République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire

EN VUE DE L'OBTENTION DU DIPLOME DE MASTER PROFESSIONNEL.
Option : Administration et sécurité des réseaux.

Thème

Etude mise en œuvre d'une solution de supervision réseaux basée sur Zabbix au profit de Cevital

Réalisé par :

Mlle ALLOU Lydia Imene

Encadré par :

Mr OUZEGGANE Redouane

Mr BOUKIRAT Massinissa

Les membres du jury :

Président : Dr AISSANI Sofiane

Examinatrice : Dr MAMMERI Souheila

Année universitaire 2022/2023

Remerciements

Je tiens à remercier :

Mes parents pour leur soutien et leurs efforts quotidiens.

Mon promoteur Mr OUZEGUANNE Redouane pour l'aide qu'il m'a apporté.

Mon encadreur au sein de CEVITAL Mr BOUKIRAT Massinissa pour son encouragement, son aide et orientation durant la période du projet et aussi tout le personnel du Département Informatique pour leur sympathie.

Enfin, ma profonde gratitude et mon respect à toute personne ayant contribué de près ou de loin à l'élaboration de ce travail.

Et avant tout et tous je rends Grâce à DIEU pour m'avoir donné la force d'aller jusqu'au bout de ce travail.

Dédicace

Je dédie ce travail :

A mes chers parents, ma famille, mes enseignants, et à tous ceux à qui je dois reconnaissance.

Table des matières

Table des figures

Liste des abréviations

ACL	Access Control List
AD DS	Active Directory et Domain Services
ARPANET	Advanced Research Projects Agency NETwork
BDD	Base De Donnée
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMAP	Distributed Management Application Processus
DNS	Domain Name System
DSI	Direction des Systèmes d'Information
GNS3	Graphical Network Simulator-3
GNU	General Public Licence
HSE	Hygiène, Sécurité et Environnement
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
IR	Infra Rouge
ISO	Organisation internationale de normalisation
JMX	Java Management Extensions
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitain Area Network
MIB	Management Information Base
MSA	Managed System and Agents
NMS	Network Management Station
OID	Object IDentifier
OS	Operating System
OSI	Open System Interconnexion
P2P	Peer to Peer
PAN	Personale Area Network
PHP	Hypertext Preprocessor
RAM	Random Access Memory
RMON	Remote Network Monitoring
RRD	Round-Robin Database
SIA	Signs Partnership Agreement
STP	Spanning Tree Protocol
SMFA	Specific Management Function Area
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language Server
SSH	Secure Shell
SSMTP	Secure Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Technologies d'Information et de Communication

ToR Top of Rack
UDP User Datagram Protocol
USB Universal Serial Bus
USM User-based Security Model
VLAN Virtual Local Area Network
VTP Vlan Trunking Protocol
WIFI WIreless FIdelity
WMI Windows Management Instrumentation
WAN Wide Area Network

Introduction générale

De nos jours, les systèmes d'information et les réseaux jouent un rôle essentiel dans les opérations des entreprises, en particulier dans des domaines critiques. Certaines entreprises ont des réseaux qui s'étendent sur de longues distances et sont au cœur de leur activité commerciale, ce qui rend leur contrôle crucial. En effet, à mesure que les données sont stockées sur des ordinateurs et que leur volume augmente, le nombre d'utilisateurs, qu'ils soient connus ou inconnus, ayant potentiellement de mauvaises intentions sur les réseaux, augmente également. Ces individus peuvent chercher à accéder à des informations sensibles afin de les lire, les modifier ou même les détruire, ce qui compromettrait le fonctionnement normal du système et le rendrait vulnérable. Par conséquent, il est impératif de garantir la sécurité et de surveiller en permanence l'état du réseau afin d'assurer sa disponibilité, sa fiabilité et son efficacité.

En raison de la forte demande des utilisateurs de ces réseaux, il est nécessaire de vérifier leur état en temps réel en mettant en place des équipements de surveillance qui nous alertent en cas de problème. Grâce à un tel système, les administrateurs réseau et système peuvent réduire le nombre d'interventions nécessaires, ce qui permet de résoudre rapidement les anomalies.

L'objectif de ce projet est de mettre en place un outil de supervision basé sur le logiciel Zabbix, que nous allons configurer sur une machine virtuelle utilisant le système d'exploitation Linux (Debian).

Afin d'atteindre les objectifs visés, nous avons divisé ce travail en quatre parties :

• La première partie aborde des concepts et généralités sur les réseaux.

• La deuxième partie portera sur la description du concept de supervision et la comparaison entre les différents outils de monitoring existantes.

• La troisième partie sera consacrée à la présentation de l'organisme d'accueil Cevital et sa structure organisationnelle, ceci afin de tirer une problématique à traiter dans le cadre de notre projet et énumérer les différentes solutions.

• Dans la dernière partie concerne la modélisation et l'implémentation de la solution de su-

pervision retenue.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce mémoire.

Chapitre 1

Généralité sur les réseaux informatique

Introduction

Grâce au développement et aux progrès dans le domaine des TIC (Technologies d'Information et de Communication), le monde est plus connecté que jamais. Ce progrès touche les aspects logiciels et applicatifs ainsi que l'aspect matériel et réseaux (informatiques et réseaux de télécommunication).

Dans ce chapitre, et avant d'entamer le noyau de notre travail, nous allons présenter des généralités sur les réseaux informatiques, en définissant quelques concepts de base liés à ce domaine, notamment le modèle OSI et TCP/IP ainsi que leurs piles protocolaires associées.

1.1 Définition d'un réseau informatique

Les réseaux et l'informatique sont étroitement liés. L'informatique concerne l'étude et l'utilisation des ordinateurs et des systèmes informatiques pour le traitement de l'information. Les réseaux quant à eux, sont des structures qui permettent à plusieurs appareils informatiques de se connecter et de communiquer entre eux.

Un réseau est un ensemble d'éléments interconnectés qui communiquent entre eux pour échanger des informations et des ressources. Les réseaux peuvent être de différentes natures tels que les réseaux informatiques, les réseaux de télécommunication, les réseaux électriques etc.

Les réseaux informatiques sont les plus courants, et sont utilisés pour connecter des ordinateurs, des périphériques et des serveurs afin de partager des données et des ressources. Ils permettent aux utilisateurs de collaborer et de communiquer, et utilisent généralement des protocoles de communication pour permettre l'échange d'information entre les dispositifs connectés.

1.2 les différents types de réseaux

Les réseaux informatiques peuvent être classés selon plusieurs critères, et dans notre cas, nous avons choisi de présenter uniquement une classification basée sur la distance entre les stations. Ainsi, les réseaux peuvent être classés dans quatre types de réseau :

1.2.1 les réseaux personnels (PAN (Personale Area Network))

Désigne des réseaux conçus pour une utilisation personnelle ; les plus courants sont l'USB, les technologies sans fil telles que Bluetooth ou IR (infra rouge) ou le wifi [1].

1.2.2 Les réseaux locaux (LAN(Local Area Network))

Lorsque deux stations sont séparées de quelques kilomètres, le réseau sera dit local. Généralement, le réseau local est la propriété du même organisme. C'est le type de réseau que l'on rencontre le plus souvent dans les organismes.
Etant donné la proximité des stations, le taux de transmission des données est relativement élevé. On peut utiliser les trois types de support de transmission : la paire torsadée, le câble coaxial ou la fibre optique ; en général, la paire torsadée est la plus fréquemment utilisée [1].

1.2.3 Les réseaux métropolitains (MAN(Metropolitain Area Network))

Le réseau métropolitain se situe à mi-chemin entre le réseau local et le réseau étendu. Il couvre habituellement les stations d'une même ville. Le support de transmission utilisé est le câble coaxial ou la fibre optique. [1].

1.2.4 Les réseaux étendus (WAN)

Lorsque la distance entre deux stations situées dans des lieux différents atteint quelques centaines de kilomètres, le réseau est dit étendu. Les compagnies disposant de plusieurs sites éloignés géographiquement, tels que ceux gérant les systèmes de réservation de places

d'avion et les systèmes bancaires, utilisent ce genre de réseau. Les vitesses de transmission d'un réseau étendu sont généralement moins grandes que celles d'un réseau local [1].

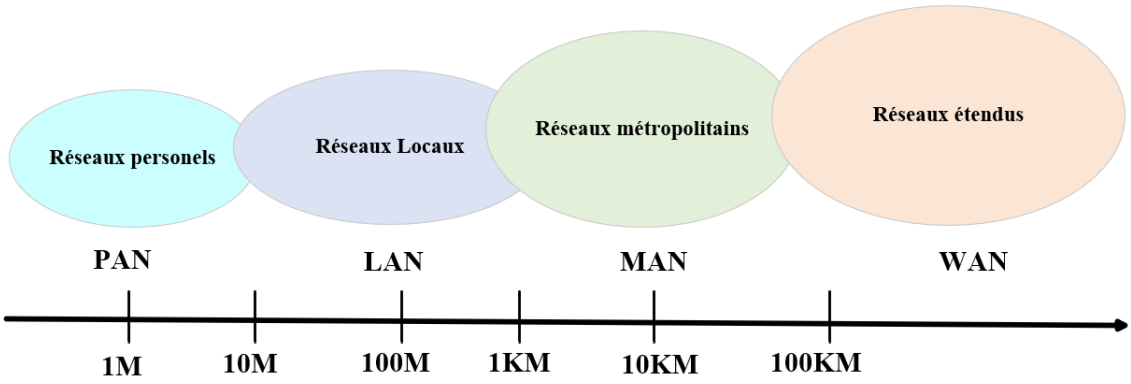


FIGURE 1.1 – Différents types de réseaux selon l'étendu.

1.3 Architecture des réseaux

L'architecture du réseau est le cadre complet du réseau informatique d'un organisme. Le schéma de l'architecture du réseau fournit une image complète du réseau établi avec une vue détaillée de toutes les ressources accessibles. Il comprend les composants matériels utilisés pour la communication, le câblage et les types d'appareils, la disposition et les topologies du réseau, les connexions physiques et sans fil ainsi que les zones mises en œuvre et les plans futurs.

On retrouve deux types d'architectures :

1.3.1 Les réseaux client-serveur

Dans le modèle client/serveur, le périphérique qui envoie une requête d'informations est nommé client et celui qui répond à la requête est nommé serveur. Le client est une combinaison matériel/logiciel que les utilisateurs exploitent pour accéder directement aux ressources stockées sur le serveur.

Les processus clients et serveurs sont considérés dans la couche application. Le client commence l'échange en requérant des données auprès du serveur, qui répond en envoyant un

ou plusieurs flux de données au client. Les protocoles de communication standards tels que TCP/IP décrivent le format des requêtes et des réponses entre clients et serveurs.
la figure 1.2 illustre comment les fichiers sont téléchargés du serveur vers le client. [2]

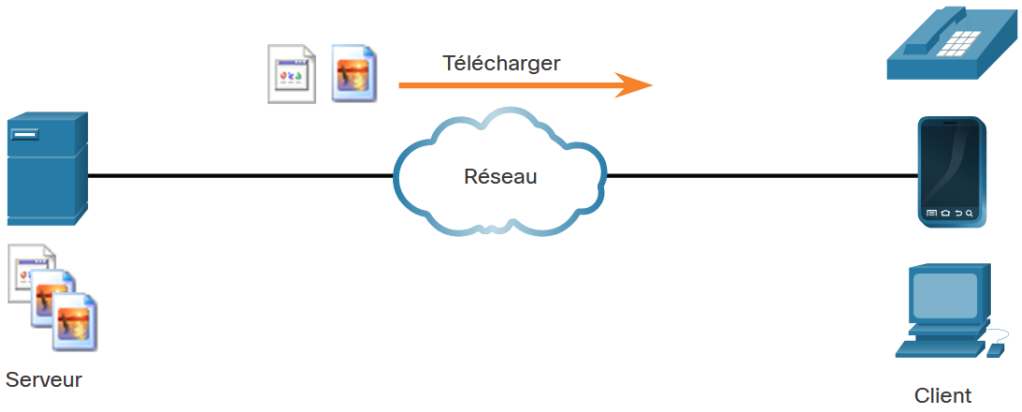


FIGURE 1.2 – Architecture client/serveur.

[2]

1.3.2 Les réseaux Post à post (Peer to Peer= P2P)

Dans le modèle de réseau peer-to-peer (P2P), les données sont accessibles à partir d'un périphérique homologue (Peer) sans l'intervention d'un serveur dédié.
Dans un réseau Peer to Peer, deux ordinateurs ou plus sont connectés via un réseau et peuvent partager des ressources (par exemple, des imprimantes et des fichiers) sans disposer de serveur dédié. Chaque périphérique final connecté (ou homologue) peut opérer à la fois en tant que serveur et client. Un ordinateur peut jouer le rôle de serveur pour une transaction et servir simultanément de client pour une autre. Les rôles de client et de serveur sont définis en fonction de chaque requête.
Outre le partage de fichiers, un réseau comme celui-ci peut autoriser par exemple le partage de connexion internet. [3]
La figure 1.3 illustre un échange Peer to Peer, les deux périphériques sont considérés comme étant égaux dans le processus de communication. Peer 1 possède des fichiers partagés avec Peer 2 et peut accéder à l'imprimante partagée qui est directement connectée à Peer 2 pour

imprimer des fichiers. Peer 2 partage l'imprimante qui est directement connectée avec Peer 1 tout en accédant aux fichiers partagés sur Peer 1.

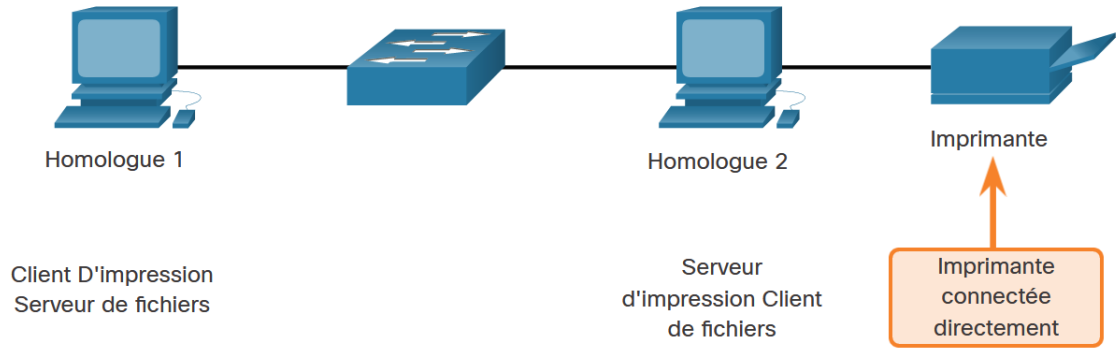


FIGURE 1.3 – Architecture Peer to Peer.

[3]

1.4 Topologie des réseaux

Elle représente une certaine disposition des différents postes informatiques du réseau et une hiérarchie de ces postes.

Il existe plusieurs topologies de réseaux informatiques dont voici les principales :

1.4.1 Topologie en bus

Un réseau en bus est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs. Les réseaux de bus permettent de relier simplement de multiples matériels.

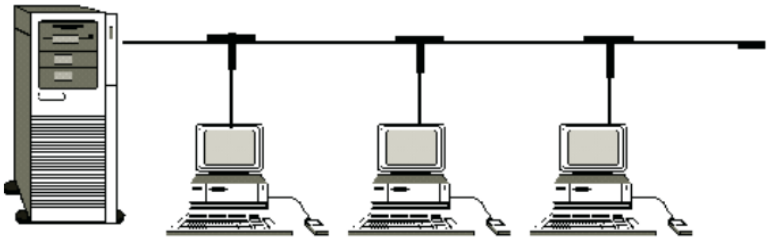


FIGURE 1.4 – Topologie en Bus.

[4]

1.4.2 Topologie en anneau

Dans cette topologie, les périphériques sont connectés en forme d'anneau. Les données sont envoyées à travers l'anneau dans une seule direction, chaque périphérique reçoit les données et les renvoie au périphérique suivant jusqu'à ce que les données atteignent leur destination. Si un périphérique est défaillant, cela peut perturber tout le réseau.

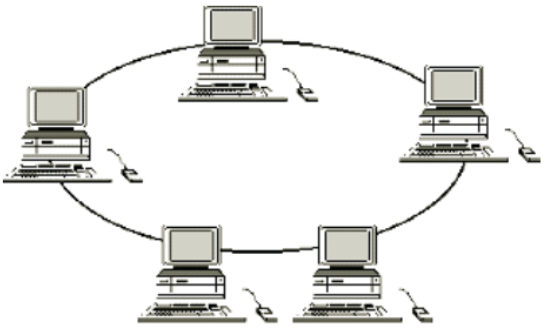


FIGURE 1.5 – Topologie en Anneau.

[4]

1.4.3 Topologie en étoile

Dans cette topologie, tous les périphériques sont connectés à un hub central. Les données sont envoyées à travers le hub, qui les transmet aux périphériques correspondants. Cette topologie est facile à étendre et permet d'isoler les problèmes dans un périphérique sans affecter le reste du réseau.

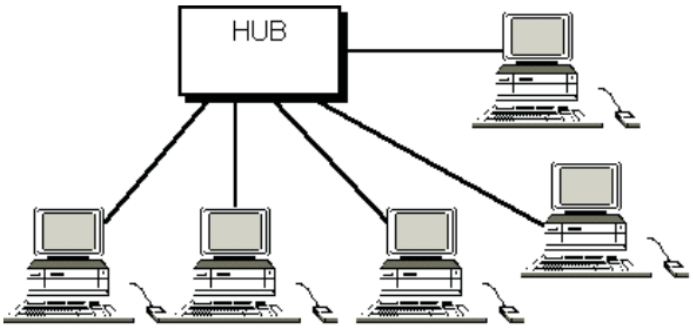


FIGURE 1.6 – Topologie en étoile.

[4]

1.4.4 Topologies en maille

C'est une topologie de type étoile mais avec différents chemins pour accéder d'un nœud à un autre. C'est la méthode utilisée sur Internet : pour un transfert entre deux points, chaque nœud va sélectionner en temps réel la route la plus rapide pour le transfert. Le principal avantage de ce type de topologie est qu'il s'adapte à toute éventualité, par exemple une ligne coupée ne perturbe pas les communications d'où son utilisation dans les réseaux sensibles.

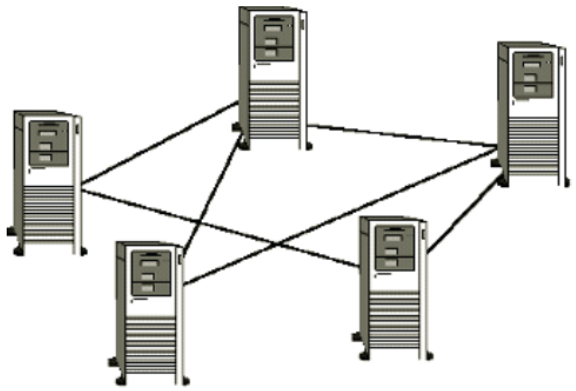


FIGURE 1.7 – Topologie maille.

[4]

1.5 Les alternatives de raccordements des réseaux

1.5.1 Les équipements d'interconnections

— **concentrateur (HUB)**

Il permet de concentrer le trafic réseau provenant de plusieurs hôtes, il agit au niveau de la couche physique du modèle OSI. [5]

— **Commutateur (switch)**

C'est un pont multiport c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau de la couche 2 du modèle OSI.[5]

— **Routeur**

C'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter. [5]

FIGURE 1.8 – Les équipements d'interconnexion.

[5]

1.5.2 les supports de transmission

Nous retrouvons plusieurs supports de transmission dont les plus utilisés sont :

— **Câbles en cuivre**

• **Paires torsadées :** Utilisées pour les connexions Ethernet, téléphoniques et certaines connexions audio.

• **Câbles coaxiaux :** Utilisés dans les réseaux câblés (par exemple, les connexions de télévision par câble) et certaines applications réseau.

• **Câbles à fibres optiques :** Utilisés pour les connexions à haut débit, à longue distance et à faible atténuation, tels que les réseaux de télécommunications et les connexions Internet à haut débit.

— **Fibre optique**

• **Câbles à fibres optiques :** Transmettent les signaux sous forme de lumière à travers des fils de verre ou de plastique. Ils offrent une large bande passante et une grande immunité aux interférences électromagnétiques, ce qui en fait un choix populaire pour les connexions à haut débit à longue distance.

— **Ondes radio**

• **Transmission sans fil :** Utilisée pour les réseaux sans fil, tels que le Wi-Fi, les réseaux cellulaires (3G, 4G, 5G) et les communications par satellite.

— **Transmission infrarouge**

• Utilisée pour la communication sans fil à courte portée, par exemple, dans les télécommandes.

— **Transmission par satellite**

• Utilisée pour les communications à longue distance, notamment pour les transmissions de données, de voix et de vidéo entre différents points du globe.

1.6 Le modèle OSI et TCP/IP

1.6.1 Le modèle OSI

Le modèle de référence OSI contient la liste complète des fonctions et services susceptibles d'intervenir dans chaque couche. Ce type de modèle assure la cohérence de tous les types de protocoles et de services de réseau en décrivant ce qui doit être fait à une couche particulière, mais sans prescrire la manière dont cela doit être accompli.
Il décrit également l'interaction de chaque couche avec les couches directement supérieures et inférieures. Les protocoles TCP/IP cités dans ce cours s'articulent autour des modèles OSI et TCP/IP. Le tableau présente des détails sur chaque couche du modèle OSI. [6]

Couche du modèle OSI	Description
7 - Application	La couche application contient les protocoles utilisés pour les processus de communications.
6 - Présentation	La couche de présentation permet une représentation commune des données transférées entre les services de couche d'application.
5 - Session	La couche de session fournit des services à la couche de présentation pour organiser son dialogue et gérer l'échange de données.
4 - Transport	La couche transport définit les services à segmenter, à transférer et à réassembler les données pour les communications individuelles entre les terminaux.
3 - Réseau	La couche réseau fournit des services permettant d'échanger les différents éléments de données individuels sur le réseau entre des dispositifs terminaux identifiés.
2 – Liaison de données	Les protocoles de la couche liaison de données décrivent les méthodes d'échange de trames de données entre les appareils sur un support commun
1 - Physique	Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et procéduraux pour activer, maintenir et désactiver des connexions physiques pour la transmission d'un bit vers et depuis un réseau.

FIGURE 1.9 – Les différentes couches du modèle OSI.

[6]

1.6.2 Le modèle TCP/IP

Le modèle de protocole TCP/IP pour les communications sur l'internet a été créé au début des années 1970 et est parfois appelé le modèle internet. Ce type de modèle correspond étroitement à la structure d'une suite de protocoles particulière. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche de protocoles au sein de la suite TCP/IP. Il est également utilisé comme modèle de référence. Le tableau présente des détails sur chaque couche du modèle OSI. [7]

Couche du modèle TCP/IP	**Description**
4 - Application	Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.
3 - Transport	Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
2 - Internet	Détermine le meilleur chemin à travers le réseau.
1 - Accès réseau	Contrôle les périphériques matériels et les supports qui constituent le réseau.

FIGURE 1.10 – Les différentes couches du modèle TCP/IP.

[7]

1.6.3 Comparaison des modèles OSI et TCP/IP

Les principales similitudes se trouvent dans les couches de transport et de réseau ; cependant, les deux modèles diffèrent dans la manière dont ils se rapportent aux couches situées au-dessus et au-dessous de chaque couche :

	Le modèle OSI	**Le modèle TCP/IP**
Nombre de couches :	Il est composé de sept couches distinctes (physique, liaison de données, réseau, transport, session, présentation et application)	Il est considéré comme ayant quatre couches principales (interface réseau, internet, transport et application).
Développement et adoption :	Il a été développé par l'ISO (Organisation internationale de normalisation)	Il a été développé par le Département de la Défense des États-Unis pour le réseau ARPANET (Advanced Research Projects Agency NETwork), qui est devenu l'Internet que nous connaissons aujourd'hui
Niveau d'abstraction :	Il est considéré comme plus abstrait et conceptuel, axé sur la normalisation et la description des fonctions de communication à un niveau théorique.	Il est considéré comme plus pratique et orienté vers la mise en œuvre des protocoles de communication spécifiques utilisés dans les réseaux, en particulier dans le contexte d'Internet.
Utilisation dans la pratique :	Il est utilisé comme outil de référence pour comprendre les concepts généraux des réseaux, l'interopérabilité et les interactions entre les différentes couches.	Il est utilisé comme cadre de travail pratique pour la conception, la mise en œuvre et le dépannage des réseaux basés sur les protocoles TCP/IP, notamment pour les applications Internet et les réseaux d'entreprise.

FIGURE 1.11 – Comparaison des modèles OSI et TCP/IP.

— **La couche 3 du modèle OSI**

Correspondant à la couche réseau, est directement liée à la couche Internet TCP/IP. Cette couche sert à décrire les protocoles qui adressent et acheminent les messages via un réseau interne. [7]

— **La couche 4 du modèle OSI**

Correspondant à la couche transport, est directement liée à la couche transport TCP/IP. Cette couche décrit les services et les fonctions généraux qui assurent une livraison ordonnée et fiable des données entre les hôtes source et destination. [7]

— **La couche application du modèle TCP/IP**

Elle inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final. Les couches 5, 6 et 7 du modèle OSI servent de références aux développeurs et aux éditeurs de logiciels d'application pour créer des applications qui fonctionnent sur les réseaux.

Les modèles TCP/IP et OSI sont couramment utilisés lors de la référence aux protocoles de différentes couches. Le modèle OSI, qui sépare la couche liaison de données de la couche physique, est généralement utilisé pour faire référence aux couches inférieures. [7]

1.7 Les protocoles

Les protocoles sont des ensembles de règles et de conventions définissant la manière dont les données sont échangées et les communications sont établies entre différents dispositifs dans un réseau. Voici quelques-uns des protocoles qui figurent dans les couches du modèle TCP/IP :

— **HyperText Transfer Protocol (HTTP)**

Le protocole HTTP est utilisé pour la communication entre les clients et les serveurs sur le World Wide Web. Il permet le transfert de ressources hypertexte telles que les pages web, les images, les vidéos, etc. [8]

— **Transmission Control Protocol (TCP)**

Gère les conversations individuelles. Il est aussi responsable de la garantie de la livraison fiable des informations et de la gestion du contrôle du flux entre les appareils finaux. [8]

— **Protocole Internet (IP)**

Ce protocole est responsable de la remise des messages de l'expéditeur au destinataire. Il est utilisé par les routeurs pour transférer les messages sur plusieurs réseaux. [8]

— **Ethernet**

Ce protocole est responsable de la remise des messages d'une carte réseau à une autre sur le même réseau local Ethernet. [8]

Les protocoles de la figure 1.12 sont décrits comme suit :

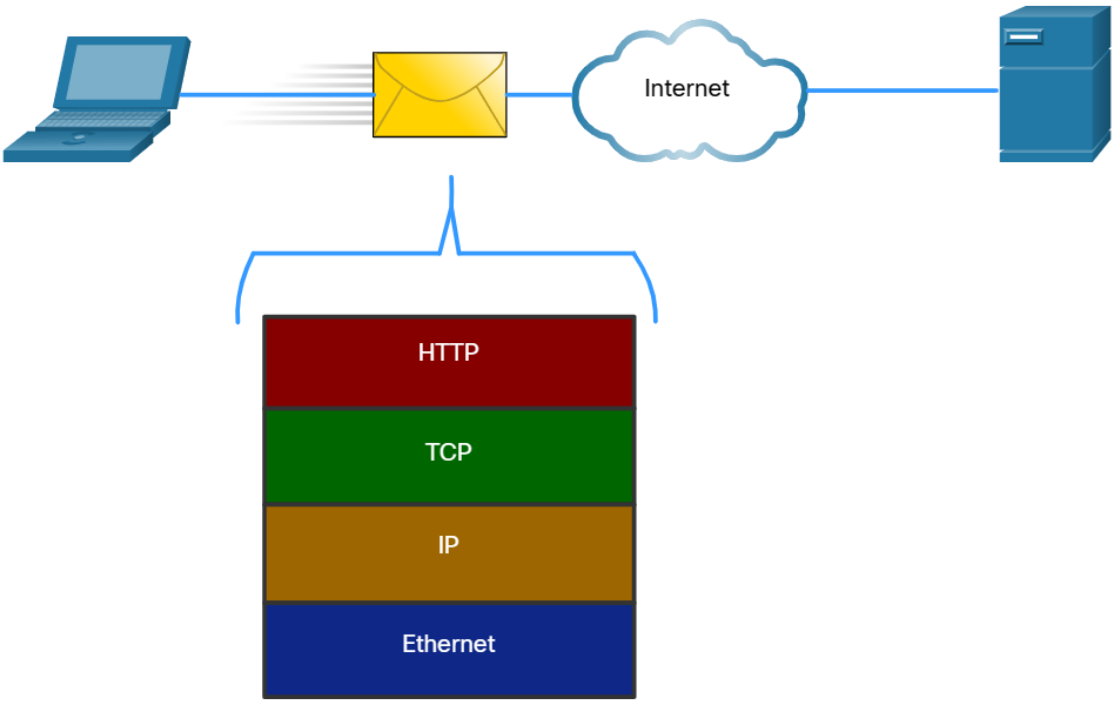


FIGURE 1.12 – Protocoles.

[8]

Conclusion

Au fil de ce chapitre, nous avons défini les réseaux, leurs différents types, leur architecture, leur topologie ainsi que les alternatives de raccordement des réseaux. Sont également présentés les modèles OSI et TCP/IP et leurs différents protocoles qui sont des notions de base afin de comprendre le fonctionnement de tous les composants du réseau.

Dans le chapitre suivant, nous allons détailler la supervision des réseaux et l'état des lieux des outils de supervision.

Chapitre 2

La supervision des réseaux et L'état des lieux de ses outils

Introduction

Un réseau ne peut pas être géré par le seul effort humain. La complexité d'un tel système impose l'utilisation d'outils de gestion de réseau automatisés, ce que nous appelons « moniteur de supervision des réseaux informatiques ». Un tel moniteur peut avoir une vue globale du fonctionnement du réseau ainsi que du niveau des performances des systèmes.
Dans ce chapitre, divisé en deux parties, nous allons présenter le concept de la supervision et ses objectifs. Par la suite, nous nous pencherons sur la présentation de quelques outils de supervision et leurs fonctionnalités.

2.1 La supervision des réseaux

2.1.1 Le concept de la supervision réseau

Le concept est né au début des années 1980, lorsque l'implantation des réseaux informatiques dans les entreprises a explosé. Ces échelles croissantes et leur hétérogénéité posent de réels problèmes de gestion et d'administration, augmentant ainsi le besoin d'administrateurs experts. C'est donc à cette époque que les premières réflexions sur un nouveau concept ont émergé. La supervision doit pouvoir s'adapter à des environnements hétérogènes, piloter automatiquement le réseau et générer un ensemble de statistiques pour mieux comprendre le réseau afin de prévenir et de remédier aux différents problèmes pouvant surgir. Ainsi, la surveillance peut être définie comme l'utilisation de ressources réseau appropriées (matériel ou logiciel) pour obtenir des informations sur l'état du réseau et son utilisation. Ces informations peuvent ensuite être utilisées comme outil de gestion optimale des dépannages et de la qualité du réseau (problèmes de surcharge). Ils peuvent également anticiper les développements futurs nécessaires. [9]

2.1.2 La norme ISO (Organisation internationale de normalisation) du point de vue de la gestion des réseaux

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

1. Un modèle organisationnel ou architectural (MSA, Managed System and Agents) qui organise la gestion OSI (Open System Interconnexion) et définit la notion de systèmes gérés et gérants (DMAP, Distributed Management Application Processus). [10]
2. Le modèle informationnel (MIB, Management Information Base) qui constitue la base de données des informations de gestion. La MIB énumère les objets gérés et les informations s'y rapportant (attributs). [10]
3. Le modèle fonctionnel (SMFA, Specific Management Function Area) qui répartit les fonctions d'administration en cinq domaines (aires) fonctionnels ». [10]

   — **Gestion des performances :** Il est nécessaire qu'elle soit capable d'évaluer les performances des ressources du système ainsi que leur efficacité. Pour ce faire, elle inclut des procédures de collecte de données et de statistiques, qui conduisent à la création de tableaux de bord. Les informations recueillies doivent également permettre de planifier les évolutions du réseau. Les performances du réseau sont évaluées en fonction de quatre paramètres : le temps de réponse, le débit, le taux d'erreur par bit et la disponibilité. [11]

   — **Gestion des configurations :** La gestion de la configuration implique de maintenir un inventaire précis des ressources matérielles (telles que le type et l'équipement) et logicielles (y compris la version, les licences et les fonctions) tout en indiquant leur localisation géographique. Pour chaque objet géré dans l'inventaire, la gestion de la configuration lui attribue un nom qui l'identifie de manière unique. [11]

— **Gestion de la comptabilité :** La fonction principale consiste à surveiller les charges des objets gérés ainsi que leurs coûts de communication. Il est possible d'établir des quotas d'utilisation temporaires ou permanents sur chaque ressource réseau. De plus, la gestion de la comptabilité permet la mise en place de systèmes de facturation basés sur l'utilisation pour chaque utilisateur. [11]

— **Gestion de la sécurité :** La gestion de la sécurité englobe toutes les tâches liées à l'administration des réseaux et nécessaires pour soutenir les politiques de sécurité dans un réseau de télécommunication. Les principales fonctions de la gestion de sécurité incluent la distribution des informations sécuritaires telles que les clés de chiffrement et les droits d'accès, ainsi que la génération de rapports sur les événements liés à la sécurité tels que les intrusions dans un réseau, les tentatives d'accès non autorisées à des informations ou à des services privilégiés, et l'accès à des données et à des services protégés. [11]

— **Gestion des pannes :** Cette fonction revêt une grande importance, car l'objectif principal de l'administration des réseaux est d'optimiser les ressources et les moyens. Il est donc essentiel d'être en mesure de prévoir et de diagnostiquer rapidement toute défaillance du système, qu'elle soit causée par des facteurs externes (par exemple, une coupure de connexion publique) ou internes au système (par exemple, une défaillance d'un routeur). [11]

La figure 2.1 represente les cinq aires fonctionnels en question ;

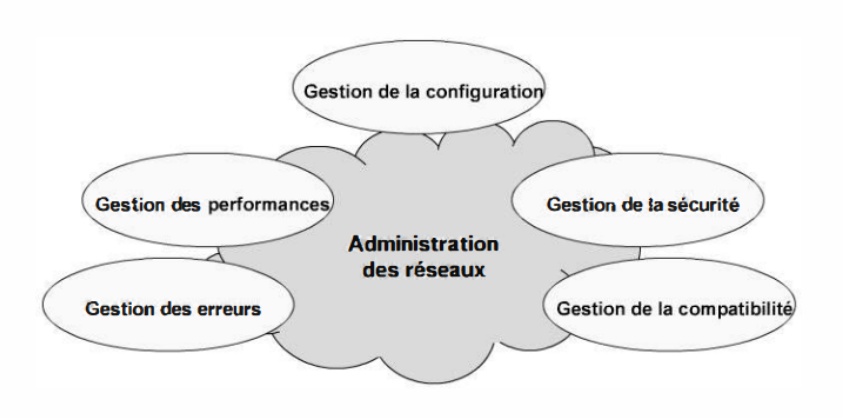


FIGURE 2.1 – Aires fonctionnelles de la gestion ISO.

[10]

2.1.3 Types de supervision

La figure 2.2 résume les principaux rôles de toute plateforme de supervision dont nous allons presenter les differents types.

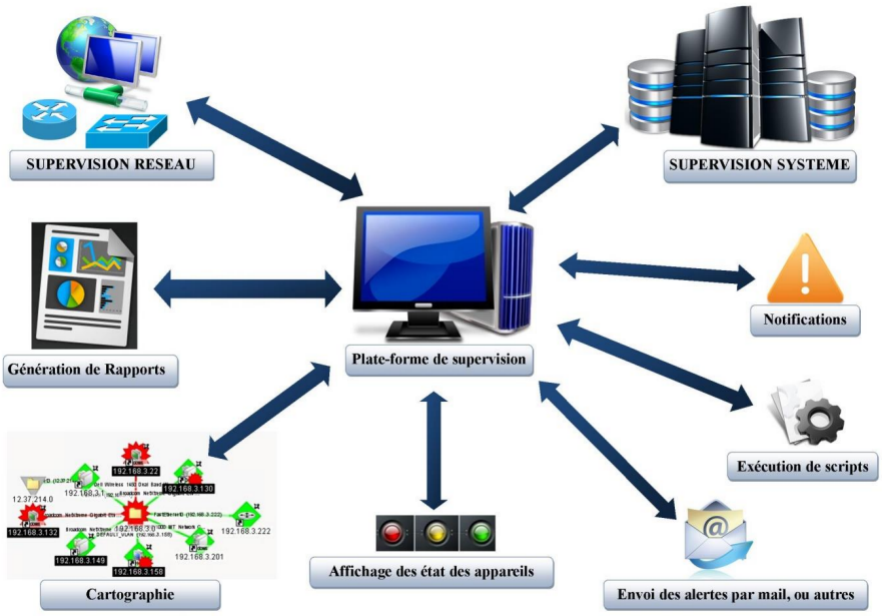


FIGURE 2.2 – les principaux rôles de la supervision.

[12]

En ce qui concerne les types de supervision, nous en distinguons trois, à savoir La supervision système, la supervision réseau et la supervision applicative.

1. **La supervision du Système :** Porte principalement sur les trois types de ressources système : Le processeur, la mémoire et le stockage. [12]
2. **La supervison du Réseau :** Porte à son tour sur la supervision de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité, mais également du contrôle des flux. [12]
3. **La supervision applicative :** (ou supervision des applications), elle, permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs. [12]

2.1.4 Les méthodes de supervision

Il en existe deux et sont utilisées avec plusieurs variantes :

a) **Supervision passive :**

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

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

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

Le protocole standardisé et privilégié pour la supervision passive est SNMP avec le mécanisme de trappes. [13]

La figure 2.3 illustre la méthode passive de supervision.

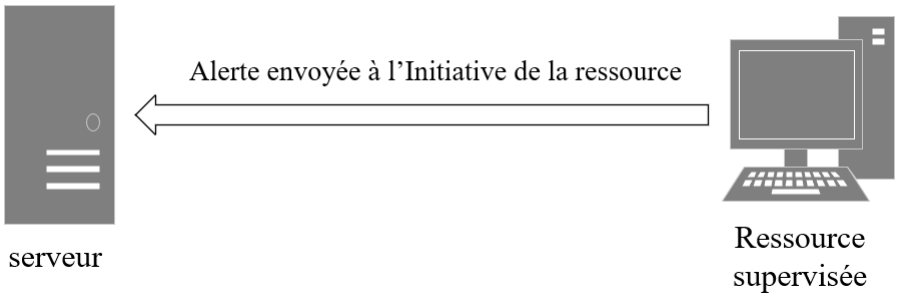


FIGURE 2.3 – Echange de message entre le serveur de supervision et la ressource supervisée.

b) **Supervision active :**

La supervision active est la plus classique et la plus utilisée. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse. Cette méthode est composée de trois étapes :

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

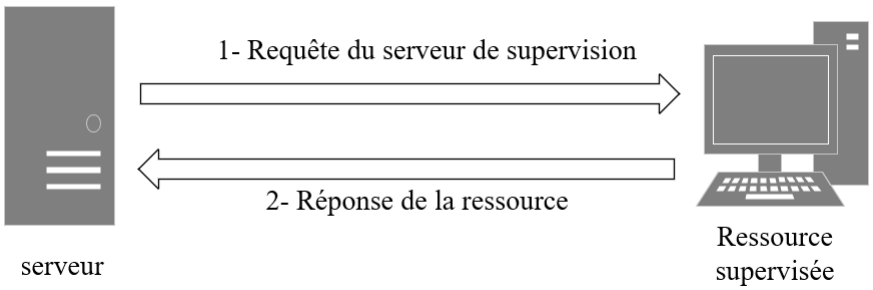


FIGURE 2.4 – Echange de message entre le serveur de supervision et la ressource supervisée.

Les protocoles de supervision active les plus couramment utilisés sont SNMP (Simple Network Management Protocol) et WMI (Microsoft Windows Management Instrumentation). Ces protocoles sont recommandés car ils sont non intrusifs : les agents nécessaires sont intégrés aux systèmes supervisés. En plus de cela, certains protocoles d'administration peuvent

également être utilisés pour la supervision, tels que IPMI (Intelligent Platform Management Interface) et JMX (Java Management Extensions). Les protocoles SSH (Secure Socket Shell) et Telnet sont également largement utilisés dans la supervision des systèmes.. [13]

2.1.5 Les protocoles de supervision

Les protocoles de supervision sont des méthodes standardisées utilisées pour collecter des données de surveillance sur un système ou une application. Ils permettent de surveiller l'état et la performance d'un système ou d'une application, d'identifier les problèmes potentiels et de les résoudre. Voici quelques exemples de protocoles de supervision :

• Simple Network Management Protocol (SNMP)

Il s'agit d'un protocole de gestion de réseau qui permet de collecter des informations sur les périphériques réseau, tels que les routeurs, les commutateurs, les serveurs, etc. SNMP permet de surveiller l'utilisation de la bande passante, l'état des interfaces, la charge du processeur, la mémoire, etc.

• Internet Control Message Protocol (ICMP)

Il s'agit d'un protocole de contrôle de la couche réseau qui permet de vérifier la connectivité entre deux périphériques réseau. ICMP permet de vérifier si un périphérique est accessible, de mesurer le temps de réponse et de détecter les pertes de paquets.

• Transmission Control Protocol (TCP)

Il s'agit d'un protocole de la couche transport qui permet de surveiller les connexions entre les applications. TCP permet de mesurer la latence, la bande passante et les erreurs de transmission.

• User Datagram Protocol (UDP)

Il s'agit également d'un protocole de la couche transport qui permet de surveiller la perfor-

mance des applications. UDP permet de mesurer la latence, la bande passante et les pertes de paquets.

• Hypertext Transfer Protocol (HTTP)

Il s'agit d'un protocole de la couche application utilisé pour les communications Web. HTTP permet de surveiller la performance des sites Web, y compris le temps de réponse, la disponibilité, la charge du serveur, etc.

Vu les références que nous avons consulté, nous avons remarqué que le protocole SNMP est parmi les protocoles les plus utilisés dans la supervision, pour cela, nous allons consacrer une section pour le détailler.

2.1.6 Le protocole SNMP

2.1.6.1 Introduction

SNMP est un protocole TCP/IP utilisé sur les réseaux Internet pour la gestion des équipements réseau. Il exploite UDP pour les communications avec des adresses sources et destinations dans chaque trame, un checksum pour la détection d'erreurs, et une communication non connectée entre la station d'administration et l'agent. Les ports 161 et 162 sont utilisés respectivement pour les requêtes et les alarmes dans le cadre du SNMP. [14]

2.1.6.2 Principe de fonctionnement

Le protocole SNMP se base sur le fait qu'il existe une station de gestion réseau. Le rôle du manageur est de contrôler le réseau et de communiquer via ce protocole avec un agent ; ce dernier est, de manière générale, une interface SNMP embarquée sur le matériel destiné à être administré à distance.
La figure 2.5 illustre le principe de fonctionnement du protocole SNMP. [15]

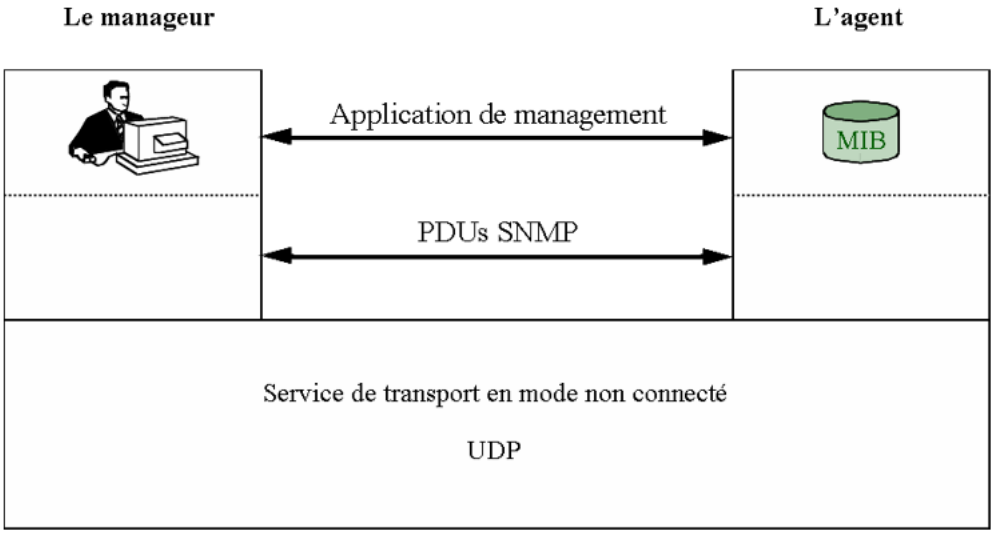


FIGURE 2.5 – Principe de fonctionnement SNMP.

[14]

Ce protocole est composé de plusieurs commandes :

— **La commande Get :** Permet au gestionnaire (manageur) d'envoyer une requête à l'agent SNMP pour demander une information spécifique. L'agent renvoie alors la valeur correspondante à cette information. [14]

— **La commande Getnext :** Est utilisée par le gestionnaire pour demander à l'agent l'information qui vient après dans une liste de variables. Elle est généralement utilisée après une requête Get pour obtenir directement le contenu de la variable qui suit. [14]

— **La commande Getbulk :** Est utilisée par le gestionnaire pour obtenir les valeurs de plusieurs variables en une seule requête, améliorant ainsi les performances en évitant des

requêtes séparées. Cette commande est introduite dans SNMPv2. [14]

— **La commande Set :** Permet au gestionnaire de modifier la valeur d'une variable sur l'agent administré. Cela permet d'effectuer des modifications sur le matériel géré. [14]

— **La commande Trap :** Est utilisée par l'agent pour envoyer une notification à la station d'administration lorsque survient un événement particulier, tel qu'une connexion ou une modification de la valeur d'une variable. Cela permet à l'administrateur réseau d'être informé en temps réel de l'événement. [14]

— **La commande Inform :** Permet à l'agent d'envoyer une Trap et d'attendre une réponse du gestionnaire pour confirmer la réception et l'analyse de la Trap. Cela permet à l'agent d'obtenir une confirmation que la Trap a été traitée avec succès. Cette commande est introduite dans SNMPv2. [14]

2.1.6.3 Principaux éléments de SNMP

— **Manager ou (station de gestion)**

« Le Manager NMS (Network Management Station) ou « station de gestion de réseau », constitue le point central de l'architecture SNMP. Il se présente souvent sous la forme d'un poste et de logiciels d'administration, fournissant à l'administrateur une vue d'ensemble des équipements, facilitant ainsi les tâches d'administration. Les logiciels d'administration de réseaux utilisent les informations rassemblées par le NMS dans sa MIB et interrogent les MIBs gérées par les agents. Le NMS met en œuvre le protocole SNMP, encapsule ou désencapsule les messages échangés, génère les commandes émises par l'administrateur et traite les alertes en provenance des agents ». [15]

La figure 2.6 illustre le fonctionnement d'une station de gestion ;

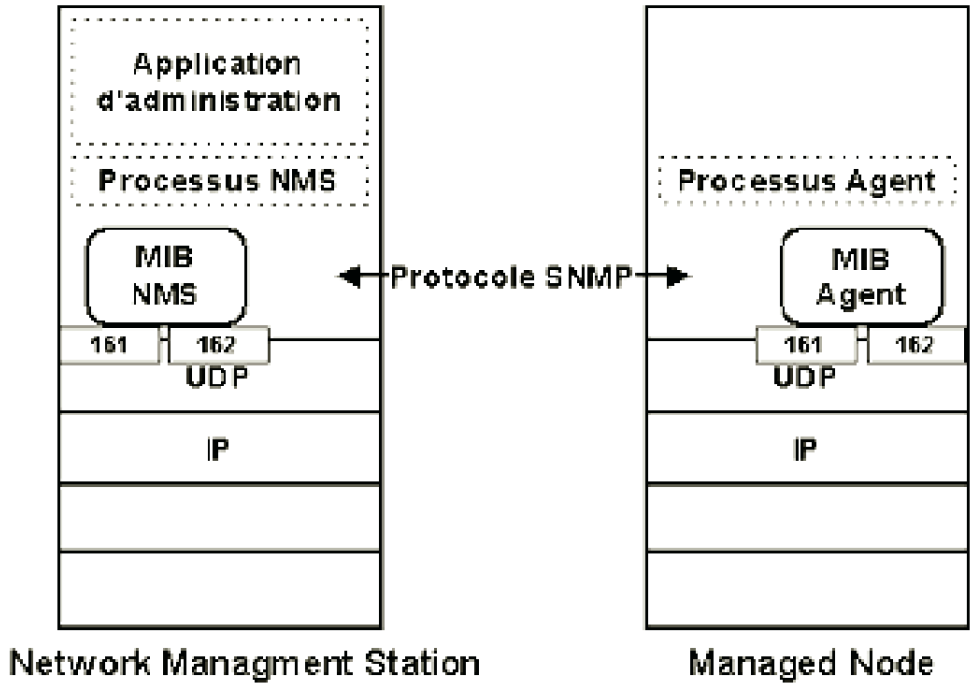


FIGURE 2.6 – Constituants de SNMP.

[15]

— **Agent SNMP**

« Un agent SNMP est un composant logiciel chargé de vérifier le fonctionnement du nœud administrable. Il peut être sollicité par le NMS au travers de commandes ou de requêtes SNMP et il peut envoyer des alertes (traps) au Manager sans forcément être sollicité. Sa MIB locale lui permet de réaliser des traitements qui lui sont propres. Il peut être autonome ou passif, c'est-à-dire entièrement dépendant du Manager. Le Manager peut procéder à des interrogations régulières de tous les agents qui renvoient alors les paramètres demandés. Cette technique porte le nom de Polling (ou le sondage). La surcharge de trafic engendrée par le polling peut toutefois se révéler pénalisante sur un réseau étendu. En effet, plus le nombre d'équipements est important et plus le polling va monopoliser de la bande passante, provoquant une surcharge (overhead) du réseau. Pour réduire ce phénomène, il est possible de mettre en œuvre des agents particuliers : les « Agent-Proxy » et les « Sondes Rmon » ». [15]

— **MIB (Management Information Base)**

La MIB (Management Information Base) est une base de données intégrée à l'agent SNMP. Elle se présente sous la forme d'une arborescence où chaque nœud est identifié par un numéro ou un OID (Object Identifier). La MIB comprend généralement des éléments communs à tous les agents SNMP d'un même type de matériel, ainsi que des éléments spécifiques à chaque fabricant. Chaque dispositif supervisé dispose de sa propre MIB, qui suit une structure standardisée.

La MIB ressemble à ce qui est illustré dans la figure 2.7 :

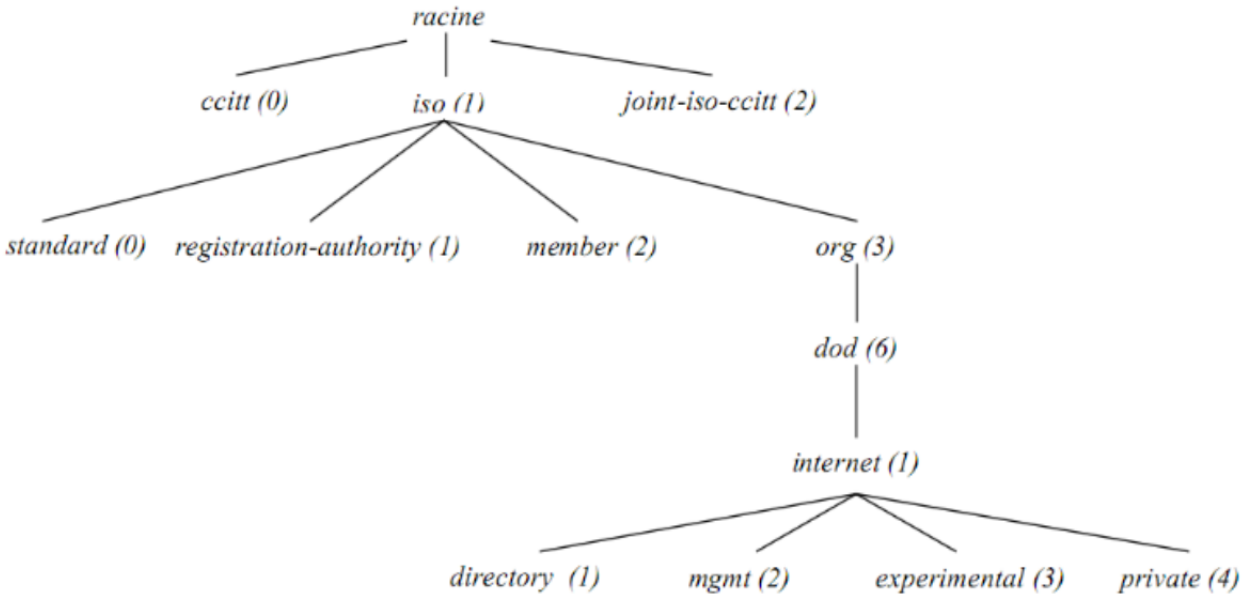


FIGURE 2.7 – Arborescence d'une MIB standard.

[16]

La branche intéressante est internet. En la détaillant on a le resultat illustré dans la figure 2.8 :

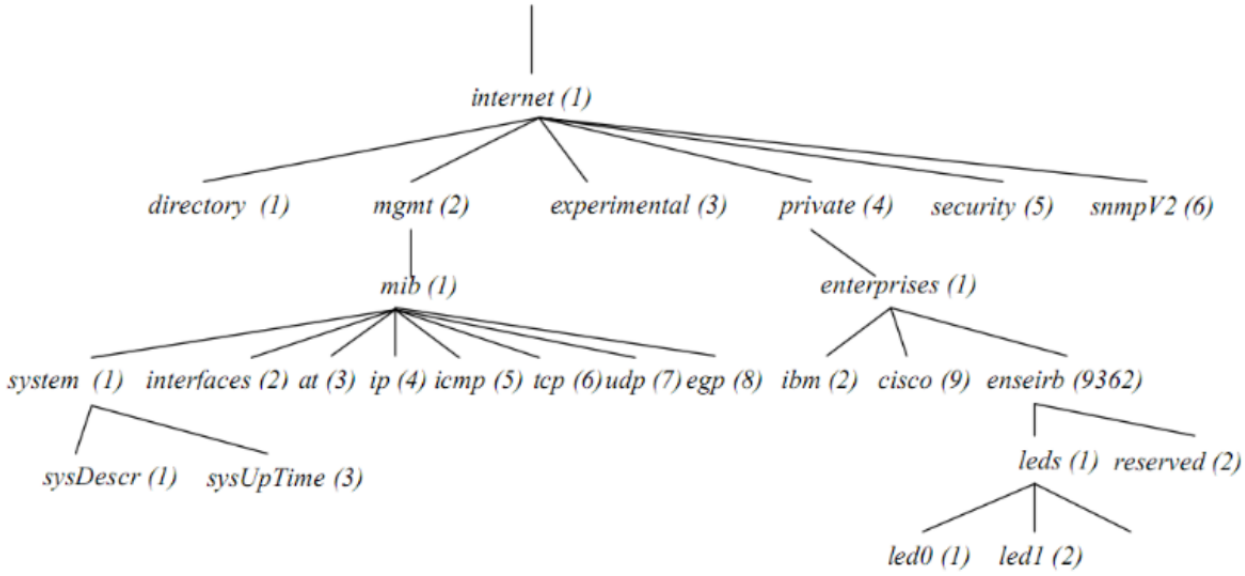


FIGURE 2.8 – Branche internet d'une MIB.

[16]

Pour obtenir les informations spécifiques à une branche de la MIB, on utilise le numéro « 0 » qui correspond à une feuille de cette branche. Par exemple, le nom symbolique « 1.3.6.1.2.1.1.3.0 » représente l'OID suivant que nous manipulerons si nécessaire. Il est intéressant de noter que la plupart des objets d'intérêt commencent par l'OID « 1.3.6.1.2.1 ».
Si une entreprise souhaite définir son propre ensemble de variables de gestion, elle enregistre son numéro d'objet sous le nœud « iso.org.dod.internet.private.entreprise ». Ces MIB sont alors considérées comme privées et correspondent à la racine « 1.3.6.1.4.1 ». [16]

2.1.6.4 Les différentes versions de SNMP

Selon GOUPILLE, P.-A [17], le protocole SNMP est basé sur l'échange de messages entre les ressources administrables et une station d'administration. Il existe 3 versions de ce protocole :

— **SNMP v1 :** Cette version est la plus utilisée car la plus « légère ». [17]

— **SNMP v2 :** Vu sa complexité (trop complexe), cette version est délaissée. Elle assure un niveau plus élevé de sécurité (authentification, cryptage...) des messages d'erreurs plus précis, autorise l'usage d'un Manager central... [17]

— **SNMP v3 :** permet de disposer des avantages de la version 2 sans en présenter les inconvénients. Elle définit un nouveau modèle de sécurité USM (User-based Security Model) évitant le décryptage des messages de commande qui transitent sur le réseau et autorise des droits différents en fonction des utilisateurs. [17]

2.2 L'état des lieux des outils de supervision

Après avoir présenté les notions et concepts liés à la supervision des réseaux informatiques, nous allons survoler trois outils de supervision de réseau informatique utilisé dans ce domaine. Ces outils sont : Zabbix, Nagios et Centreon.

2.2.1 Zabbix

2.2.1.1 Présentation de Zabbix

Créé par Alexei Vladishev en 2001, il est actuellement développé et soutenu par Zabbix SIA(Signs Partnership Agreement). Zabbix est une solution de surveillance distribuée open source, gratuite de classe entreprise. C'est un logiciel qui supervise de nombreux paramètres réseaux ainsi que la santé et l'intégrité des serveurs. Il utilise par ailleurs un mécanisme de notification flexible qui permet aux utilisateurs de configurer une base d'alerte e-mail pour pratiquement tous les événements. Il repose sur du C/C++, PHP (Hypertext Preprocessor) pour la partie front end et MySQL/Oracle pour la partie BDD (Base De Donnée).
Zabbix est un outil de supervision, ambitionnant de concurrencer Nagios. Il permet de superviser le réseau et systèmes (processeur, disque, mémoire, processus,). Ce dernier offre des vues graphiques et des alertes sur seuil. Il peut être décomposé en 3 parties séparées :

1. Le serveur de données.
2. L'interface de gestion.
3. Le serveur de traitement.

Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent Zabbix peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques de la charge CPU(Central Processing Unit), de l'utilisation du réseau, ainsi que l'espace disque...
Le logiciel peut réaliser le monitoring via SNMP. Il est possible de configurer des "proxy Zabbix" afin de répartir la charge ou d'assurer une meilleure disponibilité de service. Zabbix peut monitorer de 3 manières différentes :

1. Lancement d'un processus sur les machines à monitorer pour collecter des données locales, grâce à l'agent Zabbix (obtenir des infos sans utiliser SNMP).
2. Requêtes SNMP.
3. Checks externes qui sert à tester les services réseaux (rien à installer sur l'équipement surveillé, tests limités à des pings ou test de protocoles). [18]

2.2.1.2 Les fichiers de configuration de Zabbix

Le logiciel de supervision Zabbix utilise plusieurs fichiers de configuration voici les plus couramment utilisés :

— **zabbix.agentd.conf :** Ce fichier est utilisé pour configurer l'agent Zabbix.

— **zabbix.server.conf :** Il est utilisé pour configurer le serveur Zabbix. Il contient des informations telles que le nom d'hôte, le port, les chemins d'accès aux fichiers de données.

— **zabbix.proxy.conf :** Il est utilisé pour configurer le proxy Zabbix. Il contient des informations sur les serveurs et les agents connectés au proxy, les paramètres de journalisation.

— **apache.conf :** Il est utilisé pour configurer l'interface web Zabbix basée sur Apache. Il contient des informations sur la façon dont apache communique avec PHP.

— **php.ini :** utilisé pour configurer les paramètres de PHP pour l'interface web Zabbix. Il contient des informations telles que les limites de mémoire.

Les fichiers de configuration sont généralement situés dans le répertoire « /etc/zabbix » sur les systèmes Linux. [18]

2.2.1.3 Fonctionnalités de Zabbix

Le superviseur Zabbix offre les fonctionnalités suivantes :

• Offre une interface web de consultation et d'administration.

• Peut générer des graphes.

• Supervise des équipements SNMP.

• Gère les pannes et les performances

• Découve automatiquement des serveurs et périphériques réseaux.

• Authentifie l'agent sécurisé.

• Notification par e-mail d'événements prédéfinis.[18]

2.2.1.4 Architectures de Zabbix

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

— **Serveur :** Le serveur Zabbix est le composant central auquel les agents communiquent des informations et des statistiques sur la disponibilité et l'intégrité. Le serveur est le référentiel central dans lequel sont stockées toutes les données de configuration, statistiques et opérationnelles.

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

— **Interface Web :** Pour un accès facile à Zabbix de n'importe où et depuis n'importe quelle plate-forme, l'interface Web est fournie. L'interface fait partie du serveur Zabbix et s'exécute généralement (mais pas nécessairement) sur la même machine physique que celle exécutant le serveur.

— **Procuration :** Le proxy Zabbix peut collecter des données de performance et de disponibilité pour le compte du serveur Zabbix. Un proxy est une partie facultative du déploiement de Zabbix; cependant, il peut être très avantageux de répartir la charge d'un seul serveur Zabbix.

— **Agent :** Les agents Zabbix sont déployés sur des cibles de surveillance pour surveiller activement les ressources et les applications locales et signaler les données collectées au serveur Zabbix. Depuis Zabbix 4.4, il existe deux types d'agents disponibles : l'agent Zabbix (léger, supporté sur de nombreuses plateformes, écrit en C) et l'agent Zabbix 2 (extra-flexible, facilement extensible avec des plugins).

— **Flux de données :** Dans Zabbix, pour collecter des données, créez un hôte et un élément pour créer un déclencheur. Ce dernier est nécessaire pour mettre en place une action, par exemple, pour être alerté d'une charge CPU élevée sur un serveur. L'utilisation de modèles facilite ce processus complexe, offrant une grande flexibilité de configuration dans Zabbix. [18]

La figure 2.9 illustre l'architecture globale de Zabbix;

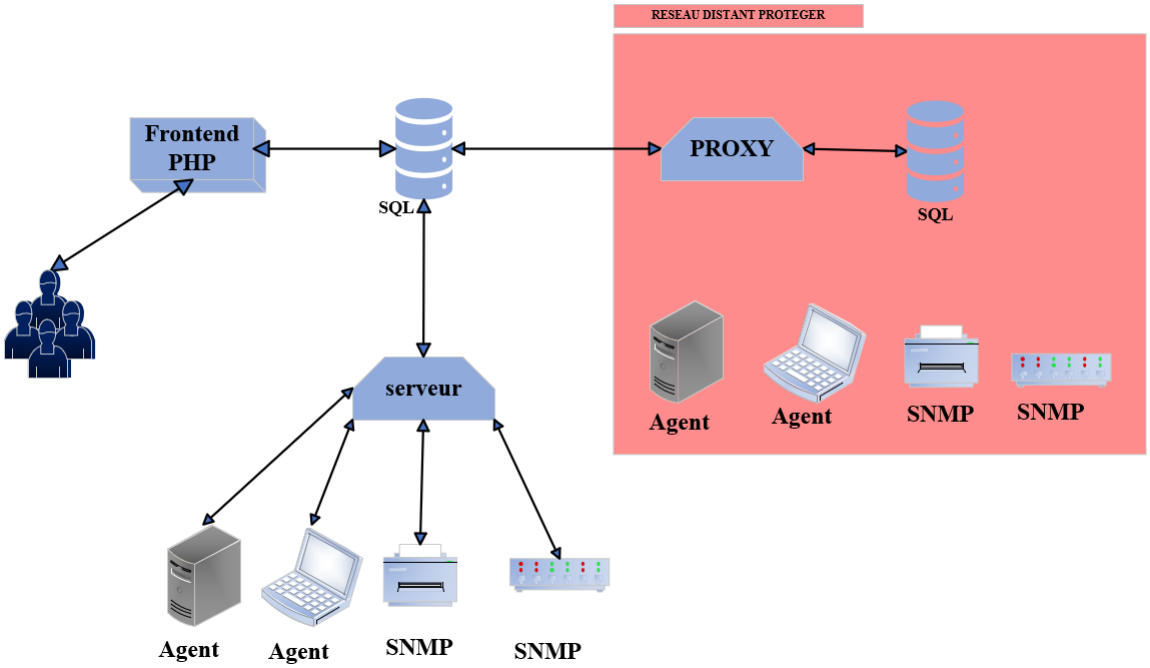


FIGURE 2.9 – Architecture globale de Zabbix.

2.2.1.5 Avantages et inconvénients de Zabbix

Le tableau suivant montre quelques avantages et inconvénients de Zabbix

Avantages	Inconvénients
✓ Multiplateforme et utilise peu de ressources. ✓ Plus léger grâce à son homogénéité ✓ Configuration et utilisation aisée. Mise à jour de la configuration via l'interface Web de Zabbix. ✓ Réalisation de graphiques, cartes ou screens. ✓ Serveur Proxy Zabbix. Surveillances des sites web : Temps de réponse et vitesse de transfert.	✓ L'agent Zabbix communique les données en clair. Nécessité de sécuriser les données (via VPN par exemple). ✓ Interface vaste, la mise en place des Template n'est pas évidente au début : petit temps de formation nécessaire.

FIGURE 2.10 – Avantages et inconvénients du logiciel Zabbix.

[18]

2.2.2 Nagios

2.2.2.1 Présentation de Nagios

Créé en 1999 par Ethan Galstad, Nagios (anciennement Netsaint) est un logiciel qui permet de superviser un système d'information. Il est considéré comme étant la référence des solutions de supervision open source, libre sous licence (GNU General Public Licence). Il reste l'outil de supervision le plus utilisé à l'heure actuelle. Moteur en langage C, base de données SQL(Structured Query Language), son interface web en PHP est la partie graphique. Via un serveur web tel qu'Apache, il va permettre à l'administrateur d'avoir une vue globale de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activités. Il permet de surveiller des hôtes et des services spécifiques en indiquant leur état en permanence. Il peut monitorer de 3 manières :

1. L'utilisation des journaux d'exploitation par l'envoi des évènements issus des fichiers log en temps réel vers un serveur central, offrant les informations nécessaires à la supervision.
2. Supervision active des services.
3. Une infrastructure qui nous permet de garder l'historique des performances.

Nagios a évolué pour inclure des milliers de projets développés par sa communauté dans le monde entier. Il est officiellement parrainé par Nagios Entreprises qui soutient la communauté, que ce soit par les ventes de ses produits ou ses services commerciaux. Le seul prérequis pour son bon fonctionnement est une machine exploitant Linux (ou une variante Unix), ce qui le rend beaucoup plus attractif que d'autres produits concurrents. [19]

2.2.2.2 Fonctionnalités de Nagios :

Le superviseur Nagios offre les fonctionnalités suivantes :

• Il centralise les informations récoltées périodiquement par le fonctionnement modulaire dont il est caractérisé.

• Il génère des rapports de surveillance, des graphes par l'interfaçage avec RRDTools et des cartographies du réseau.

• Il a la possibilité de monitorer à distance à travers un firewall.

• Il peut définir des serveurs esclaves qui prennent le relais si le serveur maitre tombe en panne.

• Il gére des alertes par différents moyens de communication (SMS (Short Message Service), mail...).

• Il permet de distinguer un serveur en panne et un serveur injoignable. [19]

2.2.2.3 Avantages et inconvénients de Nagios :

Le tableau suivant montre quelques avantages et inconvénients de Nagios

Avantages	Inconvénients
✓ Une très grande communauté qui participe activement au développement. ✓ Un moteur performant. ✓ Possibilité de répartir la supervision entre plusieurs administrateurs. ✓ La supervision à distance peut utiliser SSH.	✓ Configuration complexe mais peut s'améliorer en ajoutant un autre outil de supervision. ✓ Interface peu ergonomique et intuitive. ✓ Ne permet pas d'ajouter des hosts via Web ✓ Pas de représentations graphiques

FIGURE 2.11 – Avantages et inconvénient du logiciel Nagios.

[19]

2.2.3 Centreon

2.2.3.1 présentation de Centreon

Créé en 2003 par une société française, puis repris par une nouvelle entreprise nommée Merethis, Centreon (anciennement appelé Oreon) est un logiciel de supervision des applications, systèmes et réseaux, basé sur les concepts de Nagios. C'est une solution open source, gratuite et complète destinée aux administrateurs et exploitants du service de supervision. Il apporte de nombreuses fonctions telles que la consultation de l'état des services et des machines supervisées, la métrologie, le reporting, l'accès aux événements de supervision et la gestion avancée des utilisateurs via des listes de contrôle d'accès (ACL (Access Control List)). Il s'appuie sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision. Centreon possède sa propre version de chaque fichier de configuration de Nagios. Lorsque l'utilisateur modifie un paramètre par l'interface Centreon, ce changement est d'abord répercuté sur les fichiers "de co-

pies" de Centreon pour que les modifications soient prises en compte par Nagios. [20]

2.2.3.2 Fonctionnalités de Centreon :

Centreon offre les fonctionnalités suivantes :

• Gestion de la politique des profils utilisateurs (droits, langues, accès à distance aux ressources).
• Supervision en temps réel (détection des pannes, disponibilité, prise en compte des pannes,).
• Traitement des performances (graphiques, historique).
• Accessibilité de l'état du système à un plus grand nombre d'utilisateurs, notamment à l'aide de graphiques. [20]

2.2.3.3 Avantages et inconvénients de Centreon :

Le tableau suivant montre quelques avantages et inconvénients de Centreon.

Avantages	Inconvénients
✓ Permet d'ajout des plugins et d'adapter le système aux besoins spécifiques de leur infrastructure.	✓ Il peut y avoir une dépendance sur la disponibilité et la maintenance de ces plugins externes.
✓ Facilite l'ajout de nouvelles fonctionnalités et l'intégration avec d'autres outils et systèmes de gestion.	✓ Des mesures supplémentaires peuvent être nécessaires pour assurer une performance optimale et une supervision efficace.
✓ Permet de collecter, d'analyser et de présenter des données de supervision de manière claire et concise.	✓ Nécessite une maintenance régulière pour garantir son bon fonctionnement.

FIGURE 2.12 – Avantages et inconvénients du logiciel Centreon.

[20]

Conclusion

Dans ce chapitre, nous avons effectué une présentation de la notion de supervision et de ses enjeux. Nous avons décrit trois outils utilisés dans le domaine de la supervision des réseaux informatiques, à savoir : Zabbix, Nagios, Centreon.
Le chapitre suivant va porter sur la présentation de la structure d'accueil et l'étude détaillée de l'existant où nous cernerons la problématique de notre sujet et nous présenterons la solution adoptée.

Chapitre 3

Présentation de l’organisme d’accueil

Introduction

Ce chapitre fera l'objet d'une étude du réseau existant dans l'entreprise Cevital dans laquelle nous aborderons les améliorations proposées. Dans un premier temps, nous donnerons un bref aperçu sur l'entreprise pour mieux comprendre sa structure et ses objectifs, ensuite nous étudierons son réseau informatique et ses composants mis en place afin de proposer d'éventuelles améliorations.

Notre étude consistera à évaluer les performances et l'efficacité du réseau informatique existant. Nous analyserons sa capacité à répondre aux besoins de l'entreprise en termes de communication, de partage de données et d'accès aux ressources. Nous examinerons également les mesures de sécurité mises en place pour protéger le réseau contre les menaces potentielles. En identifiant les forces et les faiblesses du réseau, nous serons en mesure de formuler des recommandations précises pour les améliorations possibles.

3.1 Présentions de l'entreprise Cevital

3.1.1 Création et évolution

— **Création** L'entreprise fut créée par Mr Issaad REBRAB en 1998. Elle est la première entreprise privée algérienne à investir dans un domaine d'activité diversifié. Elle a traversé d'importantes étapes pour atteindre sa taille et sa popularité actuelles.

— **Evolution**

Cevital opère depuis plusieurs années à l'international, notamment en Europe (France, Italie, Espagne), en Tunisie, au Maroc et au Brésil. En 1999 entre en production la raffinerie d'huile et en 2003 entre en production la raffinerie de sucre. En 2005 se fait l'acquisition de LALLA KHEDIDJA, et enfin en 2006 elle acquiert COJEK (conserves et jus d'Elkseur).

— **Situation géographique**

Cevital est l'une des plus grandes entreprises en Algérie et un leader dans le secteur agroalimentaire. Sa localisation bénéficie de sa proximité économique, en effet il est proche du port, de l'aéroport et d'un terminal portuaire de déchargement. La figure 3.1 illustre une vue satellitaire du complexe de Cevital :

FIGURE 3.1 – Vue satellitaire du complexe Cevital.

3.2 Fiche technique de l'entreprise

Le tableau ci-dessous représente quelques informations relatives à l'entreprise Cevital où j'ai effectué mon stage de fin de cycle master.

Dénomination	Cevital
Logo	
Siège	Nouveau quai du port de Bejaia, à proximité de la route nationale N° 09 et N°26.
Secteurs d'activités	Industrie agroalimentaire. Services et manufactures. Construction Distribution Industries
Numéros de FAX	00 213 (0) 34 10 39 39
Numéros de Téléphone	00 213 (0) 34 10 38 38
Site Internet	www.cevital.com

FIGURE 3.2 – Identification sur Cevital.

3.3 Objectifs, missions et activités de l'entreprise

3.3.1 Les missions

L'entreprise a pour missions principales de développer la production et d'assurer la qualité du conditionnement des huiles, des margarines et du sucre, et ce à des prix nettement plus compétitifs, dans le but de satisfaire le client et de le fidéliser.

3.3.2 Les activités

Les travaux de génie civil de la raffinerie ont débuté en Février 1991. Le complexe Cevital a débuté son activité par le conditionnement en Décembre 1998. Cette dernière est devenue fonctionnelle, en Août 1999. L'ensemble des activités de Cevital est concentré sur la production et la commercialisation des huiles végétales, de margarine et de sucre. En mai 2023 l'entreprise a inauguré son usine de trituration de graines oléagineuses pour produire des huiles végétales.

3.3.3 Les objectifs

Les objectifs visés par Cevital peuvent se présenter comme suit :

• Encouragement des agriculteurs par des aides financières pour la production locale de graines oléagineuses. (Objectif atteint en mai 2023)

• Diversification de ses produits et leur diffusion sur tout le territoire national.

• Modernisation de ses installations et adoption de nouvelles démarches de gestion technique afin d'augmenter le volume de sa production.

• Positionnement de ses produits sur le marché international.

3.4 Organigramme général de l'organisme d'accueil

Cevital est organisée autour de différentes directions qui s'occupent des actions liées à la gestion et au développement de l'entreprise. La figure 3.3 nous montre les différentes structures qui composent Cevital :

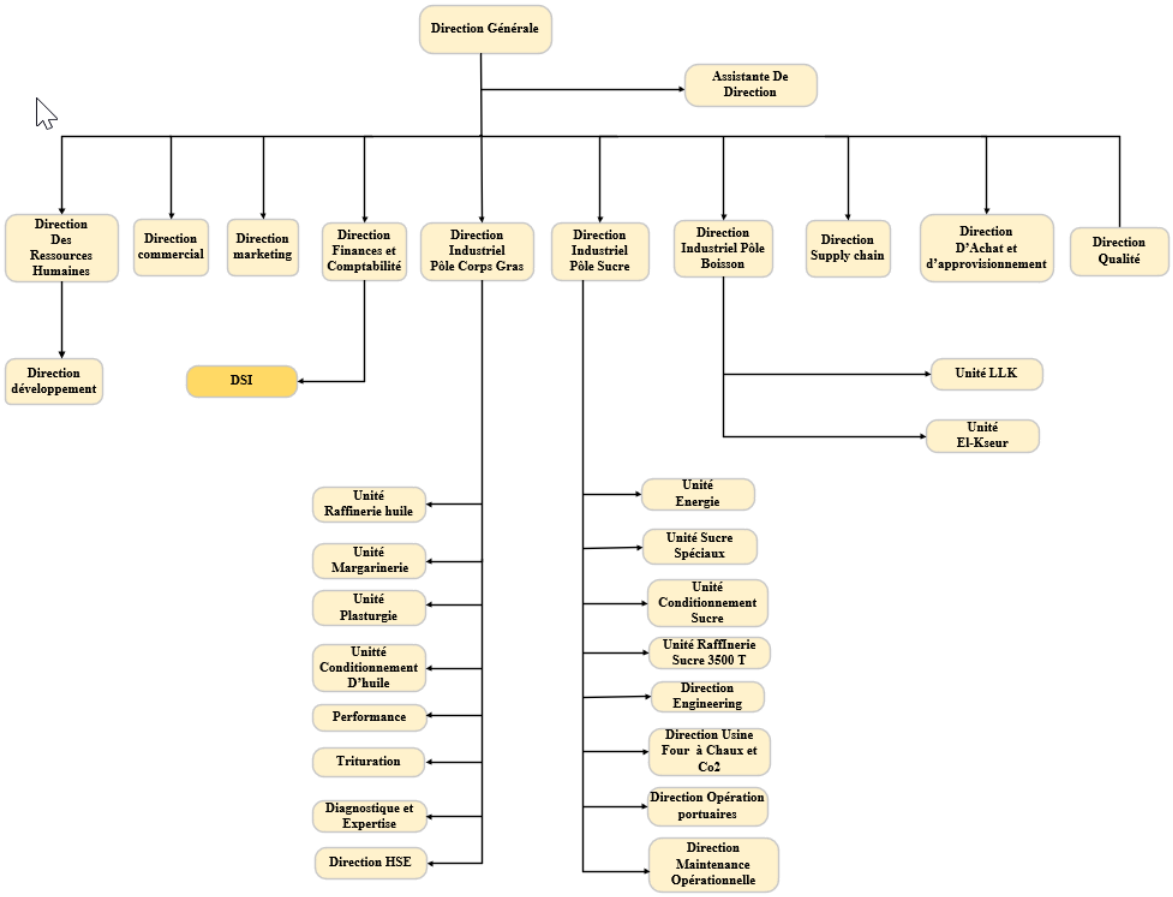


FIGURE 3.3 – Organigramme générale de Cevital.

L'ensemble des activités de Cevital est concentré sur la production qui se présente comme suit :

3.4.1 La direction des Finances et comptabilité

Chargée de préparer et de mettre à jour les budgets, tenir la comptabilité et préparer les états comptables et financiers selon les normes, et aussi pratiquer le contrôle de gestion.

3.4.2 La direction Commerciale

Chargée de commercialiser toutes les gammes des produits et de développer le fichier clients de l'entreprise. Elle met aussi en place des stratégies pour atteindre des objectifs commerciaux spécifiques, et s'occupe de la promotion des projets à base de hautes technologies.

3.4.3 La direction des Ressources Humaines

Cette direction assure un support administratif de qualité à l'ensemble du personnel de Cevital. Elle pilote les activités du social, assiste la direction générale ainsi que tous les managers sur tous les aspects de gestion ressources humaines. Elle garantit également le recrutement, la gestion des carrières et l'identification des besoins.

3.4.4 Direction Approvisionnements

Elle est chargée de mettre en place les mécanismes permettant de satisfaire les besoins en matières et services dans les meilleurs délais, avec la meilleure qualité et au moindre coût, et en réalisant des objectifs de production et de vente.

3.4.5 Direction Marketing

Chargée de varier les marques et les gammes de produits, son principal levier est la connaissance des consommateurs, leurs besoins, leurs usages ainsi que la veille sur les marchés internationaux et sur la concurrence. Les équipes marketing produisent des recommandations d'innovation, de rénovation, d'animation public-promotionnelle sur les marques et métiers de Cevital.

3.4.6 La direction HSE (Hygiène, Sécurité et environnement)

Chargée de maintenir et d'améliorer les différents systèmes de management et référentiels pour se conformer aux standards internationaux, elle veille aussi au respect des exigences règlementaires produits, environnement et sécurité.

3.4.7 La direction Industrielle

Chargée de l'évolution industrielle des sites de production, elle définit, avec la direction générale, les objectifs et le budget de chaque site. Analyse les dysfonctionnements sur chaque site (équipements, organisation...) et recherche les solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Anticipe les besoins en matériel et supervise leur achat (étude technique, tarif, installation...).

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

La direction système d'information de Cevital est composée de deux départements :

1. Métiers.
2. Département système réseaux télécom : il assure le bon fonctionnement de réseaux et de la télécommunication.

Chaque département a pour objectif d'améliorer le niveau de l'informatique et ses services pour garantir le développement et la progression des services du groupe Cevital.
Dans la figure 3.4 on retrouve l'organigramme de la direction système d'information organisé comme suit :

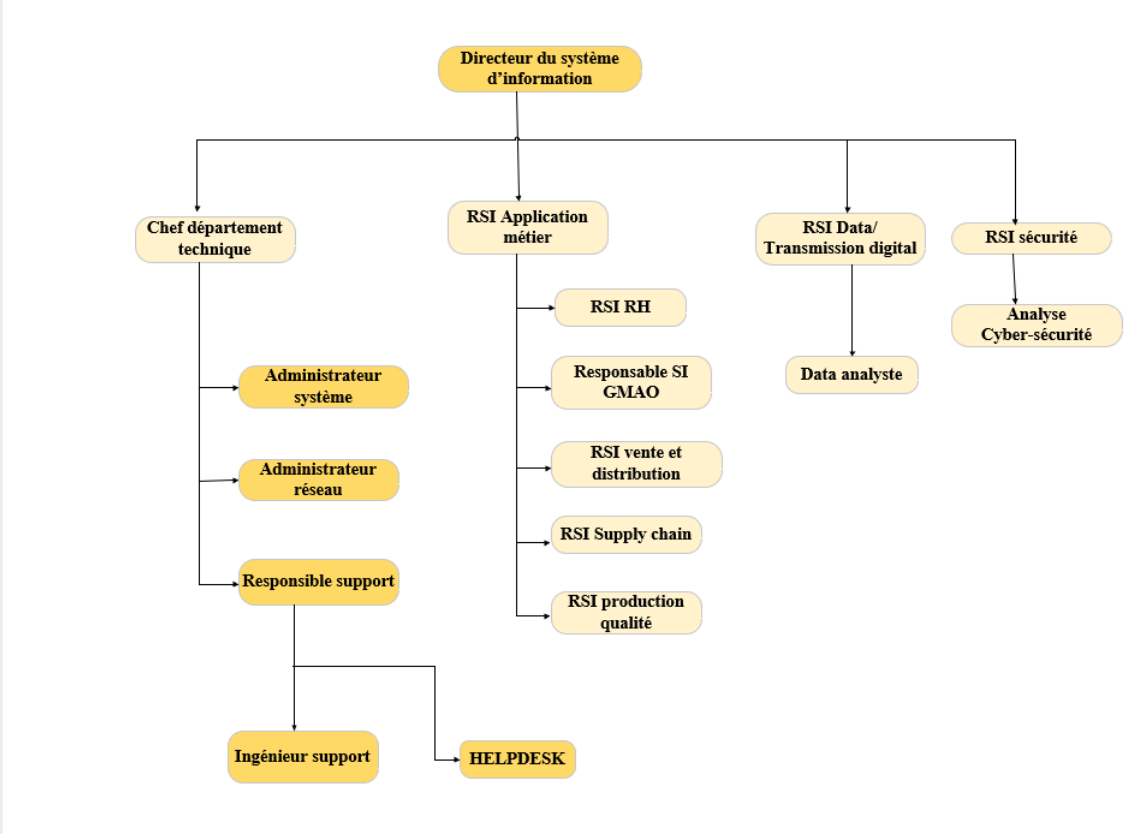


FIGURE 3.4 – Organigramme de la DSI.

Le service informatique est dirigé par des responsables et des spécialistes du domaine qui sont :

3.5.1 Directeur du système d'information

Chargé de régler les problèmes à moindre coût et dans les plus brefs délais, il optera pour des solutions informatiques améliorant la productivité de l'entreprise.

3.5.2 Administrateur système

Chargé de concevoir, d'installer et de veiller au bon fonctionnement d'une infrastructure informatique et réseau d'une entreprise, il assure également la gestion et la maintenance du système opérant sur le réseau.

3.5.3 Administrateur réseau

Chargé d'administrer le réseau et d'assurer la bonne circulation de l'information dans l'entreprise, il veille à la qualité et à la performance des équipements et du réseau, tout en répondant aux besoins des utilisateurs.

3.5.4 Responsable support

Chargé d'assurer un contrôle à distance des postes de travail, il apportera aux utilisateurs une aide pour la prise en main de leur équipement et assurera un support téléphonique interne.

3.6 Infrastructure informatique

3.6.1 Architectures réseau de l'entreprise

Cevital dispose d'un réseau commuté de taille importante et est composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements dont : deux Switchs cœur, deux ToR et deux distribution, des routeurs et des Firewall, pour la plupart de marque Cisco, pour établir la communication entre les différents sites interconnectés. Ils utilisent de la fibre optique fournie par Algérie télécom.

Le réseau du complexe Cevital s'étend actuellement sur six principaux pôles à savoir : Bejaia,

Alger, Oran, El Kseur (Cojek) et Tizi Ouzou (Lalla Khadija). Cette architecture est illustrée dans la figure 3.5 :

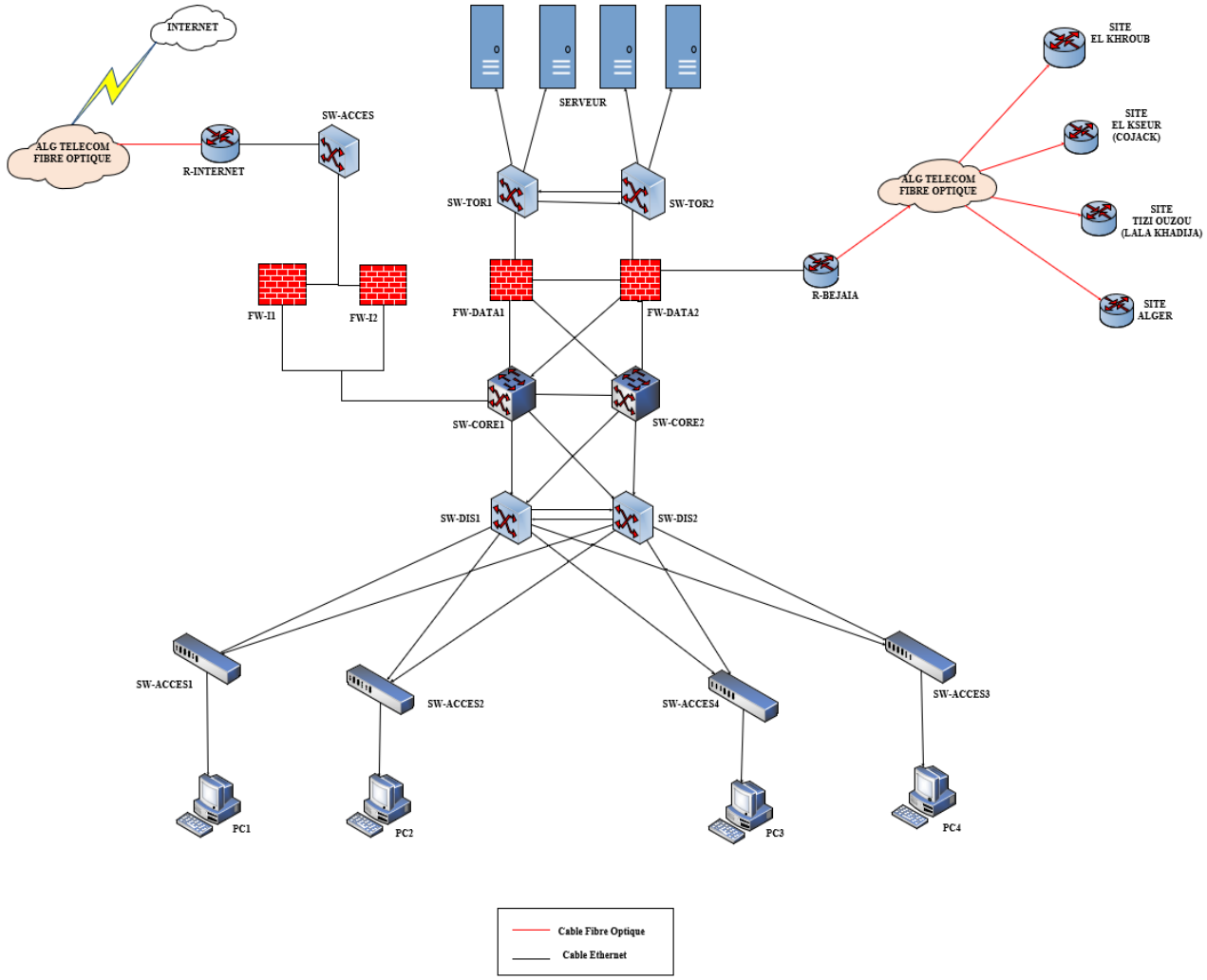


FIGURE 3.5 – Architecture réseau de Cevital.

3.6.2 Etude de l'architecture

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

— **Infrastructure matériel**

Au niveau de Cevital-Bejaia Les différentes directions de l'entreprise sont reliées au Data Center (Centre d'Information) qui est le cœur de Cevital. Il contient tous les équipements physiques et tous les serveurs dont Cevital a besoin, mises dans des armoires de brassage. Cette pièce est très importante et le droit d'accès est limité. Elle n'est réservée qu'à l'équipe du système d'information. Ci-dessous figurent les diffèrent équipements qui constituent le réseau.

Nom de l'équipement	**Le hardware (hard)**		**Le software (soft)**
Routeur 	Cisco 2900		IOS (Interworking Operating System)
Switch 	Switch cœur	Cisco 6500	IOS (Interworking Operating System)
	Switch d'accès	Cisco Catalyst 2960	
Pare-feu 	➢ Fortinet ➢ Palo Alto 3020		Linux
Switch distributeur (backbone) 	Cisco (Catalyst 4507R) 2960 et 2950		IOS (Interworking Operating System)
Server 	➢ HP		➢ Windows 2019 ➢ Windows 2022. ➢ Windows 2012 et 2016. ➢ ESXI VMware
Ordinateur 	➢ HP ➢ LENOVO ➢ ASUS		➢ Windows

FIGURE 3.6 – les différents équipements dans l'entreprise.

— **Les différents VLAN de l'entreprise**

Selon différents départements, utilisateurs et privilèges, le gestionnaire de réseau divise le réseau en plusieurs VLAN.

Un VLAN Management a également été créé pour permettre la gestion du réseau à distance (configuration, mise à jour, sauvegarde et monitoring). Le tableau ci-dessous dresse la liste des VLAN de l'entreprise.

VLAN		Description
Numéro	**Nom**	
12	IT	Direction Système d'Information
13	R.A.F Huile	Raffinerie d'huile
14	Sucre	Raffinerie de sucre
16	Wifi	Wifi destiné aux collaborateurs Cevital
17	Skeeper	Application de traçabilité
18	Imprimante réseau	Imprimante réseau
20	Téléphonie	Téléphonie IP (VoIP)
21	Visio	Equipement de visio-conférence
23	Guest Wifi	Réseau Wifi destiné à l'utilisateur non employé par Cevital
26	DFC	Direction Finances et Comptabilité
27	DG	Direction général

FIGURE 3.7 – Les différentes VLAN de l'entreprise Cevital.

3.7 Problématiques et solution proposées

3.7.1 Problématiques

La plupart des organisations et des entreprises aujourd'hui comptent sur leurs réseaux locaux dans des processus commerciaux clés. En d'autres termes, leur efficacité opérationnelle et l'amélioration continue de leurs capacités de productivité et de réponse sont prin-

cipalement basées sur la qualité de leur infrastructure réseau. Cela a provoqué l'émergence réelle de systèmes complexes spécifiquement utilisés dans la gestion du réseau. Apres avoir étudié l'architecture réseau de CEVITAL, cela nous a permis de soulever les problèmes suivants :

• Un taux important de temps est gaspillé lors du diagnostic des pannes, ce qui influe sur la qualité du service et donc le bon fonctionnement de l'entreprise.

•Plus le nombre des équipements et des services augmente plus les tâches de l'administrateur deviennent trop compliquées, il n'arrive donc pas à les assurer convenablement.

3.7.2 Solution retenue

Le responsable du projet a récemment pris une décision importante concernant la mise en place d'un outil de supervision réseau open source. Après une évaluation minutieuse des différentes options disponibles, il a choisi Zabbix pour répondre à nos besoins spécifiques. La principale raison de ce choix est la capacité de Zabbix à offrir une supervision en temps réel, ce qui est essentiel pour assurer le bon fonctionnement de notre infrastructure réseau. En plus de la supervision en temps réel, Zabbix se distingue par sa facilité d'utilisation. Son interface conviviale permettra à notre équipe de prendre rapidement en main l'outil, ce qui est crucial pour une intégration fluide dans notre environnement existant.
L'un des avantages majeurs de Zabbix est la richesse de ses fonctionnalités. Le responsable du projet a souligné que certaines de ces fonctionnalités ne se trouvent pas dans d'autres logiciels de supervision. Cela signifie que Zabbix nous offre une plus grande flexibilité et une capacité d'adaptation plus élevée à nos besoins spécifiques. Par exemple, nous serons en mesure de configurer des alertes personnalisées, de surveiller différents types de périphériques réseau, d'analyser les performances en temps réel et de générer des rapports détaillés.
En conclusion, le choix de Zabbix comme outil de supervision réseau open source est le résultat d'une analyse approfondie de ses caractéristiques et fonctionnalités. Il est considéré comme le plus adapté à notre cas, offrant une supervision en temps réel, une facilité

d'utilisation et une large gamme de fonctionnalités avancées. Avec Zabbix, nous sommes confiants quant à notre capacité à surveiller et à maintenir notre réseau de manière efficace et fiable.

Conclusion

Le chapitre en question a été élaboré dans le but de nous familiariser avec l'entreprise d'accueil ainsi que son architecture réseau. Après avoir effectué une analyse approfondie du réseau de l'entreprise CEVITAL, nous avons identifié plusieurs faiblesses présentes dans son infrastructure. Cette démarche nous a permis de comprendre la problématique centrale de notre projet.

Suite à cette analyse, nous avons choisi l'outil de supervision ZABBIX pour répondre à nos besoins. ZABBIX a été sélectionné en raison de ses fonctionnalités avancées et de sa capacité à surveiller et à gérer efficacement les réseaux complexes. Grâce à cet outil, nous serons en mesure de collecter des données en temps réel sur les performances du réseau, de détecter les problèmes potentiels et d'y remédier rapidement.

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

Chapitre 4

Implémentation de la solution de supervision Zabbix

Introduction

Au sein de ce chapitre, nous nous concentrerons sur la modélisation et l'implémentation de notre politique de supervision, qui joue un rôle crucial dans la gestion efficace de notre réseau. Nous décrirons l'environnement de travail dans lequel nous déploierons notre méthode de supervision.

Pour commencer, nous présenterons les différentes étapes impliquées dans la modélisation de notre politique de supervision. Nous expliquerons également les méthodologies utilisées. Ensuite, nous passerons à l'implémentation pratique. Nous décrirons les outils et les logiciels spécifiques que nous utiliserons et nous fournirons des schémas des interfaces ZABBIX que nous avons personnalisées pour répondre à nos besoins de surveillance spécifiques.

4.1 Méthodologie de configuration

Le diagramme ci-dessous résume la méthodologie suivie sur toutes les étapes de configuration infrastructure sous GNS3 ainsi que les étapes d'installation et de configuration du serveur ZABBIX sous VMWare présentée dans la figure 4.1 ;

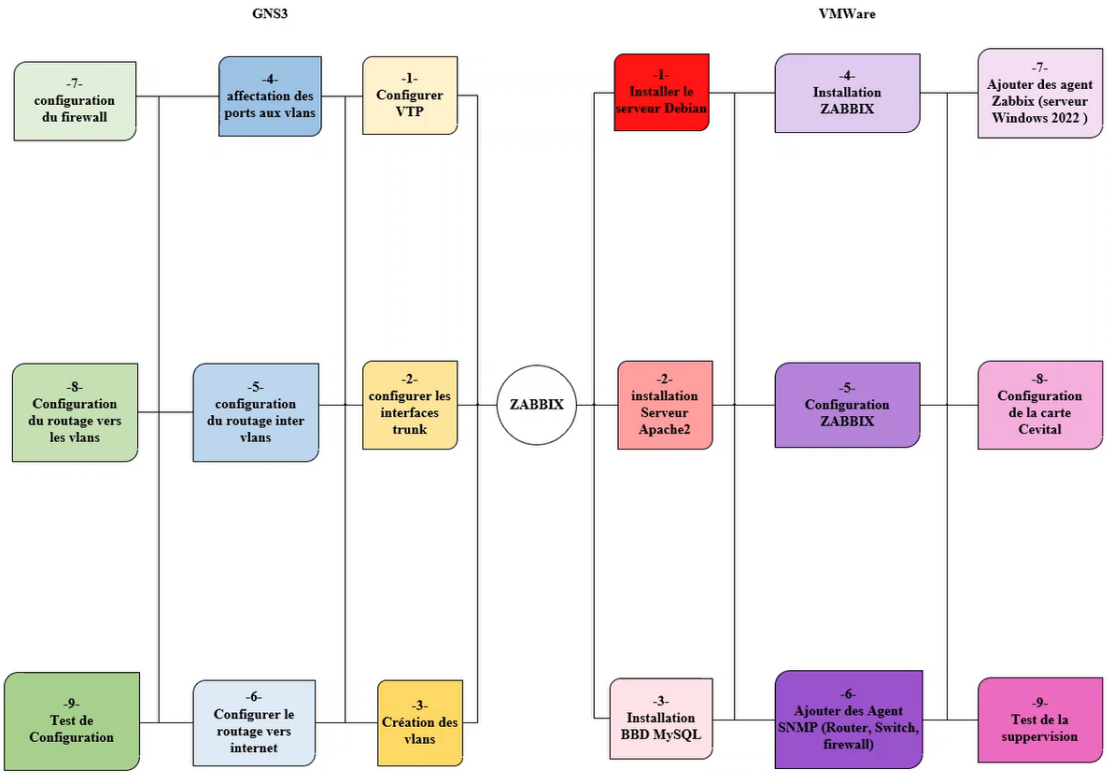


FIGURE 4.1 – Diagramme des étapes d'installation et configuration logiciels et matériels.

4.2 Reproduction du réseau LAN de Cevital

Pour configurer et surveiller le réseau local de Cevital, nous allons recréer une représentation du réseau dans le simulateur GNS3 (Graphical Network Simulator-3).

4.2.1 Réseau à superviser

Le réseau que nous allons surveiller se compose de :

• Un routeur ;

• Deux Pare-feu ;

• Switchs (deux switchs cœur, trois switchs d'accès) ;

• Un poste Windows ;

• Un serveur Linux ;

• Un Windows serveur qui fera objet de l'active directory ;

• Un serveur Zabbix qui s'occupera de la supervision et de l'analyse des informations du réseau ;

4.2.2 Configuration des VLANs

Le tableau ci-dessous montre les noms des VLANs existant au niveau de l'entreprise ainsi que leurs adresses de sous réseaux

Nom VLAN	ID VLAN	Adresse de sous réseau	Description
DSI	5	172.17.5.0/24	VLAN des postes de travail de la direction des systèmes d'information
DC	6	172.17.6.0/24	VLAN pour le data center
MANAGEUR	7	172.17.7.0/24	VLAN pour la supervision des équipements

FIGURE 4.2 – Nom des VLANs.

4.2.3 Configuration de VTP (Vlan Trunking Protocol)

Le protocole VTP est un protocole de la couche 2 qui offre un avantage majeur : ce dernier permet la propagation automatique des VLAN configurés sur un commutateur en mode « serveur » vers les autres commutateurs configurés en mode « client ». Lors de la configuration, nous mettrons les deux commutateurs principaux (Switchs Cœur) en mode « serveur » VTP, tandis que les autres commutateurs seront configurés en mode « client » VTP.
Le protocole VTP sera configuré comme illustré dans le tableau ci-dessous ;

VTP	Domain	Mode
SW-CORE-01	cevital.vtp	Server
SW-CORE-02	cevital.vtp	Server
SW-01	cevital.vtp	Client
SW-02	cevital.vtp	Client
SW-03	cevital.vtp	Client

FIGURE 4.3 – Configuration de VTP.

4.2.4 Classification des PC selon les VLANs

Les interfaces entre tous les switchs seront configurées en mode trunk pour qu'elles puissent transporter les informations des autre VLANs. Les interfaces qui seront connectées à des postes de travail seront configurées en mode Access.

La classification des PC sera selon les VLANs, comme illustré dans le tableau ci-dessous :

Nom de l'hôte	Port du Switch	ID du VLAN	Adresse IP de l'hôte	Passerelle
PC1	Port e3/3 SW-01	5	172.17.5.10/24	172.17.5.1
PC2	Port e3/2 SW-02	5	172.17.5.11/24	172.17.5.1
ZABBIX	Port e3/3 SW-02	6	172.17.6.8/24	172.17.6.1
SERVEUR-AD	Port e3/3 SW-02	6	172.17.6.9/24	172.17.6.1
PC3	Port e3/3 SW-03	7	172.17.7.10/24	172.17.7.1
PC MANAGEUR	Port e3/2 SW-03	7	172.17.7.11/24	172.17.7.1

FIGURE 4.4 – Classification des PC selon les VLANs.

4.2.5 Architecture réseau LAN liée à la supervision de Cevital

Pour concrétiser notre projet, nous allons commencer par configurer les équipements dans l'environnement GNS3. Ensuite, nous utiliserons l'outil Zabbix pour superviser ces équipements.

La figure 4.5 présente l'architecture réseau LAN de Cevital sous GNS3 :

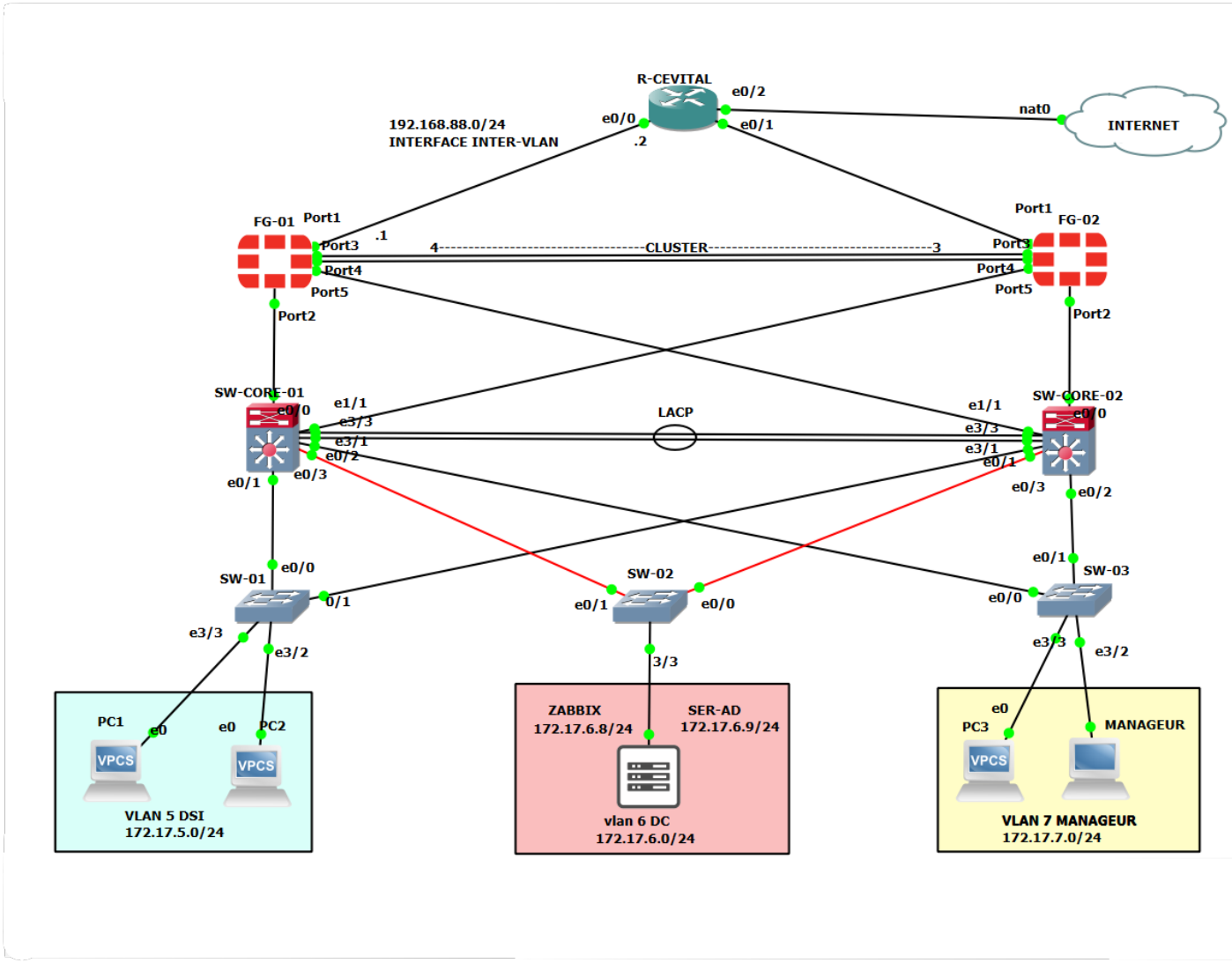


FIGURE 4.5 – Architecture réseau LAN de Cevital sous GNS3.

4.2.6 Configuration des équipements

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

• Configuration des noms des équipements ;

• Configurations de mots de passe pour le mode privilégié, la ligne console et virtuelle(Telnet et SSH) ;

• Configuration de la bannière de connexion ;

• Création des VLANs et configuration de VTP (Vlan Trunking Protocol) ;

• Configuration des interfaces du Routeur ;

• Création des VLAN ;

• Configuration du routage inter-vlan ;

• Configuration du DHCP (Dynamic Host Configuration Protocol) ;

• Configuration du routage statique au niveau du pare-feu ;

• Configuration de la politique de supervision au niveau du pare-feu.

4.3 Mise en place de la politique de supervision

Apres l'installation et la configuration du logiciel Zabbix (voir Annexe C), nous allons procéder à l'installation et la configuration de l'active directory sur la machine virtuelle Windows-Serveur, pour les bonnes pratique.

4.3.1 Création du client manageur et le configurer comme hôte dans l'interface Zabbix

Pour commencer, nous avons créé un poste d'administration (manageur) fournissant à l'administrateur une vue d'ensemble des équipements, facilitant ainsi les tâches d'administration.

Pour configurer l'hôte manageur qui est installé dans la VMWare, nous l'avons ajouté dans

l'interface Zabbix, pour cela, nous avons procédé comme suit :

Nous sommes allés dans : Configuration → Hôtes ou Surveillance → Hôtes. Cliquer sur créer un hôte à droite (ou sur le nom de l'hôte pour modifier un hôte existant). Entrer les paramètres de l'hôte dans le formulaire, comme illustré dans la figure 4.6 ;

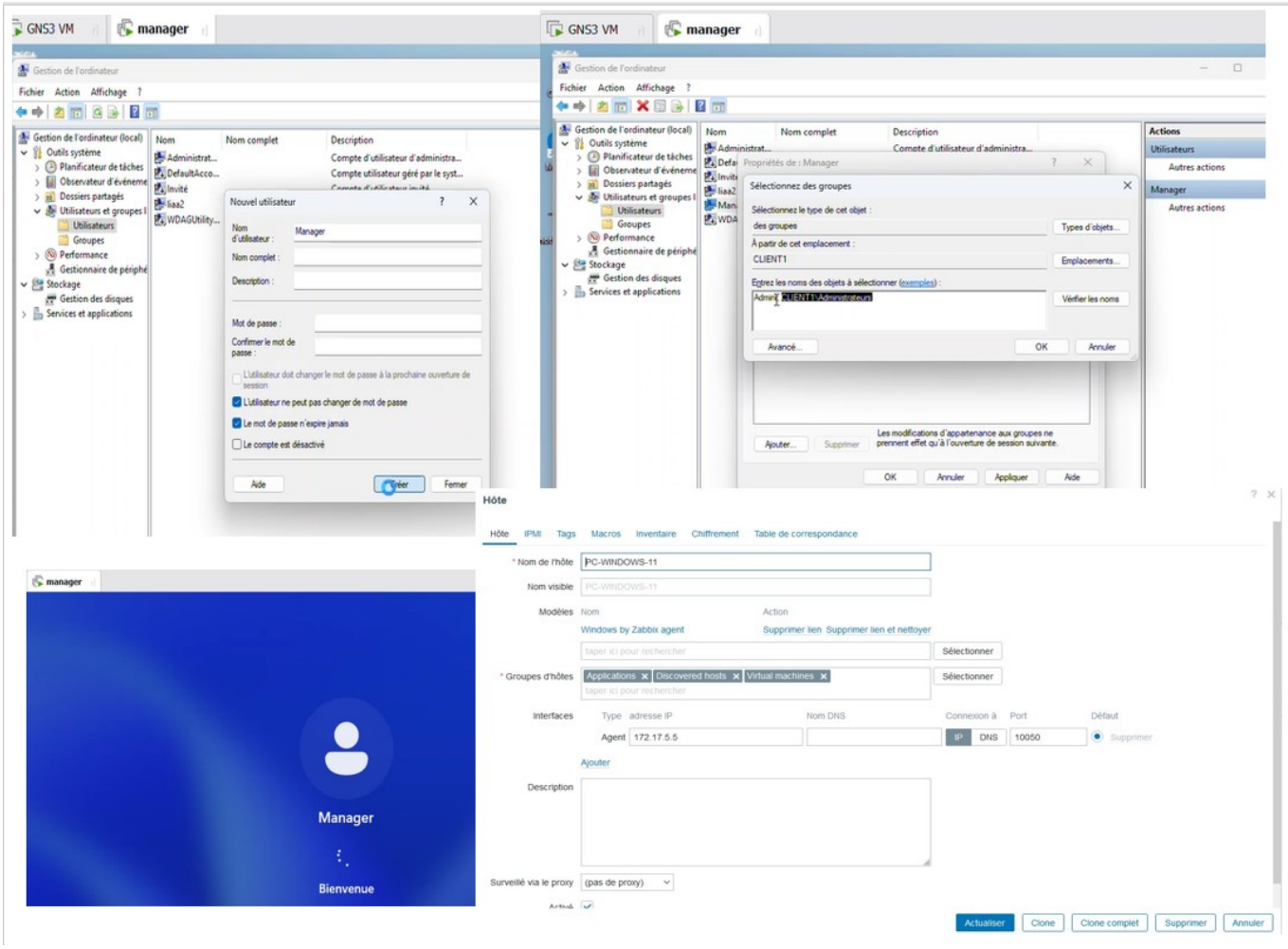


FIGURE 4.6 – Création du client manageur.

4.3.2 Installation AD+DS et la Création d'un contrôleur de Domaine

Sur la machine Windows server on a installé un contrôleur de domaine dont le nom est cevital.local. Pour commencer l'installation, il faudra ajouter le Service de Rôle Active Directory, lancer l'installation et ajouter les fonctionnalités et les rôles dont on a besoin. Une fois installé, nous commencerons à configurer notre Active Directory. D'abord il faut ajouter une nouvelle forêt appelée cevital.local, puis sélectionner le niveau fonctionnel de la nouvelle forêt Active Directory. Dans notre cas, nous avons placé un niveau de fonctionnalité de 2016. Nous allons choisir ainsi des options supplémentaires à installer comme illustré dans la figure 4.7 ;

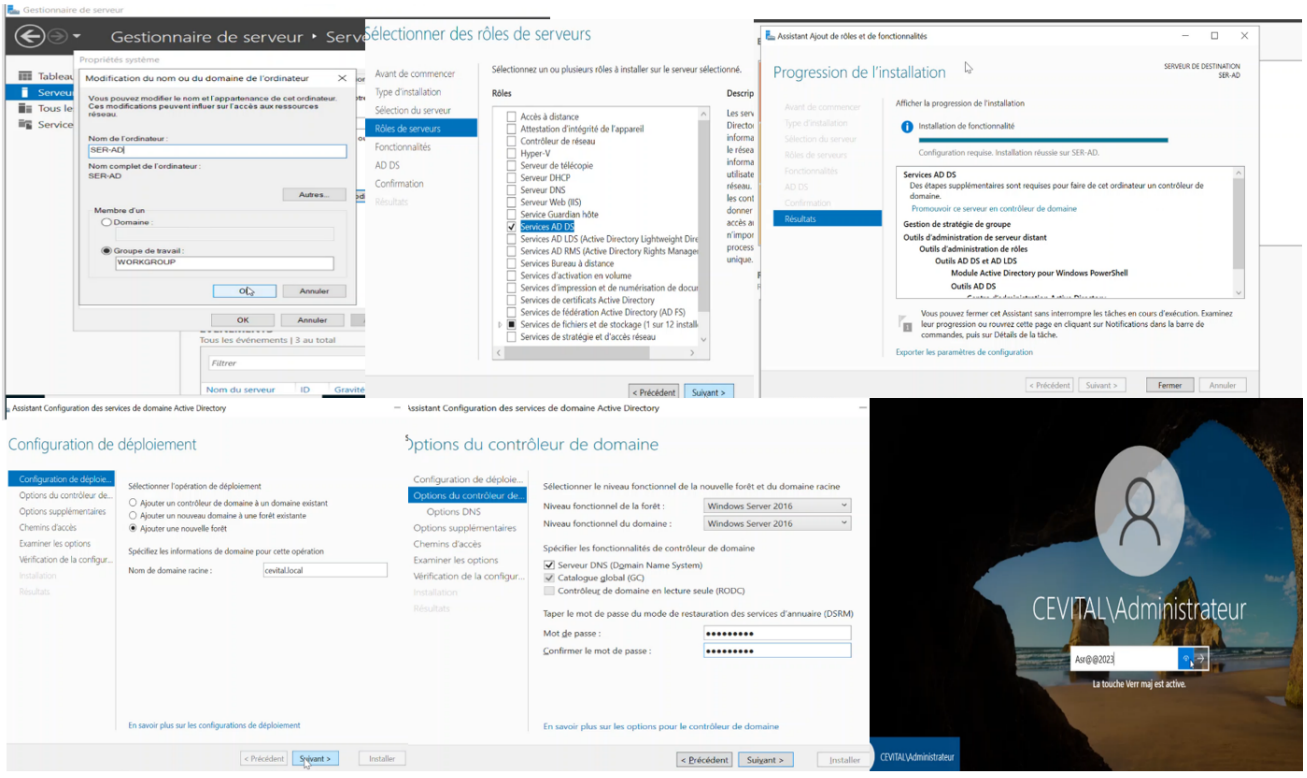


FIGURE 4.7 – Installation de l'active directory.

4.3.3 Création des Unités et des groupes d'organisation

Pour créer des comptes utilisateurs, il faut aller sur utilisateur d'abord, cliquer sur le bouton droit ''nouveau '' ensuite remplir les informations correspondantes à l'utilisateur, ainsi que le mot de passe d'ouverture de sa session et la valider ; enfin nous allons créer un pass LDAP pour la gestion des utilisateurs dans Zabbix comme illustré dans la figure 4.8 ;

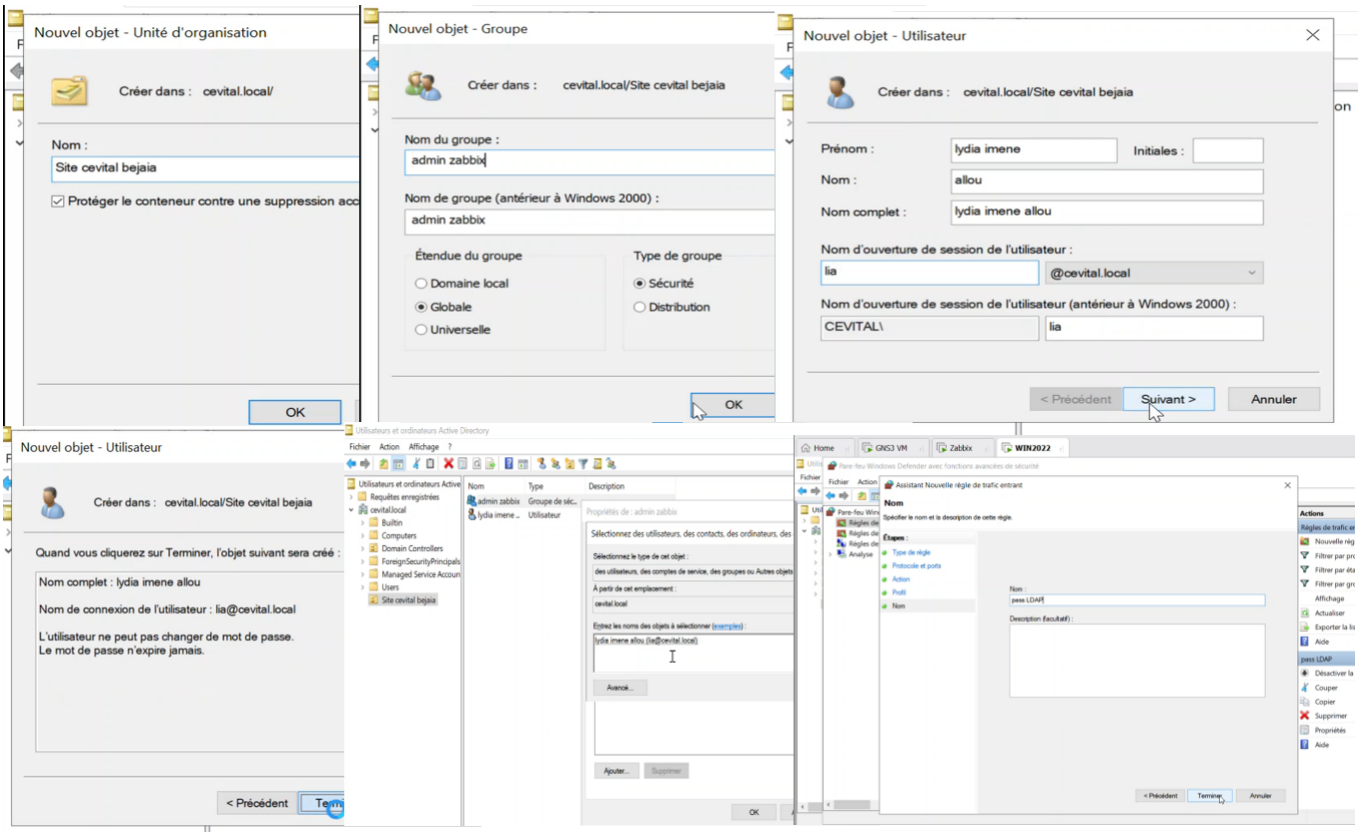


FIGURE 4.8 – Configuration des services de domaine active directory.

4.3.4 Configurations de LDAP sur l'interface Zabbix

Apres avoir créé une règle de trafic entrant qu'on a nommé pass LDAP, nous avons testé la connexion du serveur LDAP puis avons authentifié l'utilisateur qu'on a créé pour une gestion plus organisée, comme illustré dans la figure 4.9 ;

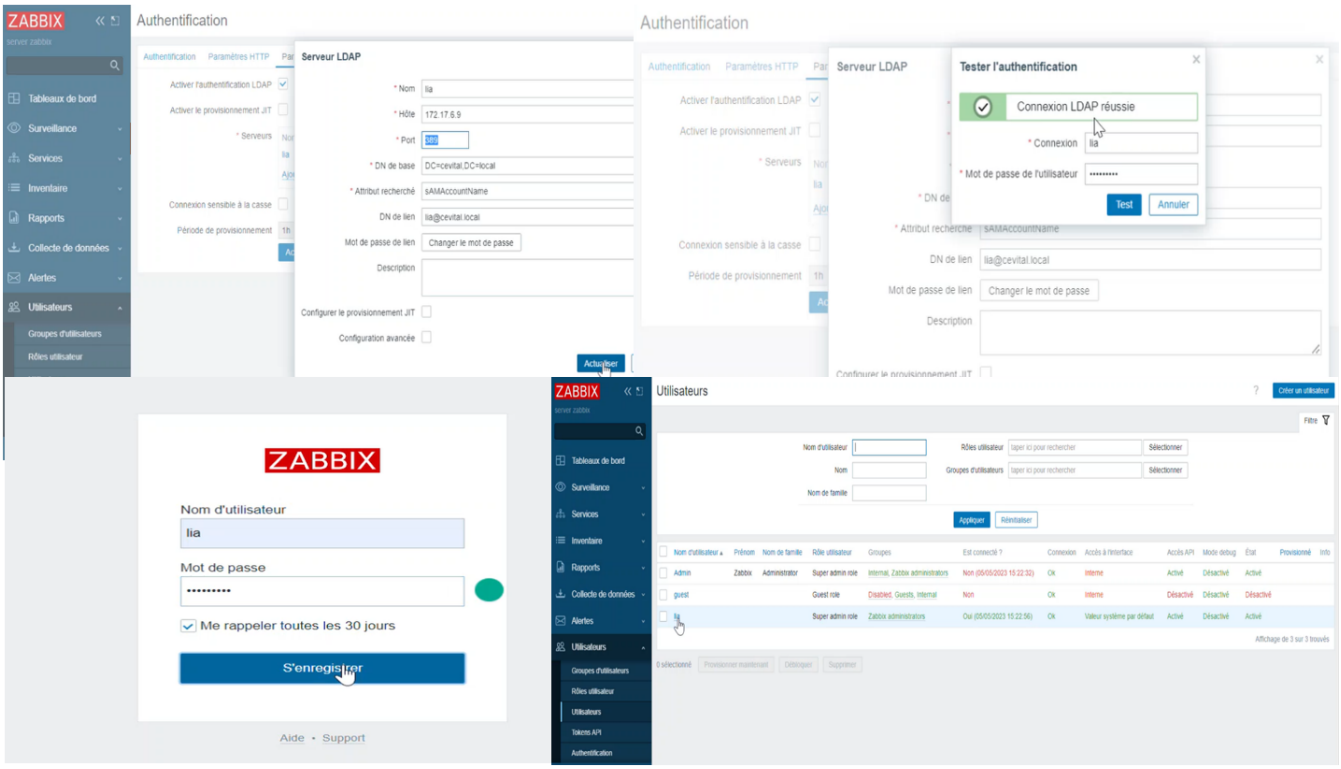


FIGURE 4.9 – Etapes de configuration LDAP sur l'interface Zabbix.

4.3.5 L'ajout et l'installation de l'agent Zabbix dans Windows-Serveur et le configurer comme hôte dans l'interface Zabbix

L'agent Zabbix Windows peut être installé à partir des packages d'installation Windows (32 bits ou 64 bits).

Pour l'étape de configuration de l'interface agent Zabbix, vous pouvez également utiliser les boutons ''clone'' sous la forme d'un hôte existant pour créer un nouvel hôte, et choisir plusieurs types d'interfaces hôtes qui sont : Agent Zabbix ou SNMP. Cliquez ensuite sur Ajouter

dans le bloc Interfaces, sélectionnez le type d'interface et saisissez les informations IP/DNS, Connexion à et Port.

Les étapes d'installation de l'agent Zabbix et l'ajout de l'hôte windows-serveur sont illustrées dans la figure 4.10;

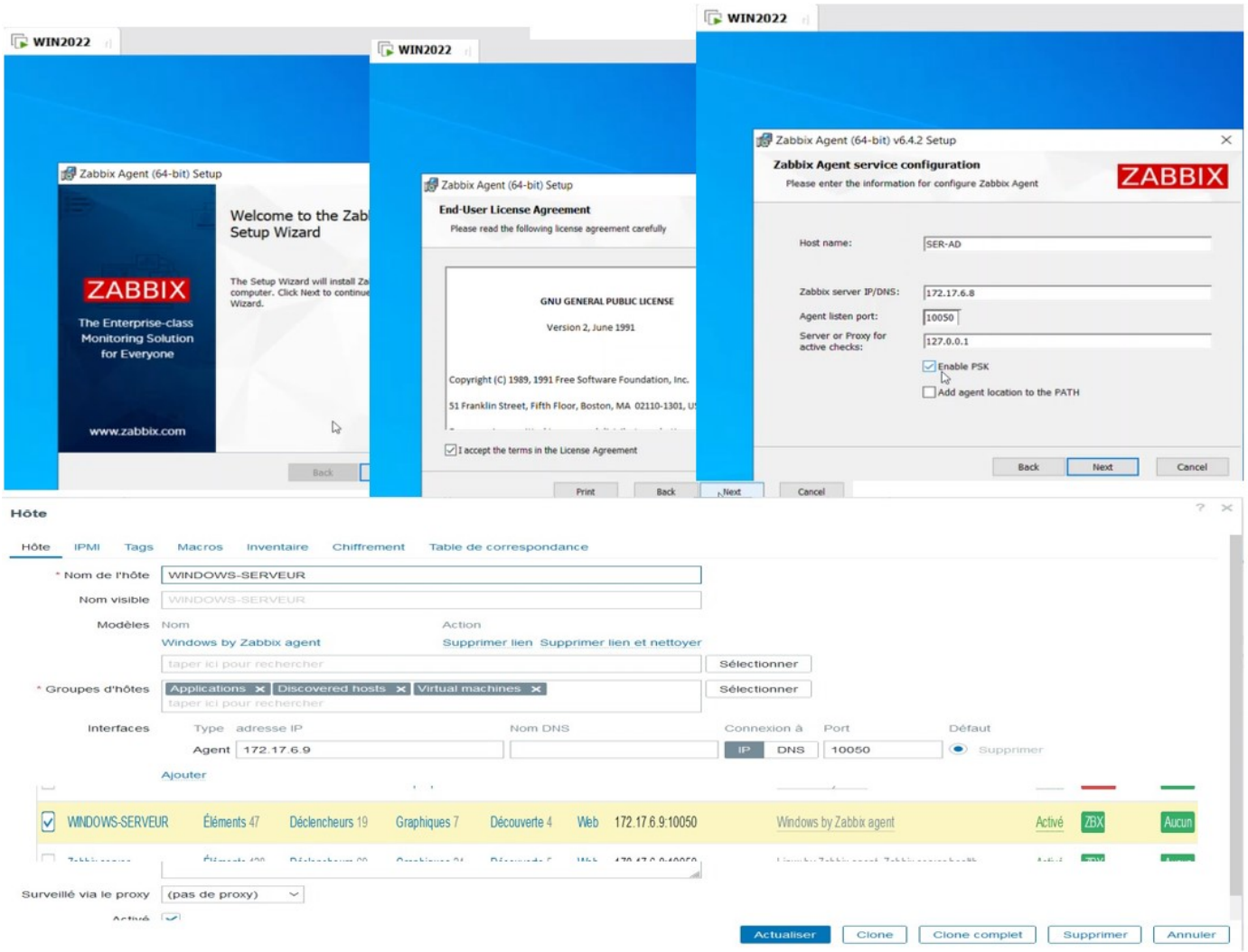


FIGURE 4.10 – Etapes d'installation de l'agent Zabbix pour Windows.

4.3.6 Importation et l'ajout d'un modèle

Pour notre exemple nous avons choisi de télécharger sur internet un modèle, ou Template en anglais, pour le pare-feu fortigate. Le fichier de configuration est en format xml pour qu'on puisse l'importer sur l'interface web de Zabbix; le but de rajouter ce modèle est de permettre le renforcement du moyen de supervision, et de détecter rapidement les problèmes qui peuvent survenir dans le réseau. Les étapes à suivre sont illustrées dans la figure 4.11 ;

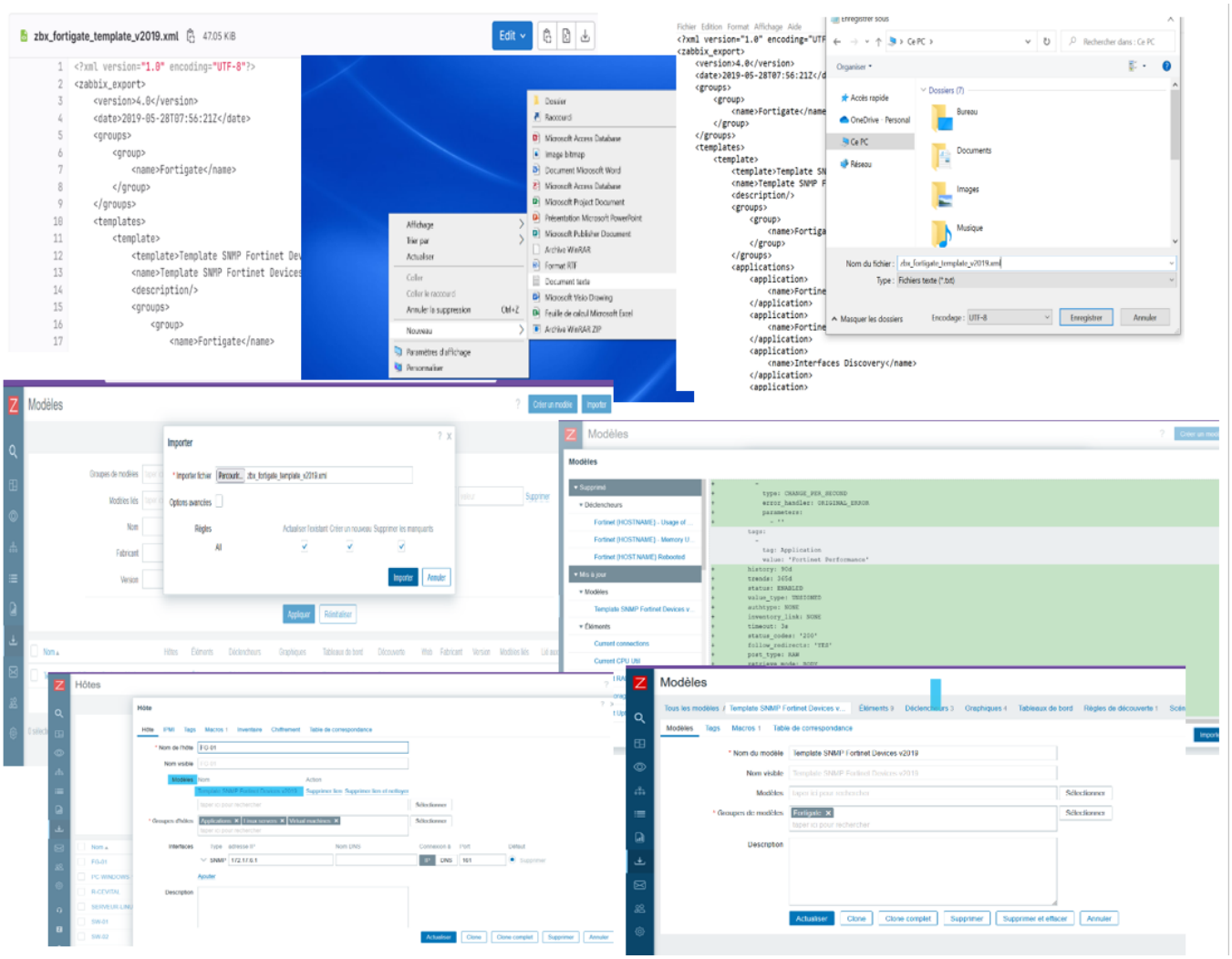


FIGURE 4.11 – Etapes de téléchargement et l'importation de la Template du pare-feu fortigate.

4.4 Personnalisation de la carte visuelle dans Zabbix

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

Les cartes sont créées et gérées dans Surveillance → Cartes, où elles peuvent être configurées, gérées et visualisées, pour cela, il suffit de cliquer sur le bouton Créer une carte, dans le coin supérieur droit.

Les icônes sont utilisées pour représenter les éléments de la carte. Vous pouvez définir les informations qui seront affichées avec les icônes et définir que les problèmes récents sont affichés d'une manière particulière.

Une fois enregistrée vous pouvez commencer à personnaliser votre console visuelle comme illustrée dans la figure 4.12 ;

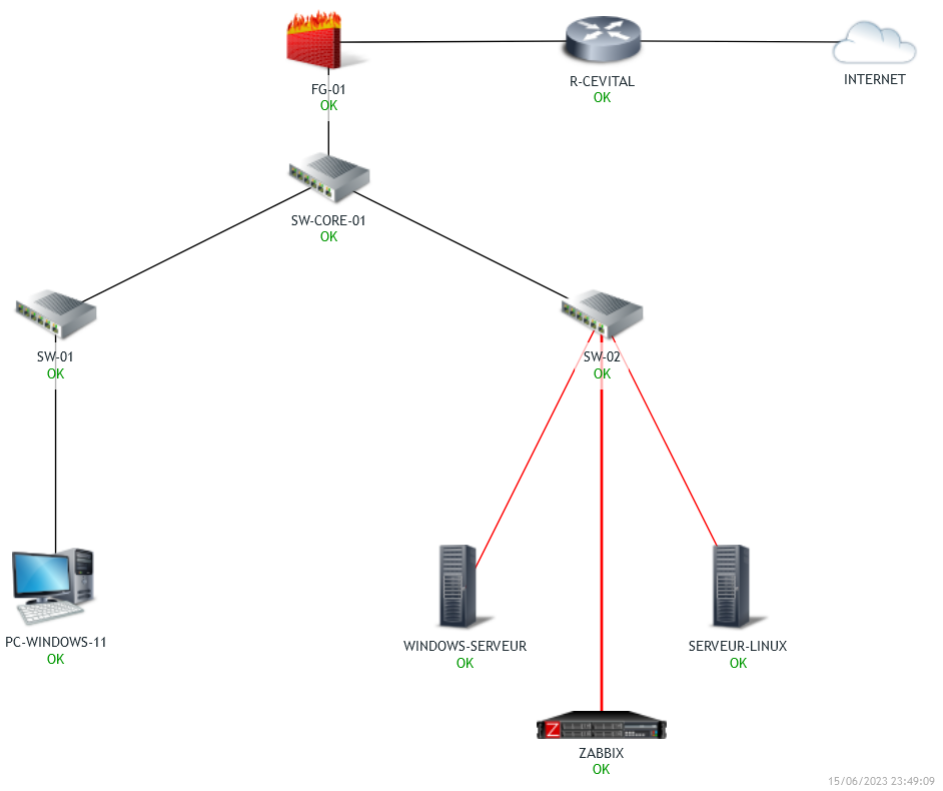


FIGURE 4.12 – Carte visuelle de Cevital sous Zabbix.

4.4.1 Visualisation des cartes

Zabbix permet de visualiser un enregistrement en temps réel de tous les événements qui se passent dans nos systèmes surveillés. Les événements sont classés en fonction de leur gravité :
Si un élément de la carte est à l'état problème, il est mis en évidence par un cercle. La couleur de remplissage du cercle correspond à la couleur de gravité du problème. Seuls les problèmes supérieurs ou égaux au niveau de gravité sélectionné seront affichés avec l'élément. Si tous les problèmes sont acquittés, une bordure verte épaisse autour du cercle est affichée.

4.5 Surveillance

4.5.1 Surveillance système et réseau

Pour assurer la surveillance de notre machine, nous allons superviser les paramètres systèmes tels que le CPU, le Traffic réseau ainsi que la mémoire afin de réaliser cette surveillance de manière efficace. Cela nous permettra de déterminer l'état du module surveillé et de diagnostiquer les éventuels problèmes en temps opportun.

Dans notre exemple illustré dans la figure 4.13 , Le module CPU, Traffic réseau et la mémoire renvoie les informations et pourcentages en usage.

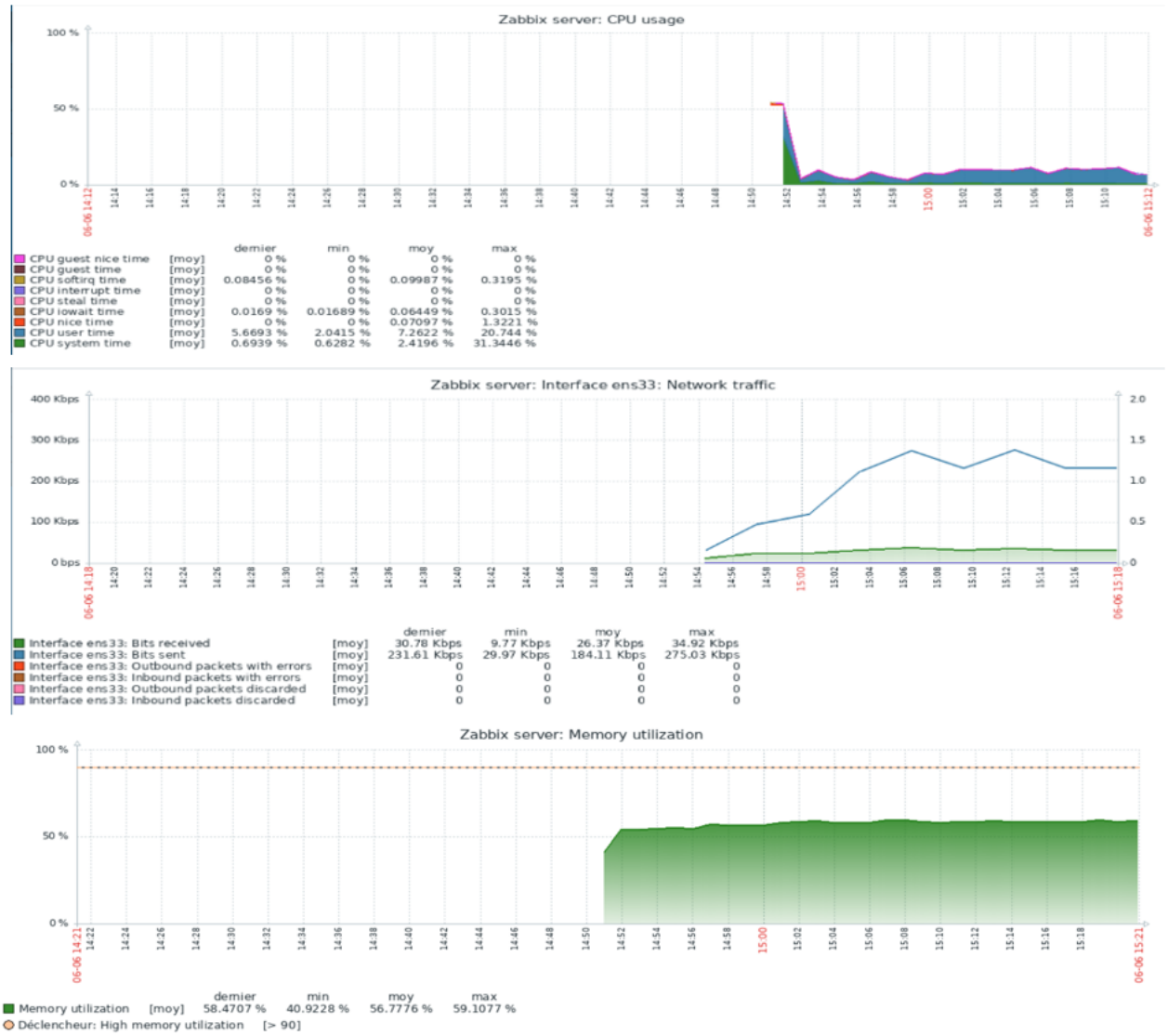


FIGURE 4.13 – Graphe des différents paramètres system de notre machine de supervision.

4.5.2 Surveillance avec SNMP

Avant de pouvoir superviser les équipements tels que les switchs et les routeurs, nous devons tout d'abord configurer le service SNMP sur chaque équipement et lui configurer la communauté SNMP. Prenons l'exemple du (SW-CORE-01), comme illustré dans la figure 4.14 ;

```
SW-CORE-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CORE-01(config)#snmp-server community SW-CORE-01 RO
SW-CORE-01(config)#interface vlan 6
SW-CORE-01(config-if)#ip add 172.17.6.200 255.255.255.0
SW-CORE-01(config-if)#no shutdown
SW-CORE-01(config-if)#end
SW-CORE-01#
*Jun  6 22:07:36.988: %SYS-5-CONFIG_I: Configured from console by
 console
```

FIGURE 4.14 – Commandes de configuration de SNMP.

La figure 4.15 illustrée montre comment configurer le protocole SNMP, au niveau de l'interface web du pare-feu (FG-01) en l'activant et en lui créant une communauté.

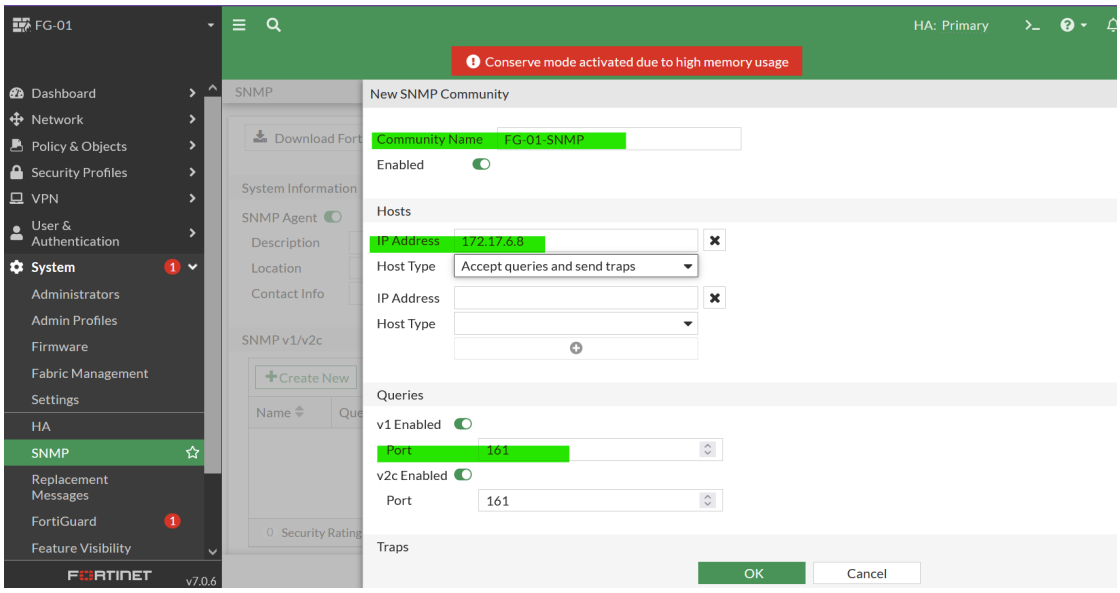
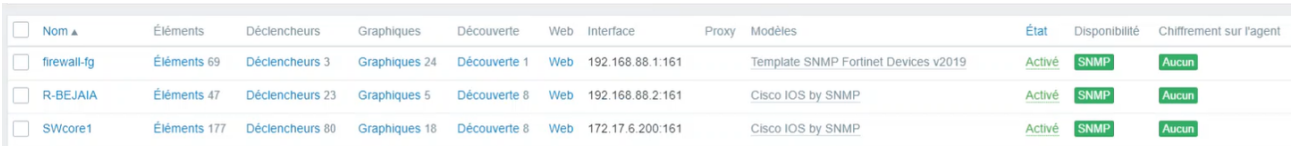


FIGURE 4.15 – Configuration du protocole SNMP sur le FG-01 et la création de sa communauté.

Dans cette étape on peut désormais afficher les différents hôtes auxquels le protocole SNMP a été configuré, tel que dans le SW-CORE-01, le Routeur ou le pare-feu. Les boutons affichés en vert veulent dire qu'il est activé, comme l'illustre la figure 4.16 ;



Nom ▲	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement sur l'agent
firewall-fg	Éléments 69	Déclencheurs 3	Graphiques 24	Découverte 1	Web	192.168.88.1:161		Template SNMP Fortinet Devices v2019	Activé	SNMP	Aucun
R-BEJAIA	Éléments 47	Déclencheurs 23	Graphiques 5	Découverte 8	Web	192.168.88.2:161		Cisco IOS by SNMP	Activé	SNMP	Aucun
SWcore1	Éléments 177	Déclencheurs 80	Graphiques 18	Découverte 8	Web	172.17.6.200:161		Cisco IOS by SNMP	Activé	SNMP	Aucun

FIGURE 4.16 – La liste des hôtes bénéficiant du protocole SNMP.

4.6 La configuration des alertes par courriel

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

Pour configurer l'e-mail comme type de média (les médias sont les canaux de diffusion utilisés pour envoyer des notifications et des alertes depuis Zabbix) : Accédez à Alertes → Types de médias. Cliquez sur Créer un type de média. Ce dernier contient les attributs généraux qu'il faut remplir obligatoirement comme illustré dans la figure 4.17 ;

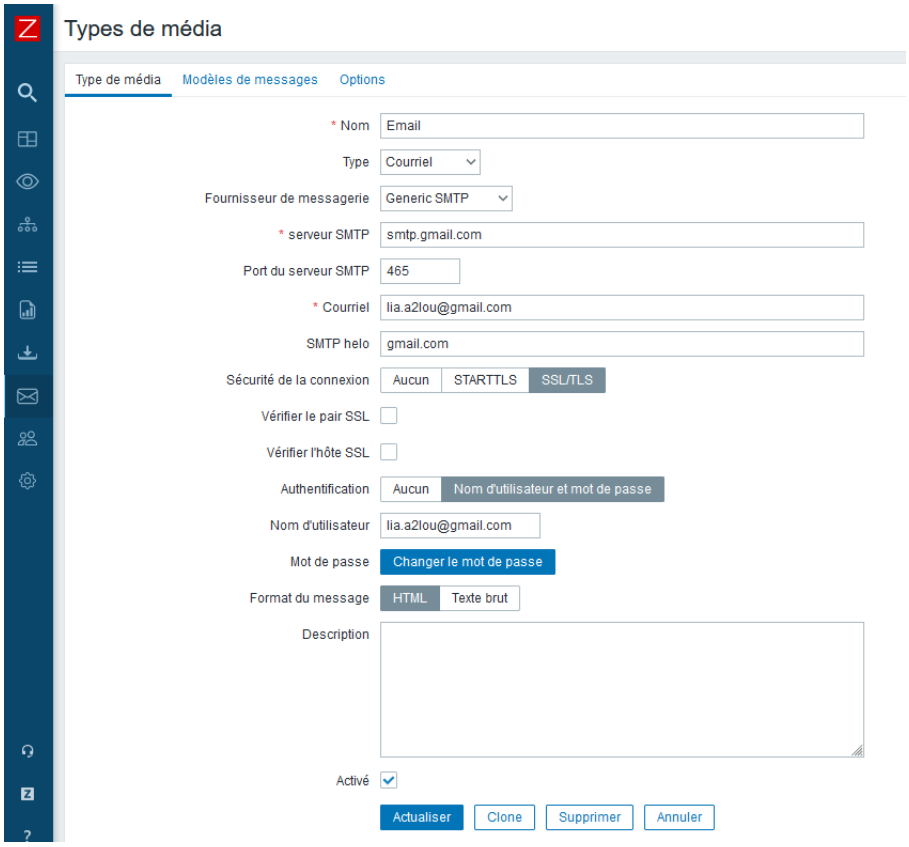


FIGURE 4.17 – Configuration l'e-mail comme type de média

Enfin, pour tester si un type de média, par exemple e-mail une fois configuré, fonctionne correctement, un message de réussite ou d'échec du test s'affiche dans la fenêtre comme illustré dans la figure 4.18 ;

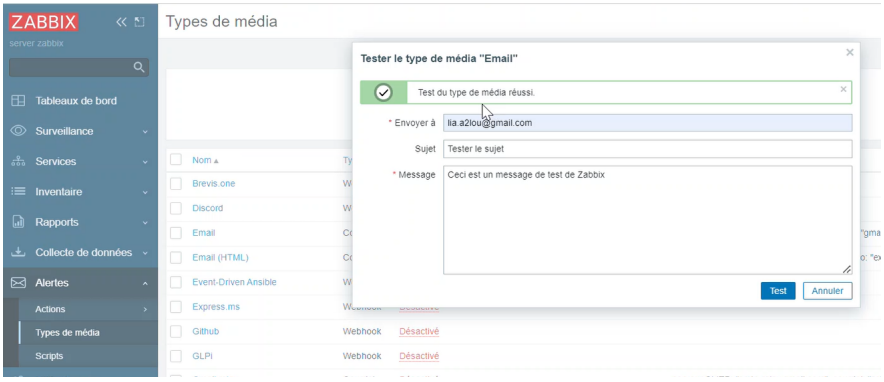


FIGURE 4.18 – Test de type de support.

Pour définir un média utilisateur et recevoir les notifications : Allez dans Administration → Utilisateurs et ouvrez le formulaire des propriétés de l'utilisateur → Dans l'onglet Média, cliquez sur ajouter comme illustré dans la figure 4.19 ;

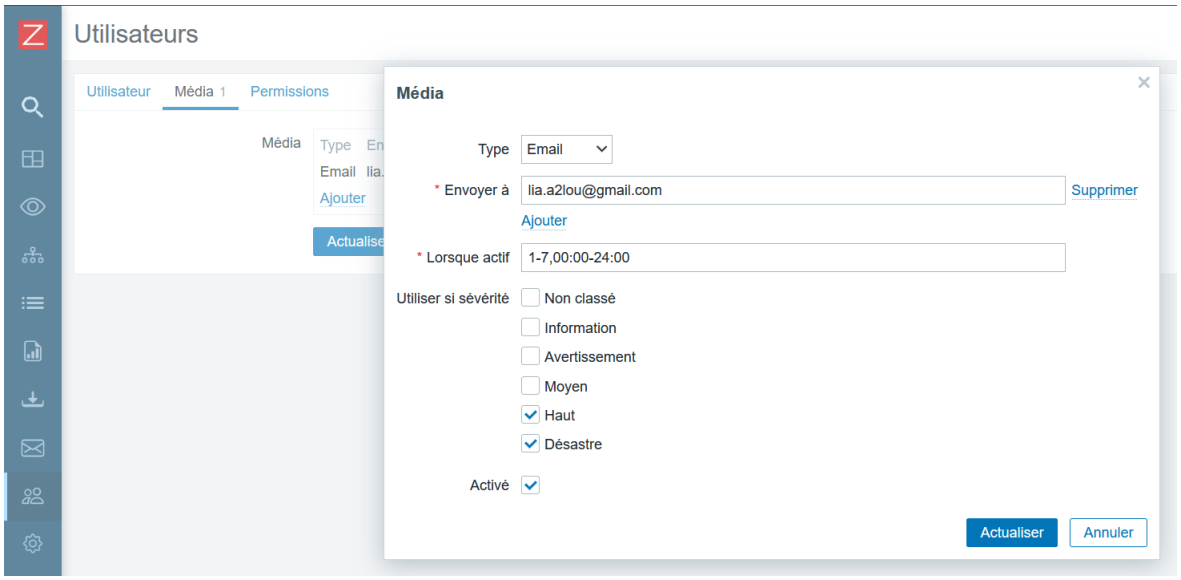


FIGURE 4.19 – Définir un média utilisateur.

Après l'enregistrement, les sévérités de déclenchement sélectionnées seront affichées dans les couleurs de sévérité correspondantes, tandis que celles non sélectionnées seront grisées comme illustré dans la figure 4.20 ;

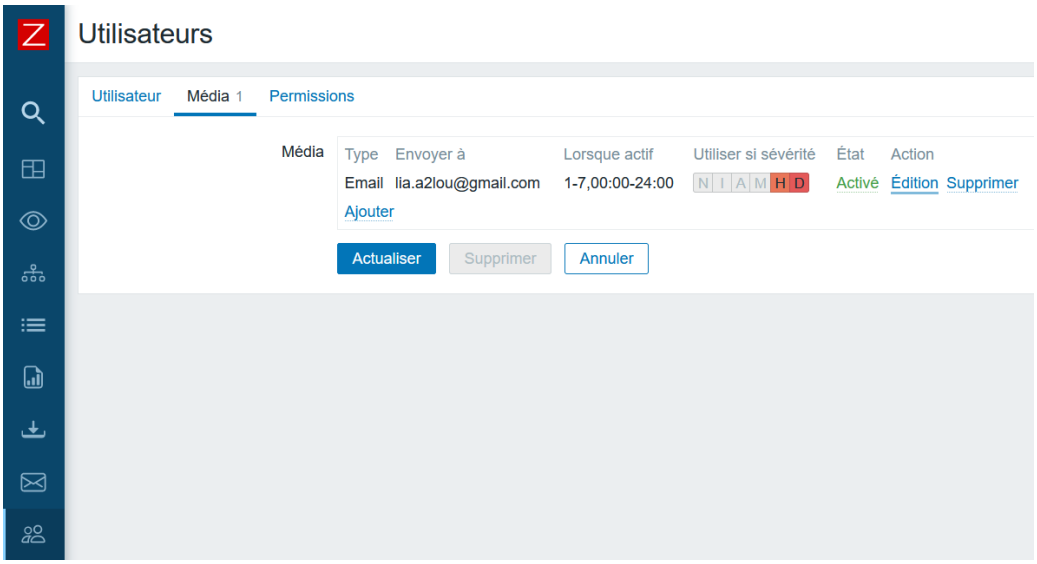


FIGURE 4.20 – Affichage des sévérités de déclenchement sélectionnées avec leur couleur

Conclusion

Dans ce chapitre, nous nous sommes focalisés sur l'aspect pratique de notre projet, tout en détaillant les étapes de mise en place et l'utilité de notre solution. Tout d'abord, nous avons modélisé notre politique de supervision pour mieux comprendre le fonctionnement de notre système, par la suite, nous avons reproduit le réseau LAN de Cevital sous GNS3 pour le superviser et enfin, nous avons décrit l'implémentation de certaines fonctionnalités de Zabbix.

Conclusion générale

Nous avons travaillé pour mettre en place une solution de supervision informatique au sein de Cevital à Bejaia. Ce projet m'a permis d'améliorer mes compétences en administration et sécurité des réseaux, et de me familiariser avec le monde professionnel lors de mon stage dans l'entreprise.

Pour atteindre notre objectif, nous avons d'abord effectué une étude approfondie de l'architecture réseau de l'entreprise. Nous avons posé la problématique et envisagé différentes solutions. Ensuite, nous avons analysé plusieurs outils de supervision, les présentant et évaluant les avantages et les inconvénients de chacun. Nous avons réalisé une comparaison entre ces outils open source, et c'est sur cette base que nous avons choisi notre solution, ZABBIX. Nous l'avons ensuite présentée en détaillant ses fonctionnalités et son architecture. Enfin, nous l'avons installée et configurée sur un serveur de virtualisation sous Linux. Cette mise en œuvre nous a permis d'appréhender les nombreuses possibilités offertes par ZABBIX.

La réalisation de ce projet a été bénéfique et fructueuse pour moi, car elle m'a permis d'approfondir mes connaissances et d'en acquérir de nouvelles. Ces deux aspects sont essentiels pour continuer à progresser.

Bibliographie

[1] YAZID, M. Cours et Travaux Pratiques, Administration des Réseaux, page 4,5, Bejaia, 2022,2023. (Consulté le 02/03/2023).

[2] Cisco certification ccna1 : Introduction aux réseaux. « Chapitre 15 : Couche application, section 15.2 Poste à pair, rubrique 15.2.1 Modèle client-serveur ». (Consulté le 04/03/2023).

[3] Cisco certification ccna1 : Introduction aux réseaux. Chapitre 15 : Couche application, section 15.2 Poste à pair, rubrique 15.2.2 réseaux Peer to Peer. (Consulté le 04/03/2023).

[4] GOUPILLE, P.-A. « Technologie des ordinateurs et des réseaux : Cours et exercices corrigés », page 326,327,328, 8 -ème Ed. Dunod, Paris, 2008. (Consulté le 04/03/2023).

[5] YAZID, M. Cours et Travaux Pratiques, Administration des Réseaux, page 10, Bejaia, 2022,2023. (Consulté le 02/03/2023).

[6] Cisco certification ccna1 : Introduction aux réseaux. Chapitre 3 : Modèles et protocoles, section 3.5 Modèles de référence, rubrique 3.5.2 Modèle de référence OSI. (Consulté le 14/03/2023).

[7] Cisco certification ccna1 : Introduction aux réseaux. Chapitre 3 : Modèles et protocoles, section 3.5 Modèles de référence, rubrique 3.5.3 Modèle de référence TCP/IP. (Consulté le 14/03/2023).

[8] Cisco certification ccna1 : Introduction aux réseaux. Chapitre 3 : Modèles et protocoles, section 3.2 Modèles de référence, rubrique 3.2.3 Interaction entre les protocoles. (Consulté le 14/03/2023).

[9] Santos, H.-A. Et Jérémias, S.-C. mémoire de fin d'étude sur le thème Conception et réalisation d'une applica-tion de surveillance réseau basée sur SNMP, université de Tizi Ouzou, 2013. (Consulté le 27/03/2023).

[10] SERVIN, C. Réseaux et télécoms, 4 -ème Ed. DUNOD, Paris, page 676,677, 2013. (Consulté le 28/03/2023).

[11] DJENNANE, L. et KASSA, R. Etude et proposition d'une solution de supervision réseau basée sur Pandora FMS au profit de l'EPB. Mémoire master, université de Bejaia, page 32,33,39. 2020. (consulté le 29/03/2023).

[12] SEUS Max Bruno, Mise en place d'une solution de surveillance permettant de superviser les bases de données, RAPPORT DE STAGE MASTER 2 INFORMATIQUE, Université de la Réunion, page14, 2014. (consulté le 30/03/2023).

[13] HOUACINE, Y. Et DJALI, L. Mise en place d'un outil de supervision dans un réseau d'entreprise. Cas d'étude : OPGI. Mémoire master, université de Bejaia ,2020. (Consulté le 30/03/2023).

[14] YAZID, M. Cours et Travaux Pratiques, Administration des Réseaux, page 37.38.39.40. 2022,2023, Bejaia (consulté le 31/03/2023).

[15] GOUPILLE, P.-A. Technologie des ordinateurs et des réseaux : Cours et exercices corrigés, 8 -ème Ed. Dunod, Paris, page 473 2008. (Consulté le 31/03/2023).

[16] PUJOLLE, G, « Les Réseaux », 6ème édition, EYROLLES, 2008. (consulté le 31/03/2023).

[17] GOUPILLE, P.-A. Technologie des ordinateurs et des réseaux : Cours et exercices corrigés, page 472, 8 -ème Ed. Dunod, Paris, 2008. (Consulté le 31/03/2023).

[18] http ://www.zabbix.com/. (Consulté le 02/04/2023).

[19] http ://www.nagios.org/. (Consulté le 03/04/2023).

[20] www.centreon.com. (consulté le 04/04/2023).

Annexe A

Questionnaire entreprise Cevital

1. Quel est le type de votre architecture (client-serveur ou post à post) ?

2. Quelle est la topologie physique de votre entreprise (hiérarchique ou étoile) ?

3. Quelle est l'architecture réseau de votre entreprise ?

4. Disposez-vous d'un réseau local ?

   ☐ Oui

   ☐ Non

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

   ☐ Oui

   ☐ Non

6. Citez les systèmes d'exploitation que vous utilisez ?

   ☐ Oui

   ☐ Non

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

   ☐ Oui

   ☐ Non

8. Quels sont les différents VLAN que vous avez ?

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

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

    ☐ Oui

    ☐ Non

    Si oui, indiquez lequel, et quels sont les équipements et les services à superviser ?

11. Quels sont les politiques de sécurité qu'utilise votre entreprise ?

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

    ☐ Oui

    ☐ Non

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

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

    ☐ Oui

    ☐ Non

    Si oui, quel est le type du pare-feu utilisé ?

14. Utilisez-vous IPS dans votre pare-feu, pour les détection et prévention contre les intrusions ?

    ☐ Oui

    ☐ Non

15. Les sites distants de votre entreprise sont (multisites ou unique) ?

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

    ☐ Oui

    ☐ Non

    Si oui, lesquelles ?

17. Quels sont les équipements d'interconnexion et réseau (serveur, switch, routeur, pare-feu ...) dont dispose votre entreprise ? quel est leur systeme d'exploitation et version ?

18. Disposez-vous d'un réseau physique ou virtuel ?

Annexe B

Configuration sous GNS3

B.1 Présentation de l'outil de simulation GNS3

GNS3 « Graphical Network Simulator 3 » est un simulateur de réseau graphique qui fonctionne sous Windows, Linux et Mac OS X. Cet outil simple et intuitif permet de créer des réseaux, les simuler, les configurer, les tester et les dépanner. Le simulateur GNS3 permet en effet de connecter également l'hyper viseur de machines virtuelles depuis Vmware.

FIGURE 1 – Logo GNS3

B.2 Configuration des équipements

1. Pour configurer les noms des équipements, il suffit de suivre les étapes illustrées dans la figure ci-dessous

```
R-CEVITAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R-CEVITAL(config)#hostname R-CEVITAL
R-CEVITAL(config)#
```

FIGURE 2 – Commande de configuration du nom d'un équipement (R-CEVITAL)

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FG-01

FortiGate-VM64-KVM (global) # end

FG-01 #
```

FIGURE 3 – Commande de configuration du nom d'un équipement (FG-01)

2. Pour configurer le mot de passe pour le mode privilégie, la ligne console et virtuelle (Telnet et SSH) pour chaque équipement, il suffit de suivre les étapes illustrées dans la figure ci-dessous

```
R-CEVITAL(config)#username admin password cevital
R-CEVITAL(config)#enable secret cisco
R-CEVITAL(config)#line console 0
R-CEVITAL(config-line)#login local
R-CEVITAL(config-line)#exit
R-CEVITAL(config)#ip domain-name cevital.com
R-CEVITAL(config)#crypto key generate rsa
The name for the keys will be: R-CEVITAL.cevital.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R-CEVITAL(config)#
*May 27 23:38:52.413: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-CEVITAL(config)#ip ssh version 2
R-CEVITAL(config)#line vty 0 4
R-CEVITAL(config-line)#login local
R-CEVITAL(config-line)#transport input telnet ssh
R-CEVITAL(config-line)#
```

FIGURE 4 – Commandes de configuration des différents mots de passe.

3. Pour configurer la bannière de connexion pour chaque équipement, il suffit de suivre les étapes illustrées dans la figure ci-dessous ;

```
R-CEVITAL(config)#banner login "ACCES INTERDIT A TOUTE PERSONNE NON AUTORISEE"
```

FIGURE 5 – Commande de configuration de la bannière de connexion.

4. Pour créer des VLANs sur le SW-CORE, précéder comme illustré dans la figure ci-dessous ;

```
SW-CORE-01#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW-CORE-01(vlan)#vlan 5 name DSI
VLAN 5 modified:
    Name: DSI
SW-CORE-01(vlan)#vlan 6 name DATA-CENTER
VLAN 6 added:
    Name: DATA-CENTER
SW-CORE-01(vlan)#vlan 7 name MANAGEUR
VLAN 7 added:
    Name: MANAGEUR
SW-CORE-01(vlan)#vlan 66 name native
VLAN 66 added:
    Name: native
SW-CORE-01(vlan)#
```

FIGURE 6 – Commande de création des VLANs sur le SW-CORE.

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

```
SW-CORE-01#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
5    DSI                              active
6    DATA-CENTER                      active
7    MANAGEUR                         active
66   native                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
66   enet  100066     1500  -      -      -        -    -        0      0
 --More--
```

FIGURE 7 – Commande d'affichage des VLANs crées.

6. Pour configurer le SW-CORE-01 en mode vtp server pruging (voir figure) et le SW-CORE-02 en mode vtp sans pruging (voir figure) et les autres switchs en mode vtp client (voir figure) et afficher sa configuration avec la commande 'show vtp status', il suffit de procéder comme illustré dans la figure ci-dessous ;

```
SW-CORE-01(config)#vtp mode server
Device mode already VTP Server for VLANS.
SW-CORE-01(config)#vtp domain cevital.vtp
Changing VTP domain name from NULL to cevital.vtp
SW-CORE-01(config)#vtp password cevital123
Setting device VTP password to cevital123
SW-CORE-01(config)#vtp version 2
SW-CORE-01(config)#vtp pruning
Pruning switched on
```

FIGURE 8 – Commandes de configuration du switch core 1 en mode vtp server pruning.

```
SW-CORE-02(config)#vtp mode server
Device mode already VTP Server for VLANS.
SW-CORE-02(config)#vtp domain cevital.vtp
Domain name already set to cevital.vtp.
SW-CORE-02(config)#vtp password cevital123
Password already set to cevital123
SW-CORE-02(config)#vtp version 2
VTP version is already in V2.
```

FIGURE 9 – Commandes de configuration du switch core 2 en mode vtp server.

```
SW-01(config)#vtp mode client
Device mode already VTP Client for VLANS.
SW-01(config)#vtp domain cevital.vtp
Domain name already set to cevital.vtp.
SW-01(config)#vtp password cevital123
Password already set to cevital123
SW-01(config)#vtp version 2
```

FIGURE 10 – Commandes de configuration du switch 1 en mode vtp client.

la figure ci-dessous illustre la commande d'affichage de la configuration vtp sur le SW-CORE 1 ;

```
SW-01#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : cevital.vtp
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0500
Configuration last modified by 0.0.0.0 at 5-28-23 14:51:31

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 12
Configuration Revision            : 9
MD5 digest                        : 0xC1 0xF3 0xF6 0x45 0xF2 0x65 0xF8 0xE9
                                    0x78 0xE4 0x60 0x5B 0x6F 0xCE 0x8A 0xDF
SW-01#
```

FIGURE 11 – CCommande d'affichage de la configuration vtp sur le SW-CORE 1.

7. Pour configurer les interfaces en mode trunk entre des commutateurs ou entre un commutateur et un routeur, il suffit de procéder comme illustré dans la figure ci-dessous

```
SW-CORE-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CORE-01(config)#interface range ethernet 0/0-3
SW-CORE-01(config-if-range)#switchport trunk encapsulation dot1q
SW-CORE-01(config-if-range)#switchport mode trunk
SW-CORE-01(config-if-range)#no shutdown
SW-CORE-01(config-if-range)#
```

FIGURE 12 – Commandes de configuration d'une interface en mode trunk (SW-Core-01).

8. Pour configurer les interfaces en mode Access entre un commutateur et un poste client, il suffit de procéder comme illustré dans la figure ci-dessous ;

```
SW-01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-01(config)#interface range ethernet 0/0-1
SW-01(config-if-range)#switchport mode access
SW-01(config-if-range)#switchport access vlan 5
SW-01(config-if-range)#end
SW-01#
```

FIGURE 13 – Commandes de configuration d'une interface en mode access (SW-01).

9. Pour configurer les interfaces du routeur R-CEVITAL, procéder comme illustré dans la figure ci-dessous;

```
R-CEVITAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R-CEVITAL(config)#interface ethernet 0/0
R-CEVITAL(config-if)#ip add 192.168.88.2 255.255.255.0
```

FIGURE 14 – Commande pour la configuration de l'interface du routeur (R-CEVITAL).

10. Pour configurer l'interface d'authentification du pare-feu (FG-01) sur le port 10 pour accéder sur son interface,il suffit de procéder comme illustré dans la figure ci-dessous;

```
FG-01 # config system interface

FG-01 (interface) # edit port10

FG-01 (port10) # set mode static

FG-01 (port10) # set ip 192.168.99.10/24

FG-01 (port10) # set allowaccess ping ssh telnet https http snmp

FG-01 (port10) # end

FG-01 #
```

FIGURE 15 – Commande de configuration du FG-01

11. La figure ci-dessous représente l'interface d'accueil du pare-feu (FG-01)

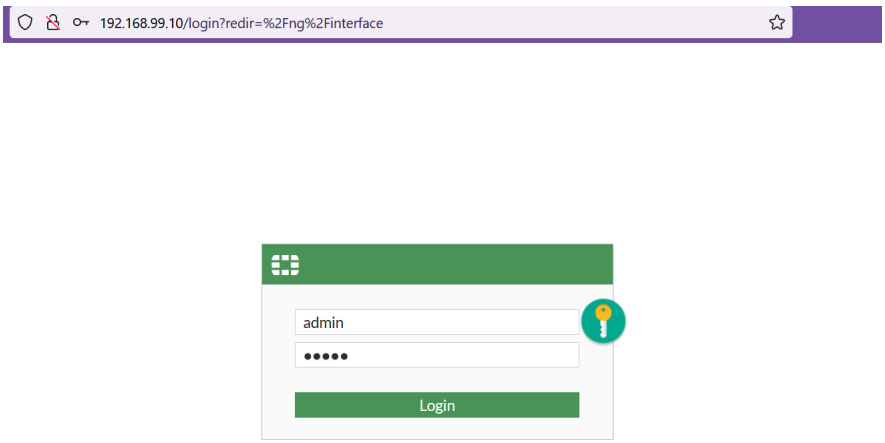


FIGURE 16 – L'interface d'accueil de FG-01.

12. Pour Configurer Etherchannel pour l'agrégation des liens soit LACP (Link Aggregation Control Protocol), sur le switch core (SW-CORE-02), procéder comme illustré dans la figure ci-dessous

```
SW-CORE-02(config)#interface range et
SW-CORE-02(config)#interface range ethernet 3/1-3
SW-CORE-02(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
```

FIGURE 17 – Commande pour activer le mode LACP du SW-CORE-02.

13. Utilisez la commande ' show etherchannel summary ' pour verifier si le port channel est actif ou non, comme illustré dans la figure ci-dessous

```
SW-CORE-02#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SD)         LACP      Et3/1(D)    Et3/2(D)    Et3/3(D)
```

FIGURE 18 – Commande pour verifier que LACP est activé.

14. Pour configurer le mode Cluster au niveau du pare-feu (FG-02), qui permet une disponibilité élevée grâce à la tolérance de panne, procéder comme illustré dans la figure ci-dessous

```
FG-02 # config system ha

FG-02 (ha) # set mode a-a

FG-02 (ha) # set group-name HD-G1

FG-02 (ha) # set password cevital123

FG-02 (ha) # set session-pickup enable

FG-02 (ha) # set hbdev port3 0 port4 0

FG-02 (ha) # set monitor port1 port2

FG-02 (ha) # end
```

FIGURE 19 – Commandes de configuration du mode cluster sur le FG-02

15. Utilisez la commande 'get system ha status' pour vérifier si le clustering est opérationnel et est connectée, comme illustré dans la figure ci-dessous

```
FG-02 # get system ha status
HA Health Status:
    WARNING: FGVMEV_RQAAJQ0A2 in conserve mode;
    WARNING: FGVMEVIWLVQND978 in conserve mode;
Model: FortiGate-VM64-KVM
Mode: HA A-A
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:30:12
Cluster state change time: 2023-05-31 16:20:46
Primary selected using:
    <2023/05/31 16:20:46> FGVMEVIWLVQND978 is selected as the primary because its overr
    <2023/05/31 16:20:46> FGVMEV_RQAAJQ0A2 is selected as the primary because it's the
ses_pickup: enable, ses_pickup_delay=disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: unset
override: disable
Configuration Status:
    FGVMEV_RQAAJQ0A2(updated 5 seconds ago): in-sync
    FGVMEVIWLVQND978(updated 1 seconds ago): in-sync
System Usage stats:
    FGVMEV_RQAAJQ0A2(updated 5 seconds ago):
        sessions=2, average-cpu-user/nice/system/idle=0%/0%/2%/93%, memory=80%
    FGVMEVIWLVQND978(updated 1 seconds ago):
        sessions=4, average-cpu-user/nice/system/idle=0%/0%/0%/96%, memory=79%
HBDEV stats:
    FGVMEV_RQAAJQ0A2(updated 5 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=4641794/10133/0/0
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=4015536/9044/0/0,
    FGVMEVIWLVQND978(updated 1 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=1387279/4195/0/0,
        port4: physical/1000auto, up, rx-bytes/packets/dropped/errors=1093855/2486/0/0,
MONDEV stats:
    FGVMEV_RQAAJQ0A2(updated 5 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=28918
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=21507/288/0/0, tx
    FGVMEVIWLVQND978(updated 1 seconds ago):
        port1: physical/1000auto, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=70428
        port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=78699/1054/0/0, t
Secondary    : FG-02           , FGVMEV_RQAAJQ0A2, HA cluster index = 0
Primary      : FG-01           , FGVMEVIWLVQND978, HA cluster index = 1
number of vcluster: 1
```

FIGURE 20 – Commande pour vérifier si le cluster sur le FG-02 est activé.

16. Pour configurer le mode Clustering au niveau de l'interface du pare-feu (FG-01), qui permet une disponibilité élevée grâce à la tolérance de panne, procéder comme illustré dans la figure ci-dessous

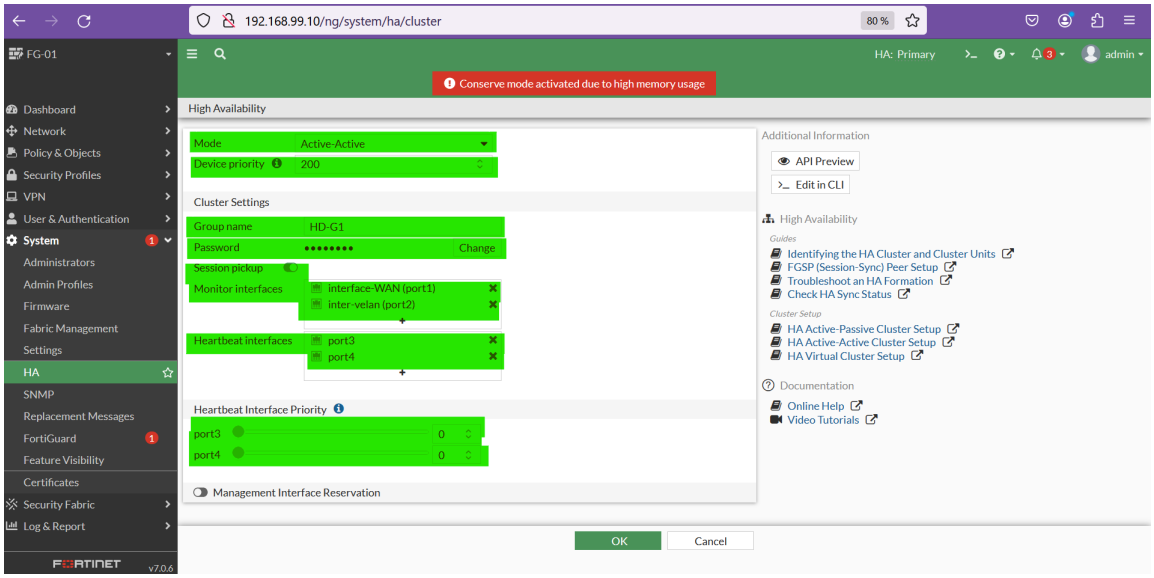


FIGURE 21 – Configuration du mode cluster au niveau du FG-01

17. Pour configurer une adresse IP de gestion sur le pare-feu (FG-02) et y accéder à distance, procéder comme illustré dans la figure ci-dessous

```
FG-02 # config system interface

FG-02 (interface) # edit port1

FG-02 (port1) # set management-ip 192.168.88.3/24

FG-02 (port1) # end
```

FIGURE 22 – Commande de configuration du management sur le FG-02

18. Pour configurer, au niveau de l'interface web du pare-feu FG-01, le routage inter VLAN sur le port 2, il faut commencer par créer des VLAN ainsi qu'une zone pour libérer le trafic intra-zone, après cela, passer à la création de l'interface WAN sur le port 1, puis créer une route statique, et enfin, terminer par la création d'une politique de sécurité comme illustré dans la figure ci-dessous

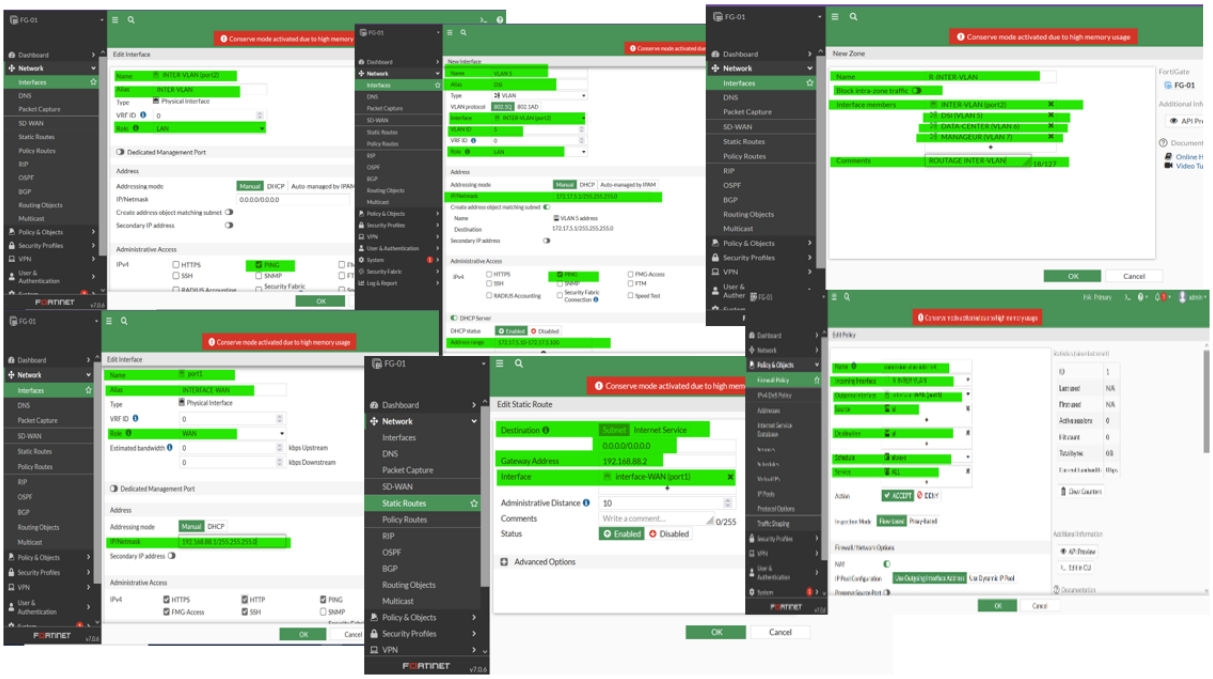


FIGURE 23 – Les étapes à suivre pour configurer le routage inter VLAN et la politique de sécurité sur l'interface web (FG-01).

19. Pour tester la connectivité entre les différents équipements, procéder comme illustré dans la figure ci-dessous

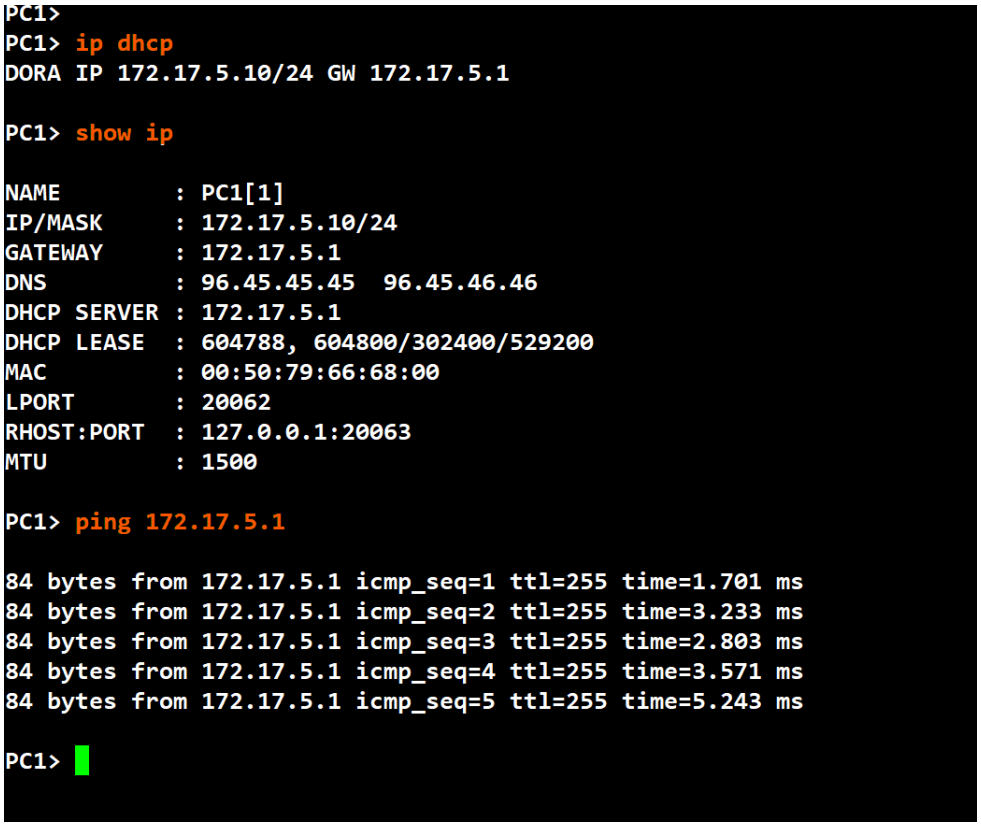


FIGURE 24 – Vérification de la connectivité.

Annexe C

Installation et configuration de Zabbix

C.1 Présentation de l'outils de simulation VMware Workstation pro

VMware Workstation est un logiciel de machine virtuelle utilisé pour exécuter plusieurs systèmes d'exploitation sur un seul ordinateur hôte physique. Chaque machine virtuelle peut exécuter simultanément une seule instance de n'importe quel système d'exploitation (Microsoft, Linux, etc.), et chacune possède : CPU, mémoire RAM, disque dur et carte réseau.

FIGURE 1 – logo VMware.

Pour bien maitriser notre outil de supervision, nous avons effectué l'installation et la configuration de Zabbix sous Debian

C.2 Les étapes d'installation de configuration de Zabbix sous Debian :

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

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

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

FIGURE 2 – Commande de mise à jour du système d'exploitation.

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

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

FIGURE 3 – Commande d'installation des dépendances et des packages requis.

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

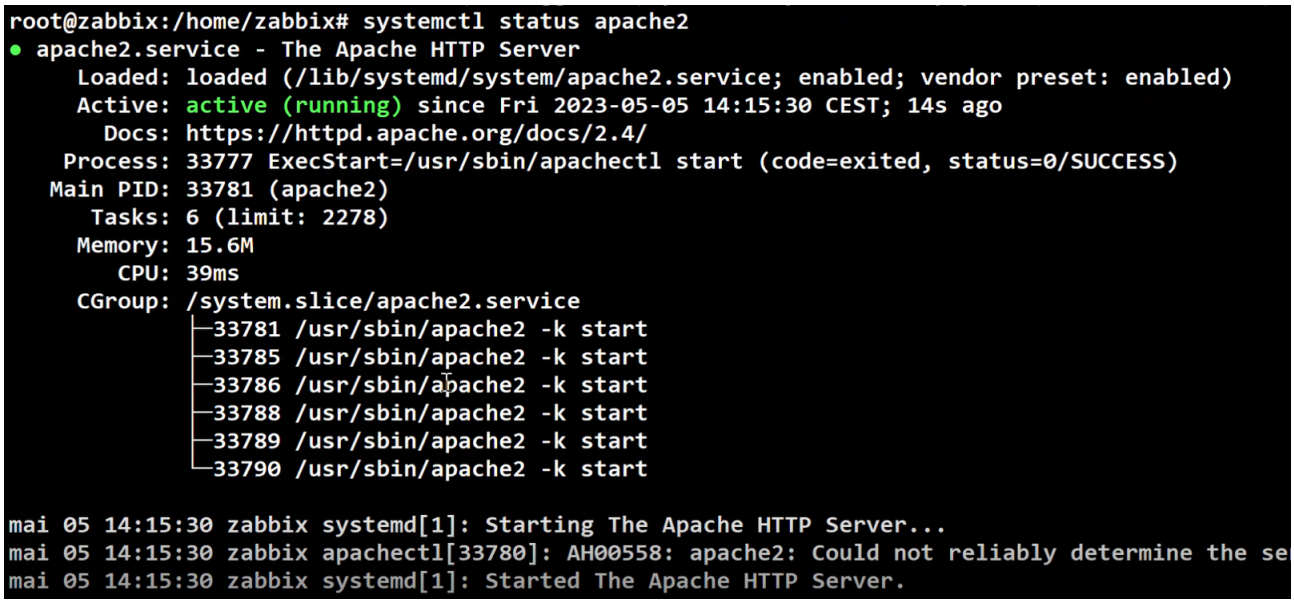


FIGURE 4 – Commande de vérification si Apache2 est en cours d'exécution

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

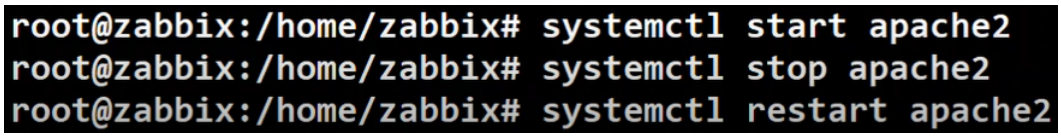


FIGURE 5 – Commande d'arrêt et de démarrage d'Apache2.

Étape 2 : Installation du serveur et du client MariaDB

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

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

FIGURE 6 – Commande d'installation de la base de données MariaDB.

2. Vérifier que le service est en cours d'exécution, comme illustré dans la figure ci-dessous ;

```
root@zabbix:/home/zabbix# systemctl status mariadb
● mariadb.service - MariaDB 10.5.19 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-05-16 11:47:59 CEST; 12min ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 575 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (c
    Process: 605 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (
    Process: 622 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=
    Process: 883 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION
    Process: 885 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 710 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 41 (limit: 2264)
     Memory: 212.6M
        CPU: 8.972s
     CGroup: /system.slice/mariadb.service
             └─710 /usr/sbin/mariadbd
```

FIGURE 7 – Commande de vérification si MariaDB est activée.

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

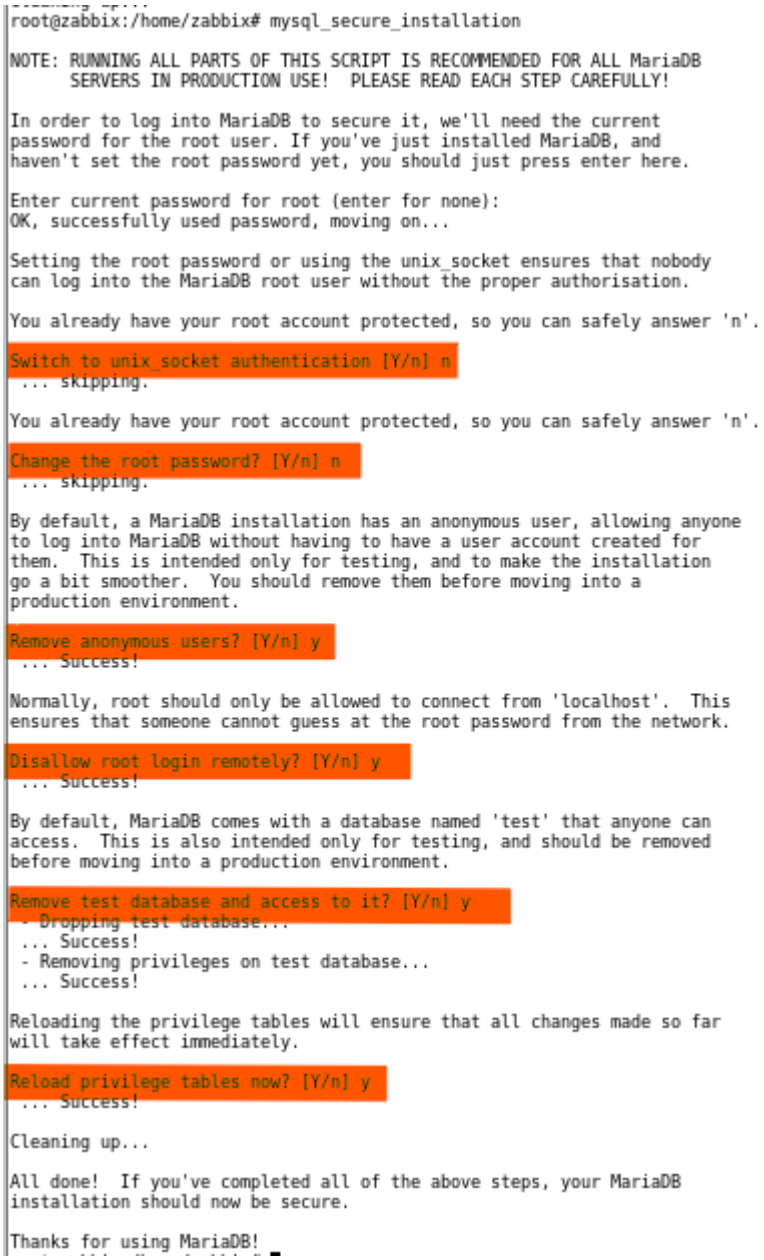


FIGURE 8 – Commande de sécurisation de MariaDB.

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

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

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

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

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

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

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

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

FIGURE 9 – Commande de configuration de la base de données MariaDB.

Étape 3 : Installation de Zabbix sous Debian

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

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

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

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

FIGURE 10 – Commandes de téléchargement des packages DEB du serveur Zabbix.

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

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

FIGURE 11 – Commande d'installation des packages DEB du serveur Zabbix.

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

```
root@zabbix:/home/zabbix# apt update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Réception de :2 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye InRelease [4 927 B]
Réception de :3 https://repo.zabbix.com/zabbix/6.3/debian bullseye InRelease [4 933 B]
Réception de :4 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye/main Sources [1 001 B]
Réception de :5 https://repo.zabbix.com/zabbix-agent2-plugins/1/debian bullseye/main amd64 Packages [621
B]
Réception de :6 https://repo.zabbix.com/zabbix/6.3/debian bullseye/main Sources [1 952 B]
Réception de :7 https://repo.zabbix.com/zabbix/6.3/debian bullseye/main amd64 Packages [5 500 B]
Atteint :8 http://deb.debian.org/debian bullseye InRelease
Atteint :9 http://deb.debian.org/debian bullseye-updates InRelease
18,9 ko réceptionnés en 21s (883 o/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
```

FIGURE 12 – Commande de mise à jour des packages DEB du serveur Zabbix.

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

```
root@zabbix:/home/zabbix# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-s
ql-scripts zabbix-agent
```

FIGURE 13 – Commande d'installation du serveur Zabbix.

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

```
root@zabbix:/home/zabbix# zcat  /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-chara
cter-set=utf8mb4 -uzabbix -p'mypassword' zabbix
```

FIGURE 14 – Commande permettant d'apporter des modifications au serveur Zabbix.

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

```
root@zabbix:/home/zabbix# nano /etc/zabbix/zabbix_server.conf
```

FIGURE 15 – Commande permettant d'ouvrir le fichier de configuration du serveur Zabbix.

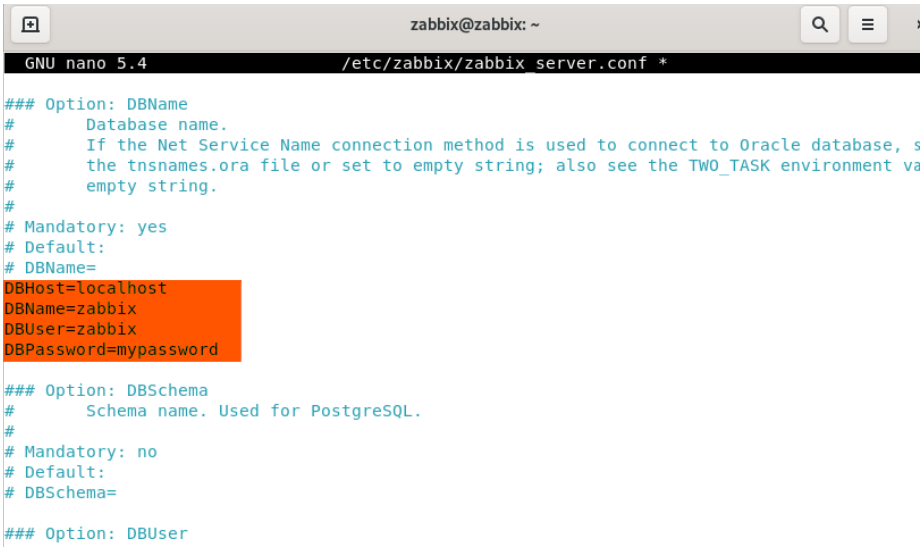


FIGURE 16 – Le fichier de configuration du serveur Zabbix.

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

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

FIGURE 17 – Commande de redémarrage de Appache2.

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

```
root@zabbix:/home/zabbix# systemctl start zabbix-server zabbix-agent
```

FIGURE 18 – Commande de démarrage du serveur Zabbix.

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

```
root@zabbix:/home/zabbix# systemctl status  zabbix-server zabbix-agent
● zabbix-server.service - Zabbix Server
     Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; vendo
     Active: active (running) since Tue 2023-05-16 12:38:17 CEST; 28min ago
    Process: 792 ExecStart=/usr/sbin/zabbix_server -c $CONFFILE (code=exited,
   Main PID: 809 (zabbix_server)
      Tasks: 48 (limit: 2264)
     Memory: 63.5M
        CPU: 9.451s
```

FIGURE 19 – Commande de vérification si le serveur Zabbix est opérationnel.

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

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

FIGURE 20 – Lien de navigateur vers le serveur Zabbix.

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

FIGURE 21 – Choix de la langue pour continuer l'installation.

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

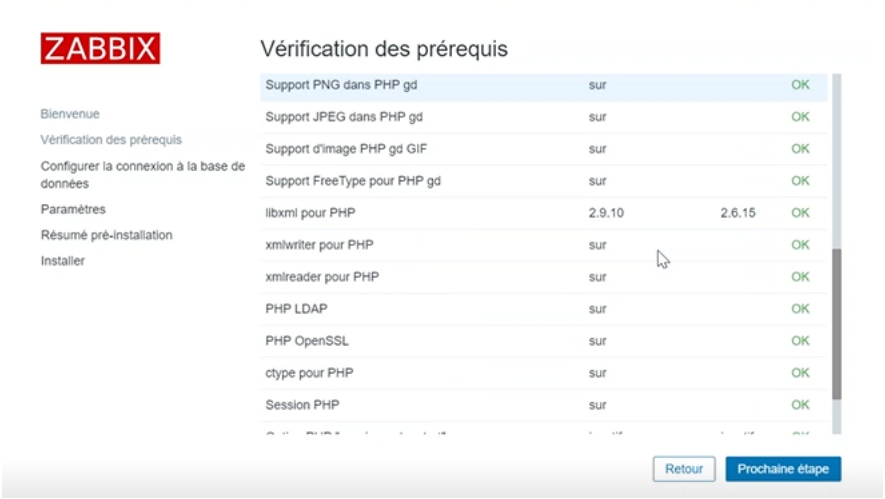


FIGURE 22 – Les conditions logicielles préalable de Zabbix.

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

FIGURE 23 – Configuration de la base de données de Zabbix.

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

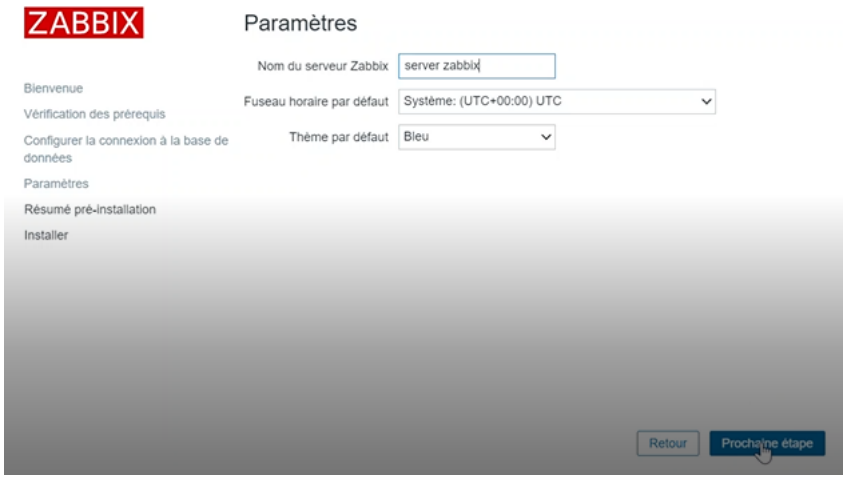


FIGURE 24 – Paramètre de saisie du nom de Zabbix.

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

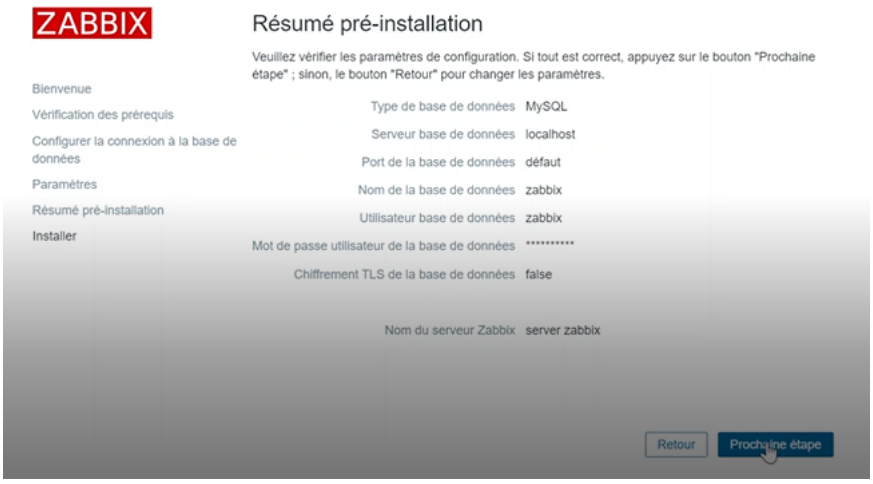


FIGURE 25 – Installation complète de Zabbix.

7. Vous pouvez désormais commencer à utiliser le logiciel Zabbix, la figure ci-dessous montre la fin de linstallation ;

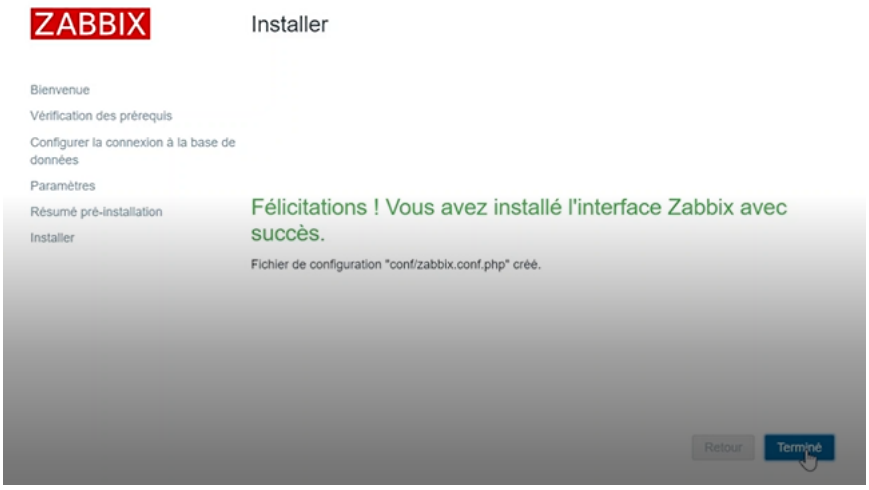


FIGURE 26 – Zabbix pret à être utilisé.

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

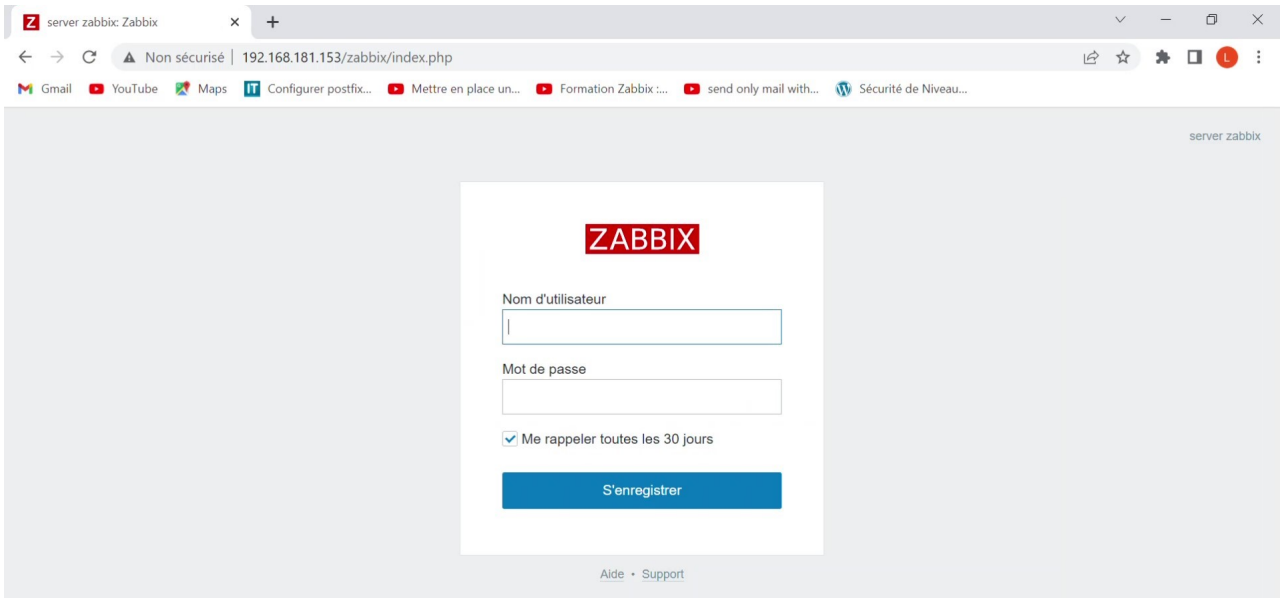


FIGURE 27 – Page de connexion de Zabbix.

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

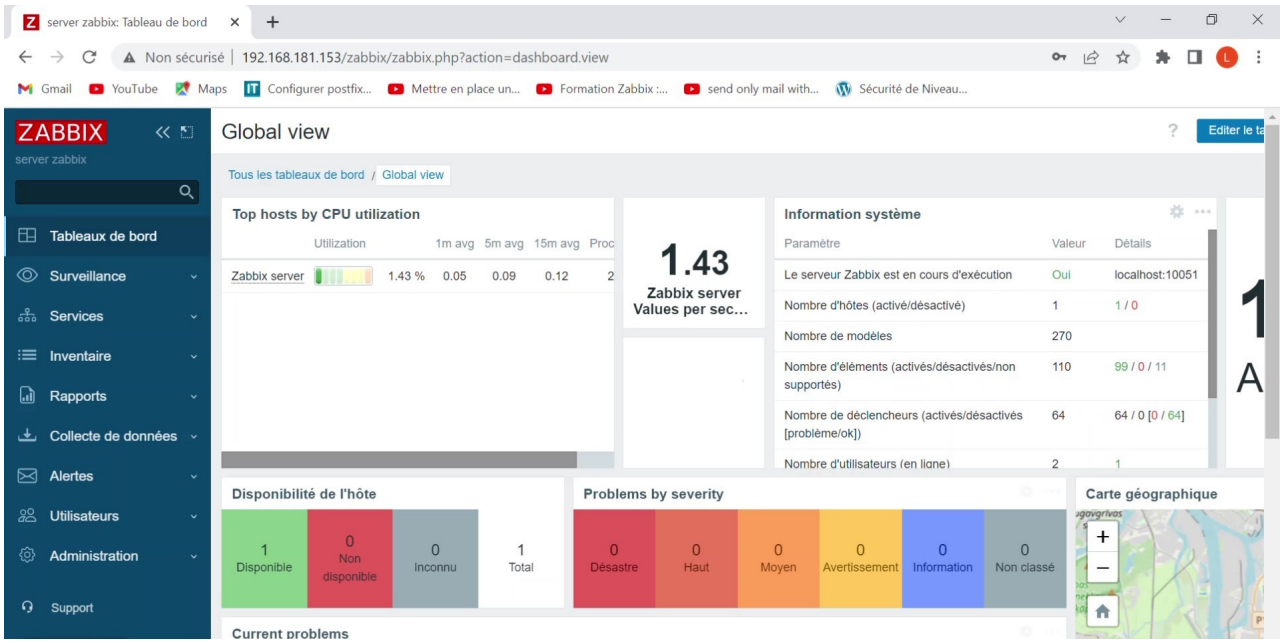


FIGURE 28 – Page d'accueil de Zabbix.

C.3 Installation et configuration du service SMTP

1. Installer le service SMTP sécurisé, comme illustré dans la figure ci-dessous;

```
root@zabbix:/home/zabbix# sudo apt-get install ssmtp
```

FIGURE 29 – Commande d'installation du service ssmtp.

2. Ouvrir le fichier de configuration ssmtp (secure Simple Mail Transfer Protocol)

```
root@zabbix:/home/zabbix# nano /etc/ssmtp/ssmtp.conf
```

FIGURE 30 – Commande permettant d'ouvrir le fichier de configuration ssmtp.

```
  GNU nano 5.4                                  /etc/ssmtp/ssmtp.conf
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=lia.a2lou@gmail.com

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:465

# Where will the mail seem to come from?
#rewriteDomain=

# The full hostname
hostname=zabbix

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
AuthUser=lia.a2lou@gmail.com
AuthPass=qdctwhvyicmpomrz
UseSTARTTLS=yes
useTLS=yes
```

FIGURE 31 – Configuration du fichier ssmtp.

3. Tester pour vérifier que ssmtp fonctionne avec la commande illustrée dans la figure ci-dessous;

```
root@zabbix:/home/zabbix# sudo echo "Ceci est un message de test de Zabbix" | ssmtp lia.a2lou@gmail.com
```

FIGURE 32 – Test du fonctionnement du service ssmtp.

4. Réception du mail envoyée, comme illustré dans la figure ci-dessous;

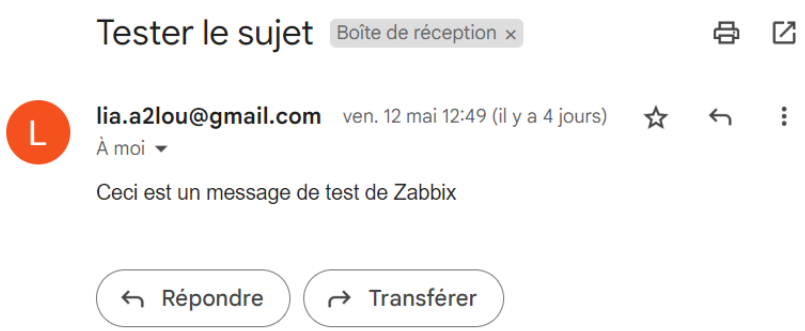


FIGURE 33 – Réception du mail.

5. Réception de l'alerte liée au problem du CPU sur le Windows-Serveur, comme illustré dans la figure ci-dessous ;

FIGURE 34 – Réception du mail concernant la CPU du Windows-Serveur.

Résumé

Ce projet est constitué de deux parties distinctes :

La première partie concerne la mise en place d'un system de supervision. L'objectif de ce travail consiste à proposer une architecture réseau sécurisée de l'Entreprise Cevital de Béjaïa. Pour cela nous avons étudié le réseau actuel, ce qui nous a permis de suggérer des solutions afin de proposer une nouvelle architecture plus sécurisée. Nous avons aussi présenté un aperçu du fonctionnement du logiciel en question, puis la configuration du réseau proposé à l'entreprise s'est faite à l'aide du simulateur réseau GNS3.

La seconde partie, concerne la supervision du réseau de Cevital. Dans cette étude, nous avons mis en place et configuré une station de surveillance Zabbix chargée d'alerter l'administrateur en cas de pannes ou de surcharge sur le réseau. Certaines fonctionnalités tel qu'Agent-Zabbix et le protocole SNMP qui permettent de surveiller les machines utilisant les systèmes d'exploitation Linux et Windows ont été configurés. Les différentes configurations sont faites sur une machine virtuelle VMware utilisant le système d'exploitation Linux.

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

Abstract

This project consists of two distinct parts :

The first part concerns the implementation of a supervision system. The objective of this work is to propose a secure network architecture for the Cevital enterprise in Béjaïa. To do this, we studied the current network, which allowed us to suggest solutions to propose a new, more secure architecture. Then, we presented an overview of the operation of the software in question, and the configuration of the proposed network for the company was done using the GNS3 network simulator.

The second part concerns the supervision of the Cevital network. In this study, we set up and configured a Zabbix monitoring station, responsible for alerting the administrator in case of failures or overload on the network. Some features such as Agent-Zabbix and the SNMP protocol, which allow monitoring of machines using Linux and Windows operating systems, were configured. The different configurations were made on a VMware virtual machine using the Linux operating system.

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