الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière Télécommunications

Spécialité Réseaux & Télécommunications

Présenté par

MERZOUG Chaima

&

ESSID Hakima

Installation et test d'un système de monitoring d'infrastructure réseaux (ZABBIX)

Proposé par : Dr. MEHDI Merouane et Mr. YALAOUI Moussa

Année Universitaire 2020-2021

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

En second lieu, nous tenons à remercier grandement Mr MEHDI Merouane, Directeur du centre de calculs et enseignant au département d'Electronique, spécialité Réseaux et Télécommunications, pour nous avoir accompagné durant tout notre cursus dans cette spécialité, et qu'il a su croire en ce projet et nous a fait confiance pour le mener à bien.

Ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de Mr YALAOUI Moussa ingénieur au sein du centre de calculs l'université, qui nous a fait l'honneur de nous encadrer dans ce mémoire.

Nous remercions vivement aussi tous les membres de ce jury, dont Mr ZAIR et Mr KABIR qui nous ont fait l'honneur de participer au jury pour l'intérêt qu'ils ont bien voulu porter à ce travail, en apportant leur valeureuse contribution en tant qu'experts et profond connaisseur du domaine (Réseaux et Télécommunications).

Merci à nos familles, Il nous est impossible d'exprimer en quelques mots tout ce que nous devons, pour leurs encouragements et leur appui moral qui nous ont permis de mener à bon terme ce travail.

Enfin, nos remerciements vont à tous ceux qui nous ont soutenus ou qui, d'une manière ou d'une autre, ont contribué à l'élaboration de ce travail.

Chaima et Hakima.

Dédicace

C'est avec une profonde gratitude et des mots sincères, que je dédie ce modeste travail de fin d'étude à ma raison de vivre, à mes très chers parents, merci de m'avoir toujours supportée dans mes études, votre confiance et surtout merci pour tout votre amour.

A mon père qui a sacrifié sa vie pour ma réussite et a éclairé mon chemin avec ses conseils avisés à sa patience sans limite, ses encouragements, son aide.

A ma mère, le meilleur aide que j'ai eue dans mes moments difficiles, elle était toujours là pour moi avec sa prière dans chaque étape que je devais faire, elle m'a donné tout le soutien dont j'avais besoin, merci maman, j'espère qu'un jour tu seras fière de moi, et que tu serais la fille que tu voulais que je sois.

A mes frères Samir, Ahmed, Zinedine, à tous ma famille il est difficile d'exprimer mes sentiments envers eux en de simples mots ; Merci pour votre amour et vos encouragements.

A tous mes amis, et à mon binôme merci pour votre attention merci pour tout.

A tous ceux qui nous ont aidé de près ou de loin

Je vous adresse ma plus profonde gratitude.

Chaima

Dédicace

C'est avec une profonde gratitude et sincères mots que je dédie ce modeste travail de fin d'études :

A mes parents, que Dieu me les garde :

Ma chère mère Malika pour sa gentillesse, son affection, sa douceur, sa tendresse, ses encouragements éternels et sans elle rien n'aurait pu être possible.

Mon cher père Mohammed pour son encouragement, sa patience, son aide continuelle sur le long chemin de mes études et son soutien financier.

A mes sœurs : Fidaa, Farahnez et Ikram. A mon binôme et à tous mes amis à qui je souhaite beaucoup de bonheur et de réussite dans leurs vies.

Et enfin, à tous ceux qui ont cru en moi et qui m'ont aidé à réaliser ce travail.

Hakima.

ملخص:

في اي شركة حديثة تمثل البنية التحتية للشبكة المعلوماتية مجموع الاجهزة و البرامج التي يجب عليها العمل بشكل كامل و دائم .لذلك يقوم الاشراف على تكنولوجيا المعلومات بالتدخل من اجل استباق المشاكل و تجميع المعلومات الخاصة بحالة مختلف هده الاجهزة . زابكس هو حل من بين الحلول التي تقوم بالإشراف على الشبكة المعلوماتية وعلى جميع الاجهزة التي لها عنوان ايبي و تستعمل البروتوكولات اس ان ام بي , اي بي ام اي و جي ام اكس, للإبلاغ عن الحالة الصحية لمختلف معدات الشبكة. البرنامج زابكس كان الحل المفتوح المصدر الامثل لتلبية حاجياتنا بفضل بنيته القوية الفعالة و القابلة للتطوير.

كلمات المفاتيح : البنية التحتية, الشبكة المعلوماتية, الاشراف, المفتوحة المصدر, زابكس, اس ان ام بي, اي بي ام اي, جي ام اكس

Résumé :

Dans chaque entreprise moderne, l'infrastructure réseau représente l'ensemble de matériels et logiciels qui doivent fonctionner pleinement et en permanence. La supervision informatique intervient alors et permet d'anticiper les problèmes et de faire récolter des informations sur l'état des équipements. ZABBIX est l'une des solutions de supervision réseau et de tout équipement qui a une adresse IP et qui utilise les protocoles SNMP, IPMI et JMX pour remonter les informations de l'état de santé des équipements du réseau. Le logiciel ZABBIX est la solution open source qui a le mieux répondue à nos besoins et contraintes, grâce à son architecture robuste, performante et évolutive.

Mots clés : Infrastructure, réseau, supervision, open source, Zabbix, SNMP, IPMI, JMX

Abstract:

In every modern enterprise, the network infrastructure represents the set of hardware and software that must operate fully and continuously. The IT supervision then intervenes and makes it possible to anticipate problems and to escalate information on the condition of the equipment. ZABBIX is one of the network monitoring solutions and any equipment that has an IP address and uses SNMP, IPMI and JMX protocol to report information on the health status of network equipments. The ZABBIX software is the open source solution that best meets our needs and constraints, thanks to its robust, efficient and scalable architecture.

Keywords : Infrastructure, network, monitoring, open source, Zabbix, SNMP, IPMI, JMX

Listes des acronymes et abréviations

ACL: Access Control List.

AMD: Advanced Micro Devices.

API: Application Programming Interface.

ARP: Address Resolution Protocol.

AT: Adresse Translation.

ATM: Asynchronus Transfer Mode.

BMC: Baseboard Management Controller.

CPU: Central Processing Unit.

CSS: Cascading Style Sheets.

DHCP: Dynamic Host Configuration Protocol.

DMTF: Distributed Management Task Force.

DNS: Domain Name System.

DSI: Direction des Systèmes d'Informations.

EGP: Exterior Gateway Protocol.

EIGRP: Enhanced Interior Gateway Routing Protocol.

FQDN: Fully Qualified Domain Name.

FRU: Field Replaceable Unit.

FTP: File Transfer Protocol.

GNU: General Public License.

HTML: HyperText Markup Language.

HTTP: HyperText Transfer Protocol.

HTTPS: HyperText Transfer Protocol Secure.

IBM: International Business Machines.

ICMP: Internet Control Message Protocol.

IETF: Internet Engineering Task Force.

IGP: Internal Gateway Protocol.

IMAP: Internet Message Access Protocol.

IP: Internet Protocol.

IPMI: Intelligent Platform Management Interface.

IPMB: Intelligent Platform Management Bus.

ISO: International Organisation for Standardisation.

IT: Information Technology.

JMX: Java Management Extensions.

LAN: Local Area Network.

L2TP: Layer 2 Tunneling Protocol.

MAC: Medium Access Control.

MAN: Mertropolitan Area Network.

MIB: Management Information Base.

MPLS: Multiprotocol Label Switching.

MRTG: Multi Router Traffic Grafer.

NMS: Network Management System.

NNTP: Network News Transfer Protocol.

OID: Object Identifier.

OS: Operating System.

OSI: Open Systems Interconnection.

OSPF: Open Shortest Path First.

PAN: Personal Area Network.

PHP: Hypertext Preprocessor.

POP: Point Of Presence.

POS: Personal Operating Space.

QoS: Quality of Service.

RAID: Redundant Array of Independent Disks.

RAM: Random Access Memory.

RFC: Request For Comments.

RIP: Routing Information Protocol.

RLE: Réseau Local d'Entreprise.

RRD: Round Robin Database.

RMCP: Remot Management Control Protocol.

SAN: Storage Area Network.

SDA: Small Computer System Interface Disk.

SDH: Synchronus Digital Hierarchy.

SDR: Sensor Data Record.

SEL: System Event Journal.

SFP: Small From-factor Pluggable.

SGBD : Système de Gestion de Base de Données.

SLA: Service Level Agreement.

SMB: Server Message Block.

SMS: Short Message Service.

SMTP: Simple Mail Transfer Protocol.

SNMP: Simple Network Management Protocol.

SOAP: Simple Object Access Protocol.

SQL: Structured Query Language.

SSH: Secure Shell.

TCP: Transmission Control Protocol.

TELNET: Terminal Network.

TFTP: Trivial File Transfer Protocol.

TLD: Top Level Domains.

UC: Unité Centrale.

UDP: User Data Protocol.

URL: Uniform Resource Locator.

VM: Virtual Machine.

VPN: Virtual Private Network.

VPS: Virtual Private Server.

WAN: Wide Area Network.

Table des matières

Liste des figures

Liste des tableaux

De jours en jours, les réseaux de transmission de données ne cessent de s'accroitre, cela est dû au volume de données échangées qui s'augmente de plus en plus. Tout est désormais informatisé, les réseaux informatiques sont partout, de nombreuses entreprises et administrations quel que soit leurs domaines d'activités mettent en place aujourd'hui des infrastructures réseau plus performantes afin d'assurer la fiabilité du service et l'accès permanent à l'information à tous les niveaux (systèmes informatiques, terminaux utilisateurs, serveurs d'applications…) [**1**].

L'administrateur réseau doit donc surveiller en permanence son infrastructure réseau, car une perte de connexion à un nœud engendre des pertes préjudiciables sur l'activité, l'économie et sur la notoriété de l'entreprise. Elle consiste principalement à assurer la surveillance au quotidien du comportement du réseau par la supervision de l'ensemble de matériels et logiciels qui le constituent, ainsi que définir des procédures et des tableaux de bord de suivi. La supervision permet donc d'avoir une vue globale du fonctionnement de toute l'infrastructure réseau informatique afin de résoudre les éventuels incidents et pannes pouvant survenir.

Une supervision efficace passe donc par des outils de monitoring qui centralisent l'information de la santé du réseau pour le compte des directions des systèmes d'informations. Ces outils devront assurer en premier lieu la surveillance des équipements et des ressources du réseau, et en second lieu, ils permettront de détecter de façon rapide les pannes pouvant affecter ces équipements. Tout évènement déclenché par un nœud quelconque du réseau devra être remonté dans le logiciel.

La gestion du réseau est donc un aspect important de chaque entreprise et pour obtenir un logiciel de surveillance de réseau qui fonctionne vraiment peut être un obstacle en raison des coûts élevés des plans et des prix. En contrepartie, Il y en a d'autres qui sont heureux de servir les entreprises sans rien demander en retour, c'est là que Zabbix appartient.

Il s'agit d'un logiciel de surveillance de réseau de niveau entreprise qui fonctionne pour toutes les infrastructures, services, applications et ressources

informatiques. Il a été conçu pour fonctionner en temps réel sur des serveurs, des périphériques réseau et même sur des machines virtuelles rassemblant des métriques à partir de millions de ces nœuds de réseau.

Zabbix est une solution open source conçue pour ceux qui ont un large réseau à gérer mais qui n'ont pas grand budget à dépenser.

Ses outils et ressources permettent de collecter et d'analyser les performances grâce à des mesures et des statistiques pouvant être visualisées tout en envoyant des alertes et des notifications sur les problèmes en cours afin que les solutions puissent être déployées rapidement [**2**].

Dans ce qui suit, nous allons étudier dans le premier chapitre l'infrastructure des réseaux informatiques ainsi que les différents matériels et logiciels qui le constituent. Par la suite, et dans le deuxième chapitre, nous allons détailler la supervision réseau ainsi que les différents protocoles qui interviennent dans cette dernière. Dans le troisième chapitre nous allons présenter le logiciel ZABBIX et ces différentes fonctionnalités ensuite nous allons montrer l'application et le test du bon fonctionnement de cette solution dans le quatrième chapitre.

A la fin nous allons conclure notre mémoire par une conclusion générale et quelques perspectives pour ce projet de fin d'études.

Chapitre I : Infrastructure du réseau informatique

I.1 Introduction

L'infrastructure réseau est indispensable pour la rentabilité de toute entreprise sérieuse. Elle doit donc être étudiée et minutieusement déployé afin de garantir un bon fonctionnement de l'ensemble de ces logiciels et matériels. Dans ce chapitre nous allons découvrir l'importance de l'infrastructure informatique ainsi que ces différents éléments qu'on doit assurer leurs performances.

I.2 Présentation d'une infrastructure réseau

En invoquant le terme infrastructure informatique, l'on se réfère incontestablement sur l'ensemble des logiciels et éléments matériels qui forment le système informatique d'une entreprise ou d'une organisation. Autrement dit, l'infrastructure informatique s'apparente à l'ensemble des équipements informatiques indispensables pour la bonne marche des sociétés. Il s'agit entre autres du service d'archivage en ligne, les diverses applications logicielles et le réseau d'entreprise. Cette structure permet sans doute de soutenir sa croissance car les sociétés y voient un centre névralgique de leur activité [**3**].

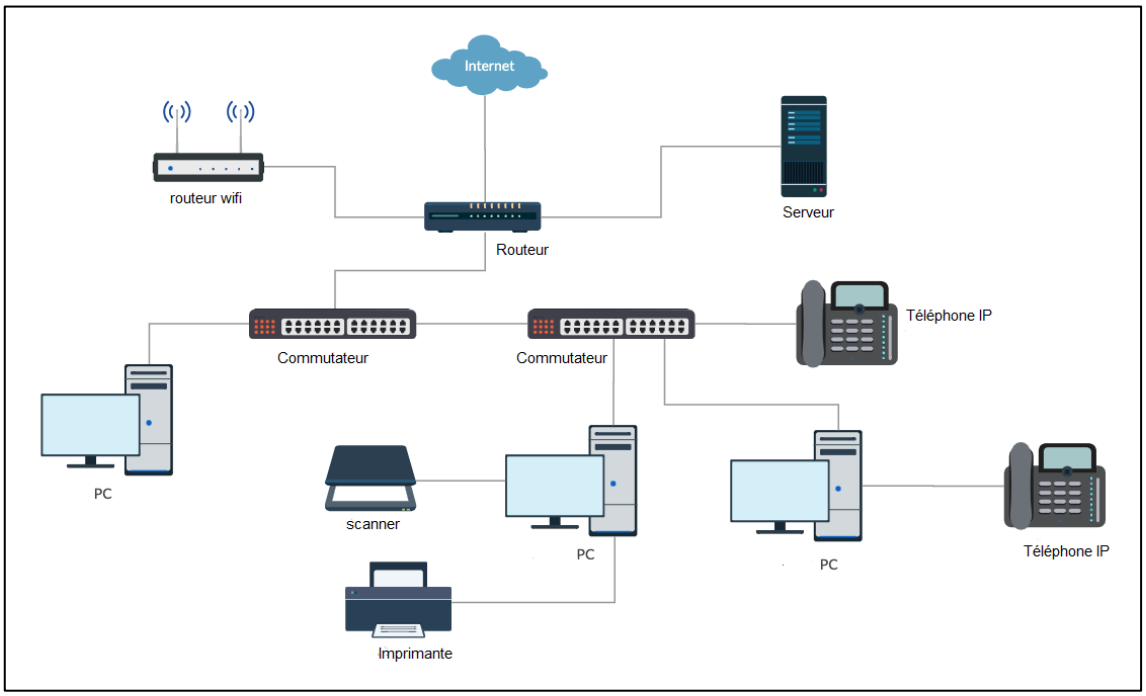


***Figure I.1**:* Infrastructure réseau [4].

I.3 Définition d'un réseau informatique

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services.

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Un réseau est constitué d'équipement appelés nœuds. Ces réseaux sont catégorisés en fonction de leur étendue et de leur domaine d'application.

Pour communiquer entre eux, les nœuds utilisent des protocoles, ou langages compréhensibles par tous [**4**].

I.4 Topologies de réseaux informatiques

Les réseaux sont qualifiés en fonction de leur étendue géographique :

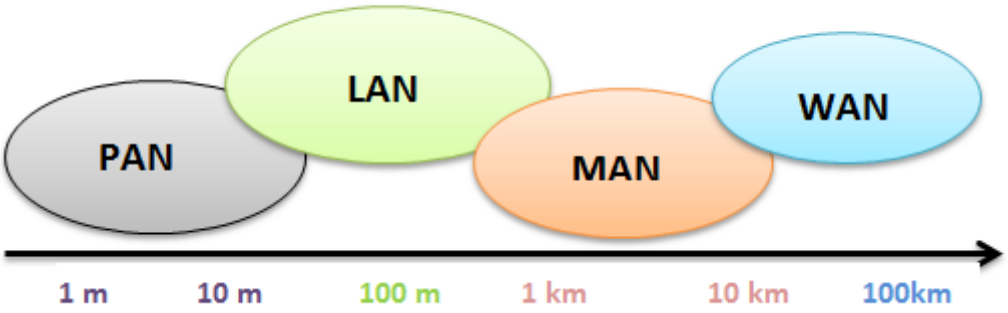


Figure I.2 : Topologies de réseaux informatiques.

I.4.1 Réseau personnel

La plus petite étendue de réseau est nommée en anglais Personal Area Network (PAN). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space (POS) [**4**].

I.4.2 Réseau local

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français Réseau local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs… Il est couramment utilisé pour le partage de ressources communes comme des périphériques, des données ou des applications [**4**].

I.4.3 Réseau métropolitain

Le réseau métropolitain ou Metropolitan Area Network (MAN) est également nommé réseau fédérateur.il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètres [**4**].

I.4.4 Réseau étendu

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constituées de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux [**4**].

I.5 Réseau Privé virtuel (VPN)

Un réseau privé virtuel ou VPN (Virtual Privat Network) est un réseau de communication virtuel qui utilise l'infrastructure d'un réseau physique pour relier logiquement les systèmes informatiques. Les données sont transférées au sein d'un tunnel virtuel qui est construit entre un client VPN et un serveur VPN.

Le réseau public est utilisé comme moyen de transport, les réseaux privés virtuels sont généralement cryptés pour s'assurer de la confidentialité des données. Les VPN sont utilisés pour connecter les réseaux locaux sur Internet ou pour permettre l'accès à distance à un réseau ou à un seul ordinateur via la connexion publique [**5**].

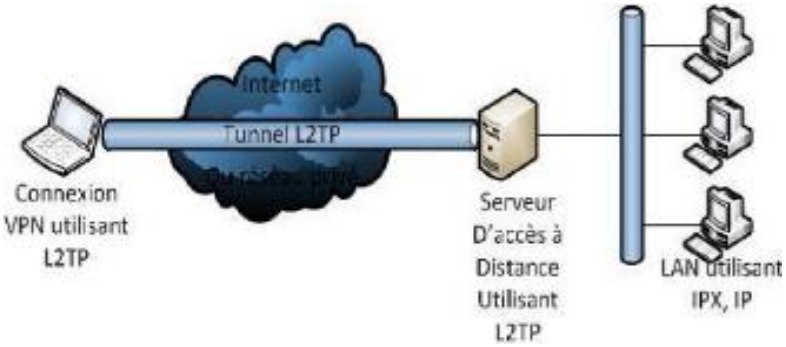


***Figure I.3*:** Réseau privé virtuel [**6**].

I.6 Réseau MPLS

Multiprotocol Label Switching (MPLS) est une norme récente, proposée par l'IETF, combinat à la fois le routage de niveau 3, comme le fait IP, et la commutation de niveau 2, exploitée dans le Frame Relay ou l'ATM.

Les services de couche 3 OSI offerts par le standard MPLS sont importants, tout en offrant des débits conséquents. Très flexible, il permet d'intégrer différents protocoles de couche 3 OSI, dont, IPV4 et IPV6. Non lié à une technique de niveau 2, il se montre indépendant de l'infrastructure et peut utiliser les services d'ATM, Frame Relay, SDH, Ethernet…etc.

MPLS est conçu pour permettre facilement la qualité de service (QoS- Quality of Service) durant les transports, cela pour tout type de données. Comme ATM, il exploite l'agrégation de flux en réduisant au maximum le nombre de connexions, afin de gagner en efficacité [**7**].

I.7 Equipements physiques d'une infrastructure réseau

Les équipements réseau, ou périphériques réseau, sont les équipements physiques nécessaires à la communication et à l'interaction entre les appareils d'un réseau informatique.

I.7.1 Répéteur

Il agit au niveau de la couche physique du modèle OSI. Il permet d'étendre la longueur maximale d'un segment, en amplifiant le signal, en même temps qu'il permet d'interconnecter deux supports physiques différents.

Il n'est pas capable de travailler au niveau sémantique du contenu d'une trame, cependant il est capable de détecter une collision et de la propager de l'autre côté.

Travailler au niveau 1, il n'est pas capable non plus, d'interconnecter des brins fonctionnant à des vitesses différentes.

On parle désormais de fonction de répéteur incorporée à un élément actif du réseau et plus vraiment de composant dédié [**4**].

I.7.2 Concentrateur (Hub)

Le Hub, est un équipement informatique opéré au niveau de la couche physique du modèle OSI. Il est utilisé dans les réseaux locaux pour connecter plusieurs machines, il permet de diffuser les données sur l'ensemble des ports.

I.7.3 Pont

Un pont (bridge) agit au niveau de la couche Liaison de données. Il permet ainsi de lier deux ou plusieurs supports physiques différents, à condition que les mêmes formats d'adresses MAC soient utilisés des deux côtés.

Un pont autorise l'extension d'un réseau dont l'étendue maximale a été atteinte avec des répéteurs [**4**].

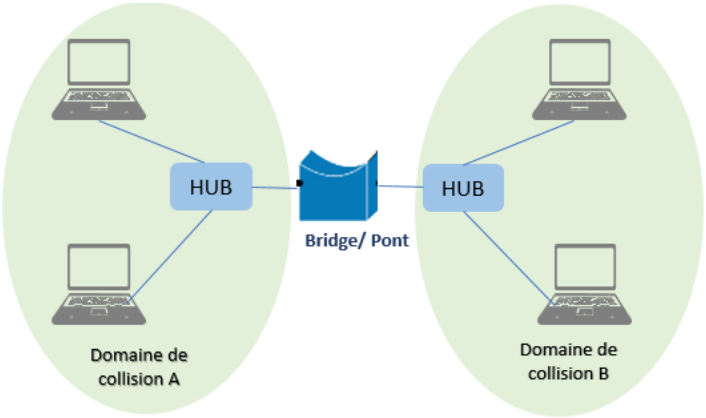


Figure I.4: Implémentation d'un pont sur un réseau.

I.7.4 Commutateur

Le commutateur (switch) est un équipement de réseau qui permet de connecter différents éléments du système informatique dans un réseau. Il intègre à la fois une fonction de concentrateur et une fonction de pont (pont multiport).

Le commutateur est désormais comme un composant clé dans les réseaux locaux. Dans tous les réseaux récents, les postes de travail et serveurs sont directement reliés à de tels équipements. Il est désormais très rare d'utiliser des équipements dédiés de concentrateur ou de ponts.

Ainsi, le réseau n'a plus une caractéristique de diffusion, mais est qualifié de commuter.

Les commutateurs sont catégorisés en fonction de leur capacité de traitement vis-à-vis du modèle OSI. Ils sont capables d'exploiter les adresses MAC des ordinateurs connectés à leurs ports, et les commutateurs d'étage, sont capables de reconnaitre les adresses IP [**4**].

I.7.4.1 Différents types des commutateurs

Il existe différents types de modèles : les non-administrables, les « intelligents » et enfin les administrables.

- **Commutateur non-administrable** : Ce type de commutateur est de réseau Ethernet, il ne dispose pas d'interface de programmation. Il se branche directement sur le réseau, car toute la programmation est déjà faite.
- **Commutateur intelligent :** Ce commutateur peut être programmable ou non programmable, il dispose d'un ensemble de capacités tels que le routage, la sécurité, la virtualisation de stockage.
- **Commutateur administrable :** Utilisé dans la couche principale où se trouvent toutes les données importantes d'un réseau. Les commutateurs administrables peuvent gérer des réseaux VLAN, de gérer le routage interne etc.

I.7.4.2 Ports du commutateur

Un commutateur disposant de plusieurs ports, peut contenir de 2 jusqu'à 48 ports, ces ports sont des ports **RJ45** qui sont utilisés dans les réseaux locaux, et qui permettent de connecter les équipements du réseau à l'aide d'un câble à pair torsadé. Et des ports **SFP/SFP+** qui permettent l'interconnexion à l'aide d'une liaison en fibre optique.

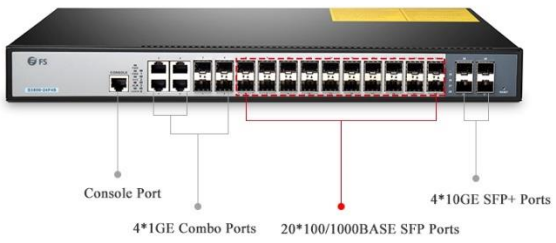


Figure I.5: Différents types des ports du commutateur ***[8]***.

I.7.5 Passerelle

La passerelle est considérée comme un dispositif permettant de faire la liaison entre deux réseaux informatique différents, ce matériel qui opère au niveau des couches 3 à7 peut être un routeur, un pare-feu, un serveur proxy.

Caractéristiques de la passerelle :

- Elle permet d'agir comme une traductrice de couches moyennes et autres : table de caractères, caractéristiques internationationaux [**4**].
- Elle permet d'éviter d'installer des composants réseau sur chaque client, en offrant un accès universel qui minimise l'hétérogénéité du réseau [**4**].

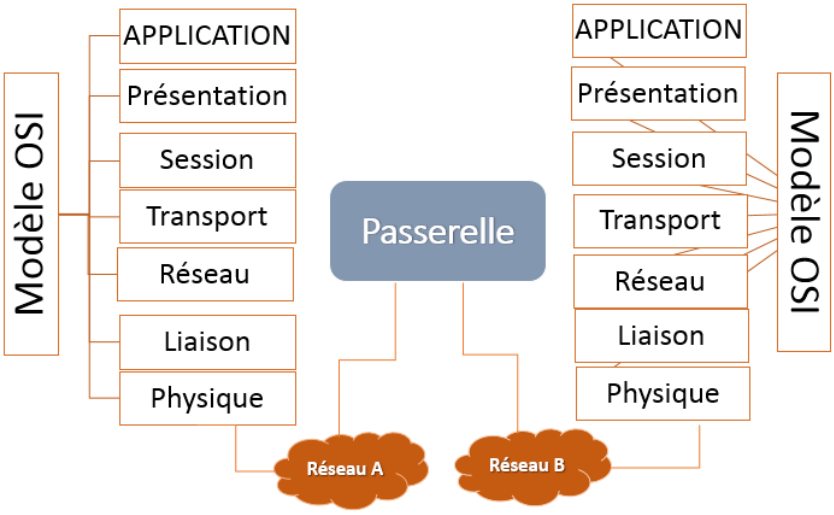


Figure I.6 : Principe de passerelle.

I.7.6 Routeur

Un routeur est un périphérique de réseaux informatiques utilisé pour rôle d'acheminer un paquet de données d'un réseau à travers un autre réseau, il permet d'assurer le routage entre le réseau local et internet en utilisant l'adresse IP [**4**].

Les routeurs doivent connaître l'ensemble des chemins pour atteindre une destination. Ils s'appuient sur une table de routage où toutes les informations sont stockées (Les chemins, Next Hop, L'interface, La métrique) pour guider le transfert des paquets vers sa destination.

I.8 Protocoles de communication avec le monde extérieur

I.8.1 RIP

Routing Information Protocol est un protocole de routage dynamique utilisé pour trouver le meilleur chemin entre la source et la destination en utilisant le nombre de sauts comme métrique de routage (nombre de routeurs) [**9**].

I.8.2 EIGRP

Enhanced Interior Gateway Routing Protocol est un protocole de routage

intérieur dynamique, développé par Cisco et classé comme un protocole à vecteur de distance, qui permet d'échanger des informations sur différents routeurs après avoir choisi le meilleur chemin.

Ce protocole ne dépend que des Neighbors qui lui sont directement connectés [**9**].

I.8.3 OSPF

Open Shortest Path First est un protocole de routage intérieur (IGP, "Internal Gateway Protocol") de type état de liaison, développé par l'IETF, son but est de trouver le meilleur chemin entre la source et la destination [**9**].

Chaque routeur a une vue d'ensemble des réseaux d'une zone, en cas de changement sur le réseau, le routeur envoie l'information en multidiffusion à tous les autres hôtes OSPF.

I.9 Protocoles d'administration

I.9.1 SNMP

SNMP (protocole simple de gestion de réseau) Protocole de communication et de gestion proposé par l'IETF, repose sur une structure simple, permet aux administrateurs d'administrer le matériel réseau (commutateurs, serveur etc.), superviser et diagnostiquer les éléments administrés et de faire la gestion des applications à distance (base de données, les logiciels etc) [**9**].

I.9.2 ICMP

Internet Control Message Protocol est un protocole de couche Internet utilisé par les périphériques réseau pour diagnostiquer les problèmes de communications réseaux. L'ICMP est principalement utilisé pour déterminer si les données atteignent ou non leur destination prévue en temps voulu. Généralement, le protocole ICMP est utilisé sur des périphériques réseau, tels que les routeurs [**10**]**.**

ICMP est aussi un protocole d'administration disponible par défaut sur tous les systèmes d'exploitation.

I.9.3 Protocole Telnet

TELNET (Telecommunication Network, terminal network ou Teltype network) définit un protocole Internet standard qui fonctionne selon une architecture

client/serveur basée sur le port TCP 23 [**11**], permettant de communiquer avec un serveur distant sur la base d'échanges de lignes de texte.

I.10 Serveur informatique

Un serveur informatique offre des services accessibles via un réseau. Il peut être matériel ou logiciel, c'est un ordinateur qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client ». C'est pourquoi on entend souvent parler de relation « client/serveur ». Par exemple, un utilisateur (côté client) va rechercher un site internet en utilisant un navigateur web, pour que ce dernier puisse l'afficher il va effectuer une requête au serveur HTTP qui est un serveur web [**12**].

I.10.1 Fonctionnement du serveur informatique

Côté fonctionnement, le serveur informatique apporte, de façon automatique, une réponse à la requête d'un client en respectant tout un ensemble de codifications et de protocoles réseau. Il exerce sa mission en toute autonomie et en toute permanence, 24 heures sur 24, pour pouvoir offrir une continuité du service.

Les serveurs disposent de leur propre système d'exploitation, calibré en fonction de la puissance de calcul que demande leur unité centrale. Certaines fonctionnalités sont communes entre le serveur et son système d'exploitation. C'est le cas par exemple des contrôles d'identité ou d'accès, des fonctions proxy ou pare-feu et autres protocoles DHCP [**13**].

I.10.2 Différents types des serveurs

Qu'il s'agisse d'une base de données d'entreprise ou d'un site Internet, il est toujours nécessaire de disposer d'un serveur adapté. Pour cela, il convient de savoir que les serveurs sont de trois sortes. En savoir un peu plus en détail sur ces types de serveurs [**14**].

I.10.2.1 Serveur mutualisé

Le serveur mutualisé réunit de nombreux espaces d'hébergement sur un même serveur. Concrètement, il consiste à héberger sur une seule et même machine de nombreux sites web. Dans ce cas, les espaces sont délimités pour pouvoir accueillir différents sites.

I.10.2.2 Serveur dédié physique

Ce type de serveur donne accès à une machine réelle qui est dédiée à son propre site, ce qui nécessite la prise en main et l'autonomie. Dans ce cas, les performances de l'hébergement seront fonction de la configuration matérielle de la machine louée.

I.10.2.3 Serveur dédié virtuel

Le serveur dédié virtuel ou virtual private server (VPS) est une machine virtuelle hébergée sur un serveur assez puissant, notamment un cloud. Ce type de serveur offre une grande flexibilité et une plus grande réactivité. Avec cette solution, il est possible d'allouer plus de ressources à son activité de manière très réactive [**15**].

I.10.3 Caractéristiques d'un serveur

Les serveurs utilisent la même architecture ou configuration de base que l'ordinateur de bureau. Toutefois, un serveur possède des fonctionnalités matérielles avancées caractérisées par :

I.10.3.1 Carte mère

La carte mère, est le circuit imprimé principal de l'ordinateur auquel sont connectés tous les autres composants du serveur. Les principaux composants de la carte système comprennent le processeur (CPU ou UC), un circuit microprogrammé appelé la puce, la mémoire, des connecteurs d'extension, un contrôleur de disque dur et des ports d'entrée/sortie (E/S) pour connecter des périphériques, tels que des claviers, souris et imprimantes [**16**].

I.10.3.2 Processeur

Le processeur est le centre névralgique du serveur. La vitesse et le nombre de processeurs du serveur ont un impact considérable sur sa capacité à prendre en charge les applications. L'évolution des processeurs étant constante, il n'est pas facile de déterminer lequel est le mieux adapté à une application particulière. Trois caractéristiques principalaux sont à prendre en compte dans le choix d'un processeur [**16**].

a. Vitesse d'horloge

Il s'agit de la vitesse de fonctionnement du processeur, habituellement mesurée en gigahertz (GHz). En général, plus la vitesse d'horloge d'un serveur est élevée, plus il est performant [**16**].

b. Nombre de cœurs

Il s'agit du nombre de processeurs physiques contenus dans le processeur. Aujourd'hui, la plupart des processeurs serveur possèdent deux ou quatre cœurs. Les serveurs équipés de plusieurs cœurs offrent de meilleures performances de traitement multitâche pour exécuter plusieurs applications [**16**].

c. Taille de la mémoire cache

Chaque processeur possède une mémoire à accès rapide intégrée située directement sur et à proximité de l'unité centrale (UC). Une mémoire cache de grande taille réduit la fréquence de récupération des données par le processeur à partir de la mémoire système située hors de ce dernier. Avec la plupart des applications, cela améliore la réactivité du système et offre par conséquent plus de satisfaction aux utilisateurs [**16**].

I.10.3.3 Mémoire

A l'ouverture d'un fichier ou d'un document, le serveur a besoin d'un emplacement temporaire pour en assurer le suivi. Il utilise des puces à grande vitesse spécialisées, appelées mémoire à accès aléatoire (RAM, Random Access Memory). Le fichier enregistré, est placé sur le disque dur. La mémoire RAM est conçue pour accélérer l'accès au fichier et retrouver rapidement son emplacement de stockage sur le disque dur permanent [**16**].

I.10.3.4 Stockage ou disques durs

Les disques durs mettent à la disposition du serveur une vaste bibliothèque contenant l'ensemble des fichiers accessibles. Il s'agit en quelque sorte d'une armoire de classement extensible à l'infini. La taille et le type des disques durs dépendent de la quantité de données à stocker [**16**].

I.10.3.5 Alimentation

Le serveur comportant généralement plus de périphériques qu'un ordinateur de

bureau ordinaire, il a besoin d'une alimentation plus élevée (en général, 300 Watts). Lorsque le serveur est équipé de nombreux disques durs, il peut nécessiter une alimentation encore plus importante [**16**].

I.11 Services offerts par les serveurs

I.11.1 Service de fichiers

Les premières formes d'informations manipulées à travers les applications réseaux sont les fichiers. Ils sont stockés dans des arborescences de dossiers (Windows), de répertoires (UNIX/LINUX) …Les services de fichiers effectuent quatre fonctions essentielles :

- **Transfert de fichiers :** il sert à l'échange d'informations en utilisant le courrier électronique et les utilitaires de transfert de fichier. En plus du partage des informations, ce service permet la sécurisation d'accès aux fichiers.
- **Stockage de fichiers et migration des données :** Le stockage centralisé permet de rentabiliser au mieux des équipements parfois onéreux. De plus, l'unité de stockage peut alors être choisie suivant les besoins, le temps d'accès, la fiabilité, la durée de vie du support.
- **Synchronisation de la mise à jour de fichiers** : Lorsqu'une modification intervient puis est enregistrée sur le serveur, la dernière sauvegarde remplace la dernière version du document. Il est alors essentiel de savoir à quel moment les dernières modifications ont eu lieu pour disposer de la version la plus récente.
- **Archivage :** Afin de se prémunir contre des pannes potentielles, il est nécessaire de mettre en place une stratégie d'archivage des données sensibles. Les informations sont copiées sur des supports hors-ligne [**7**].

I.11.2 Service d'applications

Il permet non seulement le partage des données mais aussi celui de la puissance de traitement. L'objectif principal est la spécialisation des serveurs en inter réseau, de manière à répartir au mieux les taches sur les machines les plus appropriées.

Le client demande l'exécution d'un programme se trouvant sur le serveur (sous forme d'une requête) ; le programme est exécuté sur le serveur et le résultat renvoyé au client (sous forme d'une réponse). Ainsi, c'est le processeur du serveur qui travaille

pour le client. C'est pour cela qu'un serveur d'application nécessite surtout beaucoup de puissance de traitement.

Le serveur d'application est défini comme un serveur conçu pour fournir le contexte d'exécution des applications aux ordinateurs clients [**4**].

I.11.3 Service WEB

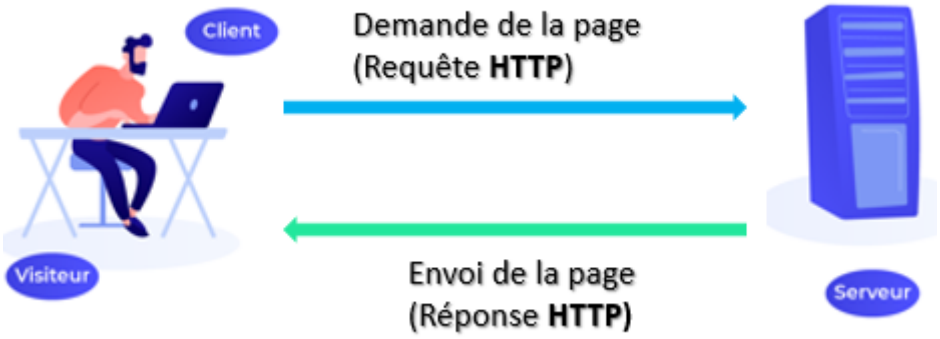


Figure I.7 : Echange de requêtes entre client-serveur.

Un serveur WEB possède deux significations Software ou Hardware :

Software : est un logiciel, utilise le serveur http qui prend en compte les URL et le protocole http pour répondre aux demandes de client [**17**].

Hardware : un serveur informatique héberge des informations sous forme de pages de texte HTML, des fichiers Java, des feuilles de style CSS et des pages web pour les traiter et les livrer à des clients sous forme HTML sur un réseau public (internet) ou privé (intranet).

I.11.4 Service DNS

Le Domain Name System est un service dont la principale fonction est d'associer un nom de domaine à son adresse IP, ce service permettant d'établir une correspondance entre un site web et une adresse IP.

Le nom de domaine totalement qualifié ou FQDN (Fully Qualified Domain Name) est l'identifiant unique d'un hôte sur internet.

La structure d'un FQDN est constituée de plusieurs champs séparés par un point, et terminée par un point : [hôte].[sous-domaine].[TLD].

Les composants de cette adresse sont :

- L'hôte : le nom du serveur dans le domaine.

- L'arborescence d'organisation du domaine, définie par le domaine et le(s) sous-domaine(s).
- Le code TLD (Top-Level Domin) : le domaine de haut niveau.

Le FQDN peut compter au maximum 255 caractères et 127 niveaux d'arborescence, pour abus de langage, on appelle souvent « nom de domaine » le FQDN.

On appelle résolution la procédure qui permet d'obtenir l'adresse IP correspondant à un FQDN [**18**].

I.11.5 Service DHCP

Il existe deux solutions pour attribuer l'adresse IP à chaque hôte soit manuellement (configurer chaque hôte), soit dynamiquement en inscrivant les hôtes auprès d'un serveur DHCP (Dynamic Host Configuration Protocole) pour qu'à chaque démarrage ils reçoivent ces informations du serveur.

L'administrateur du réseau doit configurer uniquement le serveur DHCP pour que celui-ci distribue les paramètres souhaités :

- Plage d'adresses à affecter, accompagnée de la liste des adresses à exclure, réservées pour l'adressage fixe des serveurs et autres éléments d'infrastructure
- Masque de sous-réseau;
- Passerelle par défaut;
- Durée du bail.

Lors de l'attribution d'une adresse à un hôte, le serveur initialise la durée du bail correspondant. Pour tous les redémarrages de l'hôte pendant la durée du bail défini, la même adresse lui sera affectée [**18**].

DHCP a de nombreuses fonctionnalités dans l'administration d'un réseau telles que :

- DHCP empêche les conflits d'adresses (DHCP minimise les erreurs de configuration causées par la configuration manuelle de l'adresse IP) ;
- La possibilité de définir des configurations TCP / IP à partir d'un emplacement central ;
- La Réduction de l'administration du réseau.

I.11.6 Service de messagerie

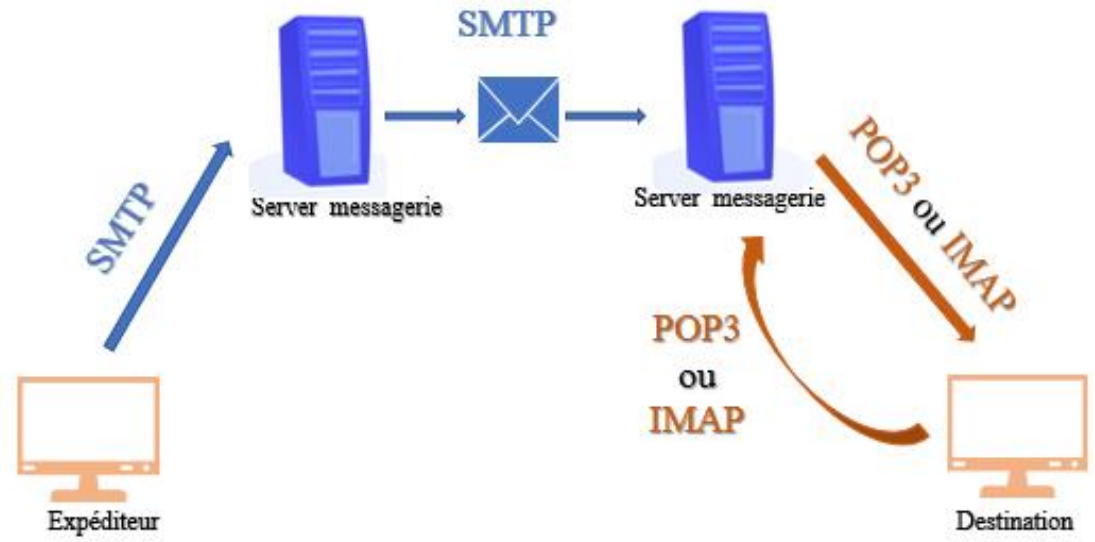


Figure I.8 **:** Principe de fonctionnement de serveur de messagerie.

Un serveur de messagerie électronique est un logiciel de courrier électronique qui s'occupe de la gestion des transferts des messages d'un serveur à un autre. Un utilisateur n'est jamais directement en contact avec ce serveur mais utilise un logiciel client, tel que Microsoft Outlook ou émulé en http (courrielleur web).

IL existe deux types de serveurs de messagerie, les serveurs de messagerie sortants et les serveurs de messagerie entrants. Les serveurs de courrier sortants sont connus sous le nom de SMTP pour le transfert de courrier. Les serveurs de messagerie entrants sont POP / IMAP pour la réception des mails [**19**].

I.12 Protocoles les plus utilisés

Le tableau suivant montre les protocoles, leur numéro de port ainsi que leur couche de fonctionnement.

Tableau I-1*:* Protocoles les plus utilisés.

Couche ISO	Protocole	N° Port
Réseau	IP	**4**
Transport	UDP	**17**
Transport	TCP	**6**
Réseau	ICMP	**1**
Réseau	OSPF	**89**
Session	DNS	**53**

Application	SNMP	**161/162**
Application	TFTP	**69**
Application	HTTPs	**443**
Application	SSH	**22**
Application	FTP	**20/21**
Application	Telnet	**23**
Application	SMTP	**25**
Application	POP3	**110**
Application	IMAP	**143**
Application	DHCP	**67/68**
Application	HTTP	**80**

I.13 Application propriétaire

I.13.1 Système de gestion de base de données

Un système de gestion de base de données (SGBD) est le logiciel qui permet à un ordinateur de stocker, récupérer, ajouter, supprimer et modifier des données. Un SGBD gère tous les aspects primaires d'une base de données, y compris la gestion de la manipulation des données, comme l'authentification des utilisateurs, ainsi que l'insertion ou l'extraction des données. Un SGBD définit ce qu'on appelle le schéma de données ou la structure dans laquelle les données sont stockées.

Le SGBD gère trois choses importantes : les données, le moteur de base de données qui permet d'accéder aux données, de les verrouiller et de les modifier, et le schéma de base de données, qui définit la structure logique de la base de données. Ces trois éléments fondamentaux contribuent à assurer la concomitance, la sécurité, l'intégrité des données et l'uniformité des procédures administratives.

Les tâches typiques d'administration de base de données prises en charge par le SGBD comprennent la gestion des changements, la surveillance/réglage des performances, la sauvegarde et la restauration [**20**].

La très grande majorité des SGBD actuels utilise SQL comme langage de commande de base.

De nombreux systèmes de gestion de base de données différents sont disponibles :

- MySQL : ce SGBD est compatible avec toutes les plateformes : Linux, UNIX, et Windows.
- Oracle Database : la base de données la plus populaire pour Linux/Unix.
- IBM DB2 : Après Oracle, IBM DB2 est la deuxième la plus utilisée sur les écosystèmes Unix/Linux.
- Microsoft SQL Server : elle est compatible exclusivement avec Windows.

I.14 Poste client

IL s'agit d'un poste connecté au réseau à partir duquel un utilisateur effectue son travail et accède aux ressources d'un serveur. La station communique avec le serveur et les autres stations grâce au réseau.

D'un point de de vue logiciel, on parlera de redirecteur ou de client. Un client est nécessairement associé à un service correspondant [**7**].

I.14.1 Caractéristiques techniques d'un poste client

I.14.1.1 Processeur

Cette puce électronique ultra-puissante est comme le cerveau de l'ordinateur, dont elle détermine d'ailleurs directement la rapidité. Pour une performance intéressante, on opte pour un processeur Intel i5 à i7 ou AMD Quad Core A8 d'au moins 3 MHz [**21**].

I.14.1.2 Disque dur

Ce dispositif stocke de manière durable les informations indispensables au fonctionnement de l'ordinateur (même une fois éteint), les programmes et les productions personnelles (documents, photos, chansons…). On choisit un modèle de grande capacité, d'au moins 1 téraoctet (To) afin d'enregistrer un grand nombre de photos, de vidéos et de fichiers [**21**].

I.14.1.3 Mémoire vive

Cet élément ne stocke que des informations dont la machine et les programmes ont besoin temporairement et leur permet d'y accéder à une vitesse supersonique. Le minimum : 4 Go de mémoire vive. À lui seul, le système d'exploitation Windows 7

utilise beaucoup d'espace de mémoire vive [**21**].

I.15 System d'exploitation

Un système d'exploitation (SE, en anglais Operating System ou OS) est un ensemble de programmes qui remplissent deux grandes fonctions à savoir : gérer les ressources de l'installation matérielle en assurant leurs partages entre un ensemble plus au moins grand d'utilisateurs et assurer un ensemble de services en présentant aux utilisateurs une interface mieux adaptée à leurs besoins que celle de la machine physique. Il est aussi un ensemble de programmes responsables de la liaison entre les ressources matérielles d'un ordinateur et les applications informatiques de l'utilisateur (traitement de texte, jeu vidéo...) [**22**]. Citons parmi les plus populaires : Windows (Le système d'exploitation le plus répandu), MacOS et UNIX.

Les rôles du système d'exploitation sont divers :

- Gestion du processeur.
- Gestion de la mémoire vive.
- Gestion des entrées/sorties.
- Gestion de l'exécution des applications.
- Gestion des droits.
- Gestion des fichiers.
- Gestion des informations [**22**].

I.15.1 Windows

Windows, qui correspond au système d'exploitation Microsoft, et en pratique représente le système d'exploitation le plus populaire. Les principaux avantages d'un système d'exploitation Windows sont attribuables au fait qu'il est facile à apprendre et à utiliser mais surtout qu'il s'agit d'un système d'exploitation universellement pris en charge. Les principaux inconvénients d'un système d'exploitation Windows sont qu'il s'agit d'un système d'exploitation payant, qui est généralement plus sujet aux virus informatiques en raison de son énorme propagation, et qui pour une raison ou une autre peut créer plus de problèmes que d'autres [**23**].

I.15.2 Linux

IL s'agit d'un système d'exploitation libre, c'est-à-dire ouvert, ou mieux encore gratuit, et qu'en plus d'offrir un large choix de programmes totalement gratuits. Le principal inconvénient d'un système d'exploitation Linux est plutôt donné par la difficulté initiale à apprendre à l'utiliser, en particulier pour les utilisateurs novices [**23**].

Il Ya beaucoup de différents types de systèmes d'exploitation Linux disponibles pour les utilisateurs, tels que Ubuntu la distribution linux la plus populaire et Debian qui est une version plus complexe.

I.15.3 MAC Os

Mac OS est un système d'exploitation à interface graphique développé par Apple.

En raison de sa nature consacrée à l'arrêt complet, macOS nécessite des pilotes et des programmes développés spécialement pour lui. Dans le même temps, cependant, macOS permet d'utiliser plus facilement tous les produits Apple, dispose d'une interface nettement plus utilisable et est également moins sujet aux virus et aux problèmes de stabilité potentiels [**23**].

I.16 Virtualisation

En informatique, la virtualisation consiste à créer une version virtuelle d'un dispositif ou d'une ressource, comme un système d'exploitation, un serveur, un dispositif de stockage ou une ressource réseau. Nous pouvons donc considérer la virtualisation comme l'abstraction physique des ressources informatiques. En d'autres termes, les ressources physiques allouées à une machine virtuelle sont abstraites à partir de leurs équivalents physiques. Chaque dispositif virtuel, qu'il s'agisse d'un disque, d'une interface réseau, d'un réseau local, d'un commutateur, d'un processeur ou de mémoire vive, correspond à une ressource physique sur un système informatique physique. Les machines virtuelles hébergées par l'ordinateur hôte sont donc perçues par ce dernier comme des applications auxquelles il est nécessaire de dédier ou distribuer ses ressources.

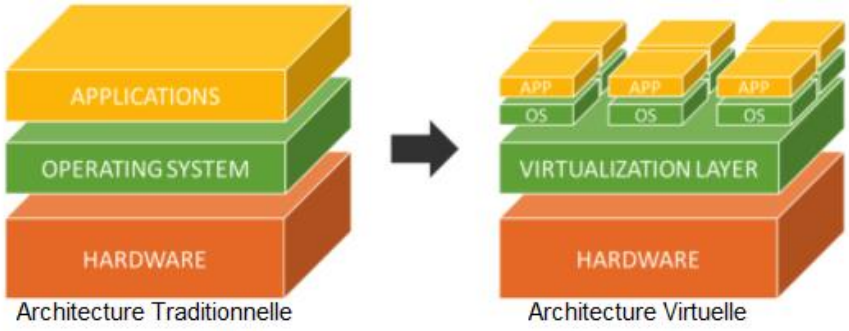


Figure I.9: Principe de La virtualisation [**24**].

Il existe de nombreux domaines d'applications à la virtualisation, s'agissant généralement de la virtualisation de serveur, de poste de travail, d'applications, de stockage et du réseau [**25**].

I.16.1 Domaine de virtualisation

I.16.1.1 Virtualisation de l'application

La virtualisation d'application est une technologie logicielle qui va permettre d'améliorer la portabilité et la compatibilité des applications en les isolants du système d'exploitation sur lequel elles sont exécutées. Elle consiste à encapsuler l'application et son contexte d'exécution système dans un environnement cloisonné. La virtualisation d'application va nécessiter l'ajout d'une couche logicielle supplémentaire entre un programme donné et le système d'exploitation ; son but est d'intercepter toutes les opérations d'accès ou de modification de fichiers [**26**].

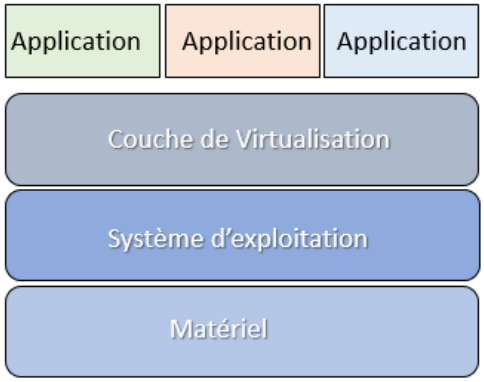


Figure I.10: Virtualisation de l'application.

I.16.1.2 Virtualisation du système d'exploitation

Ce type de virtualisation consiste à séparer le système d'exploitation (OS) d'une machine en différents environnements utilisateurs distincts. Ainsi les utilisateurs de la

machine ne se voient pas entre eux, et l'accès aux données des autres n'est pas possible. En effet ici le matériel et l'OS sont les même pour tout le monde [**27**].

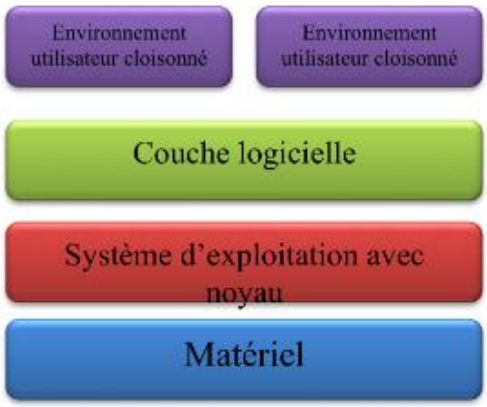


Figure I.11: Virtualisation du système d'exploitation [**27**].

I.16.1.3 Virtualisation des serveurs

La virtualisation des serveurs consiste à consolider plusieurs serveurs virtuels (qu'il s'agisse de serveurs mail, de serveurs d'applications, de serveurs de fichiers, de l'Active Directory, etc.), généralement dédiés, sur le même serveur physique, ce dernier faisant dès lors office d'hyperviseur [**25**].

Même si la virtualisation des serveurs présente de nombreux avantages, certains risques peuvent également être présents. Tous les différents serveurs sur la même machine peuvent s'arrêter si la machine hôte tombe en panne. Et dans le cas où deux serveurs communiquent entre eux après avoir été physiquement connectés à l'aide de câbles réseau mais avec la virtualisation ces opérations se font à distance et dans le logiciel, cela présente certains risques en cas d'erreurs de configuration.

I.16.1.4 Virtualisation des stations de travail

La virtualisation des postes de travail est l'évolution logique de la virtualisation des serveurs. Le poste de travail se résume à une machine virtuelle disponible sur un serveur localisé au sein du centre de données. Les utilisateurs ne font que de se connecter à cette machine virtuelle, généralement via des terminaux légers.

La figure illustre le concept décrit ci-dessus. Nous pouvons distinguer, au centre, un poste de travail virtuel situé au sein du centre de données. L'utilisateur peut accéder à cette station par le biais de tout type de client. La station de travail contient,

quant à elle, tant les applications que les données, mais également les paramétrages propres à l'utilisateur [**25**].

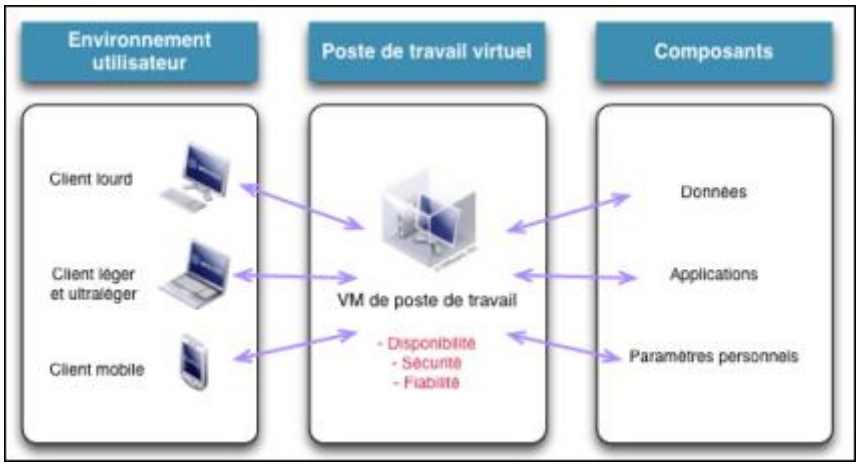


Figure I.12 : Virtualisation de stations de travail *[**25**]*.

I.16.1.5 Virtualisation du stockage

La virtualisation du stockage, appelée également abstraction du stockage, consiste à fédérer plusieurs ressources de stockage indépendantes et éventuellement hétérogènes en une ressource centralisée. Des volumes ou disques de stockage virtuels logiques sont créés à partir de ces différentes ressources et présentés par la suite aux serveurs concernés.

La virtualisation du stockage consiste en une abstraction de la couche physique du stockage, les serveurs stockant l'information sans se soucier de l'emplacement réel des données. L'accès à ces dernières devient donc logique et non physique [**25**].

I.16.2 Avantage de la virtualisation

- **Fonctionnement en parallèle de plusieurs systèmes invités :** la virtualisation prise en charge par hyperviseur permet à plusieurs systèmes d'exploitation de fonctionner en parallèle sur la même base matérielle. De nombreux hyperviseurs offrent des fonctions d'émulation pour combler les incompatibilités entre les différentes architectures de systèmes [**28**].
- **Meilleure utilisation grâce à la consolidation matérielle :** si plusieurs machines virtuelles fonctionnent sur une machine physique, les ressources matérielles peuvent être mieux utilisées. Ce type de consolidation augmente l'utilisation du matériel fourni, réduit le temps d'inactivité et réduit les coûts [**28**].

- **Forte encapsulation du système invité et de tous les processus qui s'y déroulent :** chaque système invité fonctionne isolé dans un environnement d'exécution virtuel. Si une machine virtuelle tombe en panne en raison d'un processus défectueux ou est infiltrée par des hackers ou des logiciels malveillants, cela n'a généralement aucun effet sur les machines virtuelles parallèles ou le système hôte sous-jacent [**28**].
- **Economies en ressources informatique de maintenance et d'administration :** les machines virtuelles offrent un grand potentiel d'économies dans la mise à disposition de ressources informatiques. Le passage à une plateforme matérielle puissante pour différents système virtuels réduit les coûts de maintenance et d'administration en centralisant les taches [**28**].
- **Approvisionnement et portage flexibles des serveurs virtuels et des PC :** les machines virtuelles sont indépendantes du matériel physique sous-jacent et permettent un approvisionnement flexible des ressources informatiques. Les serveurs virtualisés ou les ordinateurs personnels (PC) peuvent être facilement créés, clonés et déplacés vers une autre plateforme d'hébergement [**28**].

I.16.3 Inconvénients de la virtualisation

- **Hyperviseur (et système invité)** : les machines virtuelles sont moins efficaces que les machines physiques car certaines des ressources disponibles sont utilisées pour faire fonctionner le logiciel de l'hyperviseur [**28**].
- **Le matériel partagé peut causer des blocages pendant les pics de consommation :** Comme toutes les machines virtuelles d'un système hôte partagent les mêmes ressources matérielles, des goulots d'étranglement peuvent survenir lors des pics de performances [**28**].
- **L'hyperviseur en tant que Single Point of Failure** : si les attaques de hackers ou de logiciels malveillants sont directement dirigées contre le logiciel de virtualisation, tous les systèmes invités gérés par l'hyperviseur peuvent être affectés [**28**].
- **Situation juridique peu claire en ce qui concerne l'octroi de licences pour les systèmes d'exploitation virtuels** : l'exploitation des machines virtuelles soulève de nouvelles questions concernant l'octroi de licences pour les systèmes d'exploitation [**28**].

I.17 Conclusion

L'infrastructure informatique est donc un élément clé pour les entreprises, son rôle intervient à tous les niveaux : les réseaux, les terminaux utilisateurs, les serveurs d'applications ainsi que les données. Le système d'information doit fonctionner pleinement et en permanence pour garantir l'efficacité de l'entreprise, de ce fait la supervision informatique est née pour répondre à ce besoin.

Dans ce chapitre nous avons vu les différents éléments de l'infrastructure qu'on doit superviser, tandis que le prochain chapitre sera consacré à une étude sur la supervision informatique.

Chapitre II : Supervision Informatique

II.1 Introduction

Administrer son infrastructure réseau est un travail à temps réel. Cela devient difficile par le fait que le nombre d'équipements à gérer est souvent de plus en plus important.

Le plus grand souci d'un administrateur est les pannes. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continue l'état des systèmes d'information afin d'éviter un arrêt de production de trop longue durée.

La supervision informatique intervient alors pour répondre à ce besoin, elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements.

Dans ce chapitre nous allons introduire la supervision d'un réseau informatique ainsi que ses différentes notions de bases.

II.2 Définition et concept

La supervision d'un réseau est l'ensemble de protocoles, matériels et logiciels informatiques assurant les activités suivantes : surveiller, visualiser, analyser et agir.

Nous supervisons pour avoir une visibilité sur l'état de son système d'information. Cela permet de disposer rapidement des informations, de connaître l'état de santé du réseau, des systèmes, ainsi que leurs performances.

La supervision intervient donc, dans le cas d'un dysfonctionnement de ce système, elle permet la mise en place d'action corrective, aussi efficace que possible afin d'assurer un retour à la normale dans les brefs délais. Mais peut aussi faciliter la mise en place d'action préventive en vue d'augmenter la satisfaction utilisateur, ou simplement anticiper l'achat de matériel supplémentaire.

II.3 Principe de la supervision

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre la lumière sur d'éventuels problèmes.

La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS) les administrateurs.
Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4. Plusieurs actions sont ainsi réalisées : Acquisition de données, analyse, puis visualisation et réaction [**29**].

Un tel processus est réalisé à plusieurs niveaux d'un parc de machine que nous pouvons les résumés dans les points suivants :

II.3.1 Matériel

La supervision matérielle consiste à récolter les informations relatives à son matériel. On va par exemple récupérer l'état physique d'une machine, sa température, l'état de ses disques, si tous les ventilateurs sont fonctionnels...

Le but étant de remplacer le plus rapidement possible le matériel défectueux ou encore d'anticiper une future panne éventuelle, de faciliter la gestion des stocks de pièce de rechange.

II.3.2 Réseau

La supervision réseau est la surveillance et l'analyse de l'utilisation de son réseau ce qui revient entre autres à connaître le taux d'occupation de son réseau, le nombre de connexion simultanée...

Elle permet aussi de connaître précisément ce qui circule sur le réseau, les protocoles, leur répartition, les éléments qui consomment le plus de ressources, mais aussi la disponibilité des services rendus pas la DSI (Direction des Systèmes d'Informations).

II.3.3 Système

La supervision système permet de surveiller le bon fonctionnement de ses systèmes d'exploitation.

Elle est orientée serveur et va fournir des informations sur l'utilisation des ressources comme l'espace disque, la présence de processus...

II.3.4 Applications et services

Les applications du système d'information sont de plus en plus supervisées. Il est notion ici d'accessibilité et d'utilisabilité, le but étant d'assurer au maximum une

continuité de service et de mesurer les performances en vue d'accroître la satisfaction utilisateur.

II.4 La norme ISO 7498/4

Le concept de supervision a été normalisé par l'ISO (International Organisation for Standardisation). Voici les différentes fonctions qui ont été défini par l'ISO 7498/4 [**30**] :

***Figure II.1*:** Fonctions de la supervision informatique.

II.4.1 Gestion des performances (Performance Management)

Elle permet d'évaluer les performances des ressources (et la disponibilité) du réseau et de ses composants. Les performances du réseau sont évaluées à l'aide de quatre paramètres :

- Le temps de réponse.
- Le débit.
- Le taux d'erreur.
- La disponibilité (en termes de temps).

Le traitement des statiques se déroule en quatre étapes :

- La collecte.
- Le contrôle.
- La présentation des informations.
- L'archivage.

La gestion des performances comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau [**31**].

II.4.2 Gestion des configurations (Configuration Management)

La gestion des configurations représente l'inventaire des ressources nécessaire au fonctionnement du réseau, dont on peut identifier, paramétrer et contrôler ce qui suit :

- Le plan d'adressage et de routage IP du réseau, ou les objets de chaque couche sont concernés.
- Une éventuelle limitation du nombre de sessions applicatives simultanément établies.
- L'état du système : charge CPU ou mémoire, paramètres d'environnement (température dans le boitier ou la consommation électrique d'un appareil) [**31**].

II.4.3 Gestion de la comptabilité (Accounting Management)

Cette gestion a pour mission de relever les informations permettant d'évaluer le cout d'usage d'une ressource. Cette mesure tient compte de deux paramètres essentiels :

- Du temps d'utilisation.
- Du volume d'information échangé.

De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur [**31**].

II.4.4 Gestion des incidents (Fault Management)

Elle permet de nous informer des évènements qui peuvent perturber le fonctionnement du réseau, on distingue deux types de défauts :

- Les défauts internes résultat d'une panne de l'élément actif lui-même.
- Les défauts externes indépendants des appareils eux-mêmes, mais liés à l'environnement propre du réseau.

Le traitement d'une panne est composé de quatre étapes :

- La signalisation du fonctionnement anormal d'un élément actif ou d'un lien inter-réseau.
- La localisation du défaut sur l'infrastructure.
- La reparation.
- La confirmation du retour à un comportement normal du réseau.

L'historisation des incidents peut aider le technicien ou l'ingénieur dans la compréhension de dysfonctionnement du réseau [**31**].

II.4.5 Gestion de la sécurité (Security Management)

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisation établies. Elle veille à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées. Elle permet aussi d'éviter toute perturbation du service et dégradation des performances. Elle a également pour rôle de mettre en application les politiques de sécurité [**31**].

Ces différentes gestions sont utilisées pour gérer certain service comme les SLA

II.5 Gestion des SLA

SLA (Service-Level Agreement) ou accord de niveau de service, est un contrat passé entre un fournisseur de service et ses clients internes ou externes. Les fournisseurs de services réseau sont à l'origine des SLA.

Un service IT met au point un SLA afin que ses prestations puissent être mesurées, justifiées, voire comparées à celles de fournisseurs extérieurs.

Les SLA mesurent les performances et la qualité du fournisseur de services de différentes manières. Ainsi, un SLA peut spécifier les éléments de mesure ou indicateurs suivants [**32**] :

- Disponibilité des services.
- Nombre d'utilisateurs pouvant être pris en charge simultanément.
- Bancs d'essai de performances spécifiques à l'une desquels sont mesurées périodiquement les performances réelles.
- Temps de réponse des applications.

- Calendrier des notifications préalables à des modifications du réseau susceptibles d'affecter les utilisateurs.
- Délai de réponse du service d'assistance pour différentes catégories de problèmes.
- Statistiques d'utilisation mises à disposition.

II.6 Méthodes et standards de la supervision

Le monde de la supervision dispose de normes et standards facilitant l'interopérabilité des superviseurs et supervisés. Ces normes et standards sont souvent gérés par la DMTF (Distributed Management Task Force) qui est une organisation regroupant plus de 160 entreprises et organisations dans 43 pays différents.

Voici une présentation non-exhaustive des différentes méthodes d'interrogation d'élément [**33**].

II.6.1 Méthode de vérification

Il existe 2 méthodes de vérification pour une solution de supervision, soit active ou passive :

- **Active :** Dans cette méthode, c'est le serveur de supervision qui interroge à intervalles réguliers les composants à surveiller.

  Cette méthode est la plus utilisée. Elle a l'avantage d'être fiable, les vérifications se font de manière régulière et en mode question-réponse [**34**].
- **Passive :** Fort logiquement, cette méthode de vérification est l'exact inverse de la précédente. Ici, ce sont les composants surveillés qui envoient à intervalles réguliers (ou non) métriques et messages vers une instance centrale de supervision.

  Cette dernière peut être plus facilement tolérée par les responsables de la sécurité du système d'information étant donné qu'il s'agit de flux sortant uniquement [**34**].

II.7 Protocoles de supervision

II.7.1 Protocol SNMP

Le rôle de base de la supervision est d'avertir l'administrateur de la ressource du problème, de sorte que ce gestionnaire peut le résoudre, il y a des outils pour le faire

et SNMP est l'un d'entre eux. Pour les besoins d'avoir un outil de supervision pour l'administration du réseau internet, l'IETF (Internet Engineering Task Force) a créé le protocole SNMP [**31**].

II.7.1.1 Définition SNMP

SNMP est un protocole simple de gestion de réseau [**31**], il s'agit d'un protocole de communication qui permet aux administrateurs réseaux de gérer et d'interroger en temps réel les équipements qui contiennent des objets gérables via SNMP, et de détecter à distance les problèmes de réseau.

II.7.1.2 Port Utilisé

Le protocole SNMP utilise deux ports UDP définis par la RFC 3232 (Assigned Numbers) :

- **Le port 161** : ouvert dans l'élément active (que l'on appellera Agent), pour la réception d'un message d'interrogation ou de modification d'une variable de configuration, envoyée par la station de supervision (que l'on appellera Manager) [**31**].
- **Le port 162** : ouvert dans le Manager à l'écoute d'un message d'alarme émis par l'Agent [**31**].

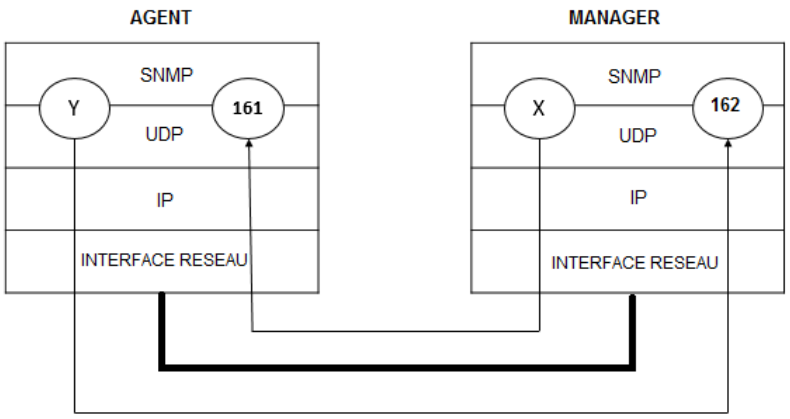


Figure II.2: Ports UDP par SNMP [**31**].

II.7.1.3 Composants de base SNMP et leurs fonctionnalités

- **Station de supervision :**

La Station de supervision appelée Manager ou bien NMS (Network Management System) c'est-à-dire une console de supervision qui permet aux administrateurs de gérer tout son infrastructure par une interface graphique qui présente l'ensemble des machines supervisées à l'administrateur du système en temps réel [**31**]. En cas de panne, ces interfaces offrent la possibilité d'alerter par notification d'alarme (SMS, Mail, etc.). NMS Permet également de collecter les données relatives aux équipements connectés au réseau.

La station contient le protocole de communication SNMP et les applications de gestion pour contrôler les éléments de réseau. Les applications de gestion sont séparées en deux, les applications de gestion propriétaires (Cisco Works, IBM Netview/600) et Les applications de gestion open source (Nagios, Zabbix, etc.).

- **Nouds gérés :**

Ce sont les équipements administrable (pont, routeur, switch, etc.) qu'il faut superviser, ils contiennent des objets de gestion peuvent être des informations sur le matériel ou des données de performance.

- **Agent SNMP :**

Un agent SNMP, est un logiciel installé sur les équipements à superviser et ce sont ces agents qui permettent de transmettre les informations à partir d'une base de données MIB et réponde aux requêtes de station d'administration au format SNMP.

Les paramètres de l'agent SNMP sont :

- L'adresse IP et le masque de sous-réseau associé ;
- L'adresse éventuelle du routeur par défaut ;
- L'adresse IP de Manager.

Notons qu'un Agent peut connaitre plusieurs Managers et que les communautés SNMP peuvent être multiples.

Dans la plupart des cas, l'implémentation IP de ces équipements intègre les protocoles TELNET pour la console distante, TFTP pour la sauvegarde des configurations et ICMP pour les tests ECHO (ping). Le protocole ARP est indispensable à la corrélation adresse MAC /Adresse IP [**31**].

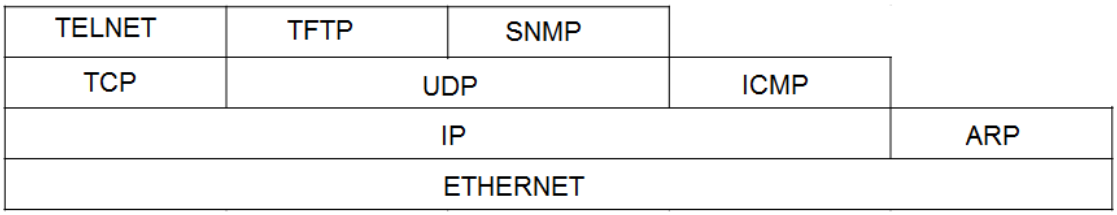


Figure II.3 : Implémentation IP typique *[**31**]*.

II.7.1.4 Base de données d'informations de gestion ou base d'informations de gestion (MIB)

La base de données, appelée MIB (Management Information Base), contenue dans l'équipement à administrer, recense ainsi toutes les informations relatives à cet équipement réseau. Il est donc possible de connaître de façon précise toutes les informations que l'équipement réseau possède dans le but de gérer, au mieux, son fonctionnement.

Elle est construite selon un concept arborescent, chacun des chemins permettant d'accéder à une information appelée OID (Object Identifier) et qui est représentée par une suite d'entiers séparés par des points selon une recommandation de l'union internationale des télécommunications. Chacun des nœuds de l'arbre représente un objet.

On peut distinguer dans la MIB deux parties, une partie standard commune à tous les équipements réseau, et une partie privée propre à un équipement [**35**].

Prenons un exemple simple : si l'on souhaite accéder via une requête SNMP à un objet de mgmt l'OID pourra s'écrire sous deux formes :

• 1.3.6.1.2. NumObjet

• iso.org.dod.internet.mgmt. NomObjet

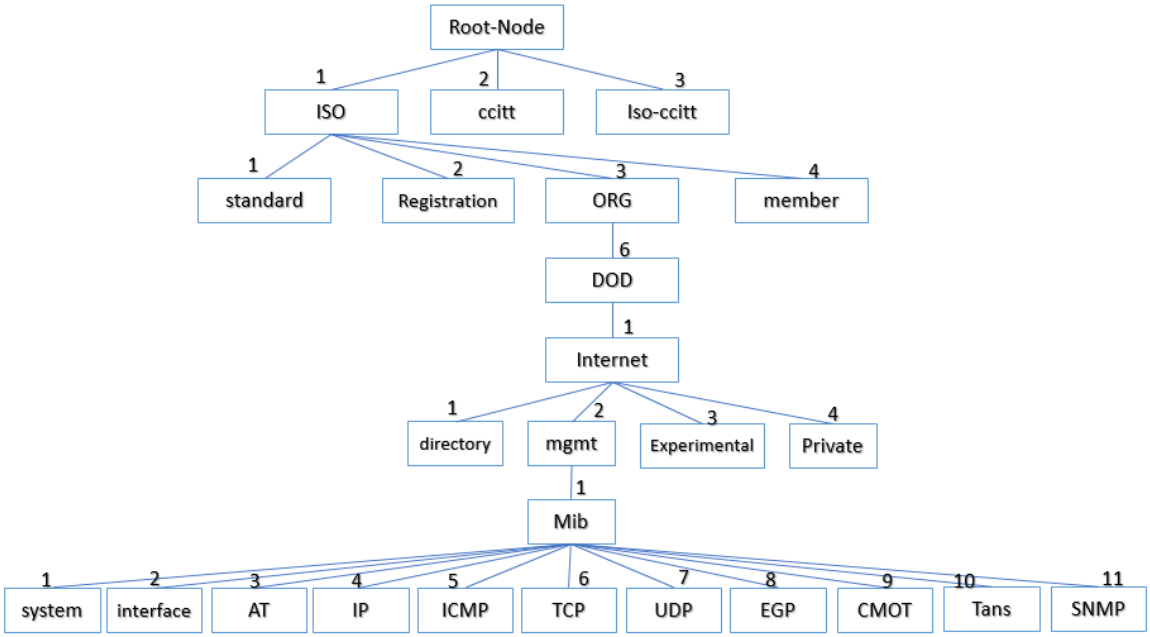


Figure II.4 : Arbre MIB.

- **System** : Description système de toutes les entités gérées.

Exemple d'objets gérés par cette branche :

sysUpTime : Durée écoulée depuis le dernier démarrage.

• **Interfaces** : Interface de données dynamiques ou statiques.

Exemple d'objets gérés par cette branche :

ifNumber : Nombre d'interfaces réseau.

• **At** (adresse translation) : Table d'adresses IP pour les correspondances d'adresses MAC.

• **IP** : Statistiques du protocole IP, adresse cache et table de routage.

Exemple d'objets gérés par cette branche :

ipInReceives : Nombre de datagramme IP reçus.

• **Icmp** : Statistiques du protocole ICMP.

Exemple d'objets gérés par cette branche :

icmpInEchos : Nombre de demandes d'écho ICMP reçues.

• **Tcp** : Paramètres TCP, statistiques et table de connexion.

Exemple d'objets gérés par cette branche :

tcpInSegs : Nombre de segments TCP reçus.

• **Udp** : Statistiques UDP.

Exemple d'objets gérés par cette branche :

udpInDatagrams : Nombre de datagramme UDP reçus.

• **Egp** : Statistiques concernant le protocole de routage EGP, table d'accessibilité.

• **Snmp** : Statistiques du protocole SNMP.

De plus, il faut savoir qu'en complément du standard MIB définissant les différentes informations d'administration réseau contenu sur un équipement, il existe aussi un standard indépendant qui normalise les règles utilisées pour définir et identifier les variables de la MIB. Il se nomme SMI (Structure of Management Information) [**35**].

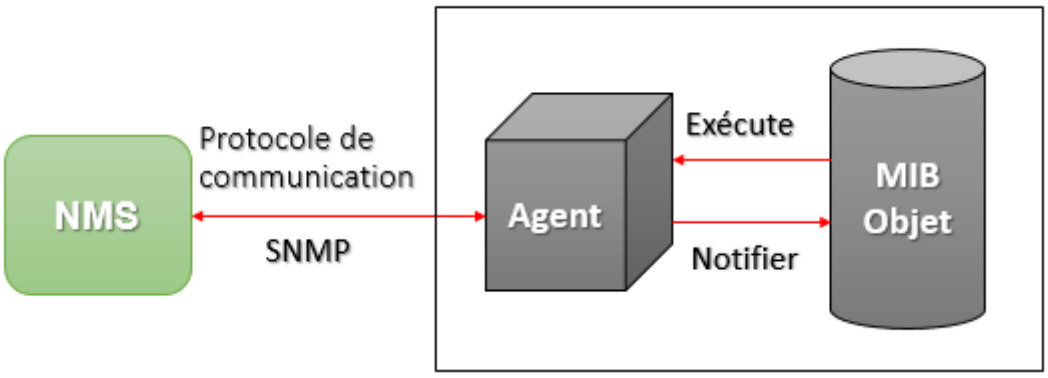


Figure II.5: Architecture SNMP.

II.7.1.5 Communauté

SNMP définit la notion communauté qui représente l'association Agent/Manager, chaque communauté est identifiée par un nom de communauté, ce nom est envoyé avec le message SNMP qui fonctionne comme un mot de passe pour l'accès en lecture seule, ou en lecture et écriture (c'est le contrôle d'accès utilisée par SNMP) à la MIB. Le nom est transmis en claire donc ce mode d'authentification est faible.

Les noms de communauté par défaut sont :

- Public pour lecture seule.
- Private pour lecture et écriture [**31**].

II.7.1.6 Structure des messages SNMP

La simplicité de communication entre la station de supervision et les agents est illustrée par les messages SNMP, trois grands types d'opérations sont réalisables :
Get pour la lecture, Set pour l'écriture, Trap pour les messages d'alertes.
Le protocole SNMP prend en charge ces types de messages :

- **Message GetRequest**

Ce message permet au manager d'interroger un agent pour récupérer une variable d'un objet de la MIB contenu sur l'équipement à gérer. L'attribut OID passé en paramètre.

- **Message GetNextRequest**

Ce message est identique au message précédent, la différence étant que le message GetNextRequest demande la valeur de l'objet suivant dans l'arbre d'objets.

- **Message GetReponse**

En termes de réponse, ce message envoyé par l'agent au manager pour répondre aux messages GetRequest, GetNextRequest et SetRequest. Si l'information demandée n'est pas disponible les réponses sont No such object, No access, No writable.

- **Message SetRequest**

Le message SetRequest permet au superviseur de mettre à jour, ou modifier la valeur d'une variable par une valeur donnée en paramètre sur un agent SNMP.

- **Message TRAP**

Contrairement à tous les autres messages, les traps sont envoyées par l'agent SNMP vers la station de supervision pour signaler un fonctionnement anormal, un changement d'état, un événement non attendu se produit.

Il s'agit d'un mécanisme d'alarme, Il y a 7 types de messages TRAPS : coldStart, WaemStart, LinkDown, LinkUp, AuthentificationFailure, egpNeighborLoss, entrepriseSpecific.

II.7.1.7 Versions SNMP

Il existe trois versions différentes de SNMP :

a. SNMP v1

Comme son nom l'indique, SNMPv1 est la première version du protocole, cette version a un défaut majeur qui est le problème de sécurité car la seule vérification est basée sur une chaine de caractère appelée communauté.

SNMPsec : le but de cette version est de sécuriser le protocole SNMP v1.

Le format générique d'un message SNMP v1.

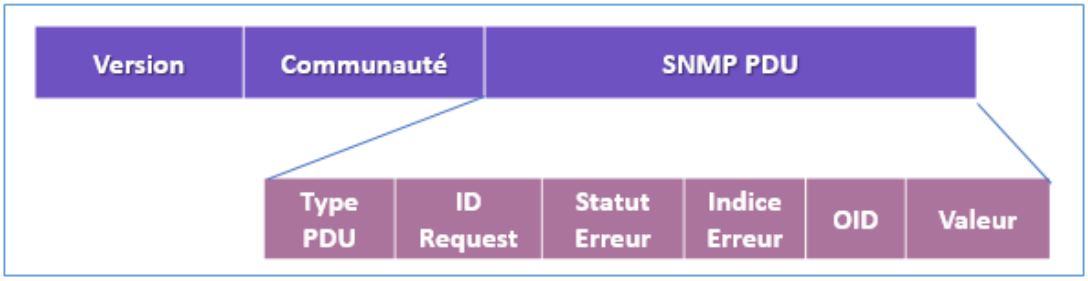


Figure II.6: Format générique d'un message SNMP v1.

Version : numéro de version SNMP utilisée :

- 0 : SNMP v1
- 2 : SNMP v2
- 3 : SNMP v3

Communauté : nom de communauté de lecture seule (RO) ou lecture/écriture (RW) défini par l'administrateur.

Type PDU : décrit le type de message :

***Tableau II-1*:** Type de Message pour chaque Type de PDU.

Type de PDU	*NOM*
0	GetRequest
1	GetNextRequest
2	SetRequest

3	GetReponse
4	Trap

ID Request : utilisé pour la vérification de l'association entre les réponses et les requêtes.

Statut Erreur : pour signaler une erreur, s'il n'y a pas d'erreur donc c'est zéro.

Indice Erreur : spécifie la source d'erreur dans la requête (La position d'erreur).

OID : Indicateur de chaque variable.

Valeur : ce champ émis par le manager pour le but de la mise à jour de la MIB, la valeur dépend du type de PDU.

b. SNMP v2

Cette version est une mise à jour de SNMP v1 pour but d'amélioration des opérations du protocole. Les principales améliorations sont de définir des nouveaux objets, le principal changement est l'ajout de nouvelles méthodes GetBulk et InformRequest.

GetBulk : cette requête permet au superviseur de récupérer les données de grande taille à la fois pour but de minimiser le nombre d'échange.

InformRequest : cette requête confirme la réception d'un TRAP et grâce à celle-ci, la station de supervision peut envoyer une alarme à une autre station de supervision.

c. SNMP v3

SNMP v3 est La dernière version du protocole SNMP, cette version sert à améliorer la sécurité et la confidentialité des informations.

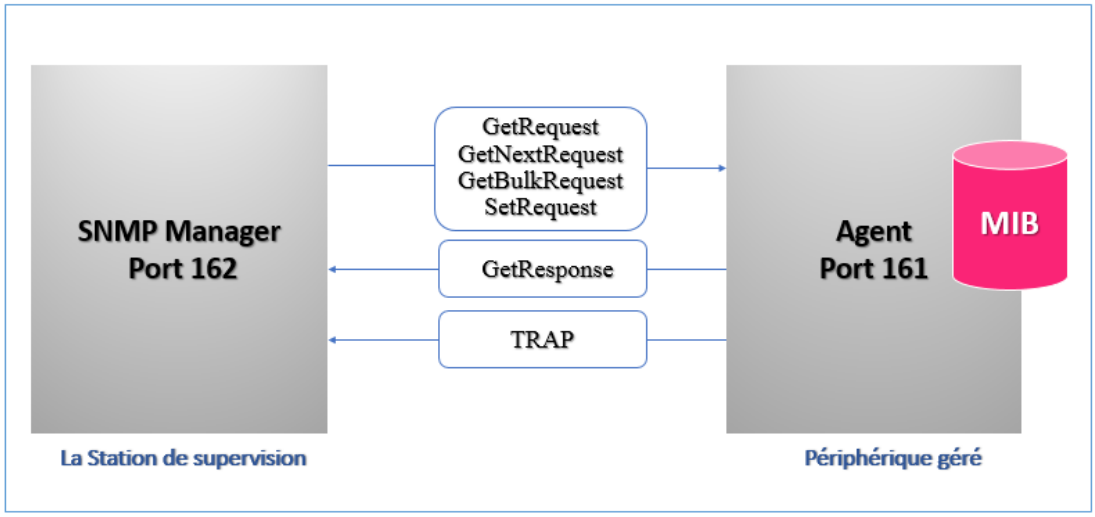


Figure II.7: Principe de fonctionnement du protocole SNMP.

II.7.2 Protocole IPMI

II.7.2.1 Définition

IPMI (Intelligent Platform Management Interface) est une interface ouverte standard, conçue pour la gestion et la maintenance des composants matériels, développée par Intel, Cisco, Dell, HP.

IPMI offre la possibilité aux administrateurs de superviser l'état de fonctionnement des machines et serveur, la surveillance de températures, alimentation électrique, la tension, ventilateurs. L'IPMI permet d'éteindre, d'allumer ou de redémarrer un ordinateur à distance.

L'IPMI permet de gérer le serveur lorsqu'il est éteint, il suffit que le serveur soit connecté au réseau électrique [**36**].

Il support la journalisation et la documentation d'état, il permet d'accéder et collecter des données indépendamment de son système d'exploitation.

II.7.2.2 Principe de fonctionnement

IPMI est considéré comme un protocole d'interrogation, il peut fonctionner par l'interrogation ou par recevoir un TRAP, il utilise le port UDP 623.

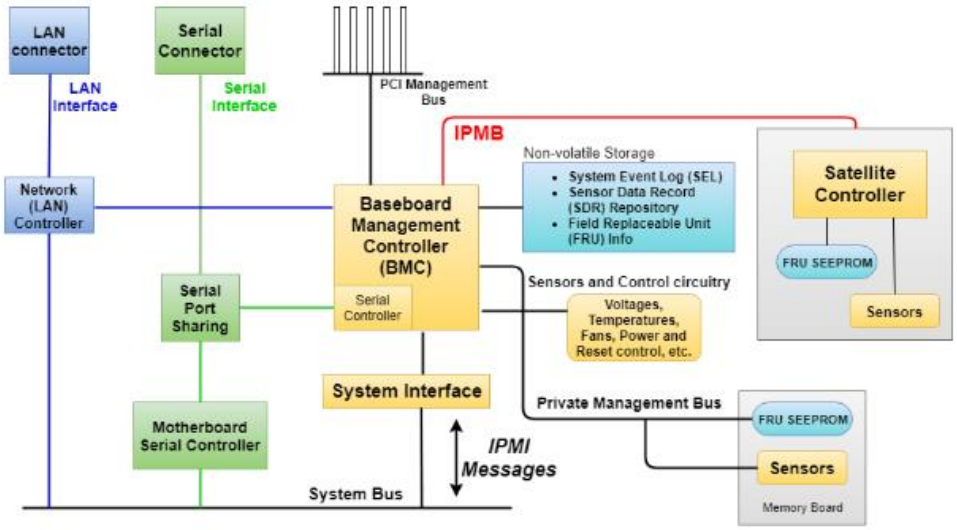


Figure II.8 : Principe de fonctionnement du protocole IPMI.

II.7.2.3 Composants IPMI

a. Contrôleur de gestion de la carte mère (BMC)

Le cœur de l'architecture IPMI est le BMC, un microcontrôleur intégré à la carte mère d'un ordinateur ou d'un serveur. Le BMC offre des capacités de gestion à distance et des tâches de surveillance telles que les températures et les tensions, et permet de gérer le fonctionnement du CPU du serveur, au moyen de capteurs (capteurs de température, batterie et processeur), le BMC prend également en charge les fonctions d'alerte et de journalisation.

Le contrôleur de gestion de la carte mère (BMC) et l'administrateur système communiquent via une connexion indépendante.

BMC est alimenté par la tension de garde de la carte mère, c'est-à-dire qu'elle fonctionne toujours, quel que soit l'état du serveur [**36**].

L'architecture IPMI est conçue de sorte que l'administrateur distant n'a pas un accès direct aux composants du système. Par exemple, pour obtenir des données à partir des capteurs, un administrateur distant envoie une commande à BMC, et BMC se tourne à son tour vers des capteurs [**36**].

b. Stockage indépendant de l'énergie

Le stockage indépendant de l'énergie reste disponible même lorsque le processeur d'un serveur se bloque, par exemple via un réseau local ; Il a trois domaines :

- **Journal des événements système (SEL) :** BMC reçoit des rapports d'événements via l'interface système et IPMB, puis les enregistre avec SEL. Les commandes IPMI permettent de lire et de supprimer le SEL. La mémoire du SEL étant limitée, le journal doit être vérifié et nettoyé périodiquement pour enregistrer les nouveaux événements.
- **Enregistrement des données du capteur (SDR) :** Un référentiel qui stocke les données des capteurs. Les enregistrements SDR sont des données sur les types et le nombre des capteurs. Les SDR contiennent également des enregistrements du nombre et des types d'appareils connectés à l'IPMB.
- **Unité remplaçable sur site (FRU):** Informations d'inventaire sur les modules système. Les entrées FRU contiennent des informations sur les modèles de parties de divers modules du système (processeur, panneaux mémoire, cartes I/O) [**36**].

c. Structure de commande IPMI

IPMI envoie des messages en format demande-réponse. Les demandes sont des commandes. Les commandes lancent des actions et fixent des valeurs. Les messages IPMI contiennent un ensemble de champs de base qui sont les mêmes pour toutes les commandes :

Network Fonction : définit la valeur du cluster auquel appartient la commande (événements, stockage, etc.).

Le champ d'identification demande/réponse : doit faire la distinction entre les requêtes et les réponses.

ID du demandeur : informations sur la source du message.

La pièce d'identité du répondeur : adresse la demande au défendeur désiré.

Commande : Unique dans le cadre des équipes de fonction réseau.

Données : options supplémentaires (telles que les données retournées en réponse) [**36**].

d. Interface d'accès à distance

Dans la version initiale d'IPMI, la console distante était connectée au BMC via l'interface série. La spécification IPMI v2.0 est basée sur l'utilisation d'une interface LAN.

L'interface LAN est fournie via un port réseau BMC dédié avec sa propre adresse IP. Lorsqu'ils sont transmis sur le LAN, les messages IPMI passent par plusieurs étapes d'encapsulation [**36**]:

- Les messages IPMI sont formés en paquets de session IPMI.
- Les paquets de session IPMI sont encapsulés à l'aide du protocole RMCP (Remote Management Control Protocol).
- Les paquets RMCP sont formés dans des datagrammes UDP.
- Des trames Ethernet sont ajoutées.

L'interface série pour connecter la console distante au BMC n'est plus utilisée, mais elle est nécessaire pour implémenter deux fonctions :

- Partage de port série.
- Série sur LAN (SoL).

Il existe également d'autres protocoles utilisés pour la supervision, tels que WMI et JMX.

II.7.3 Protocole WMI

WMI (Windows Management Instrumentation) est un protocole intégré au système d'exploitation Windows, ce protocole est considéré comme un protocole de supervision qui supporte la surveillance et la gestion des performances des systèmes Windows et permet de collecter des informations localement et à distance.

II.7.4 JMX

JMX est l'acronyme de Java Management Extension, c'est une technologie qui définit une architecture et une API pour permettre le monitoring des applications java en temps réel.

II.8 Logiciels de supervision

II.8.1 CACTI

Cacti est un logiciel de supervision dit de « capacity planning » basé sur RRDtool (Round Robin Database) permettant de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels

Cette solution n'est donc pas destinée à alerter en temps réel sur les dysfonctionnements d'un système mais bien de proposer une vision dans le temps de l'évolution d'indicateurs matériels et logiciels (trafic réseau, occupation des disques, temps de réponse, etc…). Le frontend est complètement écrit en PHP. Il supporte également SNMP et tend à se substituer à MRTG pour créer des graphiques [**37**].

II.8.2 Checkmk

Checkmk a été créé en 2008. C'est un logiciel développé en Python et C++ pour la surveillance d'infrastructures informatiques et de réseaux. Il est utilisé pour le contrôle des serveurs, réseaux, infrastructures cloud (publiques, privées, et hybrides), périphériques de stockages, bases de données et capteurs environnementaux.

Checkmk utilise différentes méthodes pour accéder aux données, les « agents spéciaux » fonctionnant sur le superviseur et communiquant avec l'API du système cible, l'API SNMP de gestion de réseau, et aussi les protocoles HTTP et TCP pour communiquer avec des services web et l'internet [**38**].

II.8.3 ZenOSS

Créé en 2005, ZenOss a pour but de fournir le nécessaire à la supervision de parcs informatique en un seul outil**.** Zenoss Community Edition est une plate-forme gratuite et open-source de gestion d' applications , de serveurs et de réseaux basée sur le serveur d' applications Zope . Publié sous la licence publique générale GNU version 2, Zenoss Community Edition fournit une interface Web qui permet aux administrateurs système de surveiller la disponibilité, l'inventaire / la configuration, les performances et les événements. Ainsi que la collecte des donées via SNMP, SHH, WMI et JMX [**39**].

II.8.4 NAGIOS

Nagios est un logiciel libre sous licence GPL qui a été créé par Ethan Galstad en 1999 sous le nom de NetSaint. Elle est aujourd'hui l'une des solutions de supervision opensource les plus connue et la plus répandues. Il permet la supervision en temps réel des systèmes et réseaux, résolution rapide d'incidents, supervision avec les agents, se dispose d'un tableau de bord, de plus c'est une solution sécurisée.

Nagios a été conçu à l'origine pour fonctionner sous Linux, mais il fonctionne aussi bien sur d'autres variantes d'UNIX.

La surveillance des équipements et systèmes cibles, à travers notamment des protocoles tels SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH [**40**].

II.8.5 Centreon

Centreon est un logiciel de supervision réseau libre basé sur Nagios, il fournit une interface web qui permet la consultation de l'état de service et gère la liste de contrôle d'accès (ACL), il s'appuie sur une base de données MySQL pour le stockage des données.

Il apporte de nombreuses fonctionnalités réelles comme la gestion d'indice, l'utilisation des graphiques, la configuration des composantes via l'interface web, la détection des pannes, alertant en cas de panne, récupérer les informations dans la base de basse de données. Centreon réalise le monitoring via SNMP [**41**].

II.8.6 SHINKEN

La solution SHINKEN, est une application de supervision open source, écrite en python sous licence GNUAGPL et compatible avec le logiciel Nagios. Il utilise l'architecteur client/serveur selon la méthode d'interrogation SNMP.

SHINEKN permet la surveillance des ressources des serveurs, les applications, et des services réseaux (SMTP, POP, http, etc.), il support la notion de notification et les plugins [**42**].

II.8.7 Op Manager

Op Manager, une solution de surveillance réseau facile à utiliser et abordable. Il surveille les périphériques réseau tels que les routeurs, les commutateurs, le pare-feu, les serveurs et tout ce qui a une adresse IP et connecté au réseau. Op Manager surveille en permanence le réseau et offre une visibilité et un contrôle approfondis sur celui-ci. En cas de panne, il est possible d'explorer la cause première et l'éliminer avant que les opérations ne soient affectées [**43**].

II.8.8 Zabbix

Zabbix est un logiciel Open source, créé par Alexei Valdishev en 1998 [**44**]. Zabbix est un moniteur qui permet la surveillance de nombreux paramètres d'un serveur, post de travail, imprimante et autres matériels, la vérification de la disponibilité des services, il permet également la vue graphique de la consommation des données.

Le logiciel est composé de :

- **Serveur** : Composant principale qui permet de surveiller à distance (et on locale) les éléments système et réseaux, et envoie des alertes dans le cas de problème.
  Zabbix server non supporté dans Windows.
- **Interface web :** développée en PHP, utilisée pour la visualisation et la navigation des données, et d'administration et de configuration de Zabbix.
- **Proxy** : Zabbix Proxy n'est pas pris en charge par Windows, il permet de récupérer, protéger, et transmettre les données au serveur Zabbix, fonctionnant comme un serveur intermédiaire pour réduire la charge sur le serveur proxy.
- **Des agents** : L'agent Zabbix se charge de la récupération des données des machines supervisées puis les transmettre au serveur Zabbix.

Il repose sur le langage C, distribué sous licence GNU General Public License.

Fonctionnalités de Zabbix

- Une application libre.
- Surveillance en temps réel.
- Gestion des alertes.
- Règlement rapide des crises.
- Traitement des graphes.
- Gestion du SLA (Service-Level Agreement).
- L'authentification et le traitement des rôles.
- Contrôle d'un ensemble d'hôtes comme un seul.

Zabbix joue un roule important dans la supervision du système qui s'effectue via le protocole SNMP et le protocole IPMI.

II.9 Conclusion

La supervision est une solution essentielle pour un système informatique, permet de récupérer un ensemble d'informations liées à l'état du réseau informatique basée sur des protocoles tels que SNMP et IPMI. Elle nous permet d'avoir une vue d'ensemble sur l'état du réseau et de mettre en place une vision pour le développement.

On a vu un ensemble de logiciels existants sur le marché qui sont des outils open source ou propriétaires ayant des caractéristiques spécifiques, dans notre projet nous avons opté pour l'utilisation de ZABBIX.

La prochaine étape sera un aperçu du logiciel utilisé. Cette dernière consistera à proposer une étude détaillée sur le logiciel open source ZABBIX.

Chapitre III : Zabbix Logiciel de supervision réseau

III.1 Introduction

Sur n'importe quel réseau avec plus d'un serveur, il peut être très utile d'avoir une image complète de ce qui se passe sous nos yeux. Dans les grands réseaux, où le nombre d'hôtes dépasse plusieurs dizaines, le suivi individuel de chacun est une tâche écrasante pour les administrateurs. Pour faciliter la tâche d'observation, des systèmes de supervision sont utilisés.

Zabbix est un outil de supervision universel capable de suivre la dynamique des serveurs et des équipements réseau, de répondre rapidement aux situations d'urgence et de prévenir d'éventuels problèmes de charge. Le système de surveillance Zabbix peut collecter des statistiques dans un environnement de travail spécifié et agir dans certains cas d'une manière spécifiée.

Dans ce chapitre, nous allons parler des principes de base, des fonctionnalités et des outils clés sur lesquels repose le système de supervision universel Zabbix.

III.2 Définition du Zabbix

Zabbix est un logiciel qui surveille de nombreux paramètres d'un réseau ainsi que la santé et l'intégrité des serveurs, des machines virtuelles, des applications, des services, des bases de données, des sites Web, du cloud et plus encore. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer des alertes par e-mail pour pratiquement tous les événements. Cela permet une réaction rapide aux problèmes de serveur. Zabbix offre d'excellentes fonctionnalités de reporting et de visualisation de données basées sur les données stockées. Cela rend Zabbix idéal pour la planification de la capacité. Zabbix est une solution de surveillance distribuée open source de classe entreprise.

Zabbix prend en charge à la fois l'interrogation et le recouvrement. Tous les rapports et statistiques Zabbix, ainsi que les paramètres de configuration, sont accessibles via une interface Web. Une interface Web garantit que l'état du réseau et la santé des serveurs peuvent être évalués à partir de n'importe quel emplacement. Correctement configuré, Zabbix peut jouer un rôle important dans la surveillance de l'infrastructure informatique. Cela est également vrai pour les petites organisations avec quelques serveurs et pour les grandes entreprises avec une multitude de

serveurs.

Zabbix est gratuit, écrit et distribué sous la licence publique générale GPL version 2. Cela signifie que son code source est librement distribué et disponible pour le grand public [**45**].

III.3 Architecture Zabbix

Zabbix fournit de nombreuses façons pour surveiller des différents aspects de l'infrastructure informatique et, en fait, presque tout ce que peut-être connecter. Il peut être caractérisé comme un système de surveillance semi-distribué avec une surveillance centralisée à utiliser distribuée avec des proxies, et la plupart des installations utiliseront des agents Zabbix [**46**].

Zabbix offre les fonctionnalités suivantes :

- Une interface web centralisée et facile à utiliser ;
- Un serveur qui fonctionne sur la plupart des systèmes d'exploitation de type UNIX, y compris Linux ;
- Des agents natifs pour la plupart des systèmes d'exploitation de type UNIX et les versions de Microsoft Windows ;
- La possibilité de monitorer directement les dispositifs SNMP (SNMPv1, SNMPv2c, et SNMPv3) et IPMI ;
- Possibilité de monitorer directement les applications Java à l'aide de JMX ;
- La possibilité de monitorer directement vCenter ou l'instance vSphere à l'aide de l'API VMware ;
- Graphiques intégrés et autres fonctionnalités de visualisation ;
- Notification permettant une intégration facile avec d'autres systèmes ;
- Configuration flexible, y compris la création de modèles [**46**].

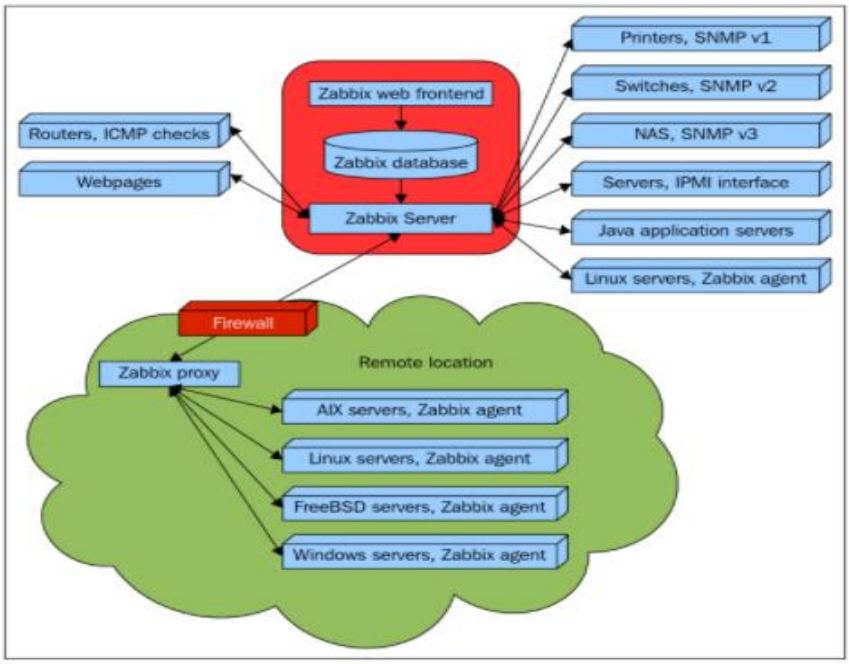


Figure III.1 : *Architecture Zabbix.*

III.4 Tableau de bord

La section Tableau de bord est une section personnalisable de l'interface Web conçue pour afficher des résumés de toutes les informations importantes.

Un tableau de bord est constitué de widgets et chaque widget est conçu pour afficher des informations d'un certain type et d'une certaine source, qui peuvent être un résumé, une carte, un graphique, l'horloge, etc.

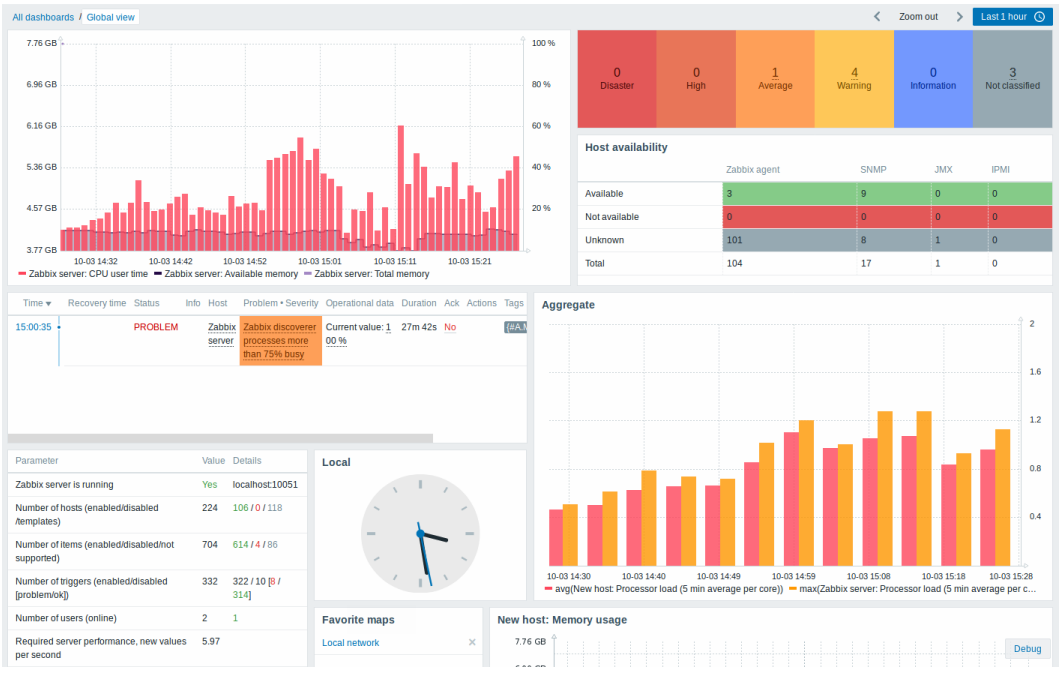


Figure III.2: Affichage de tableau de bord.

Il est possible de regrouper dans un seul tableau de bord des widgets de différentes sources pour un aperçu rapide, il est également possible de créer plusieurs tableaux de bord contenant différents ensembles de vues d'ensemble et de basculer entre eux [**47**].

III.5 Surveillance des performances

Les performances sont l'un des principaux objectifs de l'informatique. Les systèmes ne sont jamais assez rapides pour répondre à tous les besoins, nous devons donc équilibrer les opérations souhaitées avec les ressources disponibles. Zabbix peut aider à la fois à évaluer les performances d'une action particulière et à surveiller la charge actuelle.

Il est possible de commencer par des choses simples, comme les performances du réseau, indiquées par un ping aller-retour ou le nécessaire à un site Web pour renvoyer du contenu, et avancer avec des scénarios plus complexes, comme les performances moyennes d'un service dans un cluster couplées au débit de la baie de disques [**48**].

III.6 Surveillance de la disponibilité et de l'intégrité du serveur

Zabbix surveille l'intégrité et la disponibilité des dispositifs et garantit l'accès à un service ou à des ressources, et détecte également les problèmes de performance. Toutes les informations mesurées sont stockées dans une base de données et créées dans des rapports de disponibilité.

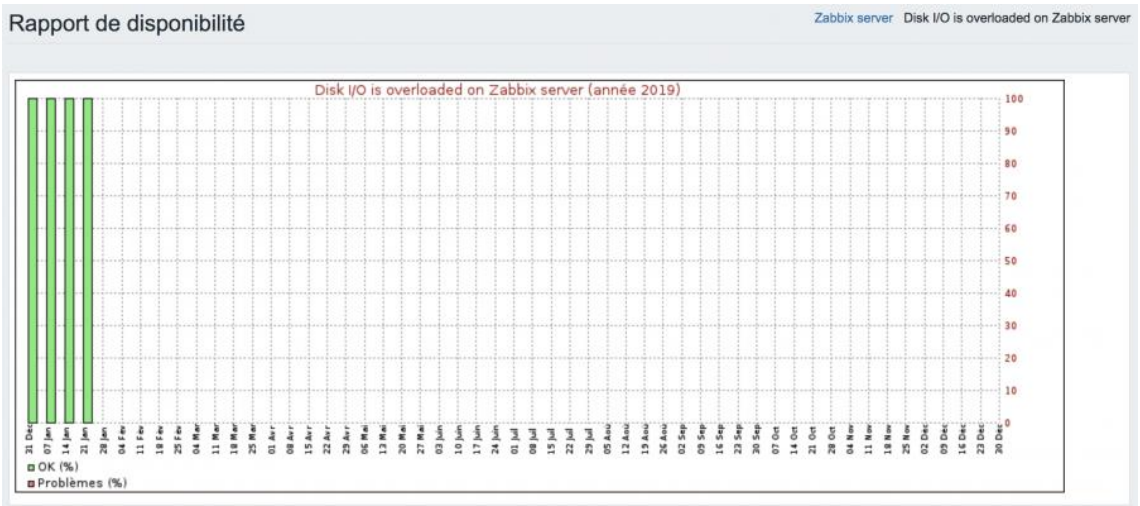


Figure III.3 : Disponibilité de disque I/o.

III.7 Surveillance des services

La fonctionnalité de supervision des services est destinée à ceux qui souhaitent disposer d'une vue de haut niveau (métier) de l'infrastructure supervisée. Ce qui nous intéresse, c'est la disponibilité du service fourni par le service informatique comme l'identification des points faibles de l'infrastructure informatique, les SLA des différents services informatiques, la structure de l'infrastructure informatique existante et d'autres informations de haut niveau.

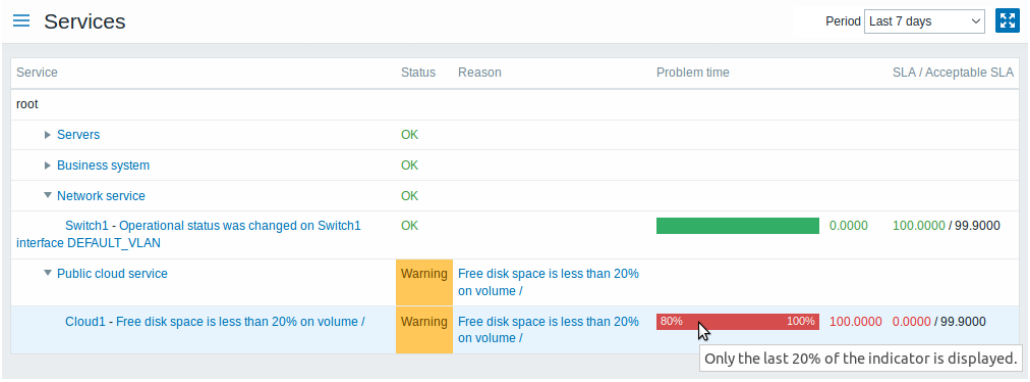


Figure III.4: Affichage des services surveillés.

Il est possible de créer une hiérarchie de l'infrastructure supervisée. Le service parent de plus haut niveau est « racine ». Puis ajouter des services parents de niveau inférieur, puis des nœuds individuels [**49**].

III.8 Surveillance de l'hôte en temps réel

Les hôtes Zabbix typiques sont les dispositifs à surveiller (serveurs, stations de travail, commutateurs, etc.).

Pour surveiller tout type d'hôte, il faut d'abord créer cet hôte dans le sous-menu Hosts des tâches de surveillance (configuration de Zabbix), puis il sera possible de surveiller les paramètres du périphérique [**50**].

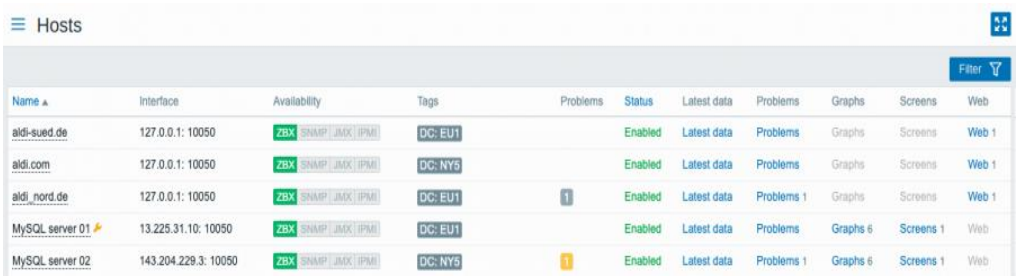


Figure III.5 : Présentation de la surveillance de l'hôte.

III.8.1 Modèle (Template)

Un modèle est un ensemble d'entités qui peuvent être appliquées de manière pratique à plusieurs hôtes. Les entités peuvent être : éléments, déclencheurs, graphes, applications, écrans, règles de découverte de bas niveau, scénarios web.

Le travail des modèles est d'accélérer le déploiement des tâches de surveillance sur un hôte ; également pour faciliter l'application de modifications en masse aux tâches de surveillance [**51**].

III.8.2 Interface d'hôte

Chaque hôte est composé d'une collection d'éléments qui représentent les données de surveillance brutes et de déclencheurs, qui représentent l'intelligence de surveillance Zabbix basée sur les données collectées [**52**].

III.8.2.1 Système d'alerte

a. Eléments (Items)

Les éléments sont ceux qui collectent les données d'un hôte. Une fois que l'hôte est configuré, il faut ajouter des éléments de surveillance pour commencer à obtenir des données réelles.

Certains types d'éléments proposés par Zabbix :

- Vérifications d'agent Zabbix.
- Vérifications de l'agent SNMP.
- Trappes SNMP.
- Vérifications IPMI.
- Contrôles simples.

La vérification de l'agent Zabbix est le type par défaut. Il existe des vérifications d'agents passifs et actifs [**53**].

- **Verifications passives et actives**

Dans une vérification passive, l'agent répond à une demande de données. Le serveur Zabbix (ou le proxy) demande des données, par exemple, la charge du processeur, et l'agent Zabbix renvoie le résultat.

Les vérifications actives nécessitent un traitement plus complexe. L'agent doit d'abord récupérer une liste d'éléments du serveur Zabbix pour un traitement indépendant. Ensuite, il enverra périodiquement de nouvelles valeurs au serveur [**54**].

b. Déclencheurs (Triggers)

Les déclencheurs sont des expressions logiques qui « évaluent » les données collectées par les éléments et représentent l'état actuel du système.

Bien que les éléments soient utilisés pour collecter des données système, il est très peu pratique de suivre ces données tout le temps en attendant une condition qui est alarmante ou qui mérite l'attention. Le travail de « évaluation » des données peut être laissé pour déclencher des expressions [**55**].

Un déclencheur peut avoir les états suivants : État OK, État problème Ou État unknown.

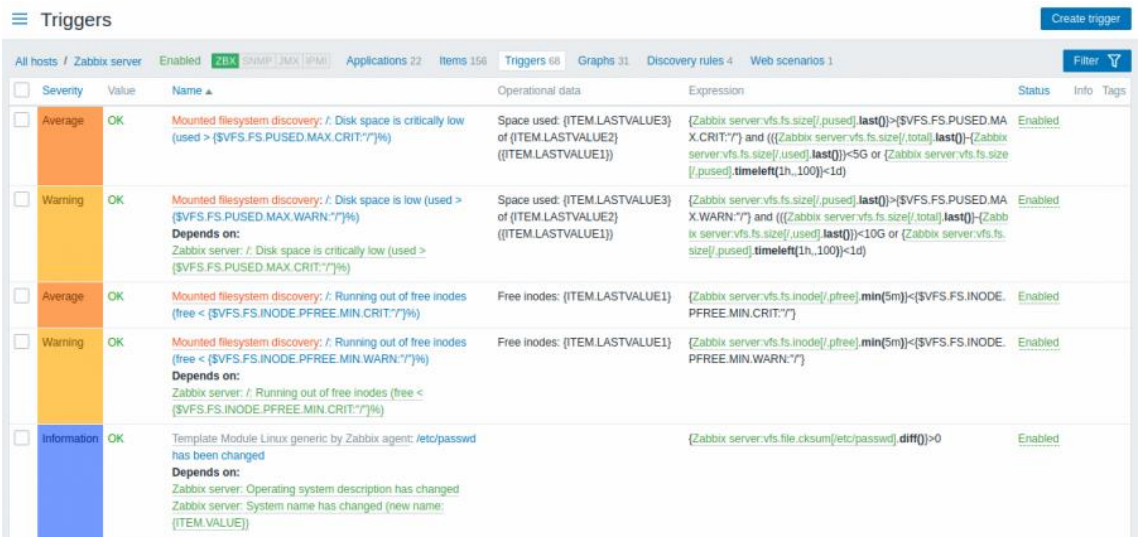


Figure III.6 : Représentation de l'état actuel du système par les déclencheurs.

c. Action

Une action est un moyen prédéfini de réagir à un événement. Elle se compose d'opérations (par exemple, l'envoi d'une notification) et de conditions (quand l'opération est exécutée) [**56**].

Les opérations d'action sont : e-mail, SMS ou script.

Les actions peuvent être définies en réponse à des événements de tous les types pris en charge [**57**] :

- Événements de déclenchement - lorsque l'état du déclencheur passe d'OK à PROBLÈME et vice-versa ;
- Événements de découverte - lorsque la découverte du réseau a lieu ;
- Événements d'enregistrement automatique - lorsque de nouveaux agents actifs s'enregistrent automatiquement (ou que les métadonnées de l'hôte changent pour les agents enregistrés) ;
- Événements internes - lorsque les éléments ne sont plus pris en charge ou que les déclencheurs passent dans un état inconnu.

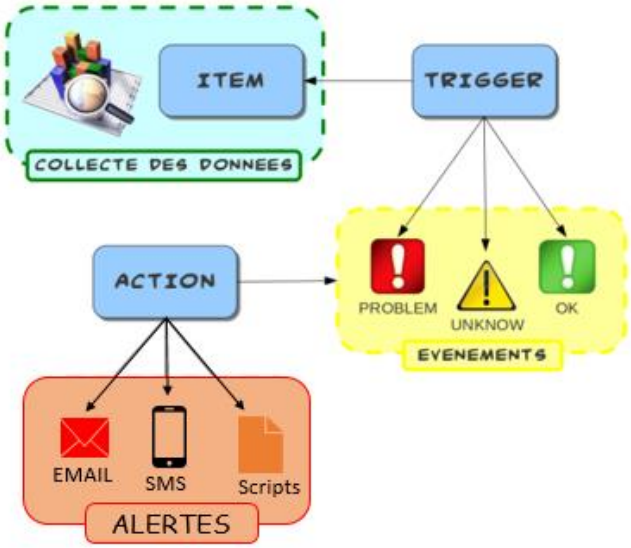


Figure III.7 : Principe de fonctionnement du système d'alerte.

III.9 Graphe en temps réel

Un graphe dans Zabbix est une représentation visuelle des données qui ont été mesurées sur un hôte en temps réel.

Ces graphes mesurent des éléments tels que :

- L'utilisation du CPU et de la mémoire ;
- L'utilisation du trafic réseau ;
- L'utilisation des disques et des files d'attente, etc.

Zabbix permet à l'utilisateur de créer des graphes en fonction de ces besoins.

III.10 Surveillance matérielle en temps réel

Zabbix permet d'obtenir en temps réel des informations sur l'état du matériel surveillé : serveur, routeur, commutateur, machines virtuelles …etc. ces informations sont présentées sous forme de tableaux et de graphes :

III.10.1 Température

La mesure de la température du processeur est l'une des plus importantes pour chaque type d'infrastructure informatique. Il est possible d'analyser la santé du matériel, vérifier la réfrigération des serveurs dans le centre des données.

III.10.2 Disque

La surveillance de la disponibilité de l'espace disque est importante pour ne pas causer de problèmes de stockage afin d'obtenir de bonnes performances dans le système. Zabbix affiche une liste de : l'espace disque utilisé, le temps de lecture du disque, le temps d'écriture du disque, la longueur de la file d'attente actuelle du disque, le taux de lecture du disque et le taux d'écriture du disque.

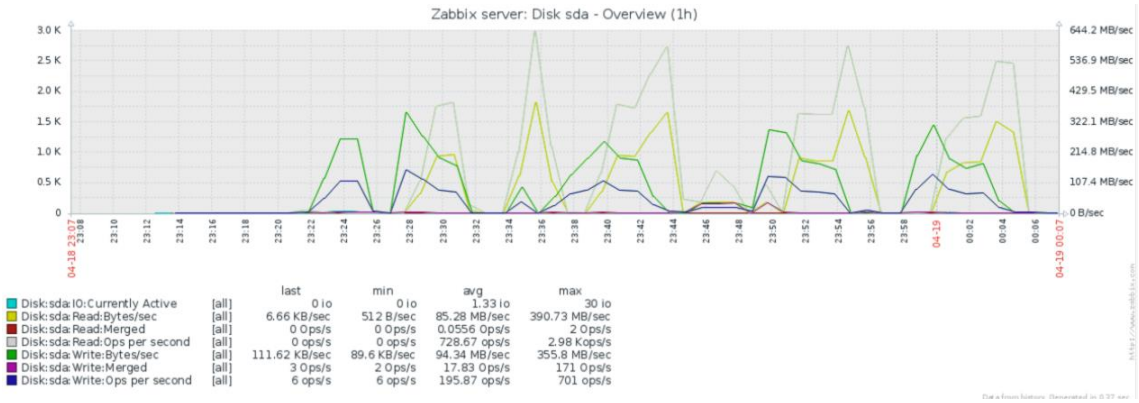


Figure III.8 : Surveillance des statistiques de disque.

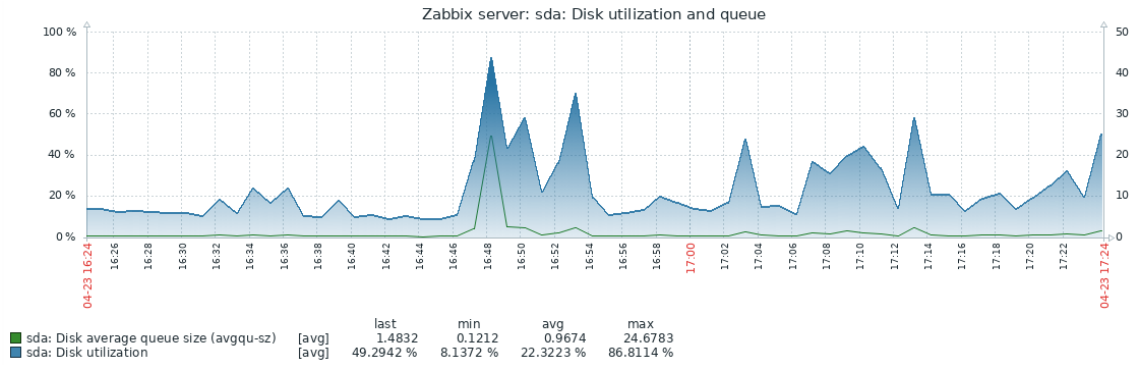


Figure III.9 : Surveillance de l'utilisation et de la file d'attente du disque.

Le graphe d'utilisation du disque montre l'espace libre, l'espace utilisé ainsi que

la taille moyenne de la file d'attente du disque.

III.10.3 CPU et mémoire

L'utilisation du processeur et de la mémoire du serveur est surveillée, enregistrée et affichée par Zabbix en temps réel sous la forme d'un graphe, afin d'analyser et surveiller les performances du serveur.

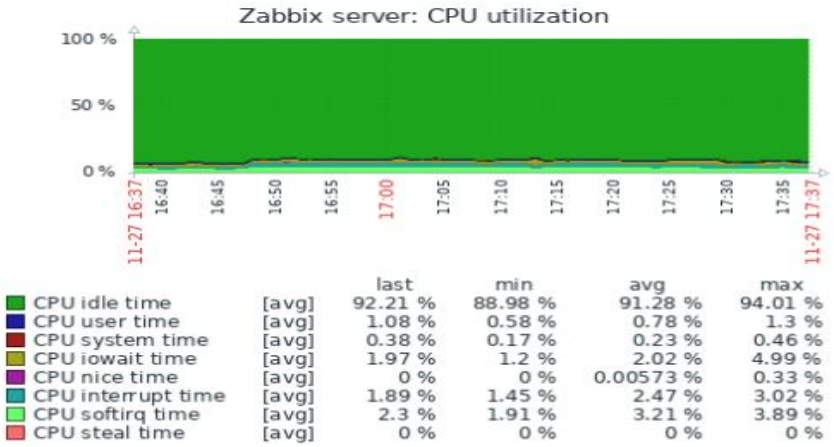


Figure III.10: *Utilisation du CPU.*

III.10.4 Vitesse du ventilateur

Zabbix assure la surveillance de la vitesse des ventilateurs des différents composants matériels qui doivent être ventilés avec une bonne répartition du flux d'air.

III.10.5 Alimentation

La surveillance de l'alimentation (la tension et le courant) des matériels se fait en temps réel pour éviter les pannes ou les courts-circuits.

III.10.6 Vitesse d'horloge du processeur

La vitesse à laquelle le processeur termine son cycle de traitement, Elle doit être surveillée afin d'assurer une meilleure utilisation des ressources.

III.10.7 Batterie

La surveillance des batteries des serveurs est faite pour éviter la perte de données de cache en cas d'un problème d'alimentation.

III.11 Surveillance des serveurs

Zabbix permet de surveiller les éventuelles mesures de performance du serveur

et les incidents :

La surveillance des performances du serveur comprend l'utilisation du processeur et la mémoire, l'utilisation de la bande passante du réseau, le taux de perte des paquets et le nombre de connexion TCP.

D'autre fonctionnalité de Zabbix, il assure la surveillance de la disponibilité des serveurs par la surveillance de l'espace disque, l'état du système ainsi que la surveillance de l'alimentation, la température et le fonctionnement du ventilateur.

En outre ce logiciel peut remonter des informations sur n'importe quel changement de configuration, par exemple si un nouveau composant est ajouté ou supprimé [**58**].

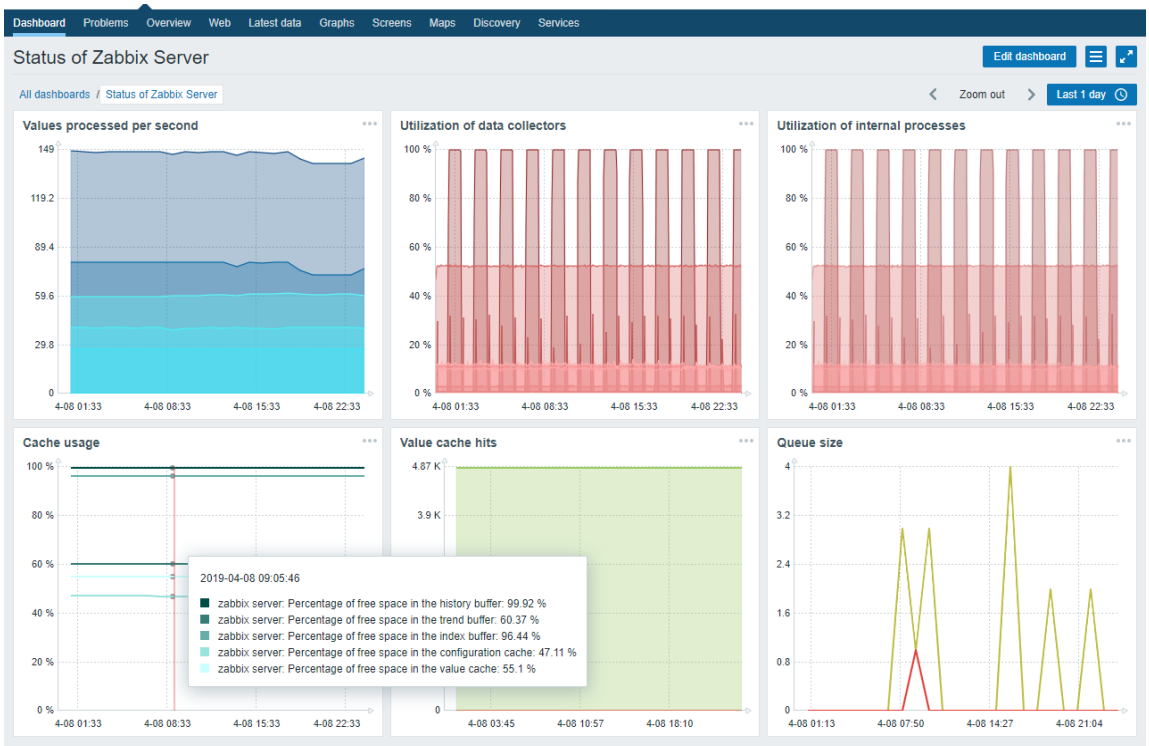


Figure III.11: Etat du serveur.

Figure III.12 *:* Informations requises du serveur.

III.12 Surveillance des commutateurs

Les commutateurs doivent être supervisés pour pouvoir identifier rapidement les perturbations et éliminer les erreurs. Les commutateurs qui supportent le Simple Network Management Protocol (SNMP), peuvent directement être intégrés dans l'environnement de supervision Zabbix.

Zabbix surveille les ports de commutation et informe rapidement l'administrateur à chaque fois qu'un port de commutateur ou un commutateur tombe en panne, Zabbix permet aussi de présenter des informations précises sur le trafic passant sur les ports sous forme de graphes ou des données.

Timestamp	Interface Fa0/1(): Operational status	Interface Fa0/2(): Operational status	Interface Fa0/3(): Operational status	Interface Fa0/4(): Operational status	Interface Fa0/5(): Operational status	Interface Fa0/6(): Operational status	Interface Fa0/7(): Operational status	Interface Fa0/8(): Operational status	Interface Fa0/9(): Operational status	Interface Fa0/10(): Operational status	Interface Fa0/11(): Operational status
2021-05-30 12:06:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)
2021-05-30 12:05:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)
2021-05-30 12:04:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)
2021-05-30 12:03:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)
2021-05-30 12:02:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)
2021-05-30 12:01:47	up (1)	up (1)	down (2)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)

Figure III.13: Surveillance des interfaces du commutateur.

III.13 Surveillance des routeurs

En cas de saturation, les routeurs (et donc les réseaux) peuvent perturber les communications et les flux de travail d'une entreprise.

Zabbix, permet de surveiller toutes nos connexions routeur. Il est possible donc de visualiser la quantité de bande passante consommée par chaque connexion, identifier les appareils, programmes ou utilisateurs qui génèrent le plus de trafic et localiser les points de formation de goulots d'étranglement sur le réseau. Zabbix dispose ainsi d'une multitude d'informations précieuses qui faciliteront grandement le travail d'administrateur.

Fort d'un large éventail de fonctionnalités, Zabbix permet de surveiller facilement le trafic routeur 24h/24, d'archiver l'activité du réseau et de mesurer l'utilisation qui en est faite.

Outre le trafic et la bande passante, il permet aussi de superviser l'appareil lui-même. Zabbix permet de garder constamment à l'œil les ventilateurs, la température et l'alimentation électrique, ainsi que la mémoire du routeur.

III.14 Surveillance et analyse des données de trafic réseau

Zabbix, permet de surveiller et mesurer le trafic sur le réseau en explorant les indicateurs sur les chemins des paquets et la bande passante. Il permet de détecter et de diagnostiquer facilement des problèmes de performance du réseau. Zabbix facilite le suivi du trafic réseau via une interface qui affiche une vue tout-en-un que peut-être personnalisé. Identifier les problèmes en utilisant des graphes et des données qui affichent des vues globales et des détails essentiels.

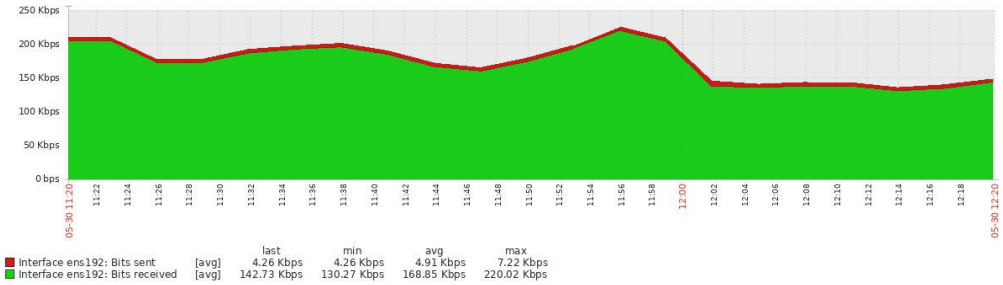


Figure III.14: Surveillance du trafic réseau.

III.15 Carte

Dans la section Cartes, il est possible de configurer, gérer et afficher les cartes du réseau. A l'ouverture de cette section, une carte parait à laquelle il y avait un dernier accès ou une liste de toutes les cartes récemment accédées. La liste des cartes peut être filtrée par nom [**59**].

- **Liste des cartes:**

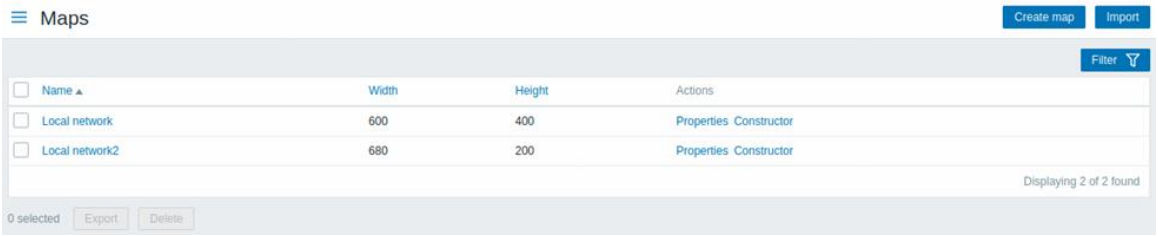


***Figure III.15*:** Affichage des listes des cartes.

- **Visualisation des cartes :**

Visualisation d'une carte est depuis son nom dans la liste de toutes les cartes.

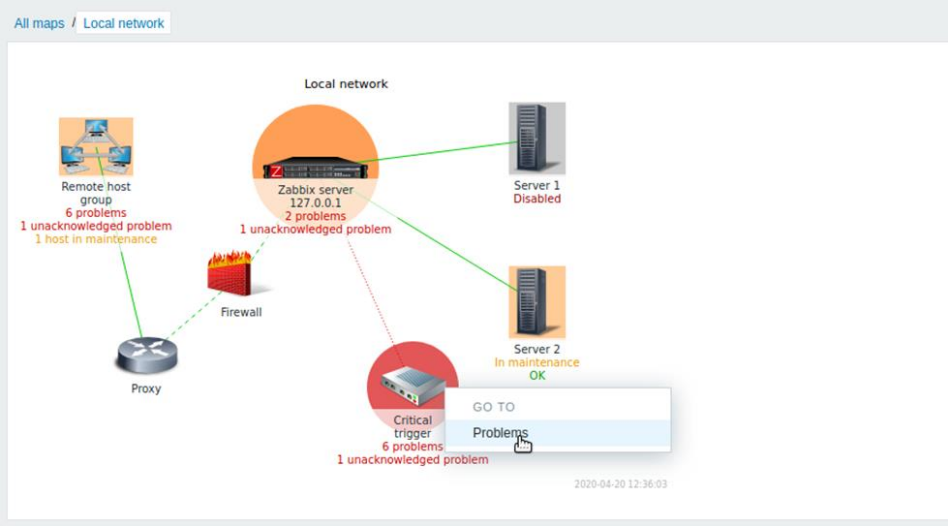


Figure III.16: Visualisation des cartes des réseaux.

Il est passible d'utiliser la liste déroulante de la barre de titre de la carte pour sélectionner le niveau de gravité le plus bas des déclencheurs de problème à afficher.

La gravité marquée par défaut est le niveau défini dans la configuration de la carte. Si la carte contient une sous-carte, la navigation vers la sous-carte conservera la gravité de la carte de niveau supérieur (sauf si elle n'est pas classifiée, dans ce cas, elle ne sera pas transmise à la sous-carte) [**59**].

III.16 Découverte automatique du réseau

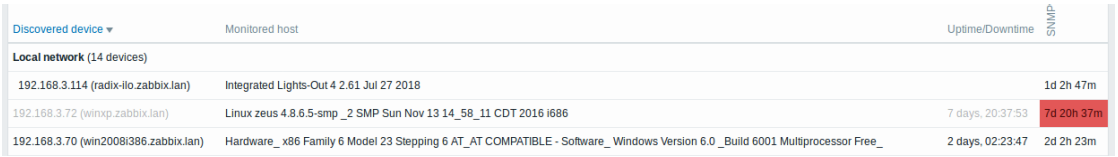
Zabbix offre une fonctionnalité de découverte automatique du réseau efficace et très flexible [**60**].

Avec la découverte du réseau correctement configurée, il est possible de [**60**] :

- Accélérer le déploiement de Zabbix ;
- Simplifier l'administration ;
- Utiliser Zabbix dans des environnements en mutation rapide sans administration excessive.

La découverte du réseau Zabbix est basée sur les informations suivantes [**60**] :

- Les plages IP ;
- La disponibilité de services externes (FTP, SSH, WEB, POP3, IMAP, TCP, etc.) ;
- Les informations reçues de l'agent Zabbix (seul le mode non crypté est pris en charge) ;
- Les informations reçues de l'agent SNMP.



Discovered device ▾	Monitored host	Uptime/Downtime	SNMP
Local network (14 devices)			
192.168.3.114 (radix-ilo.zabbix.lan)	Integrated Lights-Out 4 2.61 Jul 27 2018		1d 2h 47m
192.168.3.72 (winxp.zabbix.lan)	Linux zeus 4.8.6.5-smp _2 SMP Sun Nov 13 14_58_11 CDT 2016 i686	7 days, 20:37:53	7d 20h 37m
192.168.3.70 (win2008i386.zabbix.lan)	Hardware_ x86 Family 6 Model 23 Stepping 6 AT_AT COMPATIBLE - Software_ Windows Version 6.0 _Build 6001 Multiprocessor Free_	2 days, 02:23:47	2d 2h 23m

Figure III.17 : Résultat de découverte automatique dans le réseau.

III.17 Enregistrement automatique d'agent

Il est possible d'autoriser l'enregistrement automatique d'agents Zabbix actifs, après quoi le serveur pourra commencer à les surveiller. De cette façon, de nouveaux hôtes peuvent être ajoutés pour la surveillance sans les configurer manuellement sur le serveur.

L'enregistrement automatique peut se produire lorsqu'un agent actif précédemment inconnu demande des vérifications.

Cette fonctionnalité peut s'avérer très pratique pour la supervision automatique de nouveaux nœuds Cloud. Dès qu'un nouveau nœud dans le cloud apparait, Zabbix lance automatiquement la collecte des données de performance et de disponibilité de l'hôte [**61**].

III.18 Notifications des problèmes

Avec des éléments collectant des données et des déclencheurs conçus pour « déclencher » des situations problématiques, il serait également utile de disposer d'un mécanisme d'alerte qui nous informerait des événements importants même si nous ne regardons pas directement l'interface de Zabbix [**62**].

III.18.1 Types des médias (Media types)

Les médias sont les canaux de diffusion utilisés pour envoyer des notifications et des alertes depuis Zabbix. Il est possible de configurer plusieurs types de supports : E-mail, SMS, Scripts d'alerte [**63**].

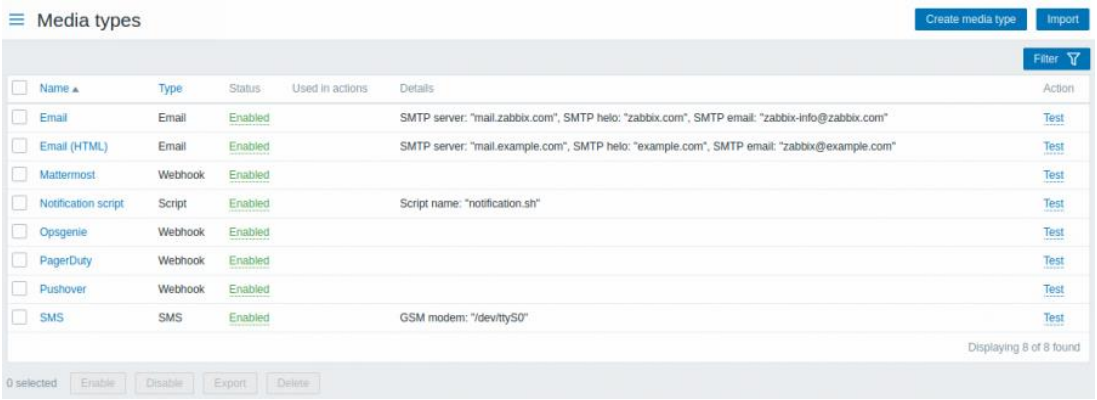


Figure III.18 : Types des Médias.

III.19 Surveillance Web

Zabbix permet de vérifier plusieurs aspects de disponibilité des sites Web. Pour activer la surveillance Web, des scénarios Web doivent être définis.

III.19.1 Scénario Web

Un scénario Web consiste en une ou plusieurs requêtes HTTP ou « étapes » pour vérifier la disponibilité d'un site Web. Les étapes sont périodiquement exécutées par le serveur Zabbix dans un ordre prédéfini. Si un hôte est surveillé par proxy, les étapes sont exécutées par le proxy [**64**].

Les informations suivantes sont collectées dans n'importe quel scénario Web [**64**] :

- Vitesse de téléchargement moyenne par seconde pour toutes les étapes du scénario entier ;
- Numéro de l'étape qui a échoué ;
- Dernier message d'erreur.

Les informations suivantes sont collectées à chaque étape du scénario Web :

- Vitesse de téléchargement par seconde ;
- Temps de réponse ;
- Code de réponse.

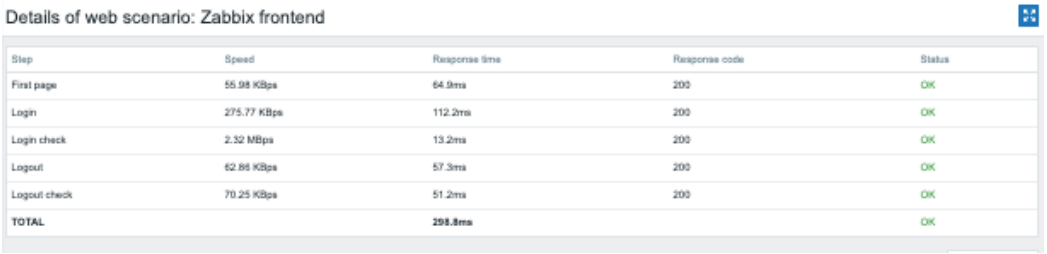


Figure III.19 : Présentation des détails du scénario web.

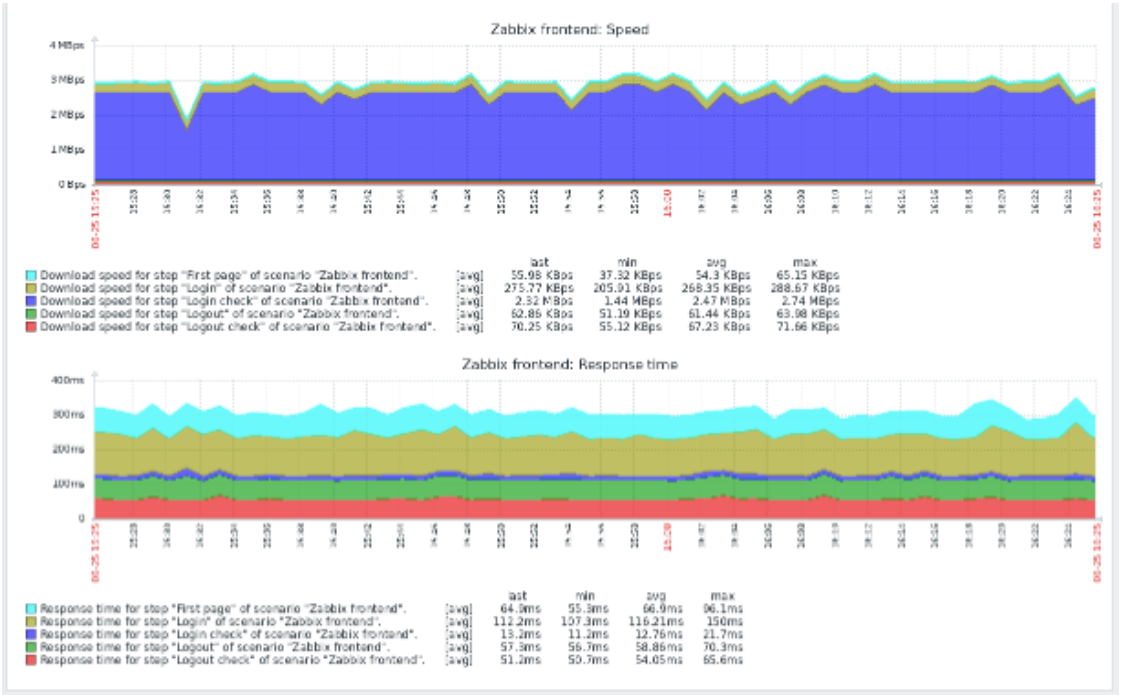


Figure III.20: Surveillance Web.

III.20 Surveillance de la machine virtuelle

Zabbix peut utiliser des règles de découverte de bas niveau pour découvrir automatiquement les hyperviseurs VMware et les machines virtuelles et créer des hôtes pour les surveiller, sur la base de prototypes d'hôtes prédéfinis.

La supervision de la machine virtuelle s'effectue en deux étapes. Premièrement, les données de la machine virtuelle sont collectées par les processus Zabbix VMware collector. Ces processus obtiennent les informations nécessaires auprès des services Web VMware via le protocole SOAP, les traitent préalablement et les stockent dans la mémoire partagée du serveur Zabbix. Ces informations sont ensuite récupérées par les pollers à l'aide des clés VMware des vérifications simples de Zabbix [**65**].

III.21 Surveillance distribuée (Distributed monitoring)

Zabbix fournit un moyen efficace et fiable de surveiller une infrastructure informatique distribuée à l'aide de proxies Zabbix [**66**].

III.21.1 Proxies

Un proxy Zabbix peut collecter des données de performances et de disponibilité pour le compte du serveur Zabbix. De cette façon, un proxy peut assumer une partie de la charge de collecte de données et décharger le serveur Zabbix.

En outre, l'utilisation d'un proxy est le moyen le plus simple de mettre en œuvre une surveillance centralisée et distribuée, lorsque tous les agents et proxys relèvent d'un seul serveur Zabbix et que toutes les données sont collectées de manière centralisée. Un proxy Zabbix peut être utilisé pour [**67**]:

- Surveiller les emplacements distants ;
- Décharger le serveur Zabbix lors de la surveillance de milliers d'appareils ;
- Simplifier la maintenance de la surveillance distribuée ;

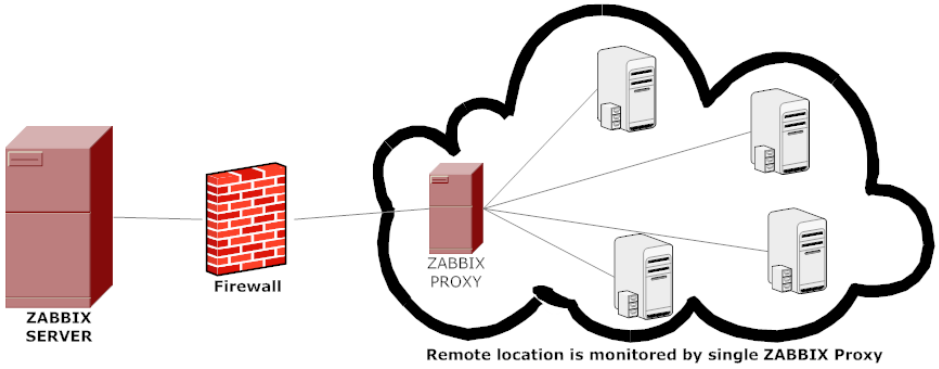


Figure III.21 *:* Surveillance distribuée.

Toutes les données collectées par le proxy sont stockées localement avant d'être transmises au serveur. De cette façon, aucune donnée n'est perdue en raison de problèmes de communication temporaires avec le serveur [**67**].

III.22 Surveillance de Windows

Zabbix prend en charge la surveillance Microsoft Windows, la surveillance sous Windows à l'aide des configurations d'éléments (Template) et de l'agent Zabbix, également en utilisant la prise en charge intégrée de WMI (Windows Management Instrumentation) [**46**].

La surveillance Microsoft Windows comprend :

- Performances Windows (telles que la charge du processeur, l'utilisation du réseau, l'espace disque) ;
- Découvrir automatiquement les services Windows [**46**];
- Prise en charge du système de journal des événements dans l'agent Zabbix [**46**] ;
- Le nombre d'interfaces disponibles sur l'ordinateur Windows.

III.23 Bases de données

Zabbix utilise la base de données pour stocker toutes les informations. Afin de surveiller la disponibilité et les performances des bases de données, Zabbix prend en charge la surveillance des systèmes de gestion de bases de données suivants [**68**] :

- Oracle.
- MySQL.
- PostgreSQL.

- SQLite.

La performance et la disponibilité inclut :

- Utilisation de la bande passante réseau.
- Taux de perte de paquets.
- Taux d'erreur d'interface.
- L'espace disque libre est faible.
- Pas de collecte de données SNMP.
- La connexion réseau est en panne.
- Utilisation élevée du Processeur ou de la mémoire.

III.24 API

L'API Zabbix permet de récupérer et de modifier par programmation la configuration de Zabbix et donne accès aux données historiques. Elle est largement utilisée pour [**69**] :

- Créer de nouvelles applications pour s'interfacer avec Zabbix ;
- Intégrer Zabbix avec un logiciel tiers ;
- Automatiser les tâches de routine.

III.25 Rapports

Un rapport est un enregistrement formel d'informations dans un format organisé. Il indique ce qui s'est passé et ce qui a été fait.

III.25.1 Rapport sur les performances du réseau et de la Disponibilité

Zabbix offre la possibilité de tracer les informations nécessaires pour suivre l'utilisation des ressources et planifier les mises à niveau dans différents rapports détaillés.

La création rapide des rapports en cas de problèmes est une partie nécessaire d'un projet ou de la performance d'un réseau.

Les rapports peuvent être :

- Rapports d'utilisation sur CPU, mémoire, disque ;

- Rapport de trafic;
- La journalisation.

- **Rapport sur l'utilisation CPU**

Le rapport sur l'utilisation du CPU résume la quantité de CPU actuellement utilisée dans le système. Lorsqu'il atteint 100 %, le profil utilise tout le CPU disponible.

La figure affiche un bref historique de l'utilisation du CPU sous forme de graphique.

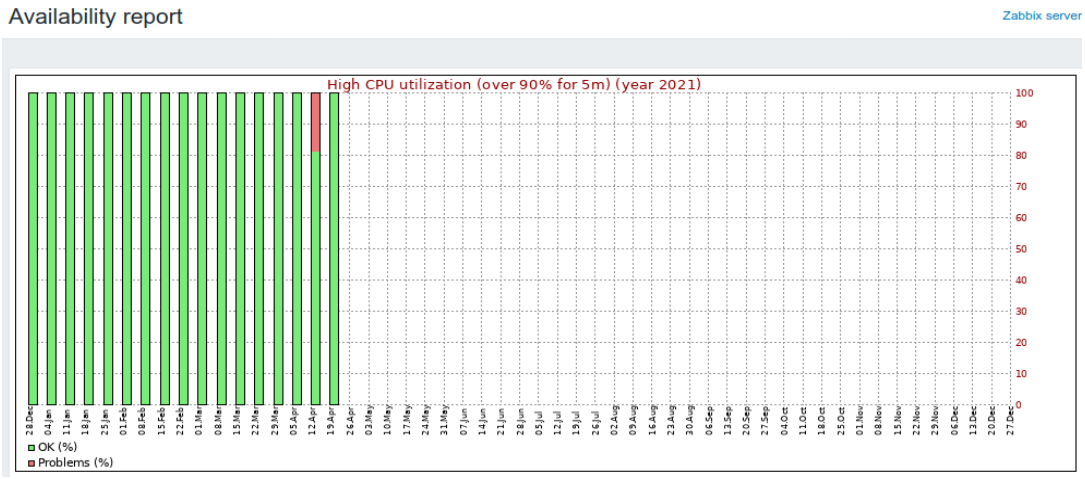


Figure III.22 : Rapport d'utilisation CPU.

- **Rapport sur l'utilisation de la mémoire**

Ceci indique la quantité de mémoire qui a été utilisée et la quantité disponible. La surveillance de l'utilisation de la mémoire est importante, les performances peuvent être réduites si l'utilisation de la mémoire atteint des niveaux critiques.

- **Rapport sur l'utilisation de l'espace disque**

Les pannes du disque entraînent l'arrêt du serveur. La surveillance de l'utilisation de l'espace disque est donc une tâche importante pour tout administrateur. Le rapport de disque inclut la disponibilité de l'espace disque dans les serveurs.

III.25.2 Rapports sur les problèmes

- **Rapport sur l'âge moyen**

Affiche l'âge moyen des problèmes non résolus pour un projet ou un filtre. Cela permet de voir si le backlog est mis à jour [**44**].

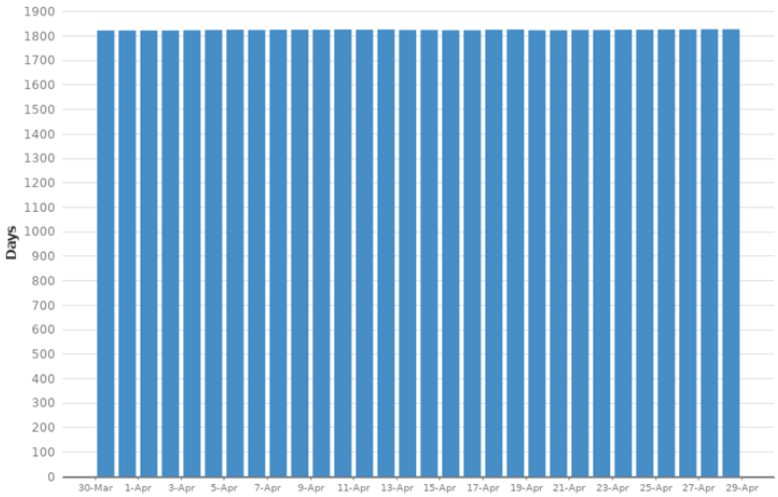


Figure III.23 *:* Age moyen des problèmes.

Ce graphe montre le nombre moyen des jours pendant lesquels les problèmes n'ont pas été résolus [**44**].

- **Rapport sur les problèmes créés et résolus**

Les cartes ont créé des problèmes par rapport aux problèmes résolus sur une période donnée. Cela peut aider à comprendre si l'arriéré global augmente ou diminue.

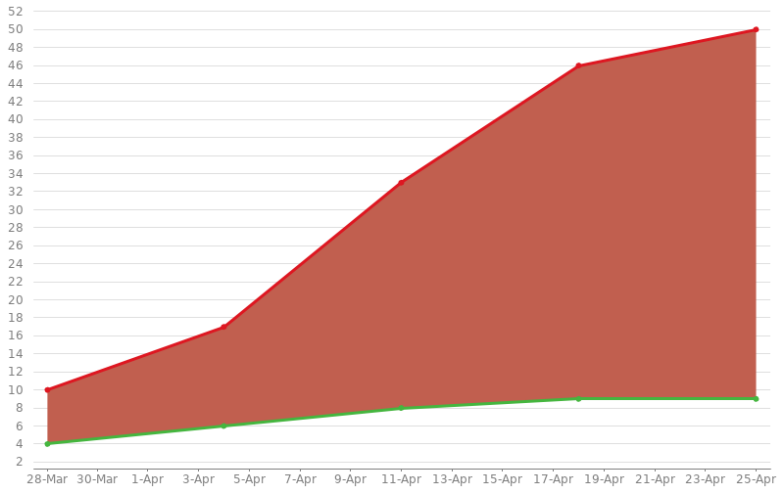


Figure III.24 : Rapport des problèmes créés et résolus.

Ce graphe montre le nombre de problèmes créés par rapport au nombre de problèmes résolus au cours des 30 derniers jours [**44**].

Rouge : Le nombre des problèmes créés.

Vert : Le nombre des problèmes résolus.

- **Rapport sur les problèmes récemment créés**

Affiche le nombre des problèmes créés sur une période donnée pour un projet / filtre, et combien ont été résolus. Cela aide à comprendre si l'équipe suit les travaux entrants.

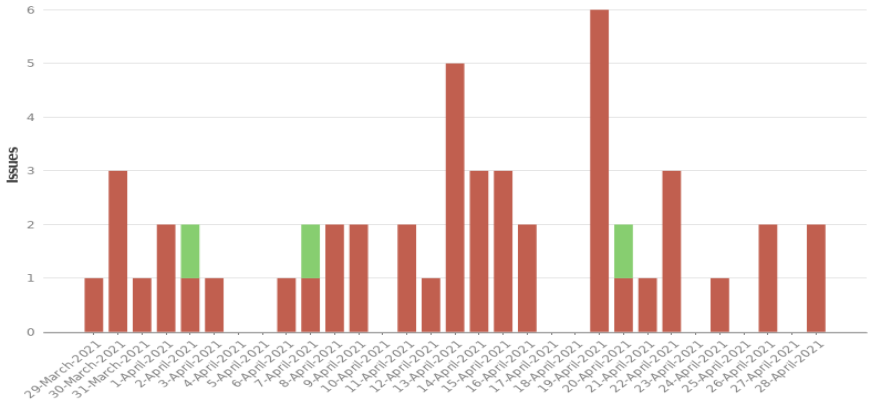


Figure III.25 : Rapport des problèmes récemment créés.

Ce graphique montre les problèmes créés au cours des 30 derniers jours [**44**].

- **Rapport sur le temps de résolution**

Affiche le temps nécessaire pour résoudre un ensemble de problèmes pour un projet / filtre. Cela permet d'identifier les tendances et les incidents afin d'approfondir les recherches.

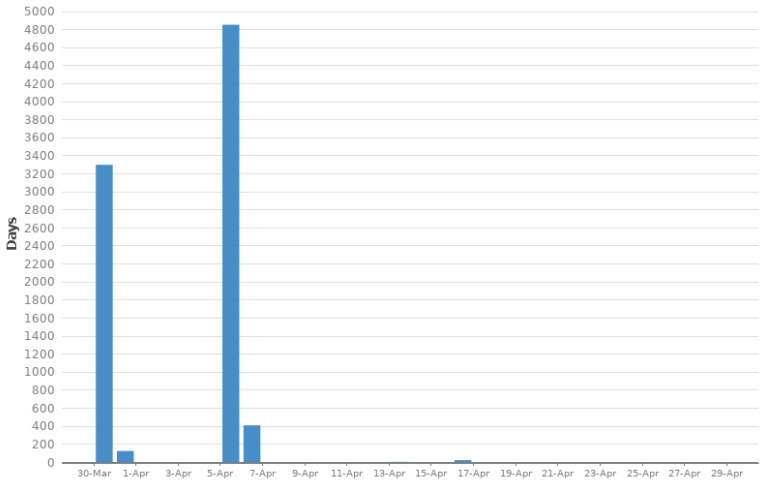


Figure III.26 : Rapport de temps de résolution des problèmes.

Ce graphe montre le nombre moyen des jours que les problèmes ont pris pour être résolus [**44**].

- **Rapport de groupe par niveau unique**

Affiche les problèmes regroupés par un champ particulier pour un filtre. Cela

nous permet de regrouper les résultats de la recherche par champ et de voir l'état général de chaque groupe [**44**].

III.25.3 La journalisation et La notification

Les logs sont des journaux d'événements sur l'état du système dans lesquels les utilisateurs peuvent afficher les détails des opérations (notifications, commandes à distance) effectuées dans une action [**70**].

Chaque action a une date d'entrée, un type et un message. L'administrateur reçoit une notification par e-mail.

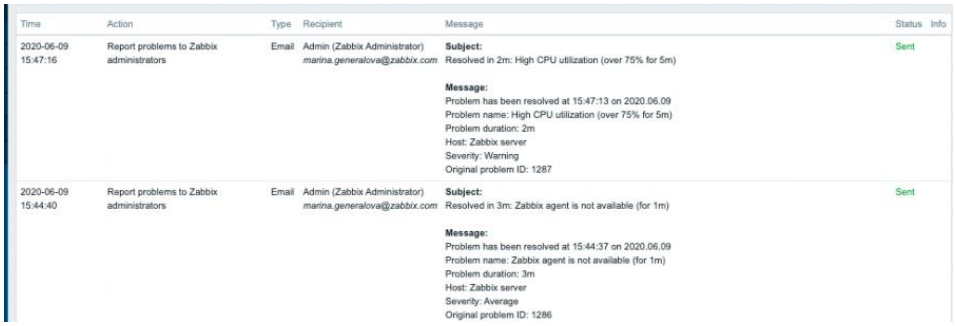


Figure III.27 : Représentation des journaux d'actions.

Dans la section Notifications, un rapport sur le nombre de notifications envoyées à chaque utilisateur est affiché [**71**].

From	Till
2020-12-28 00:00	2021-01-04 00:00
2021-01-04 00:00	2021-01-11 00:00
2021-01-11 00:00	2021-01-18 00:00
2021-01-18 00:00	2021-01-25 00:00
2021-01-25 00:00	2021-02-01 00:00
2021-02-01 00:00	2021-02-08 00:00

Figure III.28 *:* Rapport des nombres de notifications effectuées.

III.26 Conclusion

Zabbix est une solution de surveillance libre, fonctionnant dans une architecture centralisée et distribuée. Elle permet à l'administrateur de connaître à tout moment l'état du système (L'état des nœuds, L'état des serveurs. etc.), d'envoyer des alertes, d'assurer la disponibilité et de générer des rapports graphiques.

Après avoir découvrir cet outil et expliquer ses fonctionnalités, l'étape suivante consistera à tester l'application Zabbix.

Chapitre IV : Tests et Résultat

IV.1 Introduction

D'après le chapitre précédant, on a conclu que, Zabbix est une solution de supervision complète et puissante et surtout abordable pour ceux qui cherche à marquer sur un système de gestion de réseau open-source.

Dans ce dernier chapitre nous allons installer le logiciel Zabbix au sein du réseau informatique de notre université afin de tester les différentes fonctionnalités qu'il dispose pour surveiller les périphériques de notre réseau.

IV.2 Introduction Générale sur le logiciel de supervision Zabbix

Zabbix est un outil pratique et facile à mettre en place, conçu pour surveiller des millions de dispositifs, des applications comme les bases de données (MySQL, Oracle, Maria DB. etc.), la disponibilité des services et de surveiller les machines virtuelles.

Zabbix fonctionne à l'aide de trois composants essentiels le serveur qui est le composant principal et permet la surveillance à distance ou en local.

Il existe aussi l'agent Zabbix, contrairement au serveur l'agent est disponible sur presque tous les systèmes d'exploitation (Windows, Linux, MacOs, etc.).

Après que l'agent collecte toutes les données et les envoie au serveur. Les données collectées seront stockées sur la base de données du serveur comme MySQL, PostgreSQL, et Oracle, et ensuite l'administrateur peut voir les données collectées sur le frontend.

IV.3 Recommandations système

Nous recommandons le système suivant :

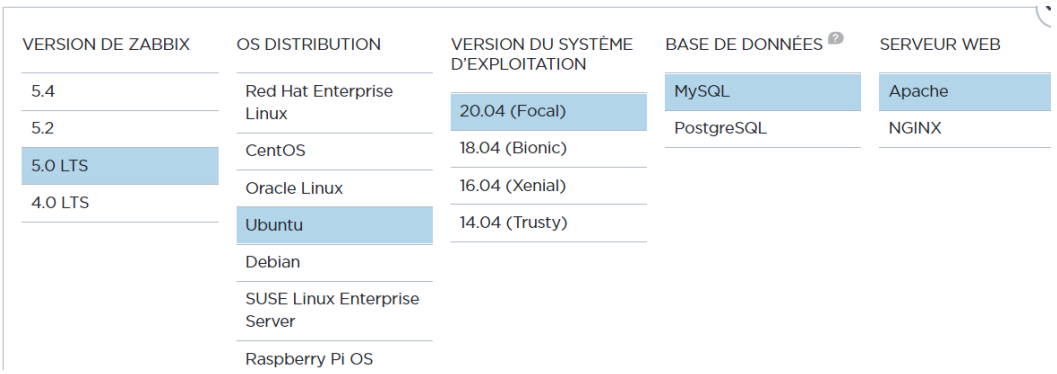


Figure IV.1 : Recommandations système.

Zabbix nécessite à la fois de la mémoire physique et de la mémoire disque. 128 Mo de mémoire physique et 256 Mo d'espace disque libre pourraient être un bon point de départ. Cependant, la valeur de la mémoire disque requise dépend évidemment du nombre d'hôtes ainsi que des paramètres qui seront supervisé [**72**].

Tableau IV-1: Exemples de configuration matérielle.

Nom	Plateforme	CPU/Mémoire	Base de données	Hôtes supervisés
Small	Ubuntu Linux	PII 350MHz 256MB	MySQL MyISAM	20
Medium	Ubuntu Linux 64 bit	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64 bit	Intel Dual Core 6400	4GB RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

IV.4 Schéma utilisé

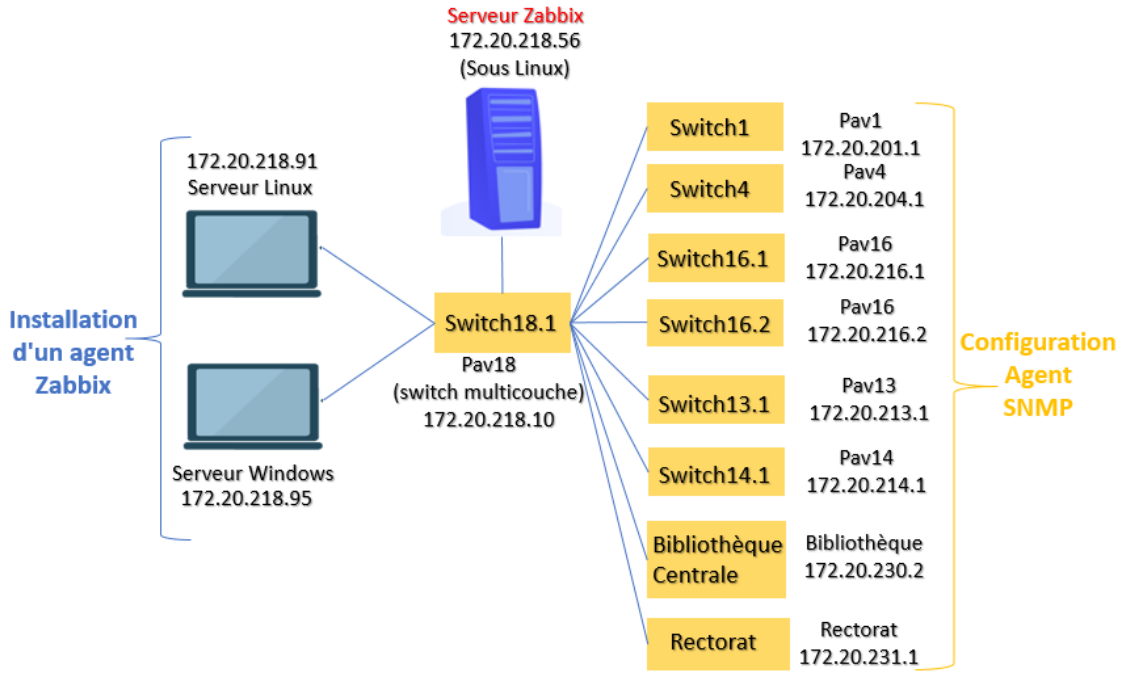


Figure IV.2: Topologie du réseau.

La figure (IV.2) représente la topologie du réseau sur lequel nous allons développer notre application au sein de l'université de Saad DAHLEB Blida.

Afin de tester la surveillance et les alertes de Zabbix, certaines étapes doivent être effectuées :

Neuf commutateurs Cisco seront surveillés par l'agent SNMP.

Deux serveurs, l'un est Windows et le second est Linux, seront surveillés par l'agent Zabbix.

Mais d'abord le serveur Zabbix sera installé sur la machine linux…

IV.5 Installation et configuration Zabbix

Sur le réseau virtuel crée par l'université, on prend une machine virtuelle nommée « Ubuntu20211 » sur laquelle un système d'exploitation Linux Ubuntu est installé pour installer aussi le serveur Zabbix.

On choisit d'installer Zabbix à partir de packages de la page de téléchargement du site officiel de Zabbix https://www.zabbix.com/download.

On choisit ensuite la plateforme : Zabbix 5.0, Ubuntu, 20.04 Focal, MySQL pour la base de données et Apache pour le serveur web.

IV.5.1 Installation du référentiel Zabbix

On commence l'installation en introduisant les commandes suivantes dans le Terminal :

```
usdb1@usdb1-virtual-machine:~$ sudo su
[sudo] Mot de passe de usdb1 :
root@usdb1-virtual-machine:/home/usdb1# wget https://repo.zabbix.com/zabbix/5.0
/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
```

Figure IV.3: Installation du référentiel Zabbix.

IV.5.2 Installation du serveur Zabbix, le fronted et l'agent

Installation de tous les composants pour MySQL, l'interface utilisateur frontale et l'agent.

```
root@usdb1-virtual-machine:/home/usdb1# apt install zabbix-server-mysql zabbix-
frontend-php zabbix-apache-conf zabbix-agent
```

Figure IV.4: Installation du serveur Zabbix, le fronted et l'agent.

IV.5.3 Création de la base de données initiale

Si on ne dispose pas d'une base de données, on doit la créer dans cette étape puis continuer l'installation :

```
mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0.02 sec)

mysql> create user zabbix@localhost identified by 'P@ssw0rd';
Query OK, 0 rows affected (0.02 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql> quit;
```

Figure IV.5: Création de la base de données initiale.

IV.5.4 Importer le schéma

Sur le serveur Zabbix, on importe le schéma et les données initiaux, en insérant notre nouveau mot de passe.

```
root@usdb1-virtual-machine:/home/usdb1# zcat /usr/share/doc/zabbix-server-mysql
*/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
```

Figure IV.6: Importer le schéma.

IV.5.5 Connexion et configuration du serveur frontal Zabbix

Le serveur Zabbix est maintenant opérationnel, il nous reste qu'à récupérer son adresse IP avec la commande « ipconfig » pour se connecter.

```
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 193.194.83.186  netmask 255.255.255.224  broadcast 193.194.83.191
        inet6 fe80::a4bc:ffb2:1f69:9c66  prefixlen 64  scopeid 0x20<link>
```

Figure IV.7: Récupération de l'adresse IP du serveur Zabbix.

Maintenant, on peut visiter notre serveur à partir du site :

http://193.194.83.186/zabbix

On appuie plusieurs fois sur Etape suivante. A la fin on peut se connecter à la nouvelle installation terminée du serveur Zabbix en utilisant les informations d'identification par défaut :

Nom d'utilisateur : **Admin**

Mot de passe : **zabbix**

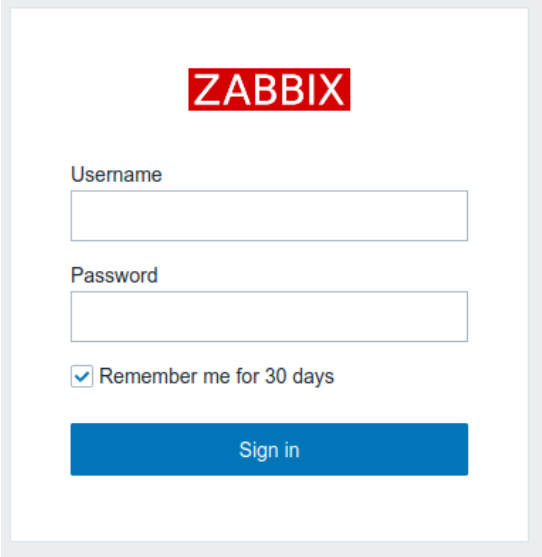


Figure IV.8: Connexion au serveur Zabbix.

IV.6 Surveillance avec SNMP

IV.6.1 Switch

IV.6.1.1 Configuration Switch Multicouche

Nous allons commencer par le switch 18, qui est le switch qui connecte tous les hôtes existant sur le même sous-réseau que le serveur Zabbix.

Le switch 18 et tous les switches du réseau seront surveillés par le protocole SNMP.

a. Configuration SNMP

```
switch>enable
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
switch(config)#snmp-server community public RO
switch(config)#snmp-server community private RW
switch(config)#exit
```

Une fois le switch est configuré, nous exécutons la commande snmpwalk après l'avoir installé pour nous assurer que le serveur Zabbix peut surveiller le switch.

S'il n'y a pas de réponse pour la commande snmpwalk (timeout), cela signifie que quelque chose ne va pas et que le serveur ne peut pas accéder à l'hôte par SNMP.

```
usdb@usdb-virtual-machine:~$ snmpwalk  -v2c -c public 172.20.218.10 1.3.6.1.2
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version 12.1(8a)EW1,
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
C"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.448
```

Figure IV.9: Configuration SNMPwalk.

b. Ajouter Le Switch dans Zabbix

On accède maintenant au tableau de bord Zabbix. Dans le champ configuration on sélectionne l'option Hôte puis sur Créer un nouvel hôte pour saisir les informations ci-dessous afin de créer un commutateur appelé switch18.1 représentant le premier commutateur du pavillon 18.

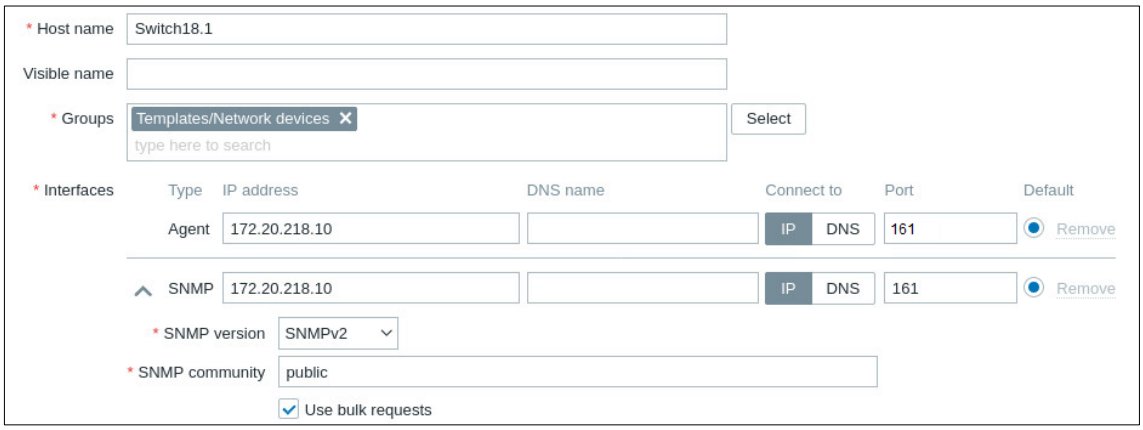


Figure IV.10: Ajouter le switch multicouche.

Après la création de l'hôte, il est important d'associer un modèle prédéfini à notre hôte SNMP pour la supervision.

Par défaut, Zabbix est livré avec une grande variété de modèles de surveillance. On accède à l'onglet Modèles (Template) en haut de l'écran, ensuite on clique sur le bouton Sélectionner pour rechercher le modèle nommé : Template Net Cisco IOS SNMPv2.

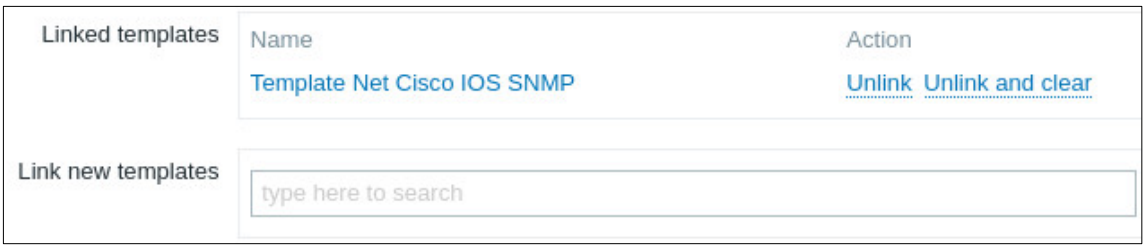


Figure IV.11 *:* Attribuer un modèle au Switch multicouche.

Une fois La configuration est terminée, la couleur verte sur SNMP indique que le switch fonctionne.

IV.6.1.2 Configuration Switch1

a. Vérification du protocole SNMP

Sur la console du serveur Zabbix, on fait un ping au switch1 pour vérifier l'accessibilité de ce dernier dans le réseau.

```
usdb@usdb-virtual-machine:~$ ping 172.20.201.1
PING 172.20.201.1 (172.20.201.1) 56(84) bytes of data.
64 octets de 172.20.201.1 : icmp_seq=1 ttl=255 temps=0.588 ms
64 octets de 172.20.201.1 : icmp_seq=2 ttl=255 temps=0.579 ms
64 octets de 172.20.201.1 : icmp_seq=3 ttl=255 temps=6.91 ms
^C
```

Figure IV.12 *:* Ping du serveur Zabbix au switch1.

On utilise la commande SNMPWALK pour tester la communication SNMP entre le serveur Zabbix et le commutateur. Dans notre cas le switch1 qui a l'adresse IP 172.20.201.1 s'agit d'un commutateur Cisco comme le montre l'échantillon de la sortie SNMPWALK.

```
usdb@usdb-virtual-machine:~$ snmpwalk  -v2c -c public 172.20.201.1 1.3.6.1.2.1
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 04:33 by yenanh"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.694
iso.3.6.1.2.1.1.3.0 = Timeticks: (17172250) 1 day, 23:42:02.50
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "SWC2960-PV1-A12-S11"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 2
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
```

Figure IV.13 *:* Vérification du protocole SNMP.

b. Ajouter le Switch1 dans Zabbix

Comme chaque hôte doit être surveillé, nous commençons par créer un hôte, sur la configuration de l'hôte nous mettons les paramètres essentiels suivants :

- Le nom d'hôte;
- Le groupe;
- La version SNMP, Le Port et L'adresse IP du Switch1.

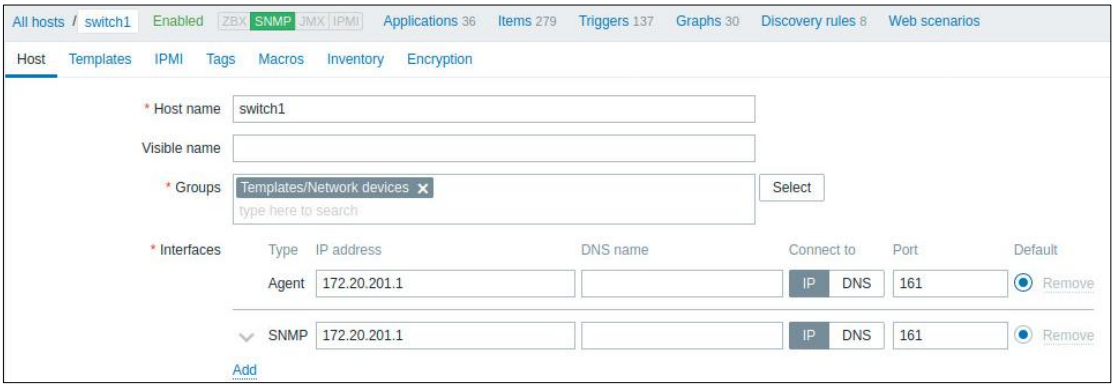


Figure IV.14: Ajouter le switch1 dans Zabbix.

Ensuite, nous devons associer le commutateur créé à un modèle (Template) de moniteur de réseau spécifique Template Net Cisco IOS SNMP.

A la fin, on termine cette configuration en cliquant sur mettre à jour.

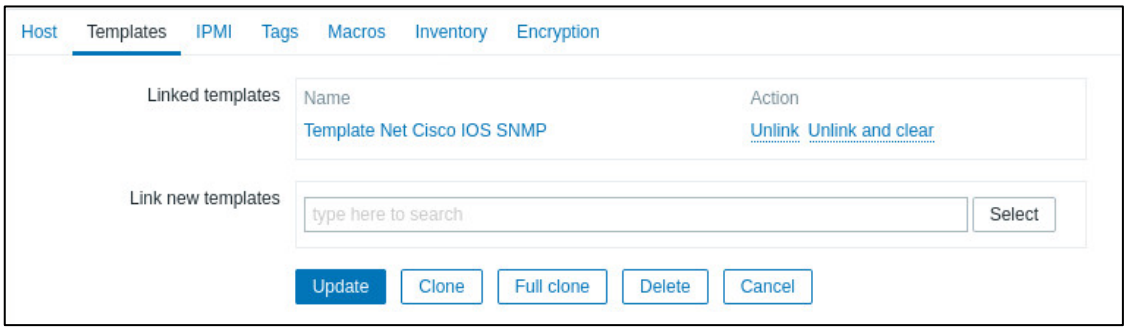


Figure IV.15 : Attribuer un modèle au switch1.

Après quelques minutes, nous pourrons voir le résultat initial sur le tableau de bord Zabbix qui indique que le switch1 est activé.

Le résultat final prendra au moins une heure.

Figure IV.16 : Switch1 activé.

De la même façon qu'on a fait avec le commutateur « switch1 », on ajoute le reste des commutateurs : switch4, switch16.1, switch16.2, switch13.1, switch de la bibliothèque centrale, switch du Rectorat, switch14.1

IV.7 Surveillance avec l'agent Zabbix

IV.7.1 Serveur Linux

Pour que le serveur Zabbix puisse récolter des informations sur la machine ubuntu21, on installe sur cette dernière un agent Zabbix qui fonctionnera comme un service Linux.

IV.7.1.1 Téléchargement et installation du référentiel

Tout d'abord on doit télécharger et installer le référentiel sur le serveur.

```
root@usdb1-virtual-machine:/home/usdb1# wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
--2021-05-11 13:01:57--  https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb
```

Figure IV.17: Téléchargement du référentiel.

```
root@usdb1-virtual-machine:/home/usdb1# dpkg -i zabbix-release_5.0-1+focal_all.deb
```

Figure IV.18: Téléchargement du référentiel.

IV.7.1.2 Installation de l'agent

Pour installer l'agent on court la commande suivante :

```
root@usdb1-virtual-machine:/home/usdb1# sudo apt install zabbix-agent
```

Figure IV.19: Installation de l'agent.

IV.7.1.3 Configuration de l'agent

On accède au fichier de l'agent Zabbix pour modifier ces paramètres ServerActive, Hostname et en associant l'adresse IP du serveur Zabbix 172.20.218.56 puis, on les enregistre :

```
root@usdb1-virtual-machine:/home/usdb1# sudo nano /etc/zabbix/zabbix_agentd.conf
```

Figure IV.20: Configuration du fichier de l'agent Zabbix.

IV.7.1.4 Ajouter le serveur linux dans Zabbix

On accède au menu des configurations puis dans l'onglet Hôte qui contient les attributs généraux de l'hôte qu'on doit les remplir avec ce qui convient à notre hôte Ubuntu21.

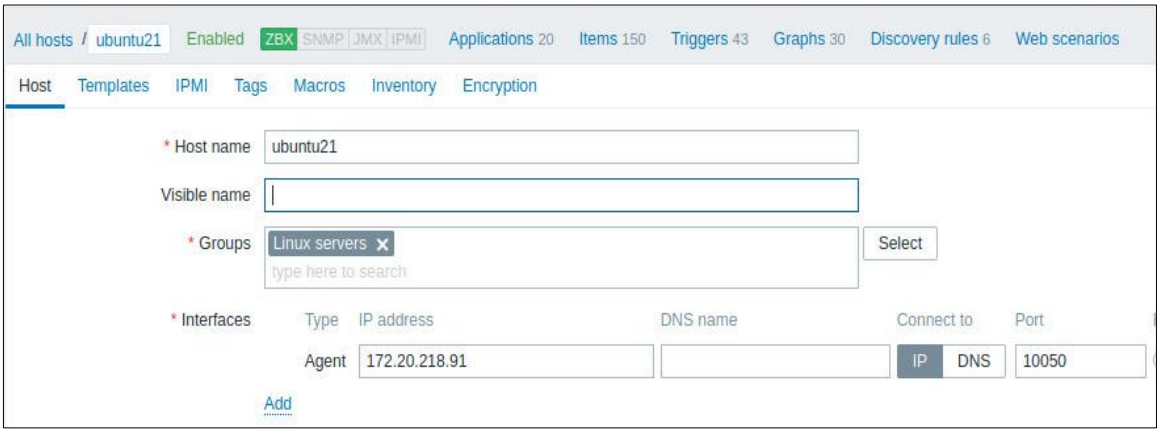


Figure IV.21 : Ajouter le serveur Linux dans Zabbix.

L'onglet Modèles nous permet de lier des modèles à l'hôte, pour lier un nouveau modèle, on saisit le nom du modèle dans le champ lier les nouveaux modèles.

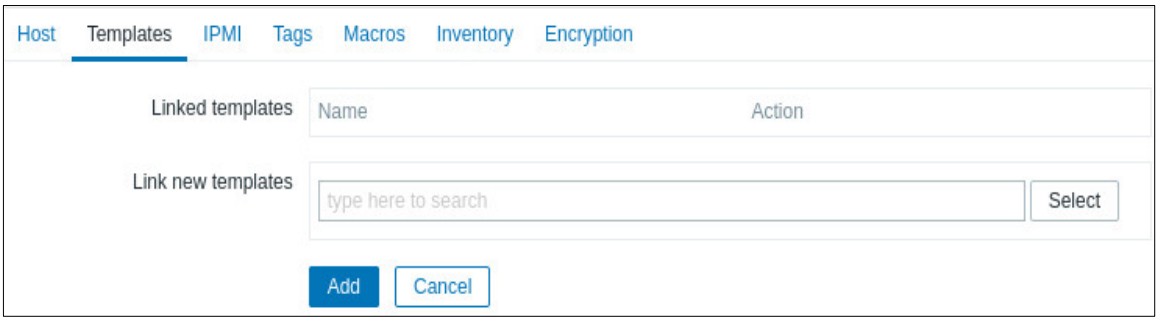


Figure IV.22 : Attribuer un modèle au serveur Linux.

Une liste des modèles correspondants apparaîtra pour sélectionner le modèle approprié.

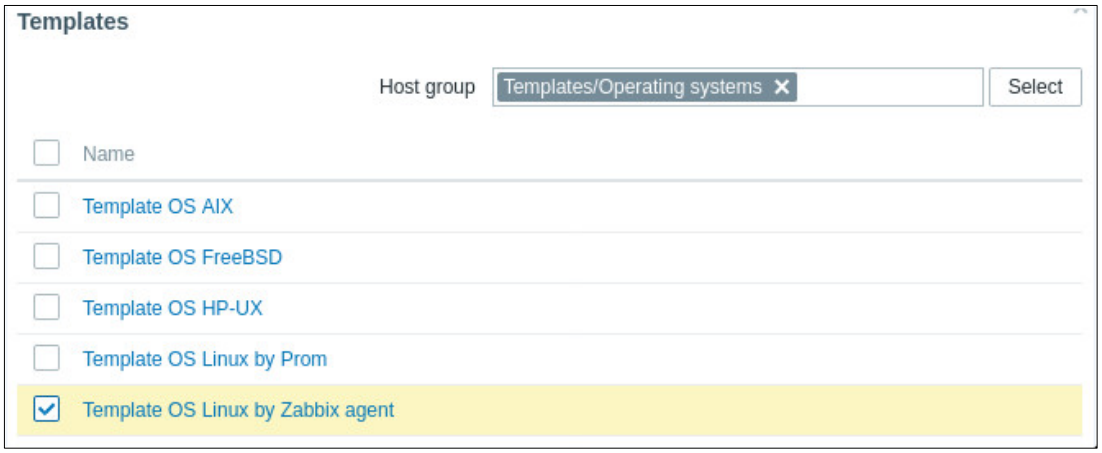


Figure IV.23 **:** Sélectionner le modèle pour le serveur Linux.

Le nouveau modèle sera lié à l'hôte lorsque le formulaire de configuration de l'hôte est enregistré.

IV.7.2 Serveur Windows

IV.7.2.1 Installation de l'agent Zabbix sous Windows

Tout comme le serveur Linux, on installe sous une machine Windows nommée «WIN-3E5TKD1D310» un agent Zabbix. Le serveur Windows fonctionne comme un service Windows, il est chargé de collecter les données et de les envoyer au serveur Zabbix.

Nous devons d'abord sélectionner la plateforme comme suit, puis lancer le téléchargement.

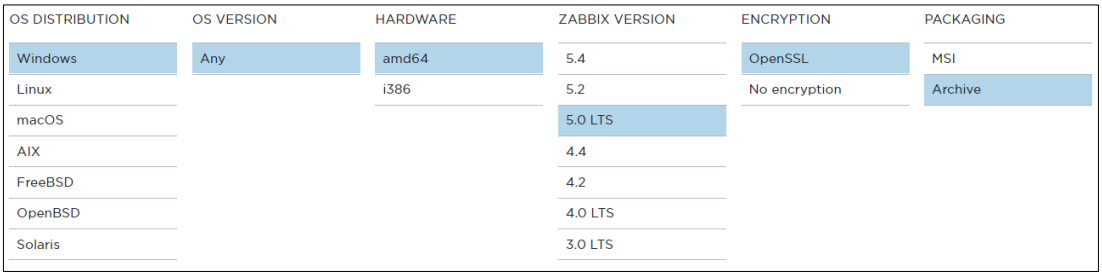


Figure IV.24 *:* Téléchargez et installez l'agent Zabbix.

L'archive téléchargé sera extrait dans un fichier de configuration pour l'agent Zabbix, dans l'invite de commande nous installons l'agent comme un service Windows.

```
C:\>zabbix\bin\zabbix_agentd.exe -c c:\zabbix\conf\zabbix_agentd.conf -i
zabbix_agentd.exe [284]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [284]: event source [Zabbix Agent] installed successfully

C:\>_
```

Figure IV.25 *:* Installation d'agent comme un service Windows.

Pour effectuer des vérifications sur le serveur, nous avons besoin de l'adresse IP du serveur Zabbix, et de définir le nom d'hôte de l'agent.

On ouvre le fichier Zabbix_agentd.conf et on commence à le modifier ;

- Sur ServerActive on doit ajouter l'adresse IP du serveur Zabbix (172.20.218.56) pour les vérifications actives, afin que l'agent puisse envoyer ses données.

```
# Default:
#ServerActive=

ServerActive=172.20.218.56
```

Figure IV.26 : Affichage de la modification du serveur.

- Puis on met la même adresse sur le serveur pour autoriser les vérifications passives et garder le port par défaut comme 10050.

```
Server=172.20.218.56
### Option: ListenPort
#   Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050
```

Figure IV.27 *:* Activer les vérifications passives sur l'hôte Windows.

- Ensuite, on change le nom d'hôte qui doit être identique au nom du serveur Windows et qui doit correspondre au nom dans l'interface Zabbix.

```
# Default:
# Hostname=

Hostname=WIN-3E5TKD1D310
```

Figure IV.28 : Modification du nom d'hôte.

IV.7.2.2 Ajouter le serveur Windows dans Zabbix

Tout ce que nous devons faire maintenant est de créer le serveur Windows dans Zabbix, en remplissant les champs comme suit : Ajouter le serveur Windows dans Zabbix.

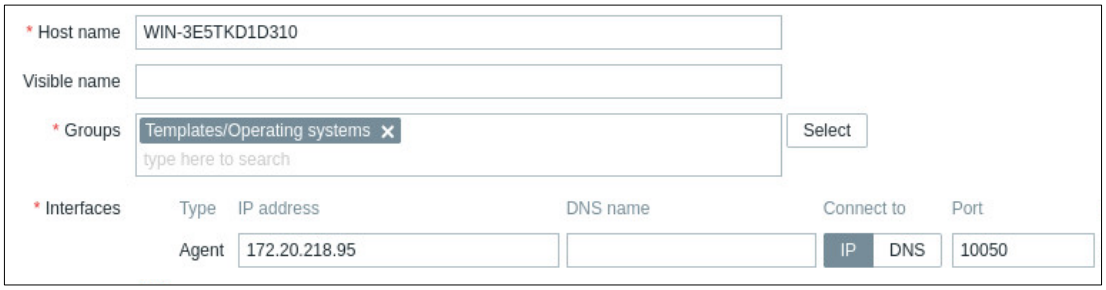


Figure IV.29 : Ajouter un serveur Windows.

Pour recevoir toutes les données des éléments, triggers, graphiques etc. nous

relions l'hôte avec le modèle approprié.

Figure IV.30 : Modèle associé au serveur créé.

Figure IV.31 : Serveur activé.

IV.8 Surveillance web

IV.8.1 Surveillance HTTP à distance à l'aide de scénarios Web

Maintenant, nous configurons des scénarios Web pour vérifier la disponibilité d'un site Web exécuté sur un serveur.

Nous commençons par l'attribution d'un modèle et l'ajouter à un groupe.

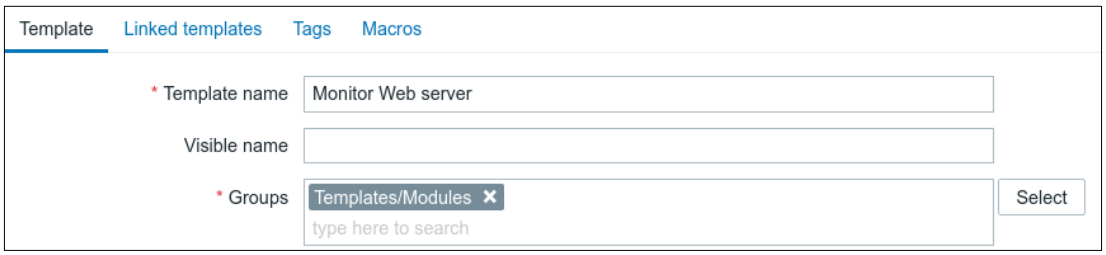


Figure IV.32 *:* Attribution d'un modèle au site web.

Sur l'onglet des scénarios Web, nous ajoutons un scénario Web pour surveiller le site Web. On remplit les paramètres de base du script : nom, intervalle de mise à jour pour tester le scénario, ajouter une application, etc.

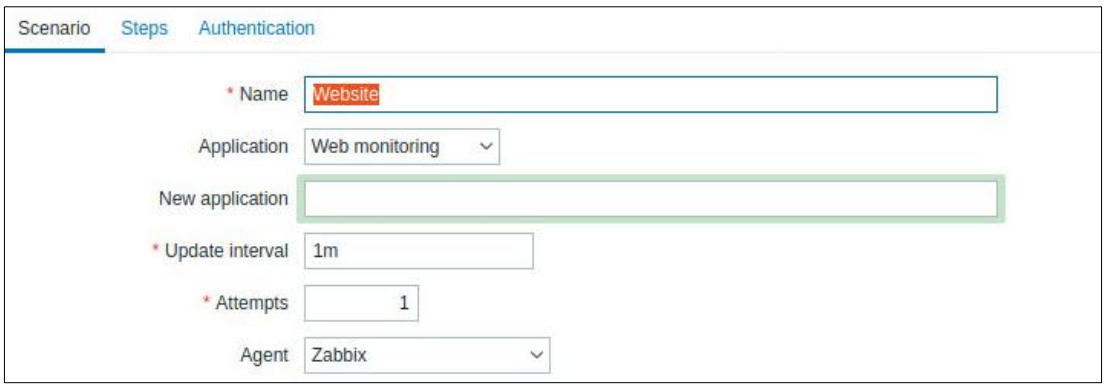


Figure IV.33 : Ajouter un Scénario web.

Dans l'onglet Steps, nous pouvons configurer des étapes pour un scénario Web,

afin que le serveur puisse exécuter des requêtes HTTP pour vérifier la disponibilité du site Web.

Nous spécifions les paramètres de Step : l'identification du site web et l'URL pour connecter les pages à vérifier.

Nous avons choisi de surveiller deux sites web, la plateforme universitaire, le site google.

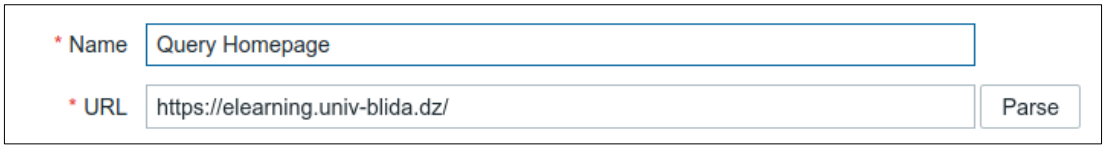


Figure IV.34 : Configuration de Step pour la surveillance du Web.

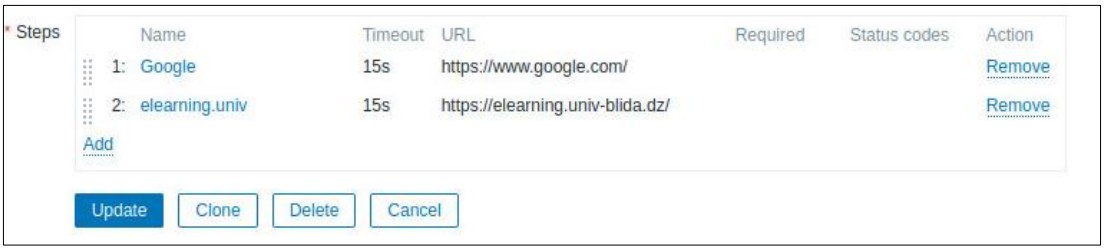


Figure IV.35 : Sites web à surveiller.

Pour les vérifications, le Template de scénario web doit être lié au serveur Windows (WIN-3E5TKD1D310).

Figure IV.36 : Lier le scénario web par le serveur Windows.

IV.9 Surveillance MySQL

Notre serveur Zabbix utilise une base de données MySQL. Nous pouvons surveiller cette base de données à l'aide du modèle : Template DB MySQL by Zabbix agent.

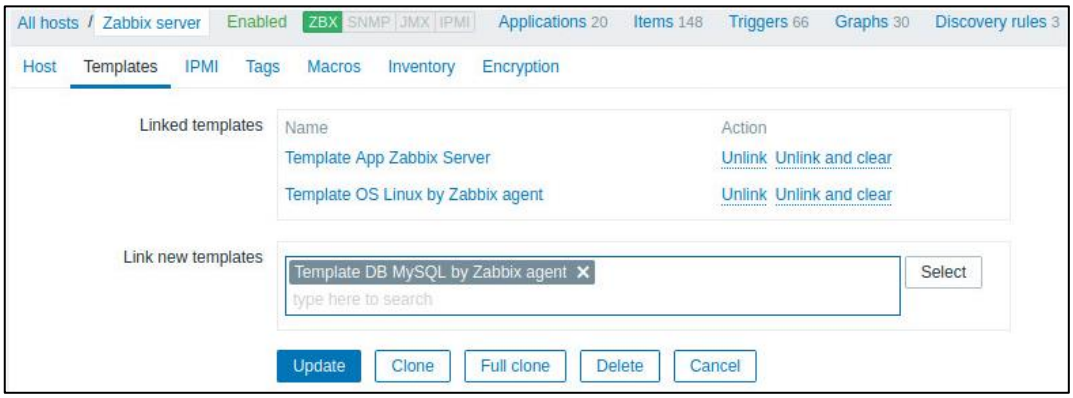


Figure IV.37 : Attribuer un modèle à MySQL.

Après avoir lié ce modèle à notre hôte, cela ne fonctionnera que si on effectue plusieurs autres configurations.

Sur le terminal du serveur Zabbix On crée un nouveau fichier dans le dossier **/etc/zabbix/zabbix_agentd.d/** nommé **template_db_mysql.conf**

```
usdb@usdb-virtual-machine:~$ sudo su
[sudo] Mot de passe de usdb :
root@usdb-virtual-machine:/home/usdb# sudo nano /etc/zabbix/zabbix_agentd.d/template_db_mysql.conf
```

Figure IV.38: Création du fichier de configuration.

On connecte maintenant à MySQL en créant un nouvel utilisateur appelé **zbx_monitor** et en lui accordant le privilège d'utilisation sur toutes les bases de données MySQL à l'utilisateur Zabbix.

```
mysql> CREATE USER 'zbx_monitor'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0,08 sec)

mysql> GRANT USAGE,REPLICATION CLIENT,PROCESS,SHOW DATABASES,SHOW VIEW ON *.* TO 'zbx_monitor'@'localhost';
Query OK, 0 rows affected (0,01 sec)
```

Figure IV.39: Création d'un nouvel utilisateur.

Ensuite, on crée un fichier nommé **.my.cnf** dans le répertoire personnel de l'agent Zabbix pour Linux (/ var / lib / zabbix par défaut).

```
root@usdb-virtual-machine:/home/usdb# cd /var/lib
root@usdb-virtual-machine:/var/lib# mkdir zabbix
root@usdb-virtual-machine:/var/lib# cd zabbix /
bash: cd: trop d'arguments
root@usdb-virtual-machine:/var/lib# cd zabbix/
root@usdb-virtual-machine:/var/lib/zabbix# ls
root@usdb-virtual-machine:/var/lib/zabbix# sudo nano my.cnf
```

Figure IV.40: Création du fichier de configuration.

Après, on ajoute le contenu ci-dessous :

Figure IV.41: Configuration du fichier du répertoire personnel de l'agent Zabbix.

Après environ une minute, nos nouveaux éléments MySQL pour notre hôte commenceront à recevoir des données.

Maintenant, nous devons accéder au tableau de bord du serveur Zabbix et compléter la configuration.

Une fois que nous avons configuré un hôte, nous devons mettre à jour les éléments de surveillance pour commencer à obtenir des données réelles.

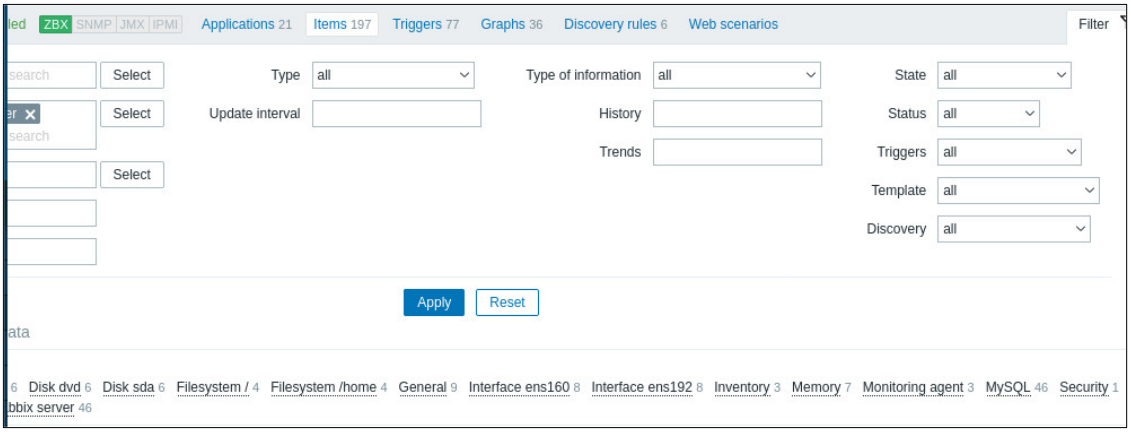


Figure IV.42 : Mettre à jour les éléments de surveillance.

Nous devons également mettre à jour les dernières données pour afficher les dernières valeurs collectées par éléments ainsi que pour accéder à divers graphiques pour les éléments.

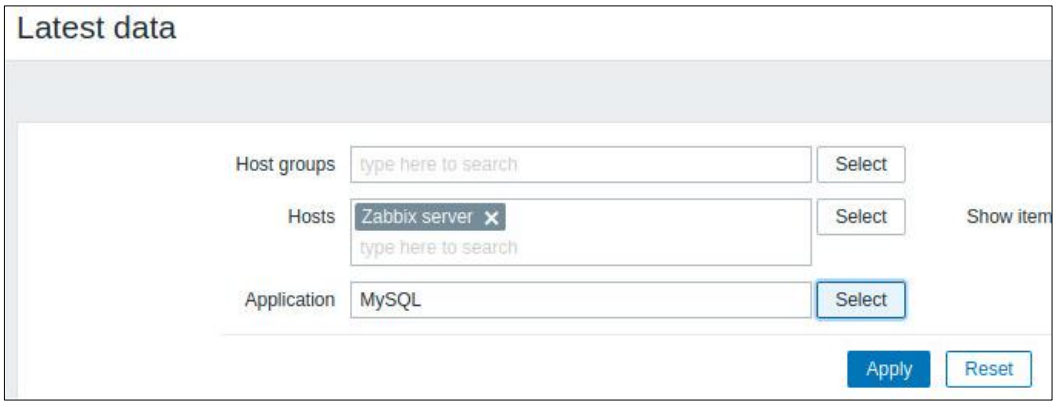


Figure IV.43 *:* Mettre à jour les dernières données.

IV.10 Configuration des notifications

L'administrateur ne peut pas vérifier le tableau de bord à chaque fois pour voir si quelque chose d'important se passe, puisque Zabbix fournit la notification par type de média, il est préférable de l'activer pour que l'administrateur soit notifié chaque fois qu'une alerte se produit.

Nous choisissons la notification par Telegram en utilisant Telegram Bot.

IV.10.1 Création d'un Bot

Tout d'abord, nous devons créer un bot afin que celui-ci puisse traiter automatiquement les messages provenant de Zabbix. Nous démarrons une conversation avec @BotFather et nous choisissons "ZabbixAlertsBot" comme nom pour notre bot.

Figure IV.44: Création d'un bot.

Après avoir créé un bot, nous avons reçu un jeton secret dont nous avons besoin

pour trouver notre identifiant de bot créé sur Telegram. Le jeton secret et l'ID de chat seront nécessaires pour la configuration de Zabbix.

Envoyer "/ start" à "@GetIDsbot" dans Telegram Messenger pour obtenir le chat d'identification.

Figure IV.45: ID chat.

IV.10.2 Configuration type de Media dans Zabbix

Dans Administration → Types de média, nous définissons le nom et le jeton secret de notre bot créé.

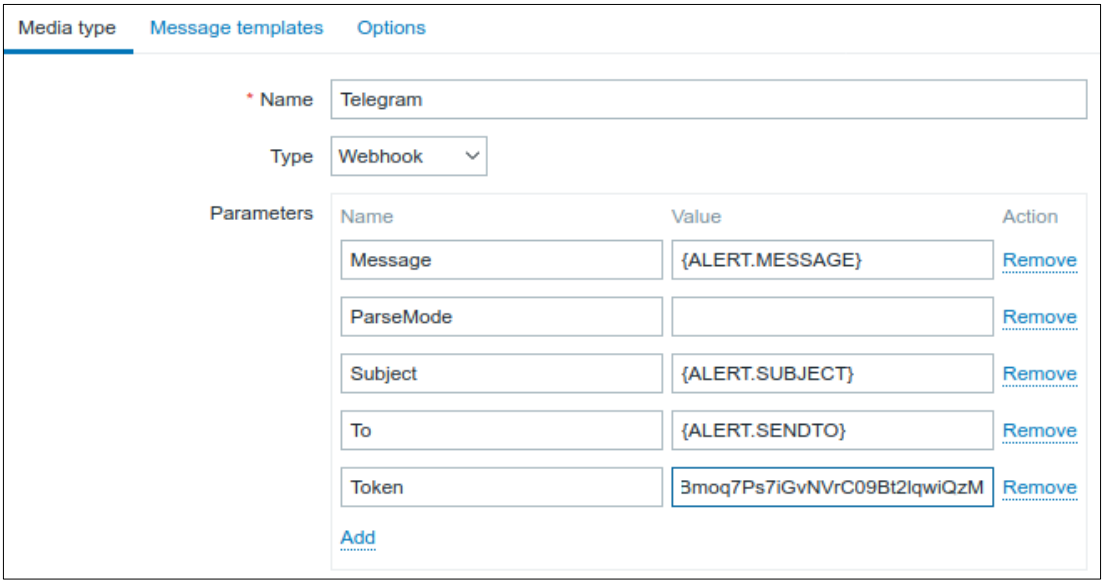


Figure IV.46*:* Configuration de Telegram en tant que média type.

On clique sur update et on teste notre type de média en utilisant notre ID chat sur "To" :

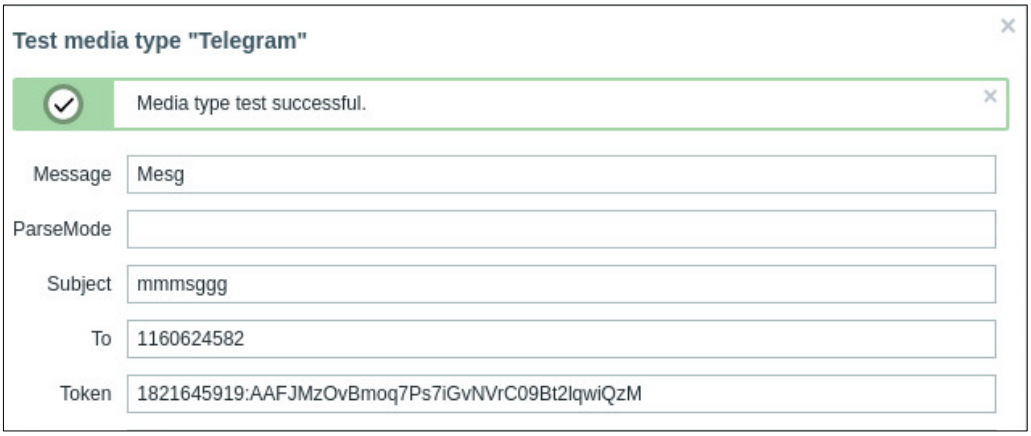


Figure IV.47: Test Telegram réussi.

Après avoir confirmé que le test a réussi, dans Administration → Utilisateurs nous devons créer un utilisateur Zabbix pour recevoir des notifications, nous définissons le type, l'ID du chat, et nous sélectionnons le type de cas que nous voulons être notifiés.

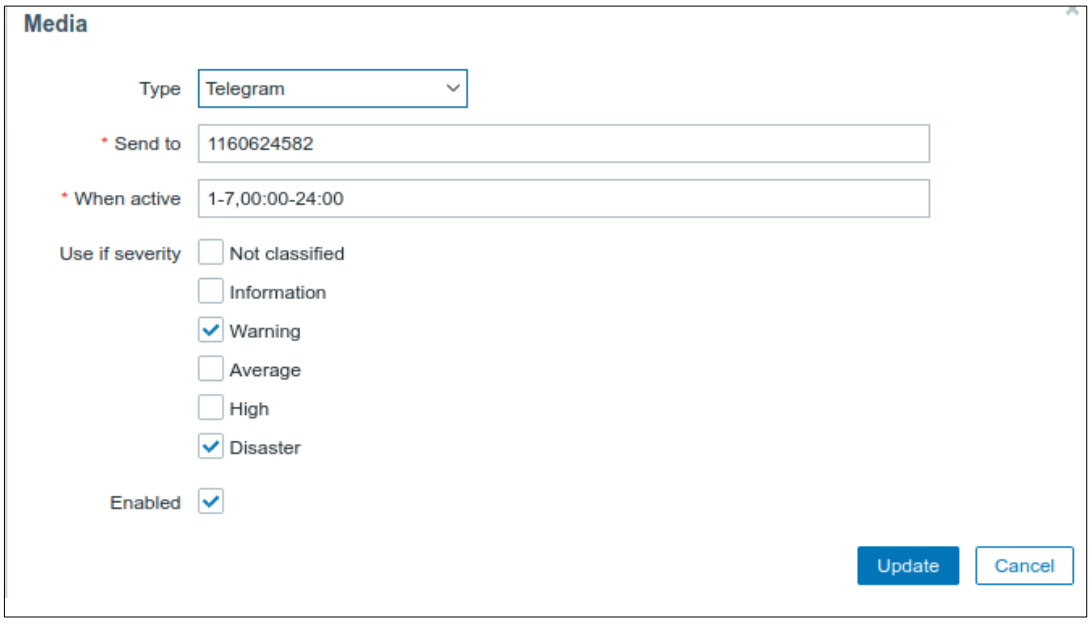


Figure IV.48: Ajout d'un média à un utilisateur.

Pour commencer à recevoir des notifications, nous activons "Report problems to Zabbix administrators" dans les actions de déclenchement.

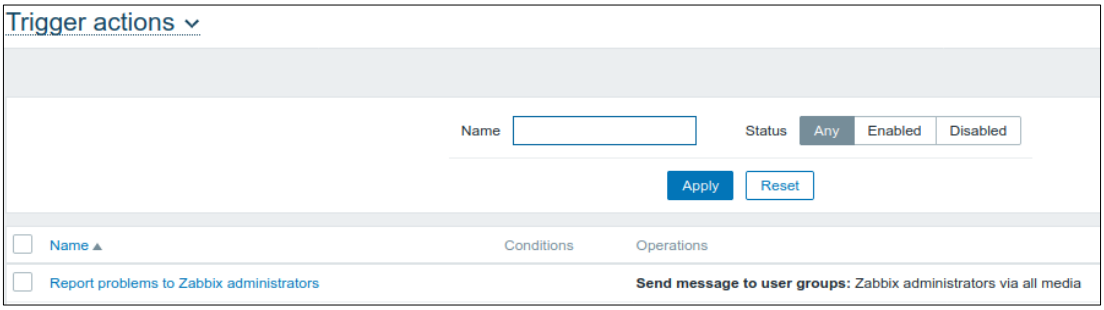


Figure IV.49: Activation d'une action.

IV.11 Création de la carte du réseau

La carte du réseau sera une représentation graphique de la hiérarchie de l'infrastructure du réseau où les différents hôtes qu'on a déjà ajoutés sur le serveur Zabbix sont distribués de façon similaire à leur distribution dans le réseau de l'université.

On commence par la configuration de la carte en créant une nouvelle carte nommée Network.

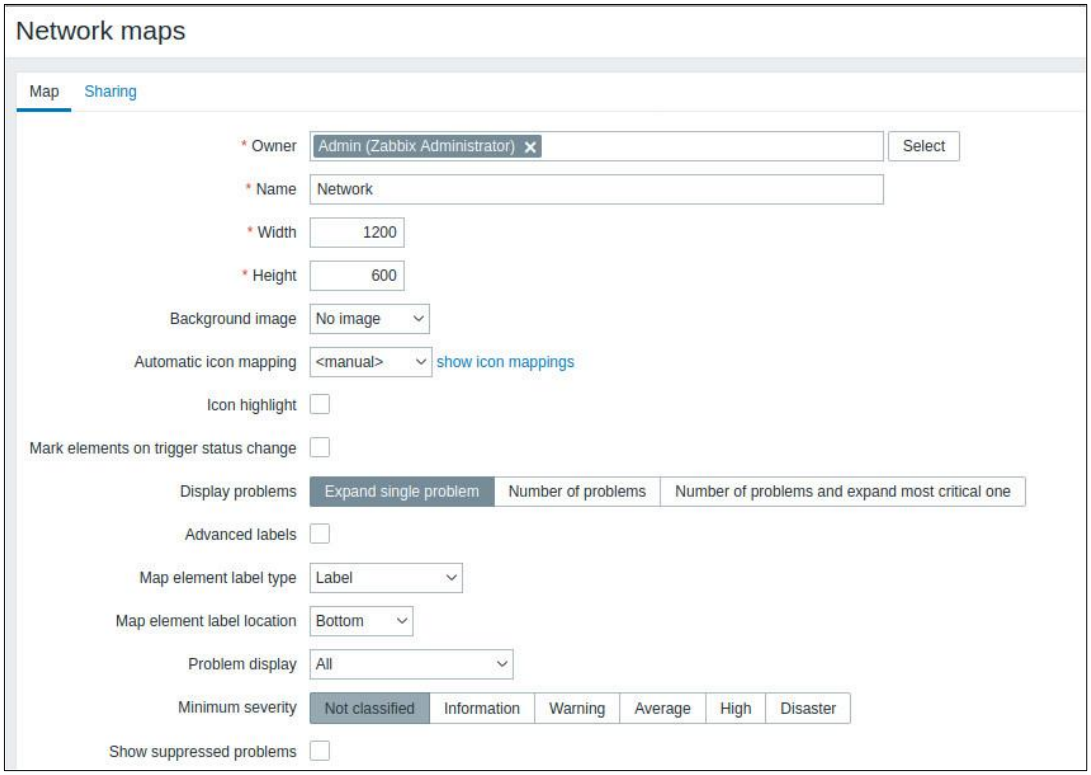


Figure IV.50 *:* Configuration de la carte du réseau.

Puis on ajoute cette configuration, et on commence à créer des icônes représentant les hôtes de notre réseau.

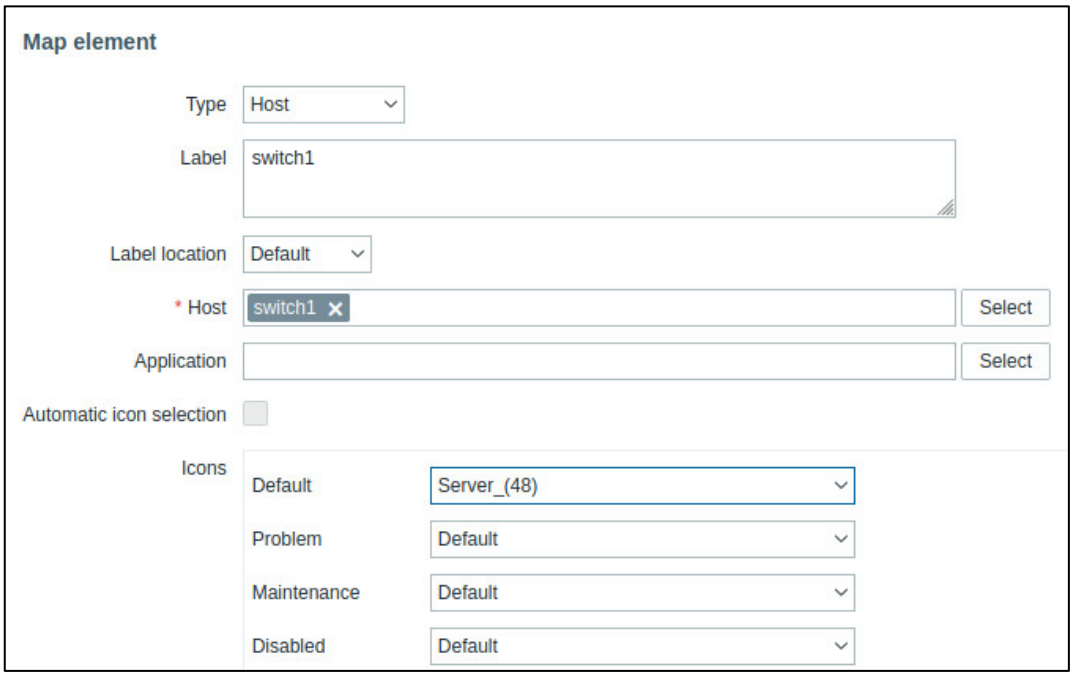


Figure IV.51: Création des icônes.

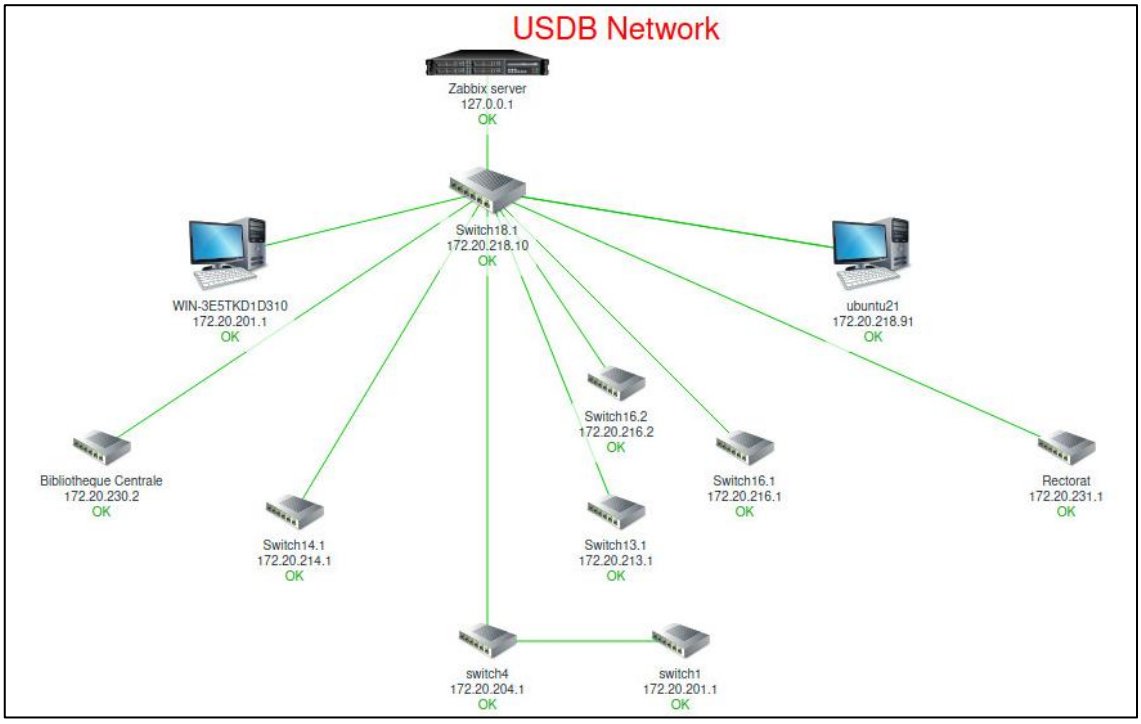


Figure IV.52 : Carte du réseau USDB.

Ensuite, on relie les icones aux hôtes afin que les problèmes d'hôtes apparaissent également sur la représentation graphique comme le montre la figure suivante.

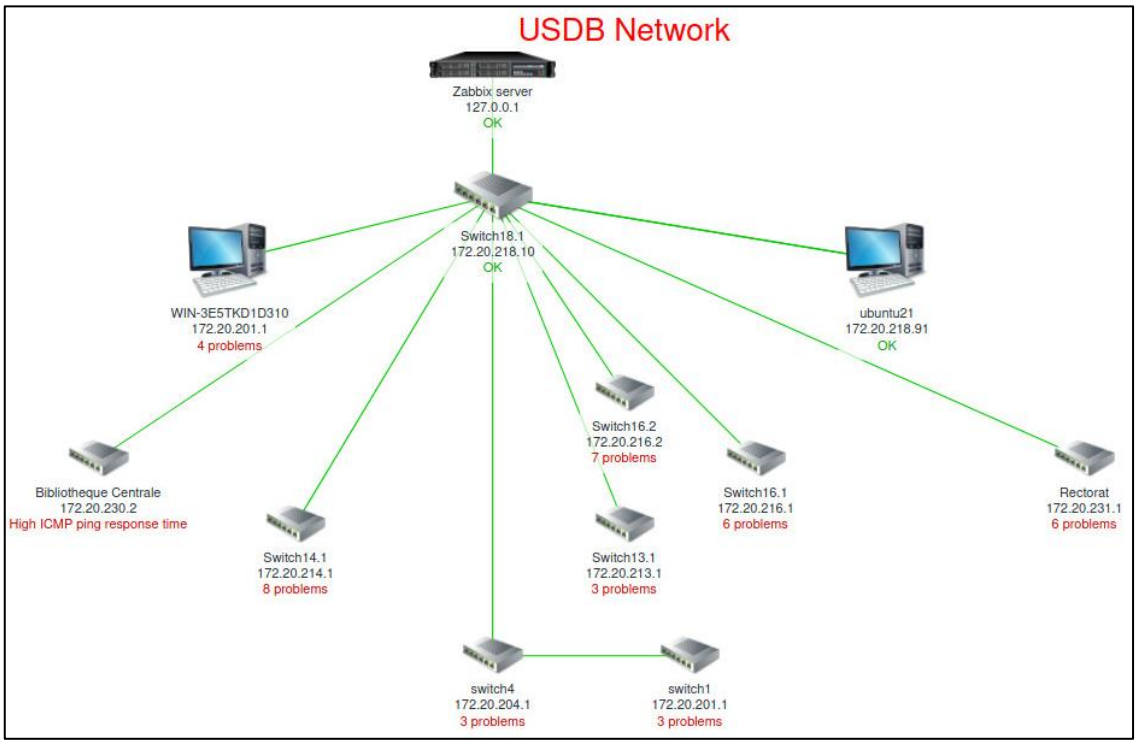


Figure IV.53 *:* Carte du réseau USDB avec les problèmes des hôtes.

IV.12 Les hôtes configurés

Après avoir ajouté et configuré les différents hôtes de notre réseau, il est possible de les afficher, et visualiser dès maintenant les résultats que Zabbix est configuré pour collecter à partir du menu surveillance.

Name	Interface	Availability	Tags	Problems	Status ▲	Latest data	Problems	Graphs
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 36
switch1	172.20.201.1: 161	ZBX SNMP JMX IPMI		3	Enabled	Latest data	Problems 3	Graphs 30
switch4	172.20.204.1: 161	ZBX SNMP JMX IPMI		2	Enabled	Latest data	Problems 2	Graphs 27
Switch18.1	172.20.218.10: 161	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems	Graphs 17
Switch16.1	172.20.216.1: 161	ZBX SNMP JMX IPMI		3 2	Enabled	Latest data	Problems 5	Graphs 25
Switch16.2	172.20.216.2: 161	ZBX SNMP JMX IPMI		3 1	Enabled	Latest data	Problems 4	Graphs 30
Switch13.1	172.20.213.1: 161	ZBX SNMP JMX IPMI		2 1	Enabled	Latest data	Problems 3	Graphs 30
Bibliotheque Centrale	172.20.230.2: 161	ZBX SNMP JMX IPMI		1 1	Enabled	Latest data	Problems 2	Graphs 30
Rectorat	172.20.231.1: 161	ZBX SNMP JMX IPMI		3 1	Enabled	Latest data	Problems 4	Graphs 30
Switch14.1	172.20.214.1: 161	ZBX SNMP JMX IPMI		4 1	Enabled	Latest data	Problems 5	Graphs 52
ubuntu21	172.20.218.91: 10050	ZBX SNMP JMX IPMI		1	Enabled	Latest data	Problems 1	Graphs 30
WIN-3E5TKD1D310	172.20.218.95: 10050	ZBX SNMP JMX IPMI		1 2 1	Enabled	Latest data	Problems 4	Graphs 20

Figure IV.54: Hôtes surveillés par Zabbix.

IV.13 Les Résultats

IV.13.1 Résultats des Switch

La surveillance des ports de commutateur fournit l'état de l'interface (Up ou Down) et aide l'administrateur à suivre les ports utilisés et non utilisés afin de garantir une utilisation optimale des commutateurs dans l'infrastructure.

A partir du menu de surveillance, on accède au champ Dernière donnée pour visualiser des dizaines de résultats de différentes informations que Zabbix a récolté ; sur l'état de tous les interfaces du commutateur, le fonctionnement du CPU et l'utilisation du mémoire…etc.

La figure suivante (IV.55) montre l'état des interfaces du switch18 (Switch multicouche) si elles sont Up ou Down.

Timestamp	Interface Gi1/1(): Operational status	Interface Gi1/2(): Operational status	Interface Gi2/1(): Operational status	Interface Gi2/2(): Operational status	Interface Gi2/3(): Operational status	Interface Gi2/4(): Operational status	Interface Gi2/5(): Operational status	Interface Gi2/6(): Operational status	Interface Gi3/1(): Operational status	Interface Gi3/2(): Operational status	Interface Gi3/3(): Operational status	Interface Gi3/4(): Operational status	Interface Gi3/5(): Operational status	Interface Gi3/6(): Operational status	Interface Vl1(): Operational status
2021-05-27 09:46:41	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:46:08	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:44:45	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:43:49	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:42:45	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:41:41	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:38:41	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)
2021-05-27 09:37:41	down (2)	down (2)	up (1)	up (1)	up (1)	up (1)	up (1)	up (1)	down (2)	up (1)	up (1)	up (1)	down (2)	down (2)	up (1)

Figure IV.55 : Interfaces du switch.

Voici un échantillon des données que Zabbix nous peut donner sur l'interface Fa0/0 du switch1.

Interface Fa0/1() (9 Items)			
Interface Fa0/1(): Bits received	2021-05-25 12:58:12	0 bps	
Interface Fa0/1(): Bits sent	2021-05-25 12:58:12	247.21 Kbps	-50.88 Kbps
Interface Fa0/1(): Duplex status	2021-05-25 12:58:13	fullDuplex (3)	
Interface Fa0/1(): Inbound packets discarded	2021-05-25 12:58:13	0	
Interface Fa0/1(): Inbound packets with errors	2021-05-25 12:58:13	0	
Interface Fa0/1(): Operational status	2021-05-25 12:58:13	up (1)	
Interface Fa0/1(): Outbound packets discarded	2021-05-25 12:58:13	0	
Interface Fa0/1(): Outbound packets with errors	2021-05-25 12:58:12	0	
Interface Fa0/1(): Speed	2021-05-25 12:48:14	10 Mbps	

Figure IV.56 *:* Résultat de surveillance de l'interface fa0/1.

Zabbix peut également récolter des informations sur l'état de la mémoire du commutateur.

Memory (displaying 3 to 6 of 6 Items)		
I/O: Used memory	2021-05-25 12:58:12	1.64 MB
Processor: Free memory	2021-05-25 12:58:13	35.73 MB
Processor: Memory utilization	2021-05-25 13:02:00	15.5161 %
Processor: Used memory	2021-05-25 12:58:12	6.56 MB

Figure IV.57 *:* Résultat de surveillance de la mémoire.

Zabbix nous offre la possibilité d'afficher les résultats sous forme de graphes, on sélectionne les objets désirés et on visualise les graphes.

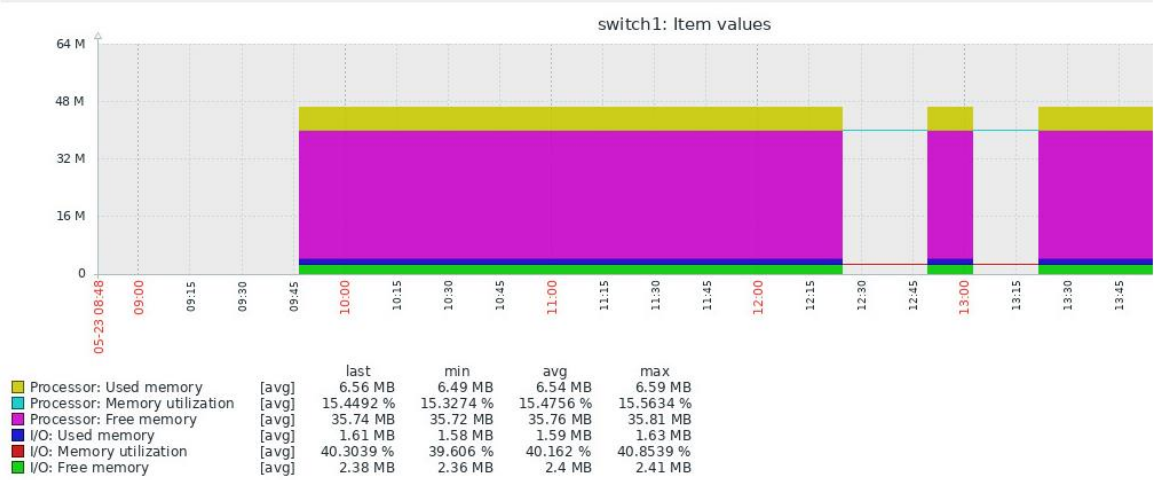


Figure IV.58 *:* Résultat de surveillance de la mémoire switch1.

On peut afficher aussi l'état d'utilisation du CPU :

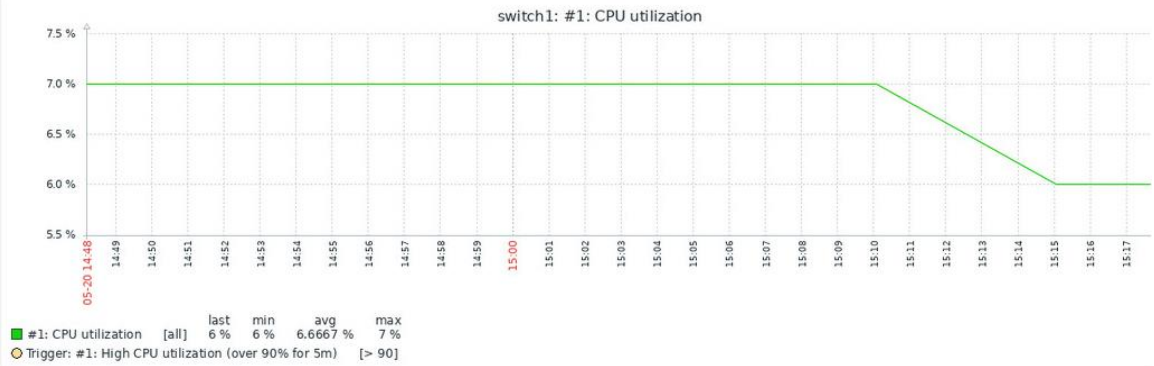


Figure IV.59 : Utilisation du CPU du switch1.

Timestamp	Interface Gi0/2(): Bits received	Interface Gi0/2(): Bits sent	Interface Gi0/2(): Operational status	Interface Gi0/3(): Bits received	Interface Gi0/3(): Bits sent	Interface Gi0/3(): Operational status	Interface Gi0/4(): Bits received	Interface Gi0/4(): Bits sent	Interface Gi0/4(): Operational status	Interface Gi0/5(): Bits received	Interface Gi0/5(): Bits sent	Interface Gi0/5(): Operational status	Interface Gi0/11(): Bits received	Interface Gi0/11(): Bits sent	Interface Gi0/11(): Operational status
2021-05-30 10:39:09	0	0	down (2)	0	0	down (2)	0	0	down (2)	0	0	down (2)	577688	5955200	up (1)
2021-05-30 10:38:09			down (2)			down (2)			down (2)			down (2)			up (1)
2021-05-30 10:37:09			down (2)			down (2)			down (2)			down (2)			up (1)
2021-05-30 10:36:09	0	0	down (2)	0	0	down (2)	0	0	down (2)	0	0	down (2)	550808	5978520	up (1)
2021-05-30 10:35:09			down (2)			down (2)			down (2)			down (2)			up (1)
2021-05-30 10:34:09			down (2)			down (2)			down (2)			down (2)			up (1)

Figure IV.60: Etat des interfaces du switch4.

IV.13.2 Résultat de serveur Linux

L'installation de l'agent Zabbix sur la machine Ubuntu21 a permis au serveur Zabbix de rassembler des informations opérationnelles et les afficher dans le menu surveillance.

Le résultat de surveillance de l'utilisation du CPU est donné comme suit :

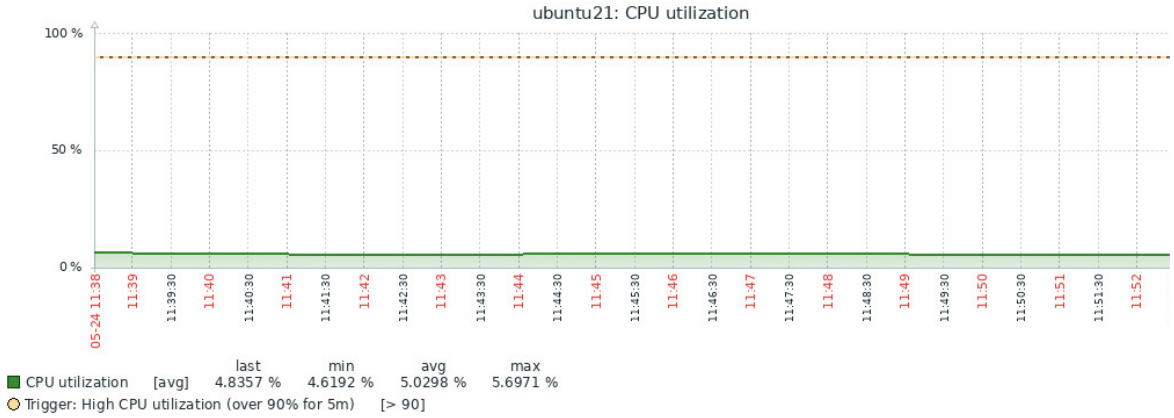


Figure IV.61 *:* Utilisation du CPU de la machine ubuntu21.

D'autres résultats sur le CPU et la charge système sont collectés et affichés :

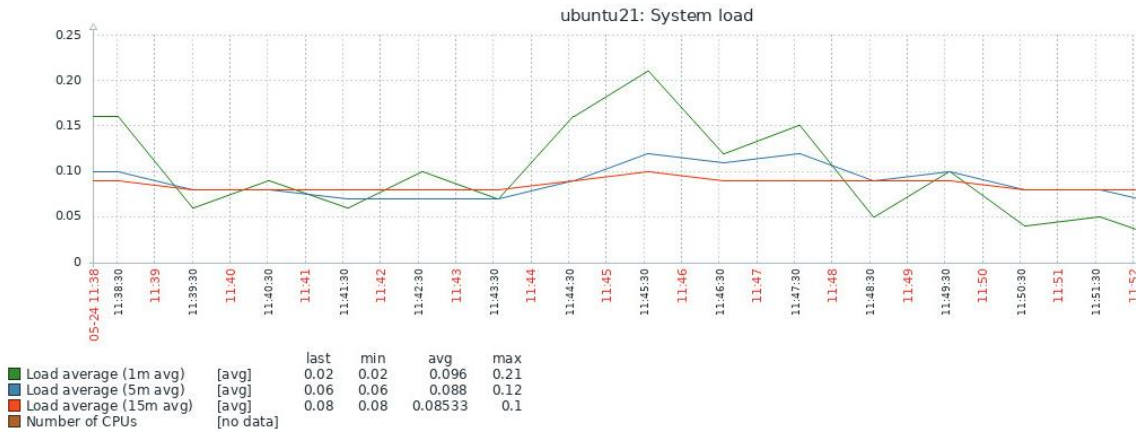


Figure IV.62 : Charge système d'ubuntu21.

Zabbix peut donner aussi des informations sur les processus effectués par la

machine Ubuntu21 sous forme de données ou de graphes, on préfère présenter le résultat sous forme de graphes pour un suivi meilleur.

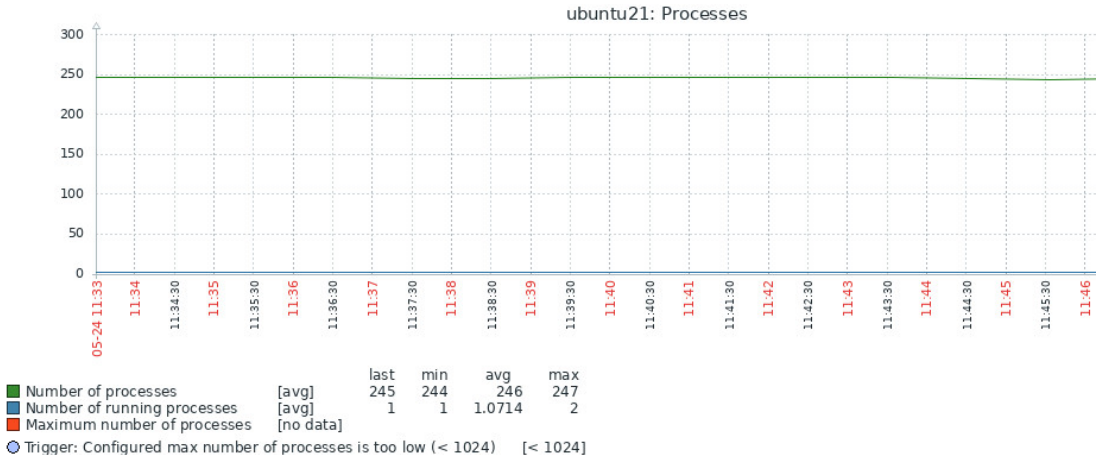


Figure IV.63 : Les processus ubuntu21.

Les résultats de surveillance du trafic réseau sont également affichés, la figure suivante représente le trafic réseau sur l'interface ens160 de la machine Ubuntu21.

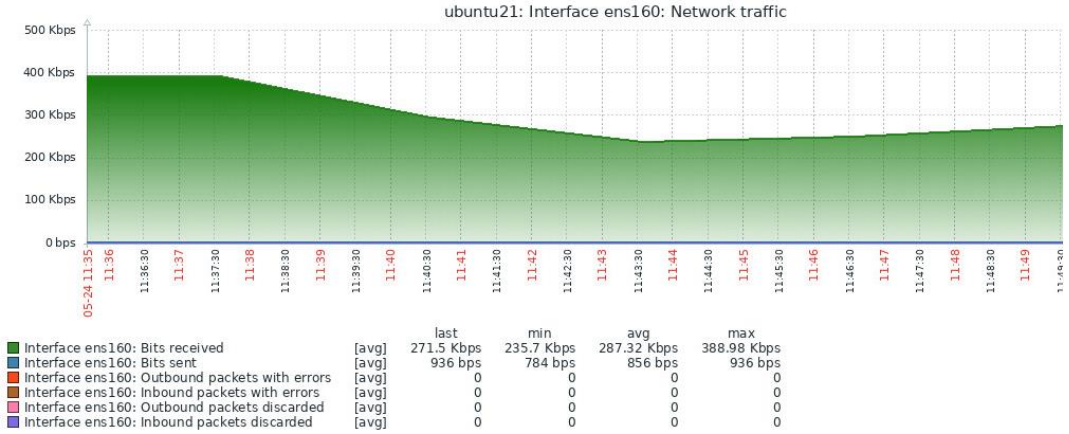


Figure IV.64 *:* Trafic réseau dans l'interface ens160.

Des résultats d'utilisation des disques peuvent être remontés, voici un exemple de surveillance du disque sda et de file d'attente.

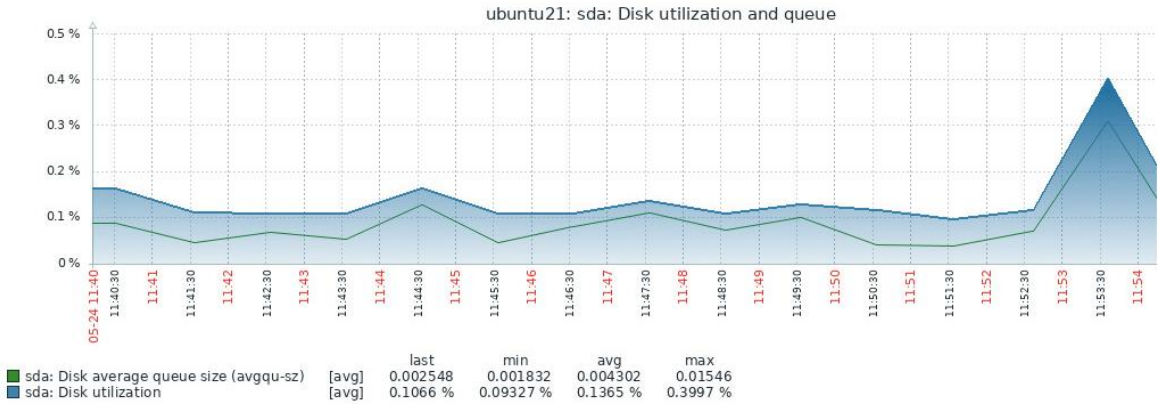


Figure IV.65 *:* Utilisation du disque sda d'ubuntu21.

De plus, Zabbix nous présente le résultat du suivi de l'utilisation de l'espace disque sous forme d'un cercle graphique comme suit :

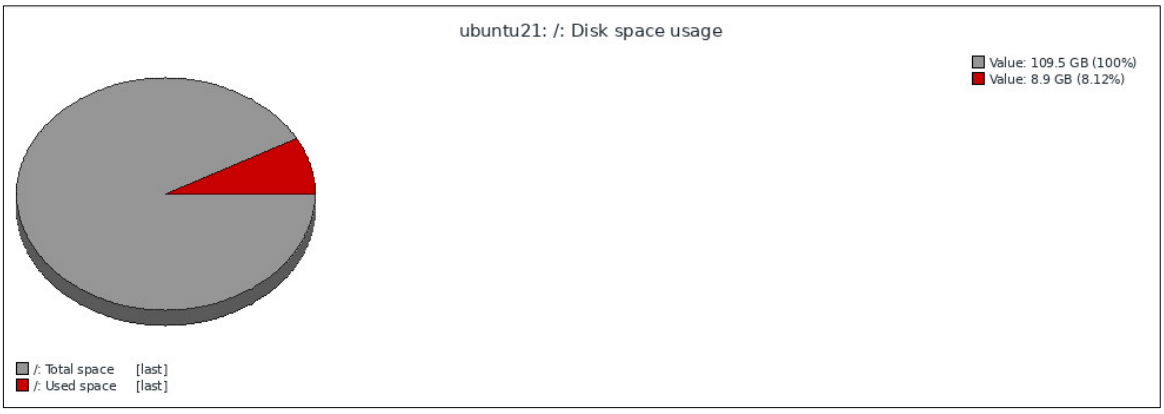


Figure IV.66 : Utilisation de l'espace disque.

IV.13.3 Résultat de serveur Windows

La bonne performance du serveur Windows liée à l'utilisation du CPU, de la mémoire et du disque.

Figure IV.67 : Utilisation CPU.

La figure (IV.67) montre une représentation graphique de l'utilisation du CPU.

La surveillance de l'utilisation de la mémoire permet à l'administrateur d'éviter les problèmes, tels qu'une utilisation élevée de la mémoire qui ralentit le serveur et empêche les programmes et les applications de répondre…etc.

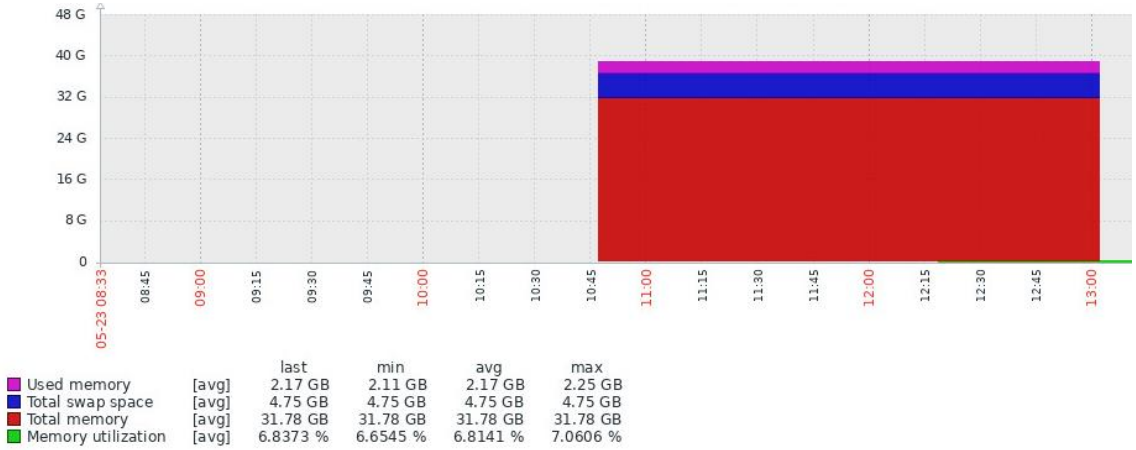


Figure IV.68 *:* Etat de l'utilisation de la mémoire.

Ce graphe illustre l'état de l'utilisation de la mémoire en Go.

Le lecteur C : est responsable du stockage des programmes, des applications et d'autres fichiers importants. Il doit donc être surveillé pour éviter tout risque pour les fichiers de stockage.

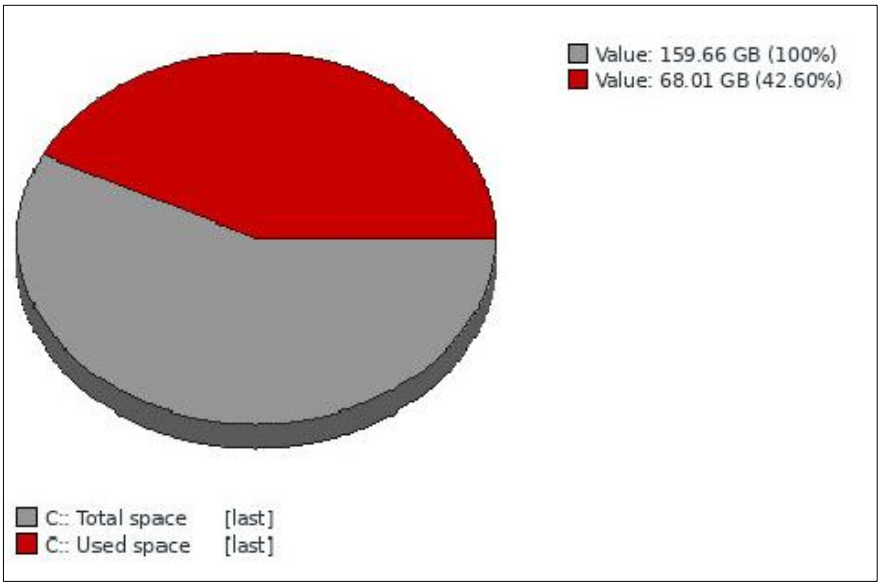


Figure IV.69: Utilisation de l'espace disque C.

La figure (IV.69) montre l'espace total du lecteur C : et la quantité d'espace utilisée.

Maintenant nous passons à la surveillance des sites web. Les paramètres

importants à vérifier sont la disponibilité du site, le temps de réponse et la vitesse d'accès.

Response code for step "elearning.univ" of scenario "Website".	2021-05-24 11:20:08	200
Response code for step "Google" of scenario "Website".	2021-05-24 11:20:04	200

Figure IV.70 *:* Code de réponse pour les sites Web.

La figure (IV.70) nous montre le code de réponse. Le code de réponse 200 confirme l'état Ok du site.

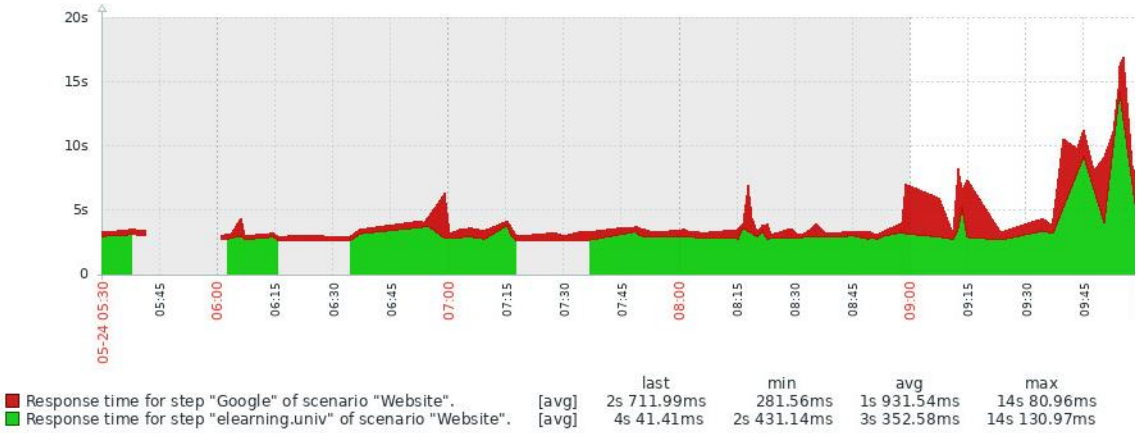


Figure IV.71: Temps de réponse des sites Web.

La figure (IV.71) représente le temps de réponse du serveur par seconde.

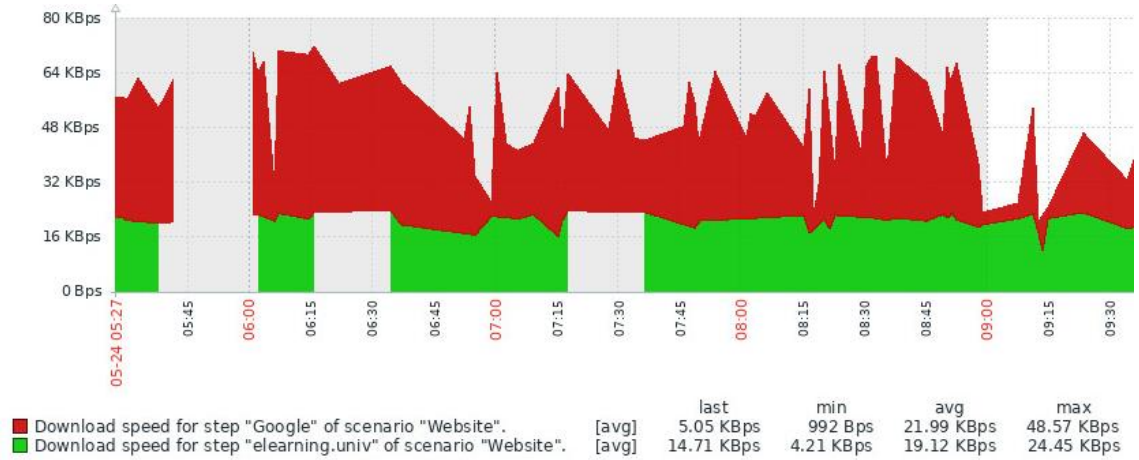


Figure IV.72**:** Vitesse de téléchargement des sites Web.

La figure (IV.72) nous montre la vitesse d'accès aux sites web.

IV.13.4 Résultat de Serveur Zabbix

On peut également superviser notre serveur principal Zabbix.

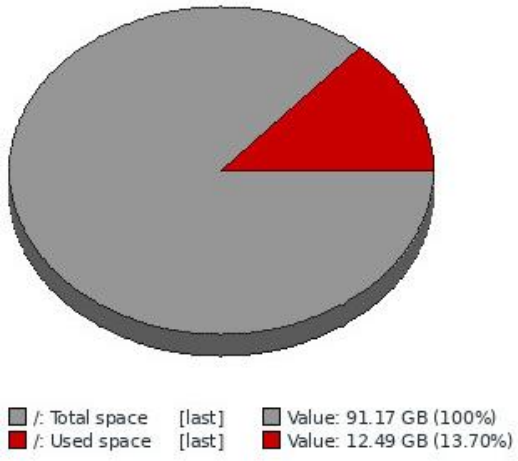


Figure IV.73 *:* utilisation de l'espace disque.

La figure (IV.73) montre l'espace disque total et la quantité d'espace utilisé.

Figure IV.74*:* Graphe des performances d'utilisation du serveur.

La figure (IV.74) montre une présentation graphique de la performance du

serveur, les graphes incluent l'utilisation du CPU, l'utilisation de la mémoire, l'utilisation du disque et la charge du système.

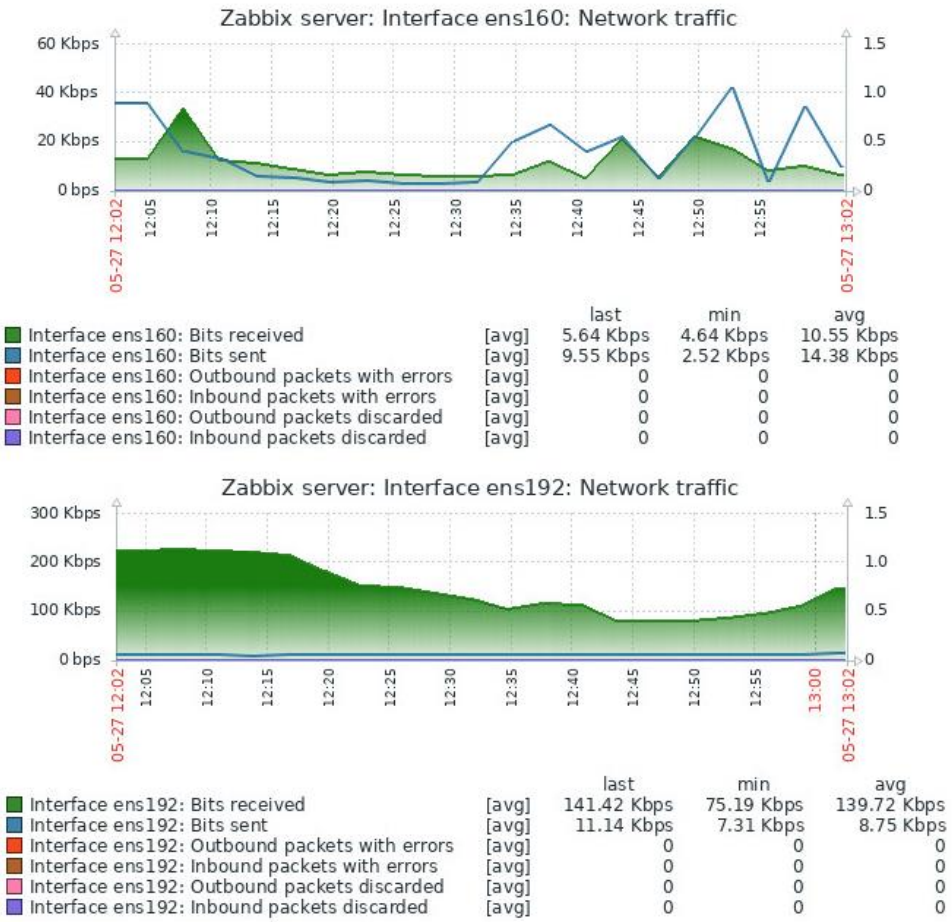


Figure IV.75: Trafic réseau.

La figure (IV.75) montre les bits reçus et les bits envoyés de deux interfaces différentes.

IV.13.5 Résultat de surveillance de la base de données MySQL

La surveillance de la base de données MySQL du serveur Zabbix peut nous informer des valeurs des éléments à tout moment, comme l'utilisation du pool de mémoire tampon, l'utilisation du disque de cache, le nombre des connexions interrompues…etc.

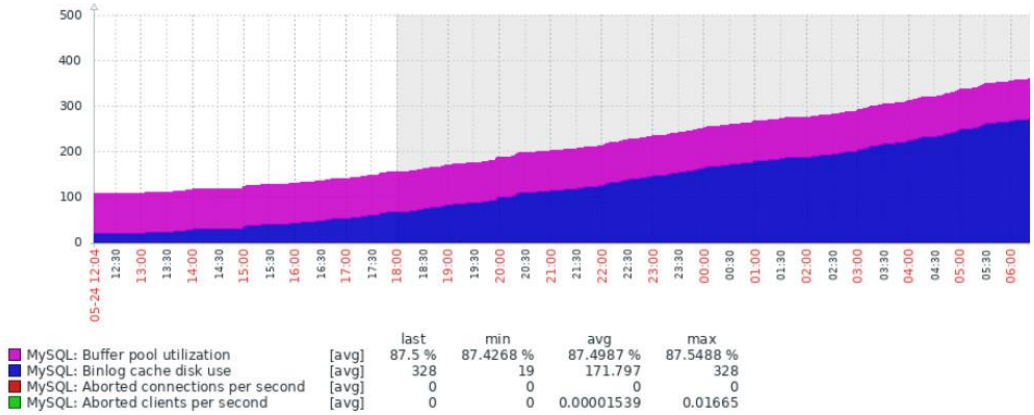


Figure IV.76 *:* Surveillance des performances MySQL.

Ainsi que d'autres éléments comme les commandes, on peut avoir un suivi par seconde des commandes supprimées, insérées, sélectées et même un suivi des mises à jour de ces commandes.

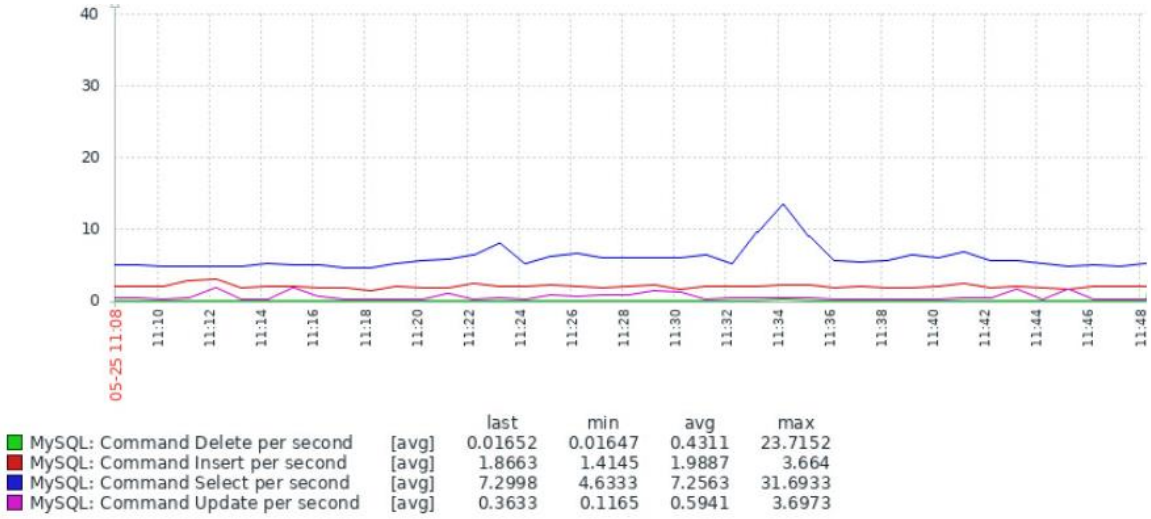


Figure IV.77 *:* Surveillance des commandes de MySQL.

De même, des informations sur la taille de la base de données sont aussi remontées parmi : la taille de la base de données Zabbix, du système et de MySQL.

Figure IV.78 : Etat de la taille de MySQL.

Tous les bits envoyés et reçus dans la base de données peuvent aussi être surveillés comme le montre la figure suivante.

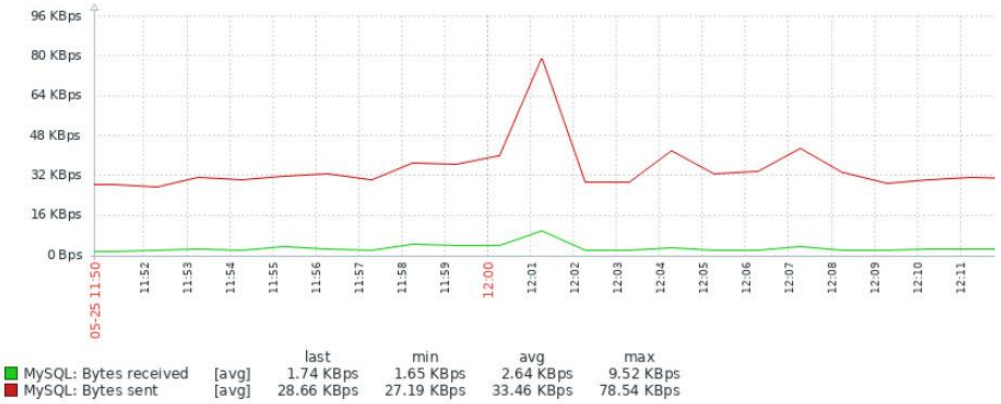


Figure IV.79 : Trafic des bites.

En utilisant les fonctionnalités de la surveillance sur Zabbix, il est possible de suivre plusieurs éléments avec plusieurs graphes sur un seul écran.

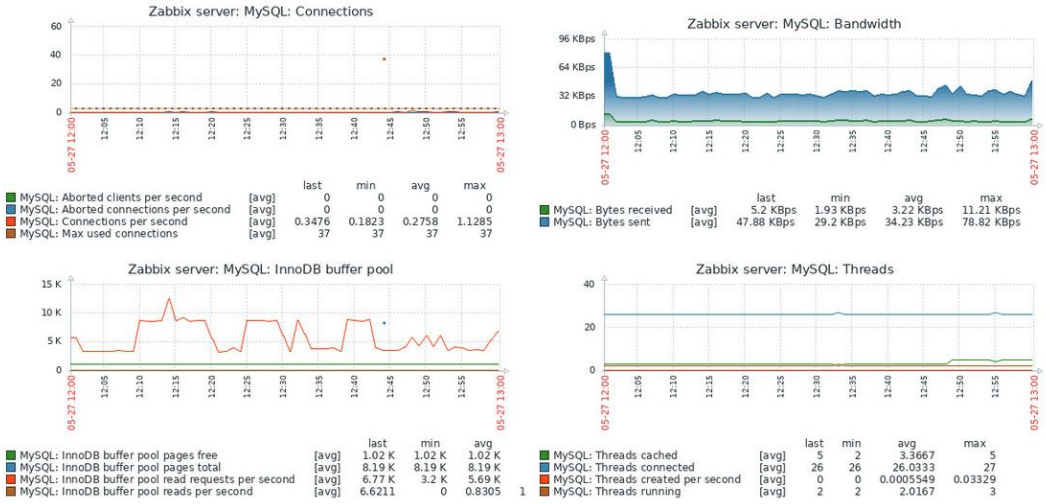


Figure IV.80 : Surveillance MySQL.

IV.14 Les alertes

Tous les problèmes et déclencheurs d'événements qui surviennent aux hôtes se présentent avec différents types d'alertes. Les alertes s'affichent avec des périodes de temps, et avec différentes couleurs, chaque couleur représente un état différent.

Figure IV.81: Différents type d'alerte.

La figure suivante (IV.82) montre une liste de déclencheurs d'événements pour différentes interfaces de commutateurs. Si certains événements ne sont pas verts ou bleus, un problème peut survenir très bientôt.

Figure IV.82*: Liste de déclencheurs d'événements.*

Les problèmes des hôtes sont affichés pendant une période précise, ces problèmes concernent l'utilisation du processeur, les interfaces, l'utilisation du disque et de la mémoire, les problèmes MySQL, etc. Ils montrent les différents changements d'état.

Figure IV.83: Alertes des problèmes.

Il y a aussi un autre type d'alerte qui se produit lorsqu'un problème est résolu.

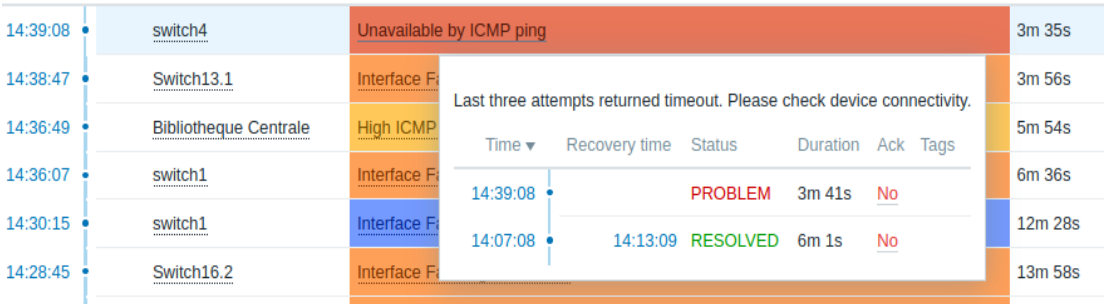


Figure IV.84: *Alertes des problèmes résolus.*

La figure (IV.84) montre un autre problème survenu à un commutateur après qu'il ait été résolu.

Si nous voulons vérifier une application spécifique comme le CPU, la mémoire, les systèmes de fichiers, la surveillance du Web, MySQL, les services, etc., nous utilisons le filtre, il suffit de la sélectionner dans la section Problèmes et d'appliquer la fonction.

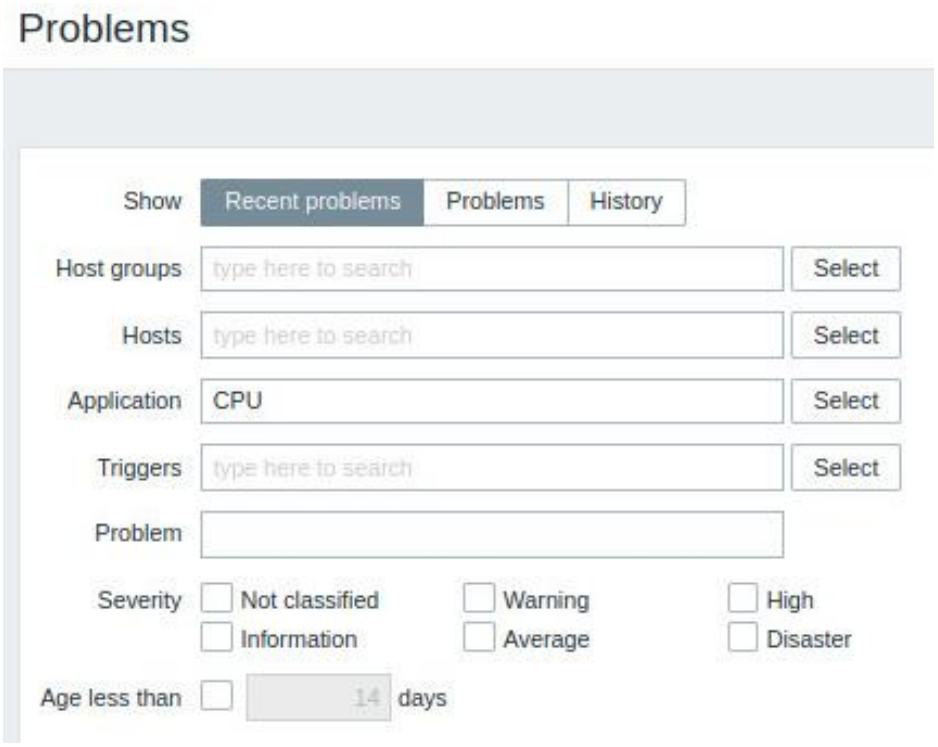


***Figure IV.85**:* Utilisation du filtre.

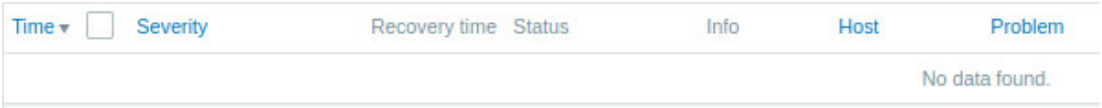


Figure IV.86: Supervision des problèmes.

S'il affiche "Aucune donnée trouvée", cela signifie qu'il n'y a aucun problème avec cette application.

IV.15 Les notifications

Après une alerte, on reçoit un message de notification par Telegram, indiquant le type d'alerte, le nom de la machine et l'état de l'hôte ainsi que l'heure.

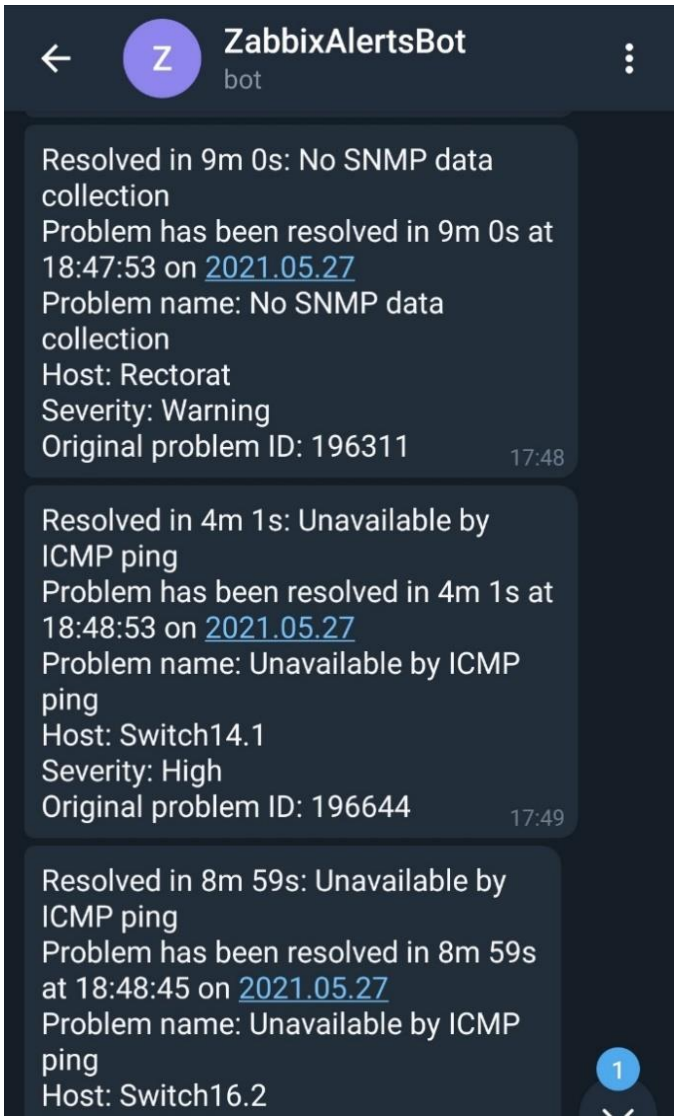


Figure IV.87: Recevoir un message d'alerte.

IV.16 Les rapports

On accède au menu des rapports, on trouve une interface avec plusieurs profils des rapports de tous les hôtes surveillés par Zabbix.

Prenant par exemple le commutateur de la bibliothèque centrale, son profil de rapport inclut le taux d'utilisation du processeur, l'utilisation de la mémoire, l'état du ventilateur du châssis et l'état de la température. La figure suivante illustre un échantillon de ce profil.

Host	Name
Bibliotheque Centrale	#1: High CPU utilization (over 90% for 5m)
Bibliotheque Centrale	Bibliotheque Centrale has been restarted (uptime < 10m)
Bibliotheque Centrale	chassis: Fan is in critical state
Bibliotheque Centrale	chassis: Fan is in warning state
Bibliotheque Centrale	chassis: Temperature is above critical threshold: >60
Bibliotheque Centrale	chassis: Temperature is above warning threshold: >50
Bibliotheque Centrale	chassis: Temperature is too low: <5

Figure IV.88 *:* Rapports du switch bibliothèque centrale.

En supplément, des rapports sur l'état de chaque interface sont remontés dont l'état de l'interface, le trafic entrant et sortant, les erreurs d'interfaces…etc.

Bibliotheque Centrale	Interface Fa0/3(): High bandwidth usage (> 90%)
Bibliotheque Centrale	Interface Fa0/3(): High error rate (> 2 for 5m)
Bibliotheque Centrale	Interface Fa0/3(): Link down
Bibliotheque Centrale	Interface Fa0/4(): Ethernet has changed to lower speed than it was before
Bibliotheque Centrale	Interface Fa0/4(): High bandwidth usage (> 90%)
Bibliotheque Centrale	Interface Fa0/4(): High error rate (> 2 for 5m)

Figure IV.89 : Rapports des interfaces du switch.

On prend un autre exemple de la base de données du serveur Zabbix MySQL, les rapports de cette dernière nous offre une vue d'ensemble complète de la base de données MySQL. Zabbix est conçu pour offrir la visibilité sur toutes les activités et ressources pouvant avoir un impact sur les performances MySQL. Les activités des services, les modifications ou n'importe quel changement, les temps d'attente, les instructions SQL et autres facteurs pertinents pour mieux diagnostiquer les ralentissements des bases de données.

Zabbix server	MySQL: Number of on-disk temporary tables created per second is high (over 10 for 5m)
Zabbix server	MySQL: Number of temporary files created per second is high (over 10 for 5m)
Zabbix server	MySQL: Refused connections (max_connections limit reached)
Zabbix server	MySQL: Server has aborted connections (over 3 for 5m)
Zabbix server	MySQL: Server has slow queries (over 3 for 5m)
Zabbix server	MySQL: Service has been restarted (uptime < 10m)
Zabbix server	MySQL: Service is down

Figure IV.90 : Rapports de MySQL.

IV.16.1 La représentation graphique des rapports

La représentation graphique des rapports sert à afficher une évaluation de l'intégrité globale du système pour obtenir un contexte clair des données de rapport qui nous permet à la fin de mieux diagnostiquer les problèmes.

Les colonnes graphiques dans la figure suivante nous montrent la disponibilité du protocole ICMP qui veut dire la possibilité de faire un ping au commutateur.

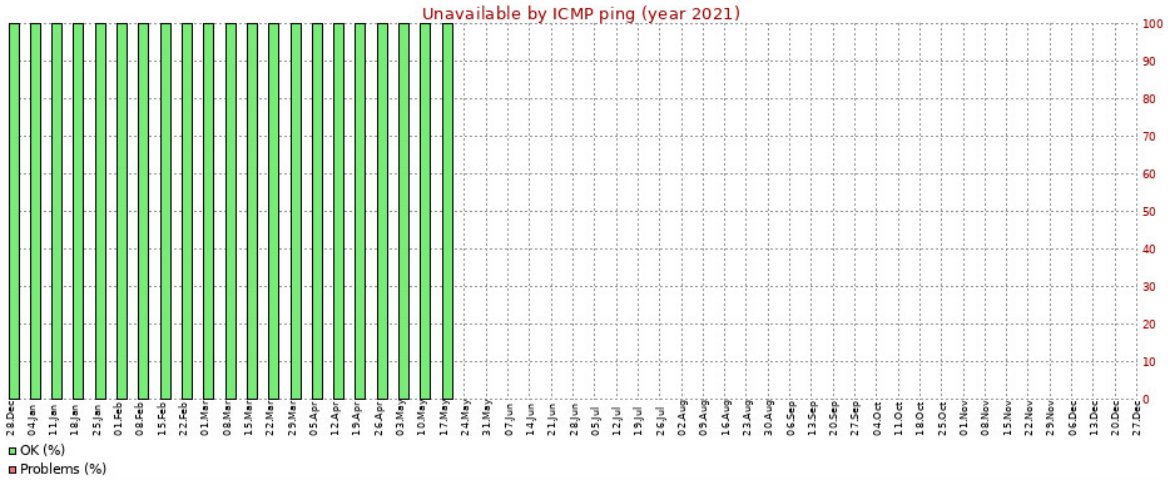


Figure IV.91 *:* Rapport de disponibilité du protocole ICMP.

Si un problème se présente comme le cas dans la figure ci-dessous, une couleur rouge s'apparait en signalant qu'un problème dans le protocole SNMP l'empêche de collecter les données du commutateur.

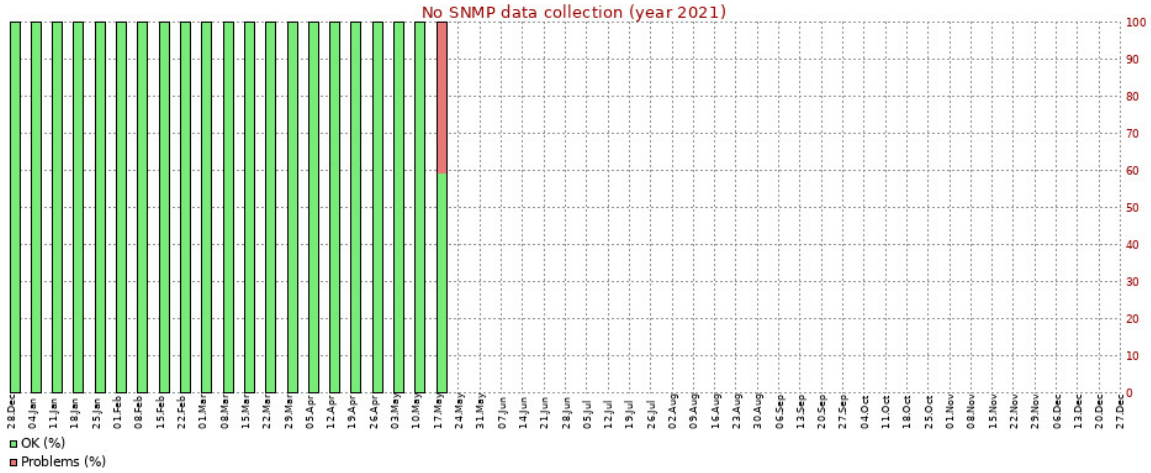


Figure IV.92 : Rapport de collecte des données du protocole SNMP.

En outre, un souci se présente au niveau de l'agent Zabbix est aussi remonté et signalé dans le rapport.

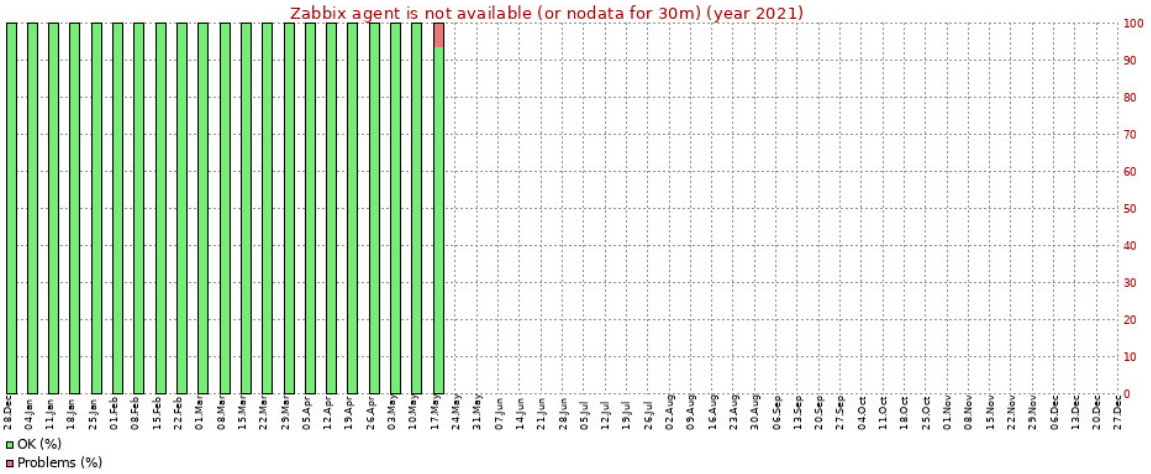


Figure IV.93 *:* Rapport de disponibilité de l'agent Zabbix.

Time	Action	Type	Recipient	Message
2021-05-27 10:34:10	Report problems to Zabbix administrators	Telegram	Admin (Zabbix Administrator) *1160624582*	**Subject:** Resolved in 2m 6s: No SNMP data collection **Message:** Problem has been resolved in 2m 6s at 11:34:07 on 2021.05.27 Problem name: No SNMP data collection Host: Switch18.1 Severity: Warning Original problem ID: 184523
2021-05-27 10:33:14	Report problems to Zabbix administrators	Telegram	Admin (Zabbix Administrator) *1160624582*	**Subject:** Resolved in 5m 1s: Unavailable by ICMP ping **Message:** Problem has been resolved in 5m 1s at 11:33:09 on 2021.05.27 Problem name: Unavailable by ICMP ping Host: switch4 Severity: High Original problem ID: 184485

Figure IV.94 : Journaux d'évènements.

La figure (IV.94) montre un journal d'action pour tous les rapports qui ont été envoyés à l'administrateur lorsqu'une alerte se produit, le journal d'action mentionne

l'heure et le type de média qui ont été utilisés pour notifier l'administrateur et le message envoyé.

IV.17 Conclusion

L'installation de la solution n'est pas très compliquée, et ne prend pas beaucoup de temps, mais la supervision des agents, des équipements et des applications demande trop de configuration et de temps.

Dans ce chapitre nous avons testé Zabbix sur deux serveurs avec l'agent Zabbix et les commutateurs par le protocole SNMP et à la fin nous avons présenté notre solution par des captures d'écran qui résument l'installation, la configuration et les résultats.

Zabbix est une solution complète qui offre diverses fonctionnalités allant de la collecte des données et la création des rapports à l'envoie des notifications d'alertes aux administrateurs.

Les réseaux sont devenus un véritable pilier de la vie économique universelle, ce qui rend les logiciels de supervision essentiels, ils permettent d'augmenter la qualité de service des systèmes d'information, et d'avoir un aperçu général du fonctionnement des systèmes informatique ainsi, d'avoir des statistiques sur l'état du système informatique ce qui permet d'éviter beaucoup de situations indésirables.

Les grandes entreprises qui disposent d'un grand nombre d'équipements tels que les routeurs, les commutateurs et les serveurs, ont besoin d'un bon logiciel de supervision, pour que l'administrateur puisse surveiller et maintenir le bon fonctionnement de son infrastructure réseau.

Ce projet de fin d'étude était sous forme d'une étude sur la supervision informatique en utilisant le logiciel Zabbix sur quelques équipements informatique de l'université de Saad DAHLEB à Blida. Zabbix permet à l'administrateur de gérer ces différents équipements à l'aide des protocoles SNMP, IPMI et JMX.

L'étude de Zabbix sur certains équipements (commutateurs, serveurs Linux, serveurs Windows) du réseau informatique de l'université nous a permis d'avoir un suivi en temps réel pour surveiller leur état de performance comme l'utilisation du CPU et de la mémoire, le trafic réseau, La surveillance de MySQL. Cependant, la limitation en temps et en matériel nous a empêchés de tester toutes les fonctionnalités de Zabbix.

A la fin, nous pouvons dire que la mise en œuvre de cette solution n'est pas assez complexe, ce qui nous a également permis d'avoir une vue sur le point de fonctionnement de ce logiciel et de connaître ses possibilités. Zabbix est un outil qui surveille l'état de chaque équipement à tout moment, offre des alertes et des rapports sur chaque panne.

Cette solution de surveillance nous donne de nombreuses possibilités pour approfondir l'étude de ces fonctionnalités tel que :

- La supervision des bases de données : ORACLE, PostgreSQL,
- La supervision des services : HTTP, FTP, LDAP, DNS, POP, IMAP. etc.
- La supervision des imprimantes.

- La supervision des Machines virtuelles : Oracle VM, VirtualBox, VMware.
- Supervision par le protocole IPMI.

Ce projet nous a permis d'acquérir de l'expérience dans l'administration sous Linux et surtout la découverte du domaine de supervision.

Bibliographie

[1] KAHLAOUI H. Etude et Développement d'une Application de supervision du réseau de l'UBCI,. MEMOIRE DE STAGE DE FIN D'ETUDES , Mastere professionnel en Nouvelles Technologies des Telecommunication et Réseaux. 2015.

[2] Revue Zabbix. [Internet]. Available from: https://www.webservertalk.com/network-monitoring-software/zabbix.

[3] Infrastructure Mi. Sig-Strasburg. [Internet]. 2018 [cited 2021 Avril]. Available from: https://sig-strasbourg.net/2018/12/13/quest-ce-quune-infrastructure-informatique/.

[4] Dordoigne J. Réseaux Informatique, Notions Fondamentales et Administration sous Windows ou Linux. France Août 2018.

[5] IONOS. [Internet]. Available from: https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/.

[6] NSIMBA ON. Implantation d?un système voip sécurisé par une technologie VPN dans une entreprise à multiple centre d?exploitation.. 2015.

[7] Philippe ATELIN JD. Réseaux informatiques Notions fondamentales. France: Editions ENI; Mars 2006.

[8] FS Communauté. [Internet]. 15 août 2018 Available from: https://community.fs.com/fr/blog/gigabit-switch-sfp-port-vs-rj45-port-vs-gbic-port.html.

[9] Cisco.goffinet. [Internet]. Available from: https://cisco.goffinet.org/ccna/.

[10] CLOUDFLARE. [Internet]. Available from: https://www.cloudflare.com/fr-fr/learning/ddos/glossary/internet-control-message-protocol-icmp/.

[11] IONOS. [Internet]. 02.07.2019 Available from: https://www.ionos.fr/digitalguide/serveur/outils/telnet/.

[12] Syloe. [Internet]. Available from: https://www.syloe.com/glossaire/serveur-informatique/.

[13] JDN LR. Serveur informatique. [Internet]. 2019 [cited 2021 Apr]. Available from: https ://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203337-serveur-informatique-definition-traduction/.

[14] GECITS-EU. [Internet]. Available from: : https://www.gecits-eu.com/quels-sont-les-differents-types-de-serveurs/.

[15] [Internet]. Available from: https://www.gecits-eu.com/quels-sont-les-differents-types-de-serveurs/.

[16] DELL. Configuration matérille du serveur. [Internet]. Available from: https://www.dell.com/fr-fr.

[17] WayTo LearnX. [Internet]. Available from: https://waytolearnx.com/2019/07/a-quoi-sert-un-service-web.html?fbclid=IwAR1ihXXMz6QcsSuPJQAU3JvjRjHJYF7OWEBzFs1YoV-GH6JOs9BtSl7AVcg.

[18] Petit B. Infrastructure des réseaux Informatique. Paris 2018.

[19] WHatIs MyIPAddress. [Internet]. Available from: https://whatismyipaddress.com/mailserver?fbclid=IwAR35ENn5hcrvH3k5a1ANZ5

MLISEVb3ZGJdefXsxvKIfrDc7F_vypeuv1ZLA.

[20] Oracle. [Internet]. Available from: https://www.oracle.com/fr/database/systeme-gestion-base-de-donnees-sgbd-definition.html.

[21] Quelles doivent etre les principales caractéristiques de votre ordinateur? [Internet]. 2013 [cited 2021]. Available from: https://www.lebelage.ca/mes-loisirs/techno.

[22] TUKANDILE CM. Modélisation et implantation d'un logiciel de gestion des ressources humaines.Cas de l'électricité du cango "EDC/Tshikapa". Institut supérieur de commerce Tshikapa RDC; 2011.

[23] Apprendre Informatique. [Internet]. Available from: https://www.apprendreinformatique.fr/windows-linux-ou-macos-quel-systeme-dexploitation-choisir/.

[24] Sullivan K. INFOSEC. [Internet]. January 30, 2018 Available from: https://resources.infosecinstitute.com/topic/11-points-consider-virtualizing-security/#gref.

[25] Berger L. La virtualisation des système d'information, Mémoire. Haut Ecole de Gestion de Genève (HEG); 28 septembre 2012.

[26] Bady B. Mise en place d'un système de virtualisation des serveurs dans un réseau informatique avec vsphere server (cas de Sri/uni lu).. Ecole Supérieure d'Informatique Salama ESIS - Ingénieur Technicien en Administration Système et Réseau Informatique; 2013.

[27] Antoine Benkemoun RH. AC-Etude de la virtualisation et du fonctionnement de la solution libre Xen. 2008.

[28] Les machines virtuelles. [Internet]. Available from: https://www.ionos.fr/digitalguide/serveur/know-how/machine-virtuelle/.

[29] VU DUONG T. Découverte de chroniques à partir de journaux d'alarme :Application à la supervision de réseau de télécommunications. Toulouse: Thèse de doctorat INPT; 2001.

[30] [Internet]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-4:ed-1:v1:fr.

[31] Pignet F. Réseaux Informatique, Supervision et Administration. 2007.

[32] whatis. [Internet]. 2018 Available from: https://whatis.techtarget.com/fr/definition/SLA.

[33] DUBREUCQ PY. Etude et mise en oeuvre d'une solution opensource de supervision systèmes et réseaux. Conservatoire national des arts et métiers centre régional de Lile: Mémoire en vue d'obtenir le diplome d'ingénieure CNAM; 16 Mars 2012.

[34] Jan O. Supervision. [Internet]. 2014 [cited 2021]. Available from: https://wooster.checkmy.ws/2014/05/monitoring-interne-externe-actif-passif/#:~:text=Monitoring%20externe%20actif%20pour%20v%C3%A9rifier,type%20%C2%AB%20Real%20User%20Monitoring%20%C2%BB.

[35] Duparo Jonathan-Minh CG. Administration du routeur Cisco 1841 via SNMP. Université François-RabeLais ; 2010/2011.

[36] Selectel (Infrastructure informatique pour les entreprises). [Internet]. 2019

Available from: https://habr.com/ru/company/selectel/blog/439834/?fbclid=IwAR0XKMBjDW0_jXZO0ZhMI0gGfsgC2ZHvfIGCVcwXB9Yt3Fl0KYSWK8R_b-s.

[37] Cacti [Internet]. Available from: https://www.cacti.net/.

[38] Checkmk. [Internet]. Available from: https://checkmk.com/.

[39] ZanOSS. [Internet]. Available from: https://www.zenoss.com/.

[40] Nagios. [Internet]. Available from: https://www.nagios.com/.

[41] Centreon. [Internet]. Available from: https://www.centreon.com/.

[42] shinken enterprise. [Internet]. Available from: https://www.shinken-enterprise.com/fr/accueil/.

[43] D.produit, guides d'installation, livres blancs, OpManager.

[44] Zabbix Support. [Internet]. Available from: https://support.zabbix.com/projects/ZBXNEXT?selectedItem=com.atlassian.jira.jira-projects-plugin:report-page.

[45] Documentation Zabbix 5.0. [Internet]. 2021-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/introduction/about.

[46] Rihards Olups. Zabbix Network Monitoring Second Edition. August 2016.

[47] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/visualization/dashboard.

[48] Rihards Olups ADVPU. Entreprise Network Monitoring Made Easy, Learn howa to gather detailed statistics and data with this one-stop. January 2017.

[49] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/it_services.

[50] Zabbix. [Internet]. 2001 - 2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/hosts.

[51] zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/definitions.

[52] Andrea Dalle Vache SKL. Zabbix Network Monitoring Essentials , Your one-stop solution to efficient network monitoring with zabbix. February 2015.

[53] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/items.

[54] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/concepts/agent.

[55] Zabbix. [Internet]. 2001-2021 Available from:. https://www.zabbix.com/documentation/5.0/manual/config/triggers.

[56] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/definitions.

[57] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/notifications/action.

[58] SME Server. [Internet]. Available from: https://wiki.koozali.org/Zabbix/fr.

[59] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from:

https://www.zabbix.com/documentation/5.0/manual/config/visualization/maps/map.

[60] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/discovery/network_discovery.

[61] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/discovery/auto_registration.

[62] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/quickstart/notification.

[63] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/notifications/media.

[64] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/4.0/manual/web_monitoring.

[65] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/vm_monitoring.

[66] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/distributed_monitoring.

[67] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/distributed_monitoring/proxies.

[68] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/database_monitoring.

[69] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/api.

[70] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/web_interface/frontend_sections/reports/action_log.

[71] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/web_interface/frontend_sections/reports/notifications.

[72] Documentation Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/1.8/fr/manual/installation/requirements.

[73] zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/event_correlation.

[74] [Internet].

[75] Zabbix. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/config/items/itemtypes/log_items.

[76] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/discovery/low_level_discovery.

Bibliographie

[77] Documentation Zabbix 5.0. [Internet]. 2001-2021 Available from: https://www.zabbix.com/documentation/5.0/manual/encryption.

[78] [Internet]. Available from: https://www.reddit.com/r/Network/comments/gidqfb/it_infrastructure_template/.

[79] IONOS. [Internet]. 06.09.2019 Available from: https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/.

[80] GECITS-EU. [Internet]. Available from: https://www.gecits-eu.com/quels-sont-les-differents-types-de-serveurs/.