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

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

Département d'Automatique, Télécommunications et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications

Thème

Étude et mise en place d'une solution de supervision - cas Cevital

Préparé par :

- **M lle IGHIT Thilleli**
- **M lle BAKOUCHE Celia**

Dirigé par :

M. DIBOUNE Abdelhani

M. BOUKIRAT Massinissa

M. SLIMANI Mennad

Examiné par :

Présidente : M me GHENNAM Souhaila

Examinateur : M. ATMANI Hakim

Année Universitaire : 2023-2024

Remerciements

Nous tenons à remercier en premier lieu Dieu le tout puissant et miséricordieux pour nous avoirdonné le courage, la force et la patience d'achever ce modeste travail.
Nous adressons nos sincères remerciements à notre encadreur Mr. DIBOUNE Abdelhani qui n'a pas hésité à mettre à notre disposition ses connaissances, ses multiples conseils et instructions et qui nous a également dirigé tout le long de ce travail ainsi que pour la confiance qu'il nous a témoigné, nous le remercions aussi pour le grand soutien moral qu'il nous a apporté et sa patience.

Nous remercions également tout le personnel d'entreprise CEVITAL Bejaia, et particulièrement Mr. BOUKIRAT Massinissa et Mr. SLIMANI Mennad, pour les informations et leurs contributions et pour mise à leur disponibilité.

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

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

Dédicace

Je tiens tout d'abord à exprimer ma gratitude envers Allah pour m'avoir accordé la force et le Courage Pouvoir réaliser ce modeste travail.

Je dédie ce projet de fin d'études à ceux qui ont été mes piliers tout au long de cette aventure

À mes très chers parents Yacine et Nedjima, que j'aime énormément pour leur Patience, leur amour, leur encouragement et leur sacrifice tout au long de mon parcours. Que Dieu leur accorde une bonne santé et une langue vie.

À mes chères frères, Djelloule, Fayçal, Ghilles et à ma belle-sœur Warda merci pour leur amour, encouragement, leur accompagne Vous avez été à mes côtés dans les moments de doute et de réussite je vous aime

À mon oncle Hakim et ma grand-mère Lilli je vous aime énormément, que dieu vous garde.

A mes meilleure amie, Liza, et à Sonia, merci pour votre amitié sincère votre générosité et votre soutien inconditionnel.

Enfin, à mon binôme « celia», avec qui j'ai partagé cette aventure, pour sa collaboration, son travail acharné et son esprit de camaraderie

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

Merci à vous tous, de tout cœur, pour votre soutien indéfectible et votre confiance en moi.

Dédicace

Je dédie ce mémoire à mes chers parents, dont l'amour incommensurable, À ma mère, pour son dévouement, sa patience et sa présence réconfortante à chaque étape de ma vie. Tu as toujours cru en moi, et c'est en grande partie grâce à toi que ce travail voit le jour.

À mon père, qui nous a quittés trop tôt, je souhaite dire que ce mémoire est aussi le tien. C'est avec une profonde émotion que je veux te dire : je l'ai fait. J'espère qu'aujourd'hui, de là où tu es, tu es fier de moi. Ton soutien indéfectible, tes valeurs et tes enseignements continuent de m'accompagner chaque jour, guidant mes pas et nourrissant ma détermination.

À mes adorables sœurs, « Hayette », « Lynda », et « Farida », et à mes frères, « Billa »l et « Nadjim », pour leurs présence bienveillante et leur réconfort indéfectible.

À mes meilleures amies, « Souhila » et « Siham », « Biba », « salima » pour leurs amitié précieuse, leurs écoute et leurs soutien inconditionnel dans les Moments de doute.

Enfin, à mon binôme « Thilleli », avec qui j'ai partagé cette aventure, pour sa collaboration, son travail acharné et son esprit de camaraderie.

Merci à vous tous, de tout cœur, pour votre soutien indéfectible et votre confiance en moi

Table de matières

Table de matières

Listes des figures

Chapitre I

Chapitre II

Chapitre III

Listes des figures

Liste des tableaux

Chapitre I

Chapitre II

Liste des abréviations

A :

API : Application Programming Interface.

AD: Active Directory.

B :

BPDU : Bridge Protocol Data Unit.

C :

CDP : Cisco Discovery Protocol.

CLI : Command Line Interface.

CPU : Central Processing Unit.

D :

DHCP : Dynamic Host Configuration Protocol.

DMZ : Demilitarized Zone.

DNS : Domain Name System.

G :

GNS3 : Graphical Network Simulator 3.

GUI : Graphical User Interface.

H :

HTTPS : HyperText Transfer Protocol Secure.

HTTP : HyperText Transfer Protocol.

HSRP : Hot Standby Router Protocol.

I :

IAB : Interactive Advertising Bureau.

ICMP : InternetControl Message Protocol.

IP : Internet Protocol.

ISO : International Organization for Standardization.

IOS : Internetwork Operating System.

ID: Identificateur.

ICMP: Internet Control Message Protocol.

L :

LAN: Local Area Network.

Liste des abréviations

M :

MKDIR : MaKe DIRectory.

MIB : Management Information Base.

MySQL : My Structured Query Language.

N :

NMS : Network Management System.

O :

OSPF : Open Shortest Path First.

OID : Object Identifier.

P :

PING : Packet Internet Groper.

PHP: Hypertext Preprocessor.

Q :

QOS : Quality of Service.

R :

RRDTOOL : round-robin database tool.

RFC : Request for Comments.

RIP : Routing Information Protocol.

RAM: Random Access Memory.

S :

SNMP : Simple Network Management Protocol.

SMTP: Simple Mail Transfer Protocol.

SSMTP: Secure Simple Mail Transfer Protocol.

SQL: Structured Query Language.

STP : Spanning Tree Protocol.

T :

TelNet : Terminal Network.

TCP: Transmission Control Protocol.

TTL: Time To Live.

U :

UDP : User Datagram Protocol.

Liste des abréviations

V :

VLAN : Virtual Local Area Network.

VM : Virtual Machine.

VTP : VLAN Trunking Protocol .

W:

WIN: Windows

WAN: Wide Area Network.

Introduction générale

De nos jours, les réseaux informatiques jouent un rôle crucial dans chaque entreprise en connectant et en assurant la communication entre systèmes distribués sur des infrastructures distinctes. Cependant, la complexité croissante de ces réseaux les expose à divers risques, tels que les défaillances et les pannes, qui peuvent compromettre leur bon fonctionnement. Il est donc essentiel de mettre en place des mécanismes de supervision robustes pour anticiper et gérer ces problèmes.

La supervision est essentielle pour surveiller et contrôler en temps réel les réseaux d'une entreprise. Les équipes informatiques peuvent recueillir et d'analyser des données en permanence grâce à des outils de supervision avancés, ce qui leur permet de détecter les problèmes avant qu'ils n'affectent gravement l'entreprise. Elle permet de suivre divers paramètres critiques tels que les performances du réseau, les temps de réponse, les niveaux de charge et la sécurité. Grâce à cette surveillance, les équipes informatiques peuvent détecter, diagnostiquer et résoudre de manière proactive tous risques et incidents potentiels pouvant survenir sur un système supervisé et entraîner une interruption de service.

La mise en place de la supervision offre plusieurs avantages clés aux entreprises. Tout d'abord, en premier lieu une surveillance continue permet d'identifier rapidement les problèmes, facilitant ainsi une réaction et une résolution plus promptes des incidents. Cela réduit l'impact sur les opérations de l'entreprise et contribue à préserver la satisfaction des clients. En outre, la configuration d'alertes aide à détecter les anomalies en temps réel, permettant une intervention rapide. Elle contribue également à limiter les erreurs causées par la monotonie et la fatigue, assurant ainsi une meilleure précisionet qualité dans le travail effectué.

Pendant notre stage chez Cevital à Bejaïa, nous avons constaté que la gestion du réseau informatique posait plusieurs défis importants. Le grand nombre d'équipements compliquait la surveillance manuelle, réduisant la visibilité globale sur l'état du réseau. Cette situation entravait la détection rapide des incidents et des pannes, pouvant entraîner des temps d'arrêt et affecter la productivité des utilisateurs.

De plus, la manipulation manuelle et l'intégration de sources disparates augmentent le risque d'erreurs, compromettant ainsi la précision des données et l'efficacité des actions entreprises. Enfin, le manque d'un système de surveillance adéquat a également augmenté les risques de sécurité du réseau, compromettant ainsi la confidentialité et l'intégrité des données et des informations.

Après avoir identifié les défis liés à la gestion et à la configuration de notre infrastructure réseau, nous avons mis en place une solution de supervision en intégrant le serveur de supervision.

Pour atteindre cet objectif, notre travail s'est structuré en trois chapitres principaux.

Le premier chapitre portera sur la supervision des réseaux informatiques, incluant une étude comparative des outils existants. Cette analyse nous permettra de choisir l'outil le plus approprié à mettre en place pour notre projet.

Le deuxième chapitre portera sur tout ce qui concerne ou présenterons l'entreprise Cevital ou nous avons effectué notre stage. Nous y présenterons sa structure hiérarchique, son réseau informatique et les protocoles utilisés. Ensuite, nous réaliserons une étude approfondie de leur problématique et expliquerons la solution adoptée pour remédier à ces problèmes.

Dans le troisième chapitre, nous commencerons par examiner l'environnement de travail. Nous aborderons ensuite la simulation de la supervision des différents équipements du réseau et la présentation des résultats.

Enfin, nous finirons par une conclusion générale récapitulative des points essentiels de notre travail et nous aborderons les perspectives futures.

Chapitre I

Supervision d’un réseau informatique

I.1 Introduction

Les systèmes informatiques sont devenus indispensables au bon fonctionnement des entreprises et administrations. Tout problème ou panne survenu sur une partie de ce système pourrait avoir de lourdes conséquences aussi bien financières qu'organisationnelles, Les entreprises adoptant un outil de supervision pour leurs systèmes informatiques sont principalement à la recherche d'une procédure d'auto- analyse leur permettant d'être bien préparées aux potentiels incidents et complications, et de les aborder efficacement. Donc surveiller un tel système devient plus que nécessaire.

Dans ce chapitre, nous allons définir précisément le concept de supervision (appelé aussi monitoring). Nous examinerons ses différents types, ainsi que les protocoles de supervision couramment utilisés tels que SNMP (Simple Network Management Protocol) et ICMP (Internet Control Message Protocol). Outre, nous aborderons les outils et utilitaires de supervision indispensables. Cette étude ressemble à un banc d'essai puisque pour chacun des logiciels nous allons faire une courte présentation et expliquer son fonctionnement, puis finir par ses avantages et ses inconvénients. Ensuite, nous procéderons à une étude comparative de ces utiles de supervision (solutions open-source). A la fin, nous préciserons le choix de l'outil retenu durant notre travail.

I.2 Définition de la supervision réseau

La supervision des réseaux (ou monitoring) comprend un ensemble de protocoles matériels et logiciels informatiques permettant en temps réel de surveiller, analyser, rapporter et d'alerter les fonctionnements anormaux des systèmes informatiques. Il s'agit de vérifier et/ou de diriger l'état d'un serveur, d'un équipement réseau ou d'un service logiciel afin de pouvoir les diagnostiquer et les résoudre.

I.2.1 Objective de la supervision

L'objective de la supervision est de surveiller le bon fonctionnement des réseaux. Elle permet [1] :

- ***La surveillance des performances***

Vise principalement à surveiller en temps réel l'infrastructure informatique. Cela

implique de vérifier les ressources système comme la CPU, la mémoire et le stockage, etc.

- ***Détection des problèmes et erreurs***

Elle permet de détecter rapidement les problèmes potentiels oules erreurs dans le système. Les administrateurs sont alertés dès qu'une anomalie est détectée, ce qui permet une intervention immédiate pour résoudre les problèmes avant qu'ils n'impactent les opérations. Cela garantit la continuité des activités.

- ***Optimisation des ressources***

En surveillant l'utilisation des ressources, la supervision informatique implique degarantir que les ressources sont allouées, utilisées et gérées de la manière la plus optimale possible.

- ***Sécurité accrue***

Contribuer à renforcer la sécurité de l'infrastructure informatique. En surveillant les journaux d'activité, les comportements anormaux et les tentatives d'intrusion.

- ***Planification de la capacité***

La supervision continue des performances permet de prévoir les besoins futurs en termes de capacité. Cela permet aux équipes informatiques de planifier et d'ajusterles ressources.

I.2.2 Type de surveillance

Il existe différents types de supervision qui permettent de gérer et maintenir l'infrastructure informatique. Voici certains des éléments de supervision :

- ***Surveillance réseaux***

Ce type de surveillance permet de superviser le bon fonctionnement des équipements réseaux. Elle inclut le suivi de la bande passante, la température, de la latence, du taux d'erreur, de la qualité de service (QoS), des protocoles utilisés et de la sécurité du réseau [2], en plus d'assurer une connectivité stable et sécurisée.

- ***Surveillance application***

Ce type de surveillance permet de vérifier la disponibilité, la réactivité et l'efficacité des applications, permet également de suivre la mise à jour de configuration des

applications, et réalise des analyses approfondies [2].

❖ ***Surveillance système***

Ce type de surveillance permet de détecter les problèmes de performances, les erreurs, les pannes, etc. Les outils de surveillance système peuvent collecter des informations sur les journaux (logs) du système, les ressources système (CPU, mémoire, disque), Elle vise à garantir qu'il fonctionne de manière optimale [2].

❖ ***Surveillance matérielle***

Ce type de surveillance consiste à surveiller les composants matériels tels que les serveurs, les routeurs et les disques durs pour collecter des données sur leur état et leurs performances, y compris la charge, la température et l'utilisation des ressources. Pour assurer le bon fonctionnement des infrastructures et d'assurer la fiabilité et la disponibilité du système [2].

❖ ***Surveillance bases de données***

Ce type de surveillance consiste à de garder un œil en permanence sur le fonctionnement de l'application qui gère la base de données. Lorsqu'un problème est détecté, déterminer son origine. L'idée est de repérer les problèmes avant qu'ils ne se muent en véritables pannes [3].

I.2.3 Les actions liées à la supervision réseau

Les actions liées aux événements détectés par les outils de surveillance peuvent inclure une variété de mesures en fonction du type d'événement. Voici quelques exemples [4] :

1. Enregistrement dans un journal

Enregistrement détaillé des événements tels que les tentatives de connexion, les modifications des fichiers, les accès aux bases de données, et les anomalies réseau. Cela permet de maintenir un historique complet des activités du réseau.

2. Le tracé graphique

Représenter graphiquement les évènements pour permettre une visualisation aux administrateurs pour interpréter plus facilement les tendances, les variations et les interactions entre différents paramètres du réseau.

3. Alerte

Des messages automatiques émis par les outils de surveillance réseau lorsqu'ils détectent des pannes ou des seuils dépassés. Par la suite, elles sont transmises aux administrateurs sous forme de message électronique (e-mail, SMS), afin de les tenir informés rapidement des problèmes critiques.

4. Exécution d'un script

L'exécution d'un script selon les règles prédéfinies implique l'automatisation d'actions pour répondre à un événement. Les scripts peuvent être utilisés pour effectuer des tâches spécifiques, par exemple redémarrer un service ou appliquer une mesure corrective pour résoudre un problème.

I.3 Protocoles utilisés pour la supervision

I.3.1 Protocole (SNMP)

Le développement rapide des réseaux informatiques la gestion manuelle est devenu complexe pour relever ce défi, les administrateurs ont ressenti le besoin d'un moyen pour surveiller les performances des équipements et gérer les erreurs et pannes à distance, c'est dans ce contexte qu'ils ont envisagé l'utilisation d'un protocole standardisé répondant à ces besoins, offrant une flexibilité et une efficacité considérable dans la gestion des réseaux.

Présentation

SNMP (Simple Network Management Protocol) est un protocole de la couche application défini par l'Internet Architecture Board (IAB) dans la RFC1157 pour échanger des données de gestion entre les dispositifs réseau [5].

1. L'architecture et principe de fonctionnement du protocole SNMP.

La gestion de réseau via le protocole SNMP repose sur un modèle client-serveur également appelé modèle agents-manager. Dans ce modèle, le client correspond à la station de gestion de réseau, souvent appelée Manager ou encore Network Management Station (NMS) par certains éditeurs, chaque périphérique réseau agit comme un "serveur" en exécutant un agent SNMP, chargé de collecter des informations sur l'état et les performances des périphériques, qui sont ensuite stockées dans une base d'informations de gestion (MIB, Management Information Base). Les MIB ne sont rien d'autre que des

fichiers texte, et les valeurs des objets de données OID sont le sujet de conversation entre les gestionnaires et les agents.

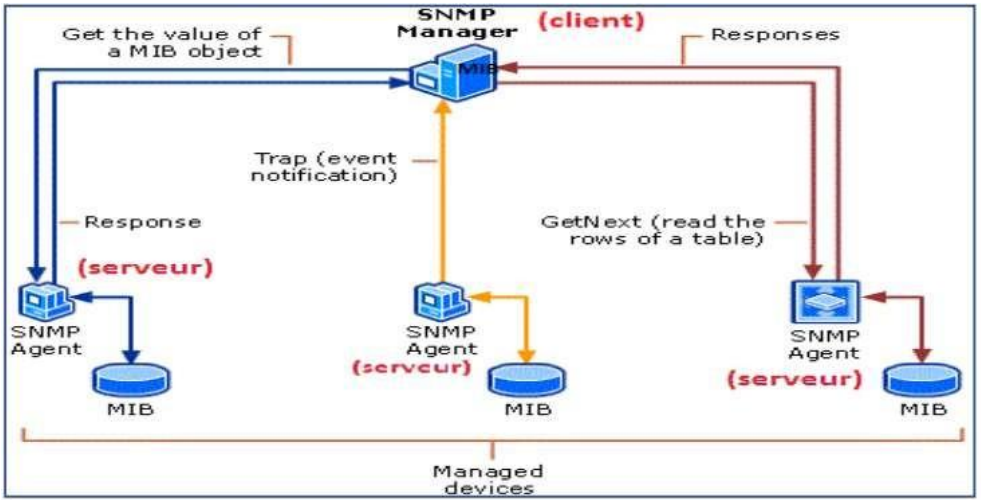


Figure I. 1: Communication Client/serveur avec les agents SNMP.

2. Les commandes SNMP

Un système SNMP prend en charge trois types de requêtes [6] :

- **Get :** cette catégorie comprend trois sous-requêtes :
  - **GetRequest :** permet aux stations de gestion NMS (Network Management Station)de consulter les objets et variables gérés par la MIB des agents.
  - **GetNextRequest :** permet aux NMS de parcourir les tables de la MIB.
  - **GetResponse :** est le message retourné par les agents en réponse aux commandesGetRequest, GetNextRequest et SetRequest des NMS.
- **Set :** la commande SetRequest permet à la NMS de modifier la valeur d'un objetdans la MIB et de déclencher une action sur le périphérique.
- **Trap** : il s'agit d'une alarme envoyée lors de la détection d'une anomalie. Cette commande permet à un agent de notifier un événement spécifique.
  Les alertes sont transmises lorsqu'un événement non attendu se produit sur l'agent.Ce dernier informe le manager via une trap.
  L'agent reçoit les requêtes sur le port 161 et le superviseur reçoit les alertes surle port 162. L'échange se déroule de la manière suivante :

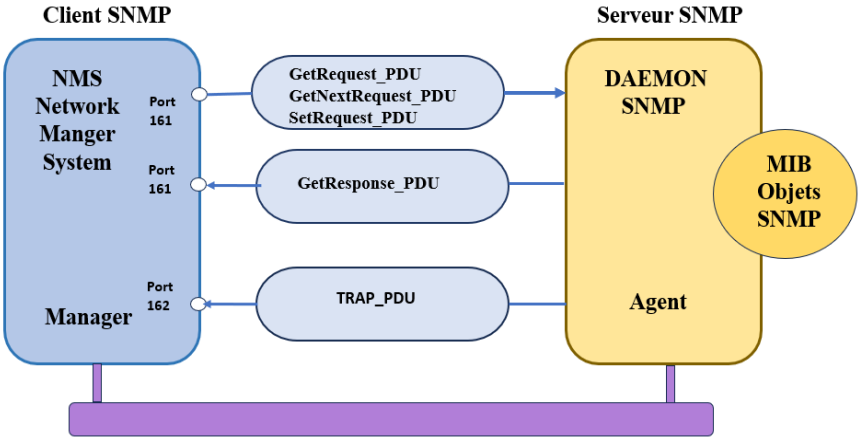


Figure I. 2 : Les types de message SNMP.

- Quand le manger veut interroger l'agent ou lui donner une instruction, il envoie une requête à l'agent. Celui-ci la traite et renvoie une réponse au mangeur.
- Quand un évènement se produit sur l'élément du réseau surveille par l'agent, ce dernier informe immédiatement le manger par une alerte de type trap ou informe. Dans le cas d'un informe, le serveur envoie une réponse à l'agent émetteur.

3. La gestion des réseaux avec le protocole SNMP

L'environnement de gestion SNMP est constitué de plusieurs composantes : La station de supervision (Manager), les éléments actifs du réseau, les variables MIB, les agents et le protocole de gestion (SNMP), ce qui est illustré dans la figure ci-dessous **:**

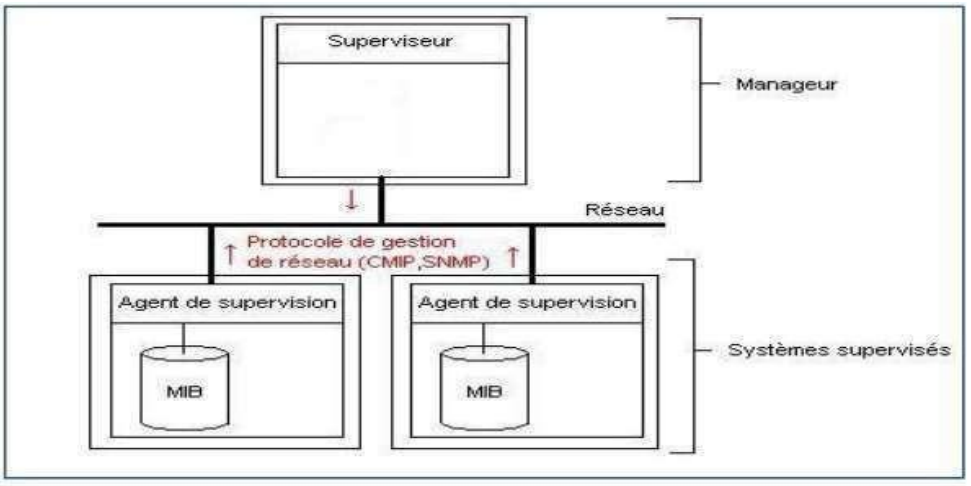


Figure I. 3: Structure de gestion des réseaux..

- ***Les agents***

Les agents sont des composants logiciels installés dans les équipements que nous souhaitons surveiller et gérer, tels que des routeurs, des ordinateurs ou des serveurs. Ils collectent périodiquement des informations sur la machine sur laquelle ils sont exécutés et les stockent localement. Si un problème est détecté, ils envoient une notification au service de gestion centralisé.

- ***Manageur/superviseur***

Dans SNMP, le manager est un système centralisé qui surveille et gère les dispositifs réseau, il envoie des requêtes aux agents SNMP sur les appareils pour collecter des informations sur leurs états et leurs performances, et reçoit des notifications des agents en cas d'anomalies. Et c'est donc cet outil qui va interroger les équipements du réseau.

- ***La* MIB (Management Informatique Base)**

La MIB (Management Information Base) est une base de données décrivant tous les objetsde données utilisés par un périphérique particulier qui peuvent être interrogés ou contrôlésà l'aide de SNMP. Chaque agent possède sa propre MIB, qui signifie qu'il y a une MIB pour chaque périphérique à surveiller.

La MIB est une structure arborescente (figure1.3) dont chaque nœud est identifié par un OID (Object IDentifier, Identifiant d'Objet) unique, qui peuvent être utilisés de manière interchangeable, de la même manière que les adresses IP et les noms d'hôte sont utilisés. Cependant, le SNMP utilise les OID (Object Identifier) pour interroger et modifier les

informations de la MIB. La MIB est essentiel pour structurer les données de manière logique et hiérarchique, facilitant ainsi la navigation et l'accès aux informations requises.

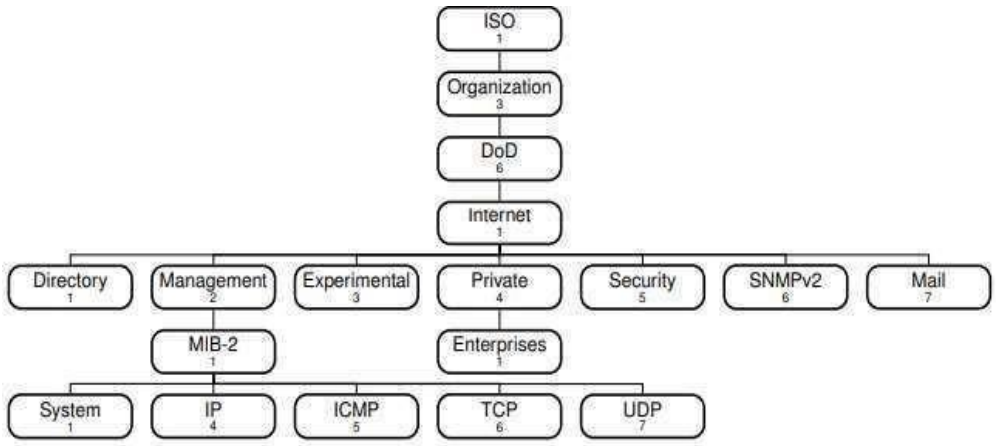


Figure I. 4: Structure arborescente de la MIB.

Pour accéder aux variables souhaitées, on utilisera l'OID qui indique l'emplacement spécifique de la variable à consulter dans la MIB. Par exemple, sur une machine, l'OID représente un chemin précis vers une variable particulière dans la structure arborescente de la MIB.

Chaque objet est représenté par un OID (Object IDentifier).

Exemple pour accéder au système : 1.3.6.1.2.1.1 ⇐⇒ iso.org.dod.internet.mgmt.mib-2. System [7].

1. Versions du protocole SNMP

Il existe trois types de version SNMP [8] :

SNMP v1

La version initiale du protocole SNMP, est définie dans les RFC 1065 à 1067 et 1155 à 1157. Développée à une époque où les normes et la sécurité Internet étaient peu considérées, SNMPv1 fonctionne sur divers protocoles, dont UDP, IP, CLNS, DDP et IPX.Il utilise un mécanisme d'authentificationen envoyant une "chaîne de communauté" (un mot de passe) en texte clair, offrant ainsi une sécurité très limitée.

SNMP v2

Apporte des améliorations significatives par rapport à la version 1, notamment entermes de performances, de sécurité et de confidentialité. Elle est définie dans RFC1441 et RFC 1452. Elle introduit des améliorations dans la communication entre gestionnaires et ajoute la requête GetBulkRequest pour récupérer de grandes quantités de données en une seule requête, remplaçant l'utilisation itérative de GetNextRequest. Cependant, son système de sécurité basé sur le parti était perçu comme trop complexe, limitant ainsi son adoption.

SNMP v3

Est la version la plus sécurisée du protocole SNMP (définie dans RFC 3414, introduisant des fonctionnalités telles que l'authentification des messages, le cryptage des données et le contrôle d'accès. SNMP v3 garantit une protection solide contre les risques de sécurité. L'objectif principal de ces améliorations est de rendre la gestion du réseau à distance plus sûre et fiable, en surmontant les limitations des versions précédentes.

I.3.2 Internet Control Message Protocol (ICMP)

Le protocole ICMP (Internet Contrôle Message Protocole) est un protocole d'information entrenœuds utilisateurs de service internet (Ping, algorithmes de traçage de route) [9]. Il permet aussi de gérer les informations relatives aux erreurs des machines connectées et d'en informer les différents émetteurs des datagrammes en erreurs. ICMP ne sait pas corriger ses erreurs et il n'a aucun moyen de s'assurer que les paquets arrivent bien à destination. Les messages d'erreurs ICMP sont transportés sur le réseau sous forme de datagrammes, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux- mêmes être sujet d'erreurs.

- Format du paquet ICMP

Un paquet ICMP, encapsulé dans un datagramme IP, comprend les champs suivants :

Type : Indique le type de message (ex. : demande/réponse d'écho).

Code : Détaille le sous-type du message (ex. : raison de l'échec).

Checksum : Vérifie l'intégrité du message.

Identifiant et numéro de séquence : Utilisés pour associer les requêtes et réponses d'écho.

Données : Contient des informations spécifiques au message.

- Types de messages ICMP

Les principaux types de messages ICMP sont :

Echo Request (Type 8) et Echo Reply (Type 0) : Test de connectivité (Ping).

Destination Unreachable (Type 3) : Indique une destination inaccessible.

Source Quench (Type 4) : Indique un débit excessif (désuet).

Redirect (Type 5) : Suggère une meilleure route pour atteindre une destination.

Time Exceeded (Type 11) : TTL expiré, utilisé par trace route.

I.3.3 Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) est un protocole de découverte de couche deliaison intégré dans périphériques est configuré en mode actif par défaut, y compris les routeurs et les commutateurs. CDP est utilisé pour découvrir et obtenir des informations sur les équipements Cisco connectés à un réseau. Il permet de collecterdes informations telles que le nom de l'équipement, le type de périphérique, l'adresse IP, le système d'exploitation, la version du logiciel, le numéro de série, etc. Cela permet aux administrateurs réseau de Mieux comprendre la topologie du réseau et de diagnostiquer les problèmes plus rapidement [10].

I.4 Quelques solutions de supervision

Il existe de nombreuses solutions Open Source dédiées au monitoring. Le choix principal dépend des différents cas d'utilisation. Nous allons présenter quelques logiciels.

I.4.1 Zabbix

Créé en 2001, puis donnant naissance à une entreprise nommée Zabbix SIA en2005. Zabbix est une solution de supervision open-source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de lasupervision et créer une communauté autour de lui pour permettre une évolution plus rapide. A côté de cela, cette société propose un service de maintenance commerciale.Zabbix permet plusieurs moyens d'acquérir les données via SNMP, via test de service, via l'agent Zabbix local qui permet d'obtenir toute information sur l'équipement sans utiliser le protocole SNMP [11].

L'architecture logicielle est découpée en composants dans le but de faciliter le monitoring distribué :

- ***Serveur***

Le serveur est le cœur de l'application Zabbix. Il centralise les données et permet de les attendre (trapping) ou d'aller les chercher (polling). Il centralise, aussi, toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème.

- ***Proxy***

Élément optionnel de l'architecture, il permet de bufférisers les données reçues des différents sites dans le but d'alléger les traitements pour le serveur.

- ***Agent***

Une fois installé sur un système, l'agent va collecter les données locales et les envoyer au serveur.

Interface Web

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

Tous ces composants sont développés en langage C afin de garder de hautes performances, hormis bien évidemment l'interface Web développée en PHP.

L'interface est divisée en cinq parties, Figure I. 5**.**

- ***Monitoring :*** C'est la partie affichage des statistiques, des graphiques, des alertes, de la cartographie, etc.
- ***Inventorie :*** C'est l'inventaire des machines et équipements.
- ***Report :*** Ce sont des statistiques sur le serveur Zabbix et un rapport de disponibilitédes services sur les machines supervisées.
- ***Configuration :*** Comme son nom l'indique, elle permet de configurer entièrement Zabbix.

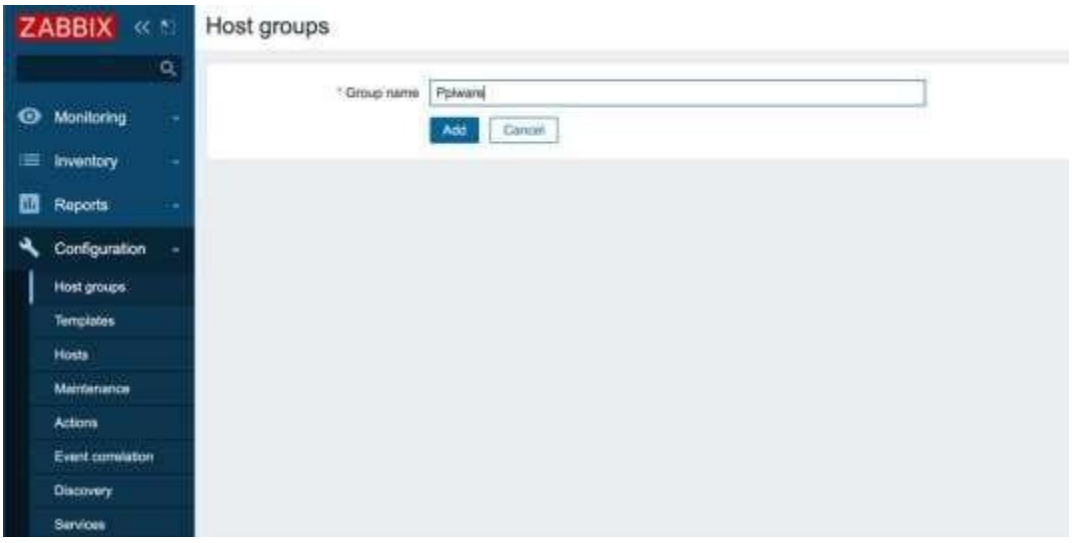


Figure I. 5 : L'interface de Zabbix.

Les avantages et les 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.

Tableau I. 1 : Les avantages et les inconvénients de Zabbix.

I.4.2 Cacti

Présentation

Cacti est un outil de surveillance de réseau qui utilise RRDtool (Round-Robin Database Tool), une base de données cyclique développée par Tobi Oetiker,

largement utilisée dans divers outils open source pour stocker des données chronologiques et générer des graphiques. RRDtool permet de gérer efficacement de grandes quantités de données en les condensant de manière à minimiser l'utilisation de l'espace de stockage tout en conservant une visibilité sur les tendancesdes performances [12].

Interface de Cacti

L'interface de Cacti est divisée en deux sections principales :

1. Console : Utilisée pour la configuration des paramètres, l'ajout de nouveaux dispositifs, la gestion des utilisateurs et des sources de données.

2. Graphs : Partie dédiée à l'affichage des graphiques générés par RRDtool, avec plusieurs modes D'affichage pour une gestion efficace :

3. Tree Mode : Classement hiérarchique des machines et équipements par groupes,utile pour gérer un grand nombre de dispositifs. Cette vue permet de naviguer facilement parmi les différents graphiques en fonction de l'organisation du réseau.

- **List Mode** : Permet de lister les graphiques associés à une machine spécifique sélectionnée dans la liste. Cela facilite l'accès rapide aux données de performance d'un dispositif particulier.
- **Preview Mode :** Semblable au List Mode, mais affiche directement les graphiques au lieu de simples liens. Cela permet d'avoir un aperçu rapide de l'état d'un équipement ou service sans avoir à naviguer davantage, idéal pour une supervision en temps réel.

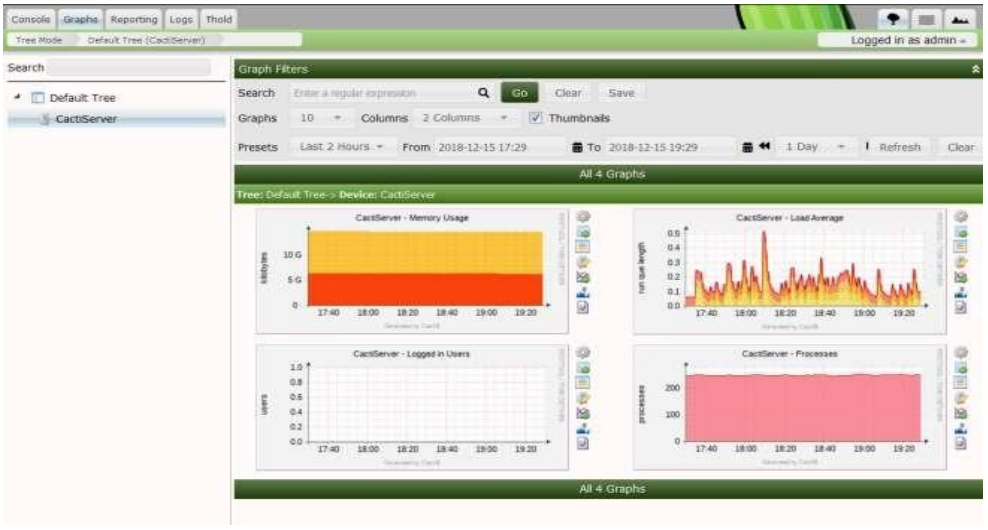


Figure I. 6: L'interface de Cacti

Les Avantages et les inconvénients de Cacti

Avantages	Inconvénients
• Interface : Interface claire, Elle permet également beaucoup plus de choses (Plus de modes d'affichages et plus de possibilités de configuration). • Configuration : Avec l'utilisation des templates pour les machines, les graphiques et la récupération des données se configurent aisément et entièrement via l'interface web. L'import/ export des templates au format XML est très simple. On peut, aussi, très facilement utiliser des options poussées de RRDTOOL. • Performance : Avec le choix du moteur de récolte des données, on peut opter pour la performance ou la simplicité. • Gestion des utilisateurs. • Communauté sur le web et présence d'une dizaine de plugins permettant d'étendre les fonctionnalités.	• Absence de gestion de panne etd'une cartographie de réseau.

Tableau I. 2: Les avantages et les inconvénients de Cacti

I.4.3 Nagios

Nagios, initialement connu sous le nom de NetSaint, est un outil de monitoring IT open source créé en1999 par Ethan Galstad.

Depuis sa création, Nagios s'est imposé comme l'un des logiciels de supervision les plus populaires, avec une communauté active de plusd'un million d'utilisateurs à travers le monde. Conçu pour alerter les administrateurs encas de problèmes et de les avertir lorsqu'ils sont résolus, Nagios contribue à maintenir la disponibilité et la performance des systèmes critiques. Initialement développé pour fonctionner sous Linux, il est également compatible avec d'autres variantes d'Unix [13].

- ***Interface de Nagios***

L'interface de Nagios est divisée en trois parties principales :

- ✓ ***Partie Monitoring* :** Propose plusieurs vues pour une gestion optimale : vue globalede tous les services surveillés, vue détaillée pour des informations spécifiques, vue de la carte du réseau, vue des problèmes en cours, et même une vue en 3D pour unereprésentation visuelle immersive.
- ✓ ***Partie Reporting* :** Regroupe des outils de rapports qui analysent les tendances, lesalertes, et les événements. Ces rapports permettent d'évaluer la disponibilité et la performance des services surveillés.
- ✓ ***Partie Configuration :*** Cette section permet deconfigurer tous les aspects de Nagios, des objets de supervision aux alertes et plugins, assurant ainsi une personnalisation complète.

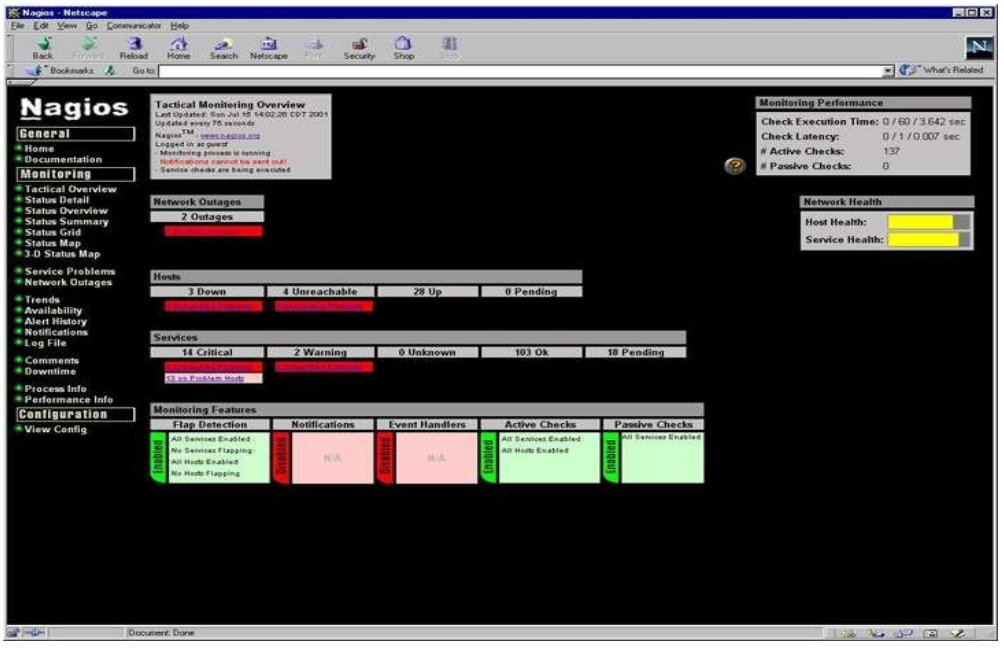


Figure I. 7 : L'interface de Nagios

Les Avantages et les 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

Tableau I. 3: Les avantages et les inconvénients de Nagios

I.4.5 Splunk

Splunk est une application logicielle qui aide les organisations à rechercher, surveiller et analyser des données provenant de diverses sources. Idéal pour l'analyse de big data, notamment les données machines, Splunk améliore la recherche grâce à des capacités intelligentes. Il permet la visualisation des données, la génération de rapports et l'analyse, aidant ainsi les équipes informatiques à améliorer leur efficacité globale grâce à l'information obtenues [14]. Splunk est composé de trois principaux composants :

1. **Le Forwarder Splunk** est un outil de transmission de données.
2. **L'Indexer Splunk** est utilisé pour l'analyse et l'indexation des données.
3. **Le Search Head** est une interface graphique (GUI) pour la recherche, l'analyse et la génération de rapports.

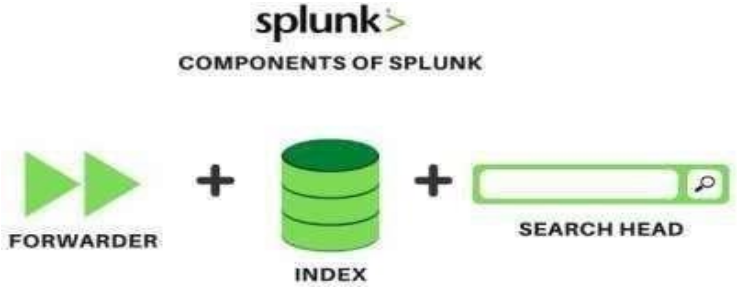


Figure I. 8: Composante de Splunk

.

L'interface principale **:** Elle donne accès aux applications installées dans la barre latérale gauche. Par défaut, la seule application installée est Search & Reporting. Les sources de données se situent dans la partie centrale haute et les rapports personnalisés (non encore ajoutés) dans la partie centrale inférieure. Voici la figure présentée ci-dessous.

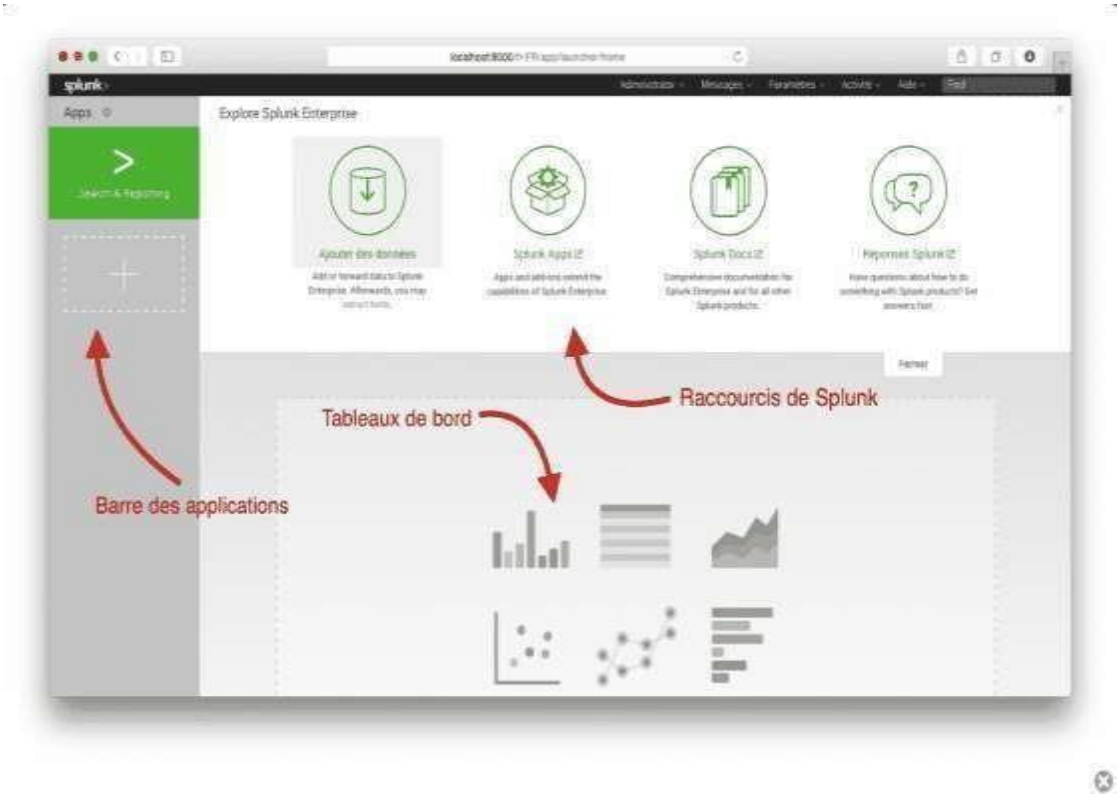


Figure I. 9: Access Splunk web interface.

Avantages et inconvénients de Splunk

Avantages	Inconvénients
✓ Interface graphique améliorée avec des tableaux de bord ✓ Les tableaux de bord de Splunk ne sont pas statiques n peut l'utiliser pour une petite structure qui crée assez peu de données ✓ Simplicité des fonctions de base. N'importe quelle personne peut créer des rapports, sans avoir besoin d'être analyste de données. ✓ Puissance du moteur d'indexation	✓ Aucun dispositif d'ETL : pas de moyen simple de corriger les données, ou d'effectuer de jointures. Il faut donc avoir un intermédiaire qui fait ce travailpour fournir des événements en entrée. ✓ Nouveau langage à apprendre en parallèle de tous les autres ✓ Prix au gigaoctet de données traité.

Tableau I. 4: Les avantages et les inconvénients de Splunk.

I.4.6 Centreon

Centreon, basé sur Nagios, se présente comme une évolution de celui-ci pour tout d'abord son interface mais aussi ses fonctionnalités. Créé en 2003 par des français souhaitant améliorer Nagios et son interface très austère, Centreon (anciennement Oréon) a été repris par une nouvelle entreprise nommée Merethis. Centreon reprenddonc les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes. Son interface reprend un découpage classique [15] :

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

Configuration : Pour tout configurer de A à Z.

- ***Administration*** *:* Configuration des accès utilisateurs.

Toujours visibles en haut à droite, un tableau récapitulatif du nombre de machines actives et des éventuelles machines ne répondant plus pour toujours garder un œil sur l'ensemble du réseau

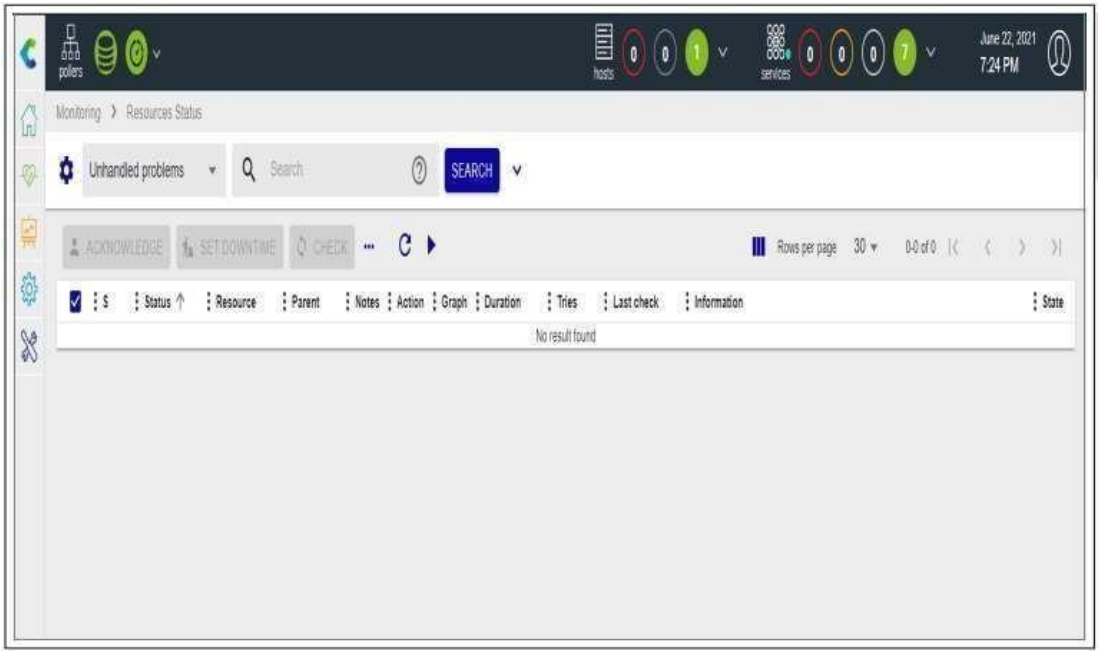


Figure I. 10: L'interface de centreon

Les Avantages et les inconvénients de Centreon

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

Tableau I. 5: les avantages et les inconvénients de Centreon.

I.5 Etude comparative et choix d'une solution de supervision

Critère	**Centreon**	**Zabbix**	**Cacti**	**Nagios**	**Splunk**
Licence	Open source + des versions entrepris es	Open source	Open source	Open source + Commercial	Commerci al (avec version gratuite)
Prix	Gratuit (version communa utaire)	Gratuit	Gratuit	Gratuit (Nagios Core) +Payant (Nagios XI)	Tarification baséesur les données
Fonctionnal itéde Découverte	Automa t-isée et manuell e	Automati -s-ée et manuelle	Principal - ement basé sur SNMP)	mais limité en Nagios Core	Avec des fonctionnal itéss avancées
Groupes	Les groupes d'hôtes et de services pour une gestion simplifiée	Les groupes d'hôtes, De Template, et d'éléments pour une organisation structurée.	Ne supporte pas nativeme ntles groupes, la configur a-tion est plus manuelle.	Support de base pou rles groupes dans Nagios Core, amélioré dans Nagios XI.	Pour la Gestion des utilisateurs et des autorisations

Méthode de configuration	GUI (Interface Web) + CLI (ligne de commande	GUI (interface web) + CLI ligne de commande	Utilise une interface web pour les configurations de base mais requiert une configuration via les fichiers	Principalement fichiers de Configuration GUI limitée (Nagios cor)	Interface web, CLI
Stockage	MySQL/ MariaDB	MySQL/ MariaDB	MySQL pour La configuration RRDTool pour les données	MySQL/PostgreSQL+ fichiers plats	Indexation et Stockage distribués
Passage à L'échelle	Bonne évoluti-vité avec centreon Engine et Broker	Très évolutif avec proxy Zabbix	Modérément évolutif limité par RRDTool	Évolutivité variable meilleure avec Nagios	Modérément évolutif limité par RRDTool
Assistance	Support commerciale disponible	Communauté active + Support commerciale disponible	Communauté active + Support commerciale direct	Communauté active + Support commerciale	Support payant disponible

Tableau I. 6 : Comparatif des solutions de la supervision d'un réseau informatique

.

I.6 Solution de supervision choisie

Centreon offre des fonctionnalités avancées de scalabilité, ce qui signifie qu'il peut gérer efficacement une grande quantité de données de surveillance, même dans les environnements IT les plus vastes et les plus complexes. Il est capable de s'adapterà des déploiements à grande échelle sans compromettre les performances ou la fiabilité. Il a été reconnu pour son architecture modulaire et offrant une grande flexibilité dans la configuration et l'extension de la supervision.

- **Gestion et configuration simplifiées** : Centreon simplifie la gestion des systèmes grâce à une interface graphique intuitive et des assistants de configuration. La combinaison de la configuration GUI et CLI, ainsi que la gestion par groupes, facilite l'administration des hôtes et des services, permettant ainsi une surveillance efficace et optimisée des opérations IT.

- **Connectivité** : Centreon se connecte à MySQL et MariaDB, permettant une intégration fluide pour le stockage et la gestion des données de supervision. Cela assure une performance optimale et facilite les rapports et analyses approfondies.

- ***La communauté et support :*** la communauté de Centreon offre un support précieux permettant aux utilisateurs d'accéder à une expertise partagée. Cela favorise l'échange de conseils, la résolution de problèmes et l'amélioration continue de l'utilisation de la plateforme.

I.7 Conclusion

Pour conclure, la surveillance des réseaux est indispensable pour garantir la fiabilitéet les performances des réseaux informatiques. Ce chapitre a été consacré à la présentation détaillée de la notion de supervision et receler des points touchants desexemples de solutions en évoquant leurs caractéristiques d'abord, en sus on a mis en évidence un tableau comparatif en fonction de nos besoin set cela nous a permisde choisir l'outil de supervision Centreon. En utilisant cet outil, les entreprises peuvent adopter une approche proactive de la gestion des réseaux afin d'optimiser l'efficacité de leurs systèmes tout en diminuant les dépenses et les interruptions.

Chapitre II

Présentation de l'organisme d'accueil et analyse de l'existant

II. 1 Introduction

Dans cette section, nous allons explorer l'organisme dans lequel nous avons effectué notre stage pour ce projet, à savoir Cevital. Nous examinerons ses activités et sa structure organisationnelle. Notre attention sera particulièrement portée sur lecentre informatique de Cevital. En identifiant la problématique centrale de notre sujet. Enfin, nous exposerons la solution adoptée pour résoudre cette problématique.

II. 2 Présentation de l'organisme d'accueil

Créée en 1998 et établie au sein du port de Bejaïa, Cevital Agro-industrie opère plusieurs unités de production ultramodernes pour le sucre, les corps gras, l'eau minérale, les boissons et les sauces. Cette entreprise répond aux besoins nationaux et a été un catalyseur essentiel dans la transformation de l'Algérie, passant du statutd'importateur à celui d'exportateur pour les huiles, les margarines et le sucre. Ses produits sont distribués dans divers pays, notamment en Europe, au Maghreb, au Moyen-Orient et en Afrique de l'Ouest [16].

1. Historique du Cevital

Aujourd'hui, CEVITAL agroalimentaire est le plus grand complexe privé en Algérie. Il est devenu le leader du secteur agroalimentaire en Afrique. CEVITAL a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle. Ci-après, quelques dates qui ont marqué l'histoire de CEVITAL [16]

- 1998 : Création de Cevital Agro-industrie
- 1999 : Entrée en production de la raffinerie d'huile
- 2003 : Entrée en production de la raffinerie de sucre
- 2005 : Acquisition de LALLA KHEDIDJA

2. Situation géographique

Le complexe CEVITAL agro-industrie s'étend sur une superficie de 45 000 M2 (c'est le plus grand complexe privé en Algérie), il se situe au niveau du nouveau quai du port de Bejaïa à proximité de la route nationale N° 09 et N°26 ; Sur un terrain à l'origine inconstructible qui a été récupéré et viabilisé avec la dernière technologie de consolidation des sols par le système de colonnes ballastées (337 km de colonnes ballastées de 18m chacune ont été réalisées)

Figure II. 1: Vue satellitaire du complexe CEVITAL.

3. Secteurs d'activités

En tant que première entreprise privée en Algérie à avoir diversifié ses investissements dans plusieurs secteurs d'activité, Cevital a franchi des étapes historiques significatives pour parvenir à sa taille et à sa renommée actuelle. Avec des domaines d'activité incluant l'industrie agroalimentaire, la grande distribution, l'électronique, l'électroménager, la sidérurgie, l'industrie du verre plat, la construction industrielle, l'automobile, les services et les médias, le groupe Cevital s'est développé progressivement autour d'une vision claire : former un ensemble économique cohérent. Avec une équipe de 18 000 employés répartis sur trois continents, le groupe représente un pilier de l'économie algérienne, s'engageant constamment dans la création d'emplois et de richesses [17].

II.2.1 Organigramme de l'entreprise Cevital

L'organigramme décrit dans Figure II.2 donne une vue générale sur les différents organes constituants le complexe CEVITAL. Il est composé de treize directions principales dont le but de chaque direction est d'assurer le bon fonctionnement de ses tâches :

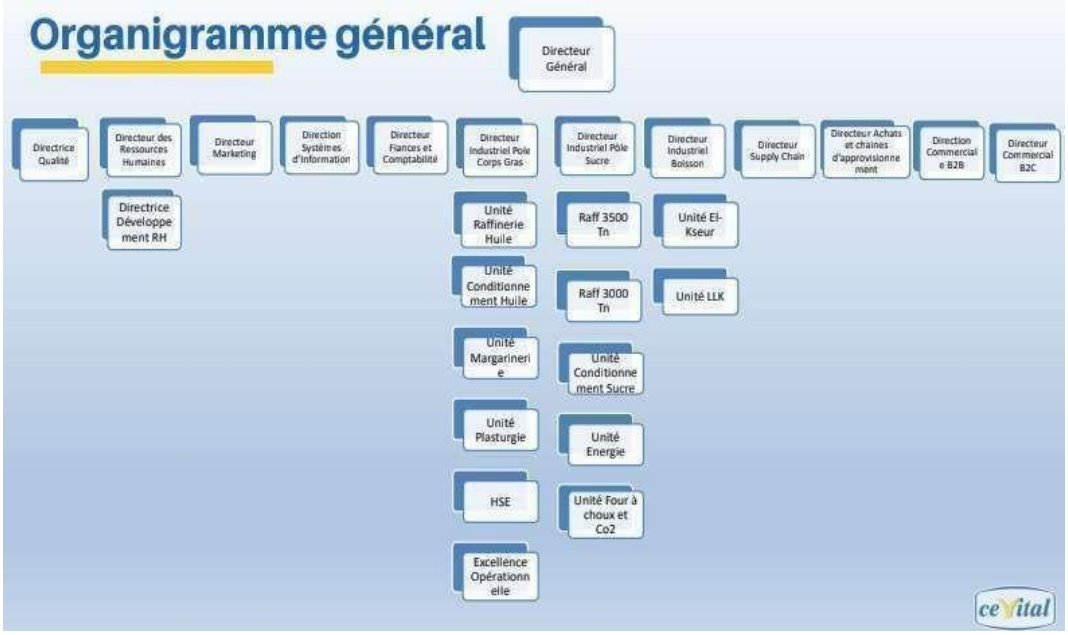


Figure II. 2 : Organigramme de Cevital.

II.2.2 Direction Système d'information

Notre stage s'est déroulé dans le service informatique de la direction des systèmes d'informations (DSI). La Direction des Services Informatiques (DSI) a pour mission de mettre en œuvre les infrastructures et les technologies de l'information nécessaires afin de soutenir et d'améliorer les activités, la stratégie et les performances de l'entreprise. Dans un souci constant de sécurité, elle assure la cohérence, la mise à jour, la maîtrise technique, la disponibilité et l'opérationnalité continue des outils informatiques et de communication. En outre, elle établit, à travers des plans pluriannuels, les orientations stratégiques requises en fonction des objectifs de l'entreprise et des avancées technologiques. Figure II.3 montre l'organigramme du système d'information.

Le service informatique est suivi par des responsables spécialistes cités ci-dessous.

- ***Directeur du système d'information*** : Il est chargé de régler les problèmes à moindre coût et dans les plus brefs délais et opter des solutions informatiques améliorant la productivité de l'entreprise.
- ***Administrateur système* :** Il conçoit, installe et veille au bon fonctionnement d'une infrastructure informatique et réseau d'une entreprise, il assume également la gestion et la maintenance de système opérant sur le réseau.

- ***Administrateur réseau :*** Il permet d'administrer le réseau et d'assurer la bonne circulation de l'information dans l'entreprise en veillant à la qualité, la continuité et la performance des équipements et du réseau, tout en répondant aux besoins des utilisateurs.

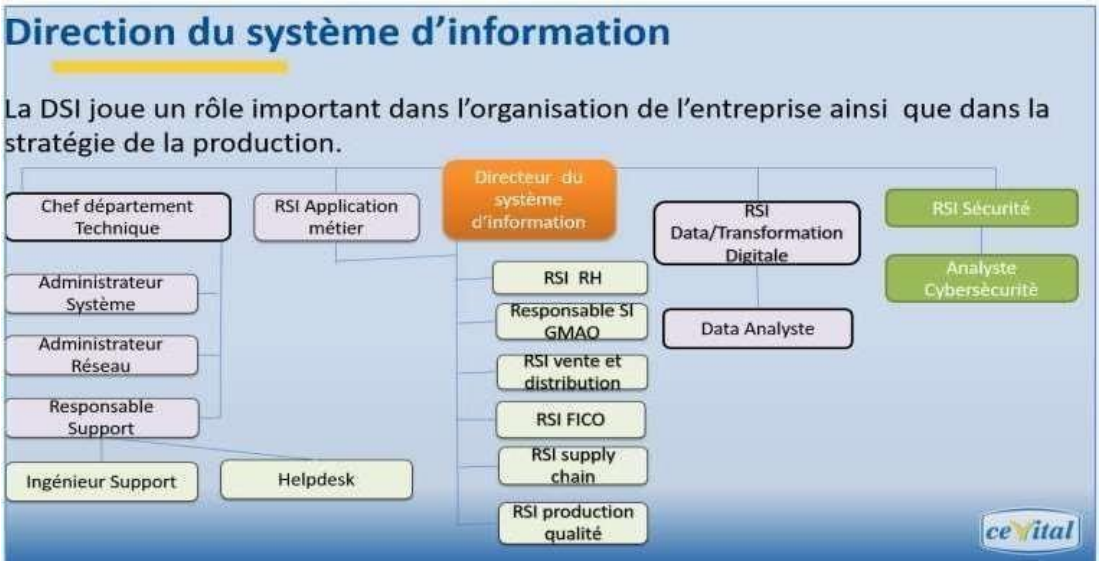


Figure II. 3: Organigramme de la direction système d'information.

II.3 Présentation du réseau

Notre réseau local est basé sur une architecture à trois couches.

II.3.1 Présentation de l'architecture à trois couches

L'architecture réseau du Cevital est basée sur un modèle hiérarchique à trois couches comme la montre la figure ci-dessous, conçu pour assurer des performances, une haute disponibilité et une sécurité optimale de son infrastructure réseau, La couche cœur est constituée de deux commutateurs de niveau 3 à qui gèrent la haute disponibilité du réseau grâce à des mécanismes de redondance tels que HSRP et EtherChannelt .Ces deux équipements sont interconnectés par des liens d'agrégation, permettant d'améliorer la disponibilité et d'assurer la continuité du service aux utilisateurs finaux. La deuxième couche, appelée couche de distribution, est constituée de deux commutateurs de niveau 3 capables de gérer des réseaux à grande échelle. Cette couche joue un rôle crucial est située au niveau intermédiaire du réseau et est responsable du traitement et de la distribution des données de la couche d'accès à la couche cœur. La couche d'accès est constituée de commutateurs de niveau 2 Cisco, assurent la connectivité des utilisateurs en mode

accès avec les VLANs configurés, facilitant ainsi une segmentation efficace du réseau. Pour la communication avec la couche cœur, les liaisons sont configurées en mode trunk, permettant le transport des VLANs vers le reste du réseau tout en maintenant une séparation claire et contrôlée des différents types de trafic.

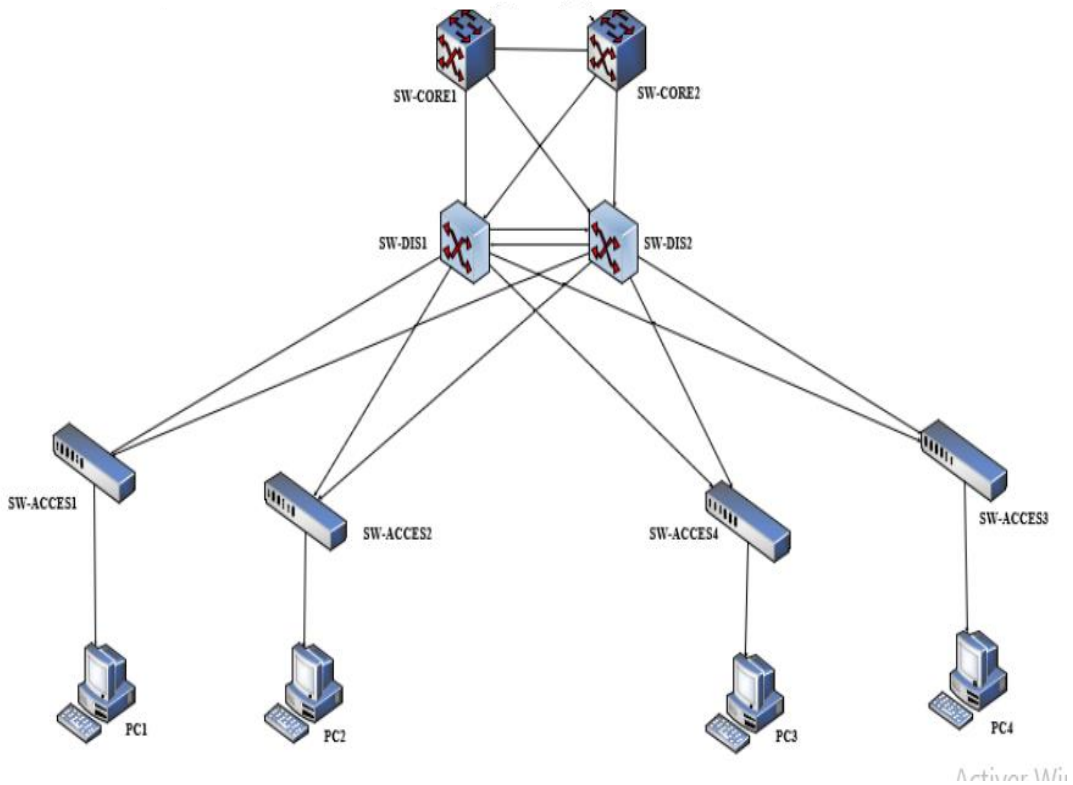


Figure II. 4: Modèle de conception hiérarchique à trois couches

II.3.2 Protocoles Utilisés

II.3.2.1 Le protocole VTP

Est un protocole de couche 2, son principal avantage est sa capacité de propager automatiquement des VLANs configurés sur un commutateur en mode 'server' les autres commutateurs sont configurés en mode client [18].

- ***Serveur :*** Associé à un domaine VTP, il déclare et modifie les VLANs. Les changements sont automatiquement propagés à tous les commutateurs du domaine VTP, et il maintient et diffuse la liste des VLANs aux clients.
- ***Client :*** Il est associé à un domaine VTP. Il n'est pas possible de modifier la configuration des VLANs. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.

Transparents : Il n'est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant, il propage les listes de VLAN qu'il les reçoit.

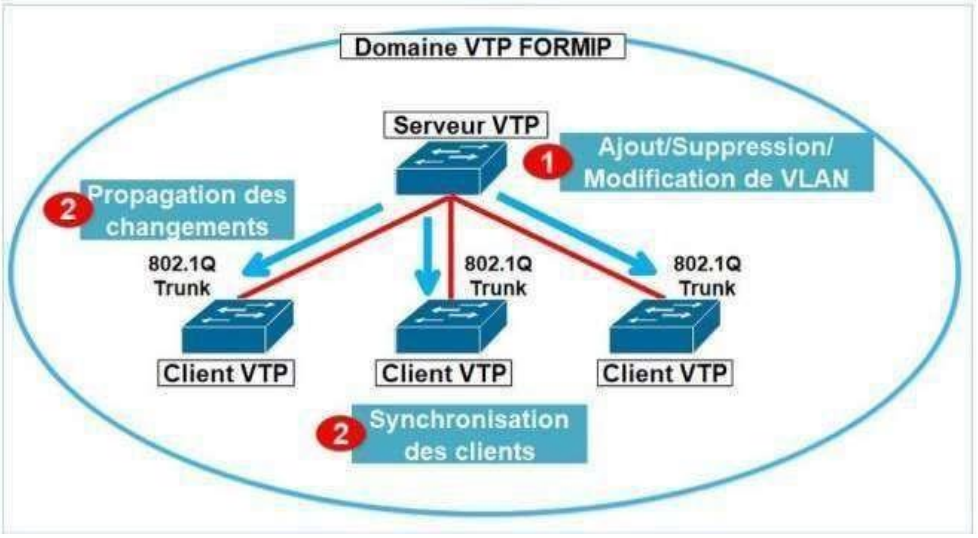


Figure II. 5: schéma du fonctionnement du protocole VTP.

II.3.2.2 HSRP (Hot Standby Router Protocol)

Le HSRP est un protocole Cisco propriétaire de la haute disponibilité accrue de la passerelle d'un réseau, implémenté pour la gestion des liens de secours. Il permet à plusieurs routeurs ou switches de niveau 3 de fonctionner comme une seule passerelle virtuelle. Le routeur actif envoie des messages de disponibilité, et en cas de panne, un routeur passif prend automatiquement le relais. Ce processus de réélection est invisible pour les utilisateurs, car ils continuent de voir la même IP et adresse MAC de la passerelle virtuelle. Cela garantit une continuité de service sans interruption perceptible du point de vue des hôtes du réseau [19].

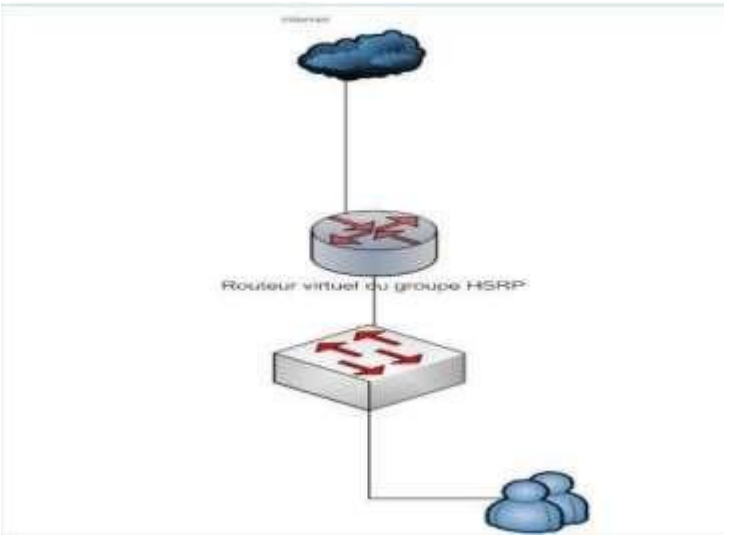


Figure II. 6: Schéma illustrant le protocole HSRP vue d'un hôte d'un réseau

L'état réel du réseau

Les routeurs physiques forment un routeur virtuel. Un des routeurs est en état actif et transmet les échanges alors que l'autre est en passif et reste à l'écoute de l'état de routeur actif prêt à prendre la relève.

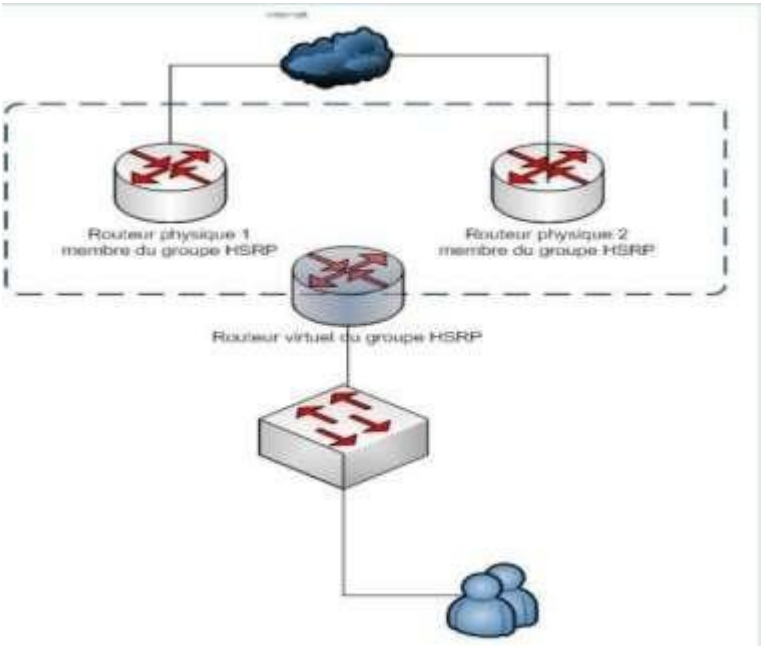


Figure II. 7: Schéma physique et virtuel d'un réseau HSRP

II.3.2.3 EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique appelé une agrégation de liens. Cette technologie a pour but d'augmenter la bande passante et d'assurer la redondance. Si une liaison échoue, le trafic est redistribué sur les autres liaisons actives.

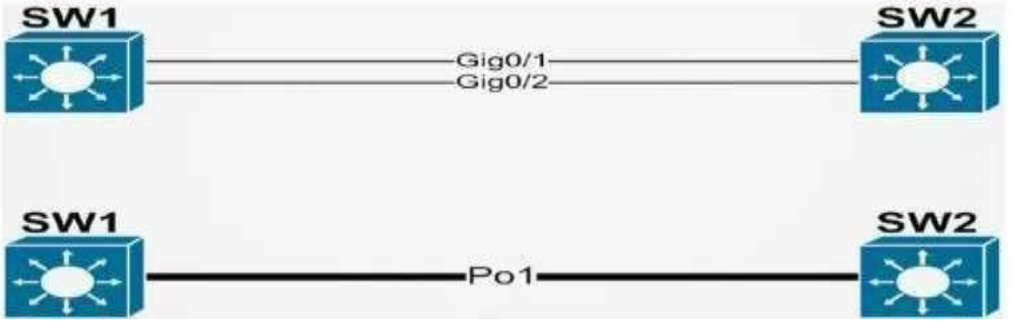


Figure II. 8: Schéma du fonctionnement EtherChannel.

II.3.2.4 STP (Spanning Tree Protocol)

Pour assurer la fiabilité des liaisons entre des commutateurs du réseau, la mise en œuvre d'une topologie de redondance est primordiale. Toutefois, si les commutateurs acheminent le trafic de diffusion et multicast par tous les ports sauf celui d'origine et si les trames Ethernet ne disposent pas de durée de vie (TTL) [20].

- ***Le fonctionnement du Spanning Tree Protocol (STP)***

Son fonctionnement repose sur la sélection d'un commutateur principal (Root) pourcommuniquer sa priorité et son adresse MAC. Le commutateur ayant la plus basseadresse MAC ou la plus haute priorité est élue comme Root Bridge calcul des chemins les plus courts vers ce commutateur. Les commutateurs peuvent passer par cinq états, incluant le "Blocking" qui arrête la transmission de données et le "Forwarding" qui la permet. STP échange régulièrement des BPDU (Bridge Protocol Data Unit) pour détecter et ajuster toute modification potentielle de la topologie afin d'éviter les boucles.

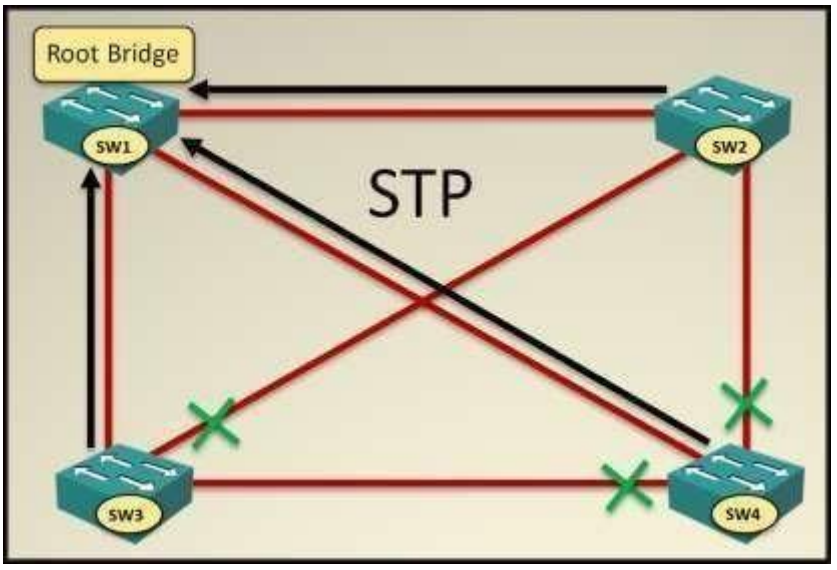


Figure II. 9 : Schéma du fonctionnement STP.

II.3.2.5 Le protocole de routage OSPF

Le protocole utilisé est l'OSPF (Open Shortest Path First), un protocole de routage à état de liens largement utilisé dans les réseaux d'entreprises. Il collecte les informations sur l'état des liens entre les routeurs du réseau pour construire une carte topologique. Contrairement à RIP, qui se base sur le nombre de sauts, OSPF utilise l'état des liaisons pour déterminer le chemin optimal, permettant une vue précise du réseau et des décisions de routage plus efficaces. OSPF améliore ainsi labande passante utile par rapport à RIP [21].

II.4 Schéma de la topologie réseau

Pour élaborer notre propre topologie, nous avons pris inspiration du réseau Cevital pour concevoir notre propre topologie, basée sur le modèle hiérarchique qui améliore la sécuritéet la fiabilité globales de notre architecture. Pour ce faire, nous avons décidé d'utiliser quatre chambres qui correspondent à des départements spécifiques de l'entreprise. Nous avons adopté une structure à deux couches, combinant la couche d'accès et la couche cœur. L'absence de la couche de distribution s'explique par la taille réduite de notre réseau, où la gestion du trafic et le routage sont directement assurés par la couche cœur, ce qui simplifie l'administration, réduit les coûts, et diminue lalatence.

De plus.Nous avons disposé également d'une zone démilitarisée (DMZ), qui est isolée du réseau principal en plaçant les serveurs AD, Ubuntu et serveur monitoring pour surveiller l'ensemble du réseau. En ce qui concerne la sécurité, nous avons mis en place un pare-feuconnecté au cloud afin de protéger le réseau contre les attaques externes. Cette architecturepermet de séparer les ressources et les applications en fonction de leurs besoin spécifiques, améliorant ainsi la sécurité et la fiabilité globales de notre réseau. Latopologie de cette infrastructure réseau est décrite dans la Figure II.10.

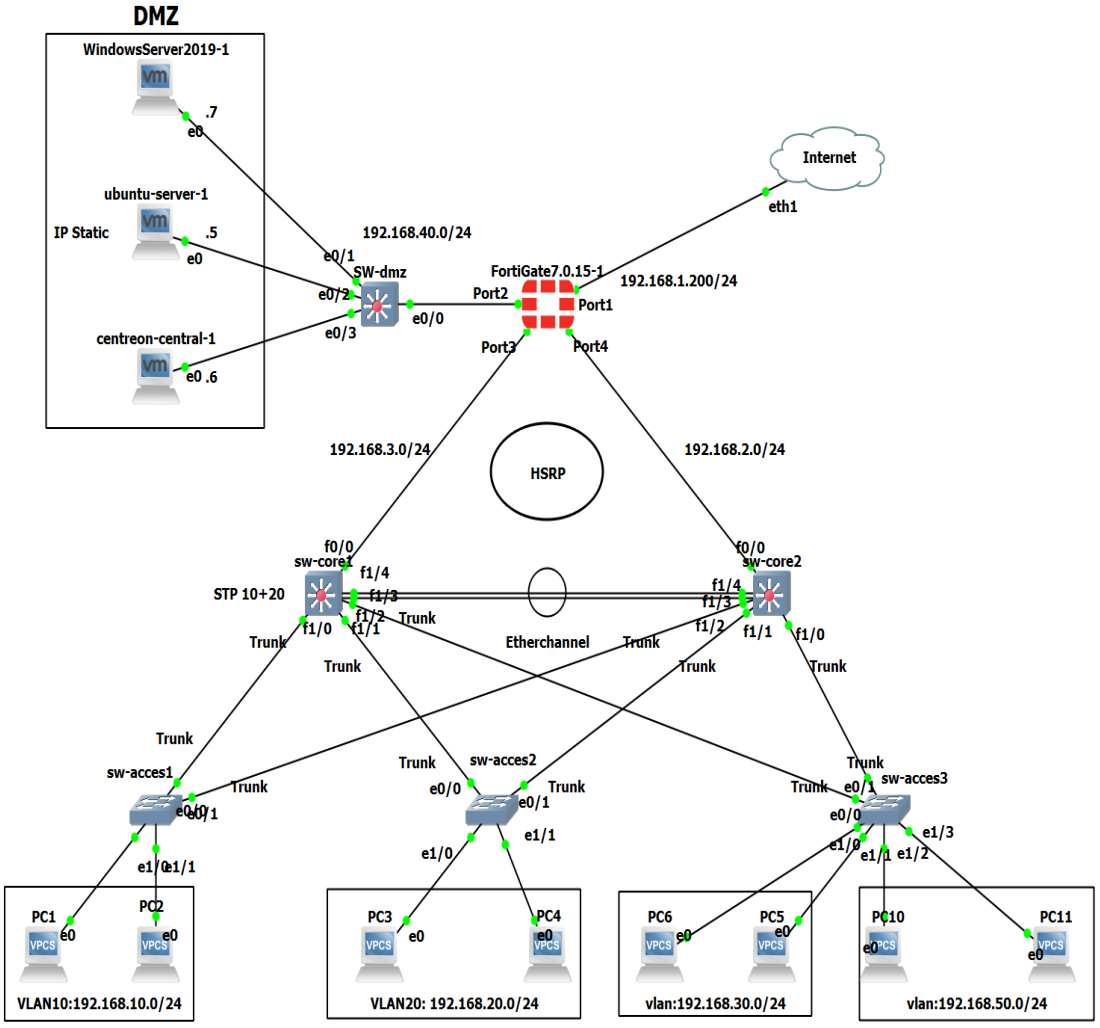


Figure II. 10 : Schéma réseau.

- ***Présentation de l'infrastructure réseau matérielle et logicielle***

	Equipements	**Le hardware (hard)**	**Software (soft)**
Couche cœur	Switch	Cisco Catalyst 3725	IOS (Internetwork Operating System)
	Pare-feu	FortiGate 7.0.15	Linux
	Server	SERVER_EVAL	Windows server 2019
	Server	Ubuntu-24.04	Linux
Couche accès	Switch	Cisco Catalyst 3725	IOS (Internetwork Operating System)
	Client	Hp	Windows 10

Tableau II. 1: L'environnement matériel et logiciel.

- ***Table d'adressage et liste des VLANs***

Le tableau II.2 présente la liste des VLAN utilisés dans le réseau du client :

Nom de VLANs	**ID de VLAN**	**Adresse du sous-réseau**	**Passerelle du sous-réseau**
Informatique	10	192.168.10.0/24	192.168.10.254
Système	20	192.168.20.0/24	192.168.20.254
Réseau	30	192.168.30.0/24	192.168.30.254
DMZ	40	192.168.40.0/24	192.168.40.254
Management	50	192.168.50.0/24	192.168.50.254
Native	1	…..	.....

Tableau II. 2: Table d'adressage des VLAN

.

- ***Plan d'adressage des équipements d'interconnexion***

Equipements	Interface réseau	Adresse IP
Pare-feu	External (WAN) DMZ Internal LAN1 Internal LAN2	 192.168.40.1/24 192.168.3.1/24 192.168.2.1/24
Server Windows 2019	DMZ	192.168.40.7/24
Server linux (Ubuntu)	DMZ	192.168.40.6/24
Server Centreon	DMZ	192.168.40.2/24
Sw-core1	Ethernet 0/0	192.168.3.2/24
Sw-core2	Ethernet 0/0	192.168.2.2/24
Sw-access1	Vlan 10 Info	192.168.10.0/24
Sw-access2	Vlan 20 Rh	192.168.20.0/24
Sw-access3	Vlan 30 finances Vlan 50 Management	192.168.30.0/24 192.168.50.0/24

Tableau II. 3: Table d'adressage des équipements d'interconnexion.

II.4.1 Avantage de l'infrastructure existant

Le modèle hiérarchique utilisé nous a permis de garantir les services suivants :

1. La performance

Dans notre schéma, la performance du réseau repose sur sa capacité à transmettre des données à une vitesse élevée et de manière fiable. Nous utilisons des switches de niveau 3 à haut débit, prenant en charge Gigabit Ethernet et des connexions 10 Gigabit. L'intégration de liens d'agrégation (EtherChannel) permet d'augmenter la bande passante disponible et d'assurer une redondance des connexions, de plus l'équilibrage de charge est possible entre les liaisons qui font partie d'un même EtherChannel. Des politiques de gestion de la bande passante et de qualité de service (QoS) sont mises en place pour prioriser le trafic critique. Ensemble, ces mesures assurent une qualité de service élevée, ce qui améliore la

satisfaction et la productivité des utilisateurs finaux.

2. Haute disponibilité

Dans notre architecture réseau, nous avons mis en œuvre plusieurs stratégies clés pour garantir une haute disponibilité telle que la redondance matérielle avec deux switches de niveau3 dans la couche cœur en utilisant le protocole HSRP pour assure la résistance du réseau : si l'un des switches tombe en panne, l'autre prend automatiquement le relais pour minimiser les temps d'arrêt et assurer une continuité opérationnelle et pour la gestion du trafic. De plus des liens d'agrégation via EtherChannel sont déployés pour agréger plusieurs liens physiques entre les switches de niveau 3 formant ainsi un lien logique unique pour assurer une continuité de service en cas de panne d'un équipement mais aussi et surtout, assurer un plus haut débit. En outre la redondance des liens entre la couche accèset la couche distribution/cœur (les boucles sont éliminées par stp).

La combinaison de ces mesures, assurant ainsi une expérience utilisateur optimale et sécurisée grâce à une disponibilité accrue des services.

3. Sécurité

Dans notre schéma réseau, la sécurité est assurée par des équipements de niveau 4, tels que le pare-feu FortiGate, qui contrôlent les flux de données entre le LAN, le WAN et la DMZ.

❖ ***Pare-feu***

- Le pare-feu FortiGate effectue une analyse approfondie de chaque paquet de données.
- Il met en place des dispositifs de sécurité pour bloquer les tentatives d'accès non autorisées au réseau.
- Il permet de mettre en place des politiques de sécurité particulières pour contrôler le trafic entre la DMZ, le LAN et le WAN, assurant ainsi une protection ciblée.

La segmentation du réseau en VLANs renforce la sécurité en isolant les différentes parties du réseau, ce qui limite la propagation des menaces

.

- Il offre des fonctionnalités de routage avancées telles que le routage inter VLAN et statique, ainsi que des services comme le DHCP et la haute disponibilité pour optimiser les performances du réseau.
- En surveillant le flux Internet, il identifie et prévient les risques externes pour assurer une protection complète du réseau.
- Segmentation des zones de sécurité.

❖ ***DMZ***

Dans notre réseau, la DMZ offre des avantages essentiels en matière de sécurité. Elle isole les services externes comme les serveurs, réduisant les risques de compromission des ressources internes sensibles. En contrôlant précisément les flux de données entre le réseau interne, les serveurs DMZ et l'Internet, la DMZ protège le cœur du réseau contre les menaces extérieures. De plus, elle simplifie la gestion des risques, améliore la supervision et permet une flexibilité accrue pour les services nécessitant un accès externe, tout en aidant à se conformer aux normes de sécurité.

❖ ***LAN***

Grâce à la mise en place du LAN, l'accès aux ressources réseau est restreint aux seuls utilisateurs autorisés, ce qui diminue les risques d'accès non autorisé aux données sensibles ou aux services essentiels.

❖ ***WAN***

Dans notre schéma réseau, le WAN offre plusieurs avantages essentiels. Il permet la connectivité avec l'extérieur, facilitant l'accès à Internet. Grâce à l'utilisation d'un pare-feu FortiGate, le WAN bénéficie d'une sécurité renforcée, avec des politiques de filtrage de trafic et une protection contre les menaces externes. De plus, le WAN assure une disponibilité élevée et une redondance des connexions, garantissant la continuité des services même en cas de défaillance. Enfin, il permet une gestion centralisée et un contrôleefficace des accès, améliorant ainsi la performance et la fiabilité du réseau global.

En segmentant le réseau en sous-réseaux distincts à l'aide de VLANs, le LAN aideà limiter la propagation des menaces en isolant les secteurs sensibles, réduisant ainsiles risques de compromission du réseau.

II.4.2 Inconvénients

- Supervision réseau difficile : surveillance des équipements individuellement

n'est pas applicable dans des réseaux à moyenne ou à grande envergure, ou étant sujette à un passage à l'échelle fréquent.

- Failles de sécurités potentielles : absence d'un système centralisé de supervision des activités réseau afin de détecter toute activité malveillante, ou comportement aberrant pouvant induire un risque de sécurité.

II.5 Problématique et la contribution de la solution proposée

II.5.1 Problématique

Pendant notre stage à Cevital de Béjaïa, nous avons observé que leur réseau comprenait de nombreux équipements complexes à gérer, configurer et surveiller individuellement et manuellement. Cette situation a entraîné plusieurs problèmes, tels que :

1. ***Difficulté d'accès aux données*** *:* Les administrateurs réseau doivent consulter plusieurs sources pour obtenir une vue complète du réseau et collecter d'informations sur son état, ce qui peut être chronophage et inefficace.

2. **Gestion inefficace des ressources :** Les ressources non surveillées peuvent soudainement atteindre des niveaux critiques, provoquant des interruptions de service ou des pannes qui auraient pu être évitées avec une surveillance proactive.
3. **Gestion des changements** *:* Superviser et gérer efficacement les modifications apportées à l'infrastructure réseau pour éviter les interruptions de service et garantir que les changements sont conformes aux politiques de sécurité et de performance.
4. **Gestion des incidents et des problèmes** *:* Mettre en place des processus efficaces pour la détection, la notification, l'escalade et la résolution des incidents réseaux afin de minimiser l'impact sur les utilisateurs et les opérations de l'entreprise.
5. **Risque accru d'erreurs** : La manipulation manuelle des données et l'intégration de sources disparates augmentent le risque d'erreurs, ce qui peut entraîner une mauvaise interprétation des données et des actions incorrectes.

II.5.2 Solution proposée

Après avoir identifié les défis liés à la gestion et à la configuration de notre infrastructure réseau, nous avons mis en place une solution de supervision en intégrant le serveur Centreon dans la DMZ. Cette décision stratégique nous permet d'isoler efficacement la surveillance et la gestion des performances réseau des serveurs sensibles de l'entreprise. En réduisant les risques de compromission, nous renforçons la sécurité tout en optimisant la disponibilité globale du réseau.

Le serveur Centreon surveille les configurations réseau, détecte les modifications non autorisées, et automatise la gestion des incidents, améliorant ainsi la réactivité des équipes et minimisant l'impact sur les utilisateurs. Notre approche utilise SNMP pour collecter en temps réel des données critiques (CPU, RAM, swap, ping, espace disque et le trafic réseau) de divers équipements (serveurs Ubuntu, Windows 2019, commutateurs, pare-feu FortiGate). Ces informations permettent de configurer des alertes basées sur des seuils prédéfinis, assurant une gestion proactive des performances et une réponse rapide aux incidents, garantissant la disponibilité et la sécurité des infrastructures essentielles.

II.6 Conclusion

En conclusion, après avoir présenté l'entreprise CEVITAL et défini une problématique précise, nous avons identifié plusieurs défis importants dans l'infrastructure réseau actuelle. Notre contribution s'articule autour de ces problématiques : surveiller les ressources de manière proactive, gérer les changements avec soin, optimiser l'équilibrage de la charge, et minimiser les erreurs humaines grâce à la supervision.

Ces éléments sont au cœur de notre solution, qui vise à améliorer de manière significative la disponibilité et les performances du réseau.

Chapitre III
Mise en place et fonctionnement du système de supervision

II.1 Introduction

Dans ce chapitre on va situer notre travail dans son cadre général, Nous commencerons par examiner l'environnement de travail et expliquerons comment installer nos solutions et on a abordé la simulation qui est la supervision avec Centreon des différents équipements du réseau. Nous allons d'abord voire comment créer un compte Centreon, puis comment ajouter les équipements à superviser. Enfin, nous configurerons des alertes Centreon avec le service Gmail pour être notifiés en cas d'anomalie.

III.2 Environnement de travail

III.2.1 GNS3

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

III.2.2 VMware

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

III 2.2.1 Les machine virtuelle (Les systèmes d'exploitation utilisés)

1. Le serveur Active Directory

Après l'installation de VMware Workstation 17 Pro, les données concernant les comptes d'utilisateurs, telles que les noms et les mots de passe, sont conservées. Lamise en place du système d'exploitation Windows Server est prévue. Afin de créercette nouvelle machine virtuelle, nous allons ouvrir VMWare et sélectionner le bouton "Nouvelle machine virtuelle" dans le menu "Fichier". Puis, nous allons continuer jusqu'à ce que nous ayons terminé l'installation. On atteint la fenêtre.

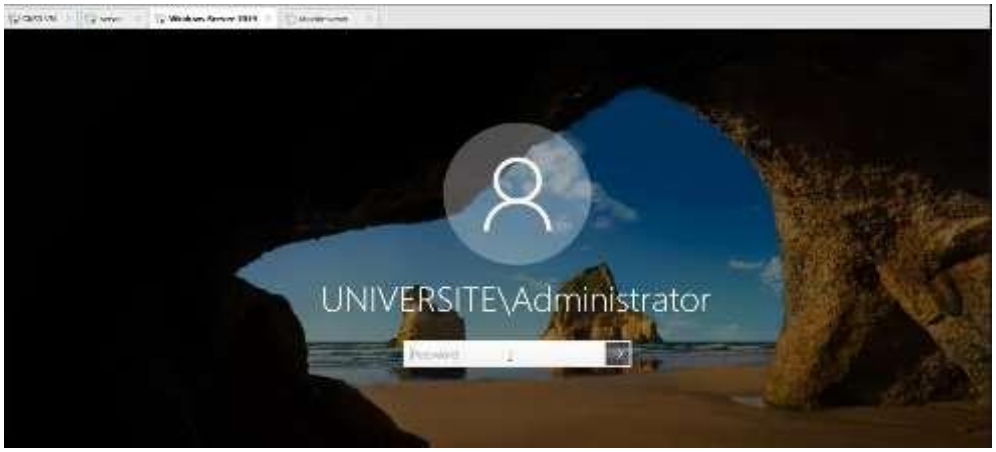


Figure III. 1: La page d'accueil de Windows 2019

2. Le serveur Ubuntu

Ubuntu est un système d'exploitation Linux populaire pour sa stabilité, sa sécurité et sa facilité d'utilisation. Distribué en tant que logiciel libre et open source, qui est largement utilisé pour l'hébergement web, les bases de données, les serveurs de fichiers, les applications d'entreprise.

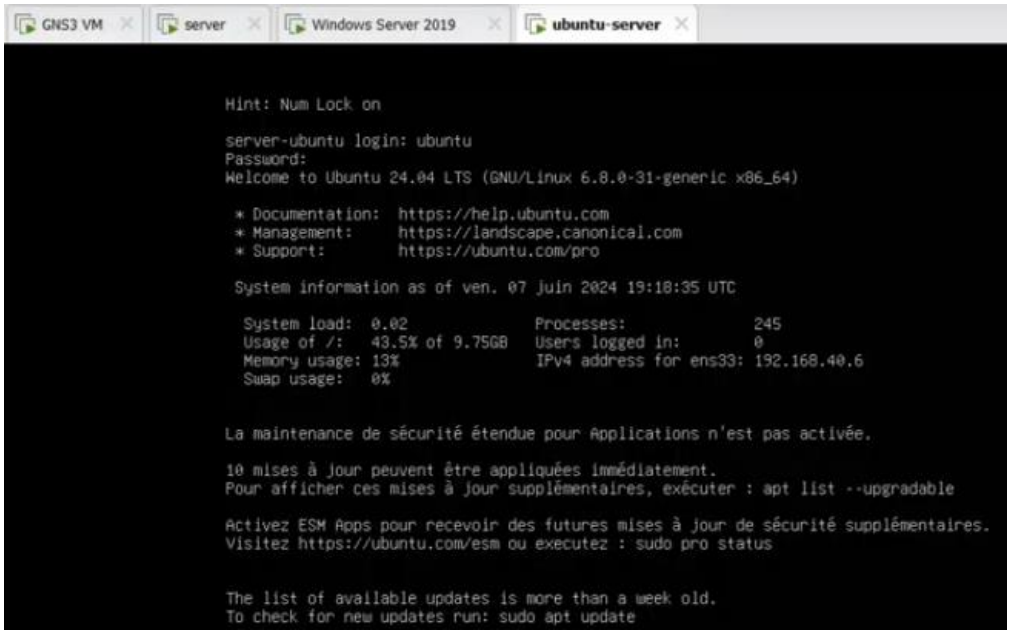


Figure III. 2 : La page d'accueil d'Ubuntu server 24.04

3. Serveur de supervision

Dans la troisième machine virtuelle, nous avons trouvé un système d'exploitation Alma Linux, un système basé sur Linux connu pour sa stabilité, sa sécurité et sa robustesse. Cette machine, déjà configurée, sera utilisée comme serveur de supervision, sur laquelle est installé l'outil de supervision Centreon.

III .3 Installation d'outil Centreon

Centreon propose une machine virtuelle prête à l'emploi au format OVA pour les environnements VMware. Cette machine virtuelle est préconfigurée avec Linux et inclut une installation complète de Centreon, permettant de démarrer rapidement et facilement la supervision de votre infrastructure. Obtenez le fichier OVA de Centreon depuis le site officiel de Centreon.

1. Assurez-vous que votre solution de virtualisation (VMWare) est installée sur votre machine est à jour.

2. Accédez à la page de téléchargement de Centreon. Dans la section 1, la catégorie "Appliance est sélectionnée par défaut.
3. Dans la section 2, sélectionnez la version de Centreon souhaitée.
4. Dans la section 3, cliquez sur le bouton "Download" à côté de "VMWare Virtual Machine (OVA)". Une nouvelle page apparaîtra.
5. Importez le fichier centreon-central.ova dans VMWare (Virtual Machine). Un terminal s'ouvre : attendez le démarrage du serveur. Quand le terminal est prêt, il affiche le message suivant :

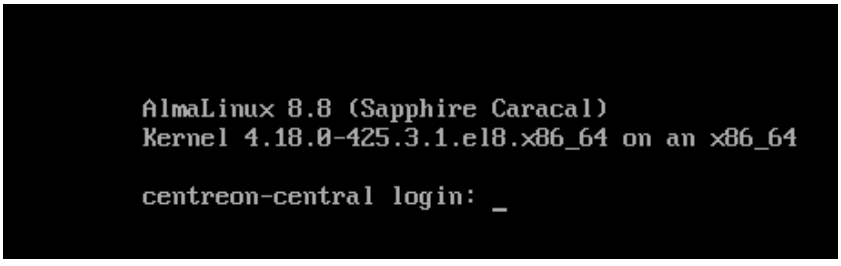


Figure III. 3 : Écran de Connexion du Serveur Centreon-Central sur VMWare

6. Selon la structure de votre réseau, ajoutez un adaptateur réseau à la configuration de votre machine virtuelle et sélectionnez le réseau permettant à la machine de communiquer avec les ressources qu'elle doit superviser.

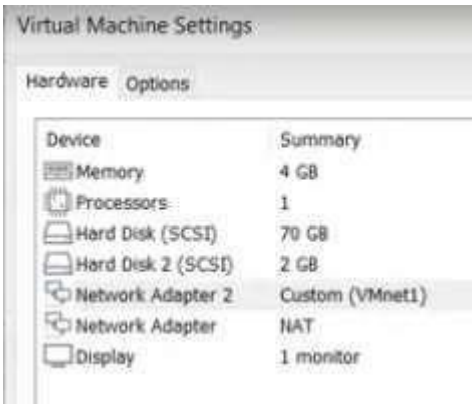


Figure III. 4: Écran de Connexion du Serveur Centreon-Central sur VMWare

Pour finaliser la configuration on doit :

7. Connectez-vous au serveur Centreon en utilisant les informations suivantes : login : root, mot de passe : Centreon !123
8. Pour connaître l'adresse IP de votre serveur, tapez la commande : « ip addr. ».

```
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5b:29:6e brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 192.168.40.6/24 brd 192.168.40.255 scope global noprefixroute ens32
       valid_lft forever preferred_lft forever
    inet6 fe80::effd:cdcb:a50a:5ef6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]# _
```

Figure III. 5: Affichage du l'adresse IP du serveur

9. Connectez-vous-en tant que root au serveur depuis une autre machine en utilisant le terminal de votre choix, en entrant l'adresse IP obtenue précédemment.
10. Lors de votre première connexion au serveur, des instructions apparaîtront pour vous guider dans la finalisation de la configuration.

Figure III. 6: Écran d'Instructions pour la Configuration du Serveur

11. Accédez à l'interface web en entrant l'adresse du serveur dans votre navigateur au format http://adresse_ip/centreon ou http://FQDN/centreon, (http://192.168.40.6/centreon)

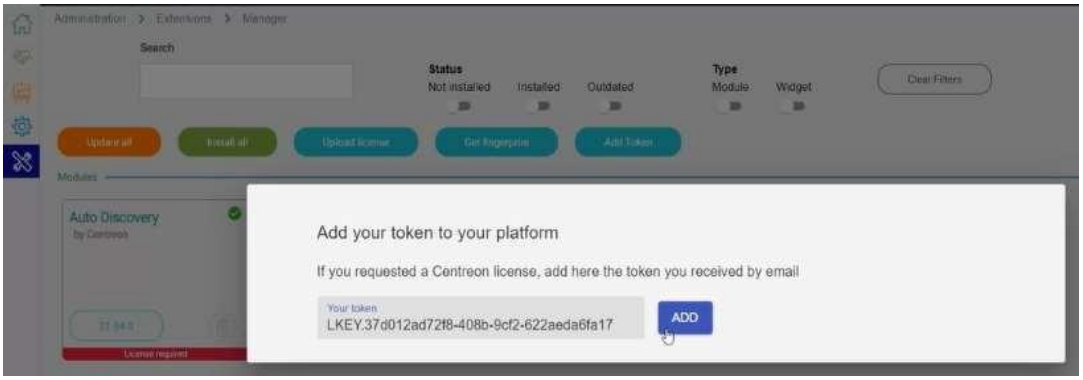
12. Connectez-vous en utilisant les identifiants suivants : Login : admin, Password : centreon. Par défaut, votre serveur est préconfiguré pour s'auto-superviser.

III. 4 Simulation avec Centreon

Pour configurer Centreon, il est essentiel d'utiliser un Token d'authentification. Ce Token sert de clé de sécurité, permettant à l'utilisateur d'établir une connexion sécurisée avec l'interface de Centreon. Ce Token est utilisé pour l'installation et la configuration des plugins, qui étendent les capacités de surveillance de Centreon. Ensuite utilisé lors des opérations d'intégration et de configuration des hôtes et services, garantissant que seules les requêtes autorisées peuvent interagir avec le système.

1. Ajouter une licence

Pour obtenir ce Token, vous devez d'abord vous connecter à l'interface web de Centreon avec un compte disposant des droits administratifs. Une fois connecté, naviguez vers le menu de gestion des API pour générer un nouveau Token (**Administration > Extensions >Manager et** cliquez sur le bouton **Add Token**).



.**Figure III. 7:** L'Ajout d'une licence.

2. Plugin Pack

Un Plugin Pack (ou pack de supervision en français) est un jeu téléchargeable de modèles de configuration qui permet un déploiement rapide de la supervision de notre infrastructure IT. Les Plugin Packs sont le moyen le plus simple de mettre un hôte en supervision. Est constitué de deux éléments, installés séparément :

• Un plugin, qui exécute les commandes de supervision depuis un collecteur. Il est installé en ligne de commande.

• Un pack, qui contient des commandes, des modèles de services et des modèles d'hôtes. Il est installé via l'interface de Centreon. Pour chaque type d'équipement, Les modèles déterminent quels indicateurs seront supervisés et définissent les valeurs par défaut des seuils Warning et Critical.

Figure III. 8: Plugins Packs Manger.

III 4.1 Gestion des comptes Centreon

La gestion des utilisateurs dans Centreon est essentielle pour garantir la sécurité, laconformité et l'efficacité de la supervision réseau. Lorsqu'un utilisateur se connecte,il doit fournir ses informations d'identification pour accéder à son compte. Les rôles des utilisateurs peuvent être variés, chacun ayant des autorisations spécifiques qui déterminent leur accès et leurs capacités au sein de la plateforme, tels que : administrateur système, utilisateur avancé, utilisateur standard.

Pour cela nous allons suivre les étapes suivant afin de crée un compte administrateur qui possède tous les droits en lecture-écriture.

1. Création d'un compte administrateur avec le nom 'Superviseur'

Pour créer un compte administrateur sur Centreon, allez à la page **Configuration > Utilisateurs > Contacts/Utilisateurs**, puis cliquez sur **Add**. Suivant les étapes illustrées dans la figure III.9 :

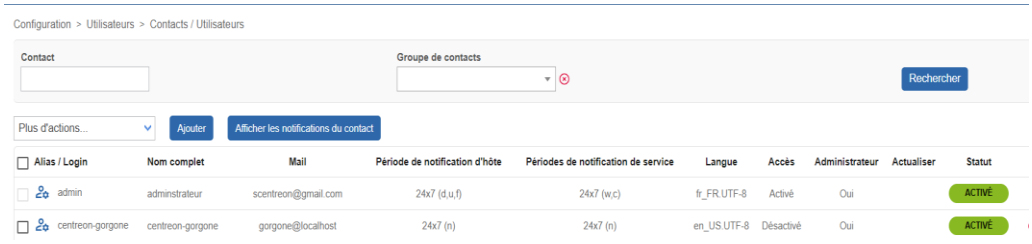


Figure III. 9: création d'un compte admin sur Centreon.

- ***Remplir les informations du compte***

Dans le premier onglet General Information renseigné : Votre pseudo (Alias), qui sera utilisé pour se connecter à l'interface web Centreon dans, votre nom complet, adresse mail via le champ Email.

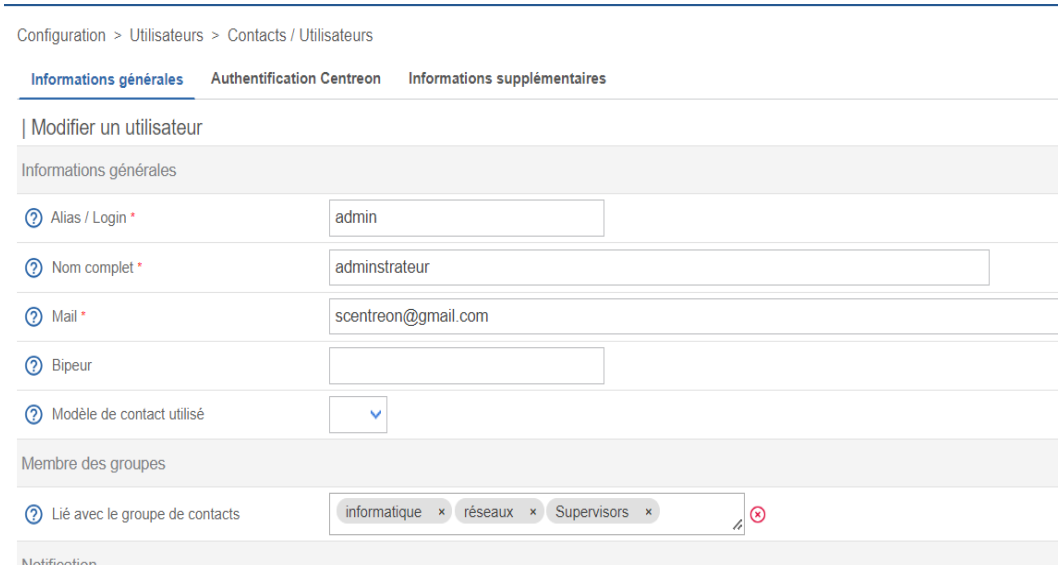


Figure III. 10 : Remplissage des informations d'utilisateur.

2. *Sélectionner le rôle d'utilisateur*

Dans cette partie on va présenter les actions accordées à l'utilisateur administrateur

- Sur les ressources : quels hôtes, services, etc. l'utilisateur aura le droit de voir
- Sur les menus de l'interface Centreon (à quelles pages il pourra accéder)
- Sur les actions que l'utilisateur pourra réaliser sur les ressources ou sur un moteur de supervision (mettre une ressource en maintenance, exporter la configuration...).

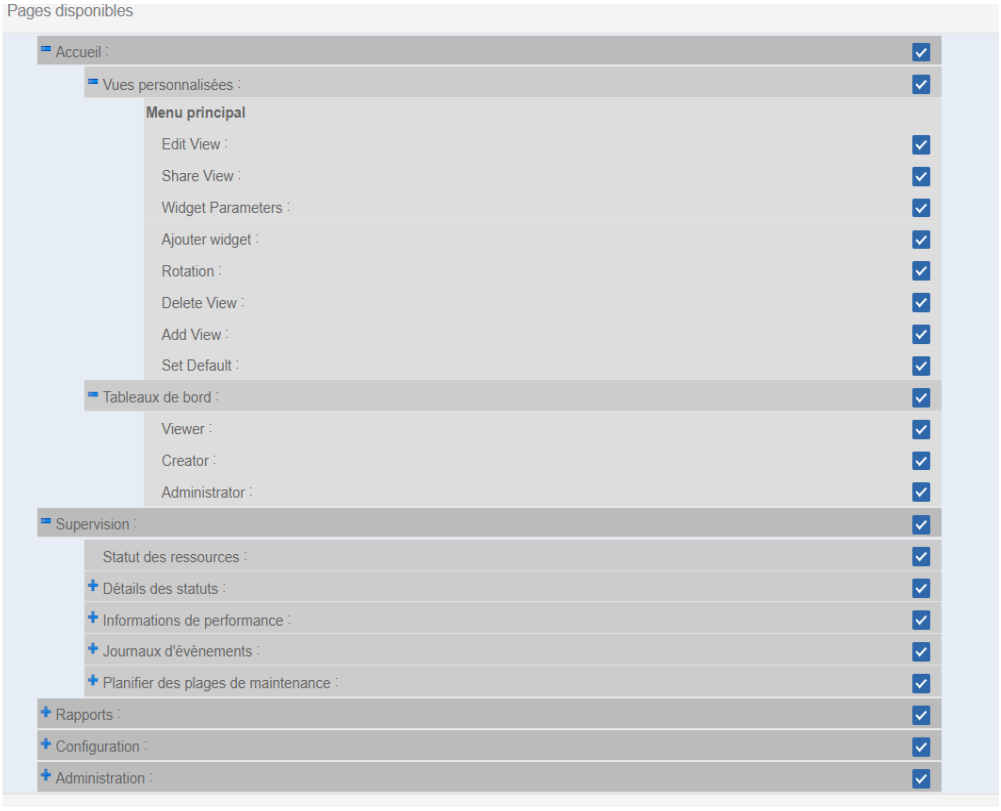


Figure III. 11 : les permissions accordées à l'utilisateur.

III 4.2 Configuration des hôtes

Un hôte est toute entité possédant une adresse IP correspondant à une ressourcedu système d'informations, telle qu'un serveur, une imprimante réseau, un serveurNAS, une base de données, une sonde de température ou une caméra IP, etc.

- Pour ajouter un hôte, connectez-vous d'abord à l'interface web de Centreon avec un compte administrateur ou un compte disposant des droits nécessaires pour gérer les objets. Ensuite, allez dans le menu **Configuration > Hosts > Hosts** et cliquez sur le bouton Add.

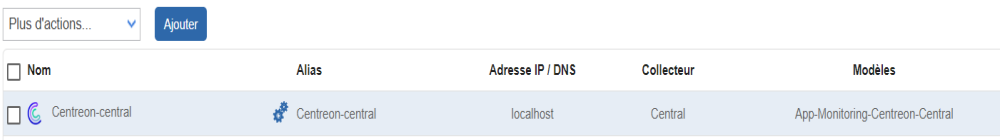


Figure III. 12: supervision du serveur Centreon.

III 4.2.1 Ajouter un serveur Windows server 2019

Pour ajouter le serveur Windows à Centreon, on doit installer et configurer le service SNMP sur le serveur.

1) Installer le service SNMP sur le serveur Windows

Pour installer le service SNMP, on suit les étapes illustrées dans les figures suivantes : D'abord on clique sur "Ajouter des rôles et des fonctionnalités" sur le serveur Windows.

On accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs de la figure, puis on clique sur bouton Save :

Pour ajouter le serveur Windows à Centreon, on doit installer et configurer le service SNMP sur le serveur.

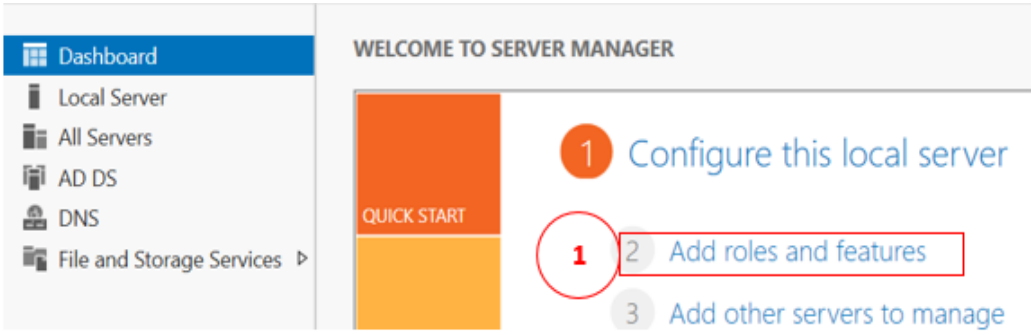


Figure III. 13: Gestionnaire de serveur.

Ensuite on sélectionne notre serveur avec son adresse IP (192.168.40.7) et on clique sur "Suivant".

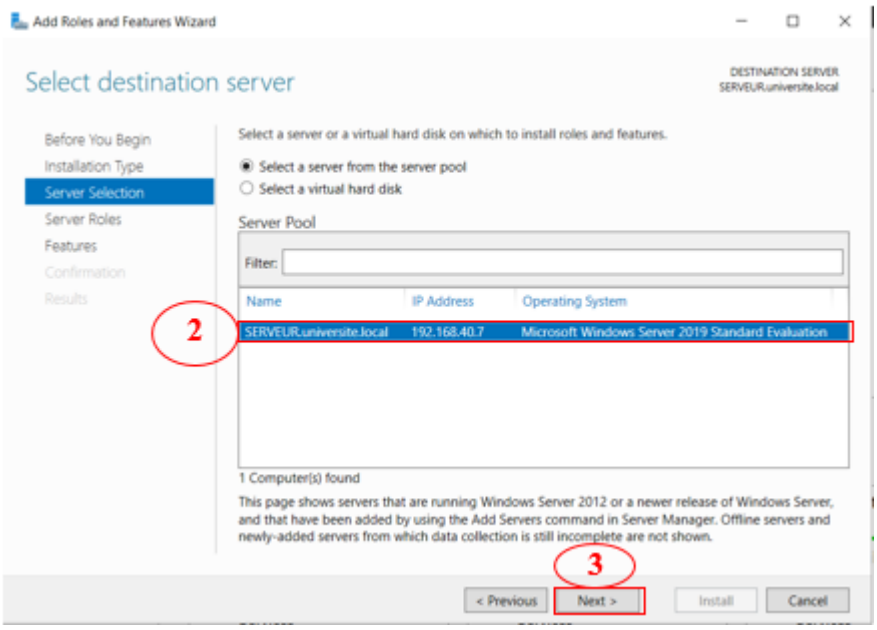


Figure III. 14: Sélectionner le serveur de destination.

On coche la case "SNMP Server" dans la liste des fonctionnalités à installer, puis on clique sur Enfin, on clique sur "Installer" pour commencer l'installation du service SNMP.,

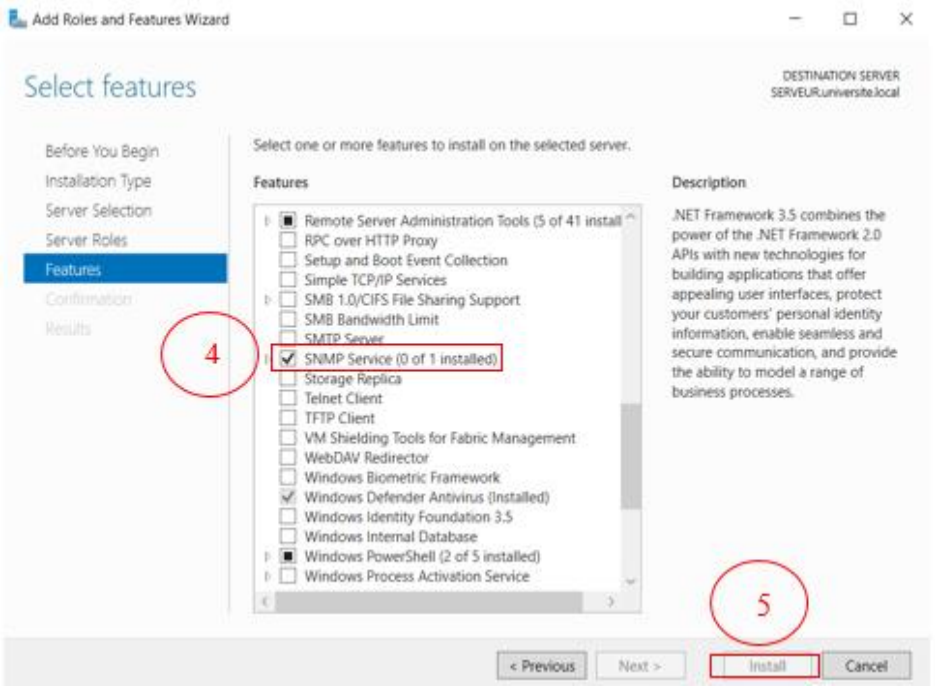


Figure III. 15: Sélectionner le service à installer.

2) Configuration du service SNMP sur le serveur Windows 2019

Après l'installation du service SNMP, il est nécessaire de le configurer. Pour cela,

dans le tableau de bord, on accède à l'option « Outils » puis on sélectionne « Services ». Une fois la fenêtre des services ouverte, on recherche le service SNMP. Voir la figure III.16.

Après ça on effectue un clic droit sur ce service et on choisit l'option « Propriétés »

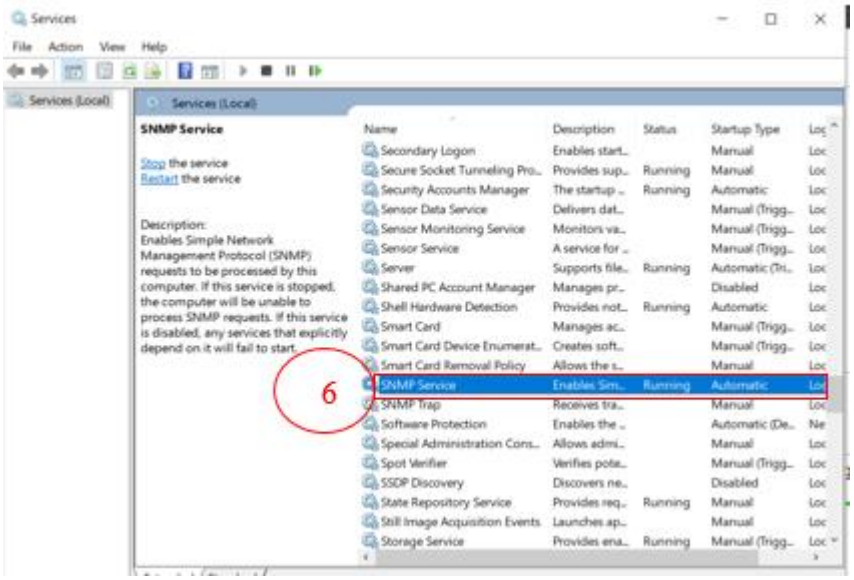


Figure III. 16: Modifier le service SNMP

Ensuite, on accède à l'onglet « Agent SNMP » où on peut renseigner les informations de contact, d'emplacement et de service liées au service SNMP. Voir la figure III.17

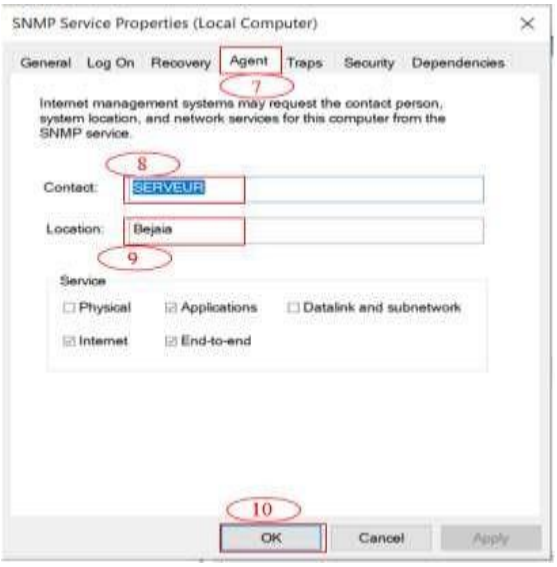


Figure III. 17: Configuration de l'agent SNMP

3) Création d'un hôte et Association de la Template importé au serveur Windows2019

Pour ajouter un serveur Windows à Centreon, commencez par télécharger la Template correspondante directement depuis Centreon. Une fois la Template téléchargée, accédez au menu pour ajouter un nouvel hôte Windows. Dans la configuration générale de l'hôte, remplissez les champs requis : donnez un nom unique à votre hôte, un alias pour une meilleure lisibilité, et entrez l'adresse IP ou le nom DNS de votre serveur Windows. Sélectionnez ensuite la Template Windows que nous avons téléchargée.

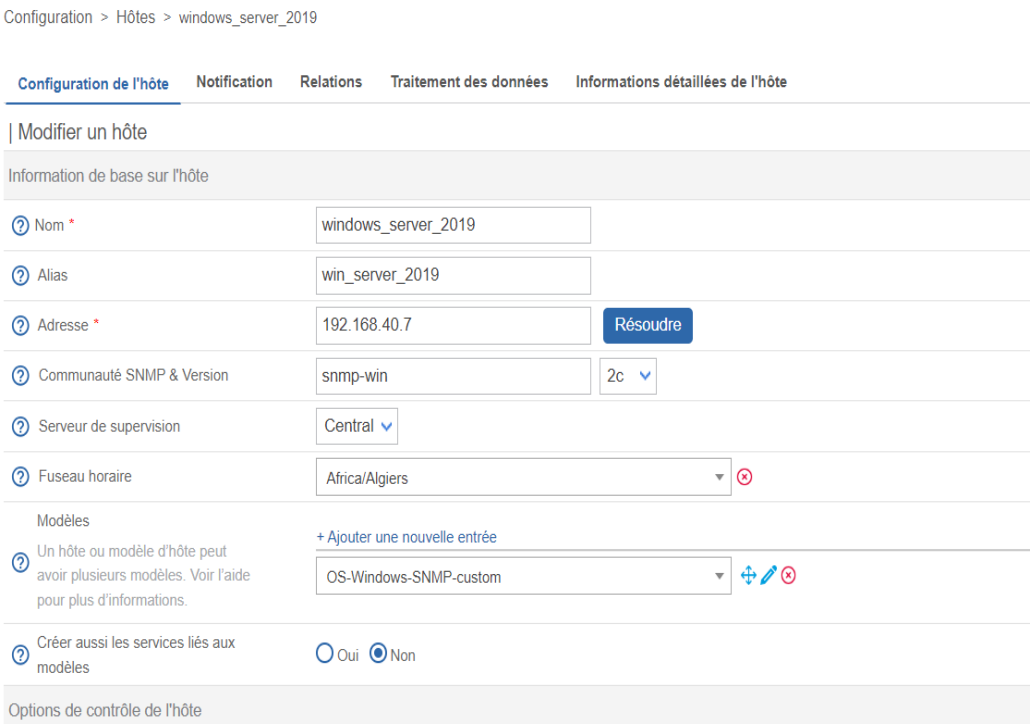


Figure III. 18 : Configuration de l'agent SNMP Ajouter le serveur Windows

.

III 4.2.2 Ajouter le pare-feu FortiGate (FG)

Avant d'ajouter un nouvel hôte sur Centreon, il est nécessaire de procéder à l'ajoutdu modèle (Template) FortiGate. Étant donné que Centreon ne dispose pas de modèles pour tous les équipements, il est indispensable de télécharger ce modèle à partir du site officiel de FortiGate. Les modèles, comme nous l'avons déjà mentionnéprécédemment, sont utilisés pour surveiller différents types de services et

d'applications. Ils contiennent des éléments de surveillance tels que des seuils de déclenchement, des graphiques et des alertes, etc.

1) Télécharger et importer la Template sur Centreon

D'abord il faut accéder au site officiel de Centreon, Ensuite, on recherche la Template spécifique à FortiGate prenant en charge SNMP, Dans notre cas, on recommande la version "Net-fortinet-fortigate_snmp_custom". Voire la figure III.19

Une fois qu'on a identifié la bonne Template, on la télécharge depuis le site officiel de Centreon. Cette Template inclut les configurations prédéfinies nécessaires pour surveiller et collecter les données du pare-feu FortiGate, telles que les seuils de déclenchement, les graphiques et les alertes.

Figure III. 19: Importation du plugin Fortinet.

2) Configuration du protocole SNMP au niveau du pare-feu FortiGate

FortiGate est dispose d'une interface web qui simplifie considérablement les configurations. Afin de mettre en place le protocole SNMP, il est nécessaire d'accéder sur cette interface et de suivre les étapes présentées dans les figures III.20 et III.21

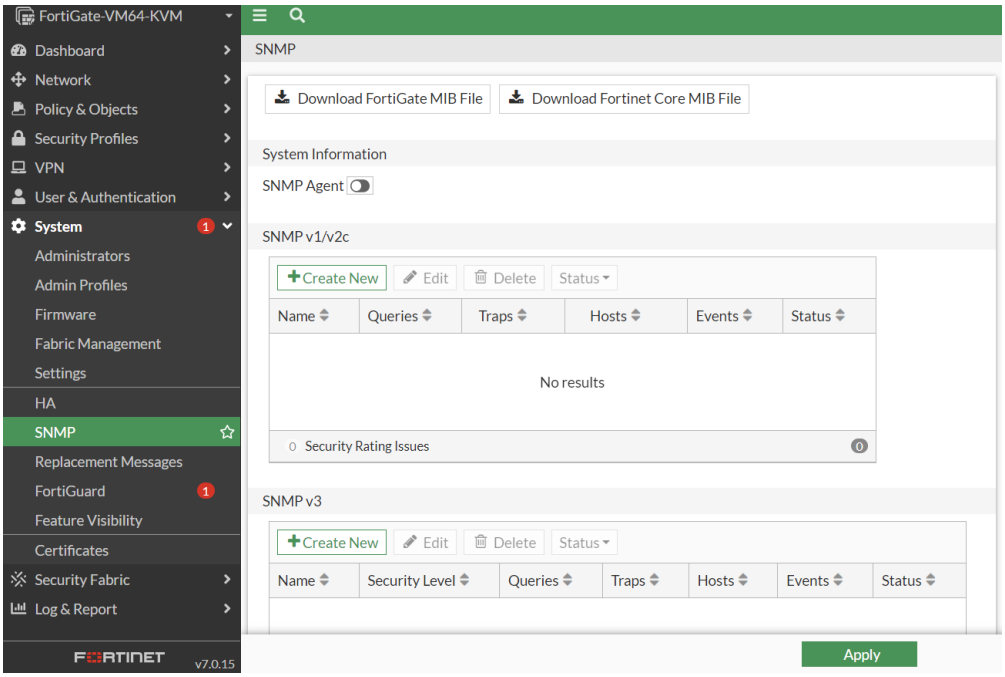


Figure III. 20: Interface Web FortiGate

.

Une fois à l'intérieur de l'interface du FortiGate, nous accédons à la section SNMP et procédonsà la configuration du protocole. Voire la figure III.21

Tout d'abord, nous activons l'agent SNMP en cochant l'option correspondante. Ensuite, nous créons une nouvelle configuration SNMP en fournissant les informations nécessaires. Dans notre cas, nous cochons la version 2 et définissons la communauté SNMP comme "snmp-fg". Il est également important de spécifier l'adresse IP du serveur Centreon pour indiquer où les données SNMP doivent être envoyées. Enfin, nous enregistrons les configurations en cliquant sur le bouton "Appliquer". Ainsi, l'agent SNMP est activé sur le FortiGate et la nouvelle configuration est mise en place, permettant à Centreon de collecter les données de performanceet de surveillance de manière appropriée.

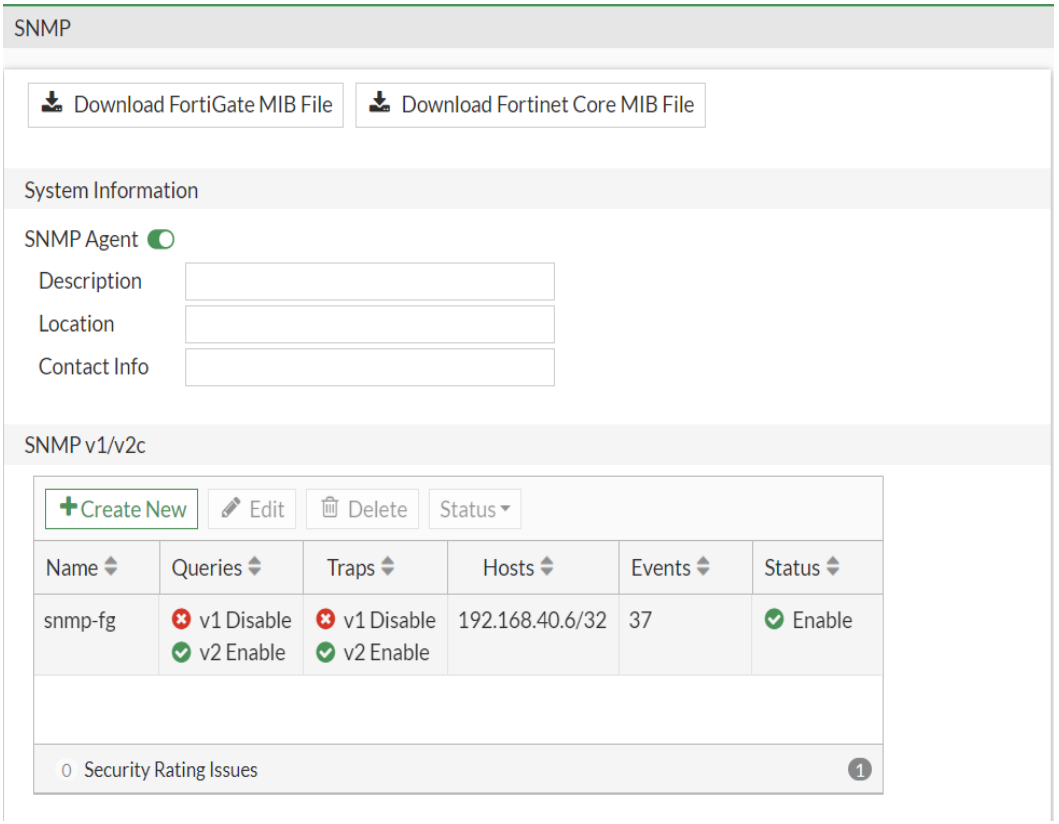


Figure III. 21 : Interface Web FortiGate

3) Création d'un hôte et Association de la Template importé au pare-feu FortiGate

L'étape suivante consiste à associer la Template importée au pare-feu FortiGate afin de commencer la surveillance et l'analyse des performances de notre équipement. Pour cela, nous devons créer un nouvel hôte en suivant la même procédure que pour les équipements Précédents. Ensuite, dans la configuration de l'hôte, nous sélectionnons le modèle (la Template importée) comme illustré dans la figure III.22.

Après avoir configuré le protocole SNMP sur Centreon et sur le pare-feu, on constate que le pare-feu a été ajouté avec succès à Centreon, sans aucun problème.

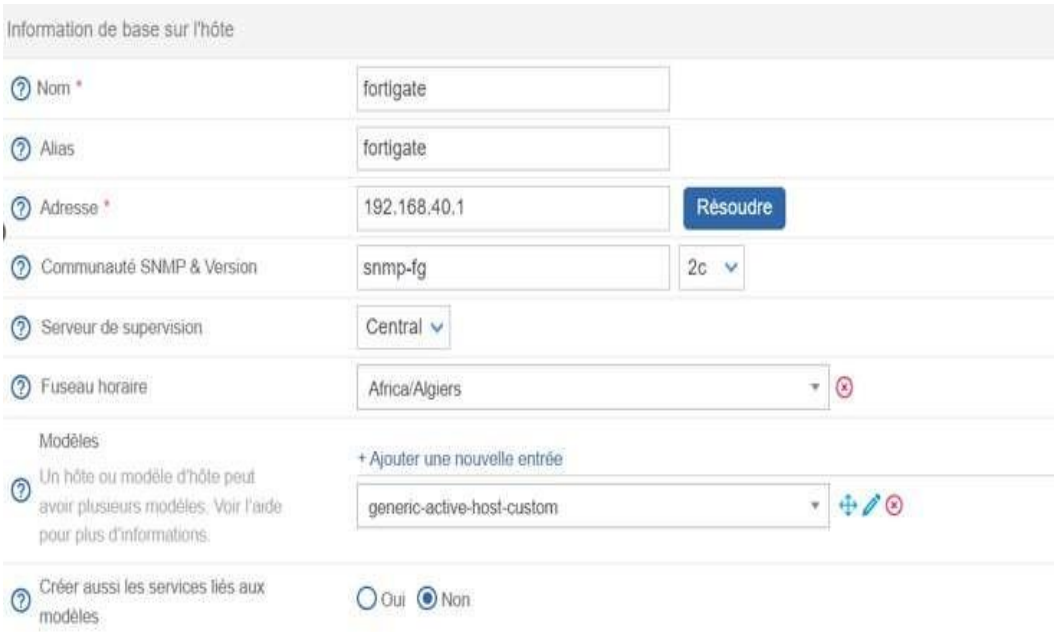


Figure III. 22: Configuration de FortiGate.

III 4.2.3 Ajouter un serveur Linux (Ubuntu)

1) Sur le serveur Linux

La première étape consiste à L'installation du service SNMP, elle se fait depuis la ligne de commande :

La deuxième étape consiste à activer et à configurer l'agent SNMP sur l'hôte à superviser, le service SNMP est configuré via le fichier **/etc/snmp/snmpd.conf**. Afin de pouvoir surveiller notre serveur Ubuntu :

- Remplacez la ligne agent adresse par l'adresse IP de l'interface sur laquelle snmpd doit écouter
- Remplacez my-snmp-community par la valeur correspondant à votre environnement.
- Ajoutez la ligne view centreon included .1.3.6.1 pour avoir accès à toutes les informations de la MIB requises par le plugin

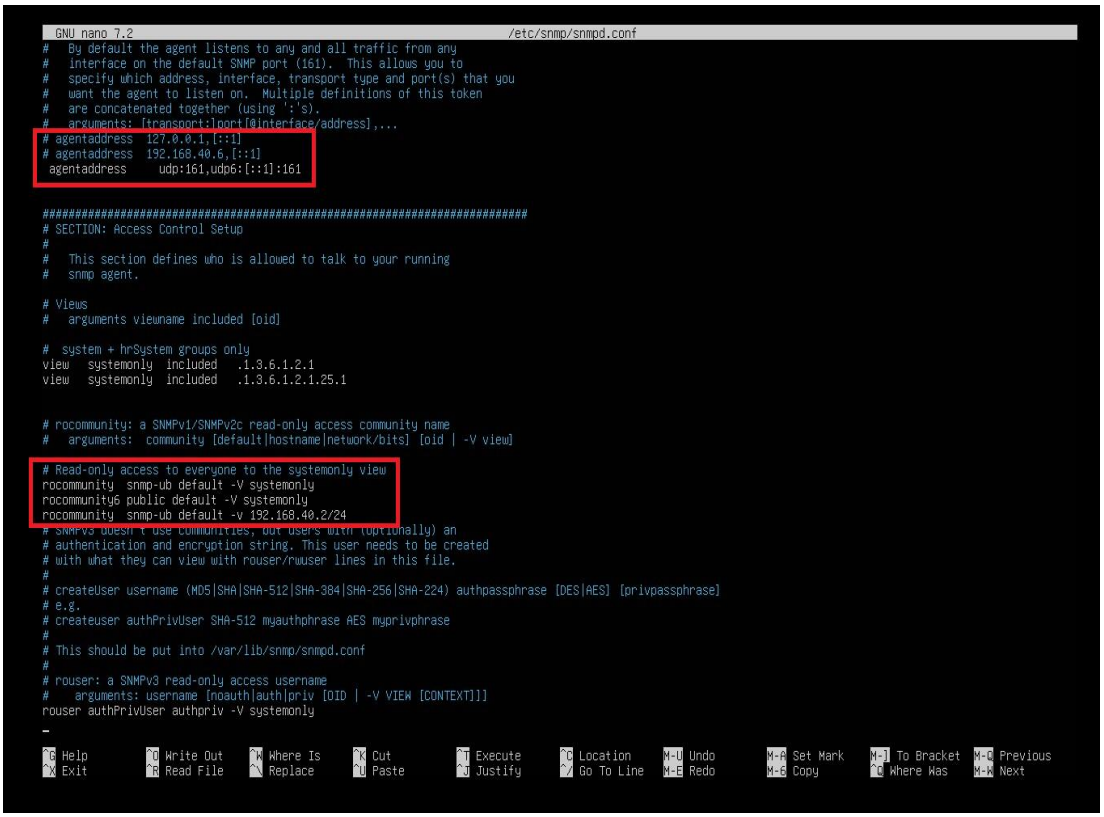


Figure III. 23 : Configuration SNMP sur Ubuntu.

1) Sur le serveur central

Dans l'interface web, allez à la page Configuration >Plugin packs et installez le connecteur de supervision Linux SNMP

Figure III. 24 : Importation du plugin linux**.**

1) Configurer l'hôte et déployer la configuration

Sur la page **Configuration > Hôtes > Hôtes** et cliquez sur **Ajouter**

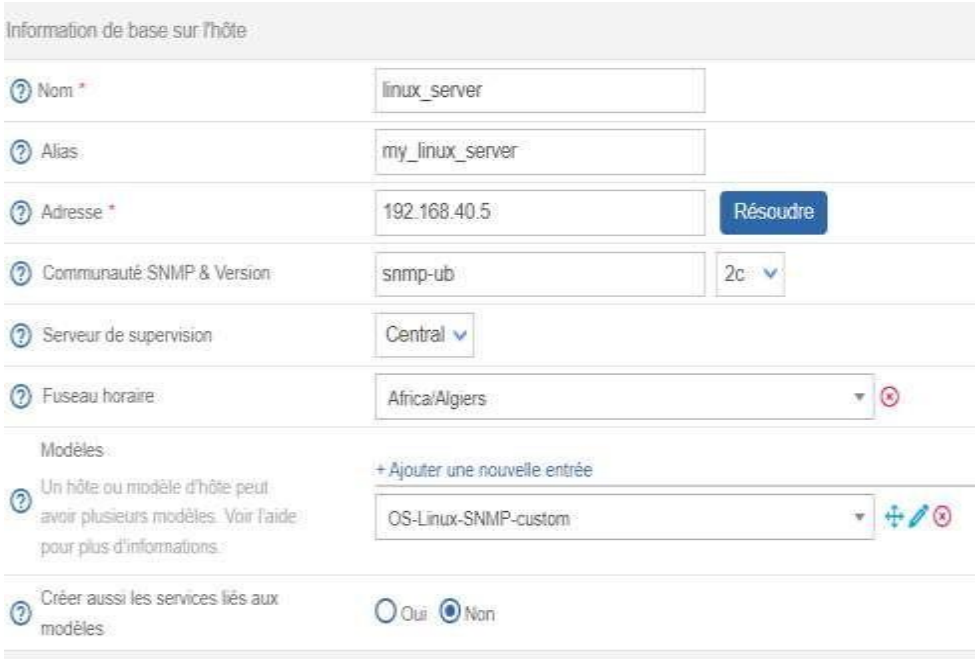


Figure III. 25: Configuration de serveur Ubuntu

III 4.2.4 Ajouter un switch (commutateur)

Le commutateur Core est le premier à inclure. Il sera expliqué en détail. Le principe sera identique pour les autres commutateurs. Ainsi, nous n'avons pas besoin de préciser leur configuration pour éviter de rendre cette partie trop longue et d'éviter de l'épuiser.

1) Sur le commutateur

- ***Configuration du commutateur Core avec une adresse IP***

Les adresses IP des commutateurs. Voire la Figure III.26.

```
sw-core1(config)#interface vlan 1
sw-core1(config-if)#ip addre 192.168.40.8 255.255.255.0
sw-core1(config-if)#end
sw-core1#c
*Sep  9 12:31:52.228: %SYS-5-CONFIG_I: Configured from console
sw-core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core1(config)#ip default-gat
sw-core1(config)#ip default-gateway 192.168.40.1
sw-core1(config)#end
```

Figure III. 26 : Configuration du commutateur Core avec une adresse IP

- ***Configuration du protocole SNMP au niveau des Commutateurs (Core)***

La configuration du SNMP sur un commutateur implique plusieurs étapes :

1. Activation du SNMP : Le service SNMP est activé sur le commutateur en utilisant la Commande « snmp-server ».
2. Communautés SNMP : Les communautés SNMP sont configurées pour permettre l'accès au commutateur avec une valeur (mot de passe partagé). On définit une communauté en lecture seule (read-only) ou une communauté en lecture/écriture (read-write). Dans notre cas, nous utilisons le mot de passe partagé « snmp-core1 » entre le serveur et le commutateur Core.
3. Niveaux d'accès SNMP : Les niveaux d'accès SNMP sont définis pour spécifier les permissions. Nous configurons la communauté SNMP en mode « RO » (read-only) pour permettre uniquement la récupération d'informations.
4. Adresses IP autorisées : Les adresses IP autorisées à accéder au commutateur via SNMP sont spécifiées pour des raisons de sécurité. Dans notre cas, nous autorisons l'adresse IP de notre serveur de supervision Centreon, avec l'adresse IP 192.168.40.6
5. La version SNMP : L'utilisation de la version SNMP appropriée garantit une compatibilité optimale avec les systèmes de gestion de réseau et permet une communication efficace entre le commutateur et le serveur de supervision. Dans notre cas nous utilisons la « version 2C ».
6. Activation des traps SNMP : Pour recevoir des notifications d'événements importants du commutateur, il est nécessaire d'activer les traps SNMP. La

commande utilisée pour cela est «snmp-server enable traps ». Voici la figure qui résume toute la configuration.

```
sw-core1(config)#snmp-server community snmp-core1 ro
sw-core1(config)#snmp-server host 192.168.40.6 version 2c snmp-core1
sw-core1(config)#snmp-server enable traps
sw-core1(config)#end
sw-core1#wr
*Sep  9 12:40:00.916: %SYS-5-CONFIG_I: Configured from console by console
sw-core1#wr
Building configuration...
Compressed configuration from 4126 bytes to 1909 bytes[OK]
sw-core1#
```

Figure III. 27: Configuration du protocole SNMP sur le commutateur Core.

2) Sur serveur Centreon

Dans l'interface web, allez à la page **Configuration >Plugin-pack**, recherchez et installez le connecteur de supervision **Cisco standard**

Figure III. 28: Importation plugin Cisco standard

.

Après avoir configuré le commutateur et le serveur Centreon, pouvons effectuer un test de ping depuis le serveur Centreon vers le commutateur Core pour s'assurer que tout est correctement connecté.

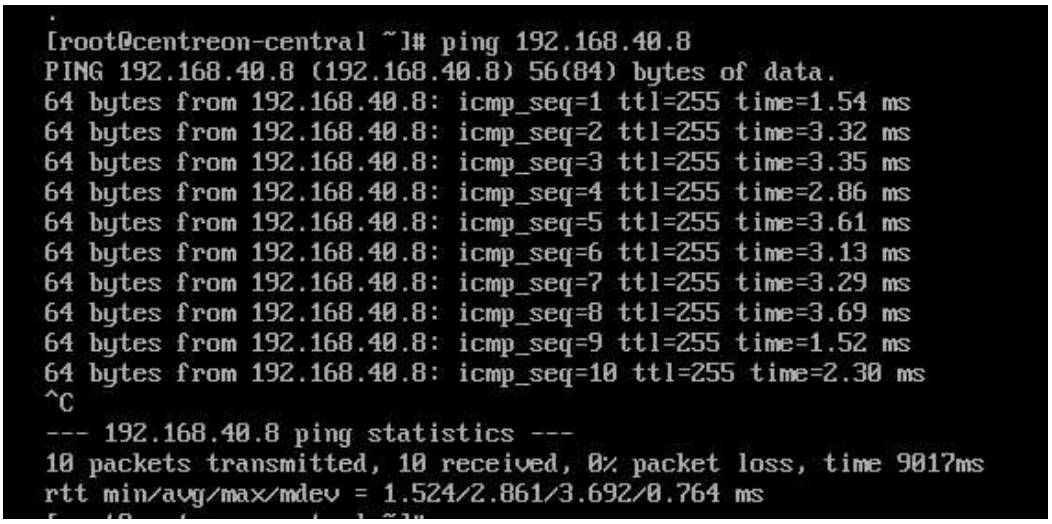


Figure III. 29: Test ping du commutateur Core1 ver le serveur Centreon

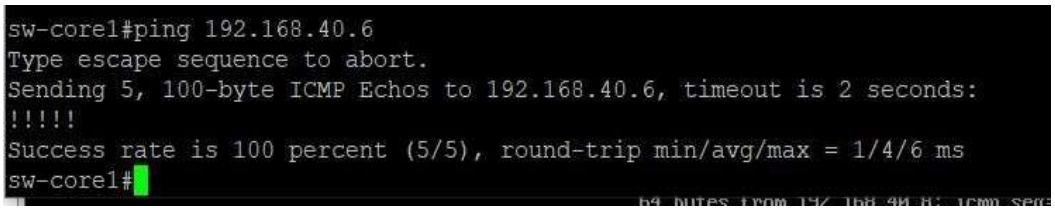


Figure III. 30: Test Ping du serveur Centreon ver le commutateur Core1

➢ ***Configurer l'hôte et déployer la configuration***

Sur la page Configuration **> Hôtes > Hôtes et cliquez sur Ajouter** Remplissez les informations comme montre dans la figure

On suivant les même étapes pour le reste des commutateur **switch-core2, switch-acces1, switch-acses2, switch-acces3.**

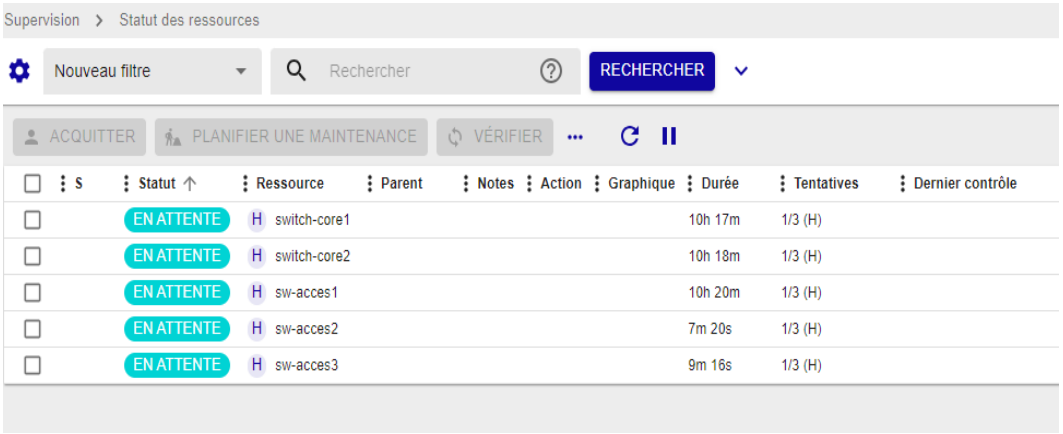


Figure III. 31: Surveillance des hôtes.

➢ *Exporter la configuration*

Au final il est nécessaire d'exporter chaque configuration Pour que les modifications soient Prises en compte.

1. Sur la page **Configuration > Collecteurs > Collecteurs**. Depuis la liste des Pollers, sélectionner le Poller et cliquer sur Exporter la configuration. 2. Cocher ensuite les quatre premières cases, sélectionner la méthode Redémarrer et cliquer sur

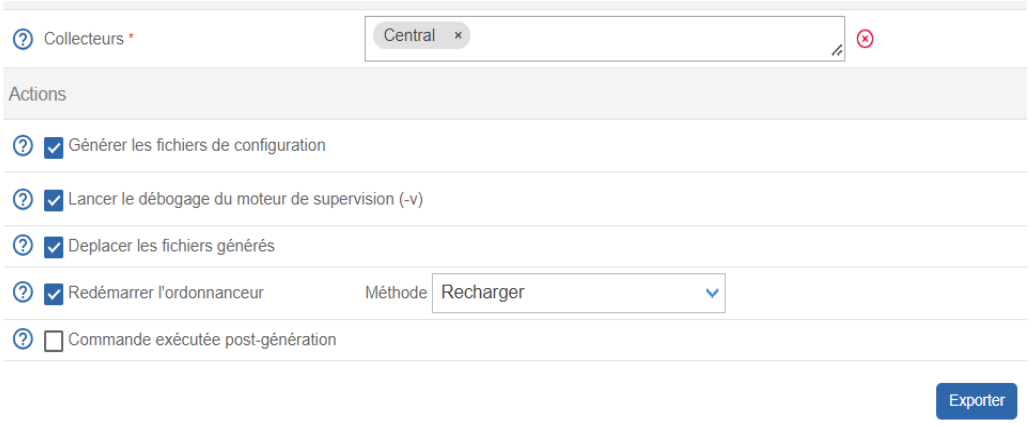
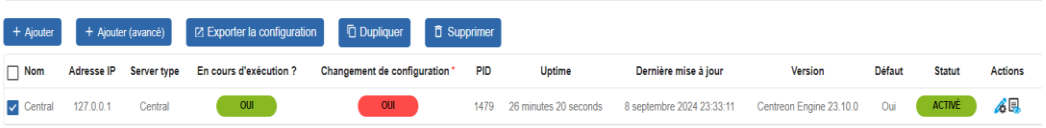


Figure III. 32 : Exporter la configuration de poller.

Le moteur de supervision du poller va alors démarrer et se connecter au Central.



.

Figure III. 33 : Moteur de supervision de poller.

Un log de l'export s'affiche. Dans le log, vérifiez que l'export a bien fonctionné et qu'aucune erreur n'a été remonté.

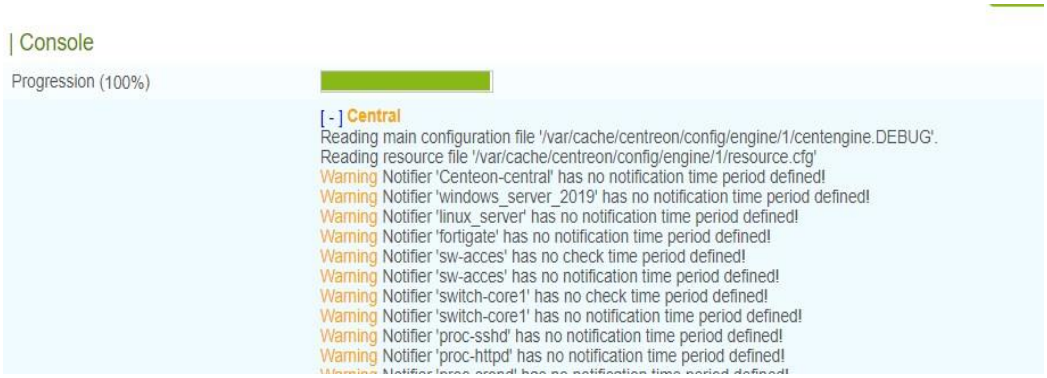


Figure III. 34: Le Log de l'export

Les hôtes sont maintenant définis dans l'interface web de Centreon (voir figure III.35) Nous pouvons confirmer que la surveillance est opérationnelle.

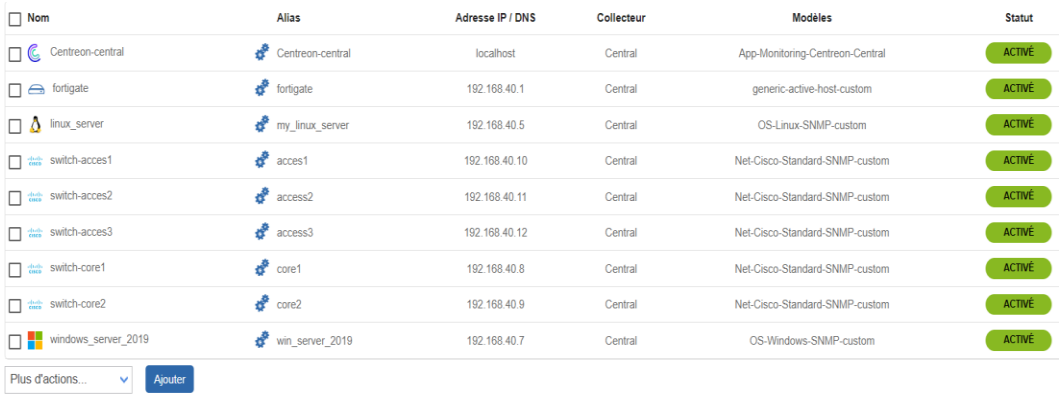


Figure III. 35 : Vue d'ensemble de la surveillance des équipements sur Centreon.

III 4.3 Configuration des services

Le service peut également être structuré selon un modèle similaire à celui des hôtes. Chaque service comprend une commande spécifique (permettant de vérifier un état) ainsi que ses paramètres. Enfin, le service est associé à un hôte ou à un ensemble d'hôtes.

Les services peuvent être créés manuellement suivant ces étapes, pour ajouter unnouveau service, nous devons nous connecter à l'interface web Centreon avec

un compte administrateur ou un compte disposant des droits d'accès pour gérer les objets. Ensuite se rendre sur Configuration > Services > Services par hôtes, puis on clique sur Ajouter.

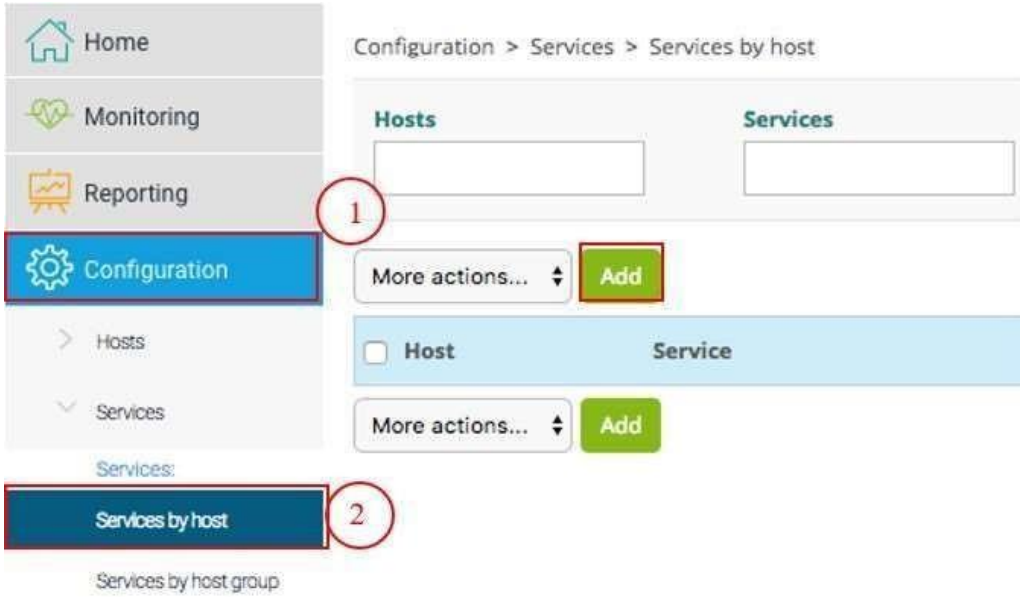


Figure III. 36 : Configuration d'un service.

Lorsque nous accédons au formulaire pour définir un nouvel équipement, l'ajout d'un service à un hôte se fait de manière simple et efficace en remplissant trois champs essentiels.

- **Sélectionner l'hôte concerné,** définir le nom du point de contrôle du service, et choisir un modèle de service approprié tel que "Base-Ping-LAN".

- **Définir le nom du point de contrôle :** Utilisez le champ "Description" pour donner un nom au point de contrôle du service.

- **Sélectionner un modèle de service :** Utilisez le champ "Service Template" pour choisir le modèle de service approprié.

Nous allons créer un service comme illustre dans la figure. Ensuite, nous appliquerons les mêmes étapes pour les autres services. Pour chaque équipement on a créé le besoin de service qu'on va superviser.

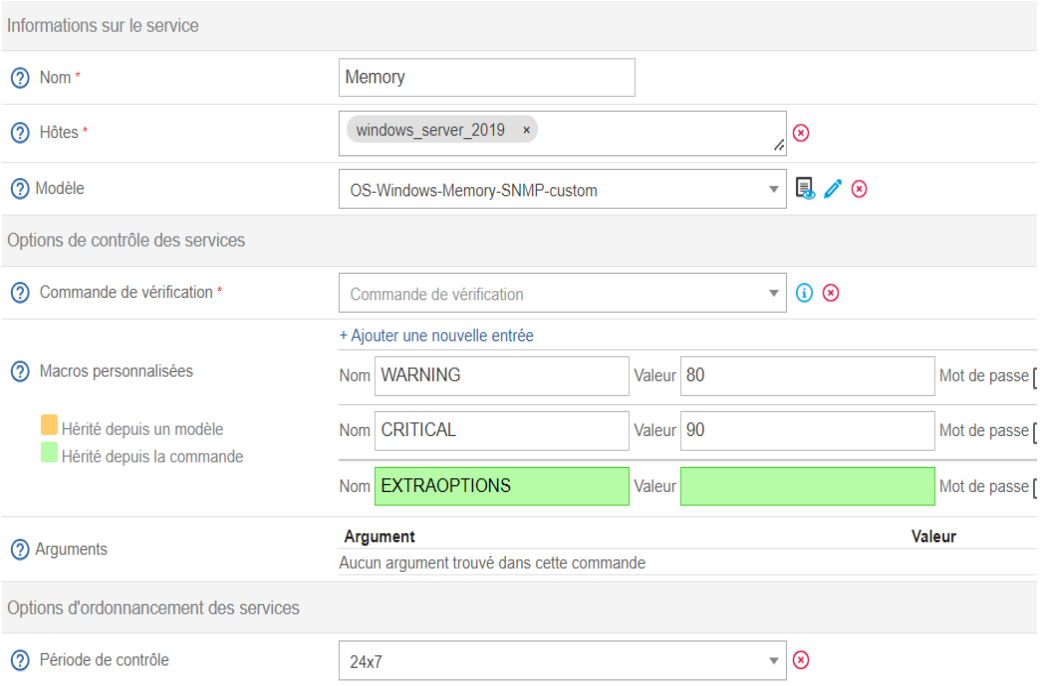


Figure III. 37 : Ajout de service MEMORY Windows server 2019.

➢ ***Les services de serveur Windows***

La figure ci-dessous illustre les principaux services de serveur Windows

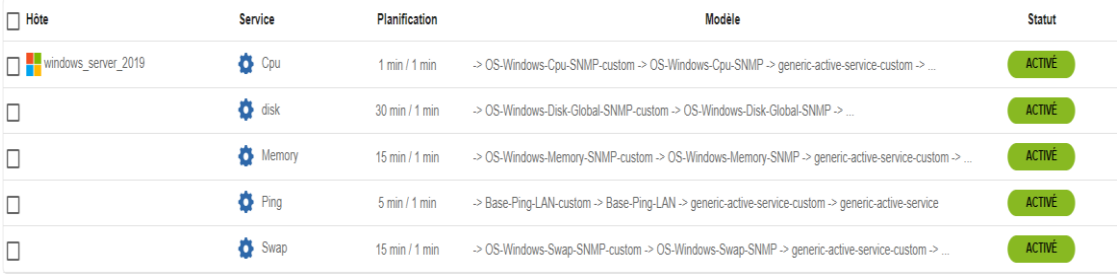


Figure III. 38: Liste des Services du Serveur Windows

➢ ***Les services de par feu FortiGate***

La figure ci-dessous illustre les principaux services de par feu

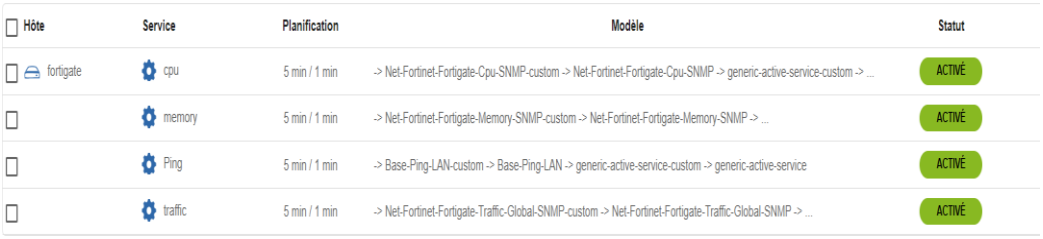


Figure III. 39: Liste des Services du Serveur Windows

➢ ***Les services du serveur Ubuntu***

La figure ci-dessous illustre les principaux services du serveur Ubuntu.

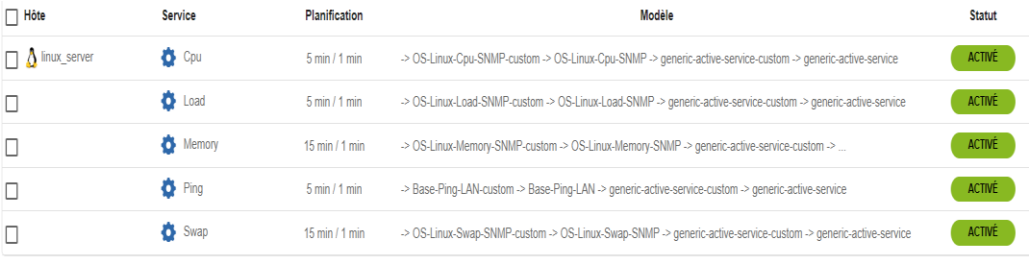


Figure III. 40: Liste des Services du serveur Ubuntu

➢ ***Les services de commutateur***

La figure ci-dessous illustre les principaux services de commutateur

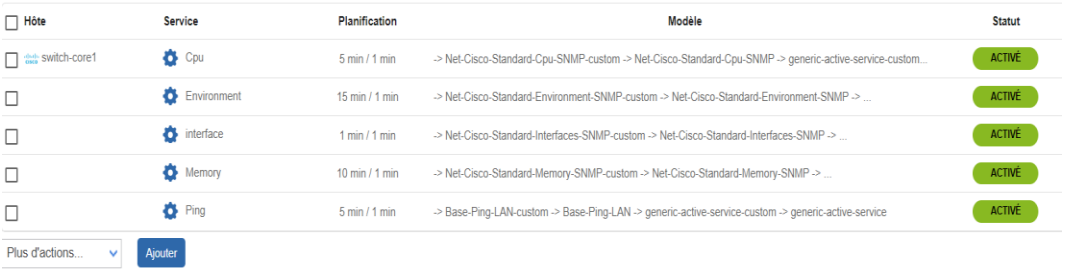


Figure III. 41: Liste des Services du commutateur

❖ Centreon permet de générer des graphiques à partir des informations de supervisionCes graphiques peuvent représenter des métriques comme la charge CPU,

l'utilisation de la mémoire, le trafic réseau, le temps de réponse des services, et d'autres indicateurs clés de performance. Dans notre exemple illustré dans la figure ci-dessous la CPU, Load, Ping du serveur Centreon.

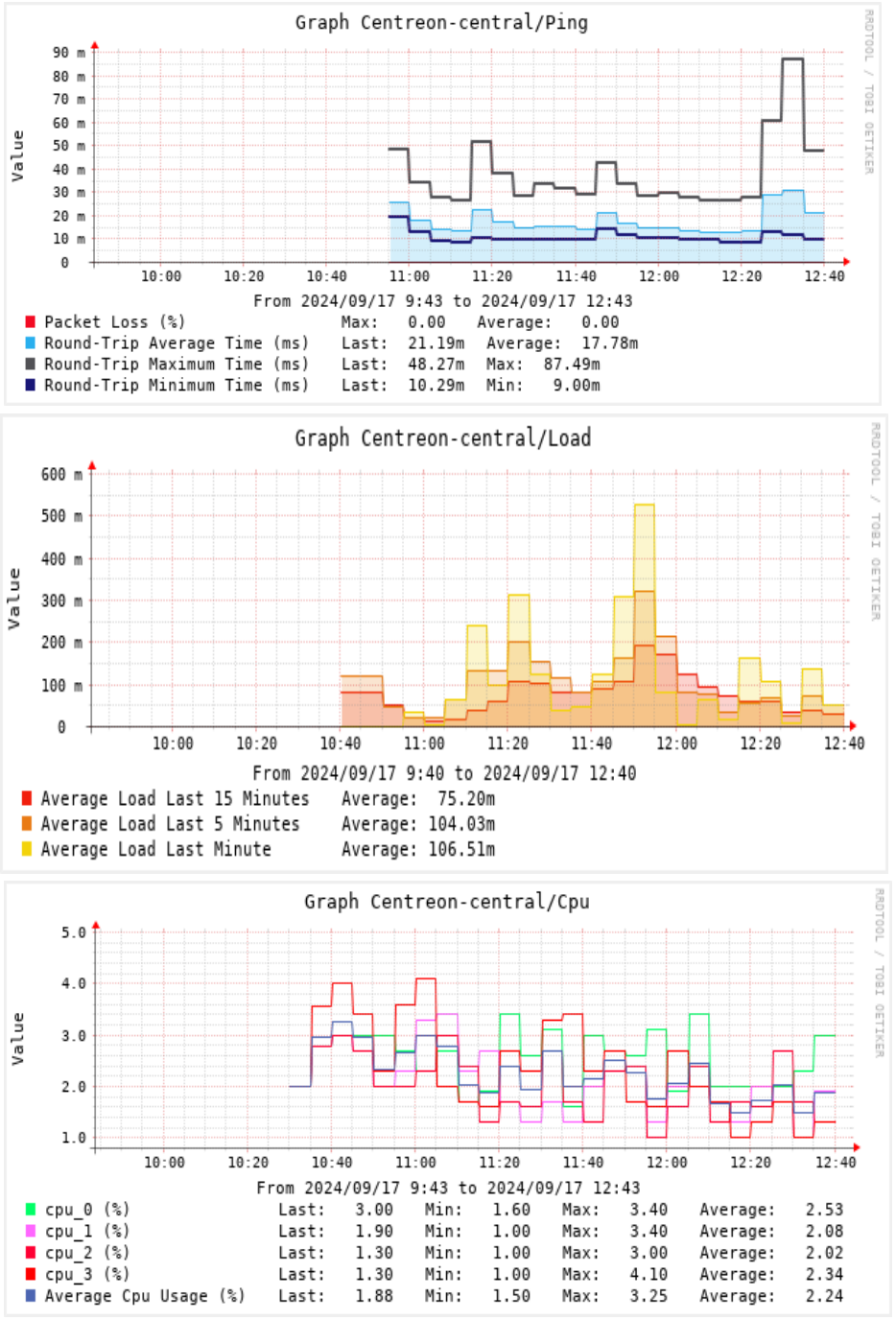


Figure III. 42: Graphe des différents paramètres de notre machine de supervision.

III.4.4 Configuration des alertes Centreon avec le service Gmail

Malgré l'existence d'une interface web permettant de visualiser l'état d'un hôte ou service en temps réel, la notification des contacts reste toujours obligatoire. Pour envoyer les notifications par mail depuis Centreon il faut d'abord installer l'outil correspondant, cela peut se faire de plusieurs manières : utiliser SSMTP, Postfix ou bien encore Sendmail.

1) Configuration de la fonctionnalité « Validation en deux étapes » du compte Gmail

Nous allons mettre en place la fonctionnalité de "Validation en deux étapes" ou" Authentification à deux facteurs" afin de créer un code ou un mot de passe supplémentaire. Ce code sera nécessaire lorsque nous configurerons des alertes dans Centreon et que nous utiliserons un compte Gmail pour recevoir les notifications par e-mail. Pour générer ce code ensuit les étapes illustrées dans les figures suivantes.

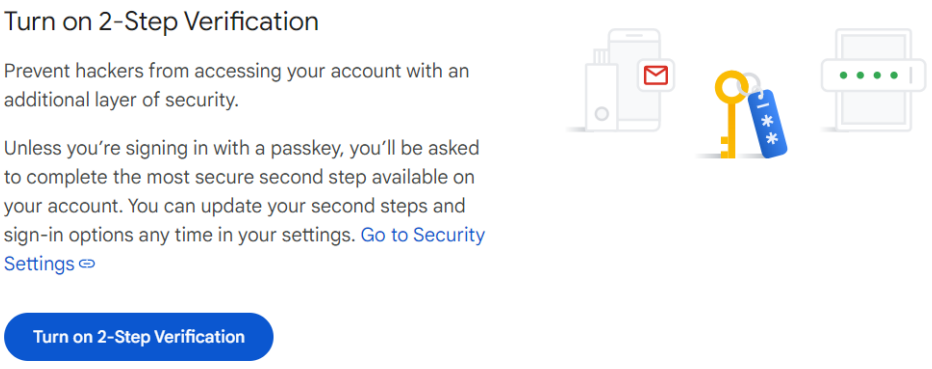


Figure III. 43: configuration de la fonctionnalité validation en deux étapes.

Une fois la validation en deux étapes activées sur notre compte Gmail, nous devons générer un code d'authentification spécifique à l'application pour permettre à Centreon d'accéder à notre compte de manière sécurisée. Lors de la génération, on sélectionne "Autre (personnalisé)" comme type d'application et on lui donne unnom significatif comme "Centreon" dans notre cas. Voir la figure III.44.

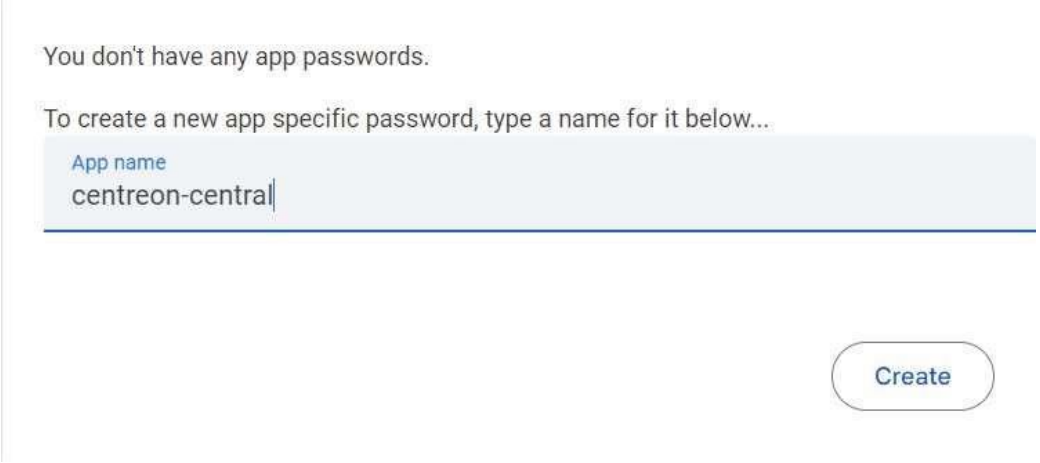


Figure III. 44: Sélectionner l'application Centreon

Une fois le mot de passe spécifique à l'application généré (voir la figureIII.46), on le note soigneusement, car on en aura besoin lors de la configuration de Centreon pour permettre l'envoi d'alertes via notre compte Gmail.

Figure III. 45 : Mots de passe généré

2) Configuration Postfix sur le serveur Alma linux

Postfix est un serveur de messagerie complet, L'objectif de l'installation sur le serveur Alma linux est de configurer Postfix comme un serveur de relais SMTP pour envoyer des courriels via un serveur SMTP externe, comme un service de messagerie tiers Gmail.

1. Dans le terminal de notre serveur, entrer la commande suivante

Pour activer l'authentification SASL pour l'envoi de courriels via un serveur SMTPqui nécessite cette méthode d'authentification

```
sudo dnf install s-nail cyrus-sasl-plain
```

Figure III. 46 : commande d'activation de l'Authentification SASL

2. Redémarrer Postfix

Pour appliquer les modifications, redémarrez Postfix en utilisant la commande appropriée comme suit :

```
sudo systemctl restart postfix
```

Figure III. 47 : Commande pour Redémarrer Postfix après Configuration

3. Configurer Postfix pour qu'il s'exécute au démarrage

Pour configurer Postfix afin qu'il s'exécute automatiquement au démarrage, suivez les étapes illustrées ci-dessous pour activer le service au démarrage du système.

```
vi /etc/postfix/main.cf
```

Figure III. 48 : Commande pour Configurer Postfix.

4. Éditer le fichier suivant

Pour appliquer les configurations nécessaires, éditez le fichier suivant en utilisantun éditeur de texte approprié.

```
sudo systemctl enable postfix
```

Figure III. 49: Édition du Fichier de Configuration pour Postfix.

5. Ajouter des informations

Ajoutez les informations suivantes au fichier pour compléter la configurationselon les spécifications requises.

```
myhostname = centreon-central
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

Figure III. 50: Ajout des Informations dans le Fichier de Configuration

- Le paramètre myhostname Définir le nom d'hôte complet de votre serveur de messagerie.
- Le paramètre relayhost : Configure le serveur SMTP auquel Postfix doit transmettre les courriels sortants.

3) Configurer les identifiants du compte qui enverra les emails

1. Créer un fichier /etc/postfix/sasl_passwd

"Créez le fichier /etc/postfix/sasl_passwd pour stocker les informations d'authentification nécessaires à l'envoi de courriels via SMTP.

```
touch /etc/postfix/sasl_passwd
```

Figure III. 51: Création du Fichier /etc/postfix/sasl_passwd

2. Ajouter la ligne suivante, en remplaçant identifiant

Mot de passe par les informations de connexion du compte qui enverra les emails de notification.

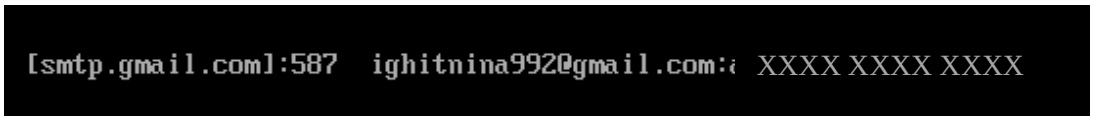


Figure III.52 : Ajout de la Ligne de Configuration dans le Fichier /etc/postfix/sasl_passwd.

3. Dans le terminal, entrer la commande suivante

Dans le terminal, entrez la commande suivante pour générer le fichier de base de données des map pages Postfix, ce qui est nécessaire pour que les modifications prennent effet.

```
postmap /etc/postfix/sasl_passwd
```

Figure III. 53: création du fichier de configuration /etc/postfix/sasl_passwd.

Ce fichier est utilisé par Postfix pour l'authentification des connexions SMTP sortantes.

4. Pour plus de sécurité, changer les permissions sur le fichier sasl_passwd.

```
sudo chown root:postfix /etc/postfix/sasl_passwd*
sudo chmod 640 /etc/postfix/sasl_passwd*
```

Figure III. 54: Changement des Permissions sur sasl_passwd.

5. Recharger Postfix pour prendre en compte les modifications

```
systemctl reload postfix
```

Figure III. 55 : Recharger Postfix

6) Tester et diagnostiquer Postfix

1. Pour envoyer un email de test, utiliser la commande suivante (Figure III.57)

```
[root@centreon-central ~]# echo "Test" | mail -s "Test" securiter00@gmail.com
[root@centreon-central ~]# _
```

Figure III. 56: Email de teste.

2. Le résultat de ce test est présenté dans la figure III le message a été envoyer avec succès

Figure III. 57: Tester l'envoi d'un email.

3. Pour vérifier si votre service Postfix tourne, entrer :

```
systemctl status postfix
```

Figure III. 58 : Vérification de l'État du Service Postfix.

Le résultat devrait ressembler à ça (figure III.60)

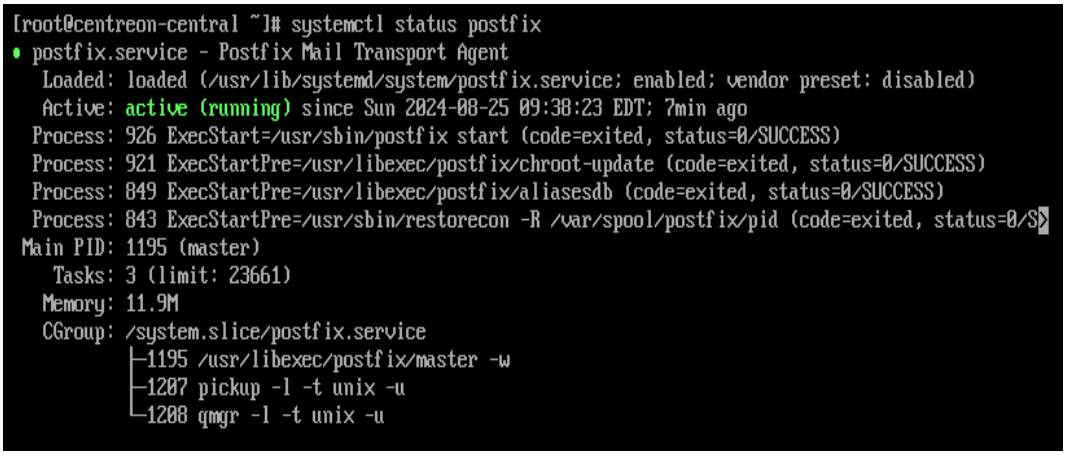


Figure III. 59 : Résultat commande de vérification de l'état du serveur Centreon.

4) Configuration des compte utilisateur

Pour permettre la notification des différentes alertes créées dans Centreon il va falloir effectuer une configuration dans le profil du ou des utilisateurs qui les recevront.

Cliquer sur « Configuration » puis sur « Users », sur « Contacts » et en fin sur « Users». Choisir l'utilisateur concerné et effectuer les modifications suivantes dans les Sections « notification », « hosts » et « services » :

- Enable notifications : yes
- Host /Service Notification Options : cocher les cases pour lesquelles on veut recevoir des notifications
- Host / Service Notification Period : 24x7 pour une notification 24h/24 et 7j/7
- Host Notification Commands: host-notify-by-email

- Service Notification Commands : service-notify-by-email

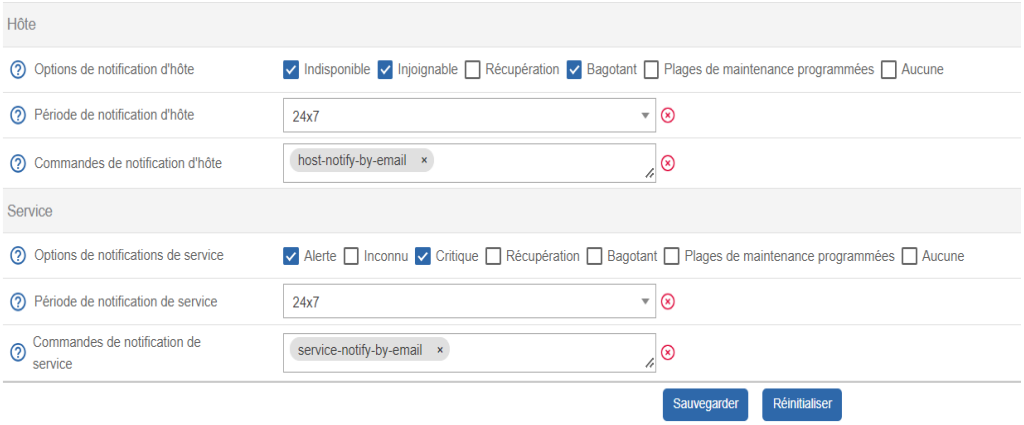


Figure III. 60: configuration du média.

Il sera également nécessaire d'effectuer la configuration suivante sur les Template de service et Template d'hôtes.

5 Exécution des tests de surveillance avec Centreon sur les hôtes ajouter

Pour vérifier que notre configuration est correcte et que Centreon fonctionne comme prévu, nous allons effectuer plusieurs tests sur les hôtes ajoutés. Ensuite, nous examinerons les résultats de ces tests en consultant le tableau de bord de Centreon et en vérifiant les notifications reçues par e-mail dans Gmail.

1) *Tester Centreon à travers le serveur Windows-serveur*

Pour tester Centreon sur notre serveur Windows, nous utiliserons un logiciel appelé HeavyLoad. Ce logiciel nous permettra d'effectuer des tests de stress sur divers composants du système tels que CPU, la RAM, les disques, etc. La figure III.61. Montre l'exécution de HeavyLoad sur le serveur Windows, où le CPU, la RAM et le stockage sont mis sous stress maximum.

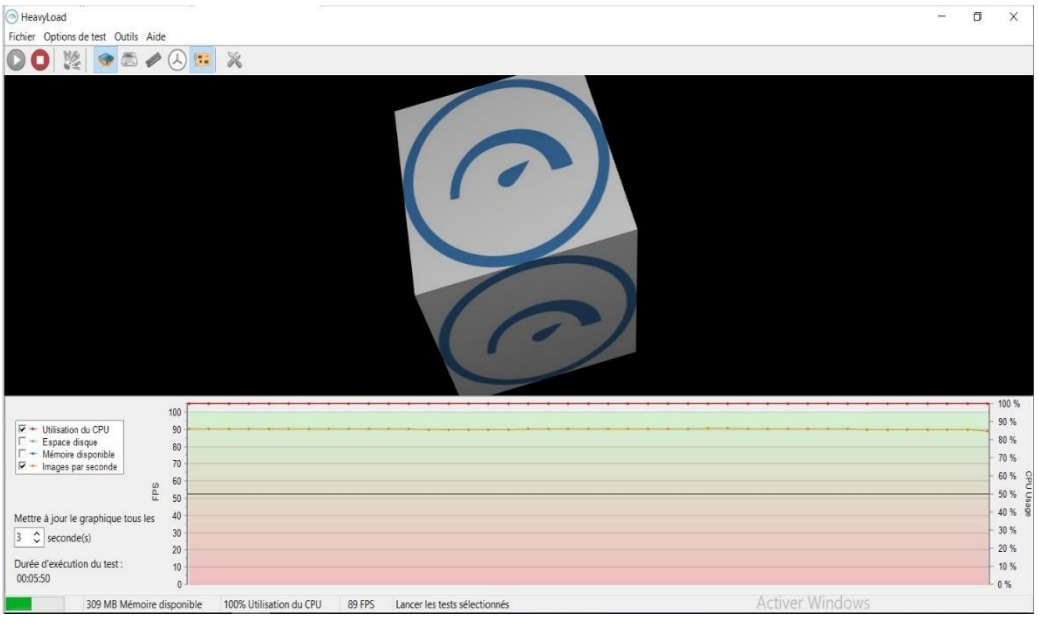


Figure III. 61 : Exécution du logiciel HeavyLoad

1.1) Résultat du test CPU, RAM, Espace Disque

Après avoir exécuté le test pendant environ 5 minutes, Centreon a détecté plusieurs problèmes sur le serveur. Plus précisément, il a identifié trois problèmes : une utilisation élevée du CPU et une utilisation élevée de la mémoire physique.

Figure III. 62 : Alerte affiché sur tableau de bord.

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

Alerte d'utilisation CPU, mémoire physique envoyer par e-mail. Voir la figure III.62

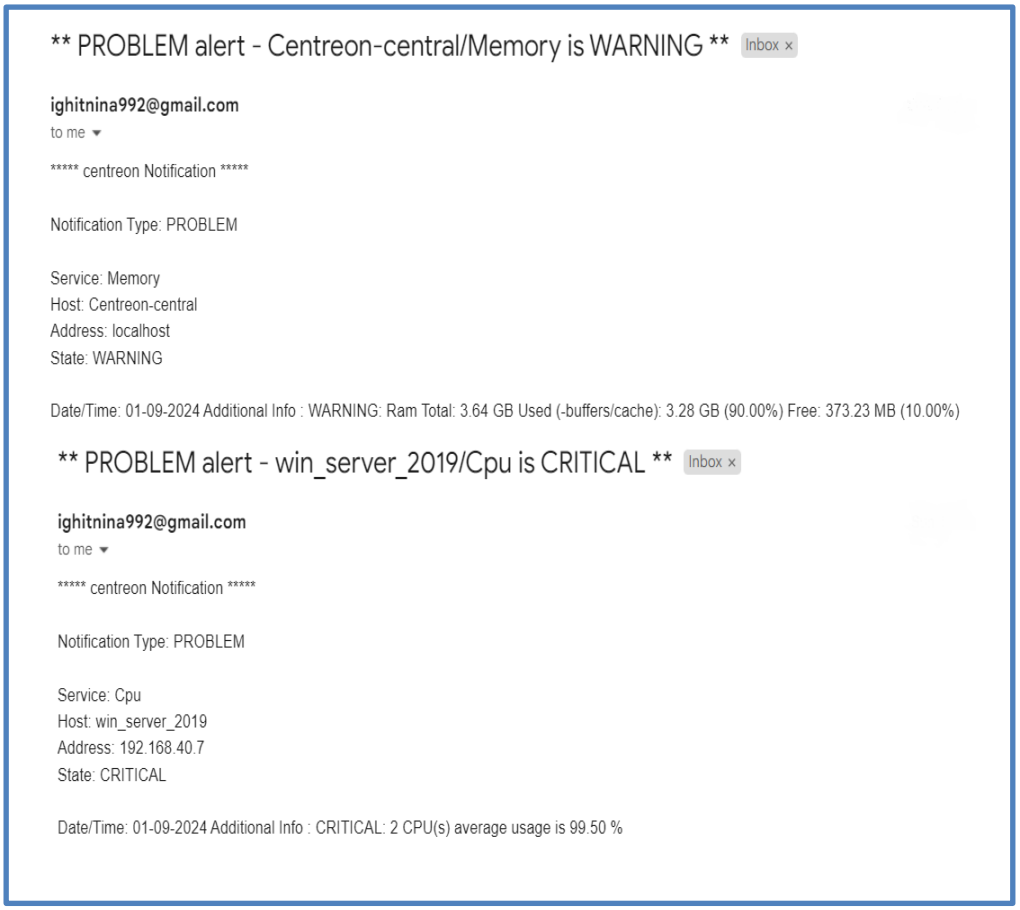


Figure III. 63 : Alerte affiché sur tableau de bord.

III.6 Conclusion

Globalement, ce chapitre a établi les fondations indispensables pour une mise en place réussie de nos solutions. En mettant en évidence comment les fonctionnalités de Centreon ont optimisé la réactivité et amélioré la gestion des problèmes, nous permettant ainsi de surveiller en temps réel, et prendre les mesures nécessaires pour les résoudre. Cette solution a donc jouéun rôle crucial dans le succès de notre mise en œuvre et dans l'efficacité globalede notre gestion.

Conclusion générale

En conclusion, notre mémoire met en évidence l'importance cruciale de la supervision dans un réseau informatique. À travers notre stage à Cevital de Bejaia, nous avons exploré les défis courants liés à la gestion, à la configuration et à la surveillance des infrastructures réseau en général,

Nous avons conçu une solution complète en utilisant Centreon pour superviser le fonctionnement du réseau. Cette solution. A permis aux administrateurs de gérer plus efficacement les ressources réseau, en centralisant les informations et en simplifiant le suivi des performances des équipements en temps réel. Grâce aux alertes précises et opportunes, les administrateurs peuvent réagir rapidement aux anomalies, minimisant ainsi les interruptions de service. De plus, la documentation et les rapports générés facilitent la gestion des actifs et aident à la planification des mises à jour ou des remplacements d'équipement. En optimisant la configuration des systèmes, les administrateurs peuvent également réduire les coûts opérationnels tout en garantissant une conformité aux normes et réglementations en vigueur.

Avec l’adoption de notre solution de supervision, nous avons observé une meilleure configuration des équipements, ce qui a réduit les erreurs humaines et les temps d’arrêt imprévus, renforçant ainsi la fiabilité des systèmes. La surveillance continue a permis de détecter rapidement les pannes et de réagir sans délai, limitant l'impact sur les opérations et assurant une bonne satisfaction des utilisateurs. Cette approche a non seulement amélioré les performances globales du réseau, mais a également assuré une continuité des services de manière plus fluide et efficace.

Références bibliographiques

[1] Briche Thierry et Voland Matthieu, Les outils d'administration et de supervision réseau L'exemple de Nagios, Décembre 2004.

[2] 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.

[3] https://www.whatsupgold.com/fr/blog/surveillance-des-bases-de-donnees.

[4] Belkadi Mourad et Bouchata Zakaria, La mise en place d'un système de supervision réseau (Cas Pratique Univ BLIDA), Blida : Université SAAD

[5] https://www.manageengine.com/network-monitoring/what-is-snmp.html

[6] François Pignet, Réseaux informatique supervision et administration, Décembre 2007.

[7] https://doc.lagout.org/network/pdf_mathrice_2009_Protocoles-3.pdf.

[8] Douglas Mauro et Kevin Schmidt, Essential SNMP 2e édition, septembre2005

[9] André VAUCAMAPS, Cisco : notion de base sur les réseaux, Mai 2009

[10] https://www.studocu.com/fr/document/institut-des-sciences-et-technologies-de-paris/sciences-de-lingenieur/cdp-cisco-discovery-protocol/53118978.

[11] https://www.zabbix.com/fr/about.

[12] https://docs.cacti.net/#cacti-overview.

[13] https://www.nagios.org/about/overview/.

[14] Ms.Nessrine Kaouane, Study and implementation of a SIEM (Security Information and EventManagement) for the management and supervision of Information Systems (Sonelgaz).

[15] https://www.centreon.com/fr/centreon-et-nagios-le-point-en-3-dates-cles/

[16] https://www.cevital-agro-industrie.com/qui-sommes-nous/

[17] https://www.cevital.com/cevital-agro-industrie/.

[18] https://www.connecthostproject.com/vtp.html

[19] https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/

[20] https://www.cisco.com/c/fr_ca/tech/lan-switching/spanning-tree-protocol/index.html.

[21] https://www.malekal.com/protocoles-routage-igp-rip-ospf-isis-eigrp/#google_vignette

Annexe A

ANNEXE A

CONFIGURATION SOUS GNS3

A.1 Configuration des équipements

1. Configuration des ports trunk

Un port trunk est un port réseau sur un commutateur utilisé pour transporter le trafic de plusieurs VLAN (réseaux locaux virtuels). Il permet la transmission de données de plusieurs VLANs sur un seul lien physique. Voici les étapes de la configuration :

```
interface FastEthernet1/0
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/3
 switchport mode trunk
 duplex full
 speed 100
 channel-group 1 mode on
!
interface FastEthernet1/4
 switchport mode trunk
 duplex full
 speed 100
 channel-group 1 mode on
```

```
interface FastEthernet1/0
 switchport access vlan 10
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport access vlan 20
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/3
 switchport mode trunk
 duplex full
 speed 100
 channel-group 1 mode on
!
interface FastEthernet1/4
 switchport mode trunk
 duplex full
 speed 100
 channel-group 1 mode on
```

Figure A.1 : show interface switch port sw-core1 et sw-core2.

2. Créez des VLANs sur le ESW1 (switch core1) comme illustré dans la figure A.2 ;

```
SW-core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-core1(config)#vlan 10
SW-core1(config-vlan)#name informatique
SW-core1(config-vlan)#vlan 20
SW-core1(config-vlan)#name marketing
SW-core1(config-vlan)#vlan 30
SW-core1(config-vlan)#name finance
SW-core1(config-vlan)#vlan 50
SW-core1(config-vlan)#name managment
SW-core1(config-vlan)#end
SW-core1#wr
```

Figure A.2 : Commande de création des VLANs sur le SW-CORE1.

3. Créez des VLANs sur le SW-CORE2 comme illustré dans la figure A.3 :

```
SW-core2(config)#
SW-core2(config)#vlan 10
SW-core2(config-vlan)#name informatique
SW-core2(config-vlan)#vlan 20
SW-core2(config-vlan)#name marketing
SW-core2(config-vlan)#vlan 30
SW-core2(config-vlan)#name finance
SW-core2(config-vlan)#vlan 50
SW-core2(config-vlan)#name managment
SW-core2(config-vlan)#end
SW-core2#wr
```

Figure A.3 : Commande de création des VLANs sur le SW-CORE2.

Utilisez la commande ‘show vlan-switch ’ pour afficher la liste des VLANs crées, comme illustré dans la figure A.4.

Figure A.4 : Commande d’affichage des VLANs créent.

4. Configurez le SW-CORE1 et SW-CORE1 en mode vtp server (voir figureA.5) et les switchs Accès en mode vtp client (voir figure A.4) et afficher sa

```
SW-core1(config)#vtp mode server
Device mode already VTP SERVER.
SW-core1(config)#vtp domain RT
Changing VTP domain name from NULL to RT
SW-core1(config)#vtp password CISCO
Setting device VLAN database password to CISCO
SW-core1(config)#
```

Figure A.5 : Commandes de configuration du switch en mode vtp server

Configuration avec la commande ‘show vtp status’. comme illustré dans la figure A.5

```
SW-core2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-core2(config)#vtp domain RT
Domain name already set to RT.
SW-core2(config)#vtp password CISCO
Setting device VLAN database password to CISCO
SW-core2(config)#
```

Figure A.6 : Commandes de configuration du switch en mode vtp client.

5.Configurez le protocole STP sur les SW-CORE1 en lui attribuant la plus grande priorité (voir figure A.7), et sur l’autre switch SW-CORE2 en lui attribuant la priorité 0 (voir figure A.8) ;

```
ESW1(config)#spanning-tree vlan 10 ro
ESW1(config)#spanning-tree vlan 10 root pri
ESW1(config)#spanning-tree vlan 10 root primary
% This switch is already the root of VLAN10 spanning tree
 VLAN 10 bridge priority set to 8192
 VLAN 10 bridge max aging time unchanged at 20
 VLAN 10 bridge hello time unchanged at 2
 VLAN 10 bridge forward delay unchanged at 15
ESW1(config)#spanning-tree vlan 20 root primary
% This switch is already the root of VLAN20 spanning tree
 VLAN 20 bridge priority set to 8192
 VLAN 20 bridge max aging time unchanged at 20
 VLAN 20 bridge hello time unchanged at 2
 VLAN 20 bridge forward delay unchanged at 15
ESW1(config)#spanning-tree vlan 30 root se
ESW1(config)#spanning-tree vlan 30 root secon
ESW1(config)#spanning-tree vlan 30 root secondary
 VLAN 30 bridge priority set to 16384
 VLAN 30 bridge max aging time unchanged at 20
 VLAN 30 bridge hello time unchanged at 2
 VLAN 30 bridge forward delay unchanged at 15
ESW1(config)#spanning-tree vlan 50 root secondary
 VLAN 50 bridge priority set to 16384
 VLAN 50 bridge max aging time unchanged at 20
 VLAN 50 bridge hello time unchanged at 2
 VLAN 50 bridge forward delay unchanged at 15
ESW1(config)#end
ESW1#
```

Figure A.7 : Commandes de configuration de STP sur le ESW1 (switch core1)

```
ESW2#conf t
Enter configuration commands, one per line.  End with
ESW2(config)#spa
ESW2(config)#spanning-tree vlan 10 root secon
ESW2(config)#spanning-tree vlan 10 root secondary
 VLAN 10 bridge priority set to 16384
 VLAN 10 bridge max aging time unchanged at 20
 VLAN 10 bridge hello time unchanged at 2
 VLAN 10 bridge forward delay unchanged at 15
ESW2(config)#spanning-tree vlan 20 root secondary
 VLAN 20 bridge priority set to 16384
 VLAN 20 bridge max aging time unchanged at 20
 VLAN 20 bridge hello time unchanged at 2
 VLAN 20 bridge forward delay unchanged at 15
ESW2(config)#spanning-tree vlan 30 root prim
ESW2(config)#spanning-tree vlan 30 root prima
ESW2(config)#spanning-tree vlan 30 root primary
 VLAN 30 bridge priority set to 8192
 VLAN 30 bridge max aging time unchanged at 20
 VLAN 30 bridge hello time unchanged at 2
 VLAN 30 bridge forward delay unchanged at 15
ESW2(config)#spanning-tree vlan 50 root primary
 VLAN 50 bridge priority set to 8192
 VLAN 50 bridge max aging time unchanged at 20
 VLAN 50 bridge hello time unchanged at 2
 VLAN 50 bridge forward delay unchanged at 15
ESW2(config)#
```

Figure A.8 : Commandes de configuration de STP sur le ESW2 (switch core2).

6. Configurez le routage inter-vlan sur le SW-CORE1 comme illustré dans la figure A.9 ;

```
SW-core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-core1(config)#router ospf 1
SW-core1(config-router)#network 192.168.3.0 0.0.0.255 area 0
SW-core1(config-router)#network 192.168.10.0 0.0.0.255 area 0
SW-core1(config-router)#network 192.168.20.0 0.0.0.255 area 0
SW-core1(config-router)#network 192.168.30.0 0.0.0.255 area 0
SW-core1(config-router)#network 192.168.50.0 0.0.0.255 area 0
SW-core1(config-router)#end
SW-core1#
*Mar  1 00:52:21.011: %SYS-5-CONFIG_I: Configured from console by
```

Figure A.9 : Commandes de configuration du routage inter-vlan.

7. Configuration d'EtherChannel entre le SW-CORE1 et le SW-CORE2 comme illustré dans la figure A.11 :

```
SW-core1(config)#interface range fastEthernet 1/3 - 4
SW-core1(config-if-range)#channel-group 1 mode on
SW-core1(config-if-range)#interface port-channel 1
SW-core1(config-if)#switchport trunk encapsulation dot1q
SW-core1(config-if)#switchport mode trunk
SW-core1(config-if)#
```

Figure A.11 : Commandes de configuration d'EtherChannel sur SW-core1.

```
SW-core2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-core2(config)#interface range fastEthernet 1/3 - 4
SW-core2(config-if-range)#channel-group 1 mode on
SW-core2(config-if-range)#interface port-channel 1
SW-core2(config-if)#switchport trunk encapsulation dot1q
SW-core2(config-if)#switchport mode trunk
SW-core2(config-if)#
```

Figure A.12 : Commandes de configuration d'EtherChannel sur SW-core2.

8. Configuration de HSRP sur les deux switchs le SW-CORE1 et le SW-CORE2 comme illustré dans les figures A.12 et A.13 afficher sa configuration avec la commande 'show standby brief'

```
SW-Core1(config)# interface vlan 10
SW-Core1(config-if)# ip address 192.168.10.251 255.255.255.0
SW-Core1(config-if)# no shutdown

SW-Core1(config)# interface vlan 20
SW-Core1(config-if)# ip address 192.168.20.251 255.255.255.0
SW-Core1(config-if)# no shutdown

SW-Core1(config)# interface vlan 30
SW-Core1(config-if)# ip address 192.168.30.251 255.255.255.0
SW-Core1(config-if)# no shutdown

SW-Core1(config)# interface vlan 50
SW-Core1(config-if)# ip address 192.168.50.251 255.255.255.0
SW-Core1(config-if)# no shutdown
```

Figure A.13 : Commandes de configuration de HSRP sur le SW-CORE1.

```
SW-Core2(config)# interface vlan 10
SW-Core2(config-if)# ip address 192.168.10.252 255.255.255.0
SW-Core2(config-if)# no shutdown

SW-Core2(config)# interface vlan 20
SW-Core2(config-if)# ip address 192.168.20.252 255.255.255.0
SW-Core2(config-if)# no shutdown

SW-Core2(config)# interface vlan 30
SW-Core2(config-if)# ip address 192.168.30.252 255.255.255.0
SW-Core2(config-if)# no shutdown

SW-Core2(config)# interface vlan 50
SW-Core2(config-if)# ip address 192.168.50.252 255.255.255.0
SW-Core2(config-if)# no shutdown
```

Figure A.14 : Commandes de configuration de HSRP sur le SW-CORE2.

Pour afficher les détails de la configuration HSRP, y compris les groupes configurés, les adresses IP virtuelles, les états des interfaces, et les priorités configurées sur le SW- CORE1.utiliser la commande suivante « show standby ». Si vous souhaitez voir la configuration spécifique à une interface ou à un groupe particulier, vous pouvez spécifier l'interface ou le groupe avec la commande « show standby brief ».

```
sw-core1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       100  200 P Active  local           unknown         192.168.3.1
Vl10        10   200 P Active  local           unknown         192.168.10.254
Vl20        20   200 P Active  local           unknown         192.168.20.254
Vl30        30   200 P Active  local           unknown         192.168.30.254
Vl50        50   200 P Active  local           unknown         192.168.50.254
sw-core1#
```

Figure A.14 : Commande d'affichage de la configuration HSRP sur le SW-CORE1.

```
sw-core2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       100  150 P Active  local           unknown         192.168.2.1
Vl10        10   150 P Standby 192.168.10.251  local           192.168.10.254
Vl20        20   150 P Standby 192.168.20.251  local           192.168.20.254
Vl30        30   150 P Standby 192.168.30.251  local           192.168.30.254
Vl50        50   150 P Standby 192.168.50.251  local           192.168.50.254
sw-core2#
```

Figure A.15 : Commande d'affichage de la configuration HSRP sur le SW-CORE2.

A.1 Configuration de firewall (FortiGate)

Etape 1. Configuration du port 1 (lié au WAN, Cloud), Saisir les commandes suivantes comme illustré dans la figure A.16.

```
FortiFirewall-VM64-KVM # config system interface
FortiFirewall-VM64-KVM (interface) # edit port1
FortiFirewall-VM64-KVM (port1) # set mode static
FortiFirewall-VM64-KVM (port1) # set ip 192.168.1.200/24
```

Figure A.16 : les commandes de la configuration du port 1 (lié au WAN, Cloud)

Vérifier que l'adresse IP attribuée est de même sous-réseau que l'adresse IP de la carte réseau physique : exécuter la commande ipconfig sur cmd).

```
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . .: fe80::ec7:8c21:d2ba:fde6%4
Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.38
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Passerelle par défaut. . . . . . . . . : fe80::1%4
                                        192.168.1.1
```

```
FortiFirewall-VM64-KVM (port1) #  set allowaccess ping https
ssh telnet
FortiFirewall-VM64-KVM (port1) # end
```

Figure A.17 : l'adresse IP de la carte réseau physique.

Etape 2 : Configurer la passerelle par défaut comme étant la passerelle de l'hôte physique comme illustré dans la figure A.17.

```
FortiFirewall-VM64-KVM # config router static
FortiFirewall-VM64-KVM (static) # edit 1
FortiFirewall-VM64-KVM (1) # set device port1
FortiFirewall-VM64-KVM (1) # set gateway 192.168.1.1
FortiFirewall-VM64-KVM (1) # end
```

Figure A.18 : les commandes de la configuration du port 1 la passerelle du hôte physique.

Vérifier les configurations du port1 Envoyer une commande Ping vers la passerelle : execute ping 192.168.1.1 comme illustré dans la figure A.18.

```
FortiGate-VM64-KVM # execute ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=13.4 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=9.8 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=5.1 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=7.6 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=14.7 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.1/10.1/14.7 ms
```

Figure A.19: test de connectivité via un ping vers la passerelle (192.168.1.1).

Envoyer une commande Ping vers Internet : execute ping 8.8.8.8

```
FortiGate-VM64-KVM # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=186.3 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=825.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=93.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=250.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=156.3 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 93.4/302.4/825.1 ms
```

Figure A.19 : Ping vers Internet (8.8.8.8**).**

Etape 3 : Configuration via l'interface web, Lancer le navigateur Web et Saisir dans la barre d'adresse l'adresse IP du port 1 : 192.168.1.200.

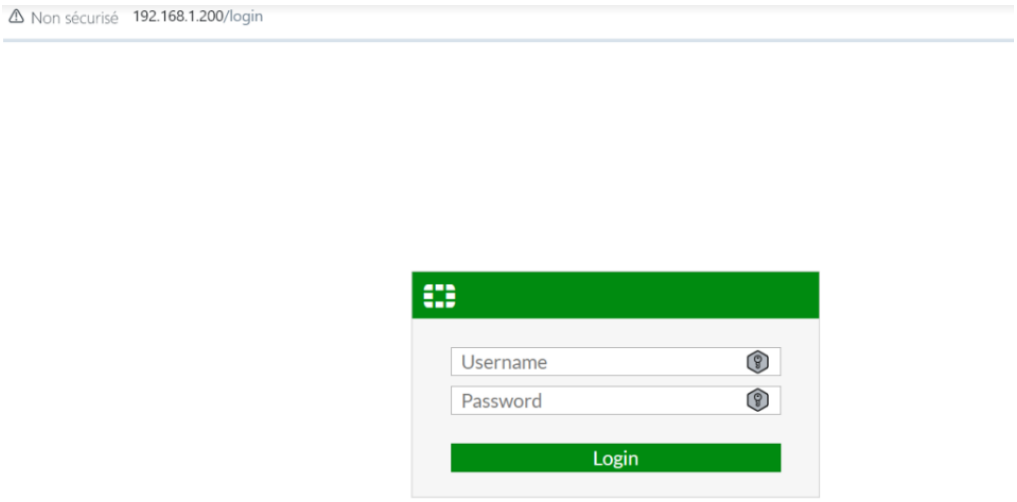


Figure A.20 : Accès à l'interface web via l'adresse IP 192.168.1.200.

Saisir le nom d'utilisateur et le mot de passe

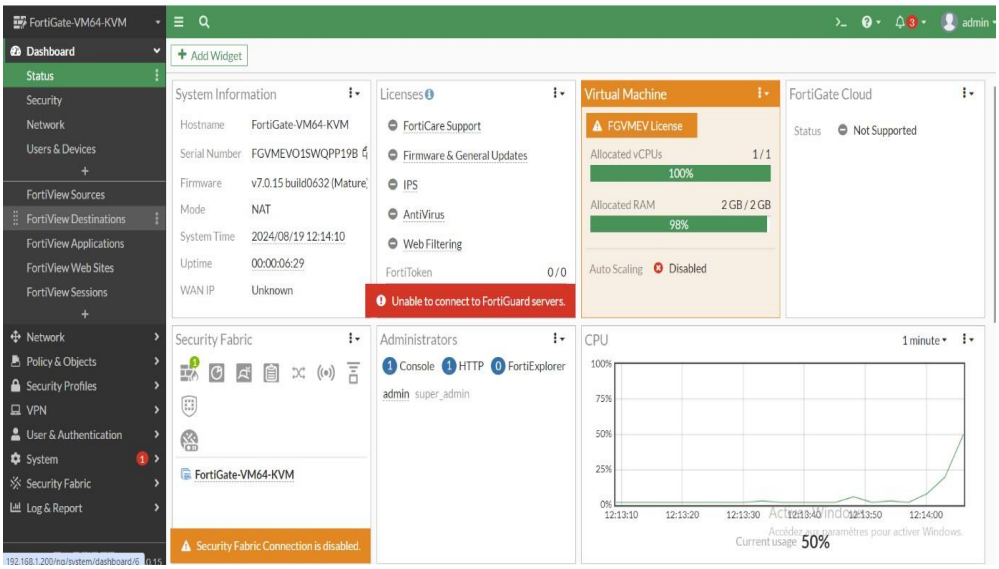


Figure A.21 : Identification avec le nom d'utilisateur et le mot de passe. Cliquer sur l'onglet Network, puis interfaces, puis choisir port1.

Ajouter les configurations suivantes : Alias : WAN , Rôle : WAN et Cliquer sur OK

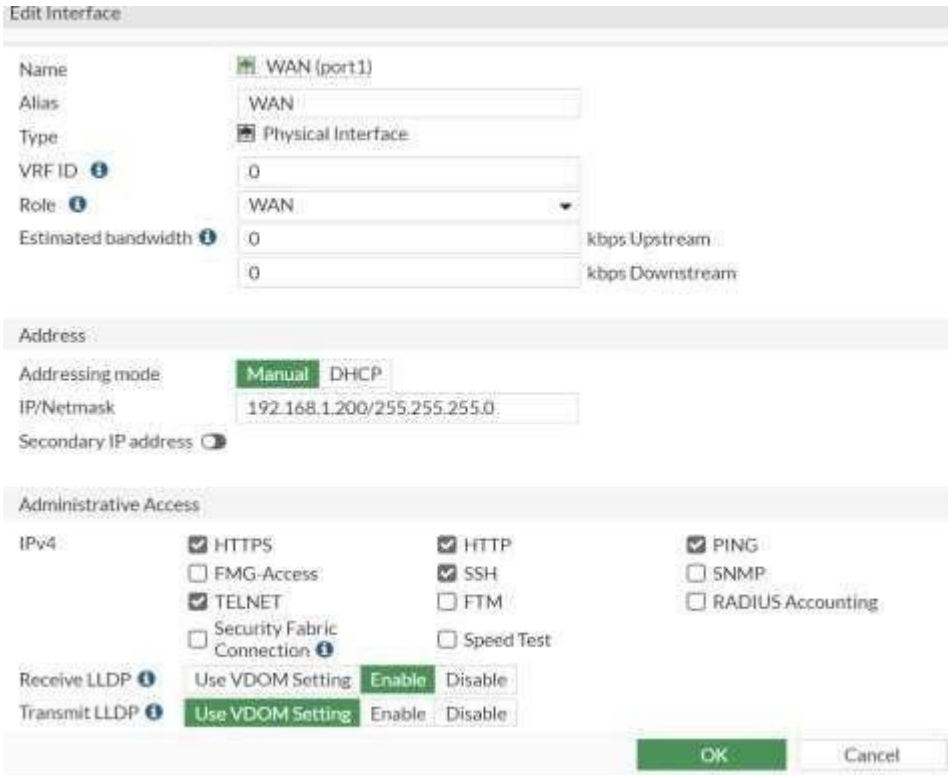


Figure A.21 : Configuration du port1 en tant qu'interface WAN.

Etape 4 : Configuration du port2

Dans l'interface web, Aller dans **Network > Interfaces > Port2 >edit** , Ajouterles configurations suivantes : ▪ Alias DMZ, Role : DMZ▪ IP/Mask : 192.168.40.1/255.255.255.0
,Allow ping et http Cliquer sur OK

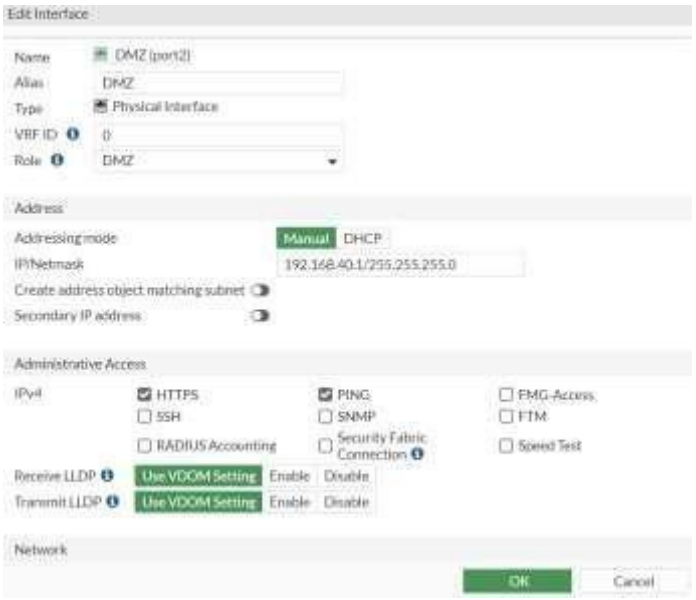


Figure A.22 : Configuration du port2 en tant qu'interface DMZ.

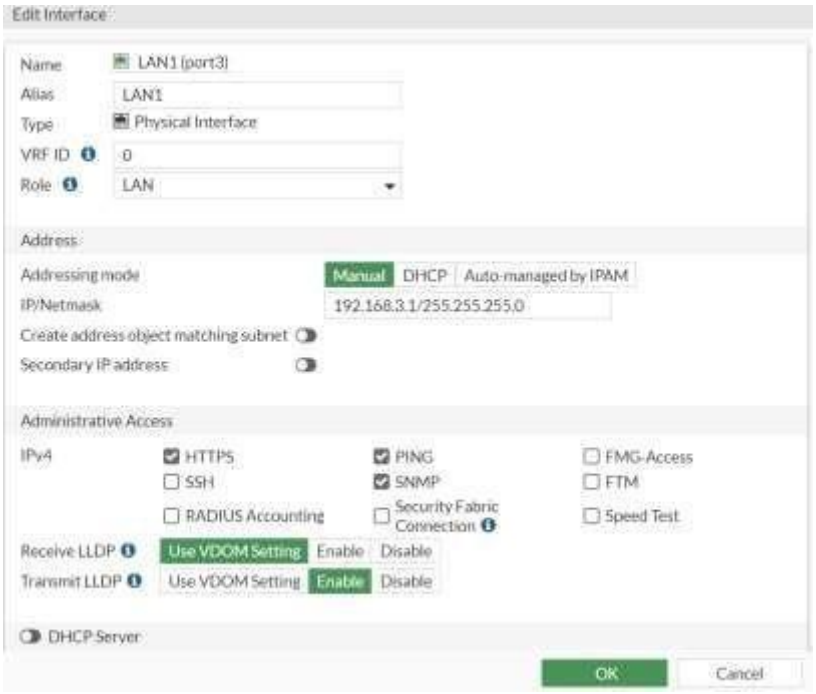


Figure A.23 : Configuration du port2 en tant qu'interface LAN1.

Etape 5 : Configuration du port 4

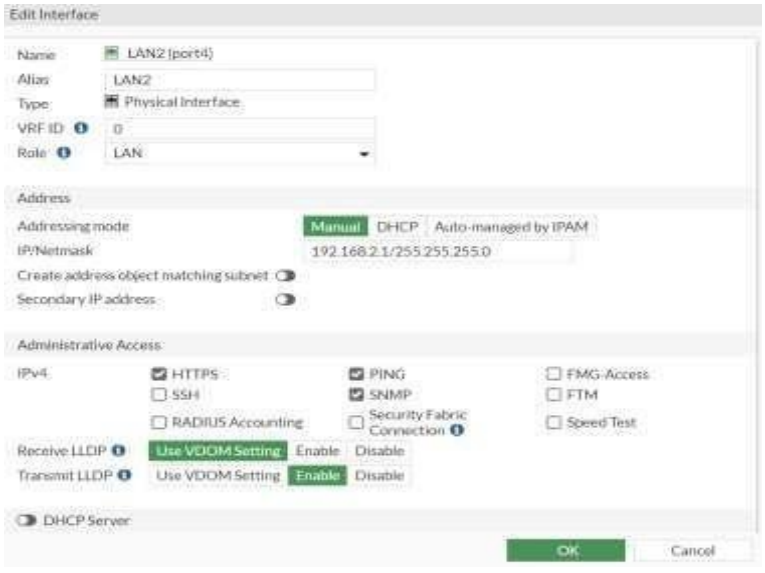


Figure A.24: Configuration du port2 en tant qu'interface LAN2.

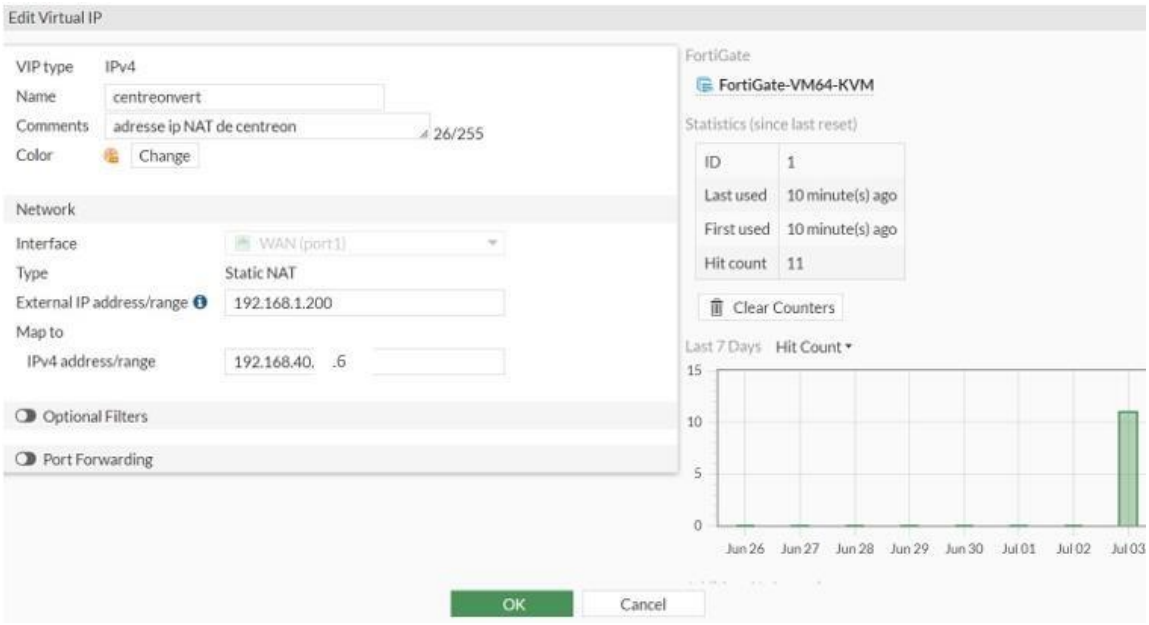
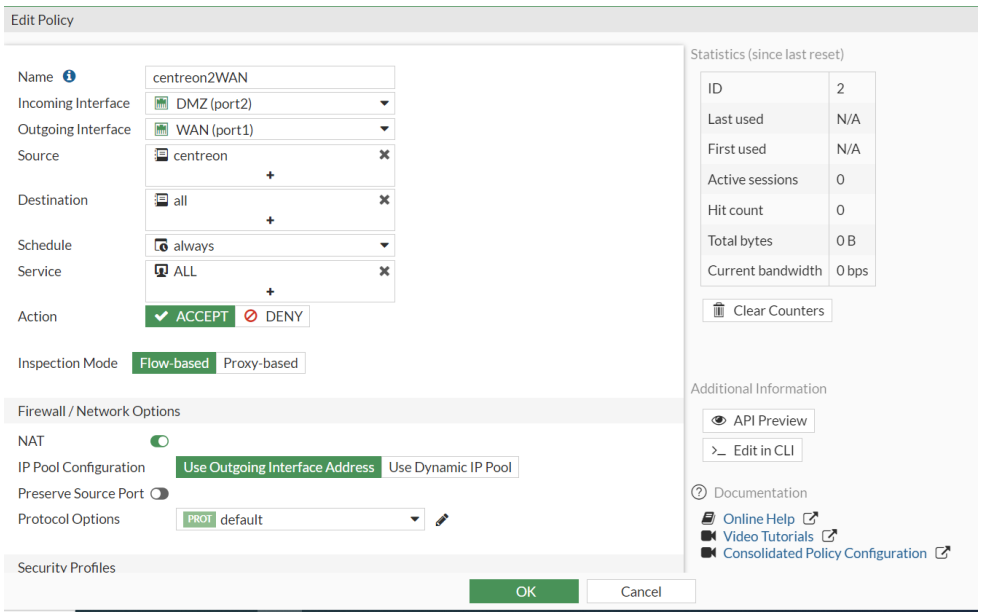


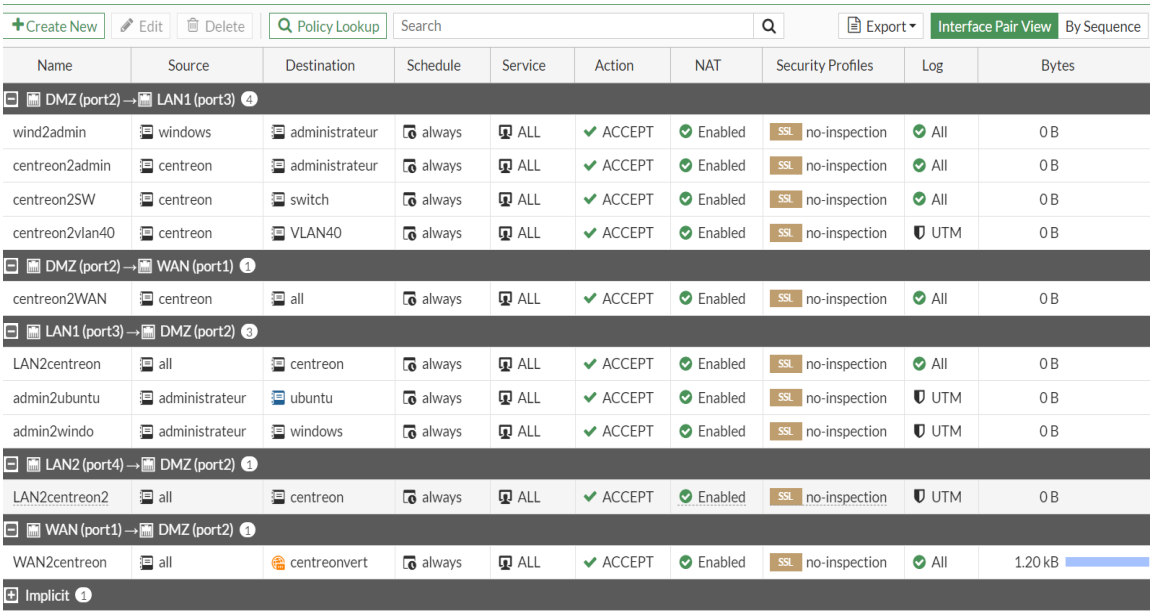
Figure A.25 : Ajout d'une adresse IP virtuelle pour la connexion Centreon ↔ WAN.

Etape 7 : Pour créer une politique de pare-feu (firewall policy) ou bien desACL dans l'interface graphique :

Accédez à Policy & Objects > Firewall Policy, Cliquez sur Cérate New La Nouvelle Politique s'affiche et Saisissez un nom et configurez les paramètres nécessairessuivants : On souhaite laisser les passer les paquets DMZ vers le WAN.



En suivant les mêmes étapes pour les autres ACL



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
DMZ (port2) → LAN1 (port3) 4									
wind2admin	windows	administrateur	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0 B
centreon2admin	centreon	administrateur	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0 B
centreon2SW	centreon	switch	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0 B
centreon2vlan40	centreon	VLAN40	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
DMZ (port2) → WAN (port1) 1									
centreon2WAN	centreon	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0 B
LAN1 (port3) → DMZ (port2) 3									
LAN2centreon	all	centreon	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0 B
admin2ubuntu	administrateur	ubuntu	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
admin2windo	administrateur	windows	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
LAN2 (port4) → DMZ (port2) 1									
LAN2centreon2	all	centreon	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
WAN (port1) → DMZ (port2) 1									
WAN2centreon	all	centreonvert	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	1.20 kB
Implicit 1									

Figure A.26 : Configuration des ACL pour les autres politiques.

Résumé

Dans le cadre de notre mémoire, nous avons réalisé une étude approfondie sur les solutions de supervision durant notre stage chez Cevital. Nous avons conçu une architecture réseau détaillée, intégrant les aspects LAN et WAN, avec le déploiement de Centreon comme solution de supervision. Notre travail a consisté à configurer Centreon pour surveiller divers équipements réseau et à effectuer plusieurs tests pour valider l'exactitude de cette configuration. Après ces tests, nous avons analysé les résultats et vérifié les notifications reçues par e-mail via Gmail pour confirmer le bon fonctionnement de la solution.

Mots clés : Réseaux informatiques, Supervision, Centreon, SNMP

Abstract

During our internship at Cevital, we conducted an in-depth study on monitoring solutions for our thesis. We designed a detailed network architecture covering both LAN and WAN aspects, deploying Centreon as our monitoring solution. Our work involved configuring Centreon to monitor various network devices and conducting several tests to verify the accuracy of our setup. After performing these tests, we analyzed the results and validated the email notifications received in Gmail to ensure that the solution was functioning correctly.

Keywords: Computer networks, Monitoring, Centreon, SNMP