et de sa popularité.

- Hôte base de données : localhost ;

Si vous utilisez MySQL comme système de gestion de base de données pour Zabbix, le nom d'hôte MySQL est généralement localhost Cela signifie que la base de données MySQL est hébergée sur le même serveur que votre application Zabbix. Si vous utilisez un autre système de gestion de base de données tel que PostgreSQL, le nom d'hôte sera différent.

- Le port de la base de données ;

Le port par défaut pour la base de données Zabbix dépend du type de base de données que vous utilisez. Si vous utilisez MySQL, le port par défaut est 3306.

- Le nom de la base de données ;

Le nom de notre base de données par défaut est ZABBIX.

- Utilisateur zabbix ;

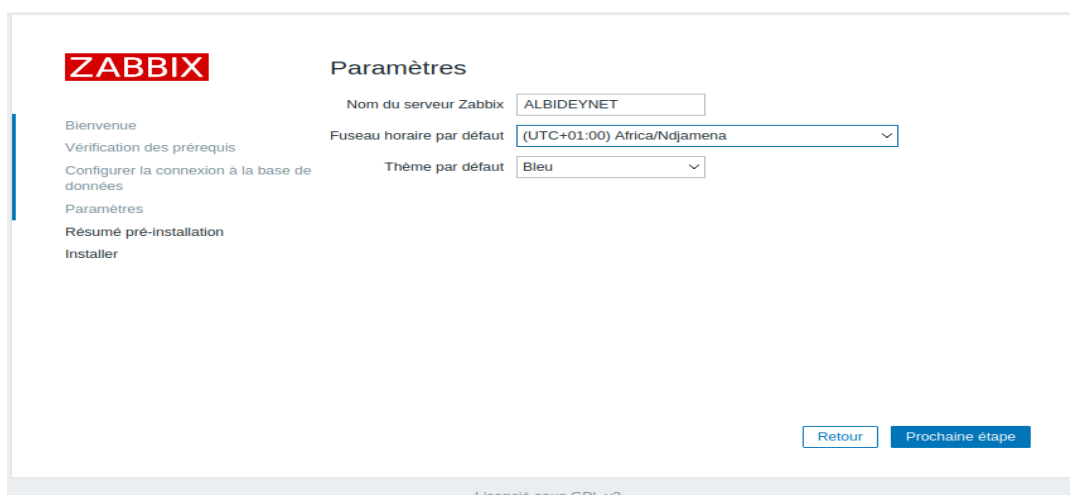
Le nom de l'utilisateur de la base de données par défaut est ZABBIX.

- Mot de passe de l'utilisateur zabbix ;

Le mot de passe de l'utilisateur zabbix est Pa\$\$word123@@#.

- Le chiffrement TLS de la base de données ;

Le chiffrement TLS (transport layer Security) permet de chiffrer les données qui sont échangées entre le client et le serveur, ce qui rend ces données illisibles pour toute personne qui intercepterait la communication. Cela peut aider à protéger les données sensibles stockées dans la base de données Zabbix.



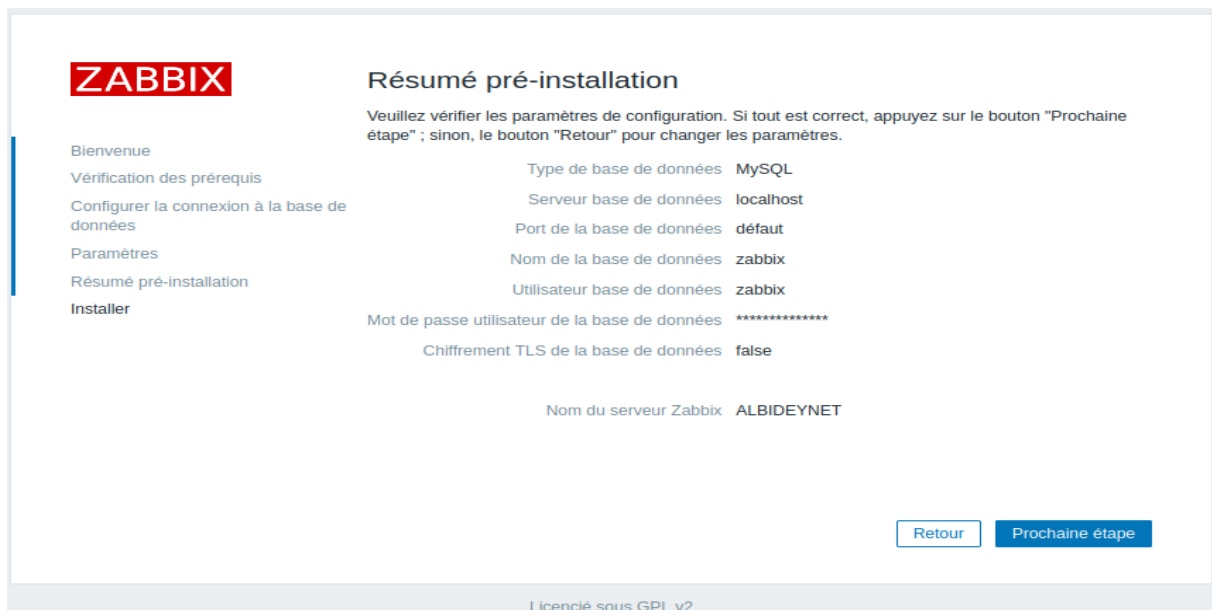
**Figure 3. 8 : Changement de Paramètres**

En cliquant sur prochaine étape, on se retrouve sur la fenêtre ci-dessous comme indique la figure 3.8.

Description de paramètres de zabbix :

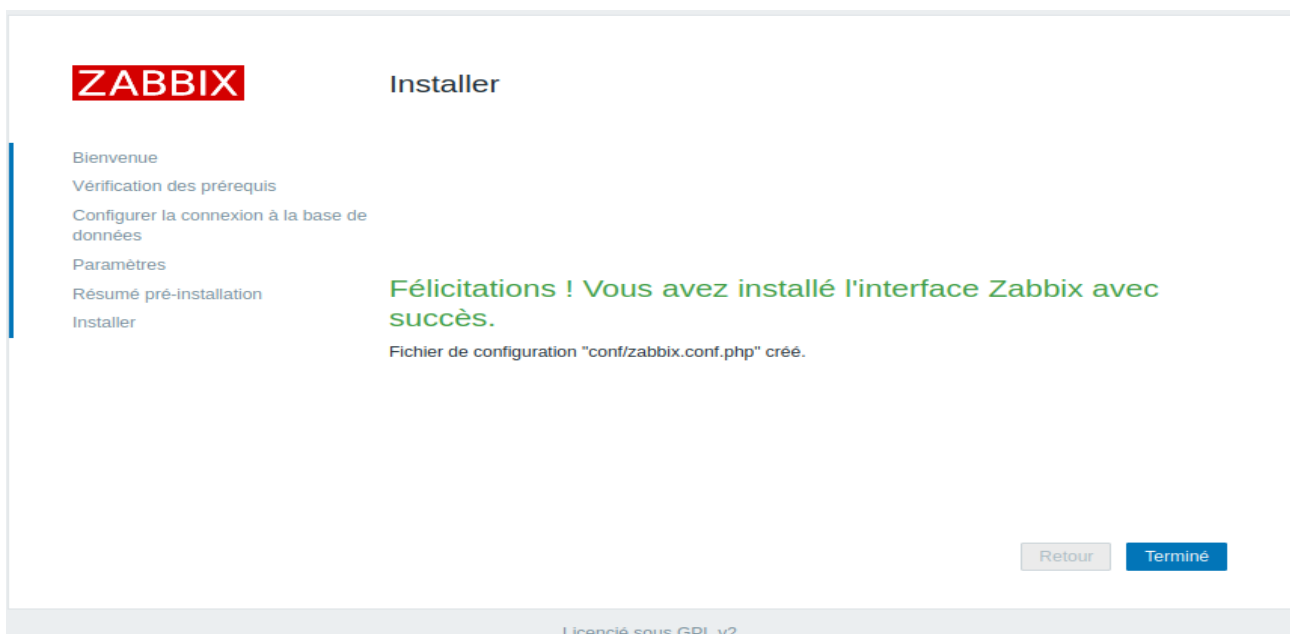
- Nom du serveur zabbix : ALBIDEYNET ;
- Fuseau horaire paramétré (utc+01 :00) Africa/Ndjamena ;
- Thème par défaut : bleu.

En cliquant sur prochaine étape on se retrouve sur la page de vérification de zabbix comme le montre la figure 3.9.



**Figure 3. 9 : Résumé de Pré-Installation**

En cliquant sur prochaine étape on se retrouve sur la page qui nous montre la fin de l'installation avec succès comme le montre la figure 3.10.



**Figure 3. 10 : Fin de l'installation avec succès**

Après avoir installé avec succès il est temps de se connecter au serveur ZABBIX comme le montre la figure 3.11.

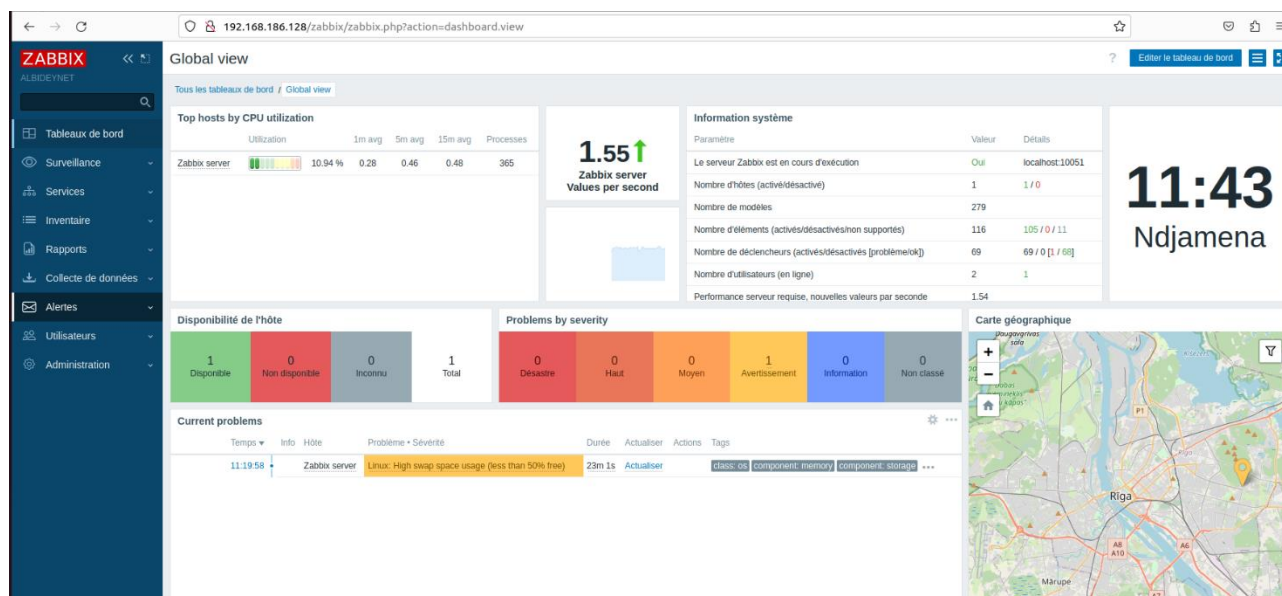


**Figure 3. 11 : Page d'Authentification de Zabbix**

Description de la page d'authentification de zabbix :

- Nom d'utilisateur : Admin (par défaut) ;
- Mot de passe : zabbix.

Après avoir fini la phase d'authentification, nous nous retrouvons dans la page d'accueil de zabbix, comme montre la figure ci-dessous [14].



**Figure 3. 12 Page d'accueil de Zabbix**

### **3.7 Conclusion**

Après avoir effectué une étude détaillée de l'outil de supervision que nous avons choisi, son installation, ses fonctionnalités, nous allons voir dans le chapitre suivant la mise en place de notre projet ainsi que les différentes configurations.

## **Chapitre 4 : PROPOSITION DE LA SOLUTION ET MISE EN OEUVRE**

## 4.1 Introduction

À travers ce chapitre, nous allons décrire la phase de réalisation de notre logiciel. Nous allons commencer par la spécification des différents environnements de développement, matériels et logiciels. Ensuite, nous décrirons les points les plus intéressants de l'application, tout en donnant un aperçu sur les différentes parties développées au cours de ce projet.

## 4.2 Environnement de travail

### 4.2.1 Environnement matériels

Afin de bien mener notre travail, nous avons eu besoin d'un environnement de travail assez convivial. Ainsi les ressources qui étaient présentes sont les suivantes : Le tableau 4.1 regroupe les ressources matérielles mises à notre disposition tout au long du déroulement du stage.

**Tableau 4. 1 : Environnement matériels**

Désignation	caractéristiques
Ordinateur portable Dell vostro 5590	Intel core i5 10 ème génération, RAM 8,00 Go, 250
Routeur MIKROTIK	Routeur os licence 5,5port gigabits, 5 port 10/100,1 port SFP, 1 port USB, 1 port PoE.

### 4.2.2 Environnement logiciels

Après avoir présenté l'environnement matériel de développement, nous allons rappeler et justifier brièvement les choix techniques que nous avons adoptés. Le tableau 4.2 regroupe les ressources logicielles utilisées :

**Tableau 4. 2 : environnement logiciels**

Nom du Logiciel	Licence	Fonction
Vmware workstation	Gratuit	Outil de virtualisation de poste de travail, utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation.
Ubuntu 22.04 LTS	Gratuit	Ubuntu est un système d'exploitation libre et open-source, qui est basé sur le système Linux. Il est conçu pour les ordinateurs personnels, les serveurs et les appareils mobiles. Ubuntu est connu pour sa simplicité d'utilisation, sa stabilité et sa sécurité. Il est disponible gratuitement et peut être utilisé par tout le monde, sans aucune restriction.
ZABBIX 6.4	Gratuit Sous GPL	ZABBIX est un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau.



## 4.3 Configurations de zabbix

### 4.3.1 Ajout d'hôte via agent ZABBIX

Pour configurer un hôte via agent zabbix, on se rend dans le site officiel zabbix via ce lien ci-dessous [https://www.zabbix.com/fr/download\\_agents](https://www.zabbix.com/fr/download_agents) pour télécharger l'agent zabbix comme montre le lien ci-dessous. [https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.6/zabbix\\_agent2-6.4.6-windows-amd64-openssl.msi](https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.6/zabbix_agent2-6.4.6-windows-amd64-openssl.msi) .

Après le téléchargement, nous allons installer l'agent avec les informations suivantes :

- le nom de la machine cliente ;
- l'adresse IP du serveur zabbix ;
- port d'écoute d'agent zabbix ;
- spécifiez l'adresse IP du serveur/proxy zabbix pour les vérifications d'agents actif ;

Comme le montre la figure 4.1.

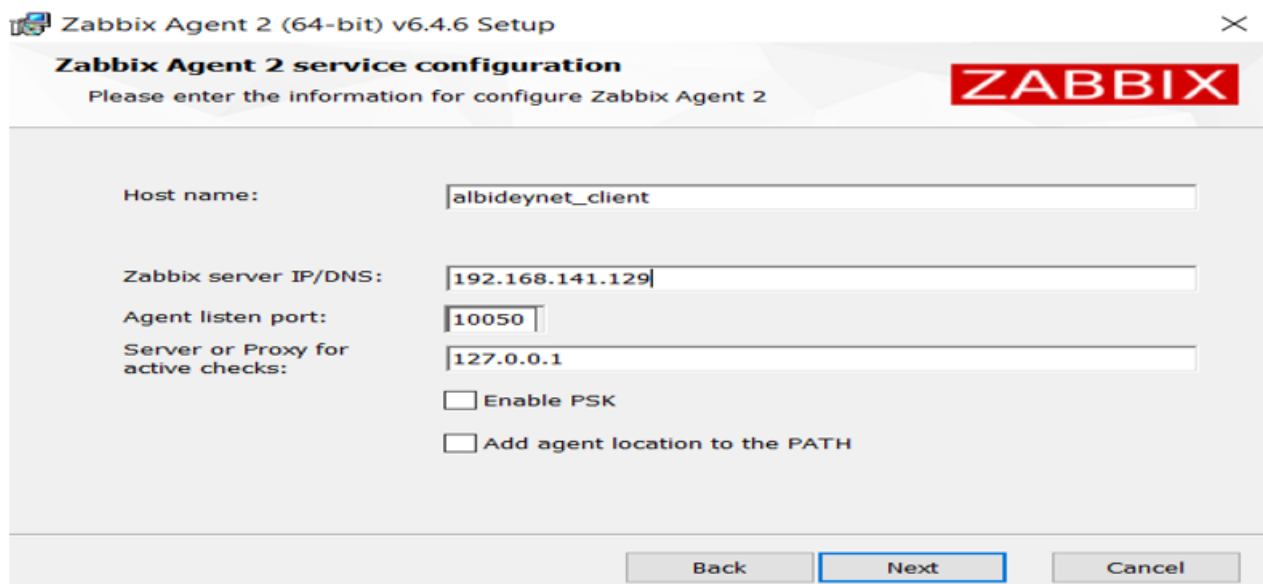
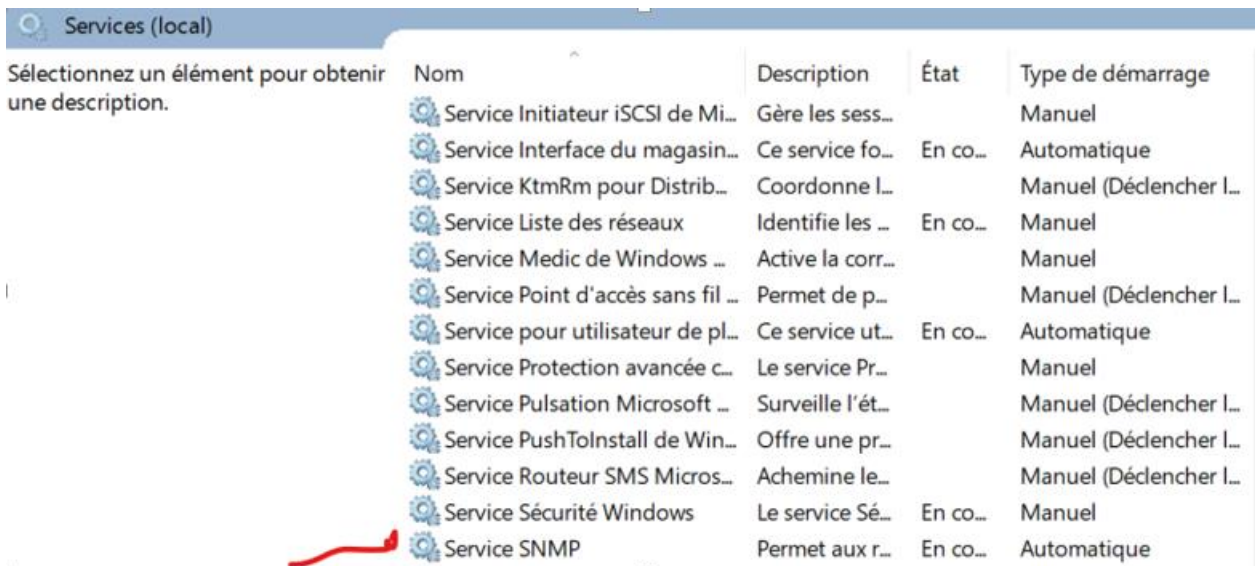


Figure 4. 1 : Installation de l'agent zabbix.

### 4.3.2 Ajout d'hôte via SNMP

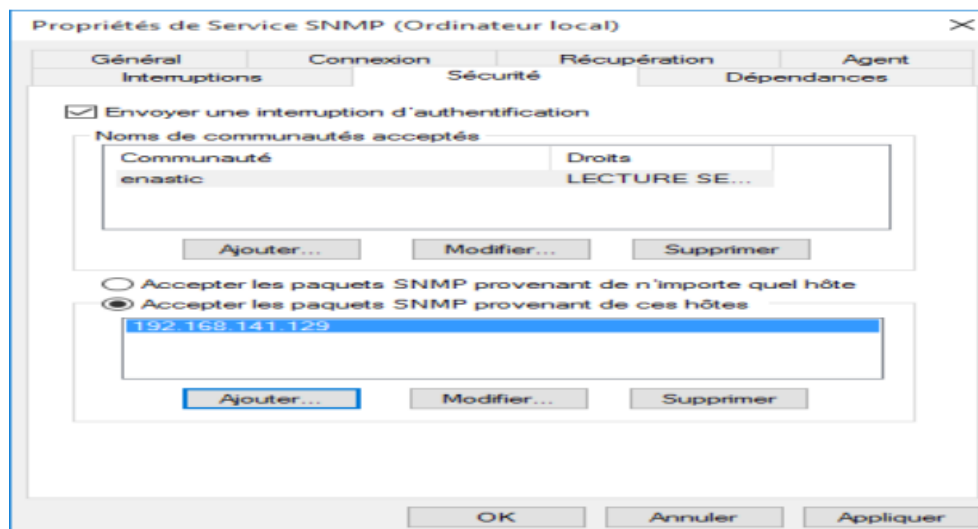
Pour ajouter un hôte via SNMP on se rend dans paramètres → applications et fonctionnalités puis on cherche le service SNMP et puis installé.

Après installation, on se rend sur la barre de recherche de Windows puis on édit «services » puis on défile vers le bas jusqu'à vous trouverez « service SNMP » comme le montre la figure 4.2.



**Figure 4. 2 : Choix de services SNMP**

Après avoir choisi le service SNMP, on se retrouve sur la fenêtre suivante.



**Figure 4. 3 : Insertion des informations SNMP**

### Description de la figure 4.3

Nous allons donner enastic comme nom de la communauté.

Communauté : est un groupe de périphériques et de systèmes de gestion qui peuvent échanger des messages SNMP. C'est comme un mot de passe qui permet aux périphériques et aux systèmes de gestion de communiquer entre eux. Seuls les périphériques et les systèmes de gestion qui sont membres de la même communauté peuvent échanger des messages SNMP [15].

Et nous allons donner une adresse de notre serveur Zabbix a notre client SNMP qui 192.168.141.129  
Ensuite on clique sur ajouter puis sur appliquer puis sur ok pour terminer.

### 4.3.3 Ajout d'un routeur MIKROTIK

Pour superviser un routeur mikrotik, on télécharge winbox est un outil utilitaire léger créé par MikroTik pour fonctionner avec son micro logiciel RouterOS.



mikrotik [18]



Winbox [19]

On accède à l'interface de routeur via le logiciel winbox on entre l'adresse IP du routeur mikrotik comme le montre la figure suivante.

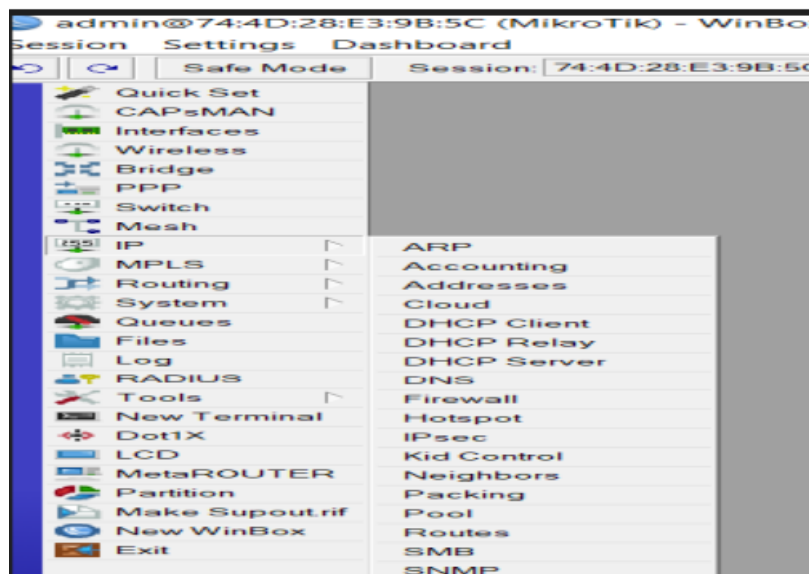
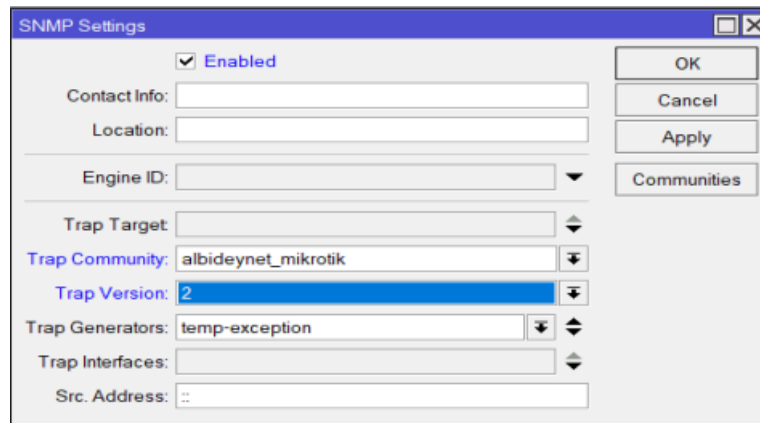


Figure 4. 4 : Interface de Winbox

Après avoir entré l'adresse IP on choisit l'option IP, puis on verra tous les services disponibles : DHCP, DNS, SNMP, etc.

Pour la supervision du routeur mikrotik nous avons choisi SNMP comme le montre la figure suivante :



**Figure 4. 5 : Configuration de service SNMP dans Winbox**

Sur la console du serveur Zabbix utilisez les commandes suivantes pour installer et tester la communication SNMP pour ça nous éditons cette commande dans notre terminal comme le montre la capture suivante.

Dans notre exemple, le routeur mikrotik à l'adresse IP 192.168.1.88

Configuration de SNMP et agent zabbix

Pour configurer un hôte dans l'interface web Zabbix, procédez comme suit :

- Aller dans : Collecte de données → Hôtes ;
- Cliquez sur Créer un hôte à droite (ou sur le nom d'hôte pour modifier un hôte existant) ;
- Entrez les paramètres de l'hôte dans le formulaire comme le montre la figure 4.6.

```
root@enastic:/home/asrs# snmpwalk -v2c -c configuration 192.168.1.88
```

Nouvel hôte ? X

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles  Sélectionner  
taper ici pour rechercher

\* Groupes d'hôtes  Sélectionner  
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		<input type="text" value="192.168.141.1"/>	<input type="text" value="windows 10"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

Surveillé via le proxy

Activé

Figure 4. 6 : Configuration d'un hôte.

Maintenant, nous devons ajouter le routeur mikrotik en tant qu'hôte. Comme le montre la figure 4.7 [17].

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles  Sélectionner  
taper ici pour rechercher

\* Groupes d'hôtes  Sélectionner  
taper ici pour rechercher

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP		<input type="text" value="192.168.1.88"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="161"/>	<input checked="" type="radio"/> Supprimer

\* Version SNMP

\* Communauté SNMP

Nombre maximal de répétitions

Utiliser des requêtes combinées

[Ajouter](#)

Description

Surveillé via le proxy

Activé

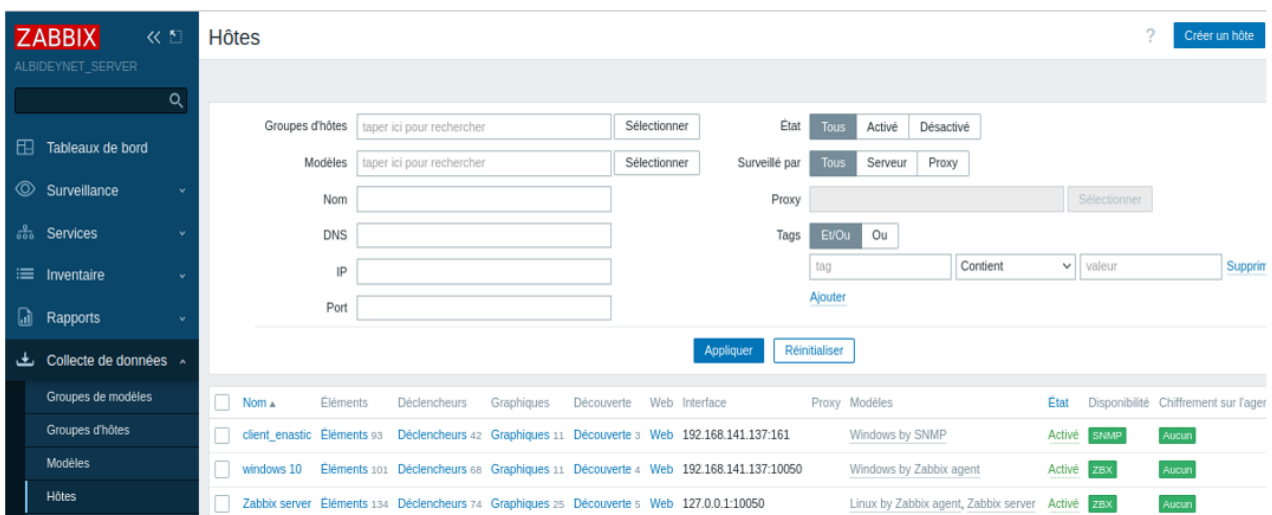
Figure 4. 7 : Ajout du routeur mikrotik

L'onglet Hôte contient les attributs généraux d'hôte :

Description de la figure 4.7 :

- Nom d'hôte sensible à la casse, il doit être identique à celui que vous avez configuré sur l'hôte ;
- Le nom visible définit comment cet hôte sera affiché dans les graphiques, les cartes, etc. et peut être laissé vide si le nom d'hôte d'origine vous convient ;
- Un modèle est un ensemble prédéfini d'éléments, de déclencheurs, de graphiques, etc. L'hôte lié à un modèle obtiendra automatiquement toutes les choses liées à ce modèle qui lui seront implémentées ;
- Groupes d'hôte Un hôte doit appartenir à au moins un groupe d'hôtes. Choisissez-en un ou créez le vôtre (tapez simplement le nom pour en ajouter un) ;
- Interfaces Appuyez ensuite sur le bouton "Ajouter" sur la ligne d'interface et choisissez son type. Zabbix est capable d'obtenir ses données via l'agent, SNMP, JMX et IPMI, aujourd'hui nous travaillons avec l'agent et SNMP ;
- Saisissez ensuite l'adresse IP ou le DNS nom de l'hôte et choisissez celui que Zabbix utilisera pour collecter les données ;
- Ajoutez une petite description si vous le souhaitez ;
- Aucun proxy ne vous permet de choisir entre la surveillance par le serveur lui-même ou un proxy ;
- Assurez-vous de cocher la case "activé" pour rendre l'hôte actif et surveillé.

À la fin on ajoute l'hôte pour avoir une vue complète du nouveau hôte supervisé comme le montre la figure 4.8.



**Figure 4.8 : Vu des hôtes superviser (Zabbix Server, SNMP, agent)**

#### 4.4 Notification via email

Malgré l'existence d'une interface web permettant de voir l'état d'un hôte ou service en temps réel, la notification des contacts reste toujours obligatoire. Pour envoyer les notifications par mail

depuis Zabbix il faut d'abord installer l'outil correspondant, cela peut se faire de plusieurs manières : utiliser SMTP, Postfix ou bien encore Sendmail.

Postfix est un élément étroitement lié à Zabbix. Effectivement, il sert à l'envoi des notifications vers votre serveur de messagerie et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail ; c'est pour cela qu'on l'a choisie comme solution. Les notifications dans Zabbix font appel à plusieurs éléments.

#### 4.4.1 Installation de postfix

Première étape consiste à vérifier que le port 587 est ouvert car si ce n'est pas le cas, on ne peut pas envoyer d'email pour vérifier, on édite `sudo IPTABLES -L` comme le montre la fenêtre suivante.

```
asrs@asrs-virtual-machine:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:submission
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:submission

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:submission
ACCEPT    tcp  --  anywhere              anywhere             tcp dpt:submission
asrs@asrs-virtual-machine:~$
```

Ouvrir le port SMTP 587 en entrée/sortie sur le pare-feu

- `Sudo iptables -A INPUT -p tcp --dport 587 -j ACCEPT`
- `Sudo iptables -A OUTPUT -p tcp --dport 587 -j ACCEPT`

Après la vérification, on fait la Mise à jour des paquets et installation de Postfix

- `Sudo apt-get update && sudo apt-get upgrade ;`
- `sudo apt-get install Postfix mailutils libsasl2-2 ca-certificates libsasl2-modules;`

Activation du service Postfix

- `sudo systemctl enable Postfix ;`

Création du certificat SSL

- `Sudo mkdir /etc/Postfix/ssl/ cd /etc/Postfix/ssl/ ;`
- `Sudo openssl req -newkey RSA:2048 -new -nodes -x509 -days 3650 -keyout cacert-smtp-gmail.key -out cacert-smtp-gmail.key ;`

#### 4.4.2 Configuration de postfix

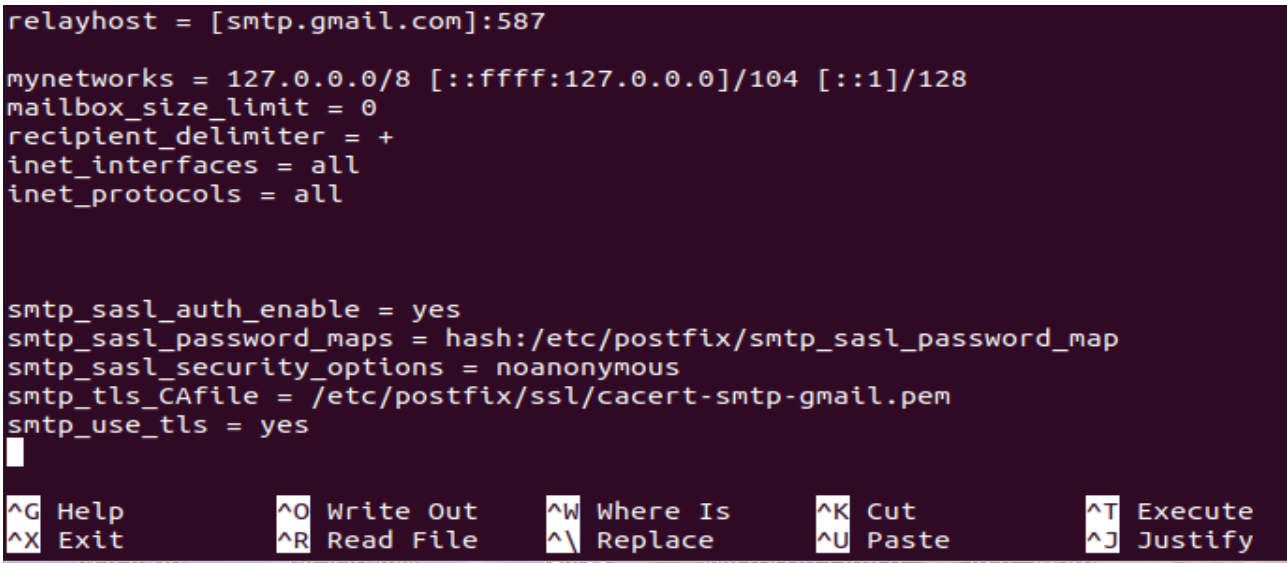
Pour la configuration on édite le fichier « `/etc/postfix/main.cf` » comme montre la capture suivante :

Création du fichier smtp\_sasl\_password\_map ;

```
relayhost = [smtp.gmail.com]:587

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/smtp_sasl_password_map
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/postfix/ssl/cacert-smtp-gmail.pem
smtp_use_tls = yes
```



On édite le fichier « /etc/Postfix/smtp\_sasl\_password\_map » ;

Comme montre la capture suivante

```
GNU nano 6.2 /etc/postfix/smtp_sasl_password_map
[smtp.gmail.com]:587 [redacted]:enzozyurglcxqzdx
```

Pour des raisons de confidentialités nous avons masqués l'adresse Gmail

Sudo chmod 400 /etc/postfix/smtp\_sasl\_password\_map pour limiter les droits du fichier contenant nos informations confidentielles.

Sudo systemctl restart postfix pour redémarrer le service postfix.

Sudo systemctl status postfix pour voir statut du service comme montre la capture.

```
asrs@asrs-virtual-machine:/etc/postfix/ssl$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2023-08-19 19:40:30 WAT; 13s ago
     Docs: man:postfix(1)
   Process: 63120 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 63120 (code=exited, status=0/SUCCESS)
      CPU: 3ms
```

## ← Accès moins sécurisé des applications

Certaines applications et certains appareils utilisent une technologie de connexion moins sécurisée, qui rend votre compte vulnérable. Vous pouvez désactiver l'accès pour ces applications (recommandé) ou l'activer si vous voulez les utiliser malgré les risques encourus. Google DÉACTIVE automatiquement ce paramètre s'il n'est pas utilisé. [En savoir plus](#)

Paramètre "Autoriser les applications moins sécurisées"  
activé

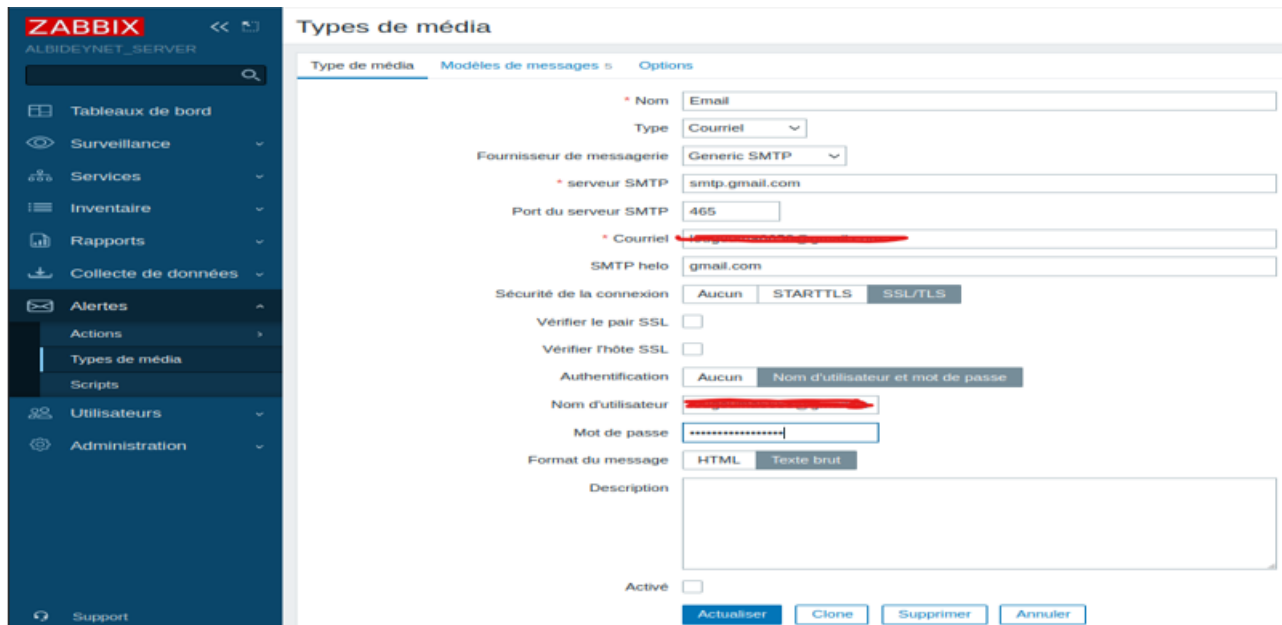


Figure 4. 9 : Paramètre Google



Maintenant que l'option « Autoriser les applications moins sécurisées » est activée, configurons Zabbix pour envoyer des e-mails à l'aide de Notre compte Gmail.

On se rend dans alerte → types de media → Email, comme le montre la figure 4.10.



The screenshot shows the Zabbix web interface for configuring a media type. The left sidebar contains navigation options like 'Tableaux de bord', 'Surveillance', 'Services', 'Inventaire', 'Rapports', 'Collecte de données', 'Alertes', 'Actions', 'Types de média', 'Scripts', 'Utilisateurs', and 'Administration'. The main content area is titled 'Types de média' and shows the configuration for an 'Email' media type. The settings include: 'Nom' (Email), 'Type' (Courriel), 'Fournisseur de messagerie' (Generic SMTP), 'serveur SMTP' (smtp.gmail.com), 'Port du serveur SMTP' (465), 'Courriel' (redacted), 'SMTP helo' (gmail.com), 'Sécurité de la connexion' (SSL/TLS selected), 'Authentification' (Nom d'utilisateur et mot de passe selected), 'Nom d'utilisateur' (redacted), 'Mot de passe' (redacted), 'Format du message' (HTML selected), and 'Description' (empty). At the bottom, there are buttons for 'Actualiser', 'Clone', 'Supprimer', and 'Annuler', and an 'Activé' checkbox.

**Figure 4. 10 : Paramètres de messagerie Zabbix pour le serveur de messagerie Gmail**

Description de la figure 4.10 : [16].

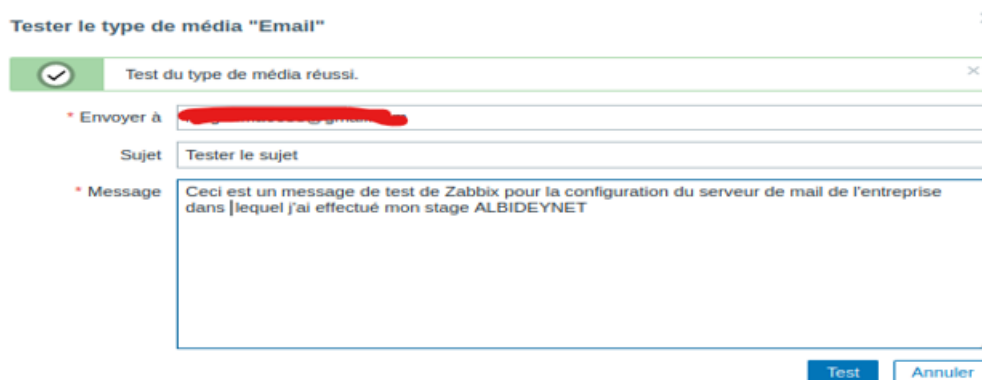
- Utilisez le type de média par défaut appelé « Email » fourni avec Zabbix (ou créez-en un nouveau) dans la section « Alerte "→"Types de médias » ;
- Définissez « Serveur SMTP » sur smtp.gmail.com pour gérer les e-mails sortants ;
- Définissez « Port du serveur SMTP » sur le port 465 ;
- Définissez « SMTP hello » sur gmail.com ;
- Définissez votre e-mail Google dans le champ « Courriel » que Zabbix utilisera comme « Adresse de l'expéditeur » dans les e-mails sortants. Sélectionnez l'option « SSL/TLS » dans la section « Sécurité de connexion » ;
- Sélectionnez « Nom d'utilisateur et mot de passe » dans la section « Authentification » ;
- Définissez votre adresse e-mail Google comme « Nom d'utilisateur » ;
- Définissez le mot de passe de votre compte Google dans la section « Mot de passe » ;
- Sélectionnez « Format de message », utilisez « HTML » ou « Texte brut » (par défaut) ;
- Activez ce « Type de média » en cliquant sur l'option « Activé » ;
- Appuyez sur le bouton « Actualiser ».

Avant de procéder à la configuration de nos notifications par e-mail Zabbix, nous devons nous assurer que notre configuration de l'étape précédente fonctionne comme prévu. Testez votre

Configuration à l'aide de l'option « Tester » pour un type de média que vous venez de configurer dans la section « Alerte » → « Types de médias ».

Cliquez sur l'option « Test » dans la dernière colonne de la ligne où se trouve votre type de média et une nouvelle fenêtre apparaîtra. Dans le champ « Envoyer à », entrez l'e-mail auquel Zabbix enverra des alertes et cliquez sur le bouton « Tester ».

Comme le montre à figure 4.11.



**Figure 4. 11 : Image montrant comment tester le type de média « Email » via l'interface Zabbix**

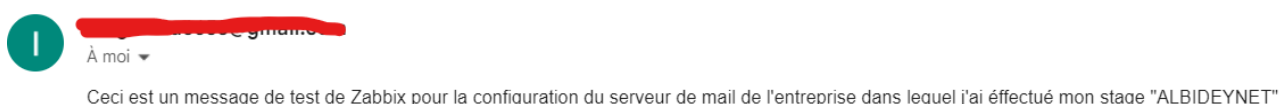
Description de l'image :

- Le nom du destinataire a été masqué pour des raisons de confidentialité ;
- Sujet : consiste à donner une idée à la personne cible avant même d'ouvrir la notification ;
- Message : permet d'écrire une description plus détaillée du sujet.

Vous pouvez passer à l'étape suivante si vous recevez « Test de type de média réussi » sinon vérifiez le pare-feu et essayez de Googler le message d'erreur généré par l'outil de test.

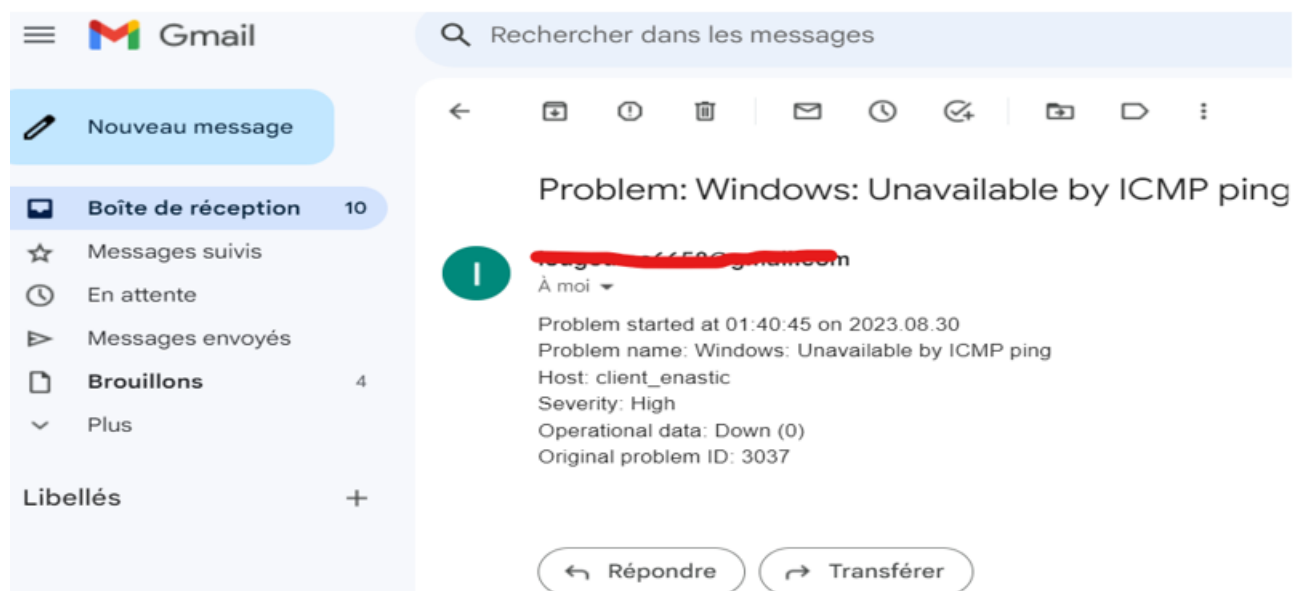
### 4.4.3 Teste de notification

Réception du mail pour le test



Test de notification depuis le serveur Zabbix alertant une machine cliente est « DOWM ».

Comme le montre la figure 4.12.



**Figure 4. 12 : Alerte d'indisponibilité d'une machine cliente**

**Description de la figure 4.12 :**

- Le temps où le problème a commencé : (le 30/08/20 à 01 :40 :45) ;
- Nom du problème : Windows n'est pas disponible par ICMP ping ;
- Nom du machine : client\_enastic ;
- Niveau de sévérité : élevé ;
- données opérationnelles : en panne ;
- ID du problème d'origine : 3037.

#### **4.5 Conclusion**

Dans ce chapitre, nous avons décrit l'aspect pratique de notre projet, où nous avons expliqué les étapes de préparation, configuration de Zabbix, et testé cette solution sur quelques équipements de l'organisme d'accueil.

De plus, nous avons mis en place un système de notification via mail qui va alerter à l'administrateur en cas de panne selon les degrés de sévérité configurés dans le serveur Zabbix.

## Conclusion Générale

L'objectif de notre projet est de mettre au sein d'Albideynet un outil de supervision open source, pour mieux superviser les équipements et les services de son réseau.

L'outil de supervision d'un système informatique offre une visibilité claire et simple à interpréter. En effet, ces outils permettent de vérifier ce qu'il se passe à tout moment au niveau du réseau, et nous autorisent à réagir rapidement en cas de problème et d'alerter l'administrateur via e-mail.

Dans un premier lieu, nous avons pu étudier l'existant et dégager ses limites afin de fixer la solution retenue après avoir réalisé une étude comparative entre les différentes solutions open source existantes sur le marché. Dans la partie réalisation, nous avons mis en place l'outil Zabbix, installé sous Ubuntu, et nous avons configuré une machine cliente et un routeur MikroTik.

Cette excellente expérience nous a amené à faire beaucoup de recherche et avoir une visibilité concrète sur un domaine bien spécifique, qui est la supervision d'un réseau informatique. En plus, ce travail nous a permis d'acquérir une expérience en Linux, à travers laquelle nous avons eu l'occasion d'appliquer nos connaissances et de confronter et appliquer la notion théorique à la pratique sur le terrain dans le domaine réseau informatique.

Comme perspectives, nous proposons l'amélioration de ce travail par :

- Utiliser un système de supervision basé sur le Cloud ;
- La configuration des notifications par SMS.

## Bibliographie

### ❖ Mémoires

- [3] P.Djibril, P.Clavair N.Amadou, «Étude et mise en place d'un outil de supervision du système d'information de SOFTNET», 2017/2018.
- [9] A.Hatim/etude\_et\_mise\_en\_place\_dune\_solution\_de\_monitoring\_open\_source\_slides.pdf 2017/2018.
- [10] C.Pierre-Adrien et R.Serge, « Supervision réseau » ,2015 page.

### ❖ Webographies

- [1] <http://www.albideynet.com/> visité le 05 juin 2023.
- [2] <https://www.axido.fr/tout-savoir-sur-la-supervision-informatique/> consulté le 10 juin 2023.
- [4] <http://igm.univ-mlv.fr/~dr/XPOSE2010/supervision/index.html> consulté le 13 juin 2023.
- [5] [https://www.zabbix.com/documentation/1.8/fr/manual/about/overview\\_of\\_zabbix](https://www.zabbix.com/documentation/1.8/fr/manual/about/overview_of_zabbix) consulté le 27 juin 2023.
- [7] [http://igm.univmlv.fr/~dr/XPOSE2013/administration\\_reseau\\_SNMP\\_LDAP/architecture.html](http://igm.univmlv.fr/~dr/XPOSE2013/administration_reseau_SNMP_LDAP/architecture.html) Consulté le 01 juillet 2023.
- [8] <https://www.paessler.com/fr/it-explained/snmp> consulté le 10 juillet 2023.
- [11] [https://docs.google.com/spreadsheets/u/0/d/1abH1oL3RkGvcaoIDBT6oo6AD\\_eH77roMAvoT](https://docs.google.com/spreadsheets/u/0/d/1abH1oL3RkGvcaoIDBT6oo6AD_eH77roMAvoT) Consulté le 14 juillet 2023.
- [12] <https://megancortesblog.wordpress.com/ppe-2-mise-en-place-dune-solution-de-supervision-zabbix/> consulté 17 juillet 2023.
- [13] <https://wiki.monitoring-fr.org/zabbix/zabbix-work.html> consulté le 11 juillet 2023.
- [14] <https://www.zabbix.com/fr/download> consulté régulièrement dans le mois de juin-juillet-Août.
- [15] <https://www.paessler.com/fr/whatisansnmpcommunitystring> consulté le 15 Août 2023.
- [16] <https://bestmonitoringtools.com/zabbix-alerts-setup-zabbix-email-notifications-escalations> consulté le 05 Août 2023.
- [17] <https://techexpert.tips/fr/zabbix-fr/surveiller-mikrotik-avec-zabbix/> consulté le 03 septembre 2023.
- [18] <https://blog.avast.com/mikrotik-routers-targeted-by-cryptomining-campaign-avast> consulté le 03/03/2023.
- [19] <https://www.wizcase.com/download/winbox/> visité le 03 juillet 2023.

- [20] <http://www.o00o.org/monitoring/solutions.html#zabbix> consulté le 05 juillet 2023.
- [21] <http://www.o00o.org/monitoring/solutions.html#nagios> consulté le 05 juillet 2023.
- [22] <http://www.o00o.org/monitoring/solutions.html#centreon> consulté le 05 juillet 2023.
- [23] <https://www.bing.com/?/ai> visité régulièrement dans le mois de juin-juillet-Août .
- [24] [www.wikipédia.com](http://www.wikipédia.com) visité régulièrement dans le mois juin-juillet-Août.
- [26] <https://lecrabeinfo.net/installer-ubuntu-22-04-lts-le-guide-complet.html> consulté le 04 septembre 2023.
- [27] <https://support.academicsoftware.eu/hc/fr/articles/4408526898577-Comment-installer-VMware-Workstation-Pro> consulté le 04 septembre 2023.
- [28] <https://www.axido.fr/tout-savoir-sur-la-supervision-informatique/> consulté le 10 juin 2023.

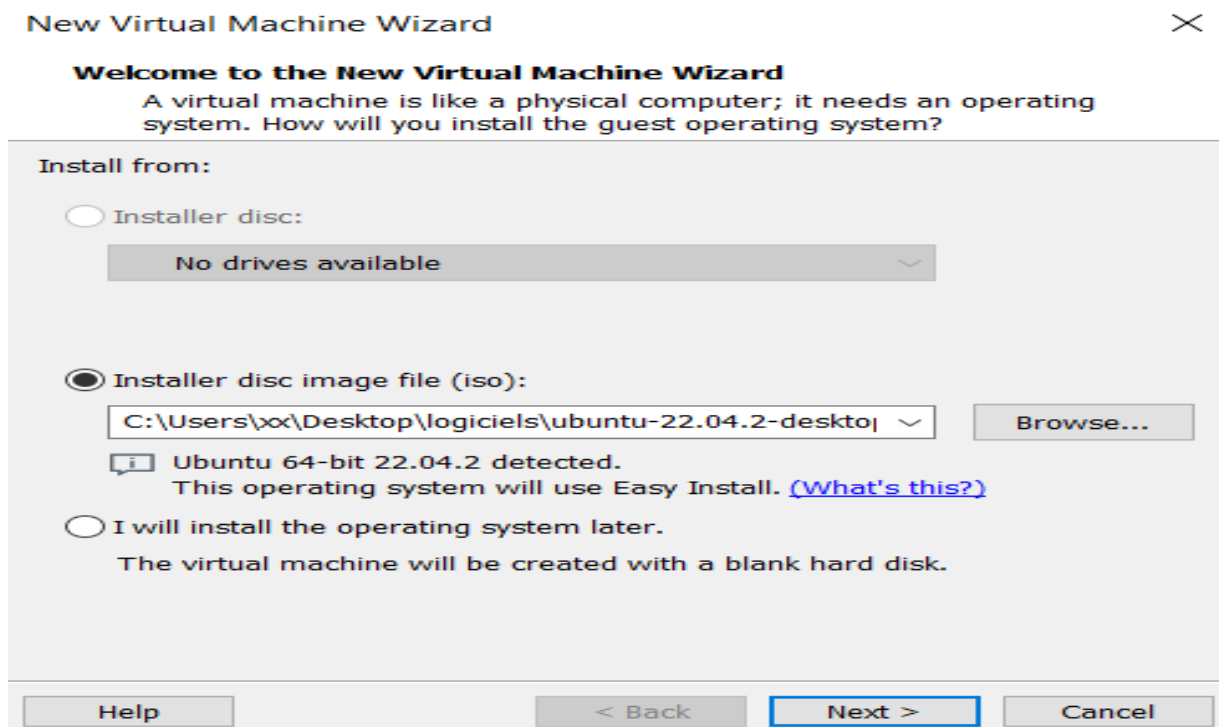
#### ❖ Tutoriels

- [29] <https://www.udemy.com/course/zabbix-6-2023/> cours payant (44,99 \$) complet de zabbix, consulté régulièrement entre juin et septembre.
- [30] [https://www.youtube.com/watch?v=UuEx\\_JwNI2s&t=1160s](https://www.youtube.com/watch?v=UuEx_JwNI2s&t=1160s) consulté le 12, 13,14,15 juillet 2023.
- [31] [https://www.youtube.com/watch?v=Keyui\\_0e5H4&list=PLhr5ujubO71OVNhUzRYBjpLHS2zP4356](https://www.youtube.com/watch?v=Keyui_0e5H4&list=PLhr5ujubO71OVNhUzRYBjpLHS2zP4356) consulté durant le mois de juillet.

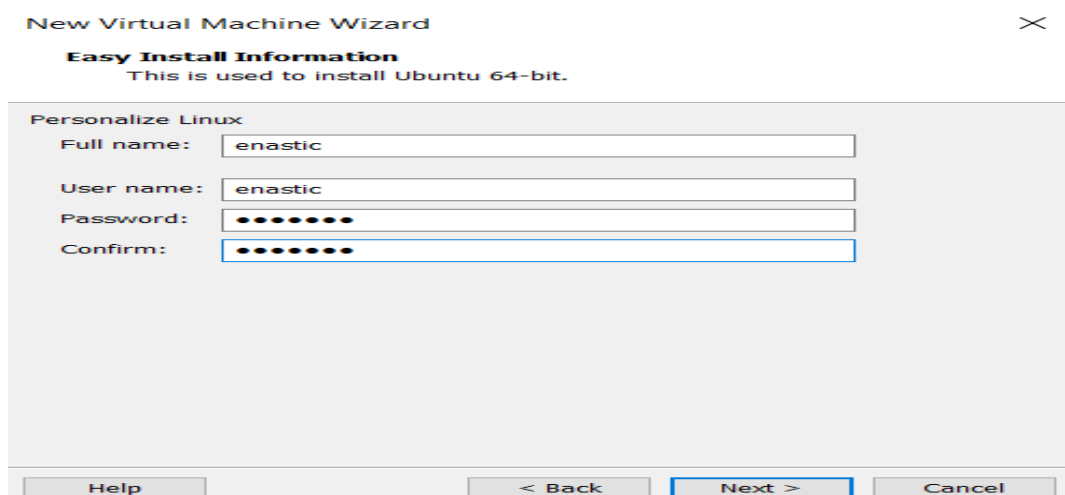
# ANNEXES

## ANNEXES A : Installation Ubuntu 22.04 (jammy)

Pour installer Ubuntu sous VMware workstation 17 on doit choisir l'image ISO pour choisir la version comme le montre la figure.



Puis sur NEXT on se retrouve sur la fenêtre suivante

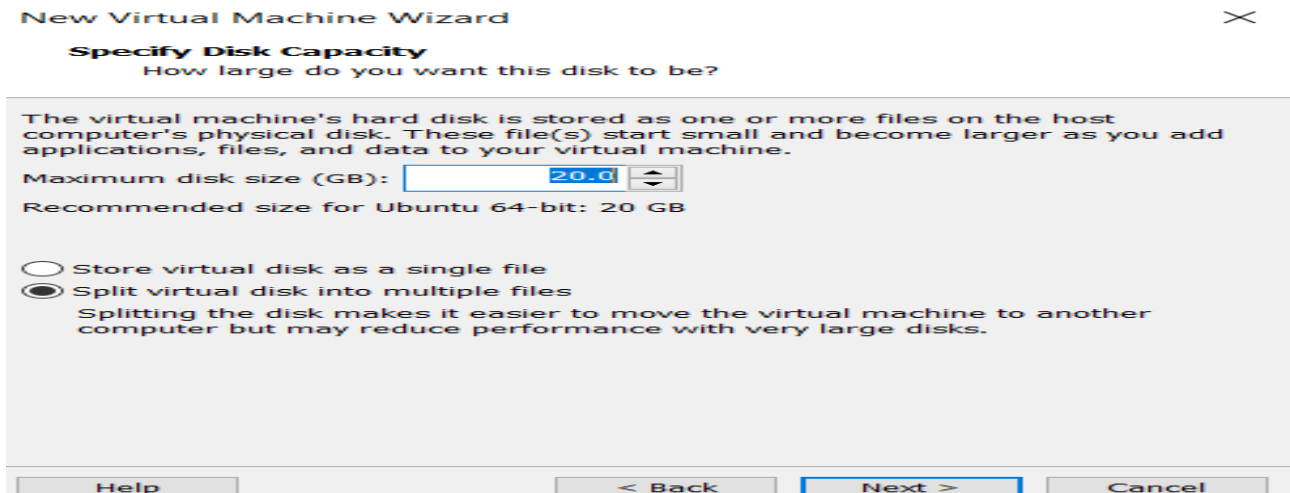


Sur ces champs on donne :

- Un nom complet ;
- Un nom d'utilisateur ;
- Un mot de passe ;
- Confirmation du mot de passe.



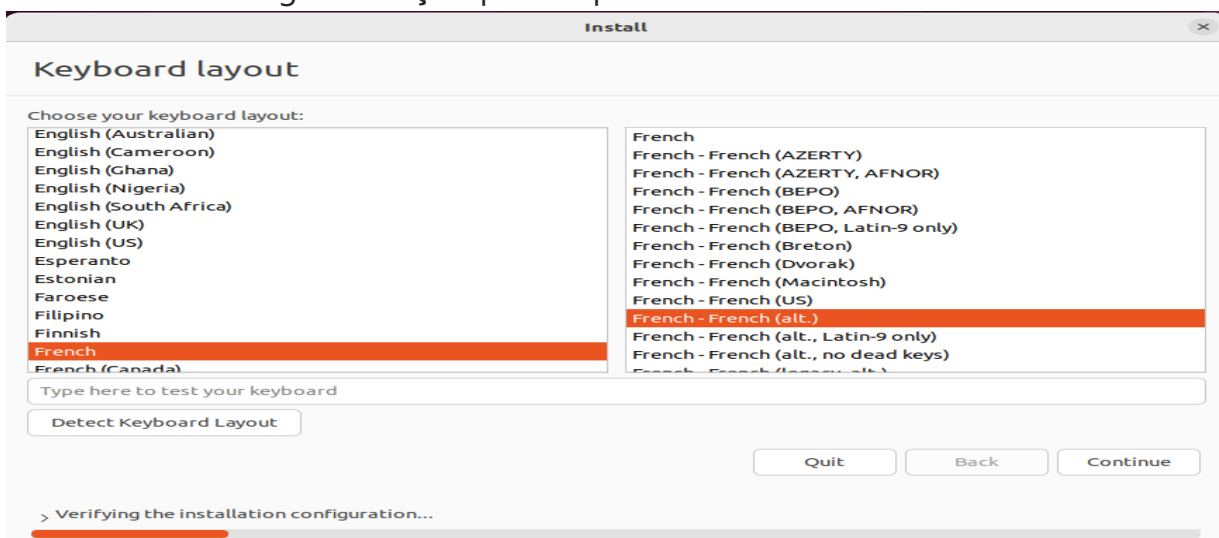
Puis sur next on se retrouve sur



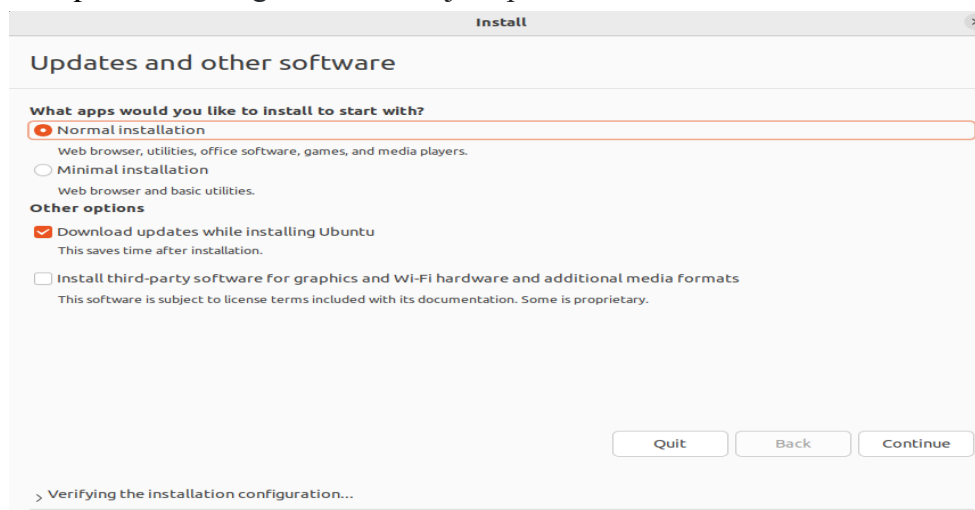
Cette fenêtre montre comment choisir la taille du disque pour notre cas nous avons pris 20 GB

Puis sur next.

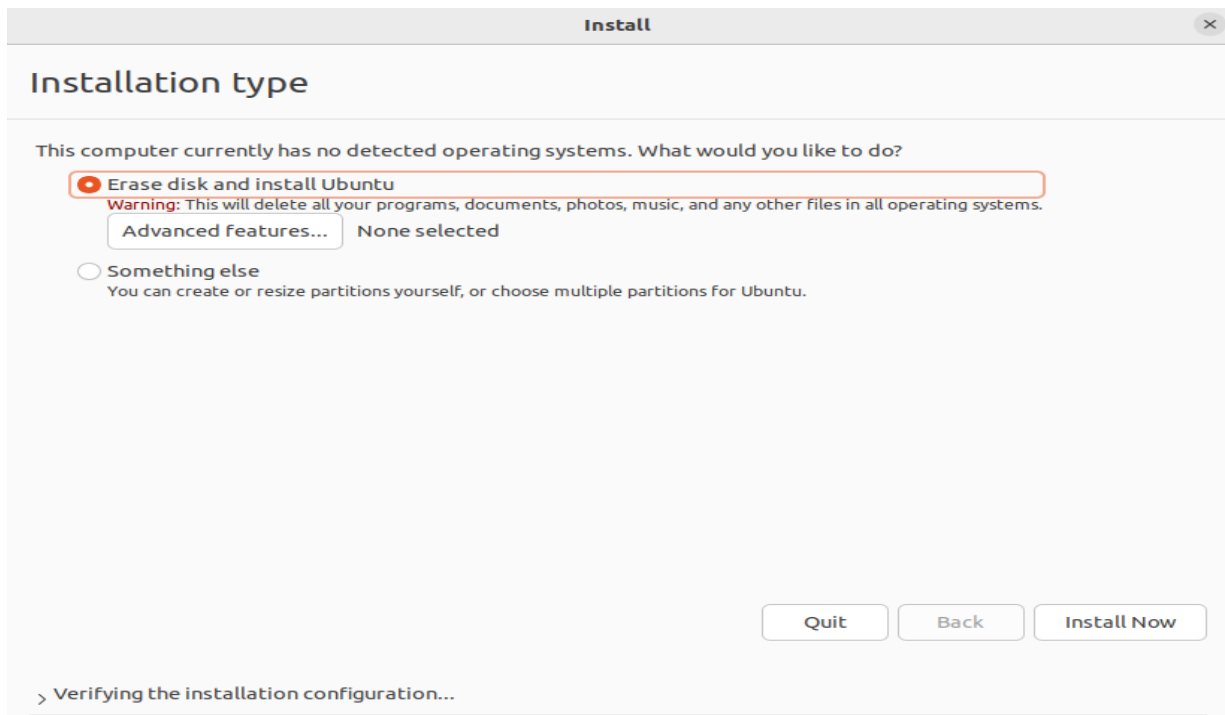
Sélectionnez la langue **Français** puis cliquez sur le bouton **Installer maintenant**.



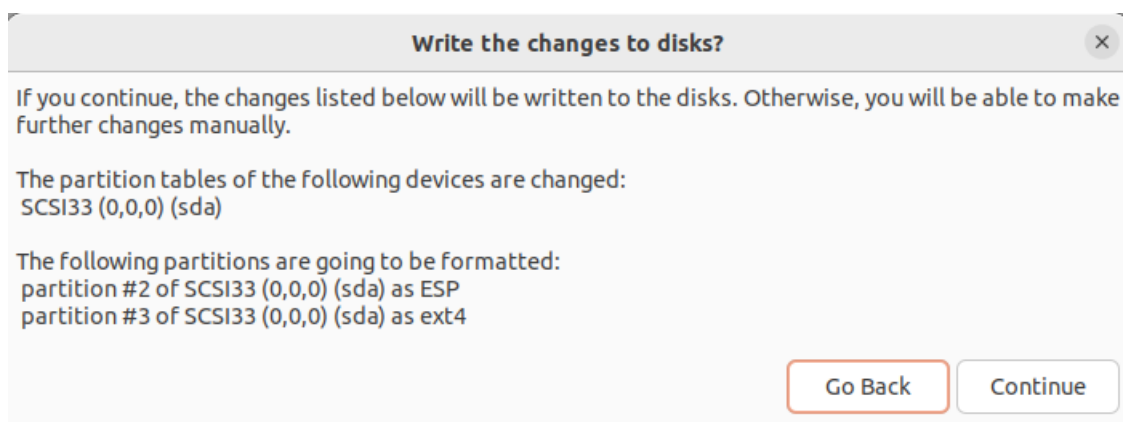
Puis sur continue pour Télécharger les mises à jour pendant l'installation de Ubuntu.



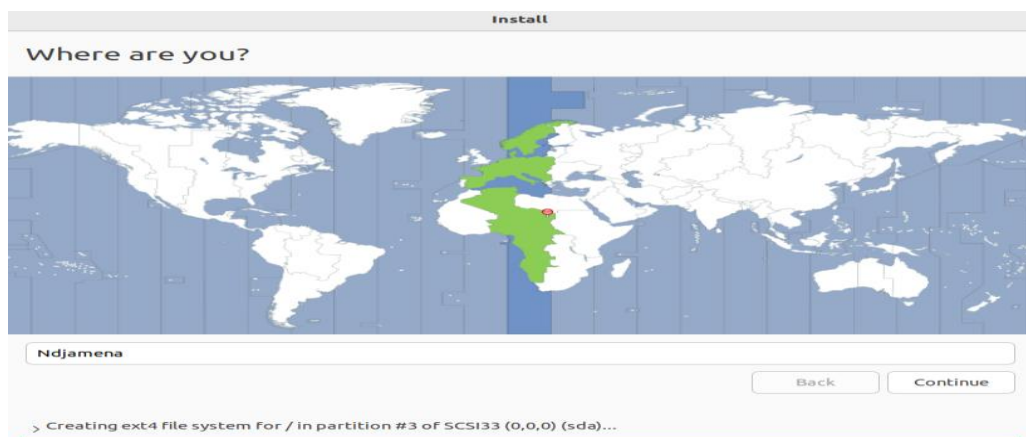
Sélectionnez **Effacer le disque et installer Ubuntu**. Puis cliquez sur **Installer maintenant**. Attention, toutes les données présentes sur votre disque seront définitivement effacées !



Validez le formatage du disque en cliquant sur **Continuer**.

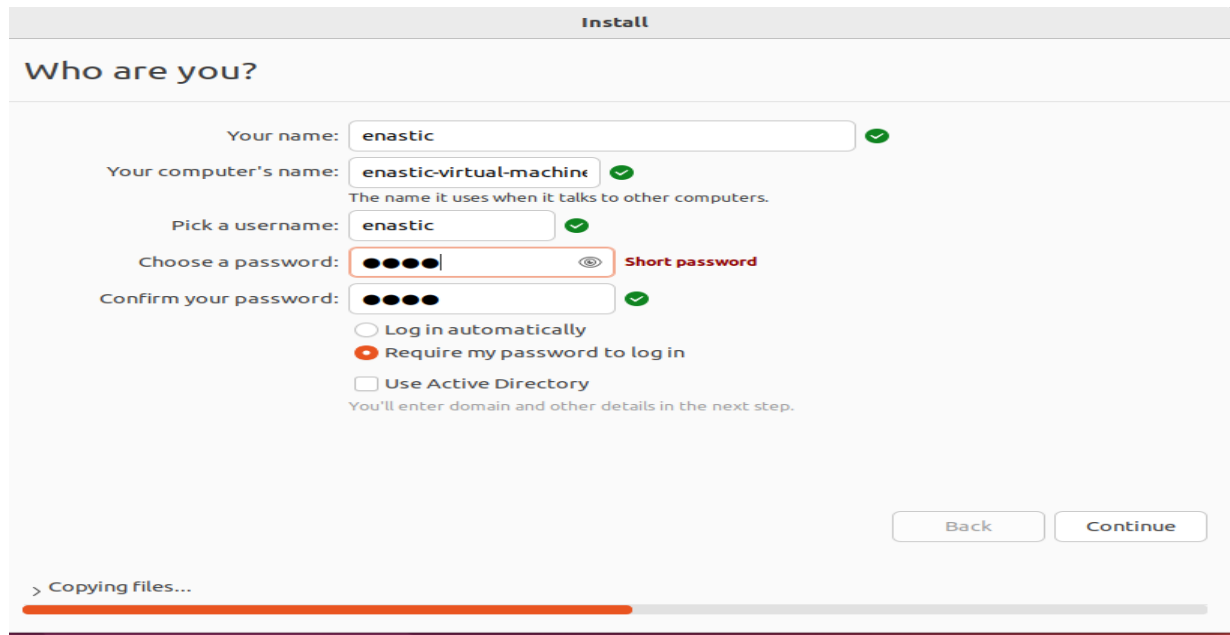


En suite Sélectionnez votre **pays** puis faites **Continuer**.



Pour notre cas nous avons choisi N'Djamena

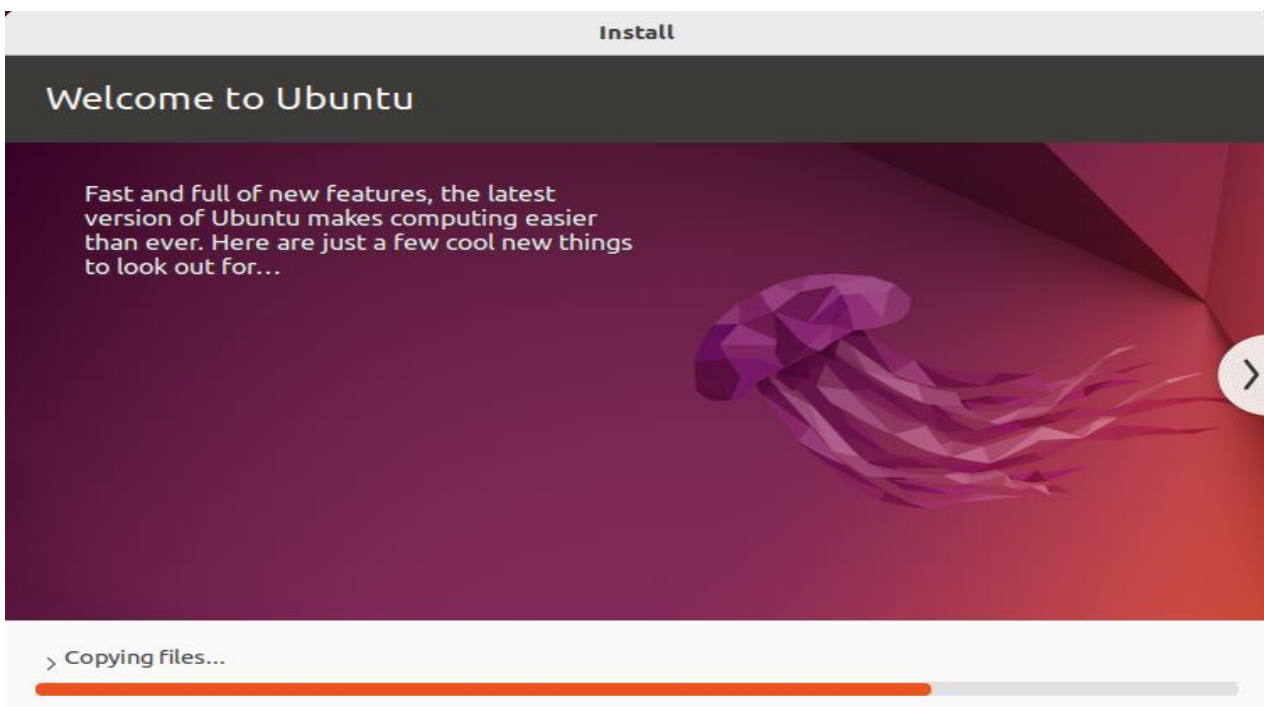
Entrez votre nom d'utilisateur, votre mot de passe, le nom du PC, puis cliquez sur **Continuer**.



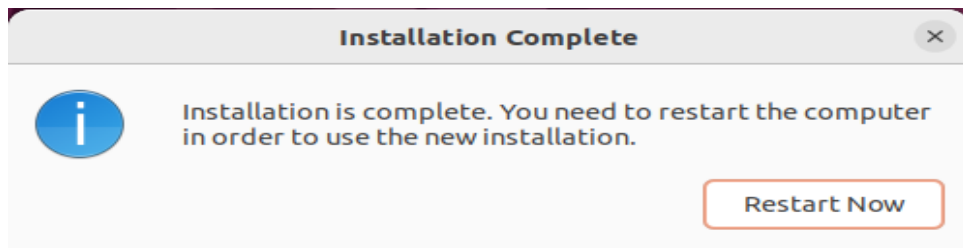
The screenshot shows the 'Who are you?' configuration screen in the Ubuntu installer. The title bar says 'Install'. The main heading is 'Who are you?'. There are several input fields: 'Your name:' with the value 'enastic' and a green checkmark; 'Your computer's name:' with the value 'enastic-virtual-machine' and a green checkmark, with a sub-note 'The name it uses when it talks to other computers.'; 'Pick a username:' with the value 'enastic' and a green checkmark; 'Choose a password:' with a masked password and a red warning 'Short password'; and 'Confirm your password:' with a masked password and a green checkmark. Below these are three radio button options: 'Log in automatically' (unselected), 'Require my password to log in' (selected), and 'Use Active Directory' (unselected). A note at the bottom says 'You'll enter domain and other details in the next step.' At the bottom right are 'Back' and 'Continue' buttons. At the bottom left, there is a progress indicator for 'Copying files...' with a partially filled orange bar.

L'installation d'Ubuntu 22.04 LTS commence !

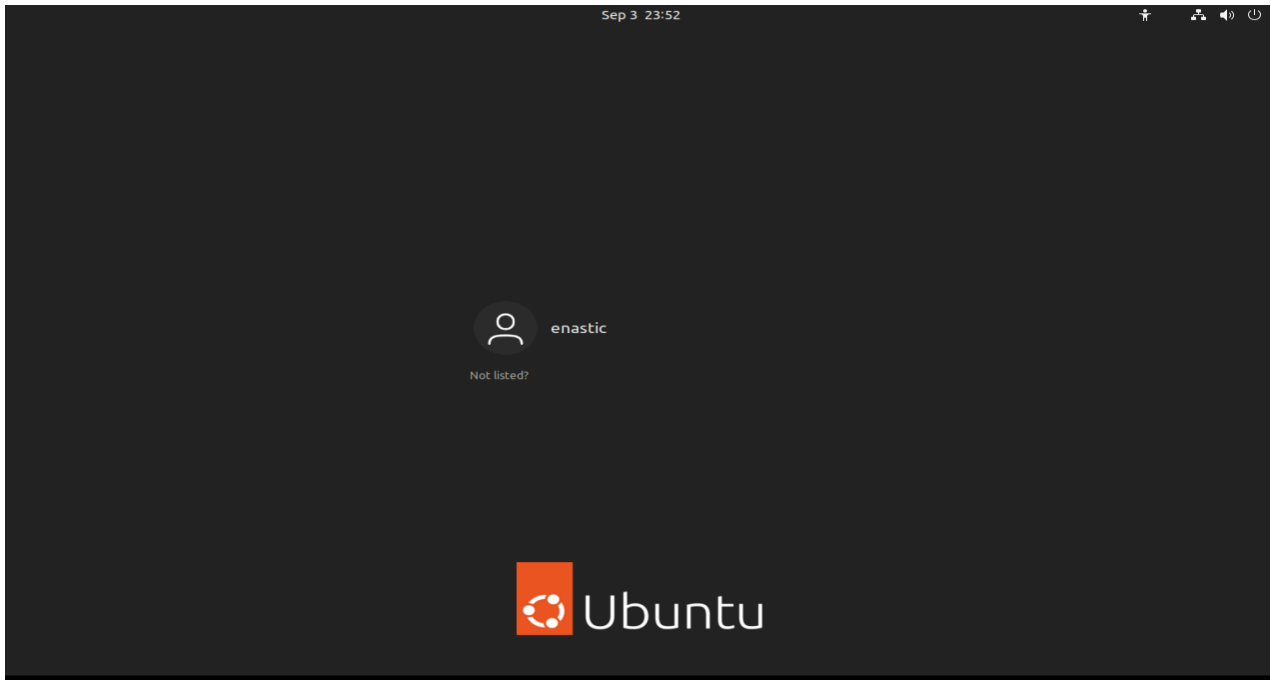
L'installation prend plus ou moins de temps selon les performances de votre système (CPU, SSD ou HDD...).



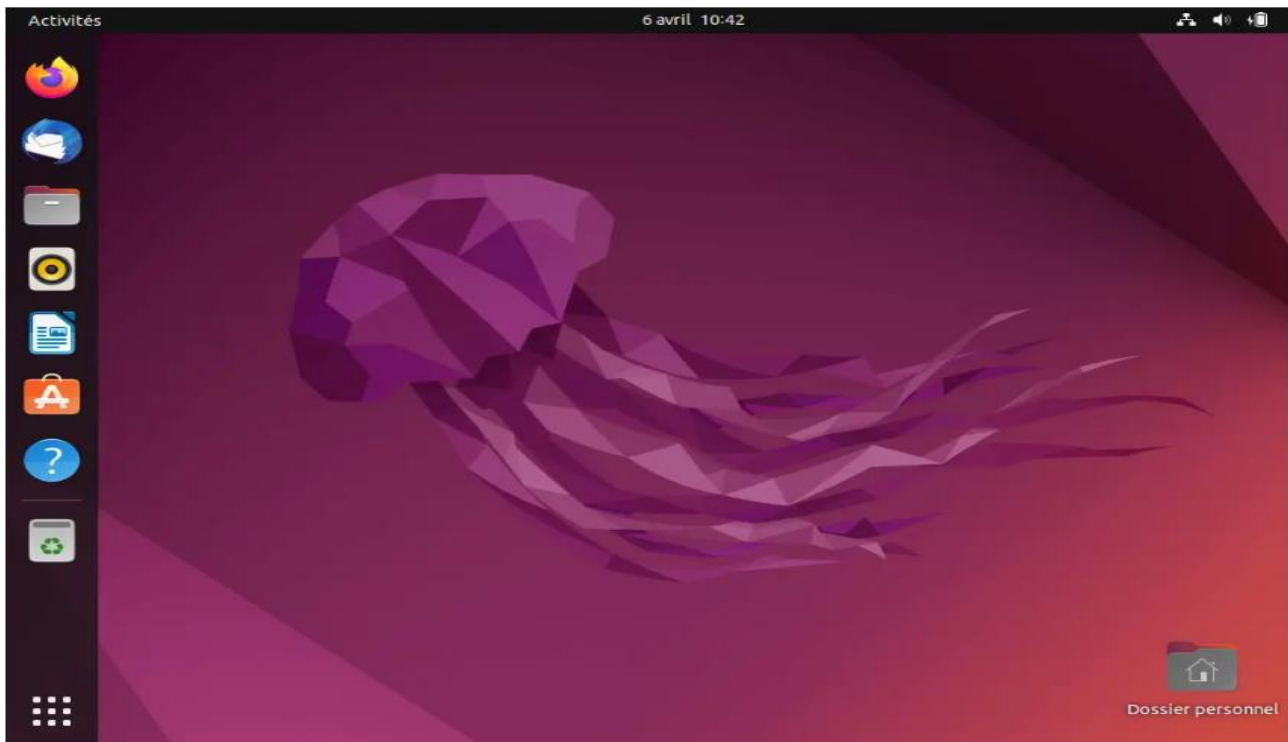
Une fois l'installation terminée, cliquez sur **Redémarrer maintenant** pour redémarrer votre PC.



À l'ouverture de session, connectez-vous avec votre compte utilisateur (enastic).



Bienvenue sur **Ubuntu 22.04 LTS** ! 😊




## ANNEXE B : installation VMware

**Étape 1 :** Allez à VMware sur Academic Software et cliquez sur le bouton Solliciter en haut à droite pour obtenir votre compte.

Dans les deux jours, vous recevrez un e-mail avec vos données de connexion.

**Étape 2 :** Cliquez sur le bouton 'Télécharger VMware Workstation Pro' pour vous connecter au portail avec vos données de connexion que vous avez reçues par e-mail.

**Étape 3 :** Ouvrez le fichier d'installation de VMware Workstation Pro.

 VMware-workstation-full-17.0.0-20800274 22/06/2023 14:12 Application 622 471 Ko

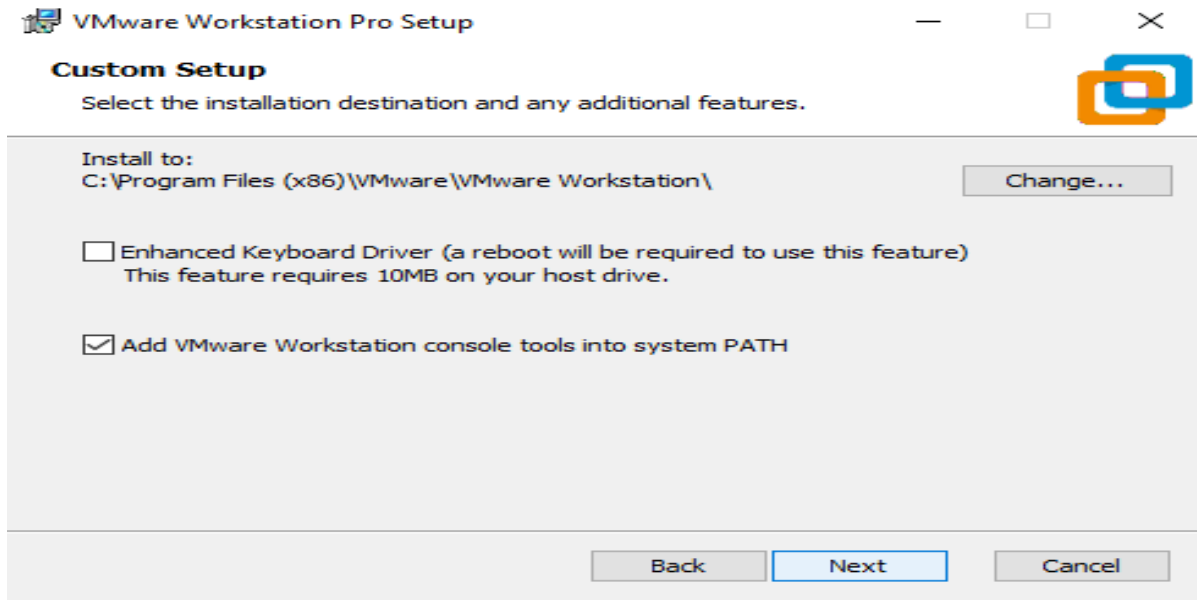
**Étape 4 :** Cliquez sur Next



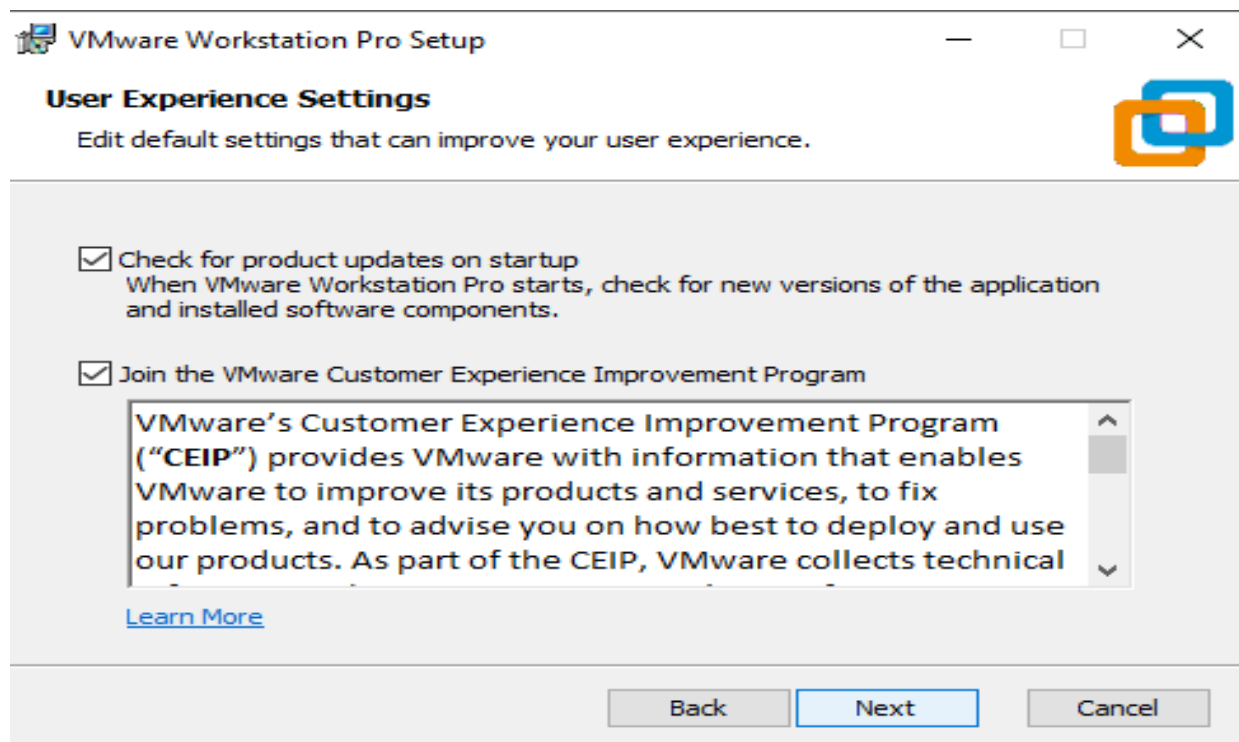
**Étape 5 :** Acceptez le contrat de licence.



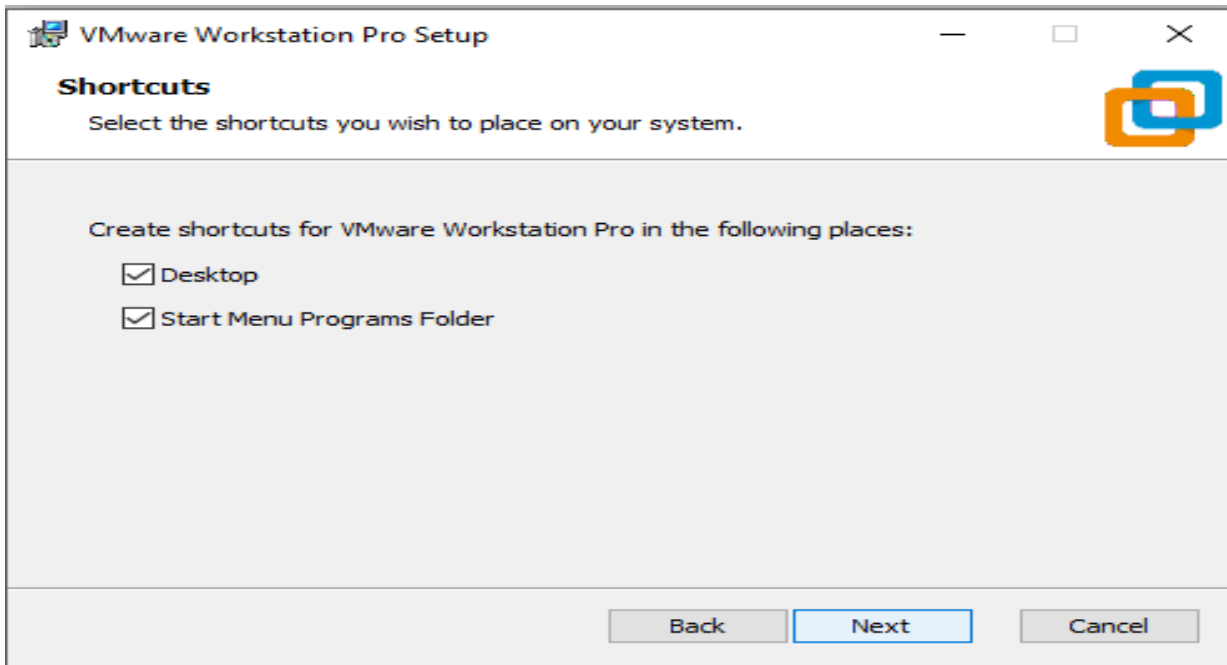
**Étape 6 :** Choisissez le lieu souhaité pour l'installation et cliquez sur Next.



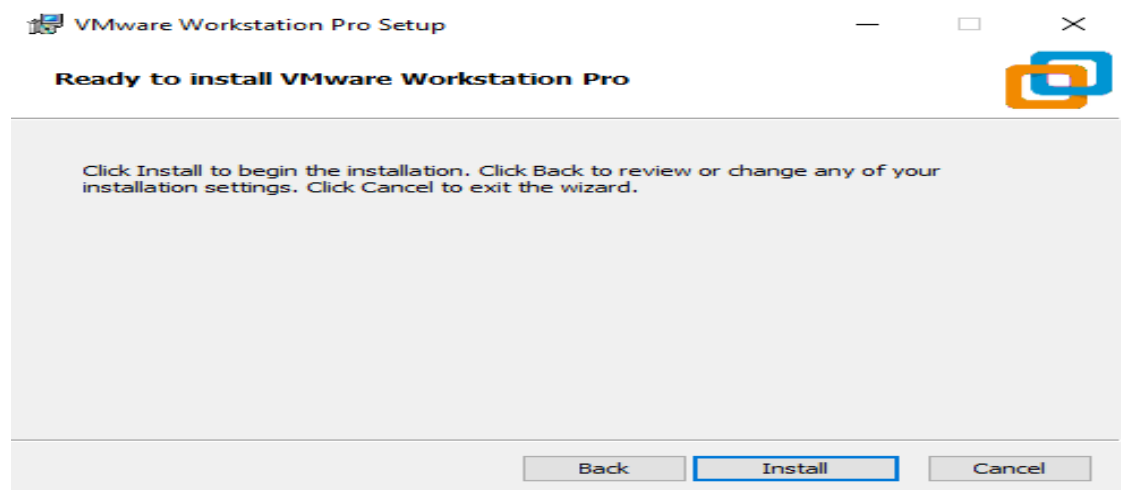
**Étape 7 :** Cochez les options si vous le souhaitez et cliquez sur Next.



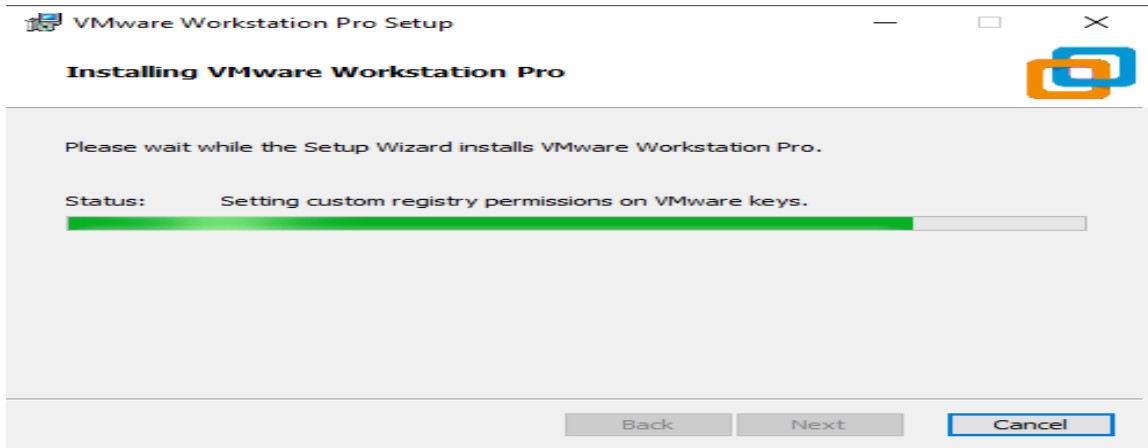
**Étape 8 :** Cliquez sur Next.



**Étape 9 :** Cliquez sur Install. La durée de l'installation dépend de la puissance de votre ordinateur.



**Étape 10 :** Installation de VMware.



**Étape 11 :** installation complète du Vmware workstation

