Royaume du Maroc
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique et de l'Innovation

Ecole Supérieure de Technologie de Salé
Université Mohammed V de Rabat

RAPPORT DE STAGE

Mise en place d'un réseau local sécurisé et superviser avec Zabbix

Réalisée avec :

Meriem BELKOURI

Hanan SAIDI

Maitre de stage :

M. Hamza BEAJ

13 JUILLET 2023

Filière : Administration Réseaux informatiques

Département : Informatique

Dédicaces :

A nos chers parents : aucune dédicace ne saurait exprimer le dévouement, le respect et l'amour que nous vous pouvez être fiers d'avoir réussi vos missions dans la vie.

A nos sœurs.

A nos frères.

A notre encadrant pour sa serviabilité, son soutien. Ses orientations et ses encouragements.

A tous ceux qui travaillent dans Enssup.

A tous nos amis et à tous les camarades de l'école supérieure de technologie de Salé.

Remerciement :

Nous tenons à exprimer notre gratitude à tous les professeurs de la filière qui nous ont préparés tout au long de l'année pour élaborer ce rapport. Nous sommes reconnaissants pour leur expertise, leurs conseils et leur dévouement à notre apprentissage. Leur soutien a été essentiel pour la réalisation de ce travail.

Nous souhaitons aussi remercier M. Mouhcine et M. Hamza BEAJ, nos maîtres de stage, Mme. Berbiche la Directrice de la direction des Systèmes d'Information (DSI), M. AMRAR Ali Chef de la Division informatique ainsi nous remercions l'ensemble des employés de La Secrétariat d'Etat Chargé de l'Enseignement Supérieur Et de la Recherche Scientifique pour Leur soutien constant, leur enthousiasme et leur disponibilité ont été d'une valeur inestimable tout au long de notre stage. Nous sommes profondément reconnaissants pour l'aide précieuse qu'ils nous ont apportée.

Finalement, nous aimerions remercier M. Mohammed Zanane de son appui et de ses encouragements. C'est sa présence et son soutien qui nous inspirent.

Nous sommes conscients que ce travail n'aurait pas été possible sans le soutien et les encouragements de toutes ces personnes. Nous leur sommes reconnaissants et nous leur exprimons notre profonde gratitude.

Sommaire :

Dédicaces : 3

Remerciement : 4

Sommaire : 5

Liste des figures : 6

Liste des abréviations : 10

Introduction Générale : 11

Partie I : 12

Présentation du cadre du projet 12

.....12

Partie II : 17

Les tâches effectuées.....17

Chapitre 1 : 21

Mise en place d'un réseau local sécurisé 21

Chapitre 2 : 77

Supervision avec Zabbix 77

Chapitre 3 : 124

Application web avec Laravel.....124

Conclusion générale : 136

Liste des figures :

Figure 1: Logo de Enssup 13
Figure 2: Organigramme Enssup 15
Figure 3:Gantt 19
Figure 4:PERT 20
Figure 5:Architecture global 23
Figure 6:switch manageable 27
Figure 7:switch non manageable 27
Figure 8: smart manager switch 28
Figure 9: Dell N2048P 28
Figure 10:configuration de switch 30
Figure 11: configuration de base 30
Figure 12:affectation des ports aux vlans 31
Figure 13: création des vlans 1 31
Figure 14: affectation des ports aux vlans et création des ports trunk 31
Figure 15: affectation des ports et les addresses aux vlans 32
Figure 16: affectation les adresses aux vlans 32
Figure 17:parfeu 33
Figure 18:firewall FortiGate 500D 38
Figure 19: configuration de FortiGate 500D 40
Figure 20:création zone Dmz privée 41
Figure 21:création de zone Dmz publique 41
Figure 22: les zones Dmz 41
Figure 23:private Dmz de 1er Groupe 42
Figure 24:Dmz privée pour 2éme Groupe 42
Figure 25:Dmz publique 1er Groupe 43
Figure 26:Dmz publique pour 2éme Groupe 43
Figure 27: Toutes les interfaces Dmz 44
Figure 28: Réservation de ports 9 pour routage 44
Figure 29: assigner une adresse IP (passerelle) au réseau virtuel administrateur 45
Figure 30: assigner une adresse IP (passerelle) au réseau virtuel employé 45
Figure 31:Vlans 46
Figure 32:Création de l’interface WAN 46
Figure 33:Inteface WAN 47
Figure 34:Politique de sécurité de notre Firewall 47
Figure 35:serveur 48
Figure 36:Server Dell PowerEdge T430 49
Figure 37:les deux types d'hyperviseur 51
Figure 38:logo Proxmox 52
Figure 39: 1er page d'installation Proxmox 53
Figure 40:Configuration de réseau dans notre serveur 55
Figure 41: Création de Virtual switch vmbr1 55
Figure 42: Création de 1er vlan 10 Dmz privée de 1er Groupe 56

Figure 43: Création de 2éme Vlan 20 publique pour 1er Groupe 56
Figure 44: Création de 3éme Vlan 30 Dmz privée de 2éme Groupe 57
Figure 45: Création de 4éme Vlan Dmz publique de 2éme Groupe 57
Figure 46: Création de 5éme Vlan Admin 58
Figure 47:Exemple de Dmz 58
Figure 48:DNS 60
Figure 49: Installation de server DNS 60
Figure 50:Configuration de fichier stage.local 61
Figure 51:configuration de fichier named.conf 62
Figure 52 :resolv.conf 62
Figure 53: Restart service named 63
Figure 54:installation de serveur web apache 64
Figure 55:on ajout le fichier site1.conf ou stage.conf dans /etc/apache2/sites-availebles 64
Figure 56:on ajoute notre site dans le chemin /var/www 64
Figure 57: Site avec domain stage.ma 65
Figure 58: Création de la machine 68
Figure 59:Config AP1 74
Figure 60:config AP2 74
Figure 61:config AP 3 75
Figure 62:Config AP5 75
Figure 63:config AP4 75
Figure 64:Config AP6 76
Figure 65: Config AP7 76
Figure 66:Nagios 79
Figure 67:zabbix 81
Figure 68:Pandora FMS 83
Figure 69: Zabbix features overview 85
Figure 70: Différents hôtes Zabbix peut les superviser 86
Figure 71:Installation Apache 89
Figure 72:Installation de MySQL 90
Figure 73: Sécuriser l'installation de MySQL 90
Figure 74: Installation de Maria DB 91
Figure 75:Sécurisé Maria DB 91
Figure 76:1ère étape d'installation Zabbix 92
Figure 77:2eme étape d’installation Zabbix 92
Figure 78: 3éme étape de d’installation de Zabbix 93
Figure 79: Configuration de Maria DB 93
Figure 80: Création de base de données 94
Figure 81: 4éme étape d'installation de Zabbix 94
Figure 82:Fichier de configuration de Zabbix server 95
Figure 83: Configuration de Zabbix server 95
Figure 84: Restart and enable Zabbix-server/Zabbix-agent 95
Figure 85: Configuration de Zabbix dans l'interface web 1 96
Figure 86:Configuration de Zabbix dans l'interface web 2 96

Figure 87: Configuration de Zabbix dans l'interface web 3 97
Figure 88: Installation de Zabbix terminée..... 97
Figure 89: Dashboard 98
Figure 90: Mise à jour..... 99
Figure 91: Installation de l'agent Zabbix 100
Figure 92:Fichier de configuration de l'agent 100
Figure 93: Spécification de port d'écoute et l'adresse de serveur Zabbix 101
Figure 94: Spécification de Serveur Active et Host Name (même nom dans le serveur Zabbix)..... 101
Figure 95: Ajout des hôtes..... 105
Figure 96: Les groupes d'hôtes de notre serveur..... 106
Figure 97: Supervision de switch..... 107
Figure 98: Création de community..... 108
Figure 99: Ajout de l'adresse IP de serveur Zabbix 109
Figure 100:on ajoute le firewall dans le serveur Zabbix et on donne le nom de Community et version de Snmp..... 110
Figure 101: l'hôte Zabbix Server..... 110
Figure 102: on ajoute la machine Dmz public et on le donne des templates spécifier 111
Figure 103: on donne l'adresse IP de l'agent installé dans la machine qu'on souhaite de superviser 111
Figure 104: On peut aussi ajouter des items..... 112
Figure 105: dans la machine Dmz publique on configure l'agent et on ajoute l'adresse de serveur Zabbix et le port d'écoute..... 112
Figure 106: Dans les cas où il y a plusieurs serveur Zabbix on spécifier l'adresse de serveur Zabbix et on ajoute le nom de la machine la même qui est dans les serveurs..... 113
Figure 107:1er étape SNMP windows server 113
Figure 108: les étapes d'installation de SNMP Windows server 115
Figure 109:Figure 10 8: Redémarrage de service SNMP 116
Figure 110: Ajoute Community Name et Adresse IP de serveur Zabbix 119
Figure 111: Ajout de la machine Windows Server dans Zabbix 120
Figure 112: Ajoute l'hôte et les templates 120
Figure 113: on ajoute l'adresse IP de l'agent 121
Figure 114: on configure l'agent 121
Figure 115:Dashboard 122
Figure 116: l'état des hôtes..... 124
Figure 117:fichier de formulaire pour ajouter un stagiaire..... 126
Figure 118: modifier un stagiaire 127
Figure 119:liste des stagiaires 127
Figure 120: fichier de migration 128
Figure 121:Model Stagiaire 128
Figure 122: Stagiaire Controller..... 129
Figure 123: les routes 129
Figure 124: layout..... 130
Figure 125: fichier de connexion avec la base de donnée 130
Figure 126: la page home 131
Figure 127: page pour ajouter un nouveau stagiaire 131

Figure 128: exemple d'ajout 132
Figure 129: la liste des stagiaires 133
Figure 130: on peut modifier un stagiaire 133
Figure 131: Stagiaire modifie 134
Figure 132: on clique sur supprimer 134
Figure 133: on clique sur ok pour supprimer le stagiaire 134
Figure 134: page explique l'objectif de l'app 135
Figure 135: toutes les modifications sont appliquées dans DB 135

Liste des abréviations :

A: address

AD CS: Services de Certificate Active Directory

AD: Active Directory

ADFS: Active Directory Federation Services

ADRMS: Active Directory Right Management Services

ADSI : Active Directory Service Interface

ADSL : ligne d'abonné numérique à débit asymétrique (asymmetrica digital subscriber line)

AP: access point ASCII: American Standard Code for Information Interchange

BIND: Berkeley Internet Name Domain

BIOS: Basic Input Output System

CGI: Common gateway interface

CIDR: Classless Inter-Domain Routing, voir CIDR

CIFS: Common Internet File System

CNAME: canonical NAME

CSS: Cascading Style Sheet

DHCP: Dynamic Host Configuration Protocol

HTML: Hypertext Markup Language

HTTP: HyperText Transfert Protocol

HTTPS: hypertext transfer protocol secure

IEEE: Institute of Electrical and Electronics Engineers

IMAP: internet Message Access Protocol

Kbit/s : kilobit par seconde

LAMP : Linux + Apache + MySQL + PHP

LDAP: lightweigt directory access protocol

PERT: Program Evaluation and Review Technique

POP3 : Post Office Protocol version 3

PTR : PoinTeR

RAM : Random Access Memory Secure FTP, le protocole FTP sécurisé par SSL SFTP

SGBD : Système de gestion de base de données

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SOA: Start of Authority

SSH: Secure Shell

SSL: Secure socket layer

SSO: Single Sign-On

TCP/IP: Transmission Protocol/Internet Protocol

TTL: Time-To-Live

UDP: User datagram protocol

URL : Repère uniforme de ressource (Uniform Resource Locator)

UTF-16: Unicode Transformation Format 16 bits

VLAN: Virtual LAN

VM: virtual machine

VMM: virtual machine manager

VoIP : Voice over IP

VRRP : protocole de redondance de routeur virtuel

WWW: World Wide Web (voir Internet)

Introduction Générale :

Toute formation théorique reste inachevée sans une réelle interaction avec le milieu professionnel qui constitue une étape tout à fait primordiale dans le cursus de l'étudiant pour la mise en œuvre de tous les acquis et les capacités développés au cours de sa formation.

L'insertion dans des organismes professionnels devrait dans une parfaite vision, permettre au stagiaire sur le plan technique, la possibilité de mettre en œuvre ses connaissances, de déployer ses efforts et ses acquis pour en acquérir d'autres, et sur le plan humain, de tisser des contacts et de développer certains aspects de sa personnalité en s'engageant au cours de la période du stage à faire de nouvelles connaissances et de développer le sens de la communication afin d'échanger les idées et savoir le maximum du savoir.

Dans le cadre de notre cursus, nous avons eu l'opportunité d'effectuer un stage au sein de le ministère d'enseignement Supérieur et de la Recherche Scientifique et de l'innovation pendant 2 mois. Ce rapport a pour objectif de présenter en détail les missions qui nous avons été confiées, les compétences développées ainsi que les enseignements tirés de cette expérience enrichissante.

Durant ce stage, nous avons eu l'opportunité d'intégrer une équipe dynamique et motivée au sein de la cellule informatique. Tout au long de cette période, Nous avons été accompagnés par M. Mouhcine et M. Hamza BEAJ *qui nous guidait et soutenu dans l'accomplissement de notre mission.*

Pour ce faire on se chargera en premier lieu d'une présentation générale de cadre de projet. En deuxième lieu, nous allons mettre à votre disposition les différentes tâches effectuées lors de stage enfin, nous résumons les apports de ce stage dans une petite conclusion.

Partie I : Présentation du cadre du projet

Présentation de l'organisme d'accueil :

Royaume du Maroc
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique et de l'Innovation

Figure 1: Logo de Enssup

L'ENSSUP (Établissement National des Œuvres Universitaires Sociales et Pédagogiques) au Maroc, relevant du Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation, joue un rôle essentiel dans le soutien et l'accompagnement des étudiants marocains tout au long de leur parcours universitaire. Voici un aperçu de ses missions, objectifs et rôle dans ce domaine :

1. Missions de l'ENSSUP :

- Gérer les œuvres universitaires sociales : L'ENSSUP est chargé de mettre en place et de gérer des services visant à améliorer les conditions de vie des étudiants, tels que la restauration universitaire, les résidences universitaires, les bibliothèques universitaires, les espaces culturels et sportifs, les services de santé, etc.
- Promouvoir les œuvres pédagogiques : L'ENSSUP s'engage à soutenir les initiatives pédagogiques et éducatives, en favorisant l'accès des étudiants à des ressources et des activités liées à leur formation académique.

2. Objectifs de l'ENSSUP :

- Favoriser l'égalité des chances : L'ENSSUP vise à offrir des services et des prestations qui permettent à tous les étudiants, indépendamment de leur situation socio-économique, d'avoir un accès équitable aux conditions de vie et d'études favorables.

- Améliorer les conditions de vie des étudiants : L'ENSSUP s'efforce d'assurer un cadre de vie et d'étude agréable en mettant à disposition des infrastructures adéquates, des équipements de qualité et des services essentiels répondant aux besoins des étudiants.
- Soutenir la réussite académique : L'ENSSUP encourage la réussite des étudiants en leur offrant un environnement propice à l'apprentissage, en proposant des services éducatifs et en favorisant l'épanouissement personnel et intellectuel.

3. Rôle de l'ENSSUP dans le soutien et l'accompagnement des étudiants :

- Restauration universitaire : L'ENSSUP gère les restaurants universitaires qui proposent des repas équilibrés à des tarifs abordables, garantissant ainsi la restauration des étudiants.
- Résidences universitaires : L'ENSSUP offre des places en résidences universitaires, permettant aux étudiants de bénéficier d'un hébergement à proximité de leurs établissements d'enseignement.
- Bourses et aides financières : L'ENSSUP octroie des bourses et des aides financières aux étudiants dans le besoin, afin de les soutenir dans la poursuite de leurs études.
- Services de santé : L'ENSSUP assure l'accès aux soins de santé de base à travers des centres médicaux et des infirmeries présents dans les campus universitaires.
- Activités culturelles et sportives : L'ENSSUP organise des activités culturelles, artistiques et sportives pour enrichir la vie étudiante et promouvoir le développement personnel.
- Services pédagogiques : L'ENSSUP met en place des bibliothèques universitaires, des espaces d'étude et des ressources pédagogiques pour soutenir les étudiants dans leur apprentissage.

4. Administration Centrale :

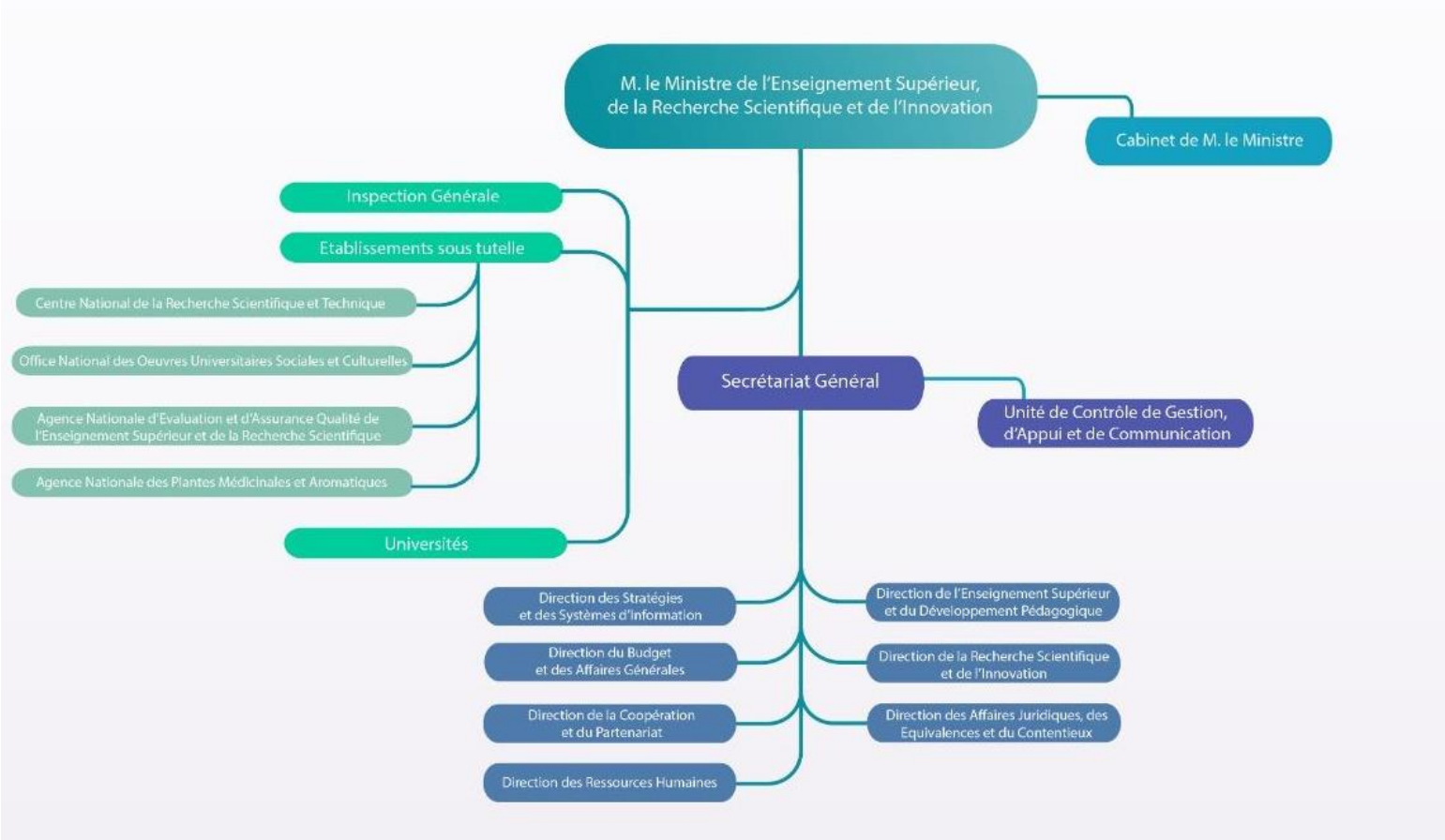


Figure 2: Organigramme Enssup

Le siège de l'ENSSUP inclut :

- ***Secrétariat général :*** La secrétariat général assure, sous l'autorité du ministre, l'animation et la coordination de l'action de l'ensemble des services de l'enseignement supérieur. Il veille à l'application des décisions du ministre.
- ***L'inspection générale :*** L'inspection générale a pour rôle d'informer régulièrement le ministre auquel elle est directement rattachée, sur le fonctionnement des services, d'instruire toute requête qui lui est confiée et de procéder, sur ses instructions, à toutes inspections, enquêtes et études visant notamment une meilleure rentabilisation de l'appareil administratif et universitaire.

- ***Direction de l'enseignement supérieur et du développement pédagogique :*** La direction de l'enseignement supérieur a pour mission de procéder, en collaboration avec les établissements universitaires, au suivi et à la coordination des activités pédagogiques des établissements universitaires et à la supervision de toute réorganisation ou réforme des enseignements universitaires et de procéder à l'évaluation du système d'enseignement supérieur et de recherche scientifique, d'en élaborer les plans de développement universitaires et d'en assurer le suivi.

- ***Direction des affaires juridiques, des équivalences et du contentieux :*** La direction des affaires juridiques a pour mission de suivre toutes les questions à caractère législatif et réglementaire, le contentieux, les dossiers de reconnaissances et d'équivalences de diplômes.

- ***Direction des ressources humaines :*** La direction des ressources humaines a pour mission d'œuvrer à la gestion et à la valorisation des ressources humaines, de veiller à l'optimalisation de l'utilisation des moyens généraux et de promouvoir la communication.

- ***Direction du budget et des affaires générales :*** La direction du budget et des affaires générales a pour mission de définir et mettre en œuvre les programmes de construction, d'aménagement, et de maintenance des bâtiments destinés à recevoir les activités d'enseignement, de recherche, d'hébergement, de sport ou d'administration. En outre, elle procède à l'acquisition, l'installation et la maintenance des équipements nécessaires au bon fonctionnement des institutions et services relevant du ministère.

- ***Division de*** l'informatique : La division de l'informatique, rattachée à la direction du budget et des affaires générales, est chargée de veiller à l'élaboration et à la mise en place d'un schéma directeur informatique de l'administration de l'enseignement supérieur, de concevoir la réalisation technique des solutions informatiques et d'en assurer l'exploitation.

Partie II :
Les tâches effectuées

Gestion de projet :

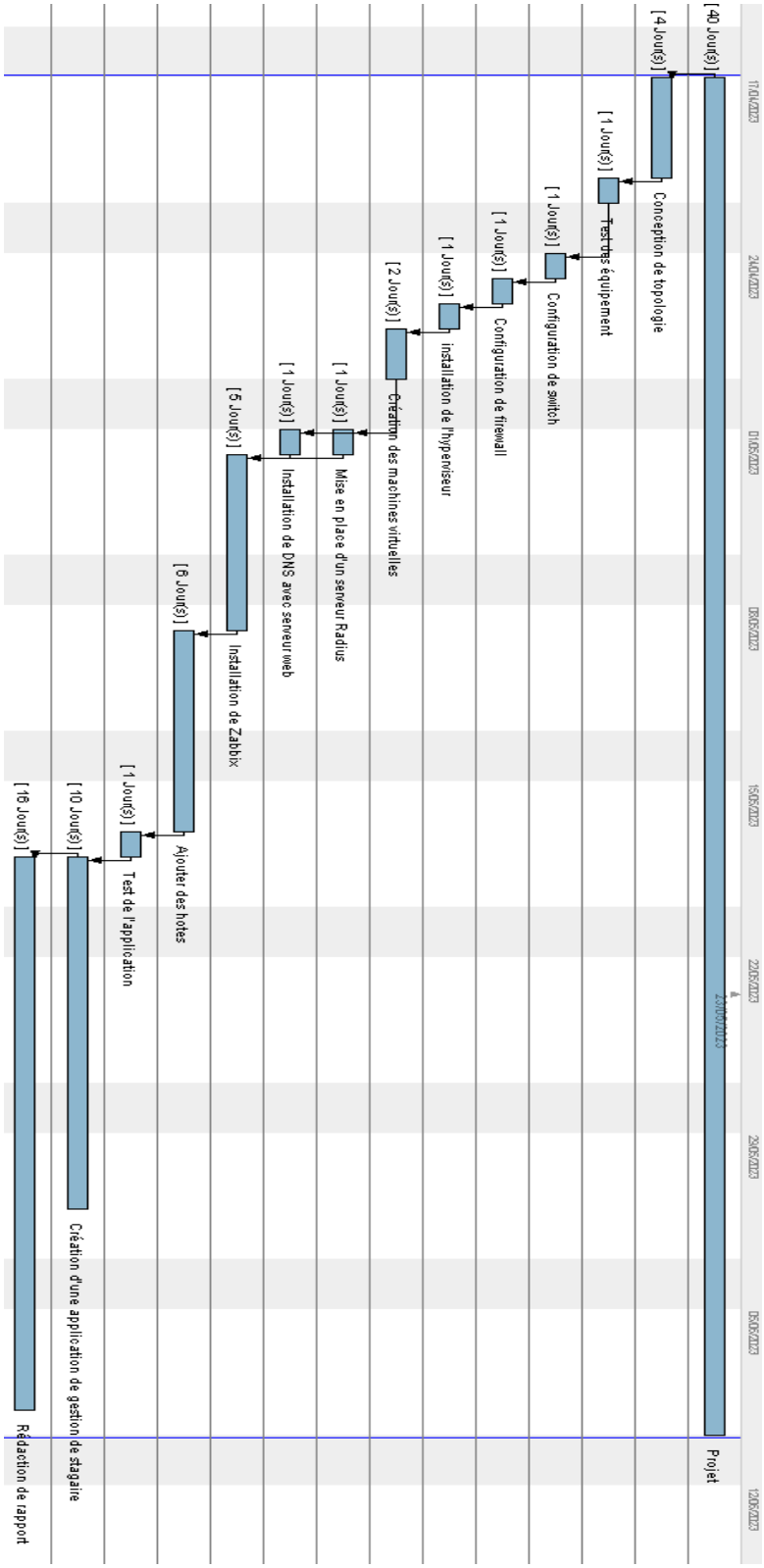
Dans cette partie de notre rapport de stage, nous aborderons les différentes tâches que nous avons réalisées lors de notre expérience au sein de l'organisme. Nous avons eu l'opportunité de travailler sur des projets importants pour notre vie professionnelle, notamment la mise en place d'un réseau local sécurisé et la supervision avec l'outil Zabbix, ainsi que le développement d'une application web utilisant le Framework Laravel. Cette section mettra en évidence les principales activités que nous avons entreprises dans ces domaines, en mettant en avant les résultats et les réalisations significatives de notre travail.

1. Tableau des tâches :

Nom	Date de début	Date de fin
Projet	17/04/2023	09/06/2023
Conception de topologie	17/04/2023	20/04/2023
Test des équipement	21/04/2023	21/04/2023
Configuration de switch	24/04/2023	24/04/2023
Configuration de firewall	25/04/2023	25/04/2023
installation de l'hyperviseur	26/04/2023	26/04/2023
Création des machines virtuelles	27/04/2023	28/04/2023
Mise en place d'un serveur Radius	01/05/2023	01/05/2023
Installation de DNS avec serveur web	01/05/2023	01/05/2023
Installation de Zabbix	02/05/2023	08/05/2023
Ajouter des hotes	09/05/2023	16/05/2023
Test de l'application	17/05/2023	17/05/2023
Création d'une application de gestion de stagaire	18/05/2023	31/05/2023
Rédaction de rapport	18/05/2023	08/06/2023

Tableau 1:Tableau des taches

2. Gantt :



Figure

3. PERT :

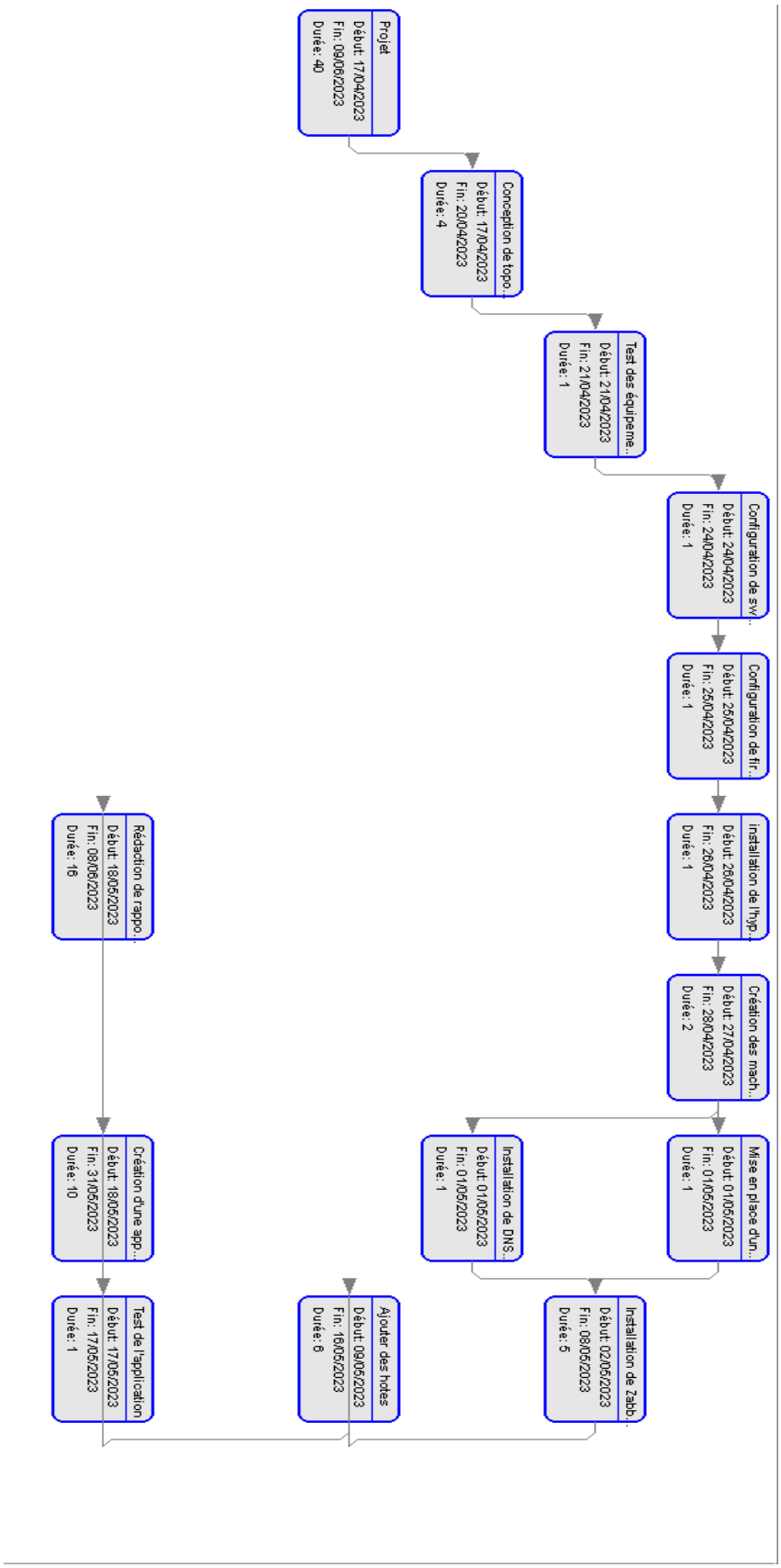


Figure 4:PERT

Chapitre 1 :
Mise en place d'un réseau local sécurisé

I. Cadre général du projet et problématique :

Le cadre général du projet consiste à mettre en place un réseau local sécurisé avec une segmentation en utilisant deux VLAN (Virtual Local Area Network) distincts, à savoir un VLAN administratif et un VLAN pour les employés. De plus, le projet prévoit la création de deux zones DMZ (DeMilitarized Zone) distinctes, l'une publique et l'autre privée pour notre groupe.

La problématique principale du projet est de garantir la sécurité du réseau local tout en permettant une connectivité et une communication efficace entre les différents segments. Il s'agit de mettre en œuvre une architecture réseau qui offre des niveaux de sécurité appropriés pour les différentes zones du réseau, tout en maintenant la connectivité entre elles de manière contrôlée.

Les objectifs spécifiques du projet peuvent inclure :

- Configuration des VLANs : Définir et configurer les deux VLANs nécessaires, à savoir le VLAN administratif et le VLAN employé, pour segmenter le réseau en fonction des rôles et des autorisations.
- Mise en place des zones DMZ : Configurer les deux zones DMZ distinctes, une zone publique et une zone privée, afin d'isoler les services publics des ressources internes sensibles.
- Sécurité du réseau : Mettre en place des mesures de sécurité appropriées telles que des pare-feux, des politiques de sécurité, des contrôles d'accès, des listes de contrôle d'accès (ACL) pour protéger le réseau contre les menaces et les accès non autorisés.
- Gestion des accès : Définir des politiques de gestion des accès pour contrôler les permissions et les restrictions d'accès au réseau et aux différentes zones, en utilisant des mécanismes d'authentification et d'identification tels que les VLANs et les sous-réseaux.

- Surveillance et gestion : Mettre en place des outils de surveillance et de gestion du réseau pour détecter et prévenir les incidents de sécurité, assurer la disponibilité des services et faciliter la gestion quotidienne du réseau.

La réalisation de ce projet nécessitera une analyse approfondie des besoins de l'organisation, la conception d'une architecture réseau adaptée, la configuration des équipements réseau (routeurs, commutateurs, pare-feux), ainsi que des tests et une validation rigoureuse pour s'assurer de la sécurité et de la fonctionnalité optimale du réseau local.

II. Architecture proposée :

1. Schéma de l'architecture globale de notre réseau :

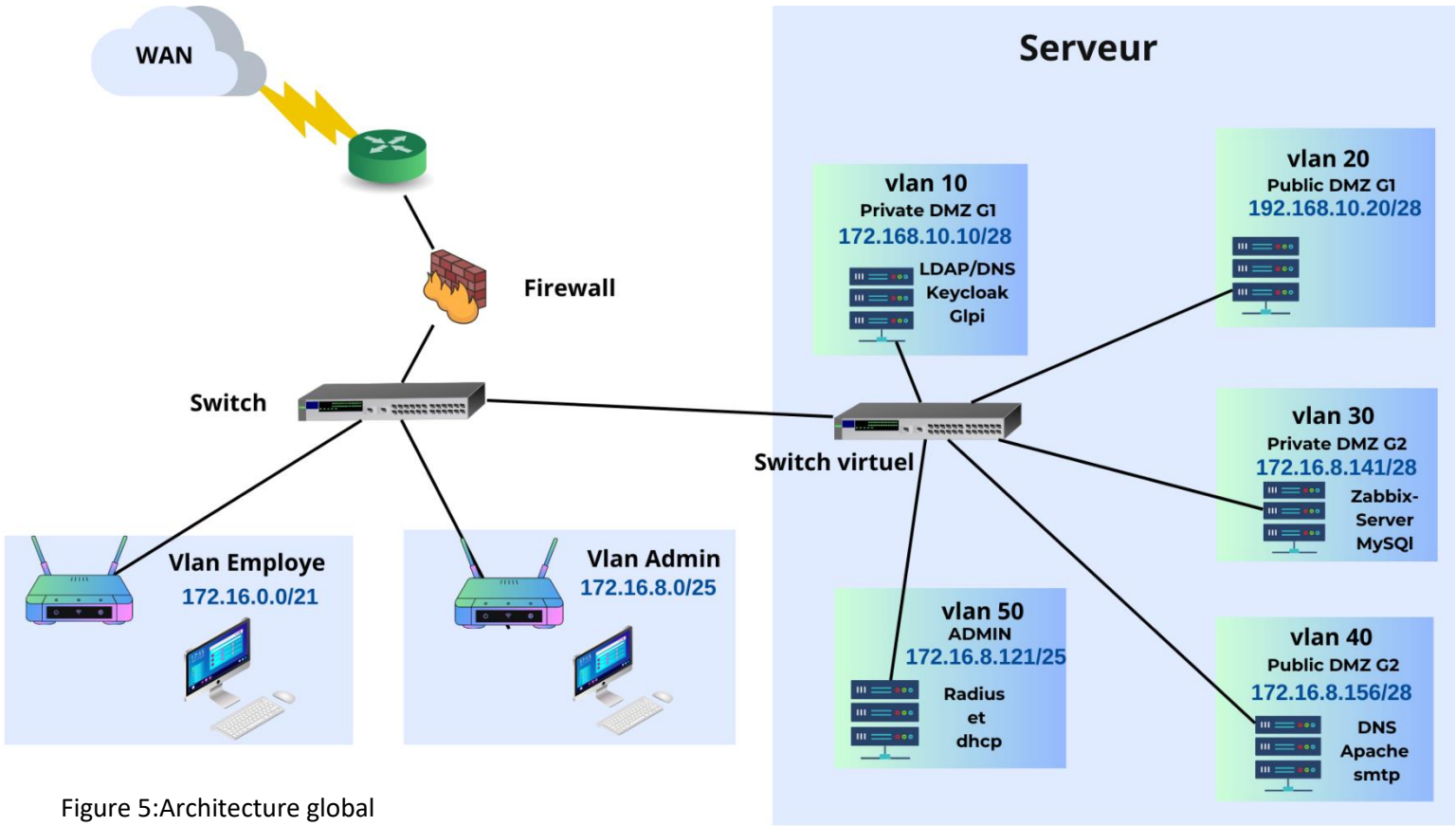


Figure 5:Architecture global

Dans notre infrastructure, nous avons opté pour la mise en place de quatre zones DMZ distinctes pour des raisons de séparation des responsabilités et de sécurité. Cette décision découle du fait que nous sommes un groupe de stage composé de quatre personnes, travaillant en binômes sur des projets et services différents, tout en utilisant les mêmes équipements tels que le pare-feu FortiGate, le serveurs DELL et le switch Dell.

En attribuant deux zones DMZ à chaque binôme, une privée et l'autre publique, nous avons pu assurer une isolation efficace des différents services et projets, garantissant ainsi la confidentialité et l'intégrité des données spécifiques à chaque binôme. Cette approche permet également de limiter les interférences potentielles entre les différentes applications et de faciliter la gestion des accès et des autorisations.

En outre, en attribuant des zones DMZ spécifiques à chaque binôme, nous avons pu organiser de manière cohérente les flux de trafic et les politiques de sécurité correspondantes. Chaque binôme est responsable de la configuration et de la gestion de ses propres zones DMZ, ce qui permet une plus grande efficacité dans la maintenance et la résolution des problèmes liés à leurs projets respectifs.

En résumé, la mise en place de quatre zones DMZ distinctes dans notre infrastructure, attribuées à chaque binôme, garantit la séparation des responsabilités, la sécurité des données et facilite la gestion des projets individuels. Cette approche assure également une cohérence dans la configuration et la gestion des équipements communs tels que le pare-feu, les serveurs et les commutateurs, tout en permettant à chaque binôme de travailler de manière autonome sur leurs services spécifiques.

2. Tableau d'adressage :

Tableau 2: Tableau d'adressage

VLANS	Adresse réseau	Passerelle
Vlan Employé	***172.16.0.0/21***	***172.16.7.254***
Vlan Admin	***172.16.8.0/25***	***172.16.8.126***
DMZ privée	***172.16.8.128/28***	***172.16.8.142***
DMZ public	***172.16.8.144/28***	***172.16.8.158***

III. Etude et configuration de matériel :

1. Le switch :

Un switch, dit aussi commutateur réseau, est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels, de recevoir des informations et de les envoyer vers un destinataire précis sur le réseau en les dirigeant sur le port adéquat, c'est donc un système de communication dans lequel les données d'un utilisateur source peuvent circuler sur différents circuits réels dans la même communication, afin d'atteindre l'utilisateur de destination. Le switch établit et met à jour une table, contenant des adresses MAC associes à des ports, autrement chaque port a une adresse MAC dans le cas du commutateur pour un réseau Ethernet, cela pour lui indiquer sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port. Il relie les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames. Intervenant au niveau de la couche 2, lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, il ouvre un circuit virtuel unique entre

les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports. Si l'adresse du destinataire est inconnue dans la table, alors la trame est traitée comme un broadcast.

a. Avantages :

- Réduction du nombre de collisions
- Multiples communications simultanément
- Amélioration de la réponse du réseau (augmentation la bande passante disponible)
- Hausse de la productivité de l'utilisateur

b. Les types de switches :

En ce qui précède, nous avons mis le point sur un switch Ethernet, à ce niveau nous allons différencier entre 3 types de switches Ethernet : les non mangeables, les ‘ smart switch ' puis les mangeables.

- **Switch mangeable :**

En général, les switches mangeables adoptent les protocoles SNMP qui permettent aux utilisateurs de surveiller l'état du switch et de ses ports, vous permettent de visualiser le débit, l'utilisation des ports, etc. Les switches Ethernet mangeables sont conçus pour les charges de travail élevées, le trafic important et les déploiements qui nécessitent des configurations personnalisées. Dans les grands centres de données et les réseaux d'entreprise, les switches entièrement mangeables sont souvent utilisés comme couche centrale du réseau, offrant un large éventail d'outils et de capacités.

Figure 6:switch

- **Switch non mangeable :**

Les switches non mangeables sont des dispositifs prêts à l'emploi sans options de configuration, de gestion ou de surveillance à distance. Vous ne pouvez pas vous connecter à un switch non mangeable, ni lire l'utilisation des ports ou le débit de l'appareil. Les switches non mangeables ont une configuration fixe et fournissent aux périphériques Ethernet des connexions réseau afin qu'ils puissent communiquer entre eux.

Les switches non mangeables sont utilisés dans les petits réseaux ou pour ajouter des groupes de périphériques provisoires à un réseau plus grand, pour augmenter le nombre de ports Ethernet et connecter les points chauds du réseau ou périphériques dans les petits réseaux indépendants.

Figure 7:switch non

- **Switch intelligent :**

Les switches intelligents (smart manage switch en anglais) sont généralement administrés via un navigateur Web, ce qui permet aux utilisateurs d'assurer la maintenance de leur réseau grâce à un guidage intuitif. Ces switches Ethernet intelligents sont particulièrement adaptés aux entreprises qui ont besoin d'une gestion de la sécurité et du dépannage à distance, permettant aux gestionnaires de réseau de surveiller et de contrôler le trafic afin d'obtenir des performances et une fiabilité optimale du réseau. Les switches intelligents ont émergé comme une solution viable pour les PME, avec comme principal avantage la possibilité de modifier la configuration du switch pour répondre à vos besoins spécifiques en matière de réseau.

Figure 8: smart manager switch

c. Les caractéristiques de notre switch DELL N2048P :

Figure 9: Dell N2048P

Le switch Dell N2048P est un commutateur réseau de la gamme Dell Networking, conçu pour offrir des performances élevées, une connectivité fiable et des fonctionnalités avancées. Voici certaines des principales fonctionnalités du commutateur Dell N2048P :

- Ports : Le switch Dell N2048P dispose de 48 ports Ethernet 10/100/1000 Mbps pour la connectivité des appareils. Il prend également en charge les connexions à haut débit avec quatre ports SFP+ pour des liens 10 GbE.
- Power over Ethernet (PoE) : Le N2048P est un modèle PoE, ce qui signifie qu'il est capable d'alimenter des périphériques réseaux compatibles avec la norme PoE, tels que des points d'accès sans fil, des téléphones IP ou des caméras de sécurité, directement via les ports Ethernet.
- Capacité de commutation : Le commutateur offre une capacité de commutation de 176 Gbps, permettant un débit élevé et une gestion efficace du trafic réseau.
- Gestion avancée : Le switch Dell N2048P prend en charge des fonctionnalités de gestion avancées, telles que l'administration en ligne de commande (CLI), l'interface graphique utilisateur (GUI), la gestion SNMP et la prise en charge du protocole de gestion de réseau simple (SNMP)
- Fonctionnalités de sécurité : Le N2048P offre des fonctionnalités de sécurité avancées, telles que la protection contre les attaques par déni de service (DoS), le contrôle d'accès basé sur les ports (802.1X), l'authentification RADIUS, les listes de contrôle d'accès (ACL) et la détection d'intrusion.
- VLANs et agrégation de liens : Le commutateur prend en charge la création de VLANs pour la segmentation du réseau, ainsi que l'agrégation de liens (LACP) pour une utilisation efficace de la bande passante.
- Qualité de service (QoS) : Le N2048P offre des fonctionnalités de QoS pour prioriser le trafic sensible, assurant ainsi une performance optimale pour les applications critiques.

- Redondance et haute disponibilité : Le switch prend en charge des fonctionnalités de redondance, telles que le protocole de redondance des commutateurs (STP) et le protocole de redondance de lien (LACP), pour assurer la disponibilité du réseau en cas de défaillance d'un lien ou d'un équipement.

d. Configuration de switch :

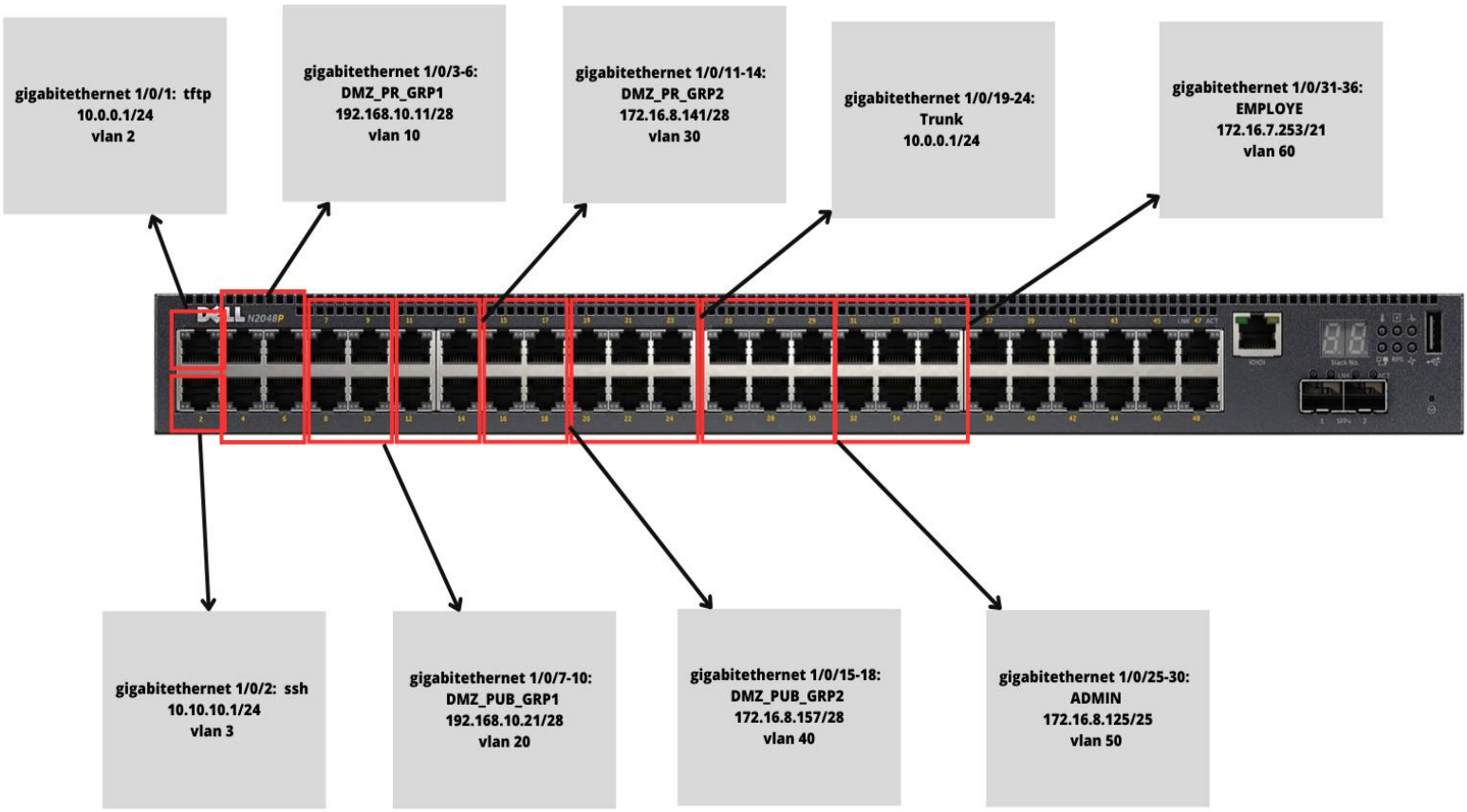


Figure 10:configuration de

```
console(config)#username STAGE password STAGE2023@ privilege 1
console(config)#enable password STAGE2023@
console(config)#hostname STAGE
```

Figure 11: configuration de base

```
STAGE(config)#vlan 2
STAGE(config-vlan2)#name tftp
STAGE(config-vlan2)#vlan 3
STAGE(config-vlan3)#name ssh
STAGE(config-vlan3)#vlan 10
STAGE(config-vlan10)#name DMZ_PR_GP1
STAGE(config-vlan10)#vlan 20
STAGE(config-vlan20)#name DMZ_PUB_GP1
STAGE(config-vlan20)#vlan 30
STAGE(config-vlan30)#name DMZ_PR_GP2
STAGE(config-vlan30)#vlan 40
STAGE(config-vlan40)#name DMZ_PUP_GP2
STAGE(config-vlan40)#vlan 50
STAGE(config-vlan50)#ADMIN
```

Figure 13: création des vlans 1

```
STAGE(config-vlan50)#name ADMIN
STAGE(config-vlan50)#vlan 60
STAGE(config-vlan60)#name EMPLOYE
STAGE(config-vlan60)#EXIT
STAGE(config)#interface gigabitethernet 1/0/1
STAGE(config-if-Gi1/0/1)#switchport mode access
STAGE(config-if-Gi1/0/1)#switchport access
Command not found / Incomplete command. Use ? to list commands.
STAGE(config-if-Gi1/0/1)#switchport access vlan 2
STAGE(config-if-Gi1/0/1)#no shutdown
STAGE(config-if-Gi1/0/1)#exit
STAGE(config)#interface gigabitethernet 1/0/2
STAGE(config-if-Gi1/0/2)#switchport mode access
STAGE(config-if-Gi1/0/2)#switchport access vlan 3
STAGE(config-if-Gi1/0/2)#no shutdown
STAGE(config-if-Gi1/0/2)#exit
STAGE(config)#interface range gigabitethernet 1/0/3-6
STAGE(config-if)#switchport mode access
STAGE(config-if)#switchport access vlan 10
STAGE(config-if)#no shutdown
STAGE(config-if)#exit
```

Figure 12:affectation des ports aux vlans

```
STAGE(config)#interface range gigabitethernet 1/0/7-10
STAGE(config-if)#switchport mode access
STAGE(config-if)#switchport access vlan 20
STAGE(config-if)#no shutdown
STAGE(config-if)#exit
STAGE(config)#interface range gigabitethernet 1/0/11-14
STAGE(config-if)#switchport mode access
STAGE(config-if)#switchport access vlan 30
STAGE(config-if)#no shutdown
STAGE(config-if)#exit
STAGE(config)#interface range gigabitethernet 1/0/15-18
STAGE(config-if)#switchport mode access
STAGE(config-if)#switchport access vlan 40
STAGE(config-if)#no shutdown
STAGE(config-if)#exit
STAGE(config)#interface range gigabitethernet 1/0/19-24
STAGE(config-if)#switchport mode trunk
STAGE(config-if)#switchport trunk allowed vlan all
STAGE(config-if)#no shutdown
STAGE(config-if)#exit
STAGE(config)#interface range gigabitethernet 1/0/25-30
```

Figure 14: affectation des ports aux vlans et création des ports trunk

```
STAGE(config)#interface range gigabitethernet 1/0/25-30

STAGE(config-if)#switchport mode access

STAGE(config-if)#switchport access vlan 50

STAGE(config-if)#no shutdown

STAGE(config-if)#exit

STAGE(config)#interface range gigabitethernet 1/0/31-36

STAGE(config-if)#switchport mode access

STAGE(config-if)#switchport access vlan 60

STAGE(config-if)#no shutdown

STAGE(config-if)#exit

STAGE(config)#exit

STAGE#copy running-config startup-config

This operation may take few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!
STAGE#configure t

STAGE(config)#interface vlan 50

STAGE(config-if-vlan50)#ip address 172.16.8.125 255.255.255.128
```

Figure 15: affectation des ports et les adresses aux vlans

```
STAGE(config-if-vlan50)#interface vlan 60

STAGE(config-if-vlan60)#ip address 172.16.7.253 255.255.248.0

STAGE(config-if-vlan60)#interface vlan 2

STAGE(config-if-vlan2)#ip address 10.10.10.1 255.255.255.0

STAGE(config-if-vlan2)#interface vlan 3

STAGE(config-if-vlan3)#ip address 10.10.20.1 255.255?

STAGE(config-if-vlan3)#ip address 10.10.20.1 255.255.255?

STAGE(config-if-vlan3)#ip address 10.10.20.1 255.255.255.0

STAGE(config-if-vlan3)#interface vlan 10

STAGE(config-if-vlan10)#ip address 192.168.10.11 255.255.255.240

STAGE(config-if-vlan10)#interface vlan 20

STAGE(config-if-vlan20)#ip address 192.168.10.21 255.255.255.240

STAGE(config-if-vlan20)#interface vlan 30

STAGE(config-if-vlan30)#ip address 172.16.8.141

Command not found / Incomplete command. Use ? to list commands.

STAGE(config-if-vlan30)#ip address 172.16.8.141 255.255.255.240

STAGE(config-if-vlan30)#interface vlan 40

STAGE(config-if-vlan40)#ip address 172.16.8.157 255.255.255?

STAGE(config-if-vlan40)#ip address 172.16.8.157 255.255.255.240

STAGE(config-if-vlan40)#exit

STAGE(config)#exit
```

Figure 16: affectation les adresses aux vlans

2. Parfeu :

Un firewall (pare-feu en français) est un dispositif de sécurité informatique qui surveille et contrôle le trafic réseau entrant et sortant d'un système informatique ou d'un réseau. Son rôle est de filtrer les données qui circulent sur le réseau et de bloquer les communications non autorisées ou dangereuses.

Le firewall est généralement configuré pour autoriser ou bloquer le trafic en fonction des règles définies par l'administrateur réseau. Les règles peuvent être basées sur différents critères, tels que l'adresse IP source, l'adresse IP de destination, le port utilisé ou encore le type de protocole.

En résumé, le firewall est un élément essentiel de la sécurité informatique, qui permet de protéger les systèmes et les réseaux des menaces extérieures telles que les attaques de hackers, les virus, les logiciels malveillants ou les tentatives d'intrusion.

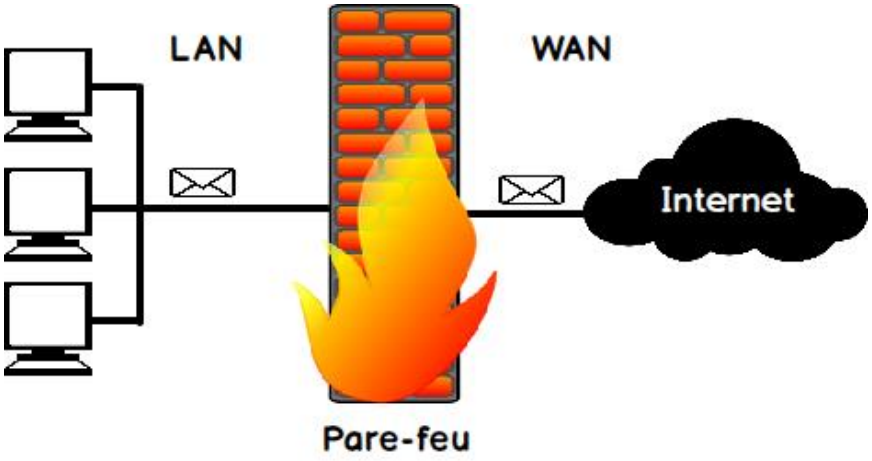


Figure 17:parfeu

a. Les concepts de pare-feu :

Les principaux concepts de pare-feu sont :

- Le filtrage de paquets, pour filtrer les paquets de la couche réseau (IP, etc.)

- Le filtrage à mémoire, pour filtrer les paquets de manière dynamique en adaptant les règles de filtrage.
- La passerelle de niveau circuit, pour filtrer les paquets en gérant le concept de session.
- La passerelle de niveau applicatif, pour filtrer jusqu'aux protocoles des couches applicatives.

b. Les différents types de firewall :

- ***Les firewall bridges :***

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de les contourner.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence. Ces firewalls se trouvent typiquement sur les Switches.

- *Les avantages :*
  - ✓ Impossibles de l'éviter (les paquets passeront par ses interfaces)

- ✓ Peu coûteux

- *Les inconvénients :*
  - ✓ Possibilité de le contourner (il suffit de passer outre à ses règles)
  - ✓ Configuration souvent contraignante
  - ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless)

- ***Les firewalls matériels :***

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur.

De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés).

Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr. Son administration est souvent plus aisée que les firewalls bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente.

Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout firewall. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur

du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoins et choisir le constructeur du routeur avec soin.

- *Les avantages :*
  - ✓ Intégré au matériel réseau
  - ✓ Administration relativement simple
  - ✓ Bon niveau de sécurité

- *Les inconvénients :*
  - ✓ Dépendant du constructeur pour les mises à jour
  - ✓ Souvent peu flexibles.

- ***Les firewalls logiciels :***

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories *:*

- *Les firewalls personnels :*

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés.

En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

- ✓ *Avantages :*

- Sécurité en bout de chaîne (le poste client)
- Personnalisable assez facilement

✓ *Inconvénients :*

- Facilement contournable
- Difficiles à départager de par leur nombre énorme

- *Les firewalls plus « sérieux » :*

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme.

✓ *Avantages :*

- Personnalisables
- Niveau de sécurité très bon

✓ *Inconvénients :*

Nécessite une administration système supplémentaire.

Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le firewall. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications… chose qui induit déjà une

intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du firewall.

c. Notre Firewall FortiGate 500D :

Figure 18:firewall FortiGate 500D

Le pare-feu FortiGate 500D est un équipement de sécurité réseau avancé conçu pour fournir une protection complète et des fonctionnalités de sécurité avancées. Voici quelques-unes des caractéristiques clés du pare-feu FortiGate 500D :

- Débit élevé : Le FortiGate 500D offre un débit de pare-feu élevé, permettant de traiter rapidement et efficacement le trafic réseau sans sacrifier les performances.
- Pare-feu de nouvelle génération : Il dispose d'une architecture de pare-feu de nouvelle génération (NGFW) qui intègre des fonctionnalités avancées telles que l'inspection approfondie des paquets (DPI), la prévention des intrusions (IPS), le filtrage du contenu, le contrôle d'applications, etc.
- VPN sécurisé : Le pare-feu FortiGate 500D prend en charge les connexions VPN sécurisées, notamment les protocoles IPSec et SSL VPN, permettant aux utilisateurs distants de se connecter au réseau en toute sécurité.
- Fonctionnalités avancées de sécurité : Il offre une gamme de fonctionnalités de sécurité avancées telles que l'antivirus, l'anti-spam, la détection des intrusions, la prévention des fuites de données (DLP), le filtrage web, la protection contre les botnets, etc.

- Haute disponibilité : Le FortiGate 500D prend en charge les configurations de haute disponibilité, permettant d'assurer une continuité de service en cas de défaillance matérielle ou de perte de connectivité.
- Gestion centralisée : Il peut être géré de manière centralisée via le Fortinet Security Management Server (FortiManager), offrant une administration simplifiée et une visibilité complète sur l'ensemble du réseau.
- Intégration avec FortiGuard Services : Le pare-feu FortiGate 500D peut être intégré aux services de sécurité basés sur le cloud de Fortinet, tels que le filtrage web FortiGuard, les services de réputation IP, les mises à jour de signatures d'intrusion, etc.
- Extensibilité : Il offre des emplacements pour des modules d'extension supplémentaires, tels que des cartes d'interface réseau (NIC), permettant de personnaliser et d'étendre les capacités du pare-feu en fonction des besoins spécifiques de l'entreprise.

Ces caractéristiques font du pare-feu FortiGate 500D un choix populaire pour les entreprises qui recherchent une solution de sécurité réseau complète, offrant à la fois des performances élevées et une protection avancée contre les menaces.

d. Configuration de Firewall FortiGate 500D :

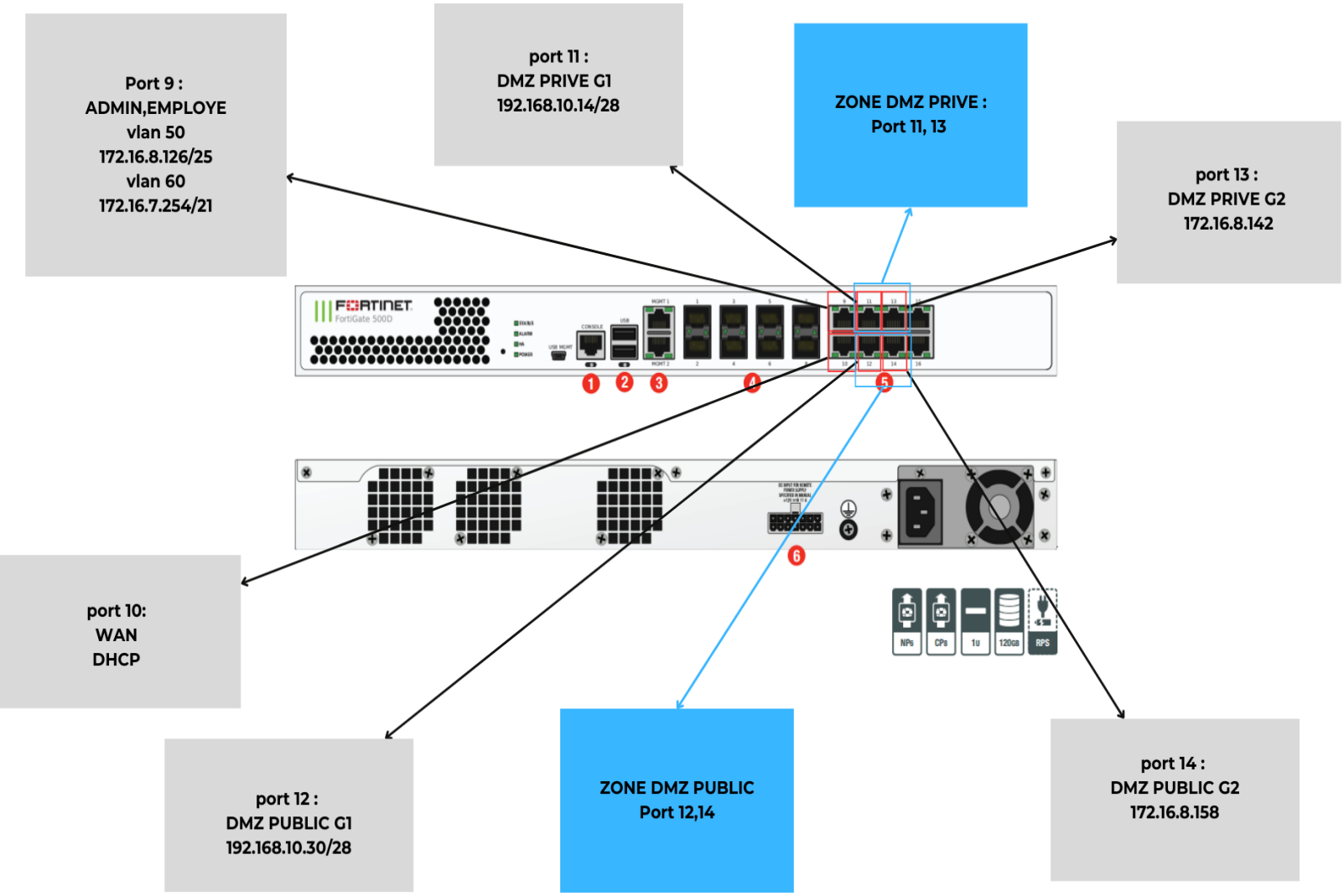


Figure 19: configuration de FortiGate

- **Création des zones Dmz :**

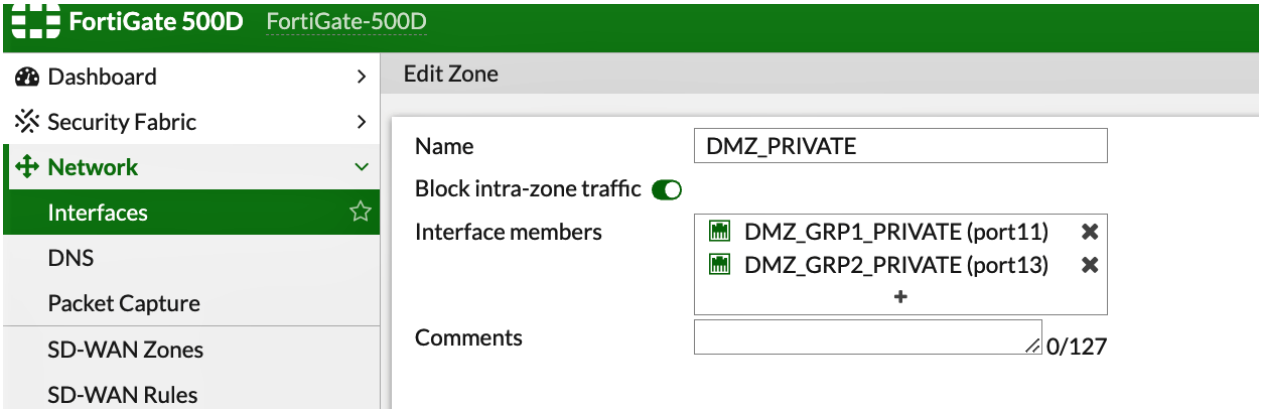


Figure 20:création zone Dmz privée

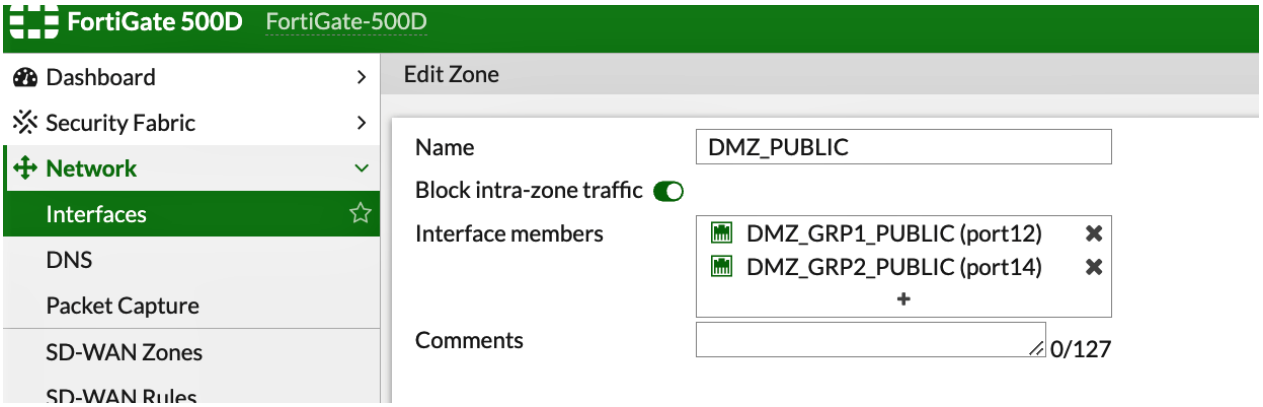


Figure 21:création de zone Dmz publique

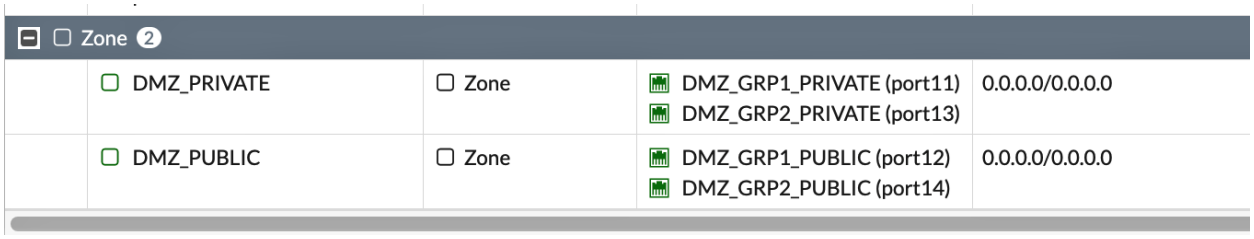


Figure 22: les zones Dmz

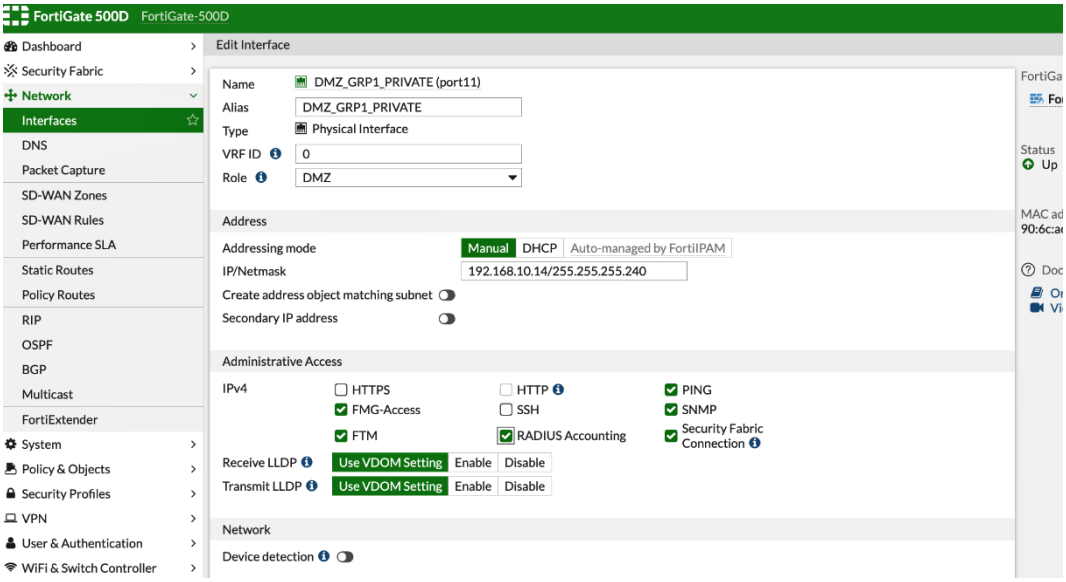


Figure 23:private Dmz de 1er Groupe

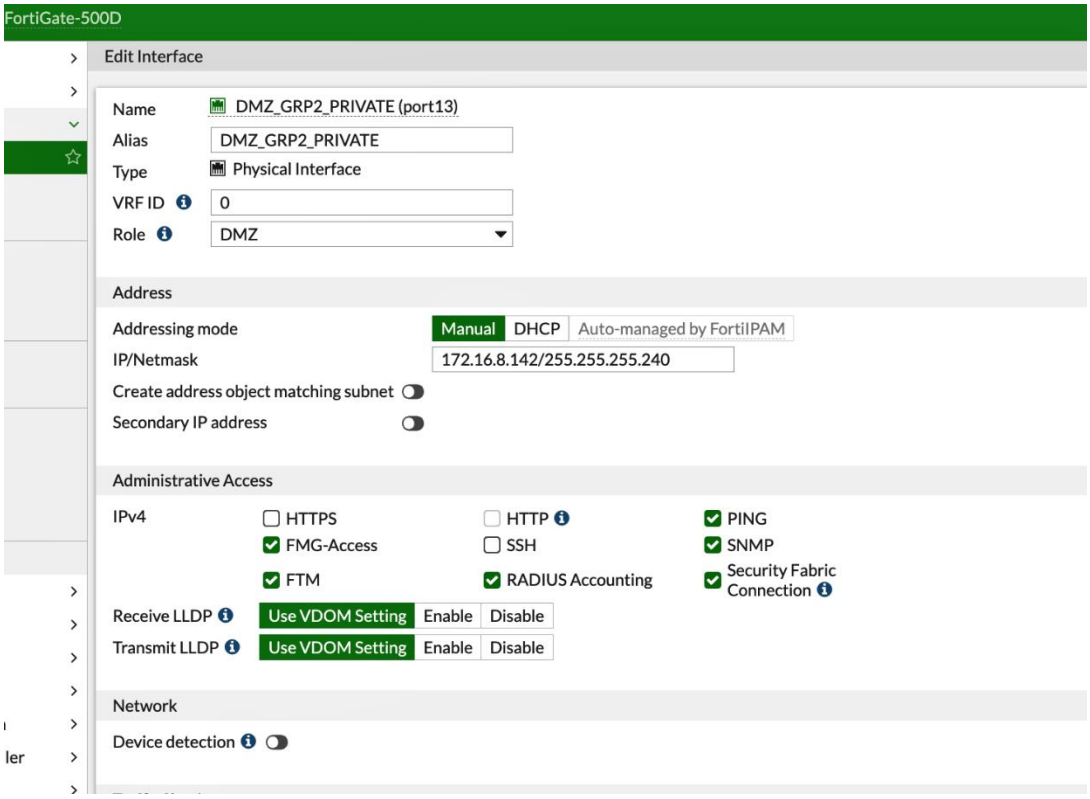


Figure 24:Dmz privée pour 2éme

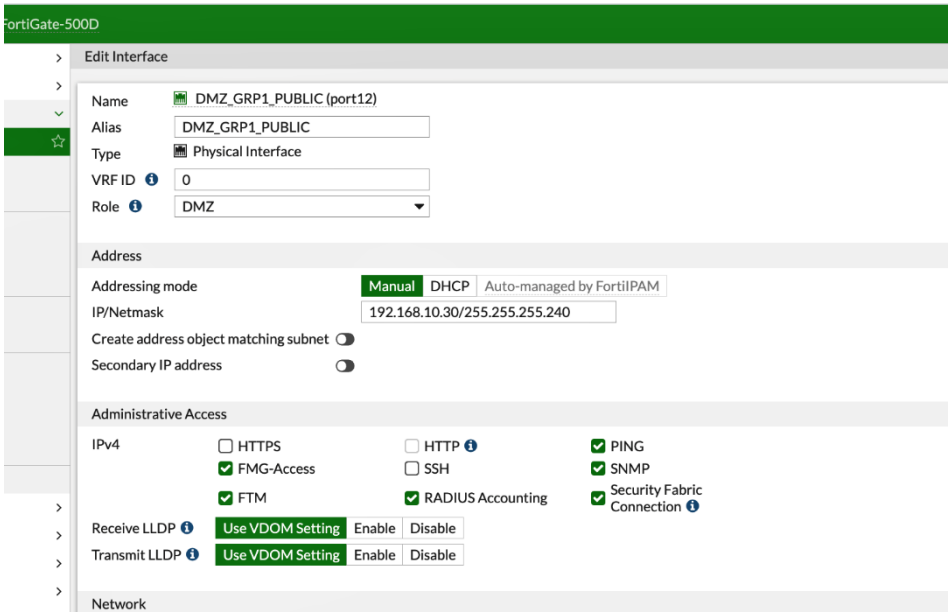


Figure 25:Dmz publique 1er Groupe

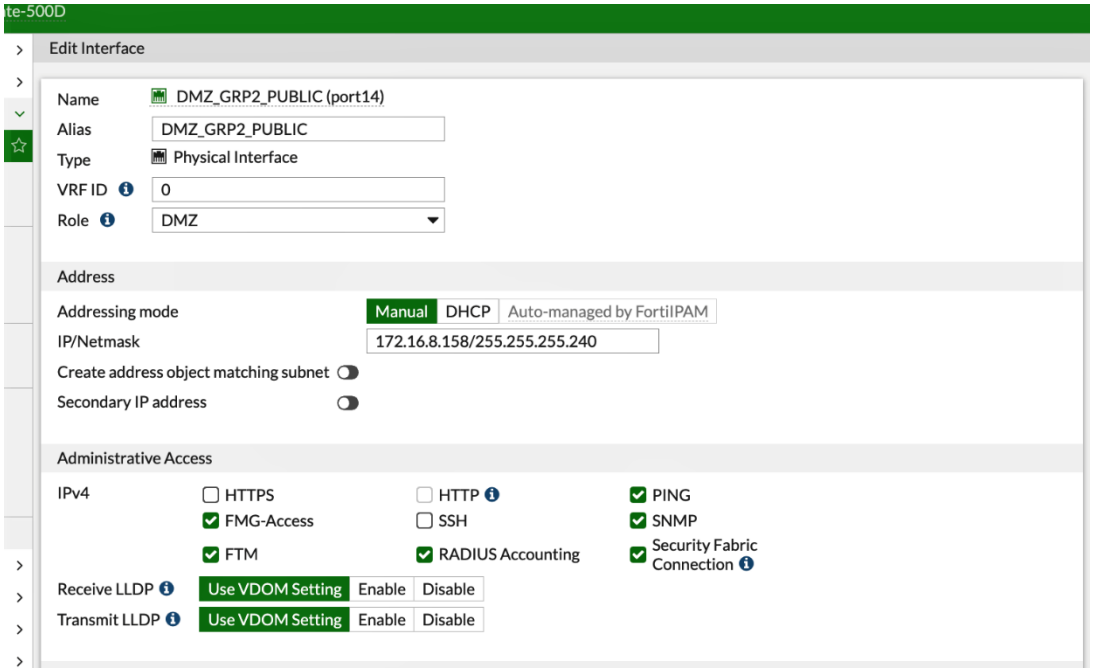


Figure 26:Dmz publique pour 2éme

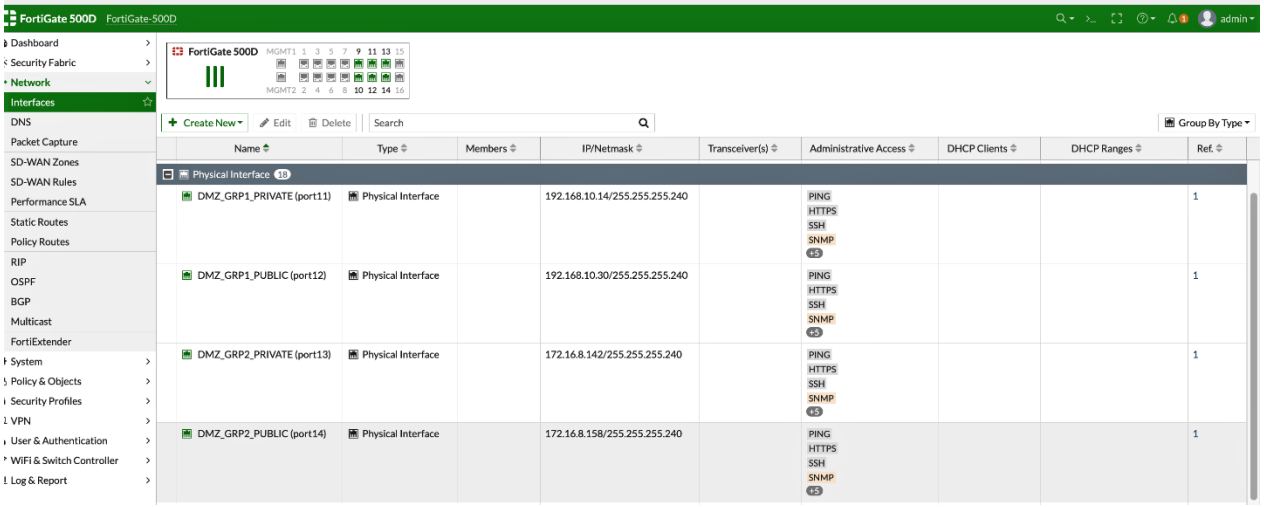


Figure 27: Toutes les interfaces Dmz

- **Création des Vlans :**

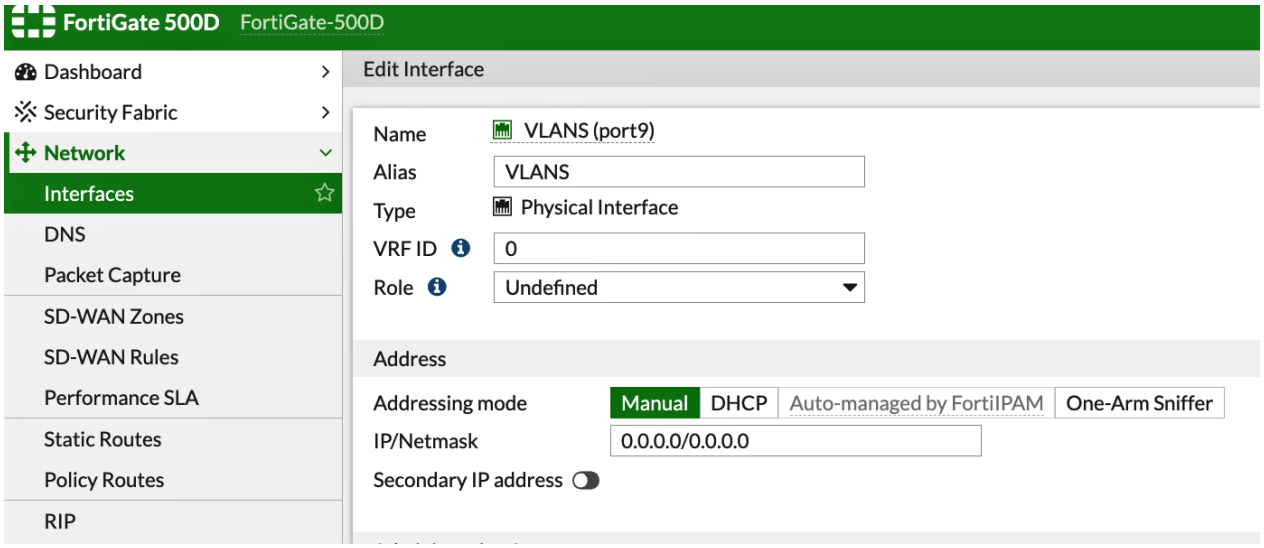


Figure 28: Réservation de ports 9 pour routage

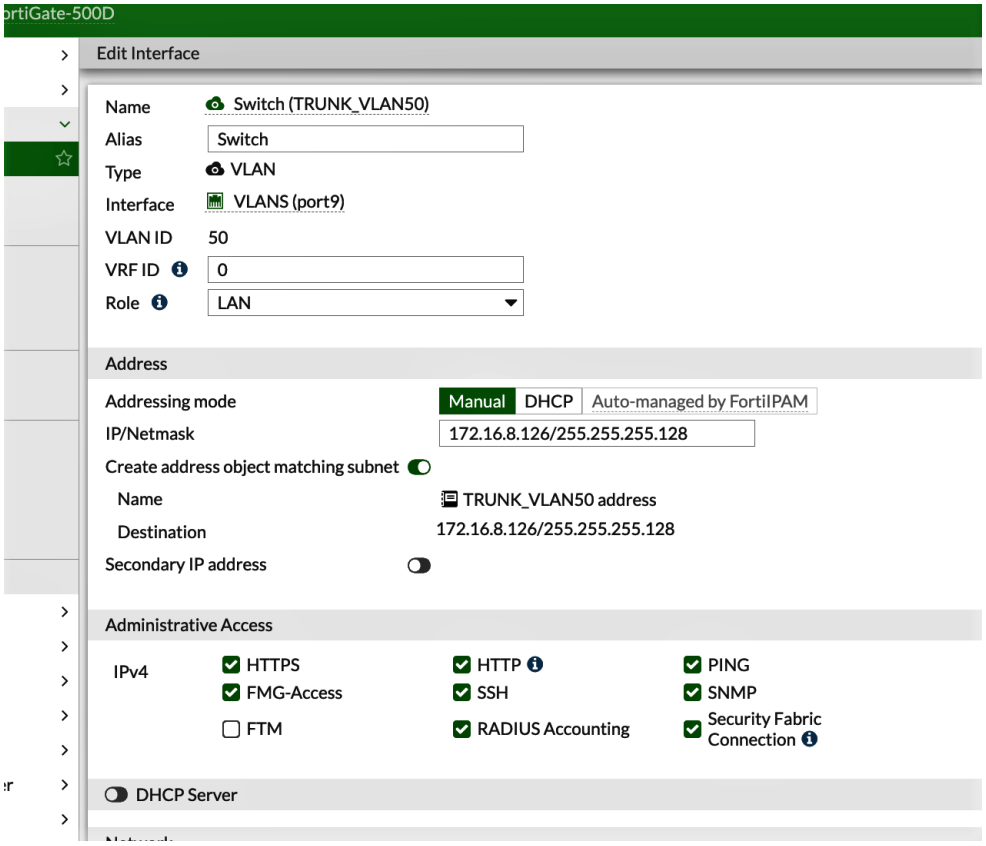


Figure 29: assigner une adresse IP (passerelle) au réseau virtuel

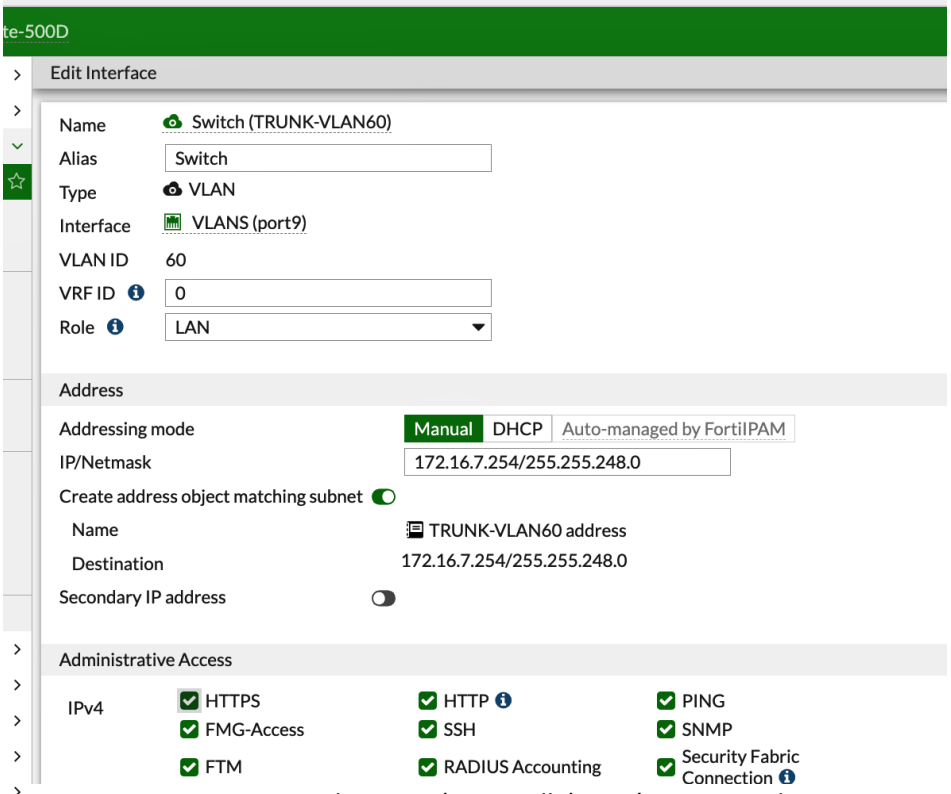


Figure 30: assigner une adresse IP (passerelle) au réseau virtuel

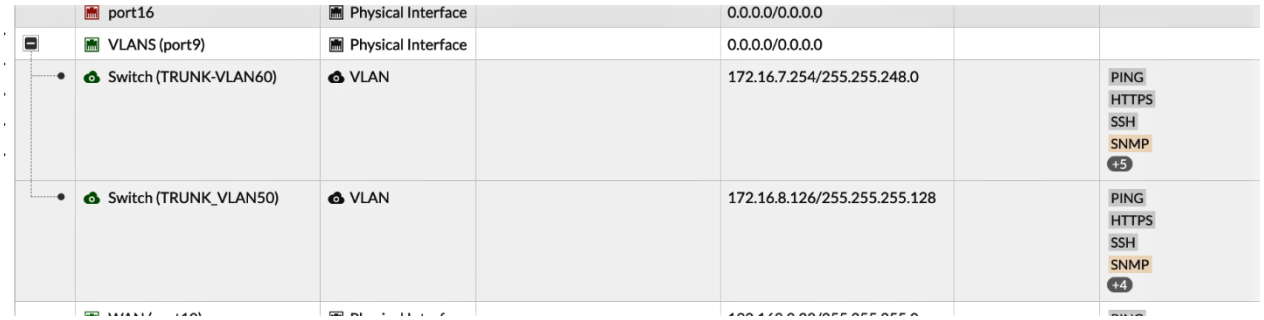


Figure 31:Vlans

- **WAN :**

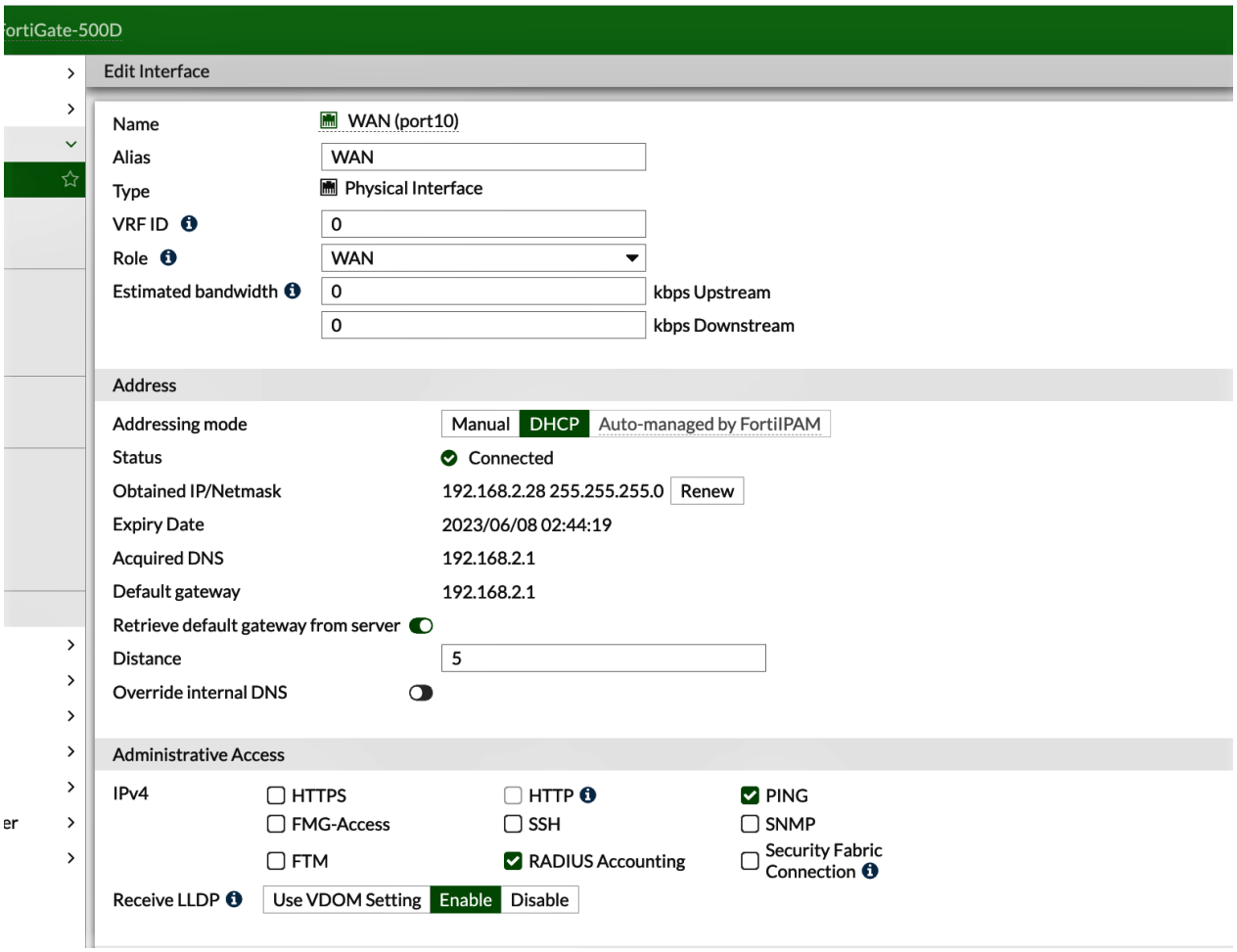


Figure 32:Création de l’interface WAN

					SNMP +4
WAN (port10)	Physical Interface		192.168.2.28/255.255.255.0		PING RADIUS Accounting
Virtual Wire Pair 3					

Figure 33:Inteface WAN

- **Ipv4 Policy (Politique de sécurité) :**

Aucun trafic ne peut passer par une unité de FortiGate à moins que spécifiquement ait permis par une politique de sécurité. Une fois qu'on permet le trafic, pratiquement toutes les caractéristiques de FortiGate sont appliquées au trafic permis par des politiques de sécurité.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
DMZ_PRIVATE → DMZ_PUBLIC 1									
DMZ_PRIVE->DMZ_PUBLIC	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	2.59 MB
DMZ_PRIVATE → Switch (TRUNK_VLAN50) 1									
DMZprivate->ADMIN	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	54.58 kB
DMZ_PRIVATE → WAN (port10) 1									
DMZ_PRIVATE->WAN	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	733.13 MB
DMZ_PUBLIC → DMZ_PRIVATE 1									
DMZ_PUBLIC->DMZ_PRIVEE	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	68.69 kB
DMZ_PUBLIC → WAN (port10) 1									
DMZ_PUBLIC->WAN	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	216.09 MB
Switch (TRUNK_VLAN50) → DMZ_PRIVATE 1									
ADMIN->DMZ_PRIVATE	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	22.51 MB
Switch (TRUNK_VLAN50) → DMZ_PUBLIC 1									
ADMIN->DMZ_PUBLIC	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
Switch (TRUNK_VLAN50) → Switch (TRUNK-VLAN60) 1									
ADMIN->EMPLOYE	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
Switch (TRUNK_VLAN50) → WAN (port10) 1									
ADMIN->WAN	Vlan Admin	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	3.45 GB
Switch (TRUNK-VLAN60) → DMZ_PUBLIC 1									
EMPLOYE->DMZ_PUBLIC	all	all	always	DHCP DNS FTP HTTP HTTPS IMAP IMAPS POP3 POP3S SMTP	ACCEPT	Enabled	no-inspection	Disabled	0 B
Switch (TRUNK-VLAN60) → WAN (port10) 1									
EMPLOYE->WAN	all	all	always	ALL_ICMP HTTP HTTPS	ACCEPT	Enabled	no-inspection	UTM	0 B
Implicit 1									
mplicit Deny	all	all	always	ALL	DENY			Disabled	6.80 kB

Figure 34:Politique de sécurité de notre Firewall

3. Serveur :

Un serveur est généralement un ordinateur plus puissant que votre ordinateur de bureau habituel. Il est spécialement conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau. Les serveurs sont dotés de composants matériels qui gèrent la mise en réseau par câble Ethernet ou sans fil, généralement via un routeur. Capables de traiter des charges de travail plus importantes et d'exécuter davantage d'applications, les serveurs tirent parti de leurs composants matériels spécifiques pour augmenter la productivité et réduire les temps d'inactivité. Les serveurs offrent également des outils de gestion à distance qui permettent à un technicien informatique de vérifier l'utilisation et de diagnostiquer les problèmes depuis un autre site. Vous pouvez également utiliser ces outils pour exécuter des tâches de maintenance régulière, telles que l'ajout de nouveaux utilisateurs ou la modification de mots de passes.

Figure 35:serveur

a. Types de serveur

- Serveur web : Les serveurs web sont le carrefour où sont installés des logiciels divers en vue de leur fonctionnement normal. Ces logiciels fonctionnent ensemble pour créer et emmagasiner des fichiers web composés de sites ou de contenus destinés à être livrés aux visiteurs. Ce sont pour la plupart des documents HTML, des images, des papiers CSS, des documents JavaScript. On en

déduit donc qu'un serveur web favorise la publication de contenu sur site : il peut s'agir d'un ordinateur ou d'un serveur HTTP composé de logiciel dynamique. Les serveurs web sont responsables de la connexion internet et des échanges de messages également.

- Serveur d'impression : Les serveurs d'impression créent une liaison entre plusieurs ordinateurs et des imprimantes pour permettre une utilisation partagée. Il suffit de bénéficier d'un même réseau et vous pouvez jouir ensemble des imprimantes à partir de vos appareils respectifs.

- Serveur de fichiers : Ce sont des serveurs utiles pour des entreprises disposant de plusieurs employés et qui ne disposent pas d'ordinateur à tous les postes. Ils peuvent s'en servir pour une utilisation commune dans le but d'y stocker leurs fichiers, procéder aux partages et échanges entre personnels. C'est une bonne alternative pour le travail en réseau. Disponibles en plusieurs types, les serveurs informatiques jouent des rôles tout aussi variés et importants les uns que les autres. Ils représentent le centre d'un système informatique.

b. ***Serveur Dell*** *PowerEdge T430 :*

Le serveur Dell PowerEdge T430 est une solution de serveur polyvalente conçue pour répondre aux besoins des petites et moyennes entreprises. Voici quelques-unes de ses caractéristiques principales :

- Processeurs : Le PowerEdge T430 prend en charge les processeurs Intel Xeon E5-2600 v4/v3 jusqu'à deux sockets, offrant une puissance de traitement élevée pour des charges de travail exigeantes.

Figure 36:Server Dell PowerEdge

- Mémoire : Il peut prendre en charge jusqu'à 12 emplacements DIMM DDR4, offrant une capacité de mémoire évolutive allant jusqu'à 384 Go pour répondre aux besoins de traitement intensif et de virtualisation.
- Stockage : Le serveur dispose de plusieurs options de stockage, notamment des baies de disques SAS, SATA et SSD, offrant une grande capacité de stockage interne pour les données et les applications.
- Extensibilité : Le PowerEdge T430 offre une grande extensibilité avec plusieurs emplacements PCI Express (PCIe), permettant d'ajouter des cartes d'extension pour répondre aux besoins spécifiques de l'entreprise, tels que les cartes de réseau, les cartes RAID, etc.
- Gestion à distance : Il est équipé de la technologie de gestion à distance intégrée iDRAC8 avec Lifecycle Controller, permettant une gestion facile et centralisée du serveur, y compris la surveillance, la configuration et la mise à jour à distance.
- Redondance et disponibilité : Le serveur offre des fonctionnalités de redondance, notamment des blocs d'alimentation redondants et des disques durs remplaçables à chaud, assurant une disponibilité élevée du système et une continuité de service.
- Flexibilité de configuration : Le PowerEdge T430 permet de configurer le serveur selon les besoins spécifiques de l'entreprise, en offrant des options de personnalisation pour le processeur, la mémoire, le stockage et les interfaces réseau.
- Gestion simplifiée : Dell Open Manage Essentials, une suite de gestion intégrée, permet une gestion simplifiée du serveur, notamment la surveillance proactive, la gestion des correctifs et la gestion des mises à jour.

c. *Virtualisation :*

La virtualisation est une technologie clé qui permet de maximiser l'efficacité et la flexibilité des infrastructures informatiques en créant des machines virtuelles (VM) sur

un seul serveur physique. Elle offre de nombreux avantages, tels que la consolidation des ressources, la réduction des coûts, la facilité de gestion et la haute disponibilité. Il existe différents types d'hyperviseurs, qui sont des logiciels de virtualisation utilisés pour créer et gérer les machines virtuelles.

Les deux principaux types d'hyperviseurs sont les hyperviseurs de type 1 (ou bare metal) et les hyperviseurs de type 2 (ou hébergés). Les hyperviseurs de type 1 s'exécutent directement sur le matériel physique et sont considérés comme plus performants et plus efficaces. Ils ont un accès direct aux ressources matérielles, ce qui permet d'obtenir des performances optimales. Certains exemples d'hyperviseurs de type 1 populaires sont VMware ESXi, Microsoft Hyper-V, Citrix XenServer et Proxmox.

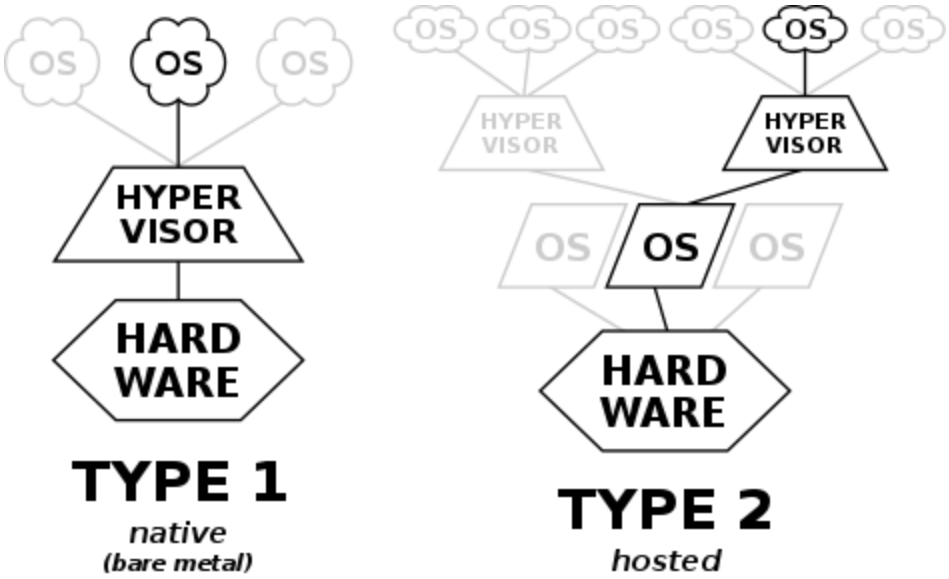


Figure 37:les deux types d'hyperviseur

Les hyperviseurs de type 2, en revanche, s'exécutent comme des applications sur un système d'exploitation hôte. Ils sont plus adaptés aux environnements de développement et de test, ou pour une utilisation sur des postes de travail. Les hyperviseurs de type 2 incluent des logiciels tels que VMware Workstation, Oracle VirtualBox et Microsoft Virtual PC.

Chaque type d'hyperviseur offre des fonctionnalités et des performances spécifiques, et le choix dépend des besoins et des contraintes de l'infrastructure informatique. La virtualisation a révolutionné la gestion des ressources informatiques en permettant une utilisation plus efficace des serveurs, une meilleure flexibilité et une réduction des coûts. Elle est devenue une technologie incontournable pour les entreprises cherchant à optimiser leurs opérations informatiques.

d. Proxmox :

Proxmox VE est une plateforme de virtualisation open source qui combine la virtualisation basée sur des conteneurs et la virtualisation basée sur des machines

Figure 38:logo Proxmox

virtuelles (VM). Il s'agit d'un système d'exploitation complet conçu pour être installé sur des serveurs physiques et permettant de créer et de gérer facilement des environnements de virtualisation.

Proxmox VE utilise un hyperviseur de type 1, basé sur la technologie de conteneurisation Linux (LXC) et le module de virtualisation basé sur le noyau Linux (KVM). Cela permet aux utilisateurs de créer et de gérer des conteneurs légers et des machines virtuelles complètes sur une même plateforme.

L'avantage de Proxmox VE est sa polyvalence et sa facilité d'utilisation. Il offre une interface web conviviale qui permet aux administrateurs de gérer les ressources, de créer et de cloner des machines virtuelles, de surveiller les performances, de configurer le stockage et les réseaux, et bien plus encore.

Proxmox VE prend en charge une large gamme de systèmes d'exploitation invités, tels que Windows, Linux, BSD et d'autres distributions populaires. Il offre également des fonctionnalités avancées, telles que la migration en direct des machines virtuelles, la sauvegarde et la restauration intégrées, la haute disponibilité, la planification des ressources et la gestion des utilisateurs et des permissions.

En résumé, Proxmox VE est une solution complète de virtualisation open source qui offre une gestion facile, des performances élevées et une grande flexibilité grâce à sa combinaison unique de virtualisation basée sur des conteneurs et des machines virtuelles. C'est une option populaire pour les entreprises et les fournisseurs de services cloud qui recherchent une solution économique et puissante pour leurs besoins de virtualisation.

e. Installation de Proxmox:

Figure 39: 1er page d'installation

Pour installer Proxmox sur notre serveur Dell PowerEdge T430, nous avons suivi une procédure simple et efficace. Tout d'abord, nous avons créé une clé USB bootable contenant l'image ISO de Proxmox. Cette clé USB nous a permis de démarrer le serveur à partir de celle-ci et de lancer le processus d'installation. Une fois que le serveur a démarré à partir de la clé USB, nous avons été guidés à travers l'assistant d'installation de Proxmox. Nous avons sélectionné le disque dur sur lequel nous souhaitions installer Proxmox et nous avons accepté les conditions de licence. Ensuite, nous avons configuré les paramètres réseau, tels que l'adresse IP, le masque de sous-réseau et la passerelle, pour permettre la connectivité à distance avec le serveur Proxmox. Après avoir terminé la configuration initiale, l'installation de Proxmox a commencé. Cela a inclus le partitionnement du disque dur, la copie des fichiers nécessaires et l'installation du système d'exploitation basé sur Debian. Une fois l'installation terminée, nous avons redémarré le serveur et nous avons pu accéder à l'interface web de Proxmox à partir d'un navigateur. Là, nous avons configuré les paramètres supplémentaires, tels que la création de comptes d'utilisateurs, la configuration du stockage et la mise en place des réseaux virtuels. Grâce à cette installation de Proxmox sur notre serveur Dell PowerEdge T430, nous avons pu bénéficier des avantages de la virtualisation et gérer efficacement nos machines virtuelles et nos conteneurs. Proxmox nous a offert une plateforme puissante et conviviale pour consolider nos ressources, améliorer la flexibilité et faciliter la gestion de notre infrastructure.

f. Configuration de réseau dans notre serveur :

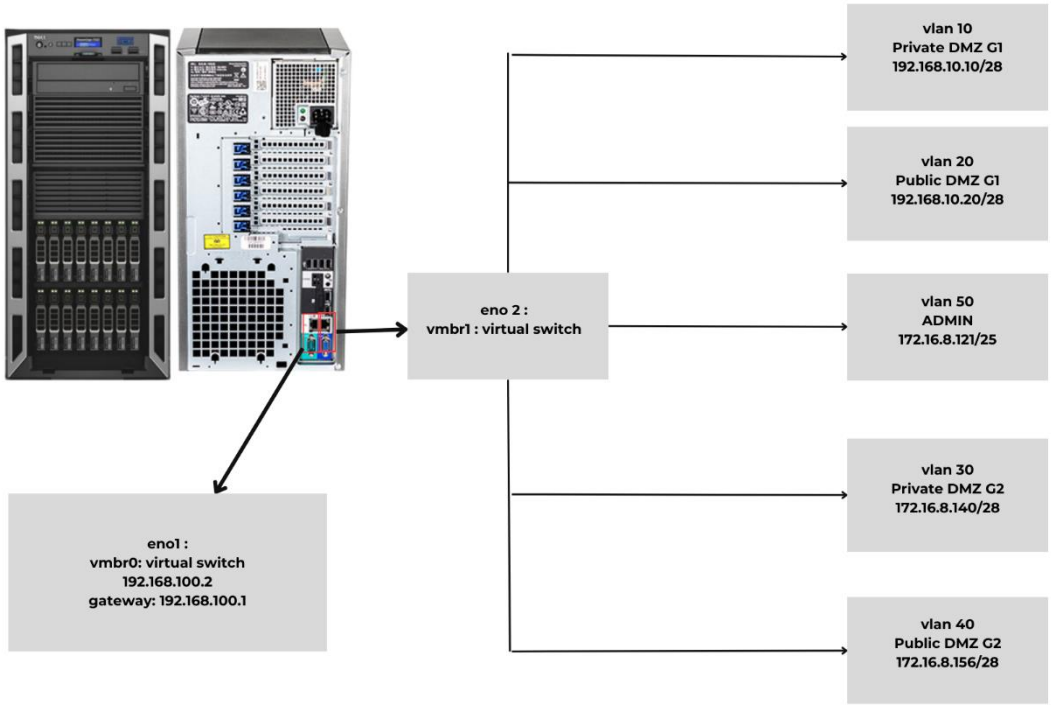


Figure 40:Configuration de réseau dans notre serveur

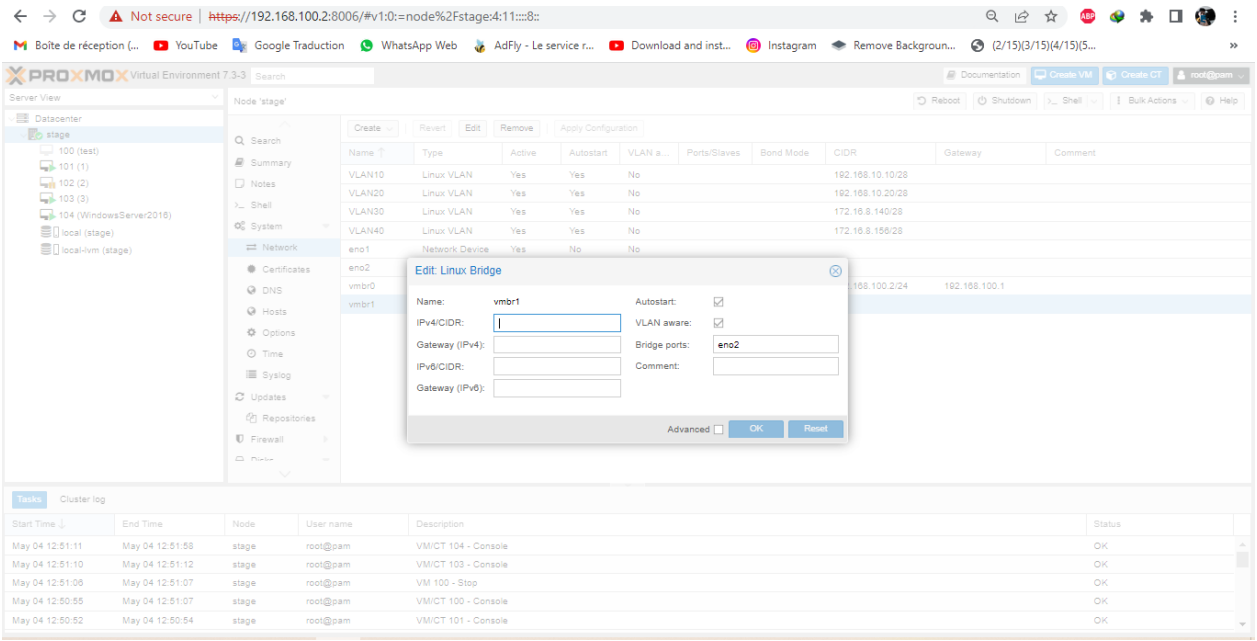


Figure 41: Création de Virtual switch vmbr1

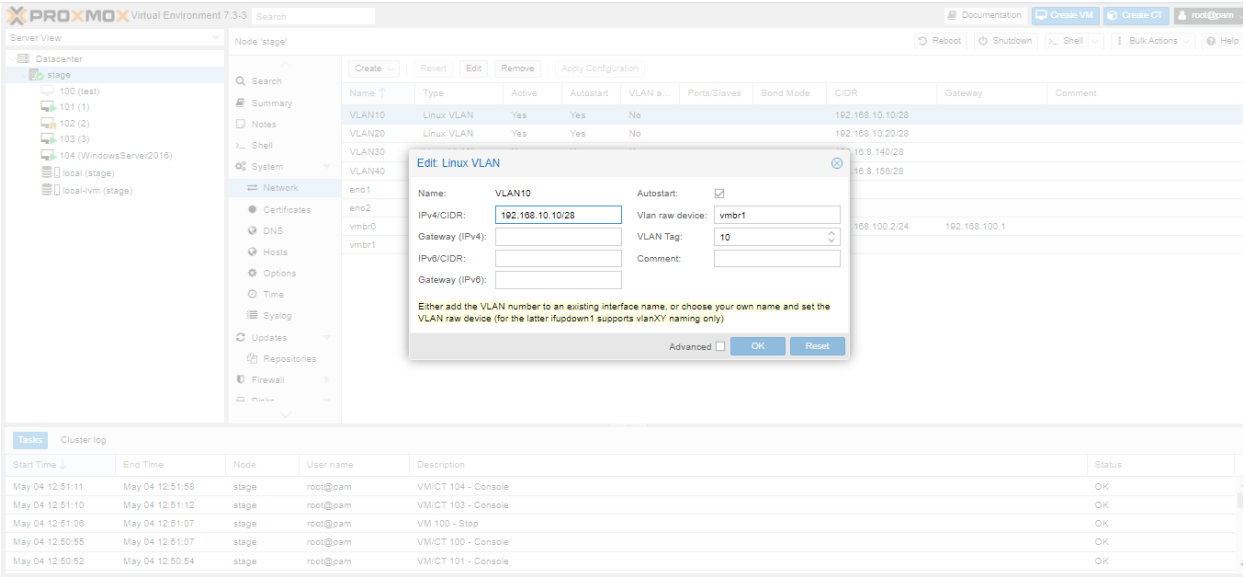


Figure 42: Création de 1er vlan 10 Dmz privée de 1er Groupe

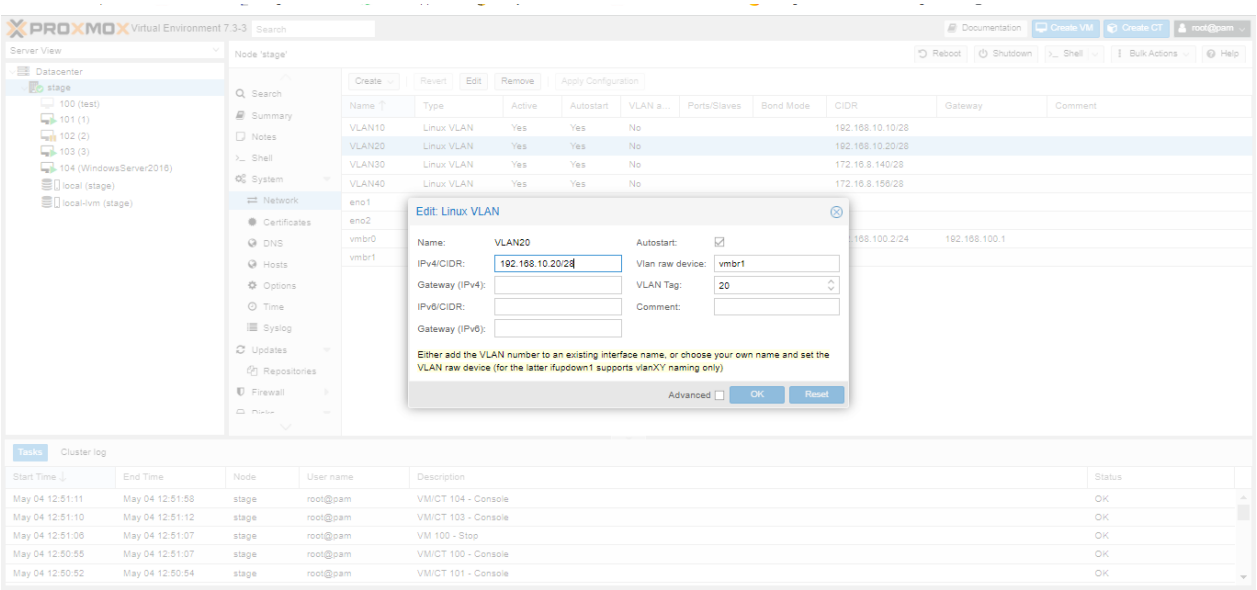


Figure 43: Création de 2éme Vlan 20 publique pour 1er Groupe

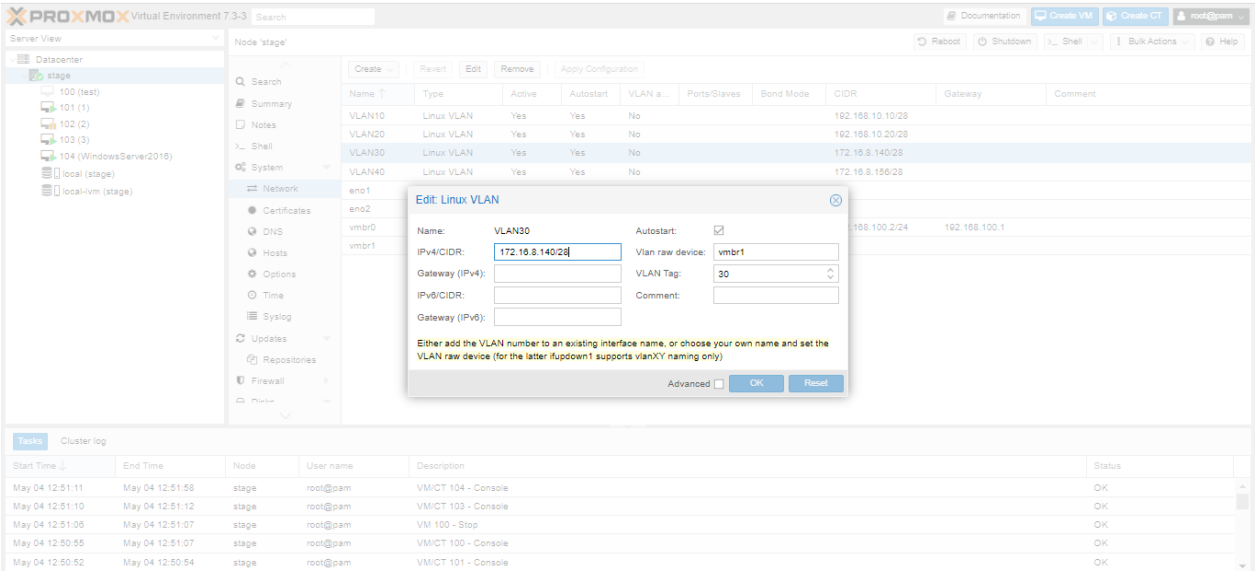


Figure 44: Création de 3éme Vlan 30 Dmz privée de 2éme Groupe

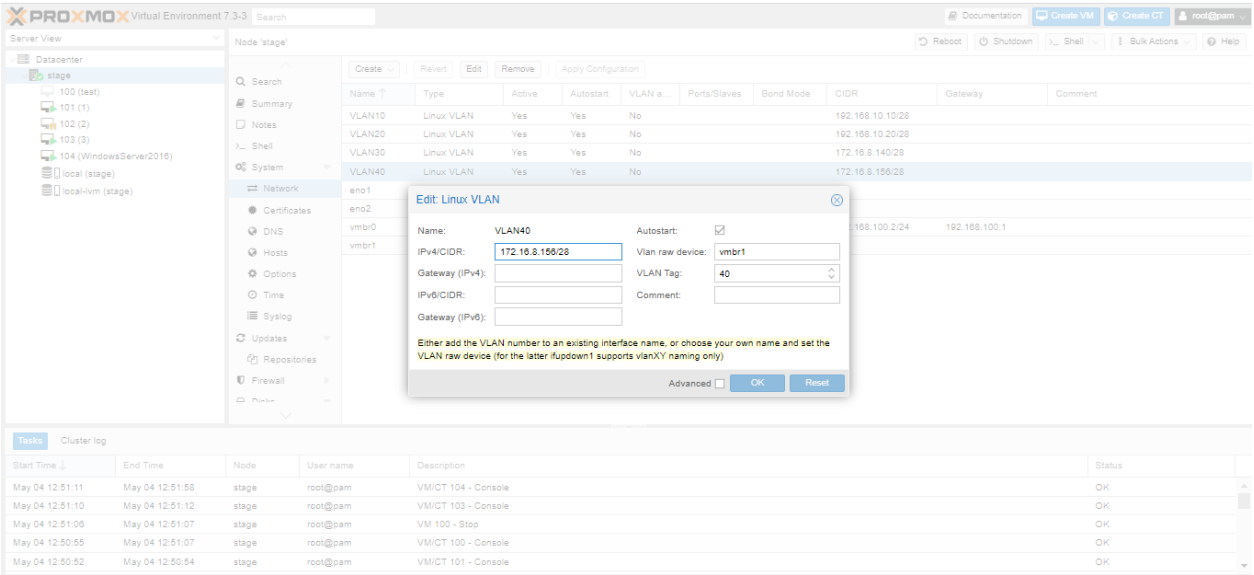


Figure 45: Création de 4éme Vlan Dmz publique de 2éme Groupe

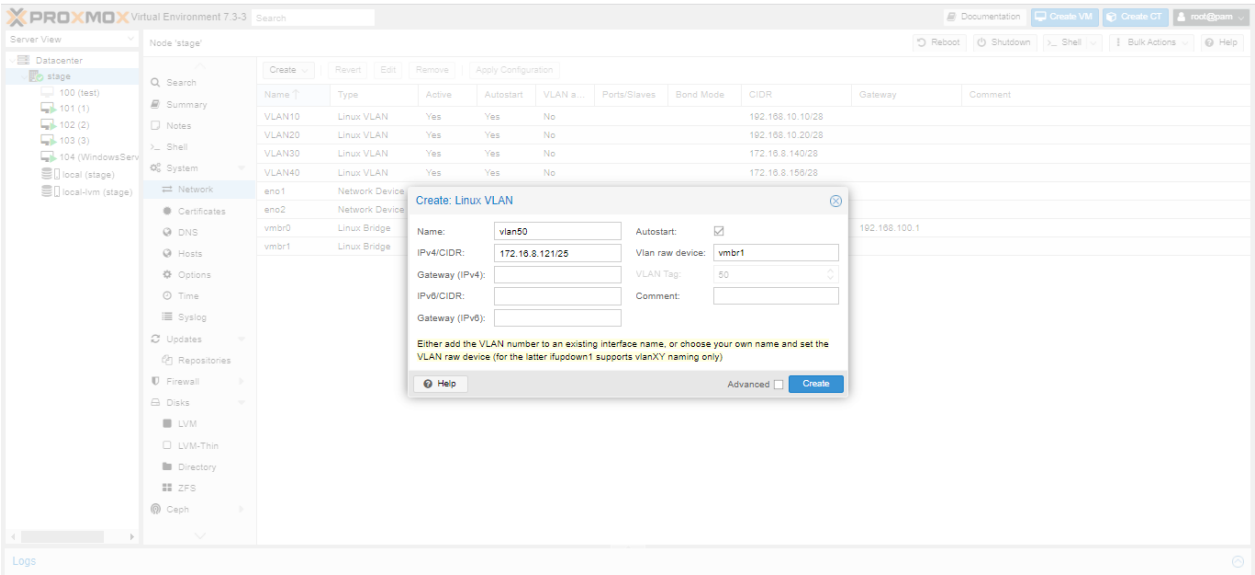


Figure 46: Création de 5éme Vlan Admin

g. Machine Dmz publique (Vlan 40):

- **Définition et principe :**

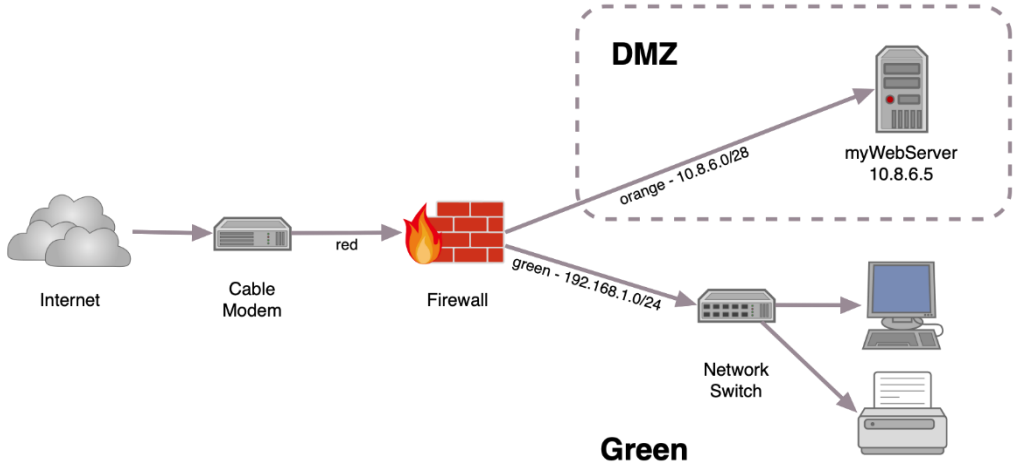


Figure 47:Exemple de Dmz

Une zone DMZ publique, également connue sous le nom de DeMilitarized Zone, est une partie d'un réseau informatique qui est séparée du réseau local interne et exposée directement à Internet. Son objectif principal est de fournir un niveau supplémentaire de sécurité en isolant les services et les serveurs accessibles publiquement, tels que les sites

web, les serveurs de messagerie ou les services VPN. La zone DMZ publique agit comme une barrière de protection entre Internet et le réseau interne. Elle permet d'héberger des services publics sans compromettre la sécurité du réseau local. En plaçant les serveurs publics dans la zone DMZ, on réduit les risques potentiels d'attaques directes sur le réseau local. La configuration d'une zone DMZ publique implique l'utilisation de pare-feu et de règles de filtrage du trafic réseau pour contrôler les accès entre Internet, la zone DMZ et le réseau local. Les règles de pare-feu peuvent être configurées de manière à autoriser uniquement les connexions entrantes nécessaires vers les serveurs hébergés dans la zone DMZ, tout en restreignant l'accès au réseau local. En résumé, une zone DMZ publique est une subdivision du réseau qui permet d'héberger des services accessibles publiquement tout en offrant une protection supplémentaire contre les attaques potentielles. Cela permet de séparer les services publics du réseau interne, minimisant ainsi les risques de compromission de la sécurité globale du réseau.

- **DNS :**

Le DNS (Domain Name System) est un système essentiel de l'infrastructure Internet qui permet de traduire les noms de domaine en adresses IP. Il s'agit d'un système distribué et hiérarchique qui joue un rôle fondamental dans la résolution des noms de domaine. Le DNS fonctionne comme un annuaire téléphonique d'Internet, où chaque nom de domaine est associé à une adresse IP. Lorsque vous entrez un nom de domaine dans votre navigateur, le DNS est responsable de trouver l'adresse IP correspondante du serveur sur lequel se trouve le site web recherché. Cela permet d'établir une connexion entre votre appareil et le serveur pour afficher le site web demandé. Le DNS utilise une structure en arborescence avec différentes zones, notamment la zone racine, les domaines de premier niveau (TLD), les sous-domaines et les enregistrements. Chaque zone est gérée par des serveurs DNS qui stockent les informations de résolution des noms pour les noms de domaine spécifiques. Lorsqu'un utilisateur envoie une demande de résolution de nom de domaine, son appareil interroge d'abord le serveur DNS local, également appelé serveur DNS récursif. Si le serveur récursif possède déjà les informations dans son cache, il les

renvoie immédiatement à l'utilisateur. Sinon, le serveur récursif contacte d'autres serveurs DNS pour obtenir l'adresse IP correspondante et la renvoyer à l'utilisateur. Le DNS offre une gestion flexible des enregistrements, tels que les enregistrements A (adresse IP), les enregistrements MX (serveur de messagerie), les enregistrements CNAME (alias) et bien d'autres. Cela permet de rediriger les requêtes vers les serveurs appropriés, d'héberger des services sur différents domaines ou sous-domaines, et de configurer des adresses de messagerie associées à un nom de domaine spécifique.

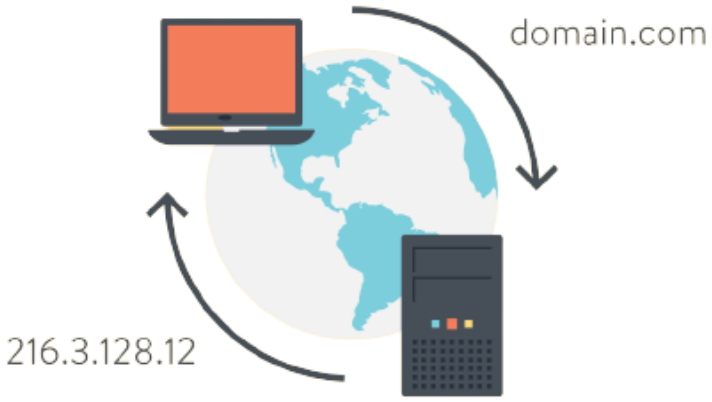


Figure 48:DNS

```
20 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@grp2-Standard-PC-i440FX-PIIX-1996:~# apt install -y bind9 bind9utils bind9-doc dnsutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.18.12-0ubuntu0.22.04.1).
The following NEW packages will be installed:
  bind9-doc bind9utils dnsutils
0 upgraded, 3 newly installed, 0 to remove and 20 not upgraded.
Need to get 3,202 kB of archives.
After this operation, 7,568 kB of additional disk space will be used.
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-doc all 1:9.18.12-0ubuntu0.22.04.1 [3,195 kB]
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 bind9utils all 1:9.18.12-0ubuntu0.22.04.1 [3,924 B]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 dnsutils all 1:9.18.12-0ubuntu0.22.04.1 [3,924 B]
```

Figure 49: Installation de server DNS

On commence l'installation de notre serveur avec la commande :

$ sudo apt install –y bind9 bind9utils bind9-doc dnsutils

```
  GNU nano 6.2                                                    stage.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     enssup.stage.ma. root.stage.ma. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@                       IN      NS              enssup.stage.ma.
@                       IN      MX      10      mail.stage.ma.
@                       IN      A               172.16.8.151
enssup                  IN      A               172.16.8.151
enssup-web              IN      A               172.16.8.151
www                     IN      CNAME           enssup
mail                    IN      A               172.16.8.151
ftp                     IN      CNAME           enssup
```

Figure 50:Configuration de fichier stage.local

```
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
zone "stage.ma"  {
        type master;
        file"/etc/bind/stage.local";
};
zone "8.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/reserve.stage.local";
};
```

Figure 51:configuration de fichier named.conf

```
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 172.16.8.151
options edns0 trust-ad
search stage.ma
```

Figure 52 :resolv.conf

```
root@grp2-Standard-PC-i440FX-PIIX-1996: /etc/bind
root@grp2-Standard-PC-i440FX-PIIX-1996:/etc/bind# service named reload
root@grp2-Standard-PC-i440FX-PIIX-1996:/etc/bind# service named restart
root@grp2-Standard-PC-i440FX-PIIX-1996:/etc/bind# service named status
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-05-24 12:21:10 +01; 12s ago
       Docs: man:named(8)
    Process: 6154 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 6155 (named)
      Tasks: 6 (limit: 4614)
     Memory: 6.1M
        CPU: 71ms
     CGroup: /system.slice/named.service
             └─6155 /usr/sbin/named -u bind

12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:500:1::53#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:7fd::1#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:500:200::b#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:500:2::c#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:dc3::35#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: network unreachable resolving './NS/IN': 2001:7fe::53#53
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
12:21:10 24 ماي grp2-Standard-PC-i440FX-PIIX-1996 named[6155]: resolver priming query complete: success
root@grp2-Standard-PC-i440FX-PIIX-1996:/etc/bind#
```

Figure 53: Restart service named

- **Apache :**

Apache, également connu sous le nom d'Apache HTTP Server, est l'un des serveurs web les plus populaires et les plus utilisés dans le monde. Il s'agit d'un logiciel open source, robuste et fiable, qui permet de fournir des services web en répondant aux requêtes des clients et en fournissant les fichiers demandés. Apache offre une grande flexibilité et une large gamme de fonctionnalités. Il prend en charge plusieurs protocoles de communication, tels que HTTP, HTTPS, FTP et bien d'autres. Il est également compatible avec divers systèmes d'exploitation, notamment Linux, Windows, macOS et d'autres plateformes. En plus de sa capacité à fournir des fichiers statiques, Apache supporte également l'exécution de scripts dynamiques, tels que PHP, Perl et Python, permettant ainsi de créer des sites web interactifs et dynamiques. Apache est hautement configurable grâce à son architecture modulaire. Il offre une grande variété de modules qui peuvent être activés ou désactivés en fonction des besoins spécifiques de l'application web. Ces modules fournissent des fonctionnalités supplémentaires telles que la compression de fichiers, la gestion des sessions, la sécurité, la réécriture d'URL, la gestion des caches, et

bien plus encore. La performance d'Apache peut être améliorée en utilisant des techniques de mise en cache, de compression et d'optimisation des requêtes. De plus, Apache est connu pour sa stabilité et sa sécurité, grâce à une communauté active de développeurs qui assurent les mises à jour régulières et la correction des éventuelles vulnérabilités.

```
root@grp2-Standard-PC-i440FX-PIIX-1996: /etc/bind
root@grp2-Standard-PC-i440FX-PIIX-1996:/etc/bind#  apt install apache2 php libapache2-mod-php mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Figure 54:installation de serveur web apache

```
root@grp2-Standard-PC-i440FX-PIIX-1996: /etc/apache2/sites-available
  GNU nano 6.2                                          site1.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName site1
    ServerAlias www.site1
    DocumentRoot /var/www/site1
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Figure 55:on ajout le fichier site1.conf ou stage.conf dans

```
root@grp2-Standard-PC-i
root@grp2-Standard-PC-i440FX-PIIX-1996:~# cd /var/www/
root@grp2-Standard-PC-i440FX-PIIX-1996:/var/www# ls
html  site1  site1.conf
root@grp2-Standard-PC-i440FX-PIIX-1996:/var/www#
```

Figure 56:on ajoute notre site dans le chemin /var/www

Voilà un exemple sur configuration d'apache dans notre Dmz publique

On a fait la même chose pour le domaine stage.ma et voilà résultat de serveur DNS et Apache en même temps :

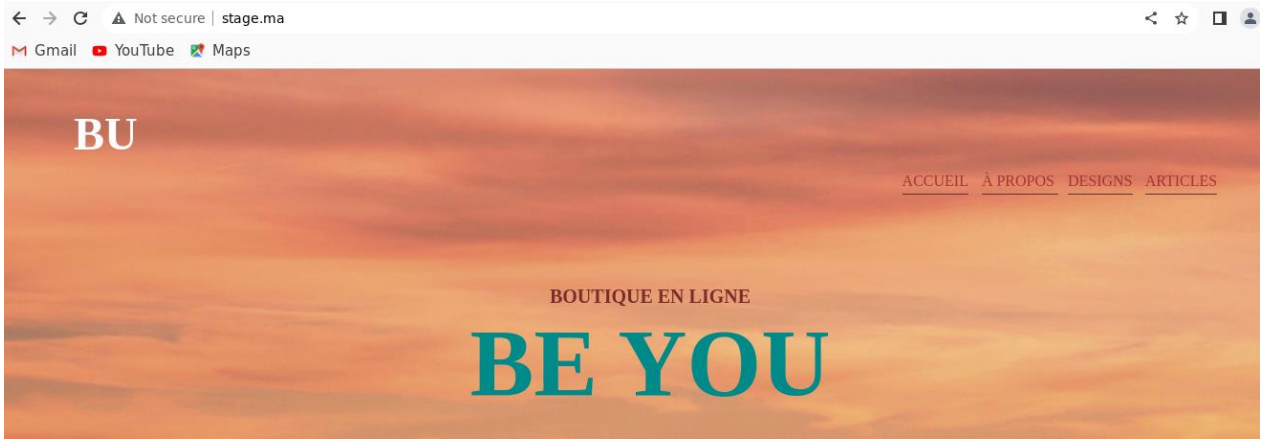


Figure 57: Site avec domain stage.ma

h. Machine Radius serveur (Vlan 50):

RADIUS (Remote Authentication Dial-In User Service) est un protocole de sécurité utilisé pour l'authentification, l'autorisation et la comptabilisation des utilisateurs qui se connectent à un réseau. Il permet de centraliser et de gérer les informations d'identification des utilisateurs, garantissant ainsi un contrôle d'accès sécurisé.

Pour configurer RADIUS sur votre machine Ubuntu Server, vous pouvez suivre les étapes suivantes :

1. Installez le serveur RADIUS en utilisant la commande suivante :

$ sudo apt-get install freeradius

2. Une fois l'installation terminée, ouvrez le fichier de configuration principal de RADIUS en utilisant un éditeur de texte, tel que nano :

$ sudo nano /etc/freeradius/clients.conf

3. Ajoutez les informations de vos clients, c'est-à-dire les dispositifs ou les utilisateurs autorisés à se connecter au serveur RADIUS. Par exemple :

```
client 172.16.8.22/25 {
    secret = STAGE2023@
}
```

4. Configurez les fichiers d'authentification et d'autorisation des utilisateurs en utilisant les fichiers suivants :

- /etc/freeradius/users : pour définir les utilisateurs et leurs informations d'identification.
- /etc/freeradius/authorize : pour spécifier les autorisations d'accès pour chaque utilisateur.

5. Ajoutez les utilisateurs spécifiés dans le fichier de configuration `/etc/freeradius/users`. Par exemple:

```
Ibrahim Cleartext-Password: = "ibrahim123"
Meriem Cleartext-Password: = "meriem123"
Mouad Cleartext-Password: = " mouad123"
Hanan Cleartext-Password: = "hanan123"
```

6. Redémarrez le service RADIUS pour appliquer les modifications :

$ sudo service freeradius restart

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui permet de fournir automatiquement les paramètres de configuration IP aux appareils se connectant

à un réseau. Il attribue les adresses IP, les masques de sous-réseau, les passerelles par défaut et d'autres informations réseau aux clients DHCP.

Pour configurer le serveur DHCP sur votre machine Ubuntu Server, vous pouvez suivre les étapes suivantes :

1. Installez le serveur DHCP en utilisant la commande suivante :

```
$ sudo apt-get install isc-dhcp-server
```

2. Ouvrez le fichier de configuration principal du serveur DHCP en utilisant un éditeur de texte, tel que nano :

```
$ sudo nano /etc/dhcp/dhcpd.conf
```

3. Définissez les paramètres du serveur DHCP, tels que les plages d'adresses IP à attribuer, les options réseau, etc. Par exemple :

```
Subnet 172.16.8.0 netmask 255.255.255.128 {
    Range 172.16.8.2 172.16.8.100 ;
    Option routers 172.16.8.122;
    Option domain-name "stage.ari” ;
}
```

4. Ajoutez les réservations DHCP pour chaque utilisateur en spécifiant leur adresse MAC et l'adresse IP correspondante. Par exemple :

```
host Ibrahim {
    Hardware ethernet 00:11:22:33:44:55;
    Fixed-address 192
```

- **Installation et configuration dans notre hyperviseur :**

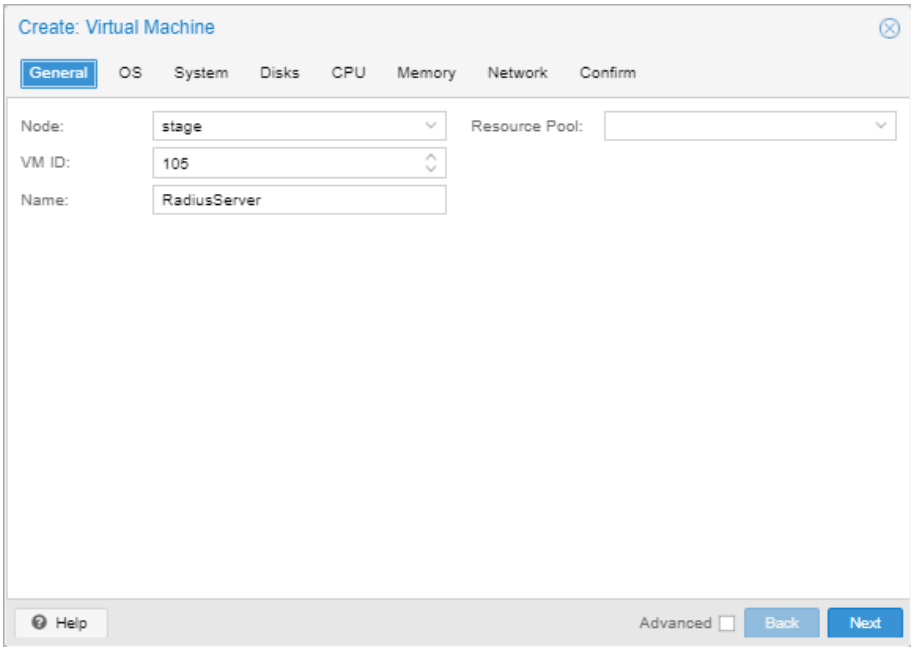
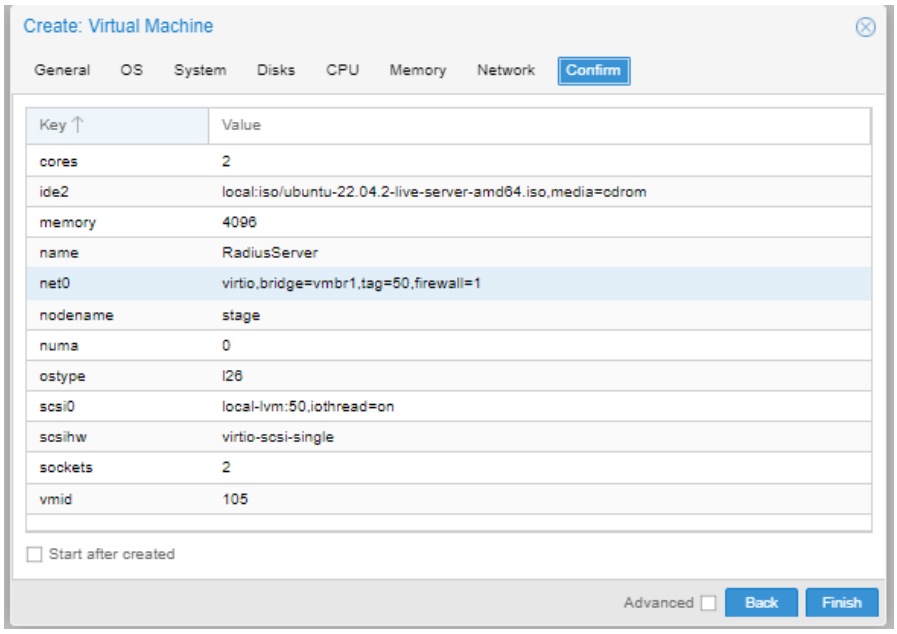


Figure 58: Création de la machine



```
Choose type of install                                                    [ Help ]

Choose the base for the installation.

(X)  Ubuntu Server

     The default install contains a curated set of packages that provide a comfortable experience for operating your server.

( )  Ubuntu Server (minimized)

     This version has been customized to have a small runtime footprint in environments where humans are not expected to log
     in.

Additional options

[ ]  Search for third-party drivers

     This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers
     should not be installed on systems that will be used for FIPS or the real-time kernel.

                                                    [ Done       ]
                                                    [ Back       ]
```

```
Network connections                                                       [ Help ]

Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient
access for updates.

  NAME    TYPE  NOTES
[ ens18   eth   -                  ▸ ]
  DHCPv4  -
  76:52:a7:00:65:0d / Red Hat, Inc. / Virtio network device

[ Create bond ▸ ]

                    Edit ens18 IPv4 configuration

IPv4 Method:    [ Manual            ▾ ]

        Subnet:  172.16.8.0/25

       Address:  172.16.8.122

       Gateway:  172.16.8.126

   Name servers:  192.168.2.1
                  IP addresses, comma separated

Search domains:  stage.ari
                 Domains, comma separated

                          [ Save       ]
                          [ Cancel     ]

                    [ Continue without network ]
                    [ Back                     ]
```

```
Storage configuration                                                    [ Help ]

FILE SYSTEM SUMMARY

  MOUNT POINT     SIZE    TYPE      DEVICE TYPE
[ /             23.996G  new ext4  new LVM logical volume      ▸ ]
[ /boot          2.000G  new ext4  new partition of local disk ▸ ]


AVAILABLE DEVICES

  DEVICE                                    TYPE                SIZE
[ ubuntu-vg (new)                           LVM volume group    47.996G  ▸ ]
  free space                                                    24.000G  ▸

[ Create software RAID (md) ▸ ]
[ Create volume group (LVM) ▸ ]


USED DEVICES

  DEVICE                                    TYPE                SIZE
[ ubuntu-vg (new)                           LVM volume group    47.996G  ▸ ]
  ubuntu-lv    new, to be formatted as ext4, mounted at /       23.996G  ▸

[ QEMU_QEMU_HARDDISK_drive-scsi0            local disk          50.000G  ▸ ]
  partition 1  new, BIOS grub spacer                             1.000M  ▸
  partition 2  new, to be formatted as ext4, mounted at /boot    2.000G  ▸
  partition 3  new, PV of LVM volume group ubuntu-vg            47.997G  ▸


                                                  [ Done       ]
                                                  [ Reset      ]
                                                  [ Back       ]
```

```
Profile setup                                                            [ Help ]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a
password is still needed for sudo.

            Your name:  RadiusServer

    Your server's name:  radius_server
                         The name it uses when it talks to other computers.

        Pick a username:  radius

     Choose a password:  **********

  Confirm your password:  **********


                                                  [ Done       ]
```

```
SSH Setup                                                                    [ Help ]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

                [X]  Install OpenSSH server

Import SSH identity:  [ No              ▼ ]
                      You can import your SSH keys from GitHub or Launchpad.

    Import Username:

                [X]  Allow password authentication over SSH

                                          [ Done       ]
                                          [ Back       ]
```

```
Featured Server Snaps                                                        [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package,
publisher and versions available.

[*] microk8s            canonical✓            Kubernetes for workstations and appliances                                  ►
[ ] nextcloud           nextcloud✓            Nextcloud Server - A safe home for all your data                            ►
[ ] wekan               xet7                  The open-source kanban                                                      ►
[ ] kata-containers     katacontainers✓       Build lightweight VMs that seamlessly plug into the containers ecosystem    ►
[*] docker              canonical✓            Docker container runtime                                                    ►
[ ] canonical-livepatch canonical✓            Canonical Livepatch Client                                                  ►
[ ] rocketchat-server   rocketchat✓           Rocket.Chat server                                                          ►
[ ] mosquitto           mosquitto✓            Eclipse Mosquitto MQTT broker                                               ►
[ ] etcd                canonical✓            Resillient key-value store by CoreOS                                        ►
[*] powershell          microsoft-powershell✓ PowerShell for every system!                                                ►
[ ] stress-ng           cking-kernel-tools    tool to load and stress a computer                                          ►
[ ] sabnzbd             safihre               SABnzbd                                                                     ►
[ ] wormhole            snapcrafters          get things from one computer to another, safely                             ►
[ ] aws-cli             aws✓                  Universal Command Line Interface for Amazon Web Services                    ►
[ ] google-cloud-sdk    google-cloud-sdk✓     Google Cloud SDK                                                            ►
[ ] slcli               softlayer             Python based SoftLayer API Tool.                                            ►
[ ] doctl               digitalocean✓         The official DigitalOcean command line interface                            ►
[ ] conjure-up          canonical✓            Package runtime for conjure-up spells                                       ►
[ ] postgresql10        cmd✓                  PostgreSQL is a powerful, open source object-relational database system.    ►
[ ] heroku              heroku✓               CLI client for Heroku                                                       ►
[ ] keepalived          keepalived-project✓   High availability VRRP/BFD and load-balancing for Linux                     ►
[ ] prometheus          canonical✓            The Prometheus monitoring system and time series database                   ►
[ ] juju                canonical✓            Juju - a model-driven operator lifecycle manager for K8s and machines       ►

                                          [ Done       ]
                                          [ Back       ]
```

```
radius@radiusserver:~$ sudo apt-get install freeradius
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2 libtevent0 libwbclient0 make ssl-cert
Suggested packages:
  freeradius-krb5 freeradius-ldap freeradius-mysql freeradius-postgresql freeradius-python3 snmp libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl make-doc
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2 libtevent0 libwbclient0 make
  ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,836 kB of archives.
After this operation, 9,999 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

```
  GNU nano 6.2                                                    users
#
#       If you are not sure why a particular reply is being sent by the
#       server, then run the server in debugging mode (radiusd -X), and
#       you will see which entries in this file are matched.
#
#       When an authentication request is received from the comm server,
#       these values are tested. Only the first match is used unless the
#       "Fall-Through" variable is set to "Yes".
#
#       A special user named "DEFAULT" matches on all usernames.
#       You can have several DEFAULT entries. All entries are processed
#       in the order they appear in this file. The first entry that
#       matches the login-request will stop processing unless you use
#       the Fall-Through variable.
#
#       Indented (with the tab character) lines following the first
#       line indicate the configuration values to be passed back to
#       the comm server to allow the initiation of a user session.
#       This can include things like the PPP configuration values
#       or the host to log the user onto.
#
#       You can include another `users' file with `$INCLUDE users.other'

#
#       For a list of RADIUS attributes, and links to their definitions,
#       see: http://www.freeradius.org/rfc/attributes.html
#
#       Entries below this point are examples included in the server for
#       educational purposes. They may be deleted from the deployed
#       configuration without impacting the operation of the server.
#
ibrahim Cleartext-Password := "Ibrahim123"
mouad Cleartext-Password := "Mouad123"
meriem Cleartext-Password := "Meriem123"
hanan Cleartext-Password := "Hanan123"
root Cleartext-Password := "root"
#
# Deny access for a specific user.  Note that this entry MUST
# be before any other 'Auth-Type' attribute which results in the user
# being authenticated.
#
# Note that there is NO 'Fall-Through' attribute, so the user will not
# be given any additional resources.
#
#lameuser       Auth-Type := Reject
#               Reply-Message = "Your account has been disabled."

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next
```

```
  GNU nano 6.2                                                    clients.conf
# -*- text -*-
##
## clients.conf -- client configuration directives
##
##      $Id$

#######################################################################
#
#  Define RADIUS clients (usually a NAS, Access Point, etc.).

#
#  Defines a RADIUS client.
#
#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,
#  to allow testing of the server after an initial installation.  If you
#  are not going to be permitting RADIUS queries from localhost, we suggest
#  that you delete, or comment out, this entry.
#
#


#
#  Each client has a "short name" that is used to distinguish it from
#  other clients.
#
#  In version 1.x, the string after the word "client" was the IP
#  address of the client.  In 2.0, the IP address is configured via
#  the "ipaddr" or "ipv6addr" fields.  For compatibility, the 1.x
#  format is still accepted.
#
client ADMIN {
        ipaddr = 172.16.8.1/25
        secret = STAGE2023@
}

client localhost {
        #  Only *one* of ipaddr, ipv4addr, ipv6addr may be specified for
        #  a client.
        #
        #  ipaddr will accept IPv4 or IPv6 addresses with optional CIDR
        #  notation '/<mask>' to specify ranges.
        #
        #  ipaddr will accept domain names e.g. example.org resolving
        #  them via DNS.
        #
        #  If both A and AAAA records are found, A records will be
        #  used in preference to AAAA.

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next
```

```
root@radiusserver:/etc/freeradius/3.0# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-05-29 09:35:30 UTC; 4h 18min ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
   Main PID: 940 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4571)
     Memory: 85.1M (limit: 2.0G)
        CPU: 1.053s
     CGroup: /system.slice/freeradius.service
             └─940 /usr/sbin/freeradius -f

May 29 09:35:29 radiusserver freeradius[832]: Compiling Post-Auth-Type Challenge for attr Post-Auth-Type
May 29 09:35:29 radiusserver freeradius[832]: Compiling Post-Auth-Type Client-Lost for attr Post-Auth-Type
May 29 09:35:29 radiusserver freeradius[832]: Compiling Auth-Type PAP for attr Auth-Type
May 29 09:35:29 radiusserver freeradius[832]: Compiling Auth-Type CHAP for attr Auth-Type
May 29 09:35:29 radiusserver freeradius[832]: Compiling Auth-Type MS-CHAP for attr Auth-Type
May 29 09:35:29 radiusserver freeradius[832]:  # Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:336
May 29 09:35:29 radiusserver freeradius[832]: Compiling Post-Auth-Type REJECT for attr Post-Auth-Type
May 29 09:35:29 radiusserver freeradius[832]: radiusd: #### Skipping IP addresses and Ports ####
May 29 09:35:29 radiusserver freeradius[832]: Configuration appears to be OK
May 29 09:35:30 radiusserver systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

- **Configuration d'AP D-Link DSL-2890AL:**

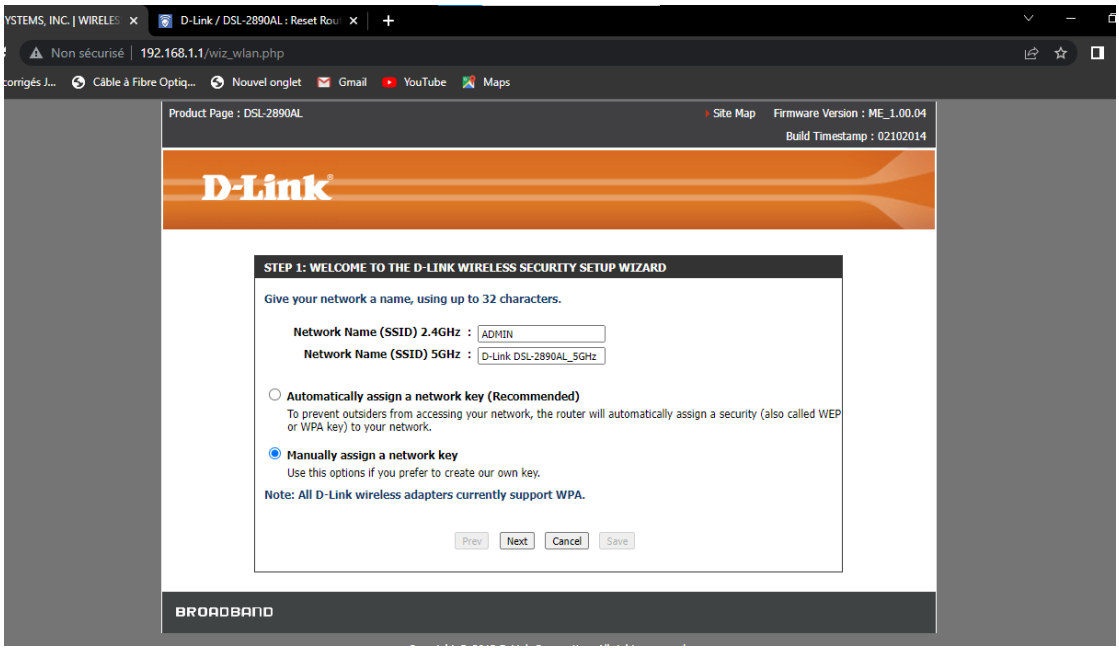


Figure 59:Config AP1

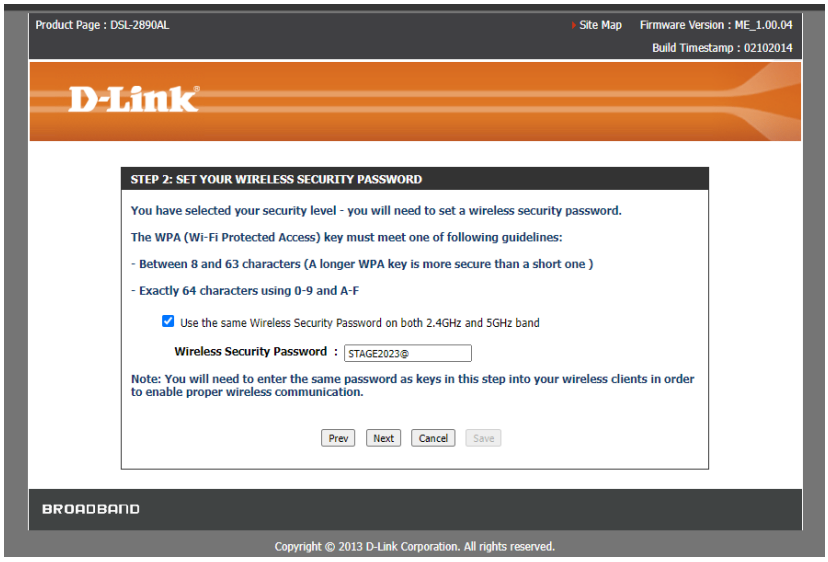


Figure 60:config AP2

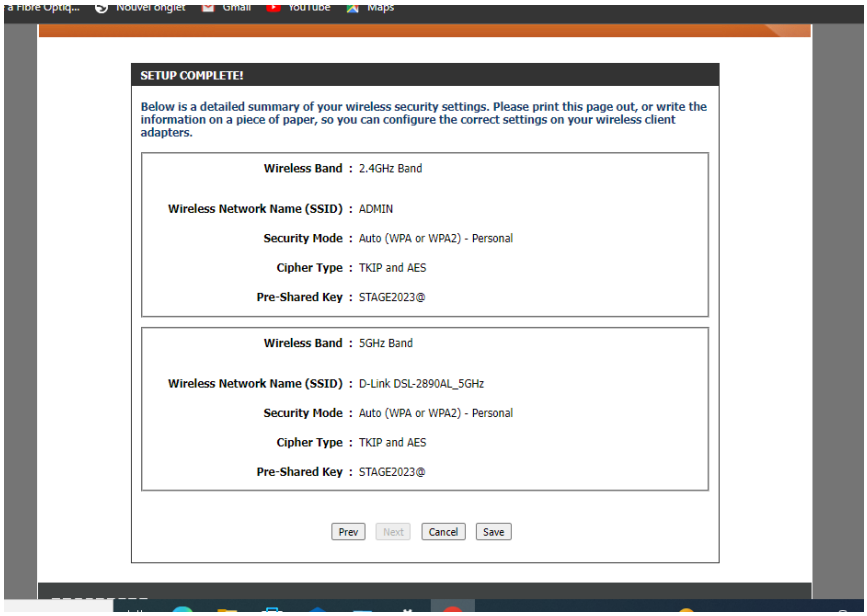
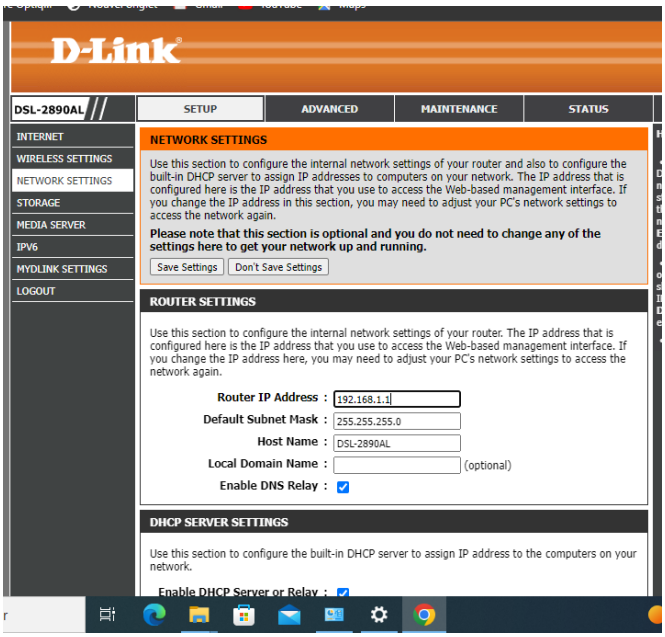


Figure 61:config AP 3

Figure 63:config AP4



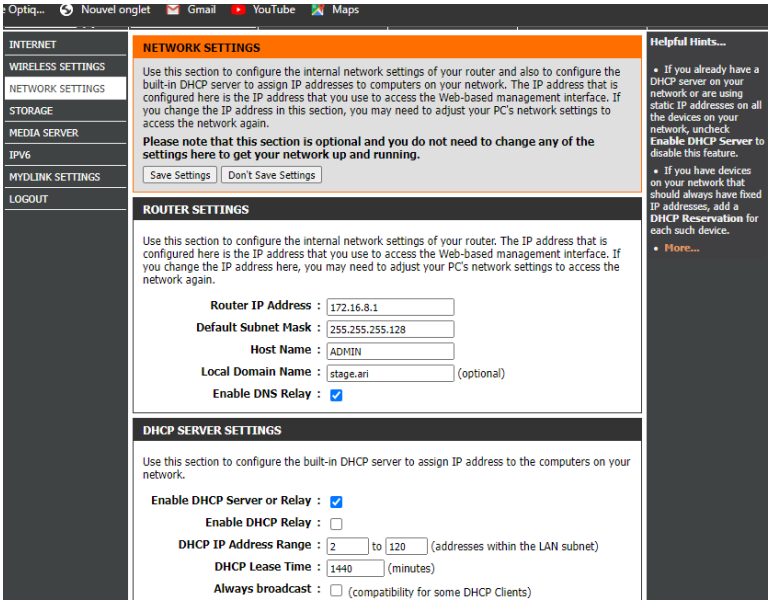


Figure 62:Config AP5

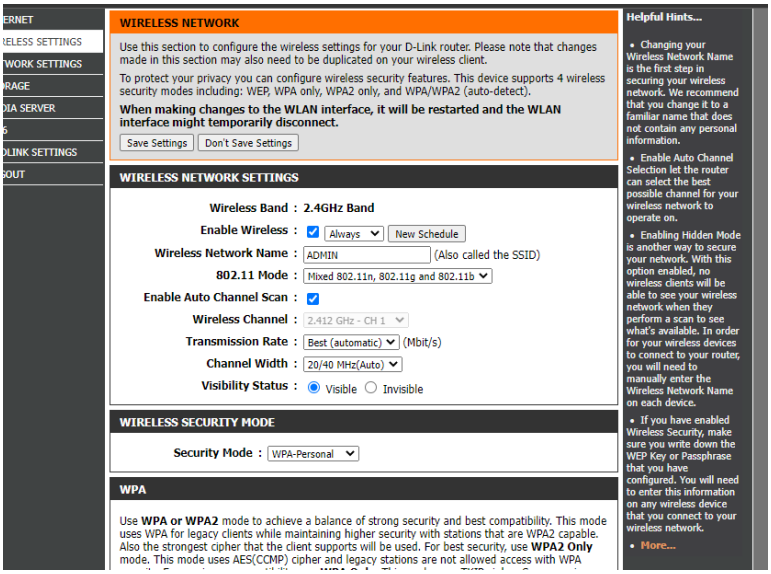


Figure 64:Config AP6

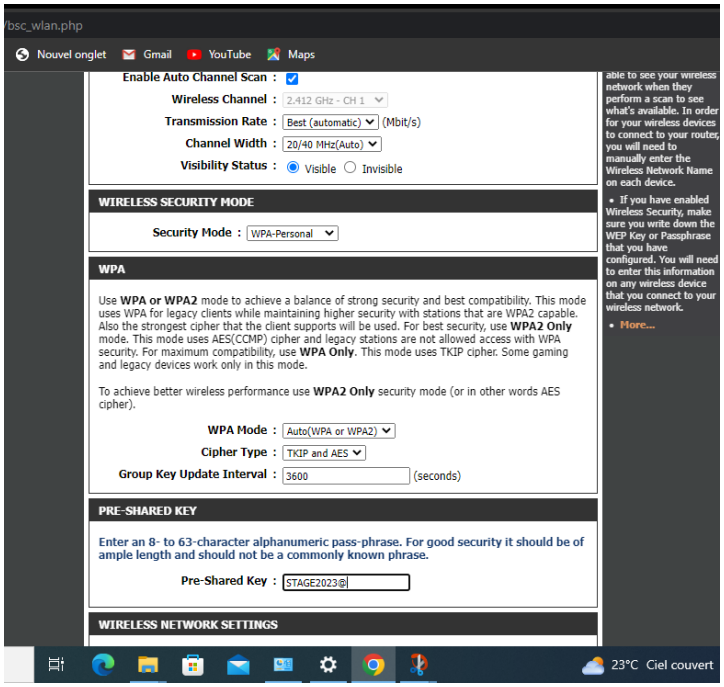


Figure 65: Config AP7

Chapitre 2 : Supervision avec Zabbix

I. La supervision :

La supervision est un concept essentiel dans de nombreux domaines, qu'il s'agisse de la gestion d'équipes, de l'éducation, de la sécurité ou de la technologie. Elle se réfère à la surveillance, à la direction et au contrôle des activités ou des individus dans le but d'assurer leur efficacité, leur sécurité et leur conformité aux normes et aux objectifs établis.

La supervision implique généralement la présence d'un superviseur ou d'un responsable chargé de guider et de superviser un groupe de personnes ou un processus spécifique. Le rôle du superviseur peut varier selon le contexte, mais il comprend généralement la définition des attentes, la fourniture de conseils et de ressources, l'évaluation des performances et la résolution des problèmes.

1. La supervision Informatique :

- La supervision est la surveillance du bon fonctionnement d'un système ou d'une activité. Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques. Elle répond à un ensemble de préoccupations comme la surveillance du réseau, de l'infrastructure et des machines, surveillance des applications…à travers des réactions automatisées en fonctions d'alertes définies.

- Supervision du réseau : Il s'agit de la surveillance des réseaux informatiques pour assurer leur bon fonctionnement, la disponibilité des services et la détection des problèmes de performance ou de sécurité. Cela peut inclure la surveillance de la bande passante, des équipements réseau, des protocoles de communication, des pares-feux, etc.

- Supervision des systèmes : Cette supervision se concentre sur la surveillance des serveurs, des systèmes d'exploitation, des bases de données et d'autres composants matériels et logiciels essentiels. L'objectif est de détecter les pannes, les goulots d'étranglement, les erreurs de configuration et d'autres problèmes

potentiels qui pourraient affecter les performances et la disponibilité des systèmes.

- Supervision des applications : Ce type de supervision se concentre sur la surveillance des applications logicielles pour détecter les problèmes de performance, les erreurs, les pannes et les vulnérabilités de sécurité. Cela peut inclure la surveillance des temps de réponse, l'analyse des journaux d'applications, la détection des incidents, etc.

- Supervision de la sécurité : La supervision de la sécurité informatique vise à surveiller les activités suspectes, les violations de sécurité et les menaces potentielles. Cela peut inclure la surveillance des journaux de sécurité, la détection d'intrusions, la surveillance des vulnérabilités, la gestion des incidents de sécurité, etc.

- Supervision des performances : Cette supervision se concentre sur la surveillance des performances des systèmes, des réseaux et des applications informatiques. Elle permet d'identifier les goulots d'étranglement, d'optimiser les ressources, de détecter les problèmes de latence, de capacité ou de disponibilité, et de prendre des mesures pour améliorer les performances globales.

2. Quelques outils de la supervision réseau :

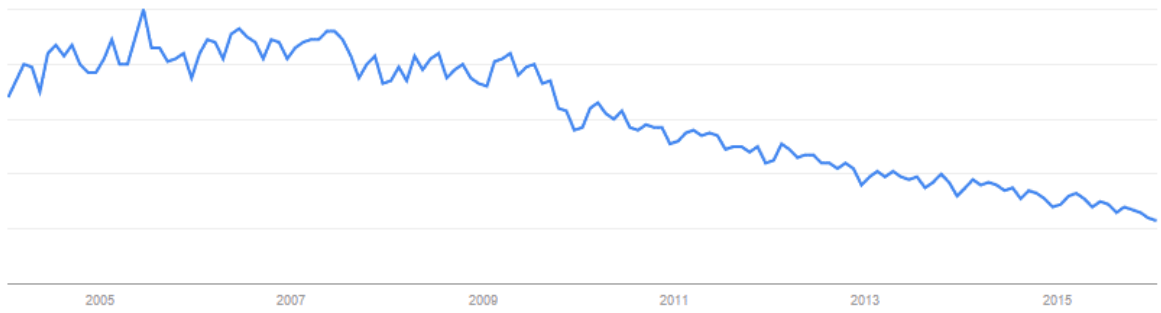
a. Nagios:

Nagios®

Figure 66:Nagios

Probablement l'outil gratuit le plus connu. Depuis 1996 ils travaillent aux États-Unis pour créer ce logiciel de supervision. Son noyau est la partie la plus importante de l'outil et des plugins peuvent être construits sur le noyau pour superviser des éléments particuliers.

Il est intéressant de voir comment la tendance de la demande sur Internet a diminué au fil du temps. Ce qui était autrefois l'un des outils de réseautage les plus puissants et les plus connus est en train de perdre du terrain.



Sa grande utilité est due au fait qu'il a été le premier acteur à développer un outil qui couvrait les fonctionnalités essentielles de la supervision réseau. Pour cette raison, Nagios est devenu une solution très populaire. Grâce à cette forte pénétration du marché initial, elle reste l'une des plus utilisées.

En bref, Nagios était à l'origine de la supervision et, en fait, de nombreux nouveaux outils de supervision réseau ont hérité du code Nagios et l'ont fait évoluer. Bien que vous ayez de nombreux profils sur le marché, ils doivent avoir des connaissances très techniques et votre installation en dépendra à 100%. La migration future peut être délicate.

- Avantages de Nagios

- Configuration et édition avancées complexes, en raison de la nécessité de faire de nombreuses modifications manuelles.
- L'interface graphique manque de convivialité.
- Coût d'apprentissage élevé.

- Chaque installation s'avère au final être un « puzzle » dans lequel plus qu'un produit standard vous avez votre propre implémentation, avec des centaines de correctifs, votre propre code ou un code tiers, et il est difficile de faire évoluer ou de maintenir par des tiers.
- Rapports simples.
- Très pauvre dans sa gestion SNMP, à la fois l'interrogation et la gestion des déroutements.

➢ Inconvénients de Nagios

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

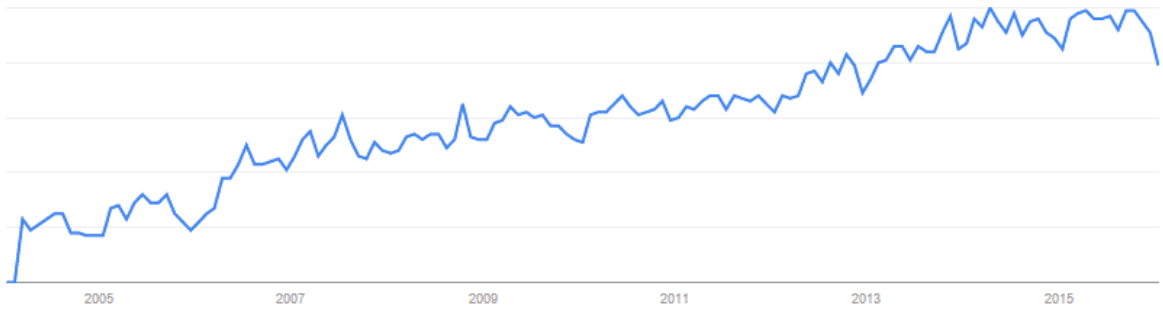
b. Zabbix :

Figure 67:zabbix

Zabbix est un logiciel qui supervise de nombreux paramètres réseaux ainsi que la santé et l'intégrité des serveurs. Zabbix utilise un mécanisme de notification flexible qui permet aux utilisateurs de configurer une base d'alerte e-mail pour pratiquement tous les événements. Cela permet une réponse rapide aux problèmes serveurs. Zabbix offre un

excellent reporting et des fonctionnalités de visualisation de données basées sur les données stockées. Cela rend Zabbix idéal "for capacity planning".

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



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

- Avantages de Zabbix

- Surveillance complète : Zabbix peut surveiller un large éventail de paramètres, notamment l'utilisation du processeur, l'utilisation de la mémoire, le trafic réseau, l'espace disque, etc. Il peut également surveiller les performances des applications et des services, ainsi que la disponibilité des périphériques réseau et des serveurs.
- Alertes personnalisables : Zabbix permet aux utilisateurs de mettre en place des alertes personnalisées basées sur des déclencheurs ou des conditions spécifiques. Cela signifie

que les professionnels de l'informatique peuvent être avertis des problèmes potentiels avant qu'ils ne deviennent critiques, ce qui leur permet de prendre des mesures et d'éviter les temps d'arrêt ou d'autres problèmes.

- Architecture flexible : Zabbix est conçu pour être flexible et évolutif, ce qui lui permet d'être utilisé dans une grande variété d'environnements. Il peut être déployé sur site ou dans le nuage, et peut être intégré à d'autres systèmes et outils.
- Interface conviviale : Zabbix dispose d'une interface conviviale qui permet aux professionnels de l'informatique de configurer et de gérer facilement les tâches de surveillance. Il fournit également des rapports et des analyses détaillés, ce qui facilite l'identification des tendances et des problèmes potentiels.

➢ Inconvénients de Zabbix

- Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire
- L'agent Zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple)
- Commence à être connu, mais pas encore auprès des entreprises : Peu d'interfaçage avec d'autres solutions commerciales

c. Pandora FMS:

Figure 68:Pandora FMS

La version libre de Pandora FMS est capable de superviser plus de 10 000 nœuds et couvre (sans limitations) la supervision réseau, serveur (basé sur un agent ou à distance) et la supervision des applications. Avec des fonctionnalités complètes de rapports, alertes, intégrations avec des tiers via API, etc.

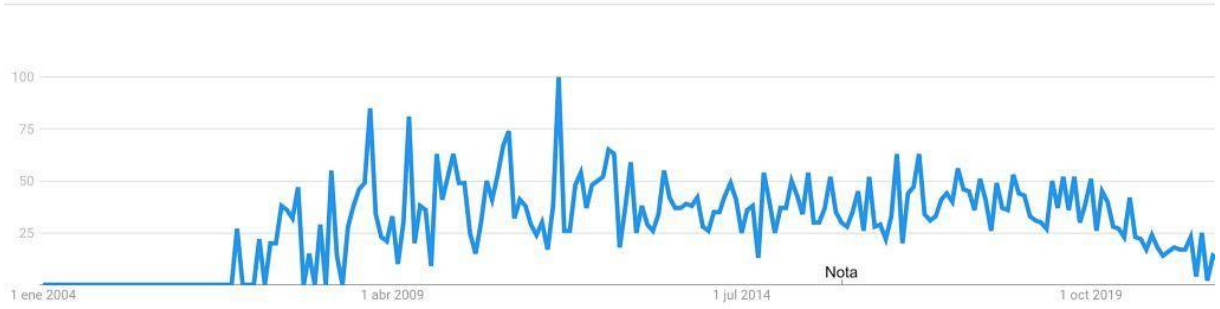
Vous pouvez UTILISER Pandora FMS GRATUITEMENT pour toujours et pour plus de 10 000 nœuds, dois-je vous dire comment ?

C'est l'un des rares outils dont l'architecture ne provient pas de Nagios, mais est créée à partir de 0, ce qui vous permet d'évoluer parfaitement dans de grands environnements. On est parvenu à superviser un environnement avec plus de 100.000 nœuds sans problème de performance.

Nous soulignons également son intégration avec les appareils mobiles, non seulement pour accéder à la console mais aussi pour les surveiller grâce à son système de géolocalisation.

Son système d'auto-découverte du réseau est capable, en peu de temps, de retrouver tous les éléments qui composent votre réseau.

L'évolution de l'intérêt pour Pandora Flexible Monitoring Software est restée stable au fil du temps, malgré de légères variations ponctuelles.



- Avantages de Pandora FMS

  - Supervisez toutes les zones (serveurs, applications, réseaux) avec une seule console centralisée.

- Scalable à grande échelle (des dizaines de milliers d'appareils).
- Cartes réseau, rapports, SLA, notifications intégrées, cartes de service, corrélation d'événements, collecte de journaux… et bien plus encore.

➢ Inconvénients de Pandora FMS

Sa communauté d'utilisateurs n'est pas aussi importante que d'autres applications comme Zabbix ou Nagios.

II. *Supervision avec Zabbix (Dmz privée Vlan 30) :*

Figure 69: Zabbix features overview

Zabbix est une plateforme de surveillance et de gestion de réseau open-source. Elle permet de surveiller en temps réel les performances et l'état de divers équipements et services informatiques tels que les serveurs, les routeurs, les commutateurs, les applications, etc.

Zabbix collecte des données à partir des équipements surveillés à l'aide d'agents ou de méthodes de collecte de données telles que SNMP (Simple Network Management Protocol), IPMI (Intelligent Platform Management Interface) ou des scripts personnalisés. Ces données sont ensuite stockées et analysées pour générer des rapports, des graphiques et des alertes en cas de dysfonctionnement ou de dépassement des seuils prédéfinis.

La plateforme Zabbix est très flexible et offre une large gamme de fonctionnalités telles que la surveillance des performances, la surveillance des journaux, la corrélation d'événements, la visualisation des données, l'automatisation des tâches, etc. Elle dispose également d'une interface utilisateur conviviale qui permet de configurer et de gérer facilement les différents aspects de la surveillance.

Zabbix est largement utilisé par les administrateurs système et les professionnels des technologies de l'information pour surveiller et gérer les infrastructures informatiques de petite et grande envergure. En tant que solution open-source, Zabbix est également apprécié pour sa communauté active, son extensibilité et sa possibilité d'adaptation aux besoins spécifiques de chaque organisation.

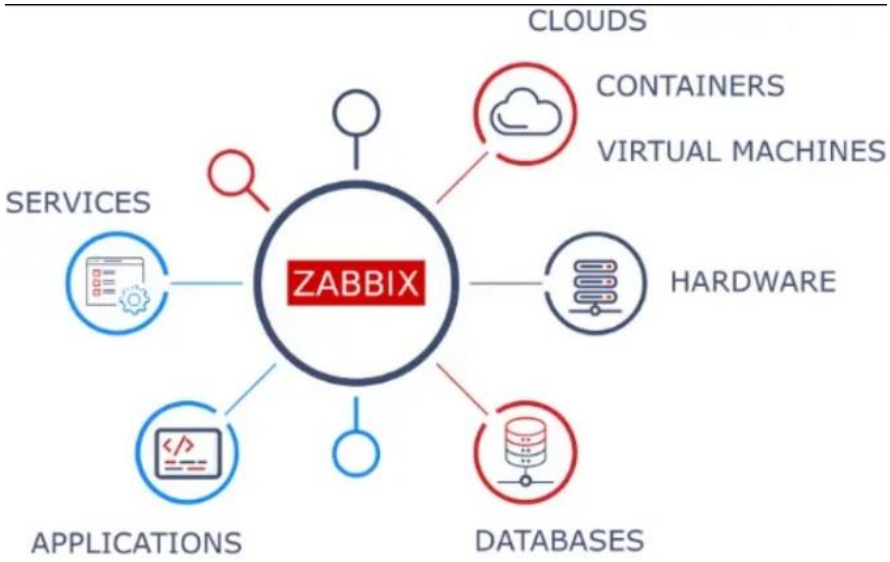


Figure 70: Différents hôtes Zabbix peut les

1. Serveur Zabbix :

Un serveur Zabbix est la pièce maîtresse de l'architecture Zabbix. Il s'agit d'un composant central qui gère la collecte des données, la configuration de la surveillance, le stockage des données et la génération d'alertes dans le système de surveillance Zabbix.

Le serveur Zabbix est responsable de la communication avec les agents Zabbix installés sur les systèmes surveillés. Il reçoit les données collectées par les agents, les traite, les stocke dans une base de données et les rend disponibles pour l'analyse et la visualisation ultérieures.

Les principales fonctions d'un serveur Zabbix incluent :

- Collecte de données : Le serveur Zabbix reçoit des données provenant des agents Zabbix, des équipements réseau via SNMP, des scripts personnalisés ou d'autres méthodes de collecte de données.
- Stockage des données : Les données collectées sont stockées dans une base de données, ce qui permet de conserver l'historique des performances et de générer des rapports.
- Configuration de la surveillance : Le serveur Zabbix permet de configurer les éléments à surveiller, les seuils d'alerte, les déclencheurs, les actions, etc.
- Analyse et visualisation des données : Le serveur Zabbix analyse les données collectées et les présente sous forme de graphiques, de tableaux de bord et de rapports pour une meilleure compréhension des performances du système.
- Génération d'alertes : Le serveur Zabbix génère des alertes en temps réel lorsqu'il détecte des anomalies ou lorsque les seuils prédéfinis sont dépassés. Les alertes peuvent être envoyées par e-mail, SMS ou d'autres moyens de communication.
- Administration et gestion : Le serveur Zabbix fournit une interface d'administration pour gérer les utilisateurs, les autorisations, les paramètres du système, etc.
- Le serveur Zabbix peut être déployé sur une machine physique ou virtuelle et peut être configuré pour superviser des environnements informatiques de petite à grande échelle.
- Dans Zabbix, les modèles et les éléments sont des concepts clés qui vous permettent de configurer la surveillance de vos systèmes. Voici une explication de ces termes :
- Modèles (Templates) : Les modèles sont des objets de configuration dans Zabbix qui définissent un ensemble de paramètres de surveillance prédéfinis. Ils

regroupent des éléments, des déclencheurs, des graphiques, des actions et d'autres objets liés à la surveillance d'un type spécifique de dispositif ou d'application. Les modèles peuvent être créés pour différents types de systèmes tels que des serveurs, des commutateurs réseau, des bases de données, des applications, etc. Vous pouvez créer vos propres modèles ou utiliser ceux fournis par la communauté Zabbix.

- Éléments (Items) : Les éléments sont des objets de surveillance individuels associés à un hôte ou à un modèle dans Zabbix. Ils définissent les métriques spécifiques à surveiller, telles que la disponibilité d'un service, l'utilisation du processeur, l'utilisation du disque, les performances réseau, etc. Les éléments sont configurés avec des types de collecte de données spécifiques, tels que Zabbix Agent, SNMP, IPMI, JMX, etc. Ils récupèrent les données à partir des cibles de surveillance et les enregistrent dans la base de données de Zabbix.

Lorsque vous configurez la surveillance dans Zabbix, vous pouvez suivre ces étapes générales :

1) Créez ou importez des modèles : Vous pouvez créer vos propres modèles dans Zabbix en définissant les éléments, les déclencheurs et d'autres paramètres de surveillance pertinents. Vous pouvez également importer des modèles déjà créés par la communauté Zabbix. Les modèles peuvent être gérés via l'option "Configuration" dans le menu principal de Zabbix.

2) Associez des modèles à des hôtes : Une fois que vous avez créé ou importé des modèles, vous pouvez les associer à des hôtes spécifiques. Cela permet d'appliquer les paramètres de surveillance du modèle à ces hôtes. Vous pouvez effectuer cette association en accédant à l'option "Configuration" dans le menu principal de Zabbix, en sélectionnant l'hôte souhaité, puis en ajoutant les modèles pertinents dans l'onglet "Modèles".

3) Configurez les éléments de surveillance : Pour chaque hôte ou modèle, vous devez configurer les éléments de surveillance spécifiques. Cela peut être fait en accédant à l'onglet "Éléments" de l'hôte ou du modèle et en ajoutant les éléments pertinents. Spécifiez le type de collecte de données approprié et les paramètres spécifiques à surveiller, tels que les clés d'éléments pour l'Agent Zabbix, les OIDs SNMP, etc.

4) Personnalisez les déclencheurs, les graphiques et les actions : Vous pouvez également personnaliser les déclencheurs pour définir des seuils d'alerte, créer des graphiques pour visualiser les données de surveillance et configurer des actions pour envoyer des notifications en cas de dépassement des seuils.

Ces étapes vous permettront de configurer la surveillance de vos systèmes à l'aide de modèles et d'éléments dans Zabbix.

2. Installation serveur Zabbix :

```
zabbix_prv@zabbix: ~
zabbix_prv@zabbix:~$ sudo apt install apache2
[sudo] Mot de passe de zabbix_prv :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 mis à jour, 8 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1,917 ko dans les archives.
Après cette opération, 7,706 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Réception de :2 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.1 [92.6 kB]
Réception de :3 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4.22.04.1 [11.3 kB]
Réception de :4 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.04.1 [9,168 B]
Réception de :5 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.5 [1,345 kB]
59% [5 apache2-bin 950 kB/1,345 kB 71%]                    42.6 kB/s60% [5 apache2-bin 978 kB/1,345 kB 73%]                    46.3 kB/s 156
```

Figure 71:Installation Apache

```
zabbix_prv@zabbix: ~
zabbix_prv@zabbix:~$ sudo apt install mysql-server -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl
  libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server-8.0
  mysql-server-core-8.0
Paquets suggérés :
  libipc-sharedcache-perl mailx tinyca
Les NOUVEAUX paquets suivants seront installés :
  libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-template-perl
  libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server
  mysql-server-8.0 mysql-server-core-8.0
```

Figure 72:Installation de MySQL

```
zabbix_prv@zabbix:~$ sudo mysql_secure_installation

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

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

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

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

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

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

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

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


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

Figure 73: Sécuriser l'installation de MySQL

```
zabbix_prv@zabbix: ~
Traitement des actions différées («triggers») pour man-db (2.10.2-1) ...
zabbix_prv@zabbix:~$ curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash
# [info] Checking for script prerequisites.
# [info] MariaDB Server version 10.11 is valid
# [info] Repository file successfully written to /etc/apt/sources.list.d/mariadb.list
# [info] Adding trusted package signing keys...
# [info] Running apt-get update...
# [info] Done adding trusted package signing keys
zabbix_prv@zabbix:~$ sudo apt-get install mariadb-server mariadb-client -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libaio1 libevent-core-2.1-7 libevent-pthreads-2.1-7 libmecab2
  libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  galera-4 gawk libconfig-inifiles-perl libdaxctl1 libdbd-mysql-perl
  libdbi-perl libmariadb3 libmysqlclient21 libndctl6 libpmem1 libsigsegv2
  libterm-readkey-perl liburing2 mariadb-client-core mariadb-common
  mariadb-server-core pv socat
Paquets suggérés :
  gawk-doc libmldbm-perl libnet-daemon-perl libsql-statement-perl mailx
  mariadb-test doc-base
Les paquets suivants seront ENLEVÉS :
  mysql-client-8.0 mysql-client-core-8.0 mysql-server mysql-server-8.0
  mysql-server-core-8.0
Les NOUVEAUX paquets suivants seront installés :
  galera-4 gawk libconfig-inifiles-perl libdaxctl1 libdbd-mysql-perl
  libdbi-perl libmariadb3 libmysqlclient21 libndctl6 libpmem1 libsigsegv2
  libterm-readkey-perl liburing2 mariadb-client mariadb-client-core
  mariadb-common mariadb-server mariadb-server-core pv socat
0 mis à jour, 20 nouvellement installés, 5 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 29.7 Mo dans les archives.
Après cette opération, 48.0 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy/main amd64 mariadb-common all 1:10.11.3+maria~ubu2204 [3,916 B]
Réception de :2 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy/main amd64 galera-4 amd64 26.4.14-ubu2204 [10.3 MB]
Réception de :3 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy/main amd64 libmariadb3 amd64 1:10.11.3+maria~ubu2204 [174 kB]
Réception de :4 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy/main amd64 mariadb-client-core amd64 1:10.11.3+maria~ubu2204 [1,2
```

Figure 74: Installation de Maria DB

```
zabbix_prv@zabbix: ~                                                    zabbix_prv@
Remove anonymous users? [Y/n] y
 ... Success!

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

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

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

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

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

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

Cleaning up...

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

Thanks for using MariaDB!
```

Figure 75:Sécurisé Maria DB

```
root@zabbix: /home/zabbix_prv
root@zabbix: /usr/share/zabbix-server-mysql    zabbix_prv@zabbix: ~    root@zabbix: /home/zabbix_prv
root@zabbix:/home/zabbix_prv# wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
--2023-05-15 16:18:37--  https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)… 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3676 (3.6K) [application/octet-stream]
Enregistre : ‘zabbix-release_6.0-4+ubuntu22.04_all.deb’

zabbix-release_6.0-4+ubuntu22.04_all. 100%[===================================================================>]   3.59K  --.-KB/s    ds 0s

2023-05-15 16:18:38 (965 MB/s) - ‘zabbix-release_6.0-4+ubuntu22.04_all.deb’ enregistré [3676/3676]

root@zabbix:/home/zabbix_prv# dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 205733 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.0-4+ubuntu22.04_all.deb ...
Dépaquetage de zabbix-release (1:6.0-4+ubuntu22.04) ...
Paramétrage de zabbix-release (1:6.0-4+ubuntu22.04) ...
root@zabbix:/home/zabbix_prv# apt update
Réception de :2 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy InRelease [7,767 B]
Atteint :1 https://downloads.mariadb.com/Tools/ubuntu jammy InRelease
Réception de :3 https://dlm.mariadb.com/repo/maxscale/latest/apt jammy InRelease [9,350 B]
Réception de :4 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy InRelease [4,952 B]
Réception de :5 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy InRelease [4,958 B]
Réception de :6 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main Sources [1,002 B]
Réception de :7 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main amd64 Packages [624 B]
Réception de :8 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main Sources [1,943 B]
Réception de :9 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 Packages [5,485 B]
Atteint :10 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :11 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Réception de :12 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Atteint :13 http://security.ubuntu.com/ubuntu jammy-security InRelease
144 ko réceptionnés en 21s (6,743 o/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
```

Figure 76:1ère étape d'installation Zabbix

```
(Lecture de la base de données... 205733 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.0-4+ubuntu22.04_all.deb ...
Dépaquetage de zabbix-release (1:6.0-4+ubuntu22.04) ...
Paramétrage de zabbix-release (1:6.0-4+ubuntu22.04) ...
root@zabbix:/home/zabbix_prv# apt update
Réception de :2 https://dlm.mariadb.com/repo/mariadb-server/10.11/repo/ubuntu jammy InRelease [7,767 B]
Atteint :1 https://downloads.mariadb.com/Tools/ubuntu jammy InRelease
Réception de :3 https://dlm.mariadb.com/repo/maxscale/latest/apt jammy InRelease [9,350 B]
Réception de :4 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy InRelease [4,952 B]
Réception de :5 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy InRelease [4,958 B]
Réception de :6 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main Sources [1,002 B]
Réception de :7 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main amd64 Packages [624 B]
Réception de :8 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main Sources [1,943 B]
```

Figure 77:2eme étape d’installation Zabbix

```
root@zabbix:/home/zabbix_prv# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libaio1 libblas3 libevent-core-2.1-7 libevent-pthreads-2.1-7 liblinear4 libmecab2 libodbc1 libodbccr2 libprotobuf-lite23 libssh2-1 lua-lpeg
  mecab-ipadic mecab-ipadic-utf8 mecab-utils nmap nmap-common
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  fonts-dejavu fonts-dejavu-extra libmodbus5
Paquets suggérés :
  zabbix-nginx-conf
Les NOUVEAUX paquets suivants seront installés :
  fonts-dejavu fonts-dejavu-extra libmodbus5 zabbix-agent zabbix-apache-conf zabbix-frontend-php zabbix-server-mysql zabbix-sql-scripts
0 mis à jour, 8 nouvellement installés, 0 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 17.9 Mo dans les archives.
Après cette opération, 57.6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-server-mysql amd64 1:6.0.17-1+ubuntu22.04 [1,346 kB]
Réception de :2 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-agent amd64 1:6.0.17-1+ubuntu22.04 [252 kB]
Réception de :3 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-frontend-php all 1:6.0.17-1+ubuntu22.04 [6,923 kB]
Réception de :4 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 fonts-dejavu-extra all 2.37-2build1 [2,041 kB]
Réception de :5 http://ma.archive.ubuntu.com/ubuntu jammy/universe amd64 fonts-dejavu all 2.37-2build1 [3,192 B]
Réception de :6 http://ma.archive.ubuntu.com/ubuntu jammy/universe amd64 libmodbus5 amd64 3.1.6-2 [23.5 kB]
Réception de :7 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-apache-conf all 1:6.0.17-1+ubuntu22.04 [7,784 B]
Réception de :8 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-sql-scripts all 1:6.0.17-1+ubuntu22.04 [7,295 kB]
17.9 Mo réceptionnés en 2min 27s (122 ko/s)
Sélection du paquet zabbix-server-mysql précédemment désélectionné.
(Lecture de la base de données... 205740 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../0-zabbix-server-mysql_1%3a6.0.17-1+ubuntu22.04_amd64.deb ...
Dépaquetage de zabbix-server-mysql (1:6.0.17-1+ubuntu22.04) ...
Sélection du paquet fonts-dejavu-extra précédemment désélectionné.
Préparation du dépaquetage de .../1-fonts-dejavu-extra_2.37-2build1_all.deb ...
Dépaquetage de fonts-dejavu-extra (2.37-2build1) ...
Sélection du paquet fonts-dejavu précédemment désélectionné.
```

Figure 78: 3éme étape de d'installation de Zabbix

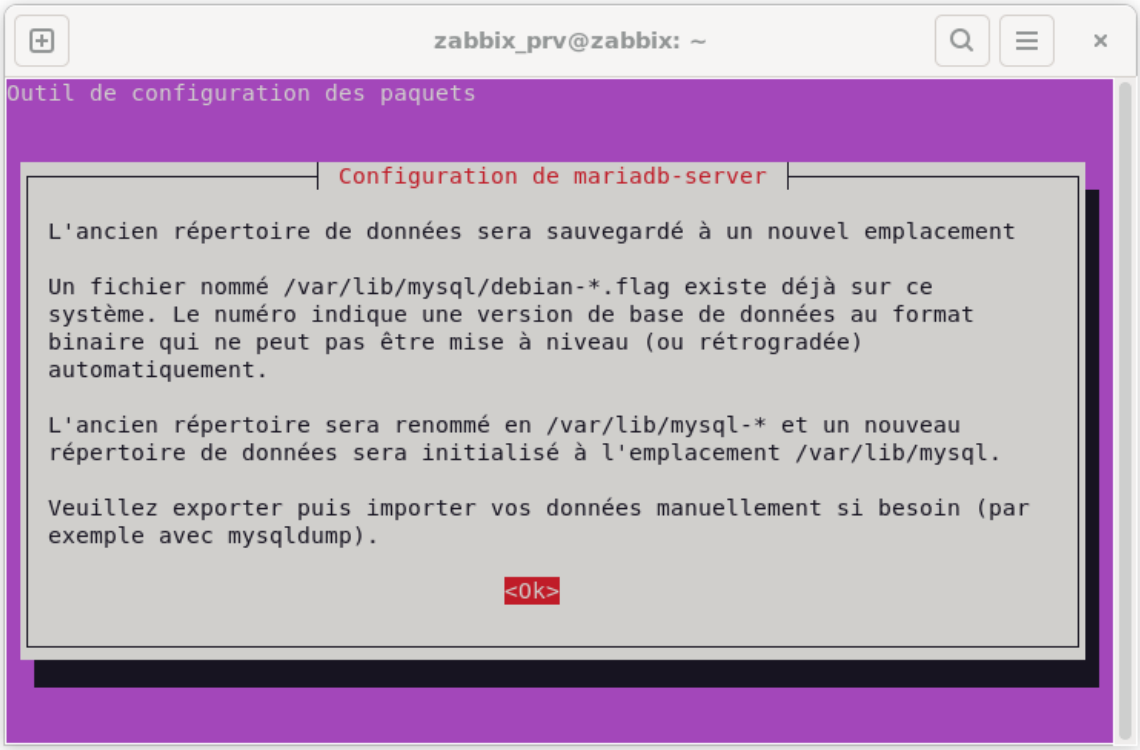


Figure 79: Configuration de Maria DB

```
root@zabbix: /home/zabbix_prv
root@zabbix: /home/zabbix_prv        zabbix_prv@zabbix: ~
Cleaning up...

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

Thanks for using MariaDB!
zabbix_prv@zabbix:~$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.3-MariaDB-1:10.11.3+maria~ubu2204 mariadb.org binary distribution

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

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

MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user zabbix@localhost identified by 'azrksdf@123';
Query OK, 0 rows affected (0.044 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.021 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> quit;
Bye
zabbix_prv@zabbix:~$ sudo su
[sudo] Mot de passe de zabbix_prv :
Désolé, essayez de nouveau.
[sudo] Mot de passe de zabbix_prv :
root@zabbix:/home/zabbix_prv#
```

Figure 80: Création de base de données

```
root@zabbix:/home/zabbix_prv# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
root@zabbix:/home/zabbix_prv#
```

Figure 81: 4éme étape d'installation de Zabbix

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

```
root@zabbix: /home/zabbix_prv
  GNU nano 6.2                                    /etc/zabbix/zabbix_server.conf
# This is a configuration file for Zabbix server daemon
# To get more information about Zabbix, visit http://www.zabbix.com

############ GENERAL PARAMETERS #################

### Option: ListenPort
#       Listen port for trapper.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10051

### Option: SourceIP
#       Source IP address for outgoing connections.
#
# Mandatory: no
# Default:
# SourceIP=

### Option: LogType
#       Specifies where log messages are written to:
#               system  - syslog
#               file    - file specified with LogFile parameter
#               console - standard output
#
# Mandatory: no
# Default:
# LogType=file

### Option: LogFile
#       Log file name for LogType 'file' parameter.
#
# Mandatory: yes, if LogType is set to file, otherwise no

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  M-U Annuler   M-A Marquer   M-] -> Crochet
```

Figure 82:Fichier de configuration de Zabbix server

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=azrksdf@123
```

Figure 83: Configuration de Zabbix server

```
root@zabbix:/home/zabbix_prv# systemctl restart zabbix-server zabbix-agent apache2
root@zabbix:/home/zabbix_prv# systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
root@zabbix:/home/zabbix_prv#
```

Figure 84: Restart and enable Zabbix-server/Zabbix-agent

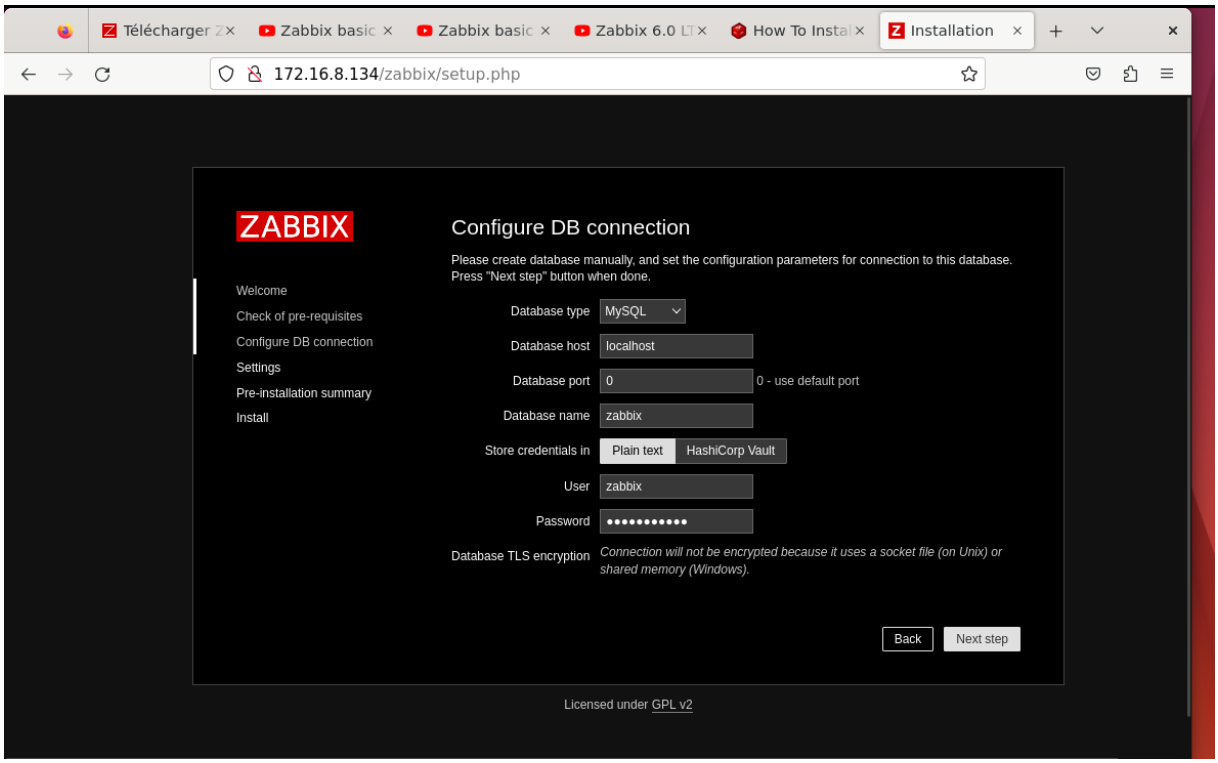


Figure 85: Configuration de Zabbix dans l'interface web 1

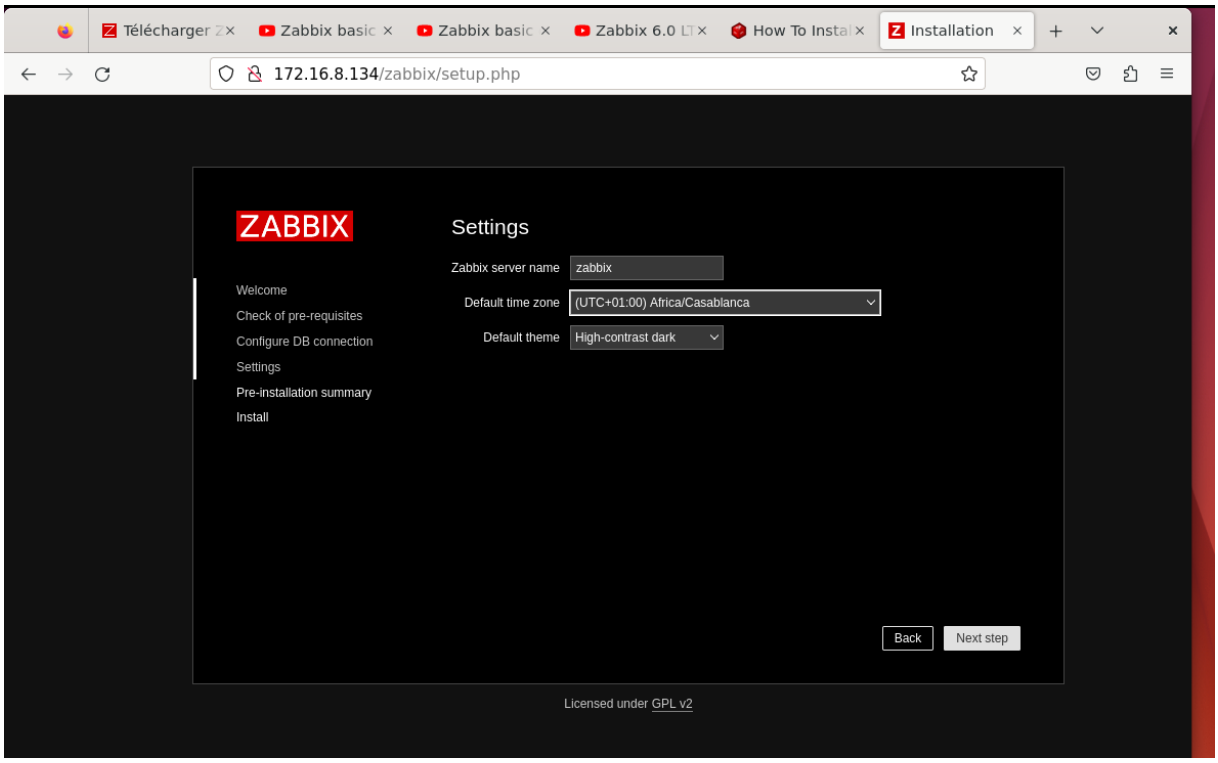


Figure 86:Configuration de Zabbix dans l'interface web 2

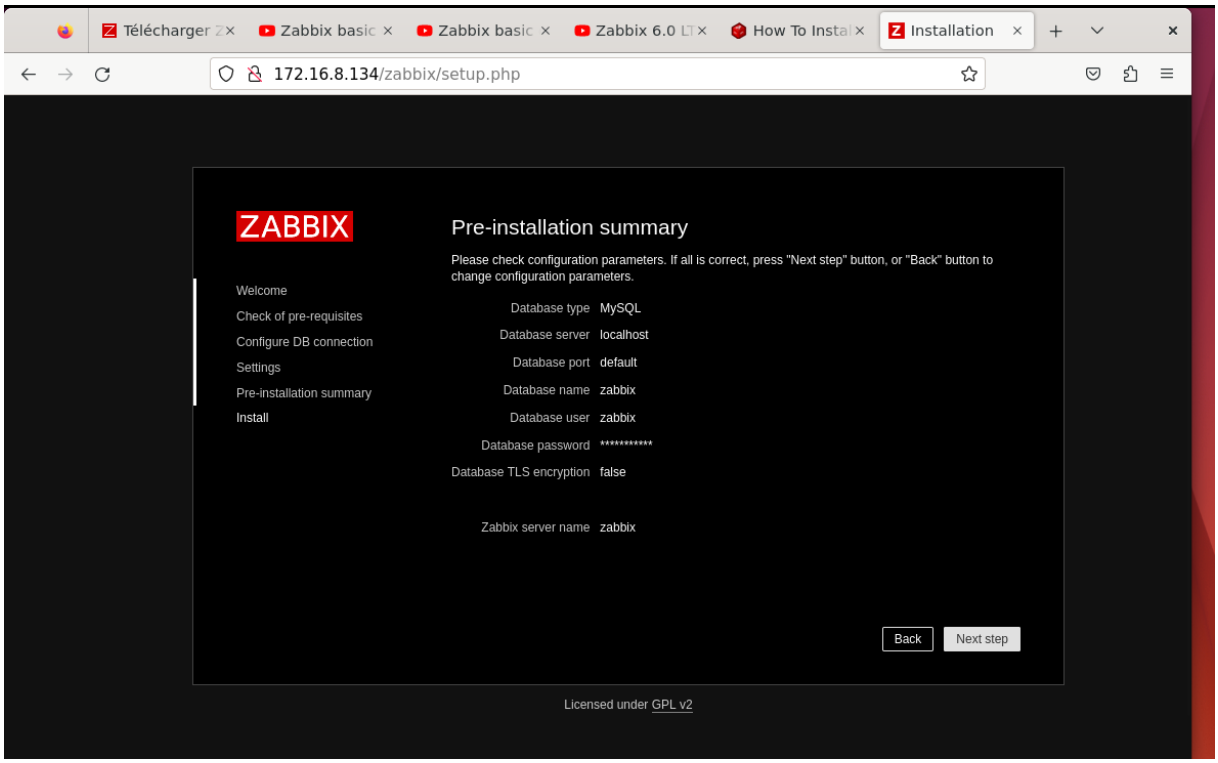


Figure 87: Configuration de Zabbix dans l'interface web 3

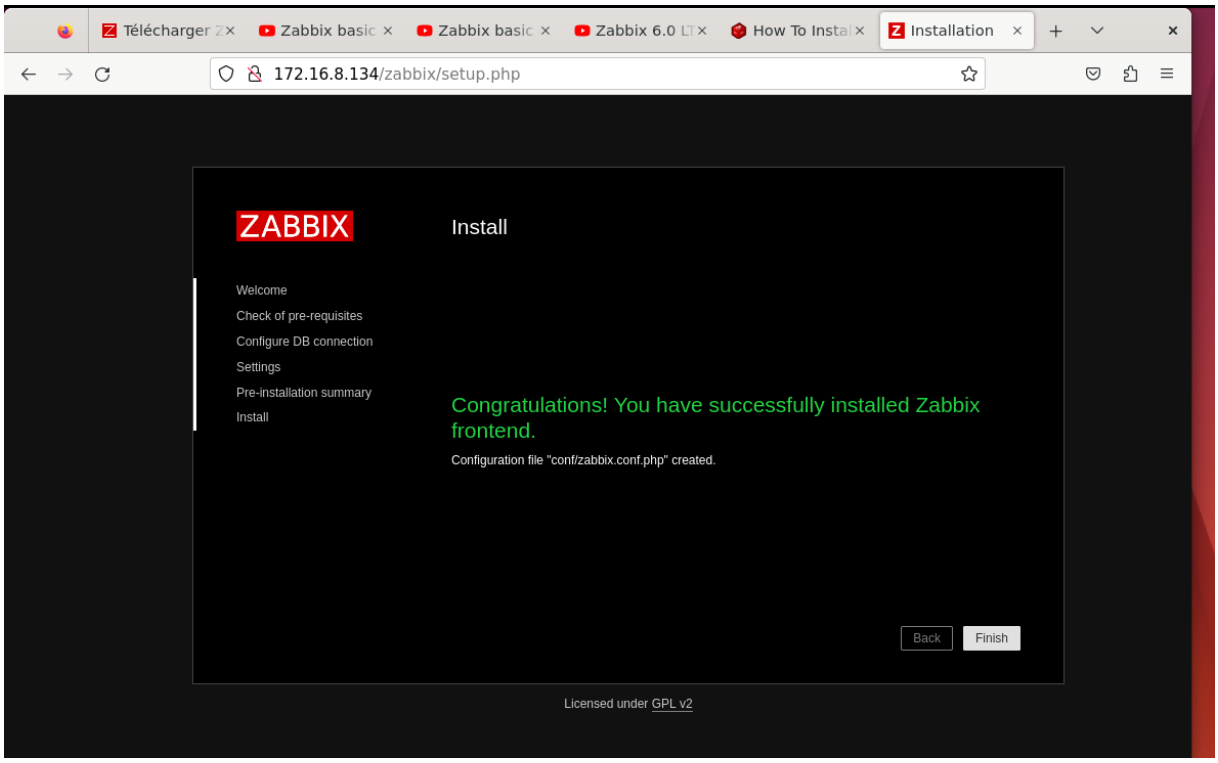


Figure 88: Installation de Zabbix terminée

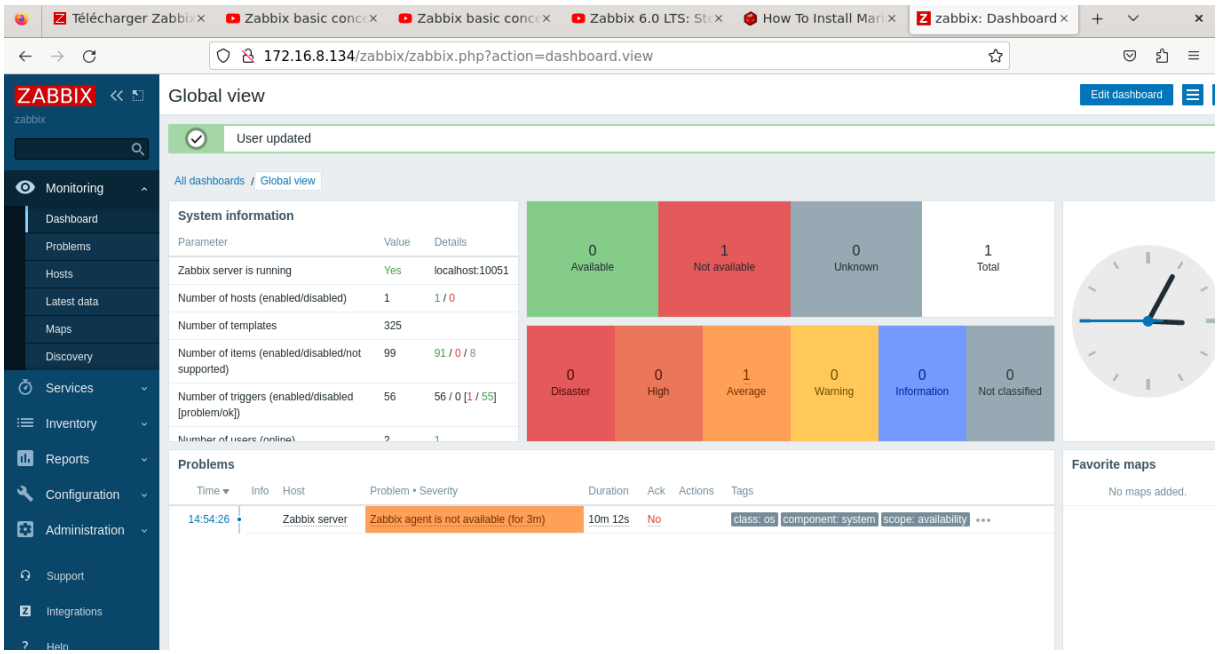


Figure 89: Dashboard

3. Agent Zabbix :

L'agent Zabbix est un logiciel qui doit être installé sur les systèmes ou les périphériques que vous souhaitez surveiller à l'aide de la plateforme Zabbix. Il s'agit d'un composant facultatif de Zabbix, mais il offre des fonctionnalités supplémentaires de surveillance et de collecte de données.

L'agent Zabbix est généralement installé sur les serveurs, les ordinateurs de bureau ou les appareils réseau que vous souhaitez superviser. Une fois installé, l'agent collecte différentes données sur le système, telles que l'utilisation du processeur, la mémoire, l'utilisation du disque, les connexions réseau, etc. Ces données sont ensuite envoyées au serveur Zabbix pour analyse.

L'agent Zabbix utilise un protocole spécifique pour communiquer avec le serveur Zabbix, généralement via TCP/IP. Il peut être configuré pour envoyer régulièrement des mises à jour des données de surveillance au serveur, ce qui permet d'obtenir des informations en temps réel sur l'état du système surveillé.

L'agent Zabbix offre plusieurs avantages, notamment une faible consommation de ressources, une configuration flexible et la possibilité de surveiller des métriques spécifiques à un système d'exploitation ou à une application. Il peut également exécuter des scripts personnalisés pour collecter des données supplémentaires.

Cependant, il est important de noter que l'utilisation de l'agent Zabbix n'est pas obligatoire pour la surveillance avec Zabbix. Zabbix propose également d'autres méthodes de collecte de données telles que SNMP, IPMI ou l'interrogation directe des services réseau. Le choix d'utiliser ou non l'agent dépend des besoins spécifiques de surveillance et des contraintes du système à supervise.

```
root@mail: /home/grp2
Reading state information... Done
60 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@mail:/home/grp2# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  grub-common grub-pc grub-pc-bin grub2-common
The following packages will be upgraded:
  code dovecot-core dovecot-pop3d fonts-opensymbol gnome-session-canberra
  google-chrome-stable iptables libcanberra-gtk3-0 libcanberra-gtk3-module
  libcanberra-pulse libcanberra0 libip4tc2 libip6tc2 libnautilus-extension1a
  libperl5.34 libpython3.10 libpython3.10-minimal libpython3.10-stdlib
  libraw20 libreoffice-base-core libreoffice-calc libreoffice-common
  libreoffice-core libreoffice-draw libreoffice-gnome libreoffice-gtk3
  libreoffice-help-common libreoffice-help-en-us libreoffice-impress
  libreoffice-math libreoffice-ogltrans libreoffice-pdfimport
  libreoffice-style-breeze libreoffice-style-colibre
  libreoffice-style-elementary libreoffice-style-yaru libreoffice-writer
  libssh-4 libuno-cppu3 libuno-cppuhelpergcc3-3 libuno-purpenvhelpergcc3-3
  libuno-sal3 libuno-salhelpergcc3-3 libxtables12 nautilus nautilus-data perl
  perl-base perl-modules-5.34 python3-uno python3.10 python3.10-minimal
  sysstat tzdata uno-libs-private ure
56 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
39 standard LTS security updates
Need to get 308 MB/325 MB of archives.
After this operation, 840 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 dovecot-pop3d amd64 1:2.3.16+dfsg1-3ubuntu2.2 [37.7 kB]
Get:2 http://packages.microsoft.com/repos/code stable/main amd64 code amd64 1.79.0-1686149120 [95.9 MB]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 dovecot-core amd64 1:2.3.16+dfsg1-3ubuntu2.2 [3,319 kB]
Get:4 https://dl.google.com/linux/chrome/deb stable/main amd64 google-chrome-stable amd64 114.0.5735.106-1 [93.9 MB]
Get:5 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 iptables amd64 1.8.7-1ubuntu5.1 [455 kB]
Get:6 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxtables12 amd64 1.8.7-1ubuntu5.1 [31.2 kB]
Get:7 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2 amd64 1.8.7-1ubuntu5.1 [20.2 kB]
Get:8 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip4tc2 amd64 1.8.7-1ubuntu5.1 [19.8 kB]
```

Figure 90: Mise à jour

```
root@mail: /home/grp2

root@mail:/home/grp2# sudo apt update
Get:1 http://packages.microsoft.com/repos/code stable InRelease [3,569 B]
Hit:2 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:5 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:6 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:7 http://packages.microsoft.com/repos/code stable/main arm64 Packages [70.3 kB]
Get:8 http://packages.microsoft.com/repos/code stable/main armhf Packages [70.6 kB]
Get:9 http://packages.microsoft.com/repos/code stable/main amd64 Packages [70.0 kB]
Get:10 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [672 kB]
Get:11 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [419 kB]
Get:12 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [182 kB]
Get:13 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [102 kB]
Get:14 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [15.0 kB]
Get:15 http://ma.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [350 kB]
Get:16 http://ma.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [52.8 kB]
Get:17 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [920 kB]
Get:18 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,080 B]
Get:19 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [622 kB]
Get:20 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [194 kB]
Get:21 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [274 kB]
Get:22 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 48x48 Icons [185 kB]
Get:23 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [455 kB]
Get:24 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 64x64 Icons [284 kB]
Get:25 http://ma.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [20.0 kB]
Get:26 http://ma.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:27 http://ma.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [7,972 B]
Get:28 http://ma.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [23.4 kB]
Get:29 http://ma.archive.ubuntu.com/ubuntu jammy-backports/universe i386 Packages [13.9 kB]
Get:30 http://ma.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [16.8 kB]
Get:31 http://ma.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [548 B]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [234 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [122 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41.5 kB]
```

```
root@mail: /home/grp2
root@mail: /etc/zabbix        root@mail: /home/grp2

root@mail:/home/grp2# apt install zabbix-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zabbix-agent is already the newest version (1:5.0.17+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
root@mail:/home/grp2#
```

Figure 91: Installation de l'agent Zabbix

```
Processing triggers for dovecot-core (1:2.3.16+dfsg1-3ubuntu2.2) ...
root@mail:/home/grp2# cd /etc/zabbix/
root@mail:/etc/zabbix# ls
zabbix_agentd.conf  zabbix_agentd.conf.d
root@mail:/etc/zabbix# nano zabbix_agentd.conf
```

Figure 92:Fichier de configuration de l'agent

```
root@mail: /etc/zabbix
  GNU nano 6.2                                        zabbix_agentd.conf
#       Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=172.16.8.134

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

### Option: ListenIP
#       List of comma delimited IP addresses that the agent should listen on.
#       First IP address is sent to Zabbix server if connecting to it to retrieve list of active checks.
#
# Mandatory: no
# Default:
# ListenIP=0.0.0.0

### Option: StartAgents
#       Number of pre-forked instances of zabbix_agentd that process passive checks.
#       If set to 0, disables passive checks and the agent will not listen on any TCP port.
#
# Mandatory: no
# Range: 0-100
# Default:
# StartAgents=3

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Figure 93: Spécification de port d'écoute et l'adresse de serveur Zabbix

```
root@mail: /etc/zabbix
  GNU nano 6.2                                        zabbix_agentd.conf
#       IPv6 addresses must be enclosed in square brackets if port for that host is specified.
#       If port is not specified, square brackets for IPv6 addresses are optional.
#       If this parameter is not specified, active checks are disabled.
#       Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=172.16.8.134

### Option: Hostname
#       Unique, case sensitive hostname.
#       Required for active checks and must match hostname as configured on the server.
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
Hostname=dmz public


### Option: HostnameItem
#       Item used for generating Hostname if it is undefined. Ignored if Hostname is defined.
#       Does not support UserParameters or aliases.
#
# Mandatory: no
# Default:
# HostnameItem=system.hostname

### Option: HostMetadata
#       Optional parameter that defines host metadata.
#       Host metadata is used at host auto-registration process.
#       An agent will issue an error and not start if the value is over limit of 255 characters.

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Figure 94: Spécification de Serveur Active et Host Name (même nom dans le serveur Zabbix)

4. SNMP :

SNMP (Simple Network Management Protocol) est un protocole largement utilisé dans le domaine des réseaux informatiques pour la supervision et la gestion des équipements réseau. Il permet de collecter des informations de surveillance à partir de périphériques compatibles SNMP tels que des routeurs, des commutateurs, des serveurs, des imprimantes, etc. Le SNMP fonctionne selon un modèle client-serveur, où un gestionnaire SNMP (SNMP Manager) communique avec des agents SNMP (SNMP Agents) présents sur les appareils réseau. Le gestionnaire SNMP envoie des requêtes aux agents SNMP pour obtenir des informations de surveillance, telles que le trafic réseau, les performances, les erreurs, les températures, etc. Les agents SNMP, quant à eux, collectent ces informations et les rendent disponibles au gestionnaire. Le protocole SNMP repose sur un ensemble de messages et de structures de données normalisées. Il utilise des identifiants uniques appelés OID (Object Identifier) pour identifier les variables et les informations de gestion. Les variables de gestion sont organisées dans une structure hiérarchique appelée MIB (Management Information Base). La MIB définit les objets SNMP et leurs attributs, fournissant ainsi une structure standardisée pour la gestion des appareils réseau. SNMP offre également la possibilité de déclencher des notifications ou des alertes (SNMP Traps) en cas d'événements spécifiques, tels qu'une panne de réseau, une utilisation excessive de la bande passante, etc. Cela permet aux administrateurs réseau de recevoir des alertes en temps réel pour prendre des mesures correctives rapidement. Pour configurer SNMP, il faut généralement activer le service SNMP sur les appareils réseau et configurer des paramètres tels que la communauté SNMP (une chaîne d'authentification), les autorisations d'accès, les adresses IP autorisées, etc.

a. Gestionnaire SNMP :

Un gestionnaire ou système de gestion est une entité distincte chargée de communiquer avec les périphériques réseau mis en œuvre par l'agent SNMP. Il s'agit généralement d'un ordinateur utilisé pour exécuter un ou plusieurs systèmes de gestion de réseau.

Fonctions clés du gestionnaire SNMP :

- Requête d'Agents
- Obtenir les réponses des agents
- Définir les variables dans les agents
- Reconnaître les événements asynchrones des agents

b. Périphériques gérés :

Un périphérique géré ou l'élément de réseau est une partie du réseau qui nécessite une certaine forme d'analyse et de gestion, par exemple routeurs, commutateurs, serveurs, postes de travail, imprimantes, onduleurs, etc ...

c. Agent SNMP:

L'agent est un programme intégré à l'élément de réseau. L'activation de l'agent lui permet de collecter la base de données d'informations de gestion à partir du périphérique localement et la met à la disposition du gestionnaire SNMP, lorsqu'il est interrogé. Ces agents peuvent être standard (par exemple Net-SNMP) ou spécifiques à un fournisseur (par exemple, l'agent HP Insight).

- Collecte des informations de gestion sur son environnement local
- Stocke et récupère les informations de gestion telles que définies dans la MIB.
- Signale un événement au gestionnaire.
- Agit en tant que proxy pour certains nœuds de réseau non SNMP gérables.

Versions du SNMP

Depuis sa création, SNMP a subi d'importantes mises à niveau. Cependant, le protocole SNMP v1 et v2c sont les versions les plus implémentées de SNMP. La prise en charge du protocole SNMP v3 a récemment commencé à rattraper son retard car il est plus sécurisé

par rapport à ses anciennes versions, mais il n'a toujours pas atteint une part de marché considérable.

- SNMPv1 : Il s'agit de la première version du protocole SNMP, qui est définie dans les RFC 1155 et 1157
- SNMPv2c : Il s'agit du protocole révisé, qui comprend des améliorations de SNMPv1 dans les domaines des types de paquets de protocole, des mappages de transport, des éléments de structure MIB mais en utilisant la structure d'administration SNMPv1 existante ("Community based " et donc SNMPv2c). Il est défini dans RFC 1901, RFC 1905, RFC 1906, RFC 2578.
- SNMPv3 : SNMPv3 définit la version sécurisée du SNMP. Le protocole SNMPv3 facilite également la configuration à distance des entités SNMP. Il est défini par RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

Bien que chaque version ait évolué vers de riches fonctionnalités, l'accent a été mis sur l'aspect sécurité de chaque mise à niveau. Voici un petit clip sur chaque aspect de sécurité des éditions.

d. Base de données d'informations de gestion ou Management Information Base (MIB) :

Chaque agent SNMP gère une base de données d'informations décrivant les paramètres du périphérique géré. Le gestionnaire SNMP utilise cette base de données pour demander à l'agent des informations spécifiques et traduit les informations selon les besoins du système de gestion de réseau (NMS). Cette base de données communément partagée entre l'agent et le gestionnaire s'appelle Management Information Base (MIB).

En règle générale, ces MIB contiennent un ensemble standard de valeurs statistiques et de contrôle défini pour les nœuds matériels d'un réseau. SNMP permet également l'extension de ces valeurs standard avec des valeurs spécifiques à un agent particulier grâce à l'utilisation de MIB privées.

En bref, les fichiers MIB sont l'ensemble des questions qu'un gestionnaire SNMP peut poser à l'agent. L'agent collecte ces données localement et les stocke, comme défini dans la MIB. Ainsi, le gestionnaire SNMP doit être conscient de ces questions standard et privées pour chaque type d'agent.

5. Ajout des hôtes :

Accès à la section "Configuration" : Dans le menu principal de Zabbix, cliquez sur "Configuration" pour accéder à la section de configuration.

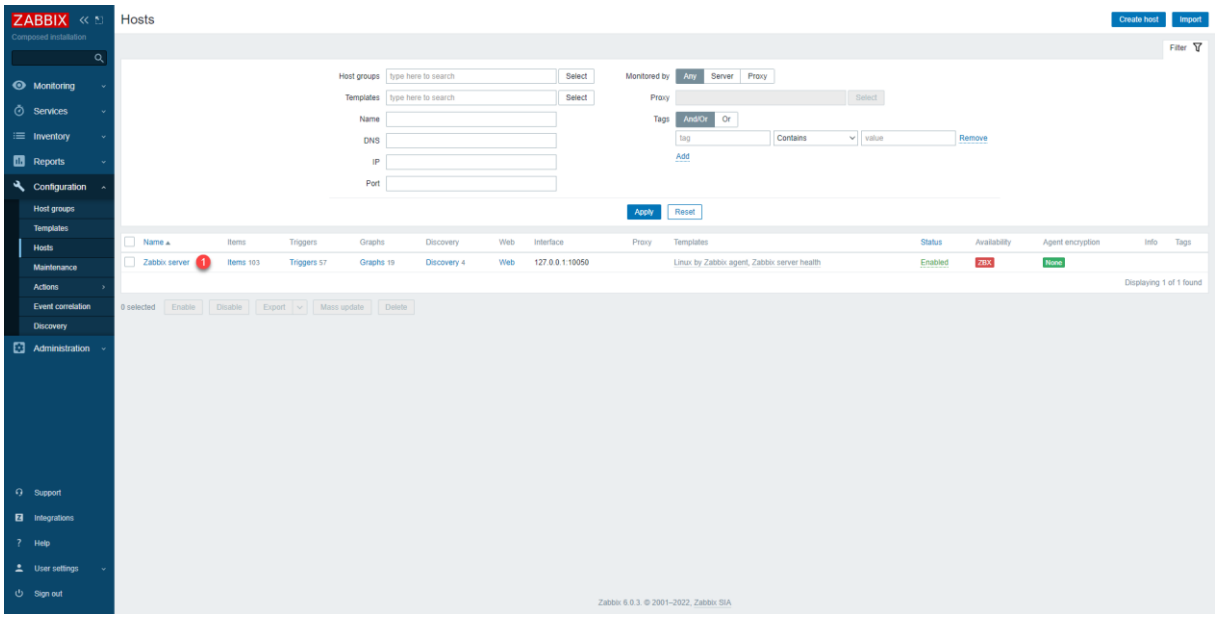


Figure 95: Ajout des hôtes

Ajout d'un groupe d'hôtes : Dans la section "Configuration", cliquez sur "Groupes d'hôtes" pour créer un groupe qui regroupera vos hôtes. Cliquez sur "Créer un groupe d'hôtes" et spécifiez un nom pour le groupe (par exemple, "Dmz public", "Radius et dhcp", etc.). Enregistrez les modifications.

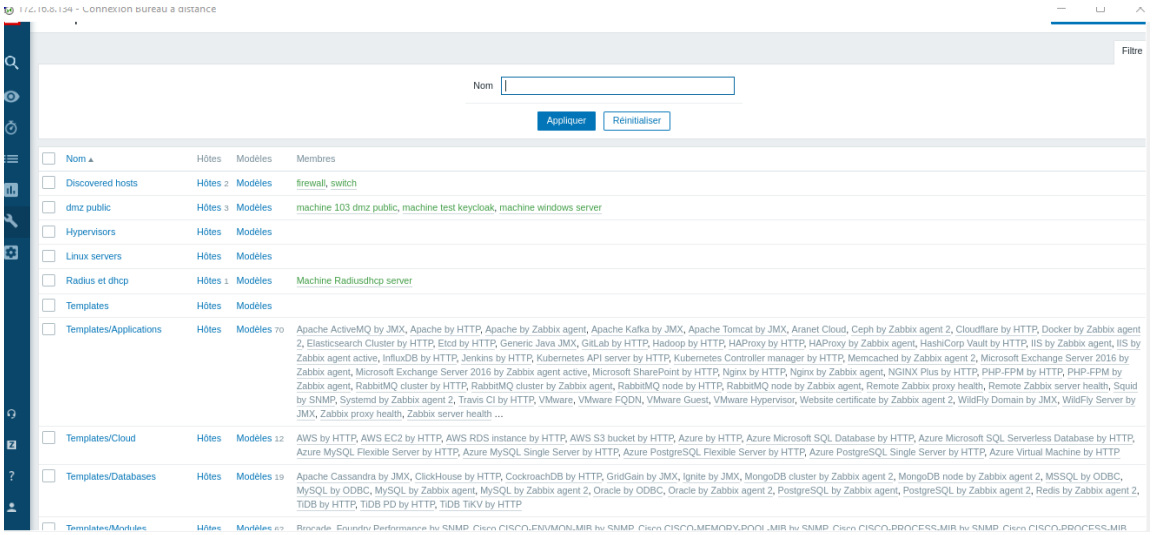


Figure 96: Les groupes d'hôtes de notre serveur

Ajout d'un hôte : Dans la section "Configuration", cliquez sur "Hôtes" pour ajouter un nouvel hôte. Cliquez sur "Créer un hôte" et remplissez les informations nécessaires, telles que le nom de l'hôte, l'adresse IP ou le nom d'hôte, le groupe d'hôtes auquel il appartient, etc.

a. Switch:

Configuration de SNMP sur switch:

STAGE # configure

STAGE(Config)#snmp-server community stage rw

STAGE(Config)#snmp-server enable traps all

STAGE(Config)#snmp-server host 172.16.8.134 stage

Dans la configuration de l'hôte, spécifiez l'adresse IP ou le nom d'hôte de l'équipement, les informations de communauté SNMP, le port SNMP

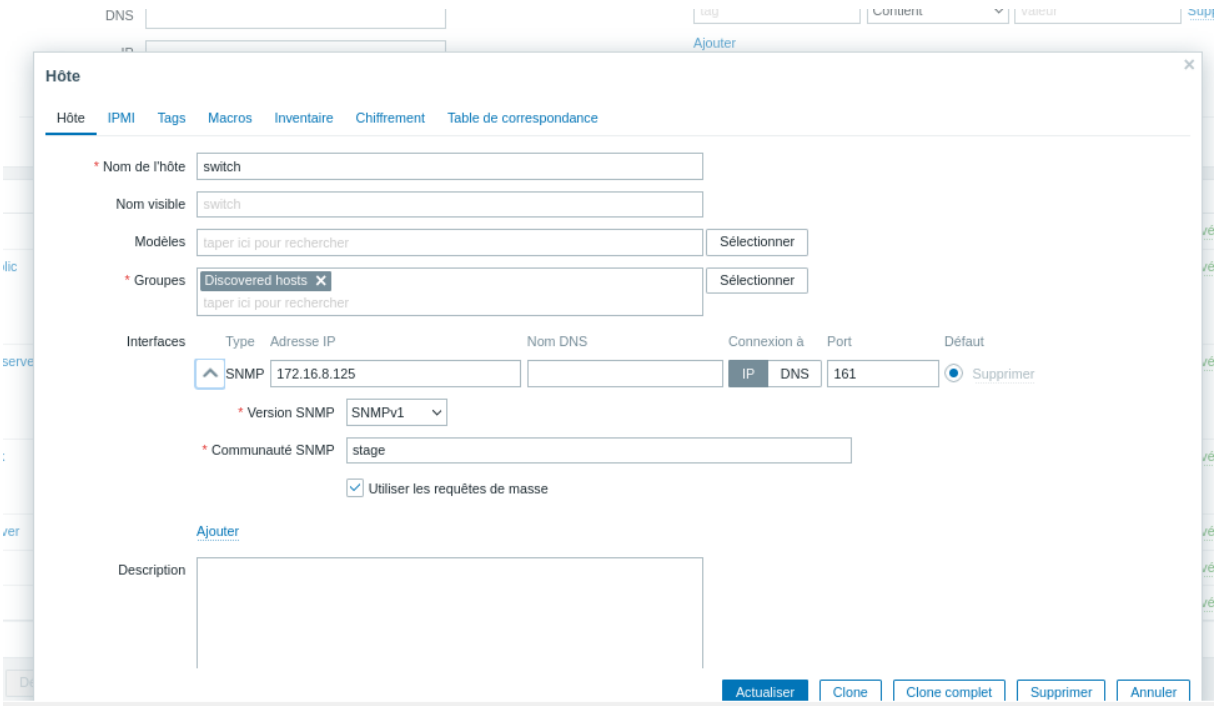


Figure 97: Supervision de switch

- Dans la section "Général", entrez le nom de l'hôte et l'adresse IP du switch Dell.
- Sous la section "Groupes d'hôtes", sélectionnez le groupe auquel vous souhaitez ajouter le switch Dell
- Dans la section "Interfaces", ajoutez une interface en spécifiant le type (Agent Zabbix, SNMP, ou JMX) et les informations d'accès SNMP appropriées (version SNMP, communauté, etc.).
- Dans la section "Applications", sélectionnez les applications SNMP que vous souhaitez superviser pour le switch Dell (par exemple, "Interface network discovery" pour superviser les interfaces réseau).
- Cliquez sur "Ajouter" pour enregistrer les modifications et ajouter le switch Dell en tant qu'hôte dans Zabbix.
- Configurez les éléments et les déclencheurs pour la supervision spécifique du switch Dell. Vous pouvez créer des éléments pour superviser des métriques spécifiques (par exemple, l'utilisation du CPU, l'état des interfaces, la

consommation de la mémoire, etc.) et des déclencheurs pour générer des alertes en cas de dépassement de seuils prédéfinis.

b. Firewall FortiGate 500D :

Configuration de SNMP sur firewall :

Accédez à l'interface d'administration de firewall et activez le support SNMP. Cela peut impliquer la configuration des informations de communauté SNMP (par exemple, la communauté SNMPv2c) et d'autres paramètres liés à SNMP

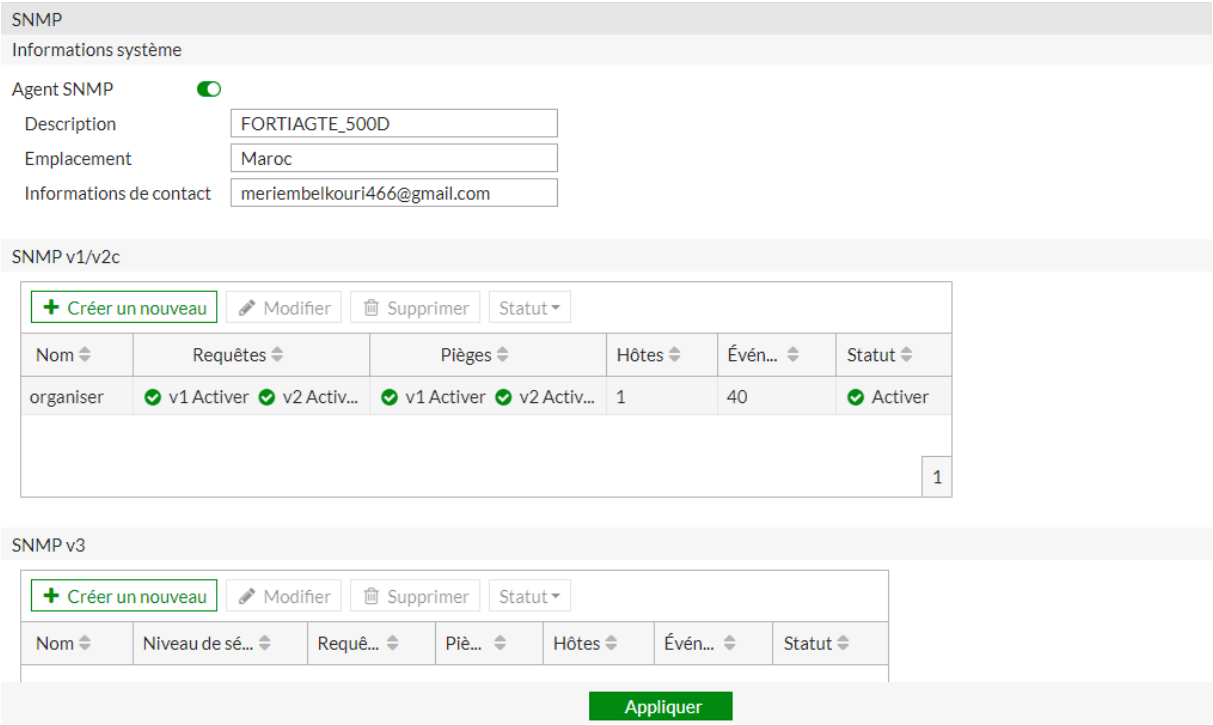


Figure 98: Création de community

Edit SNMP Community

Nom de la communauté organiser

Activé

Hôtes

Adresse IP 172.16.8.134 255.255.255.240

Type d'hôte Accept queries and send traps

Adresse IP

Type d'hôte

Requêtes

v1 activé

Port 161

v2c activé

Port 161

Pièges

v1 activé

D'ACCORD Annuler

Figure 99: Ajout de l'adresse IP de serveur Zabbix

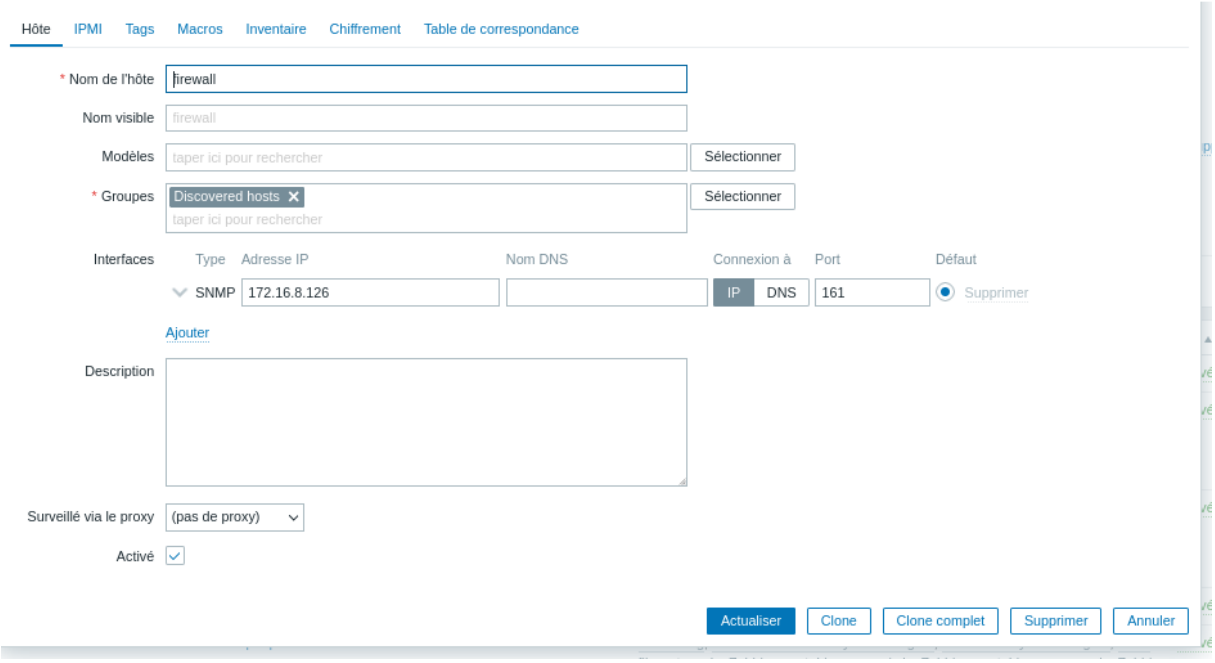


Figure 100:on ajoute le firewall dans le serveur Zabbix et on donne le nom de Community et version de Snmp

c. *Machine Zabbix server:*

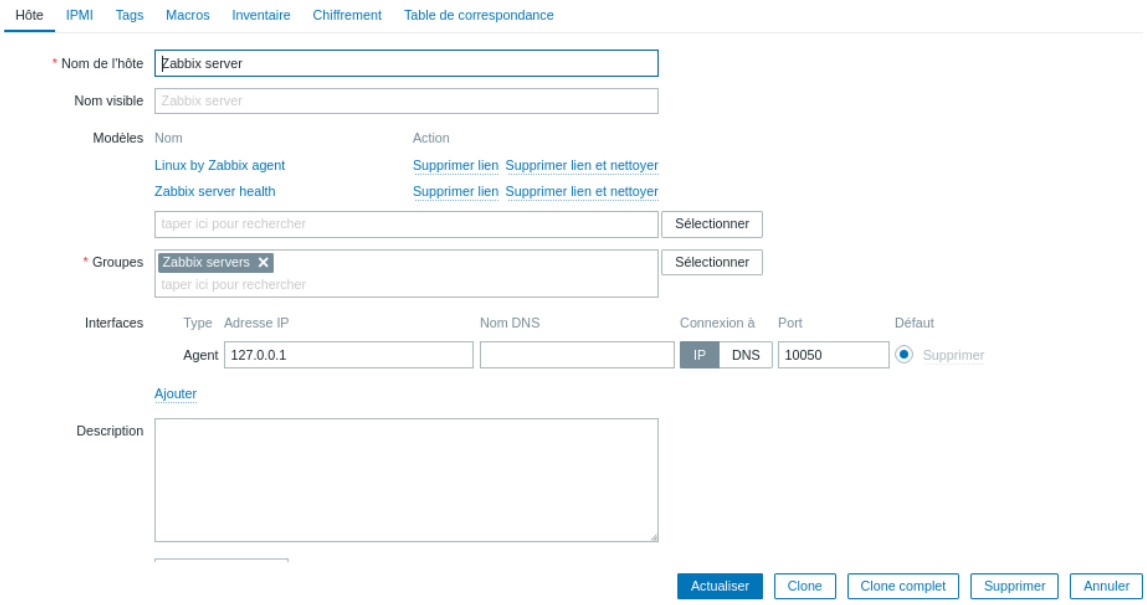


Figure 101: l'hôte Zabbix Server

d. *DMZ public :*

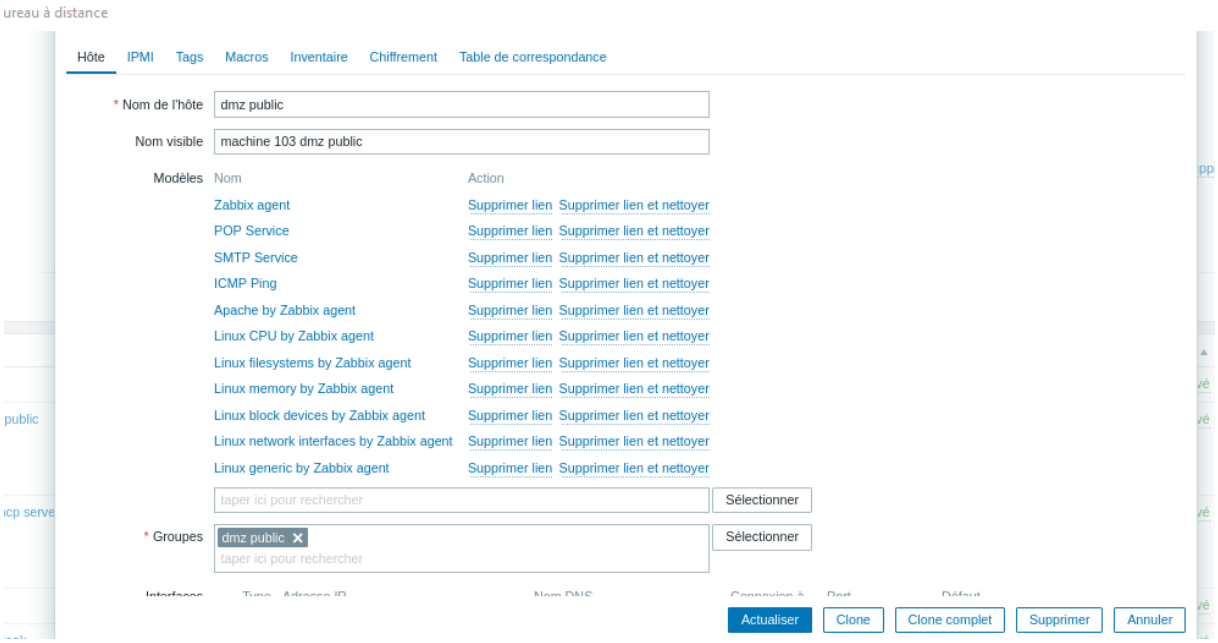


Figure 102: on ajoute la machine Dmz public et on le donne des templates spécifier

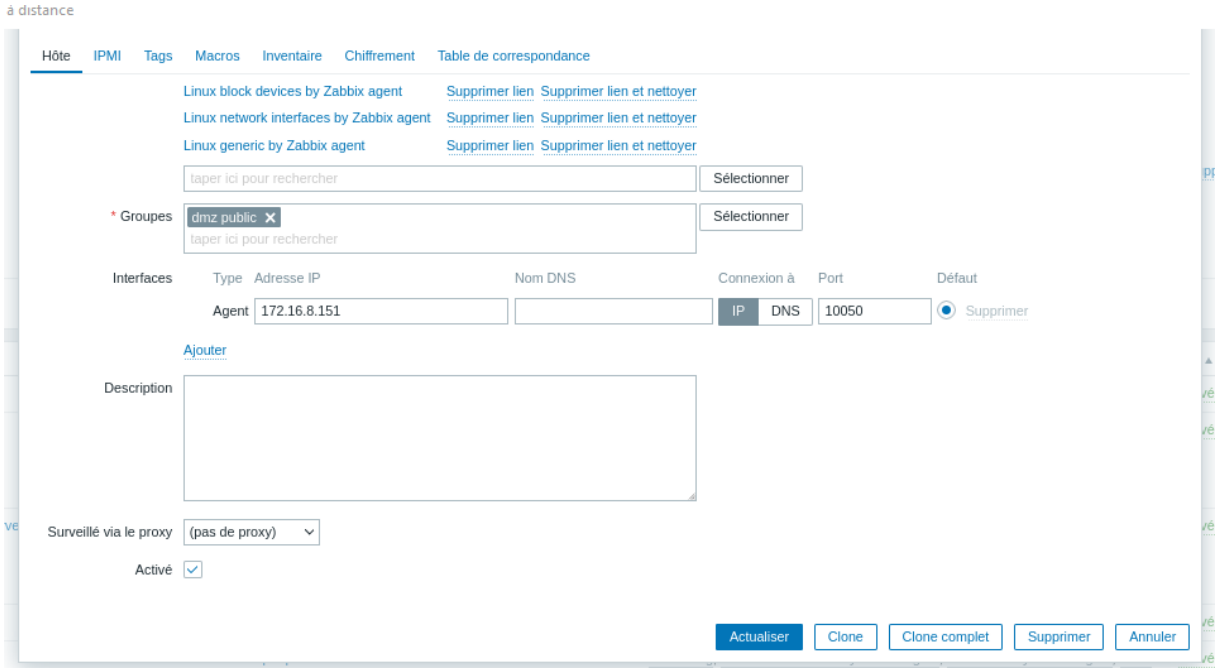


Figure 103: on donne l'adresse IP de l'agent installé dans la machine qu'on souhaite de superviser

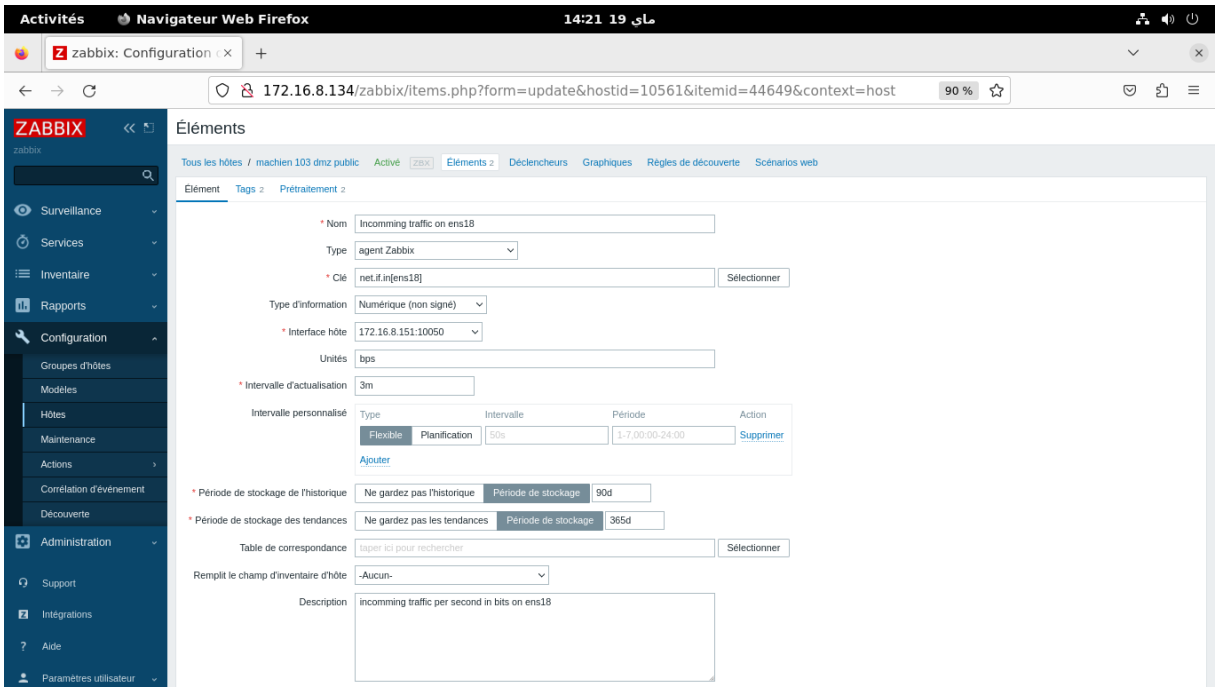


Figure 104: On peut aussi ajouter des items

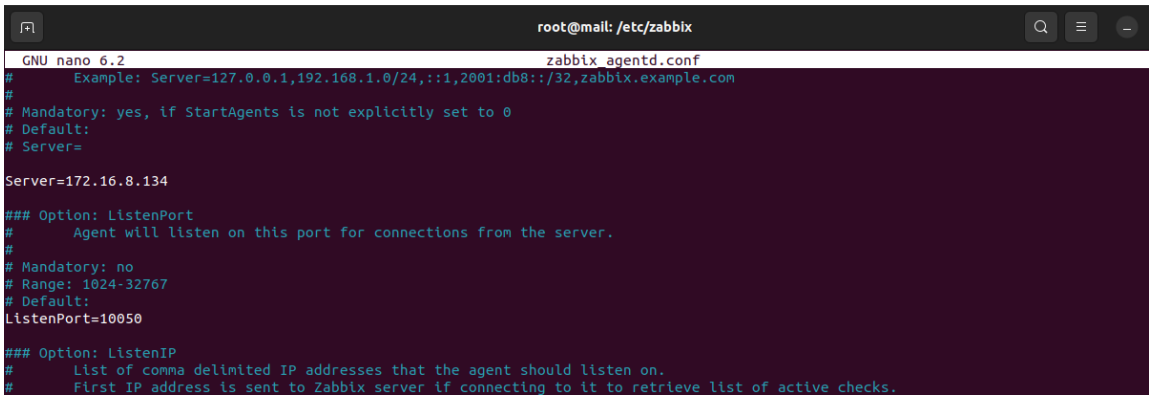


Figure 105: dans la machine Dmz publique on configure l'agent et on ajoute l'adresse de serveur Zabbix et le port d'écoute

```
root@mail: /etc/zabbix
GNU nano 6.2                                    zabbix_agentd.conf
#       IPv6 addresses must be enclosed in square brackets if port for that host is specified.
#       If port is not specified, square brackets for IPv6 addresses are optional.
#       If this parameter is not specified, active checks are disabled.
#       Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=172.16.8.134

### Option: Hostname
#       Unique, case sensitive hostname.
#       Required for active checks and must match hostname as configured on the server.
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
Hostname=dmz public


### Option: HostnameItem
```

Figure 106: Dans les cas où il y a plusieurs serveur Zabbix on spécifier l'adresse de serveur Zabbix et on ajoute le nom de la machine la même qui est dans les serveurs

e. Windows Server:

Ajoute SNMP dans Windows Server:

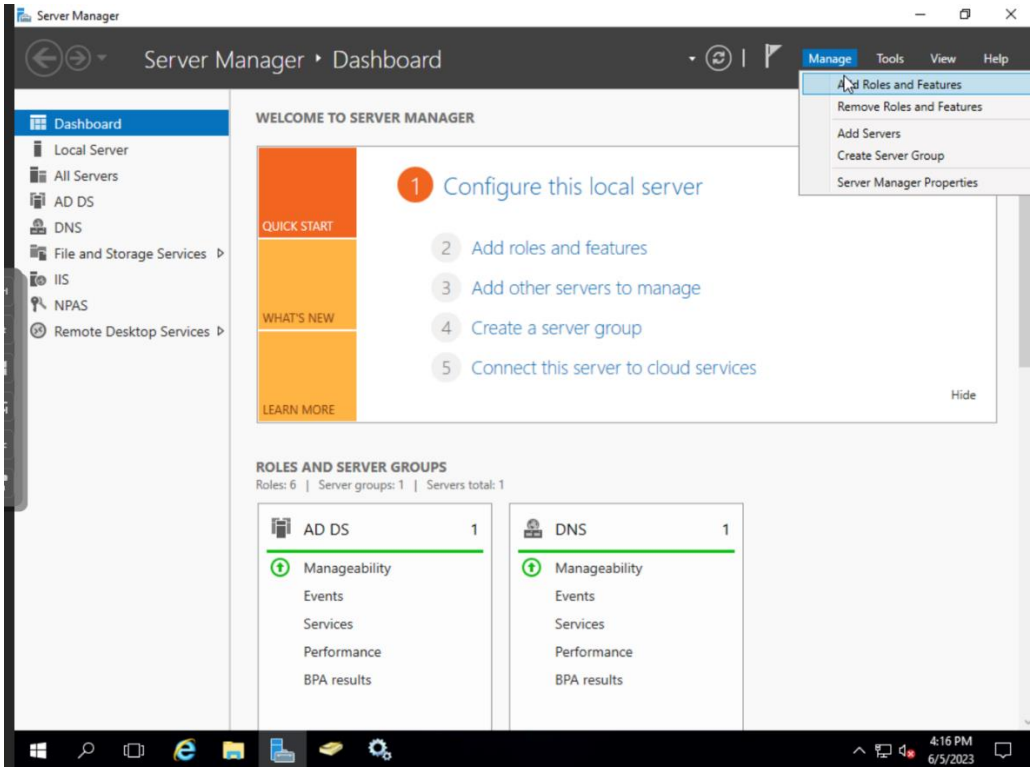
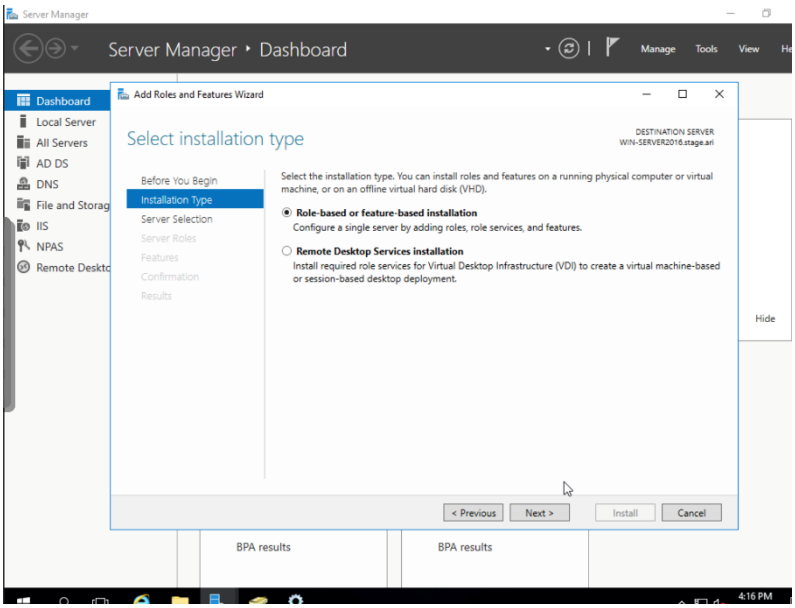
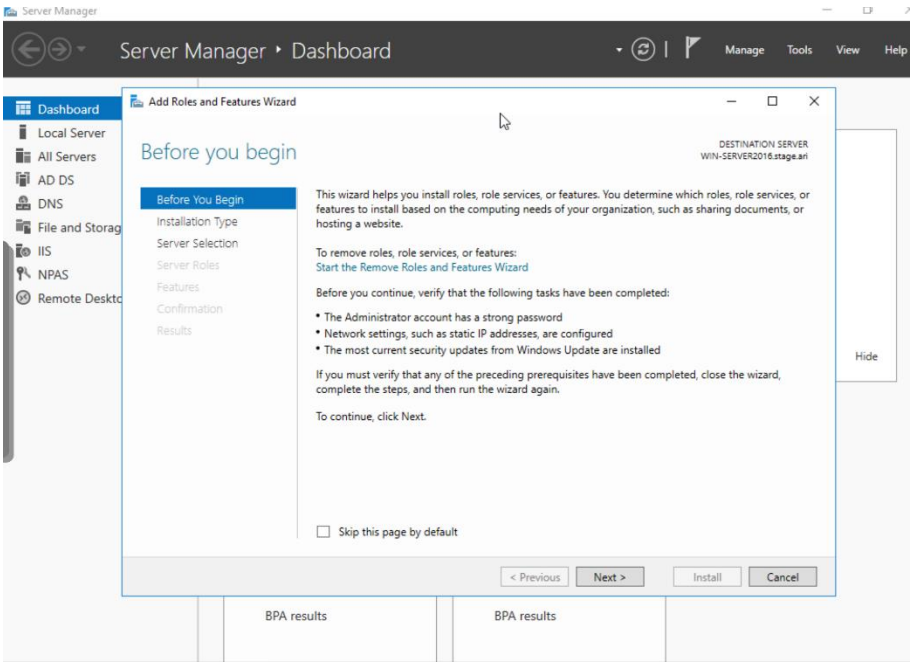


Figure 107:1er étape SNMP windows server


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
IIS
NPAS
Remote Deskto
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-SERVER2016.stage.ari
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
Hide
< Previous
Next >
Install
Cancel
BPA results
BPA results
4:16 PM


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
IIS
NPAS
Remote Deskto
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-SERVER2016.stage.ari
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
The Administrator account has a strong password
Network settings, such as static IP addresses, are configured
The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
Hide
< Previous
Next >
Install
Cancel
BPA results
BPA results

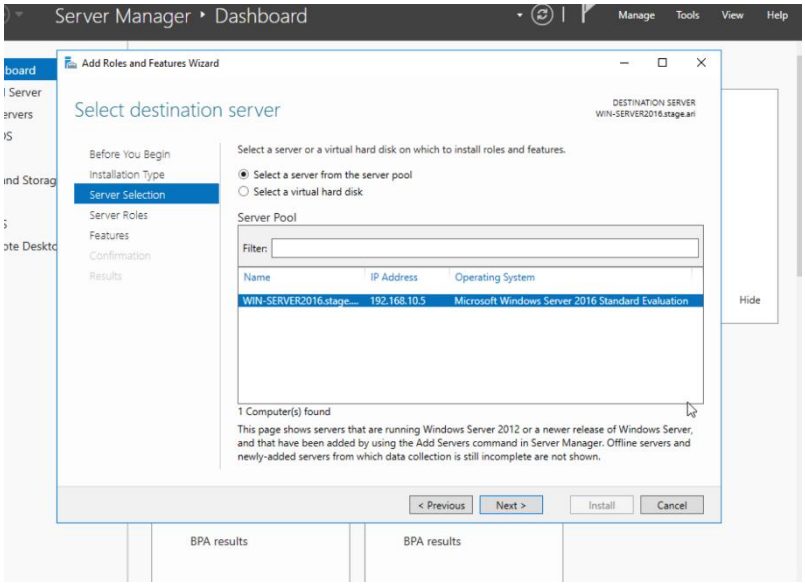
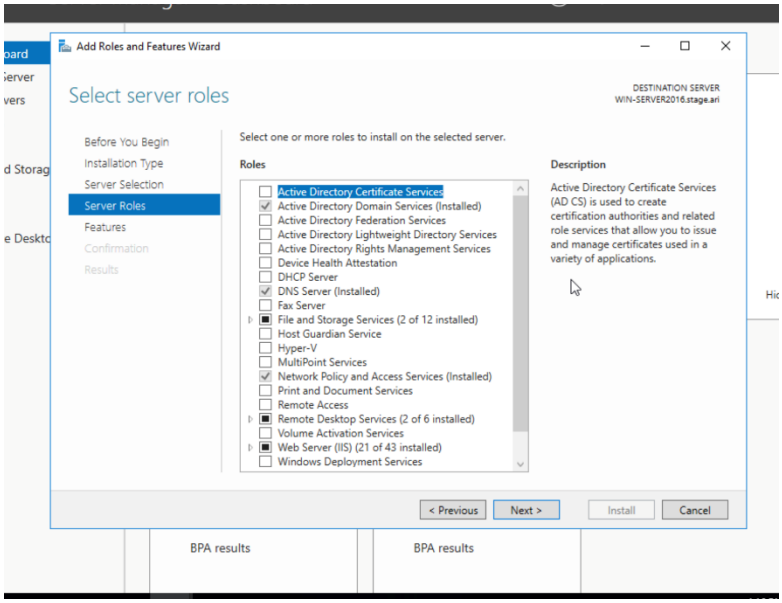
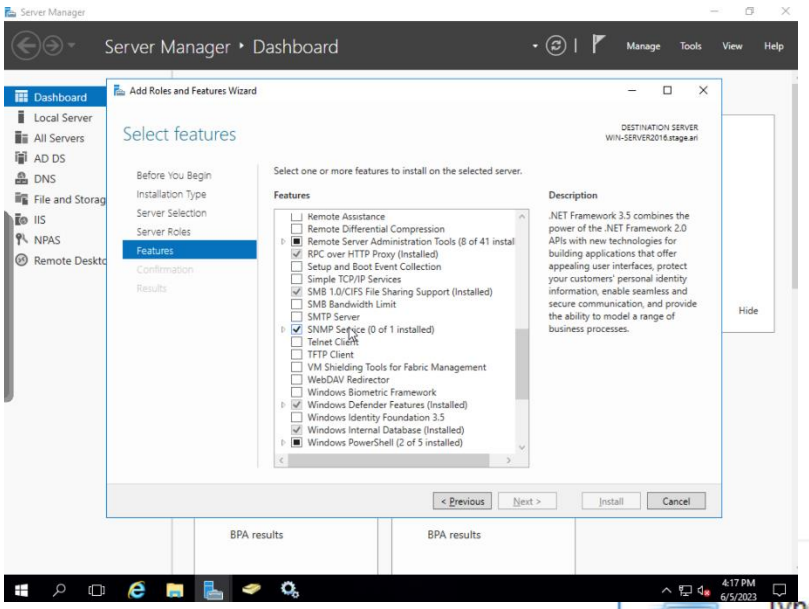


Figure 108: les étapes d'installation de SNMP Windows server





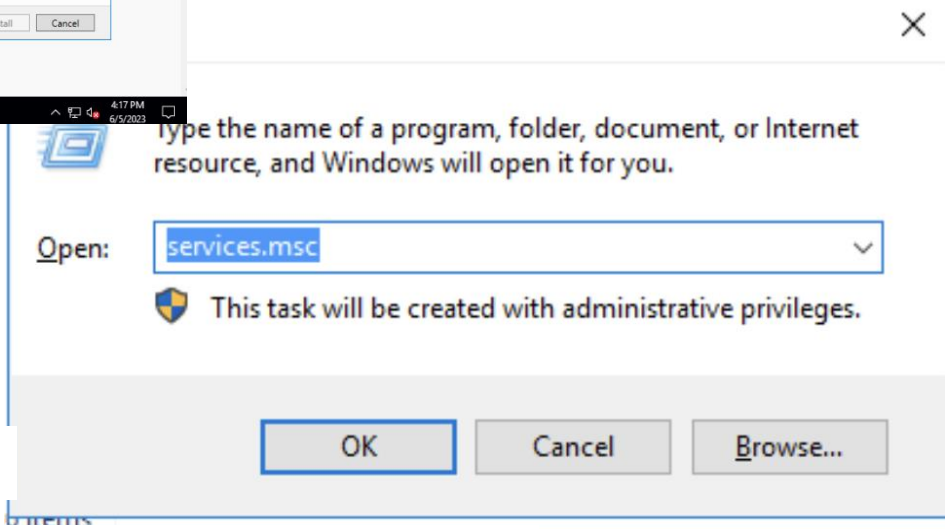
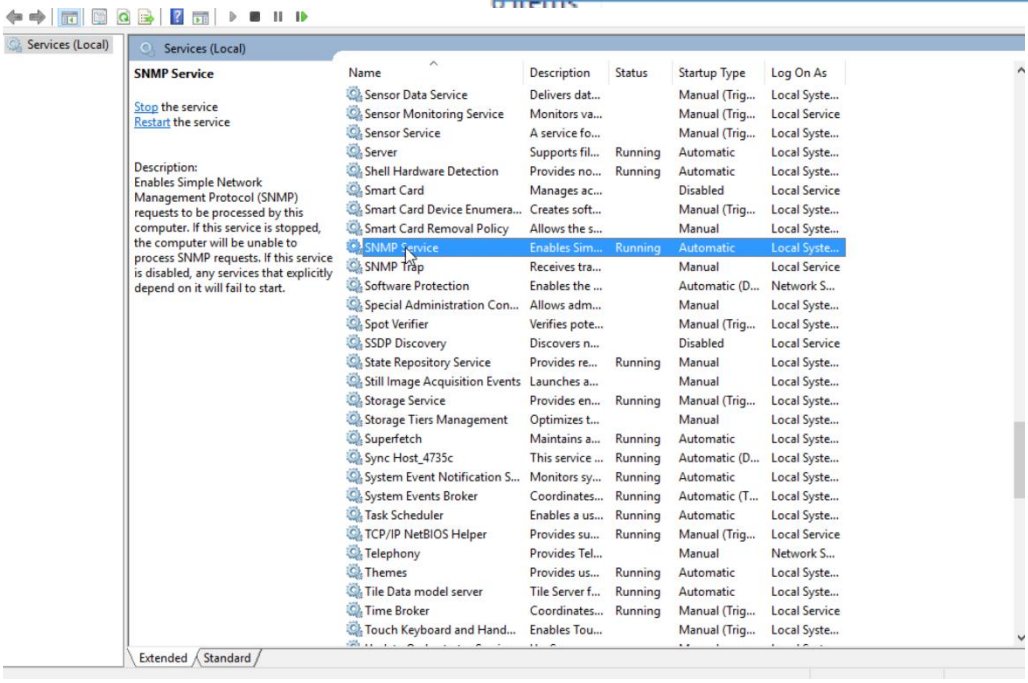
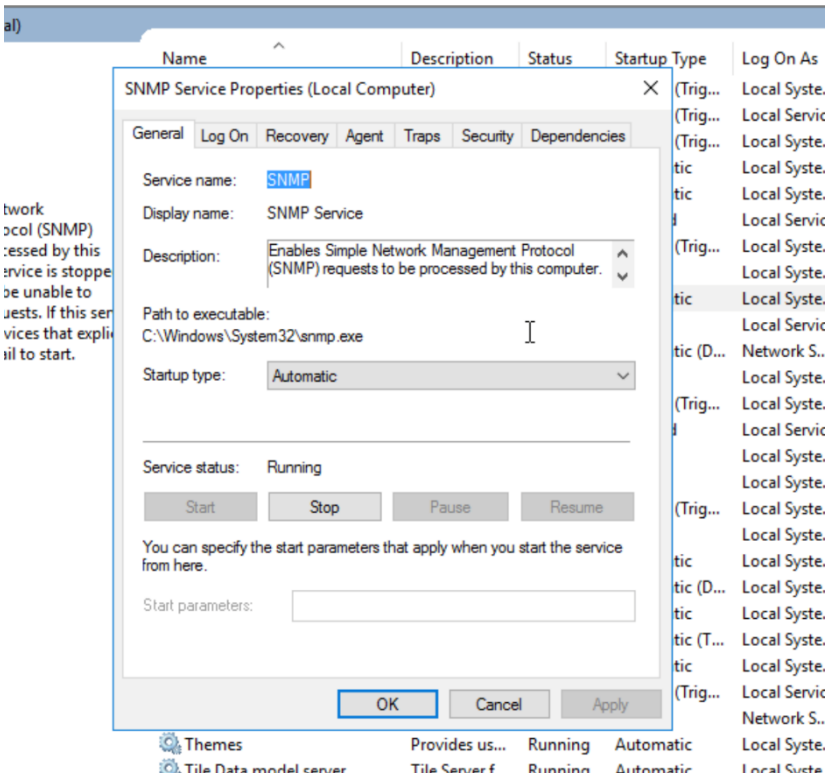
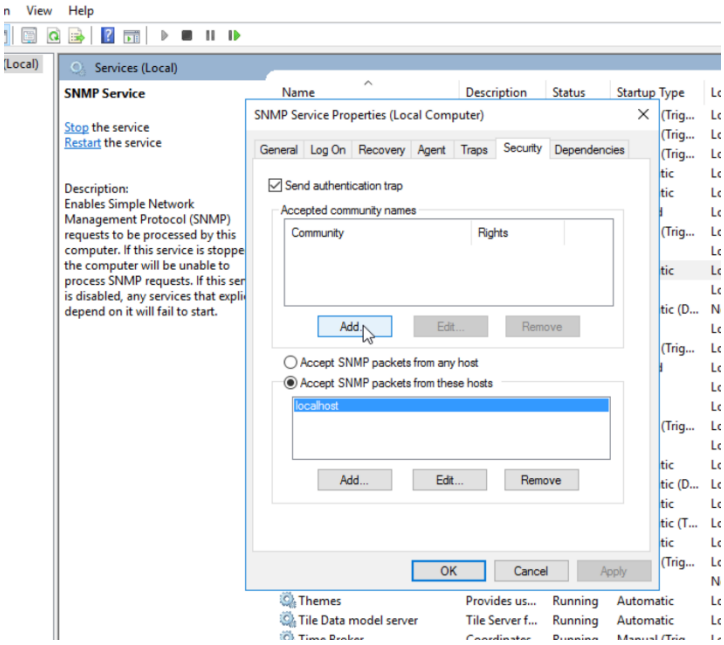
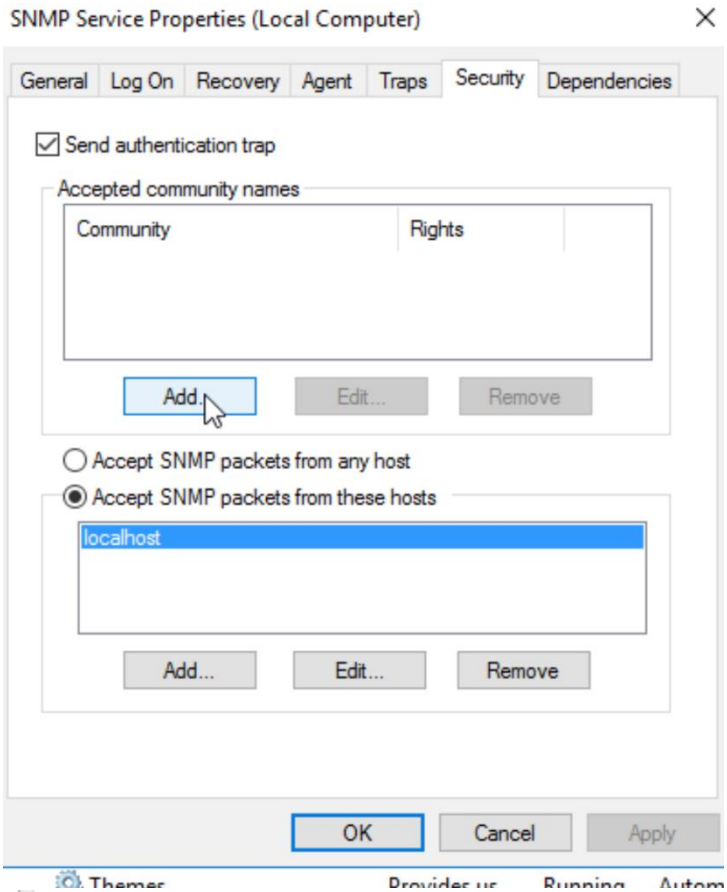


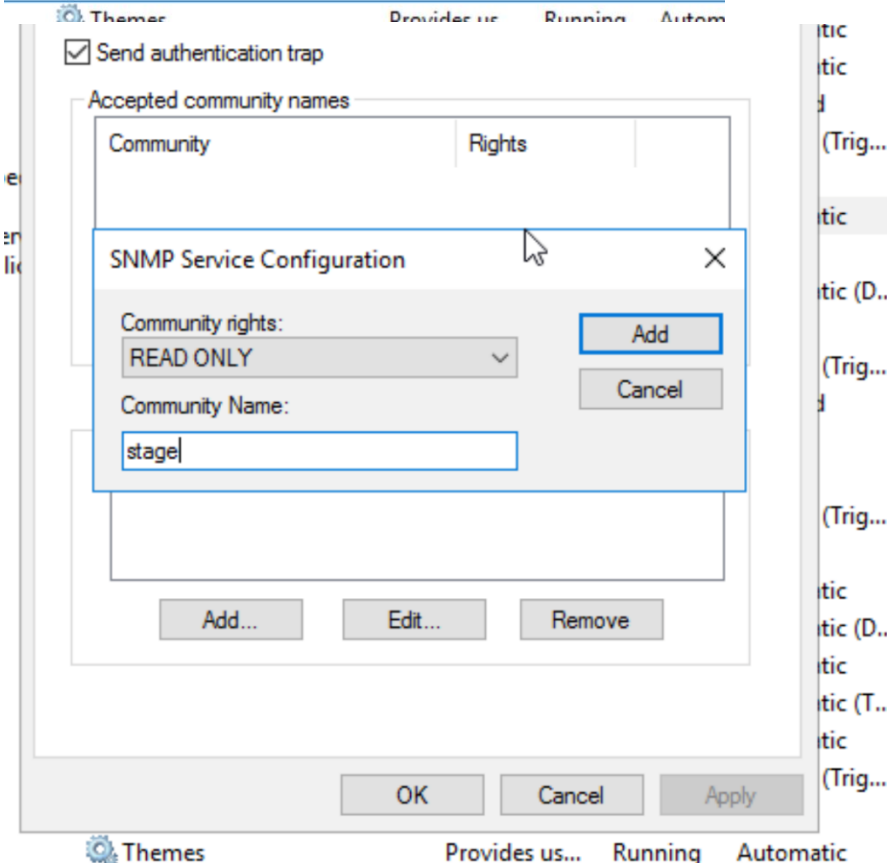
Figure 109: Redémarrage de service SNMP




SNMP Service Properties (Local Computer)
General
Log On
Recovery
Agent
Traps
Security
Dependencies
Service name: SNMP
Display name: SNMP Service
Description: Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.
Path to executable:
C:\Windows\System32\snmp.exe
Startup type: Automatic
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
Name
Description
Status
Startup Type
Log On As
Themes
Provides us...
Running
Automatic


View
Help
Services (Local)
SNMP Service
Stop the service
Restart the service
Description:
Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer. If this service is stoppe the computer will be unable to process SNMP requests. If this ser is disabled, any services that expli depend on it will fail to start.
SNMP Service Properties (Local Computer)
General
Log On
Recovery
Agent
Traps
Security
Dependencies
Send authentication trap
Accepted community names
Community
Rights
Add...
Edit...
Remove
Accept SNMP packets from any host
Accept SNMP packets from these hosts
localhost
OK
Cancel
Apply
Themes
Tile Data model server


SNMP Service Properties (Local Computer)
General
Log On
Recovery
Agent
Traps
Security
Dependencies
Send authentication trap
Accepted community names
Community
Rights
Add...
Edit...
Remove
Accept SNMP packets from any host
Accept SNMP packets from these hosts
localhost
Add...
Edit...
Remove
OK
Cancel
Apply


Send authentication trap
Accepted community names
Community
Rights
SNMP Service Configuration
Community rights:
READ ONLY
Community Name:
stage
Add
Cancel
Add...
Edit...
Remove
OK
Cancel
Apply
Themes
Provides us...
Running
Automatic

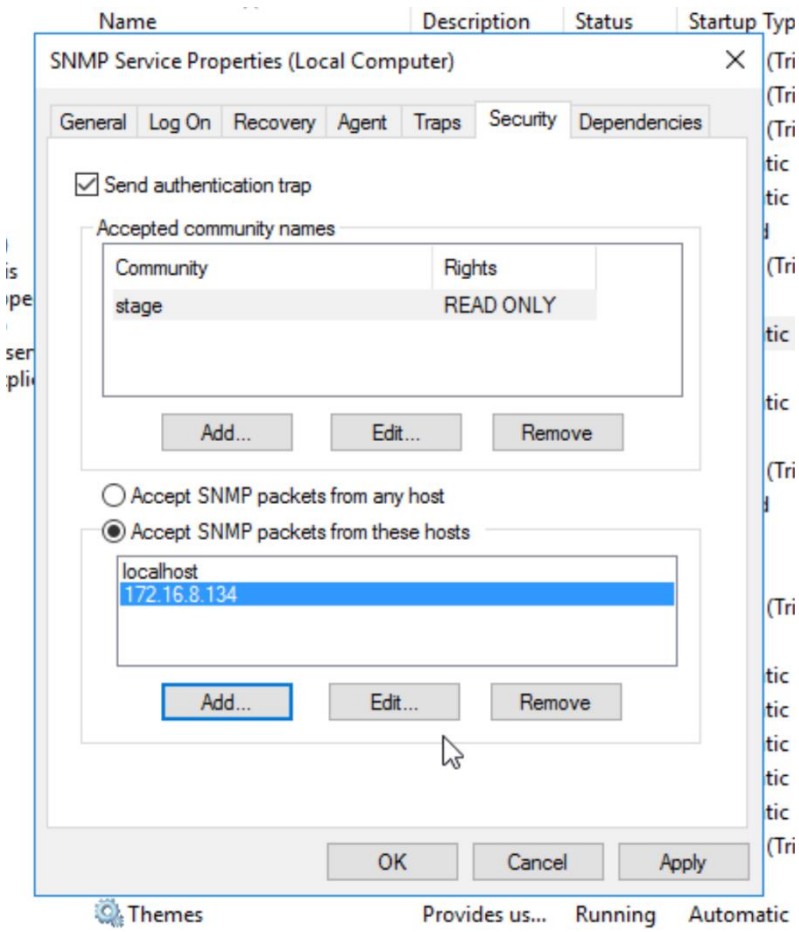


Figure 110: Ajoute Community Name et Adresse IP de serveur Zabbix

- Dans la fenêtre "Services SNMP", accédez à l'onglet "Sécurité"
- Dans la section "Accepter les messages SNMP de ces hôtes", cliquez sur le bouton "Ajouter".
- Sélectionnez les options de sécurité appropriées pour l'accès SNMP. Vous pouvez définir une chaîne communautaire SNMP (par exemple, "Stage" et spécifier les autorisations de lecture/écriture en fonction de vos besoins.
- Cliquez sur "Ajouter" puis sur "OK" pour enregistrer les modifications. Redémarrez le service SNMP en cliquant avec le bouton droit sur "Service SNMP"

dans la fenêtre "Services SNMP" et en sélectionnant "Redémarrer" dans le menu contextuel.

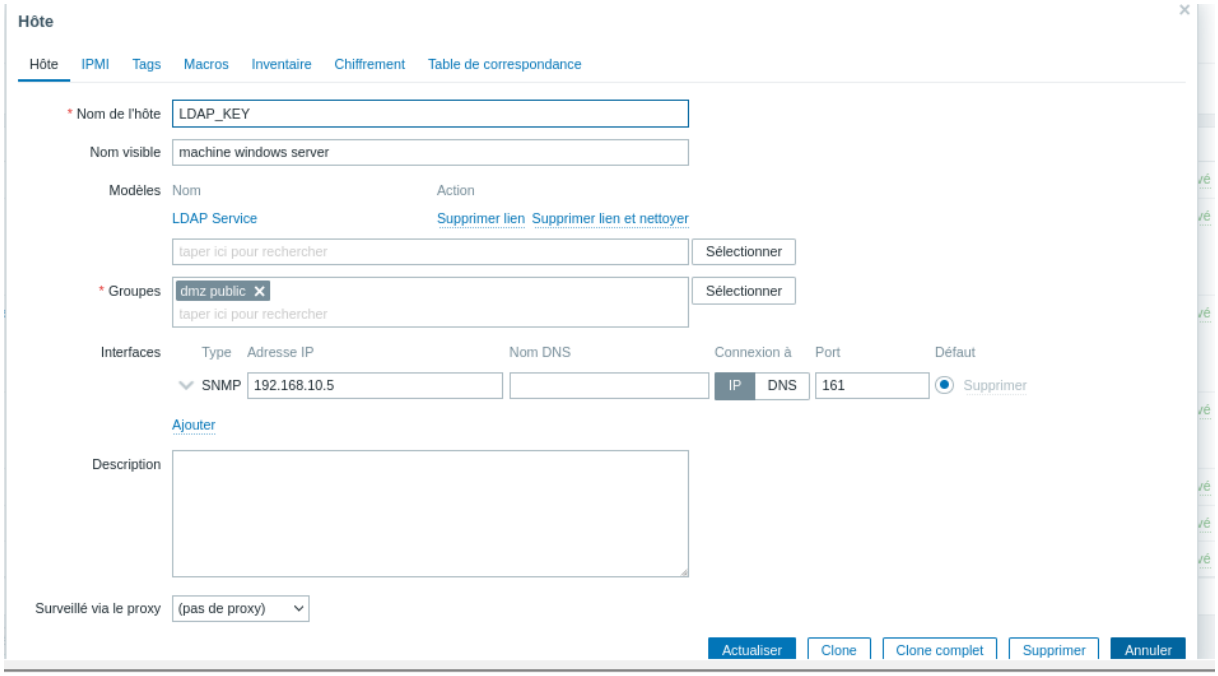


Figure 111: Ajout de la machine Windows Server dans Zabbix

f. Machine Ubuntu Server qui contient RADIUS et DHCP :

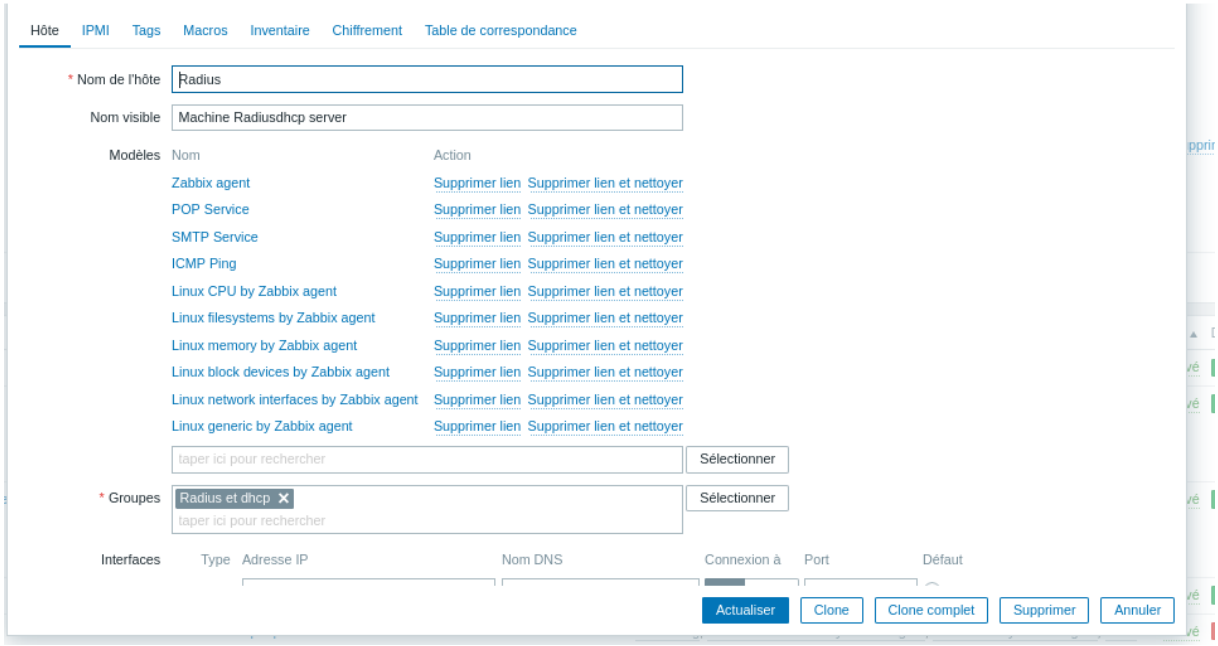


Figure 112: Ajoute l'hôte et les templates

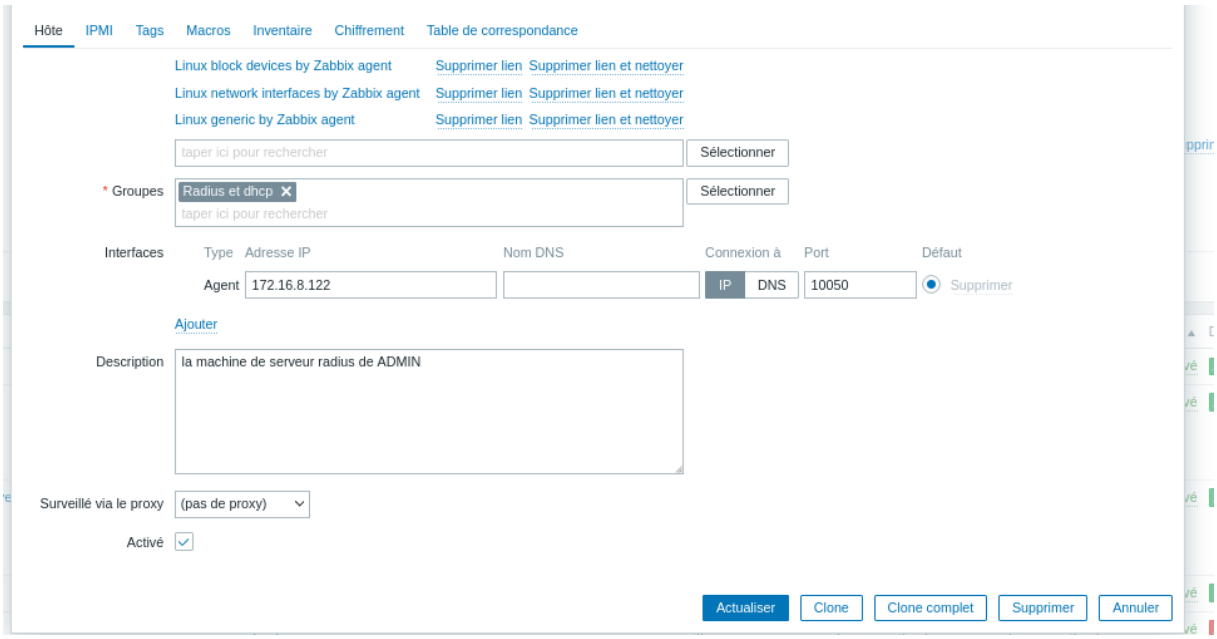


Figure 113: on ajoute l'adresse IP de l'agent

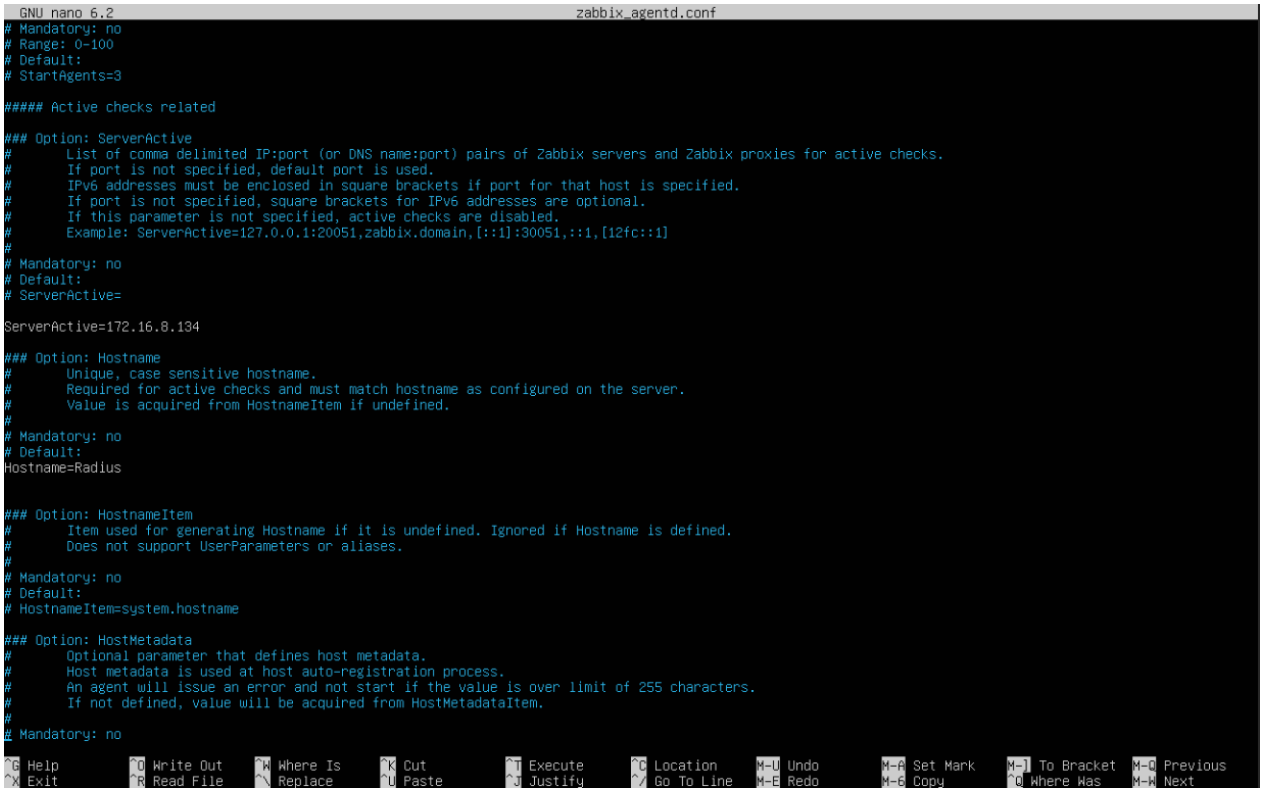


Figure 114: on configure l'agent

g. Dashboard et Surveillance:

Vous pourrez voir les problèmes non résolus affichés dans le widget correspondant. Les problèmes seront filtrés en fonction des critères que vous avez spécifiés. Vous pouvez également personnaliser davantage votre tableau de bord en ajoutant d'autres widgets pour afficher différentes informations de surveillance.

Vous pouvez accéder à vos tableaux de bord depuis le menu principal de Zabbix et les consulter régulièrement pour surveiller l'état de votre infrastructure et des problèmes éventuels.

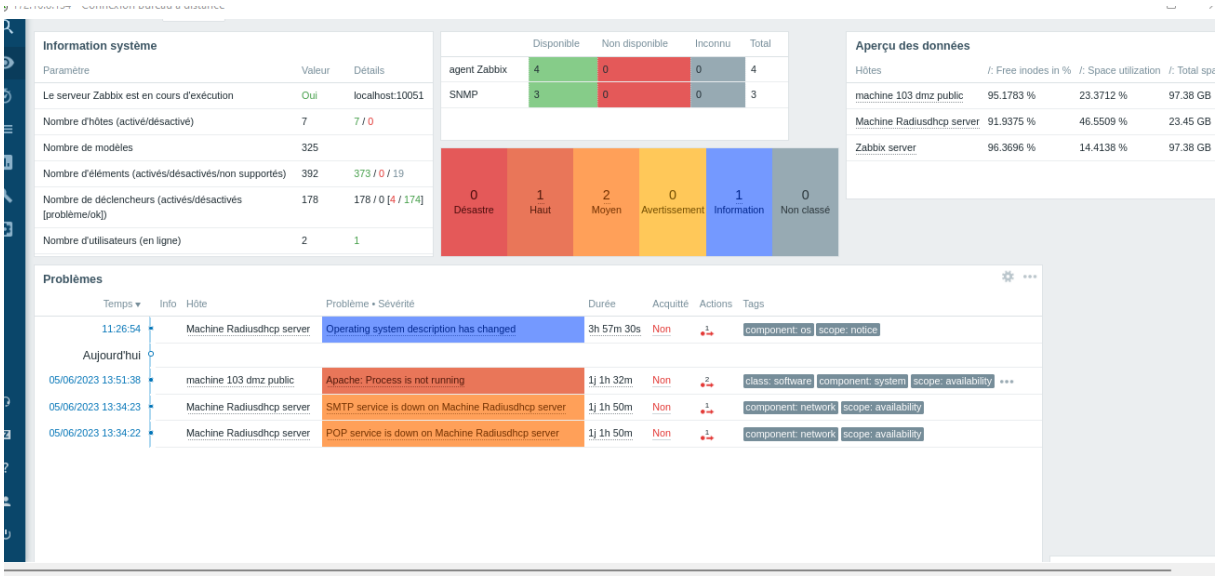
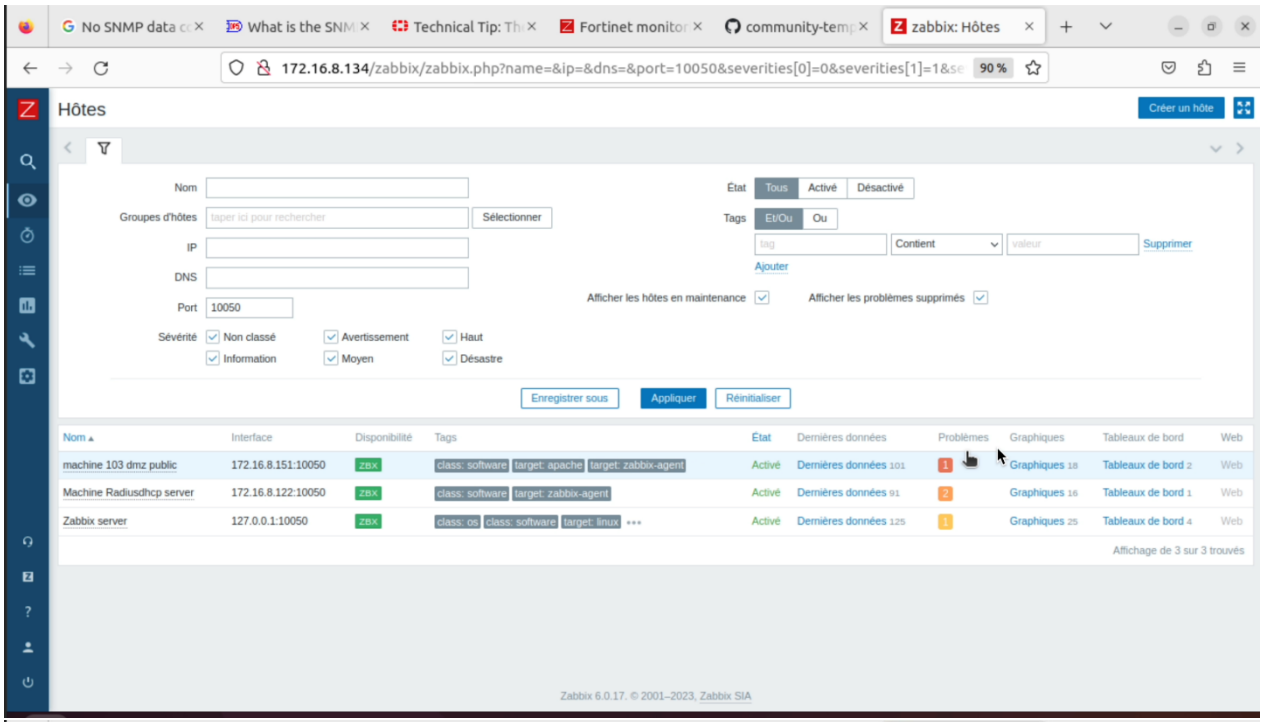
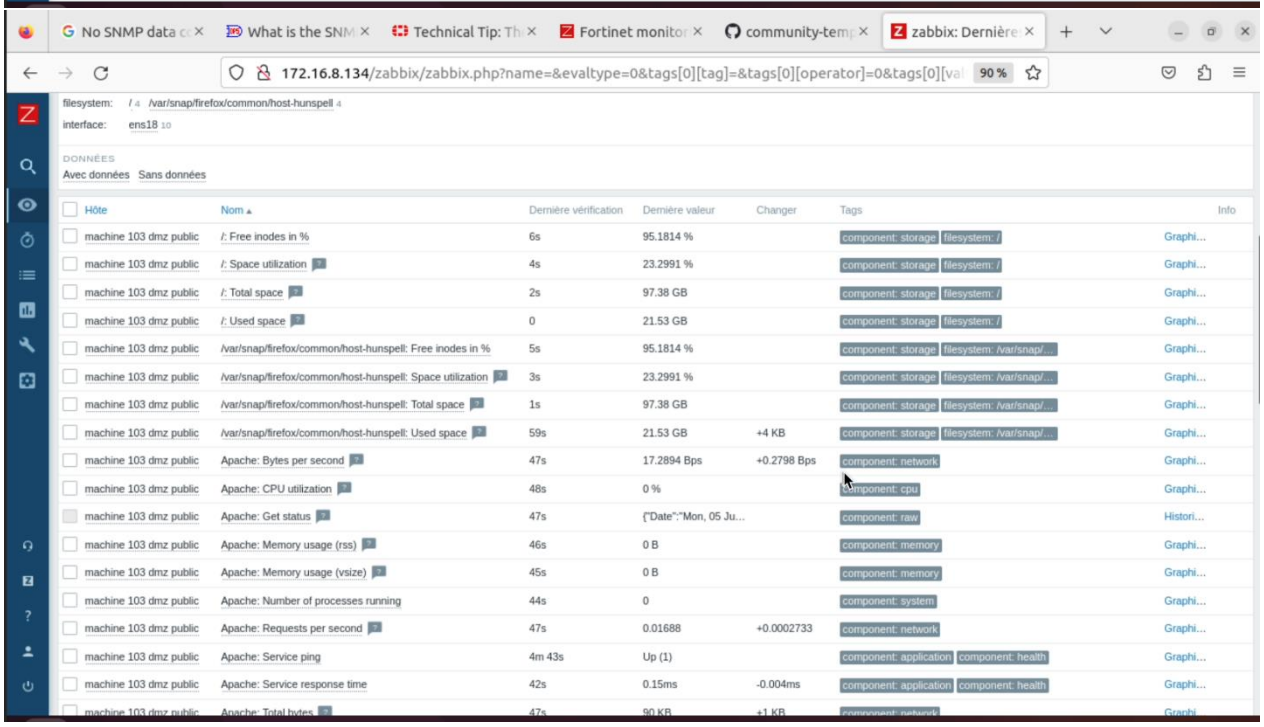


Figure 115:Dashboard


No SNMP data c
What is the SNM
Technical Tip: Th
Fortinet monitor
community-temp
zabbix: Hôtes
172.16.8.134/zabbix/zabbix.php?name=&ip=&dns=&port=10050&severities[0]=0&severities[1]=1&se
90 %
Hôtes
Créer un hôte
Nom
Groupes d'hôtes
taper ici pour rechercher
Sélectionner
IP
DNS
Port
10050
Sévérité
Non classé
Information
Avertissement
Moyen
Haut
Désastre
État
Tous
Activé
Désactivé
Tags
Et/Ou
Ou
tag
Contient
valeur
Supprimer
Ajouter
Afficher les hôtes en maintenance
Afficher les problèmes supprimés
Enregistrer sous
Appliquer
Réinitialiser
Nom
Interface
Disponibilité
Tags
État
Dernières données
Problèmes
Graphiques
Tableaux de bord
Web
machine 103 dmz public
172.16.8.151:10050
ZBX
class: software
target: apache
target: zabbix-agent
Activé
Dernières données 101
1
Graphiques 18
Tableaux de bord 2
Web
Machine Radiusdhcp server
172.16.8.122:10050
ZBX
class: software
target: zabbix-agent
Activé
Dernières données 91
2
Graphiques 16
Tableaux de bord 1
Web
Zabbix server
127.0.0.1:10050
ZBX
class: os
class: software
target: linux
Activé
Dernières données 125
1
Graphiques 25
Tableaux de bord 4
Web
Affichage de 3 sur 3 trouvés
Zabbix 6.0.17. © 2001–2023, Zabbix SIA


No SNMP data c
What is the SNM
Technical Tip: Th
Fortinet monitor
community-temp
zabbix: Dernière
172.16.8.134/zabbix/zabbix.php?name=&evaltype=0&tags[0][tag]=&tags[0][operator]=0&tags[0][val
90 %
filesystem: / 4 /var/snap/firefox/common/host-hunspell 4
interface: ens18 10
DONNÉES
Avec données
Sans données
Hôte
Nom
Dernière vérification
Dernière valeur
Changer
Tags
Info
machine 103 dmz public
/: Free inodes in %
6s
95.1814 %
component: storage
filesystem: /
Graphi...
machine 103 dmz public
/: Space utilization
4s
23.2991 %
component: storage
filesystem: /
Graphi...
machine 103 dmz public
/: Total space
2s
97.38 GB
component: storage
filesystem: /
Graphi...
machine 103 dmz public
/: Used space
0
21.53 GB
component: storage
filesystem: /
Graphi...
machine 103 dmz public
/var/snap/firefox/common/host-hunspell: Free inodes in %
5s
95.1814 %
component: storage
filesystem: /var/snap/...
Graphi...
machine 103 dmz public
/var/snap/firefox/common/host-hunspell: Space utilization
3s
23.2991 %
component: storage
filesystem: /var/snap/...
Graphi...
machine 103 dmz public
/var/snap/firefox/common/host-hunspell: Total space
1s
97.38 GB
component: storage
filesystem: /var/snap/...
Graphi...
machine 103 dmz public
/var/snap/firefox/common/host-hunspell: Used space
59s
21.53 GB
+4 KB
component: storage
filesystem: /var/snap/...
Graphi...
machine 103 dmz public
Apache: Bytes per second
47s
17.2894 Bps
+0.2798 Bps
component: network
Graphi...
machine 103 dmz public
Apache: CPU utilization
48s
0 %
component: cpu
Graphi...
machine 103 dmz public
Apache: Get status
47s
{"Date":"Mon, 05 Ju...
component: raw
Histori...
machine 103 dmz public
Apache: Memory usage (rss)
46s
0 B
component: memory
Graphi...
machine 103 dmz public
Apache: Memory usage (vsize)
45s
0 B
component: memory
Graphi...
machine 103 dmz public
Apache: Number of processes running
44s
0
component: system
Graphi...
machine 103 dmz public
Apache: Requests per second
47s
0.01688
+0.0002733
component: network
Graphi...
machine 103 dmz public
Apache: Service ping
4m 43s
Up (1)
component: application
component: health
Graphi...
machine 103 dmz public
Apache: Service response time
42s
0.15ms
-0.004ms
component: application
component: health
Graphi...
machine 103 dmz public
Apache: Total bytes
47s
90 KB
+1 KB
component: network
Graphi...

h. Les hôtes:

Dans la barre de navigation horizontale supérieure, cliquez sur "Hôtes" pour afficher la liste des hôtes surveillés.

Par défaut, vous verrez la liste de tous les hôtes enregistrés dans Zabbix, qu'ils soient actifs ou non.

Pour afficher uniquement les hôtes actifs, vous pouvez utiliser le filtre "Disponibilité". Cliquez sur la flèche déroulante à côté du filtre "Disponibilité" et sélectionnez "Actif".

La liste des hôtes sera mise à jour pour n'afficher que les hôtes actifs

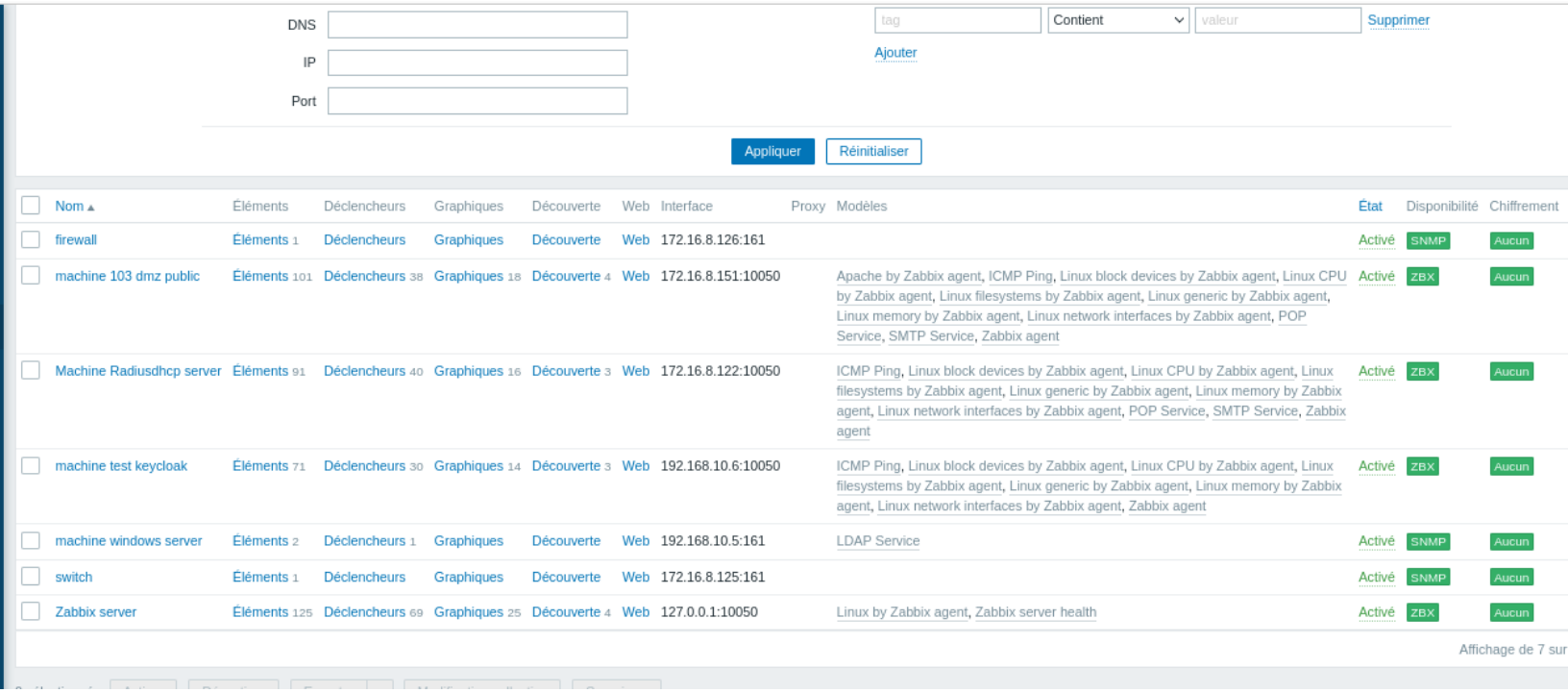


Figure 116: l'état des hôtes

Chapitre 3 : Application Web avec Laravel

I. Problématique :

Au cours de notre stage, l'une des tâches principales que nous avons réalisées était le développement d'une application web avec Laravel pour la gestion des stagiaires à l'ENSSUP. Cette application était conçue pour faciliter le processus de suivi et de gestion des stagiaires, en automatisant de nombreuses tâches manuelles et en améliorant la communication entre les différents acteurs impliqués.

Nous avons commencé par analyser les besoins et les exigences spécifiques de l'ENSSUP en termes de gestion des stagiaires. Ensuite, nous avons utilisé le Framework Laravel pour concevoir et développer une application web sur mesure répondant à ces besoins. L'application permettait aux responsables administratifs de saisir et de gérer les informations relatives aux stagiaires.

II. Codes :

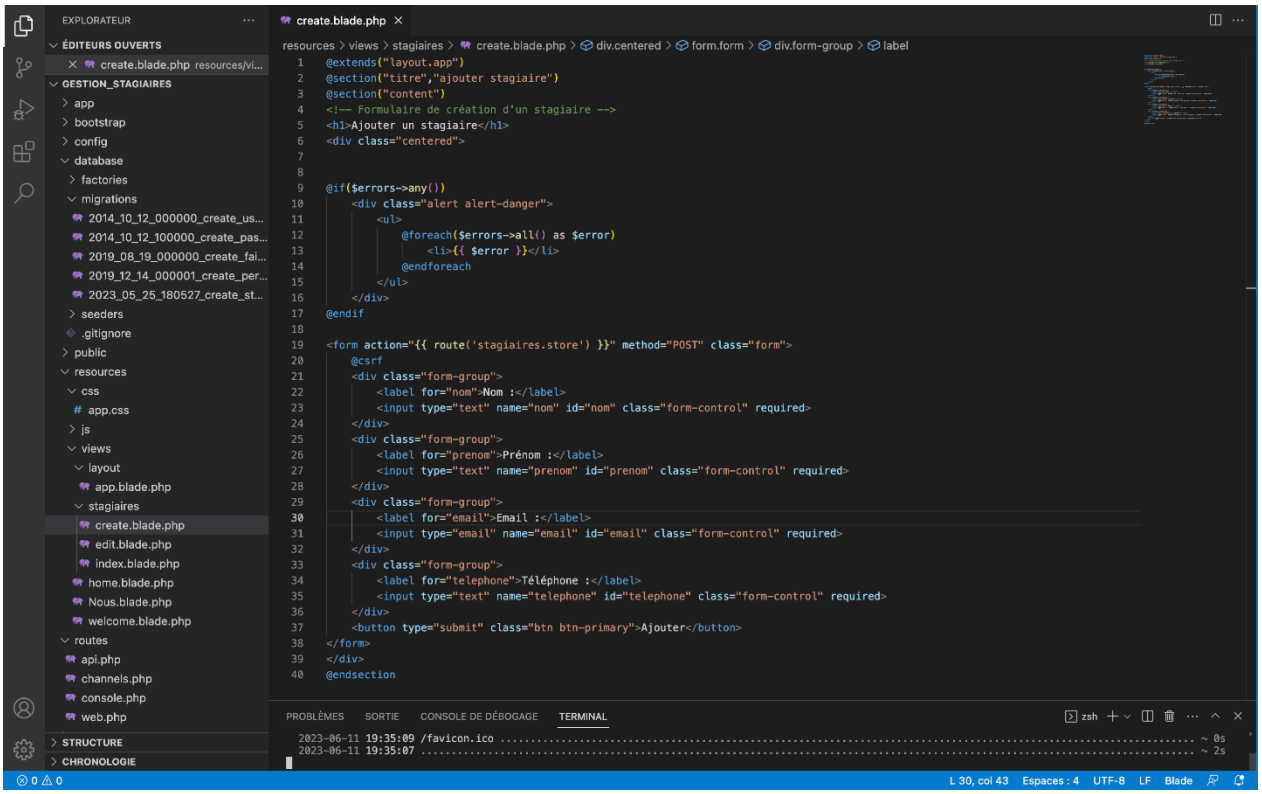


Figure 117:fichier de formulaire pour ajouter un

```
@extends("layout.app")
@section("titre","modifier un stagiaire")
@section("content")
<!-- Formulaire de modification d'un stagiaire -->
<h1>Modifier un stagiaire</h1>
<div class="centered">


    @if($errors->any())
        <div class="alert alert-danger">
            <ul>
                @foreach($errors->all() as $error)
                    <li>{{ $error }}</li>
                @endforeach
            </ul>
        </div>
    @endif
    <form action="{{ route('stagiaires.update', $stagiaire->id) }}" method="POST" class="form">
        @csrf
        @method('PUT')

        <div class="form-group">
            <label for="nom">Nom :</label>
            <input type="text" id="nom" name="nom" value="{{ $stagiaire->nom }}" required>
        </div>

        <div class="form-group">
            <label for="email">Email :</label>
            <input type="email" id="email" name="email" value="{{ $stagiaire->email }}" required>
        </div>
        <button type="submit">Modifier</button>
    </form>
</div>
    @endsection
```

Figure 118: modifier un stagiaire

```
@extends("layout.app")
@section("titre","liste stagiaires")
@section("content")
<!-- Affichage de la liste des stagiaires -->
<h1>Liste des stagiaires</h1>
<div class="centered">


@if(session('success'))
    <div class="alert alert-success">
        {{ session('success') }}
    </div>
@endif



<table class="table">
    <thead>
        <tr>
            <th>Nom</th>
            <th>Prénom</th>
            <th>Email</th>
            <th>Téléphone</th>
            <th>Actions</th>
        </tr>
    </thead>
    <tbody>
        @foreach($stagiaires as $stagiaire)
        <tr>
            <td>{{ $stagiaire->nom }}</td>
            <td>{{ $stagiaire->prenom }}</td>
            <td>{{ $stagiaire->email }}</td>
            <td>{{ $stagiaire->telephone }}</td>
            <td>
                <a href="{{ route('stagiaires.edit', $stagiaire) }}" class="btn btn-primary">Modifier</a>
                <form action="{{ route('stagiaires.destroy', $stagiaire) }}" method="POST" style="display: inline-block;">
                    @csrf
                    @method('DELETE')
                    <button type="submit" class="btn btn-danger" onclick="return confirm('Êtes-vous sûr de vouloir supprimer ce stagiaire ?')">Supprimer</button>
            </td>
        </tr>
        @endforeach
    </tbody>
</table>
</div>
<a href="{{ route('stagiaires.create') }}" class="btn btn-primary">Ajouter un stagiaire</a>
@endsection
```

Figure 119:liste des stagiaires

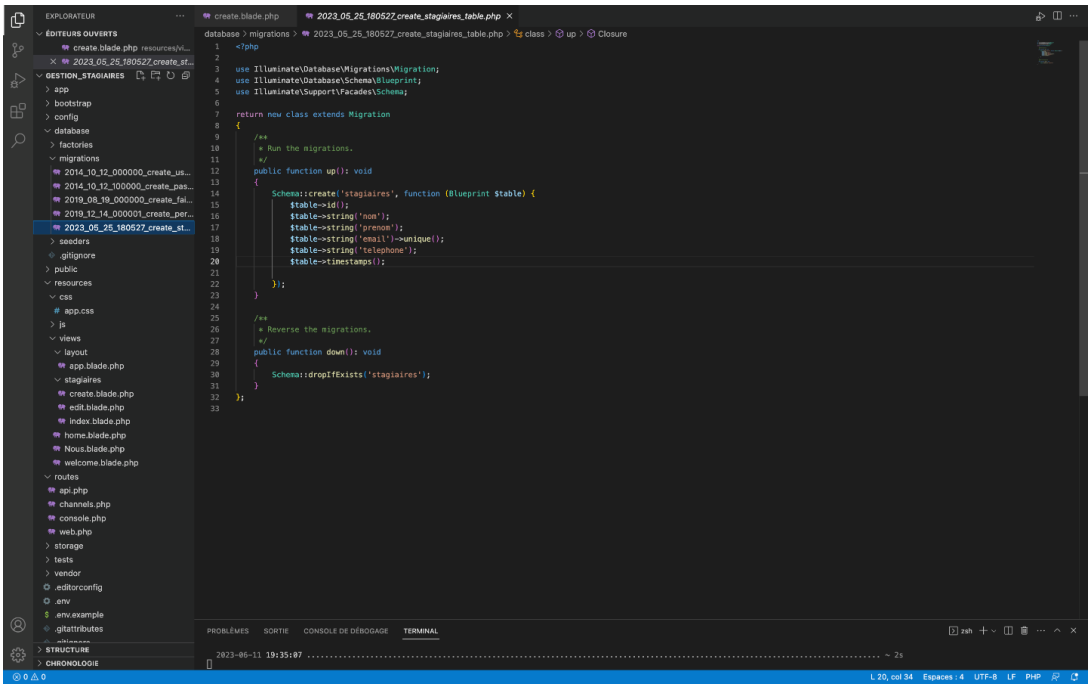


Figure 120: fichier de migration

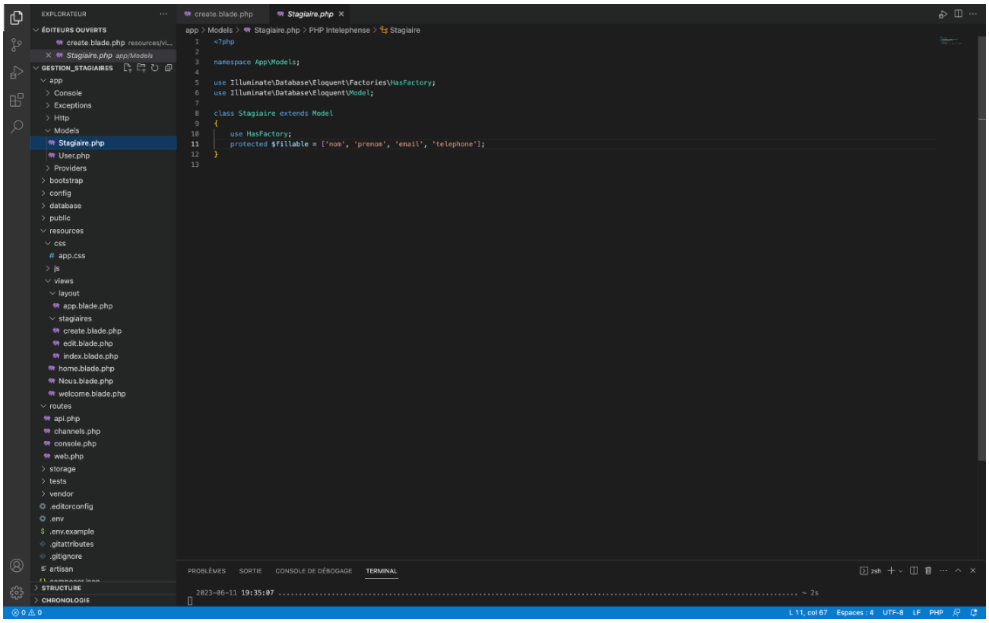


Figure 121:Model Stagiaire

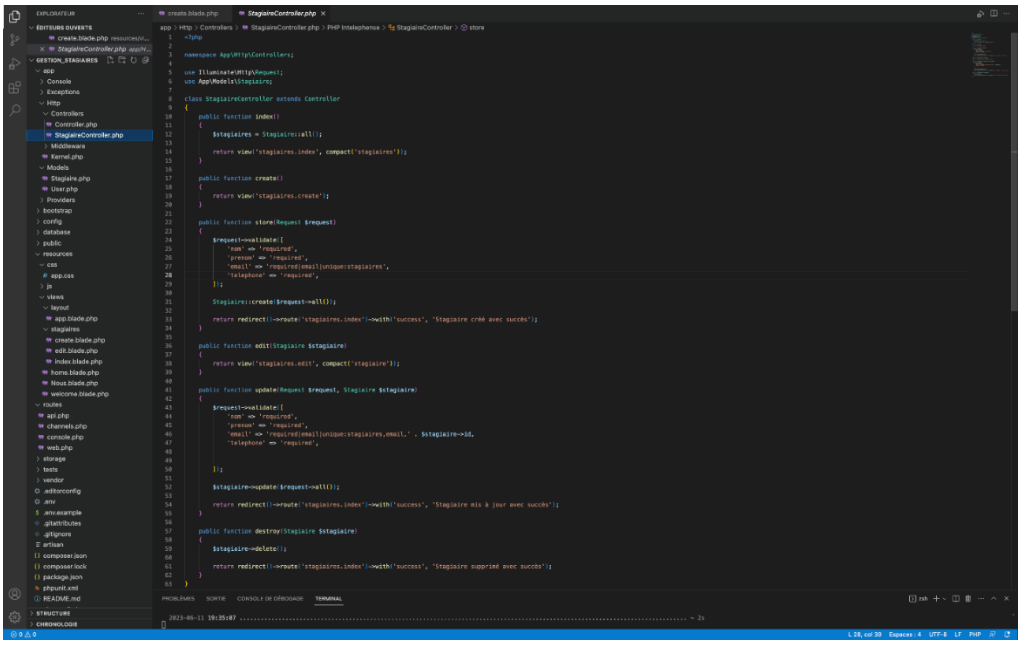


Figure 122: Stagiaire Controller

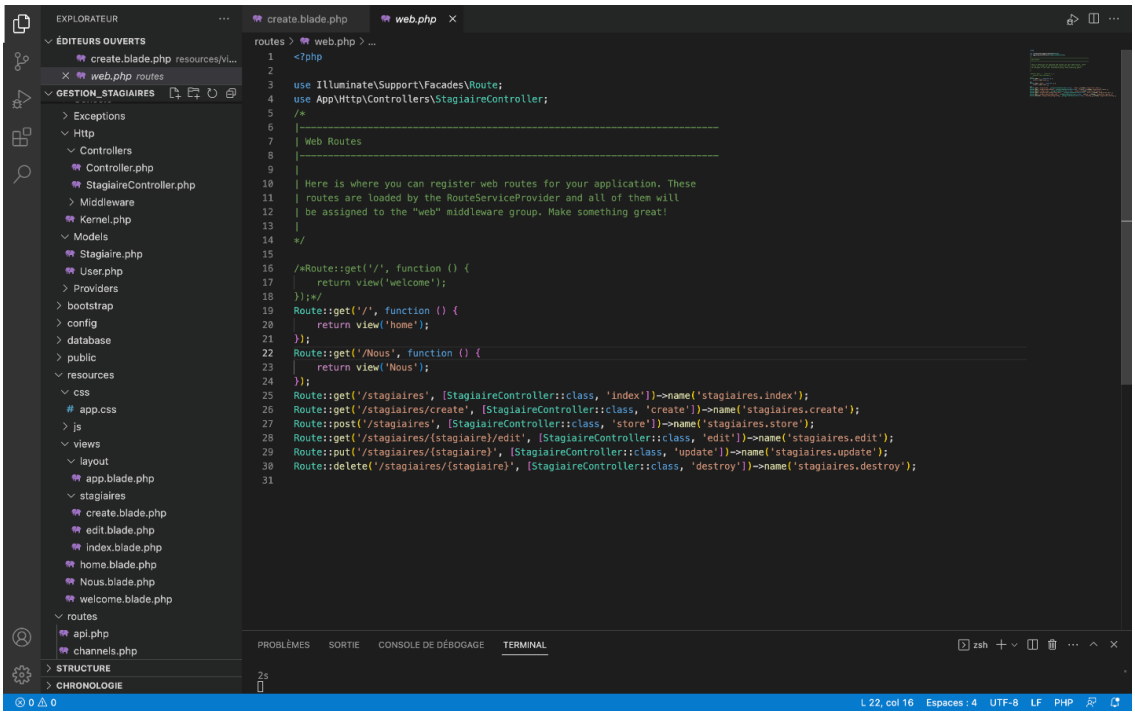


Figure 123: les routes

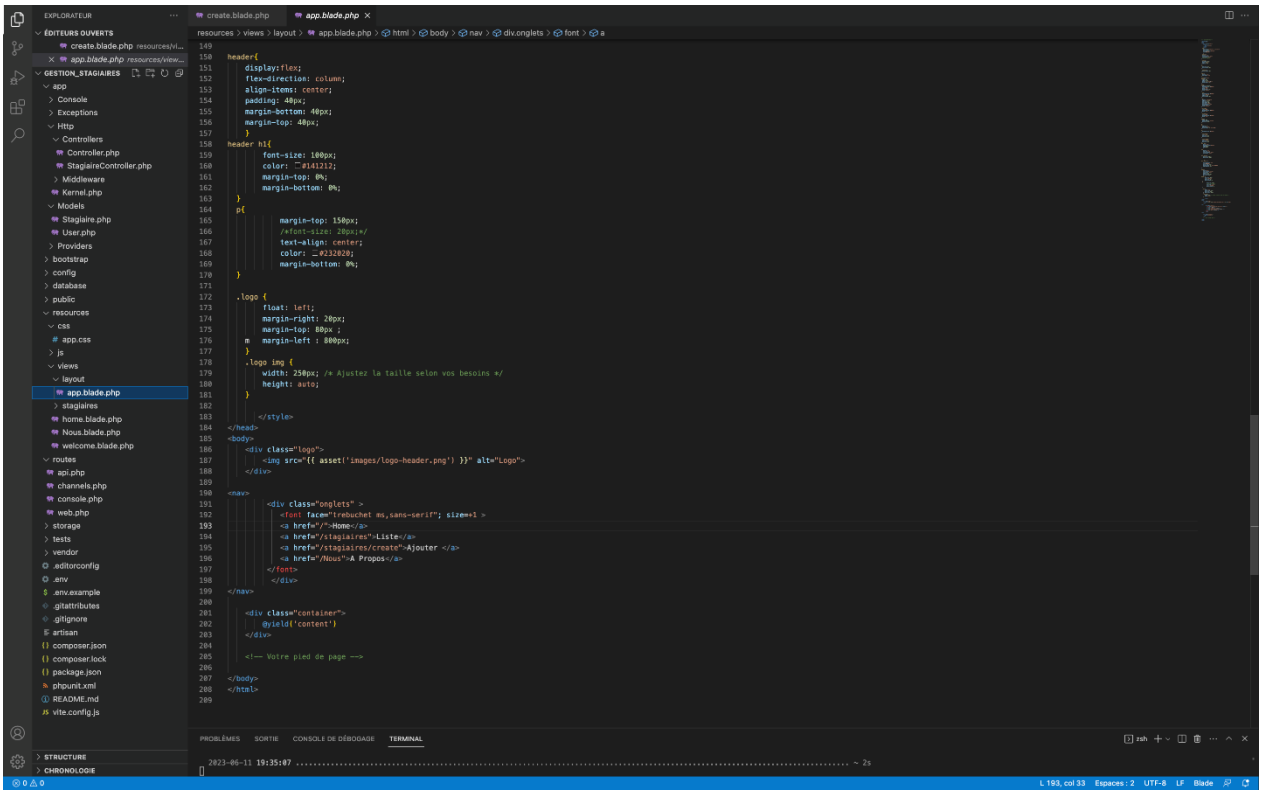


Figure 124: layout

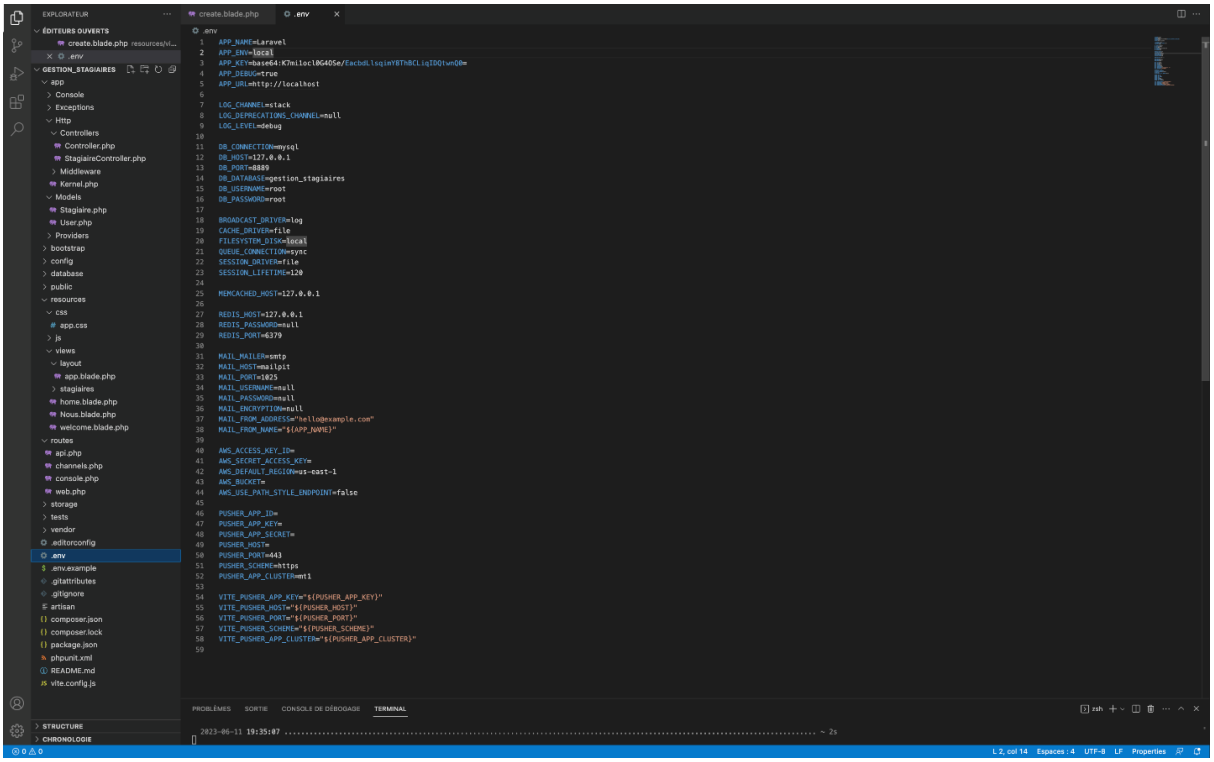


Figure 125: fichier de connexion avec la base de données

III. Application web :

Figure 126: la page home

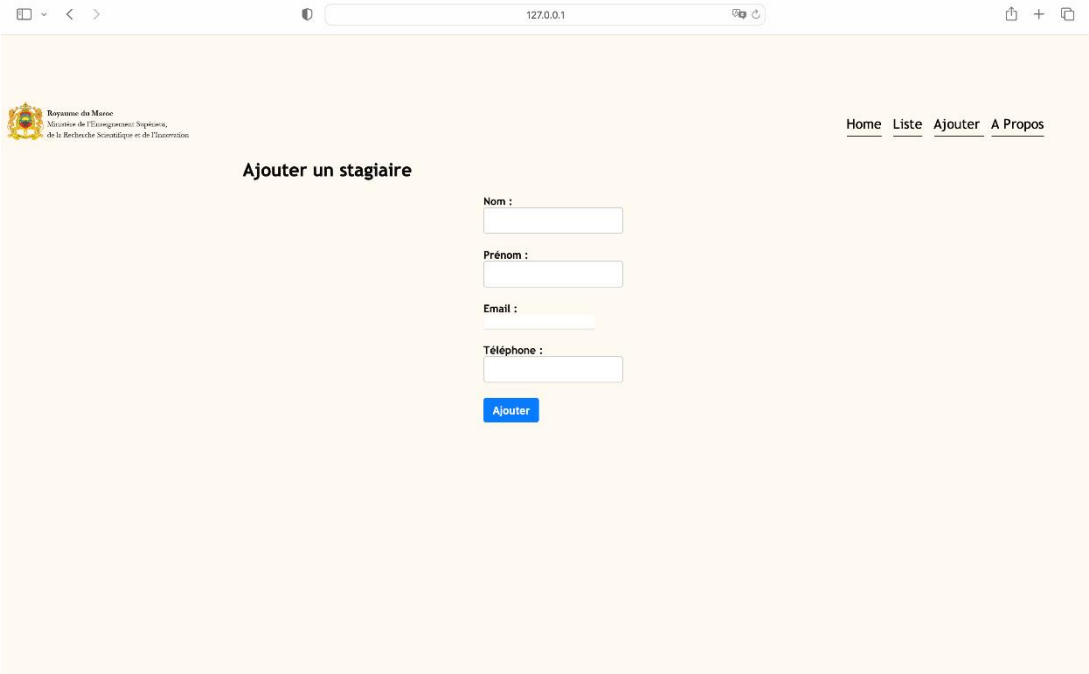


Figure 127: page pour ajouter un nouveau stagiaire

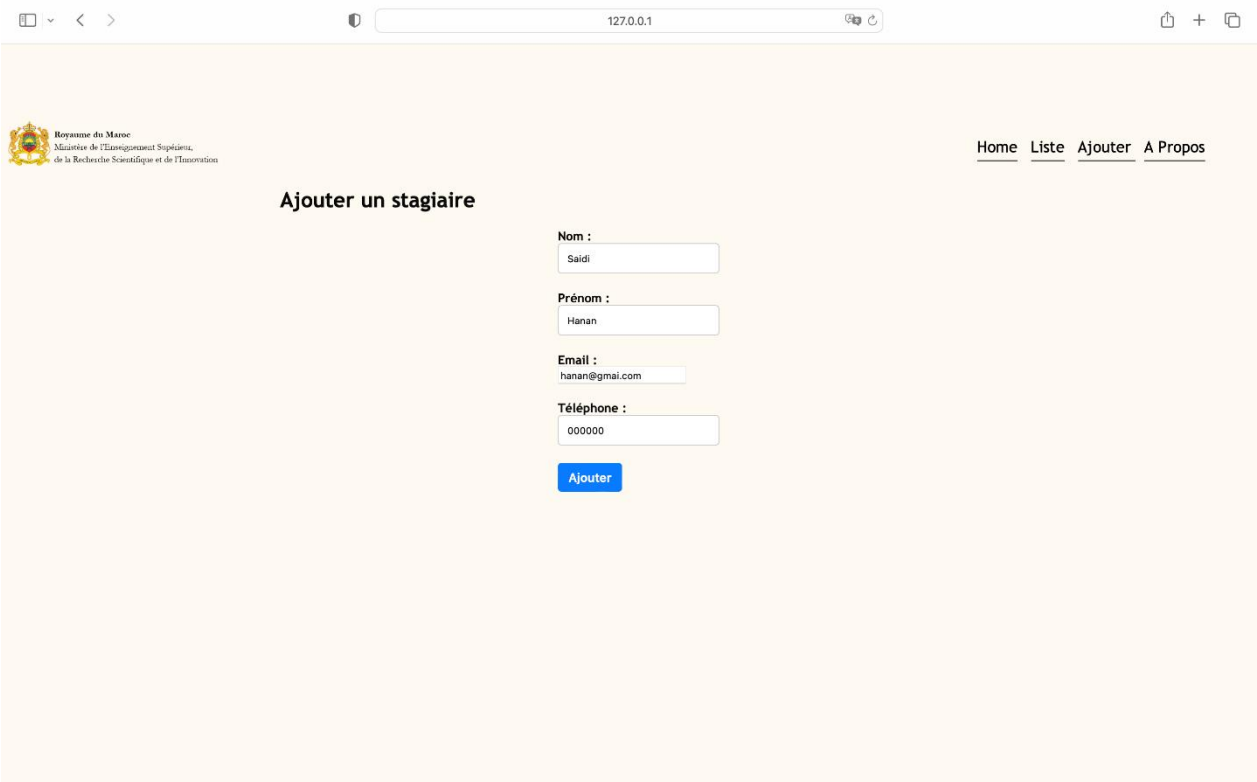
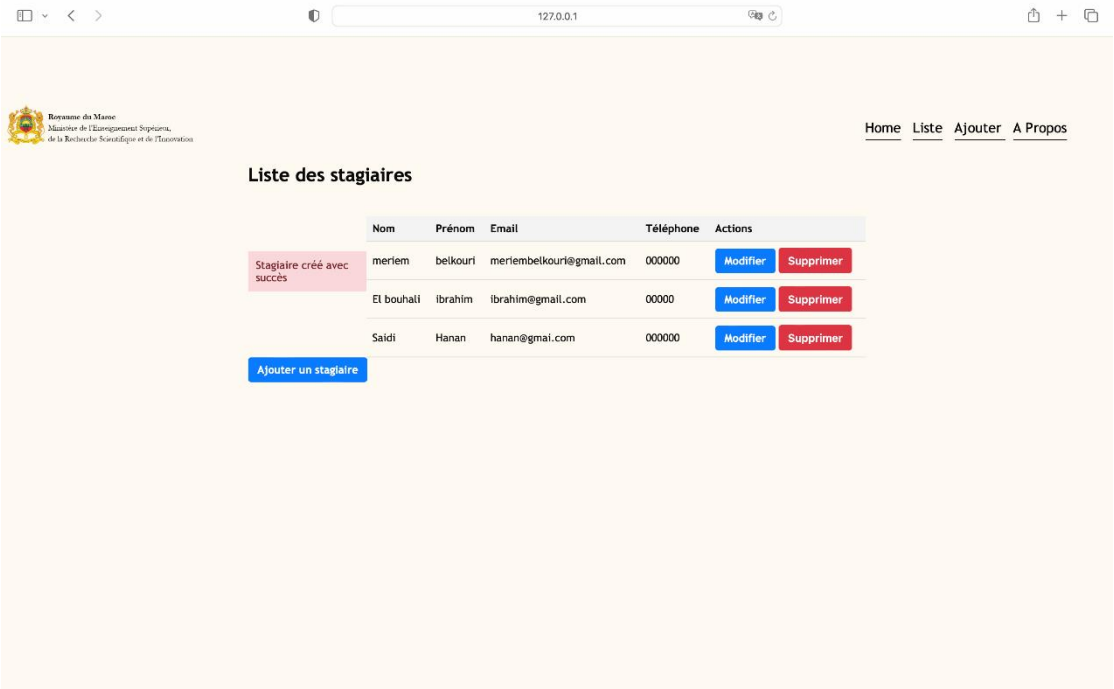


Figure 128: exemple d'ajout



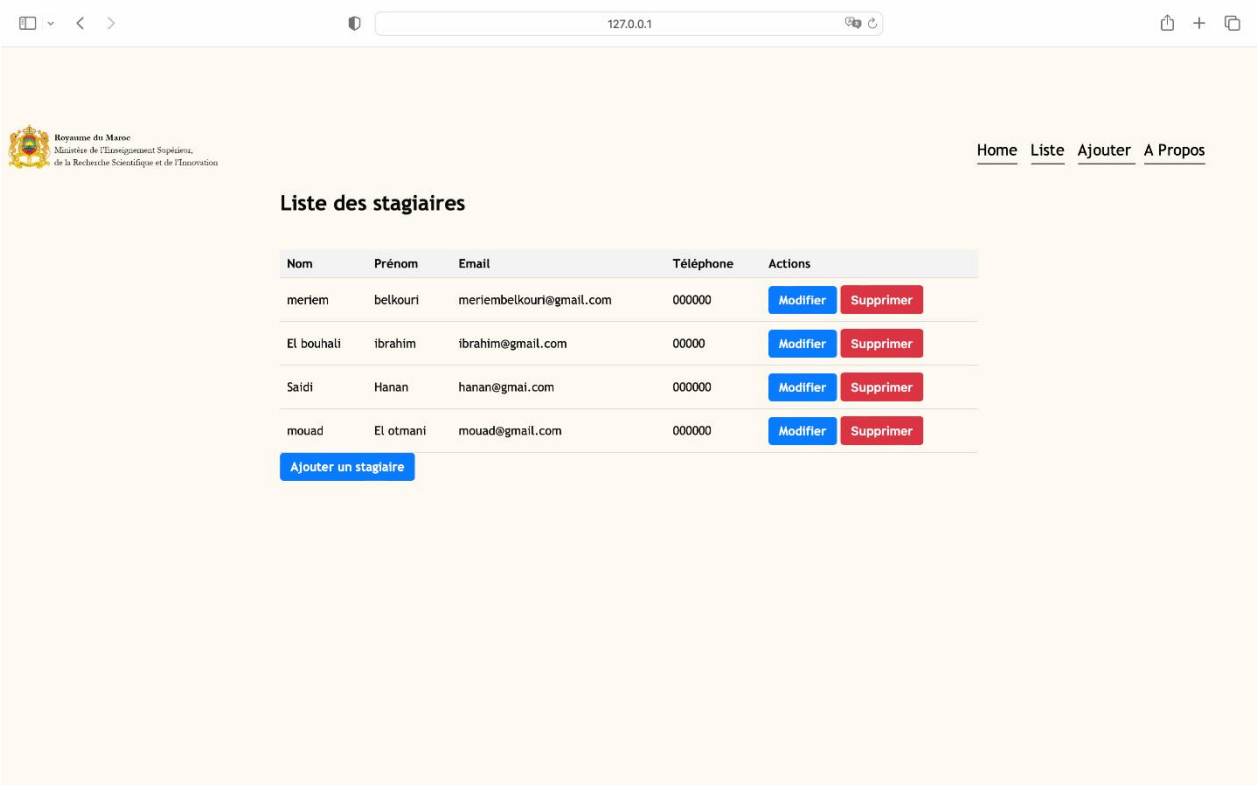


Figure 129: la liste des stagiaires

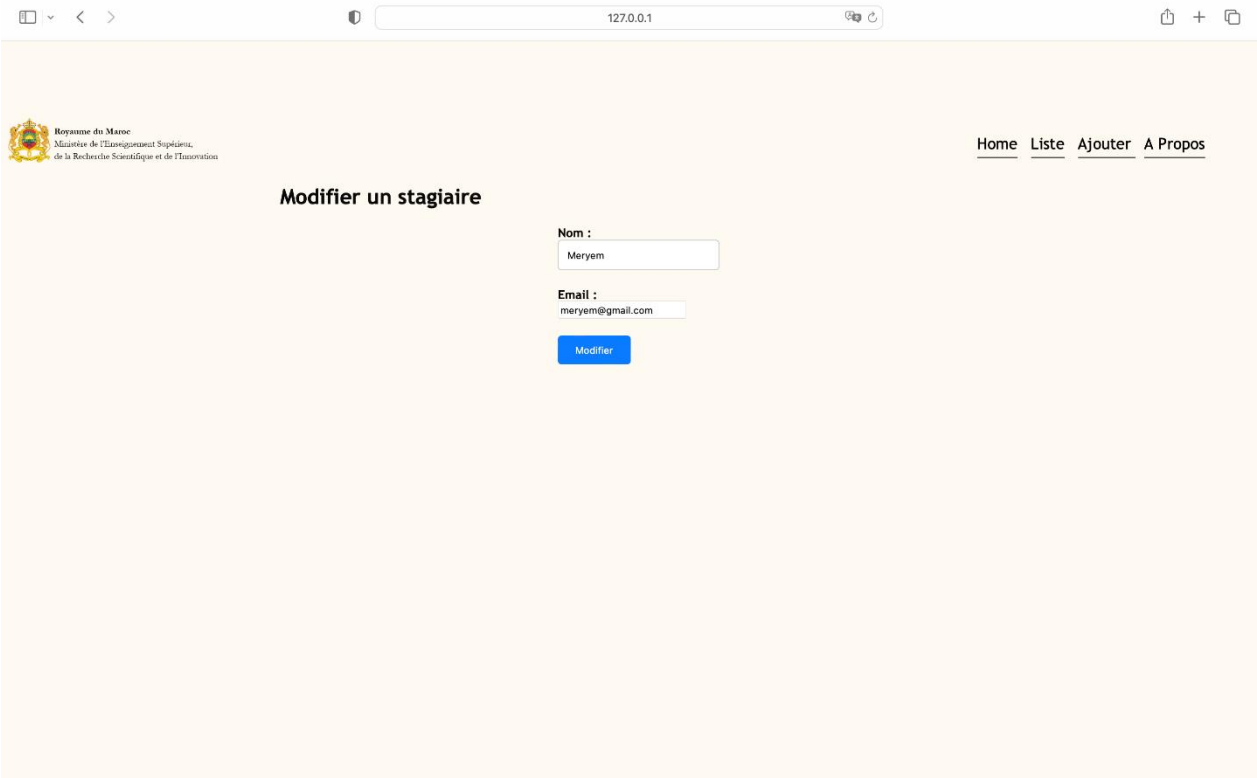


Figure 130: on peut modifier un stagiaire

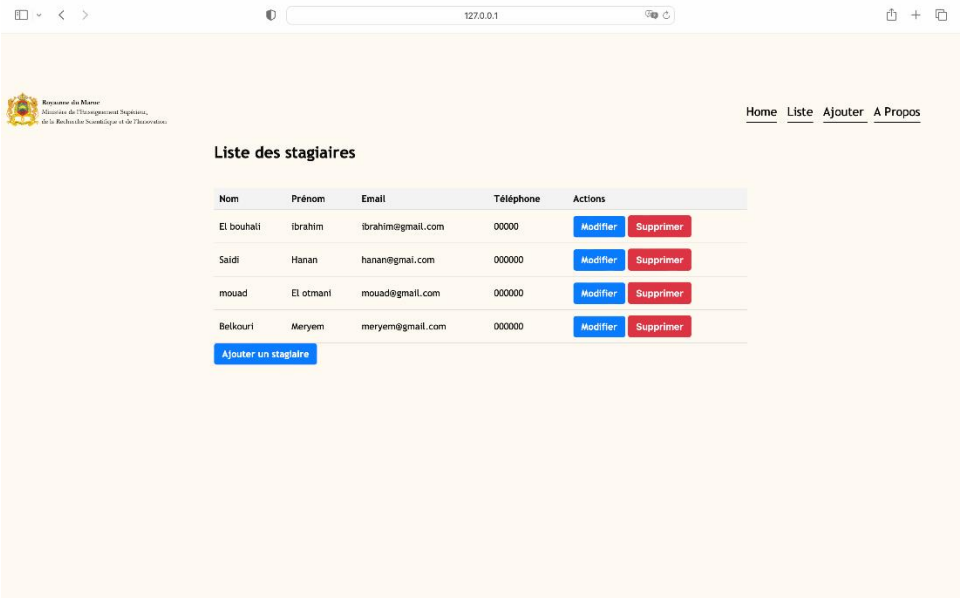


Figure 131: Stagiaire modifie

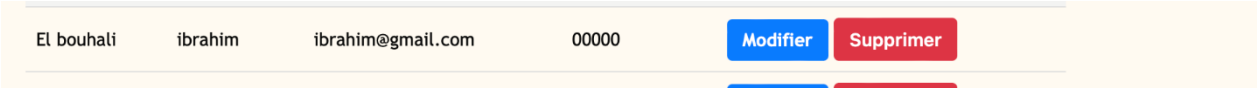


Figure 132: on clique sur supprimer

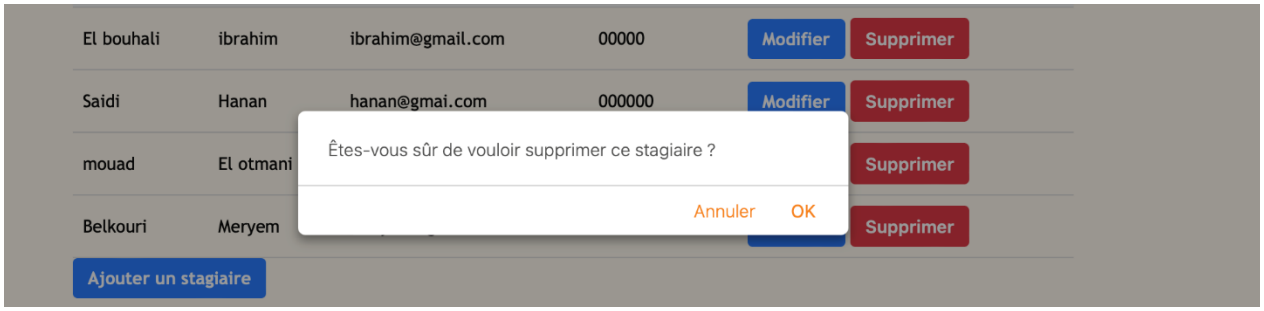
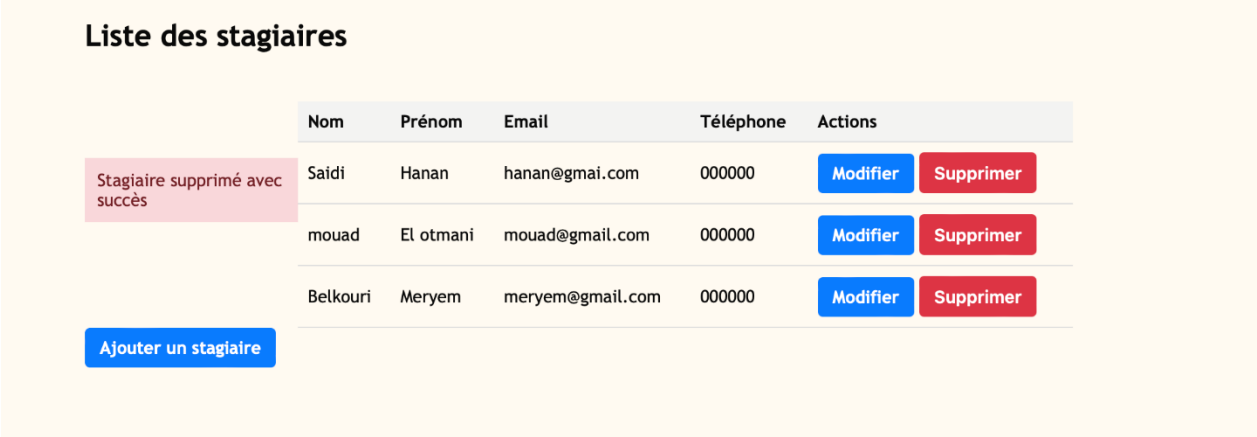


Figure 133: on clique sur ok pour supprimer le stagiaire



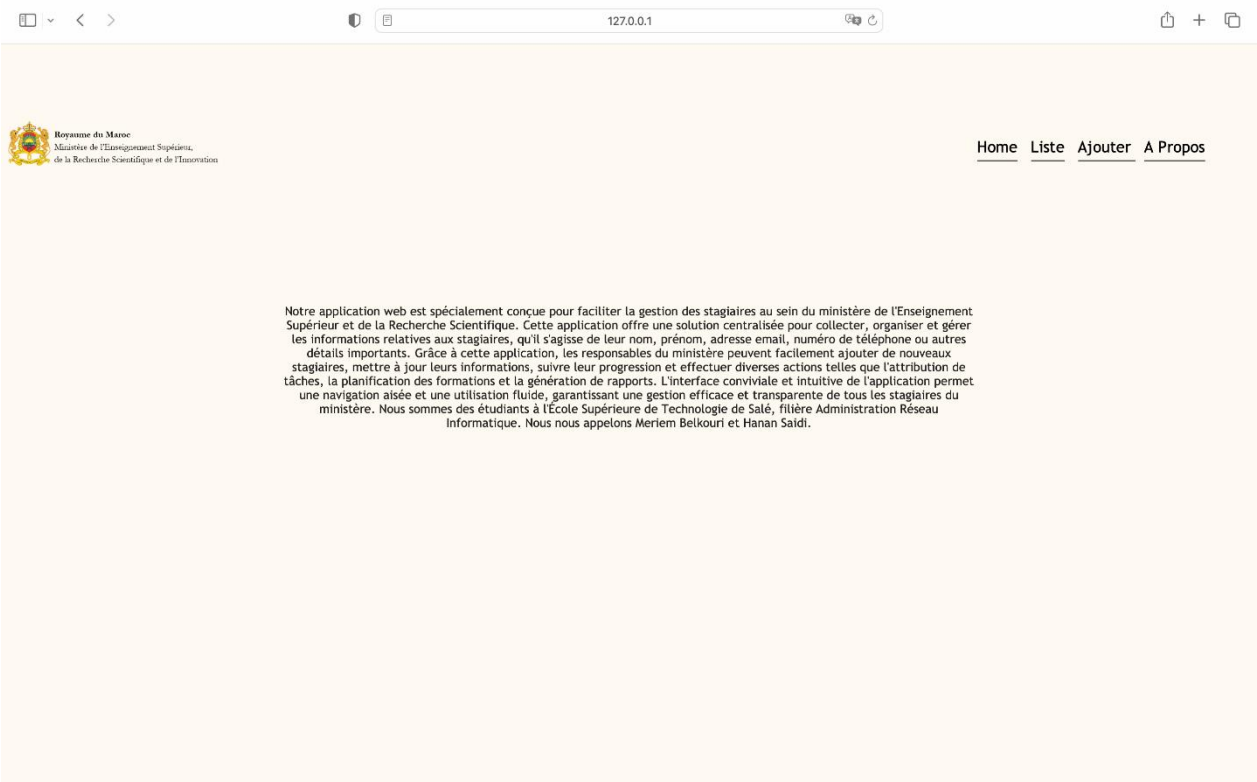


Figure 134: page explique l'objectif de l'app

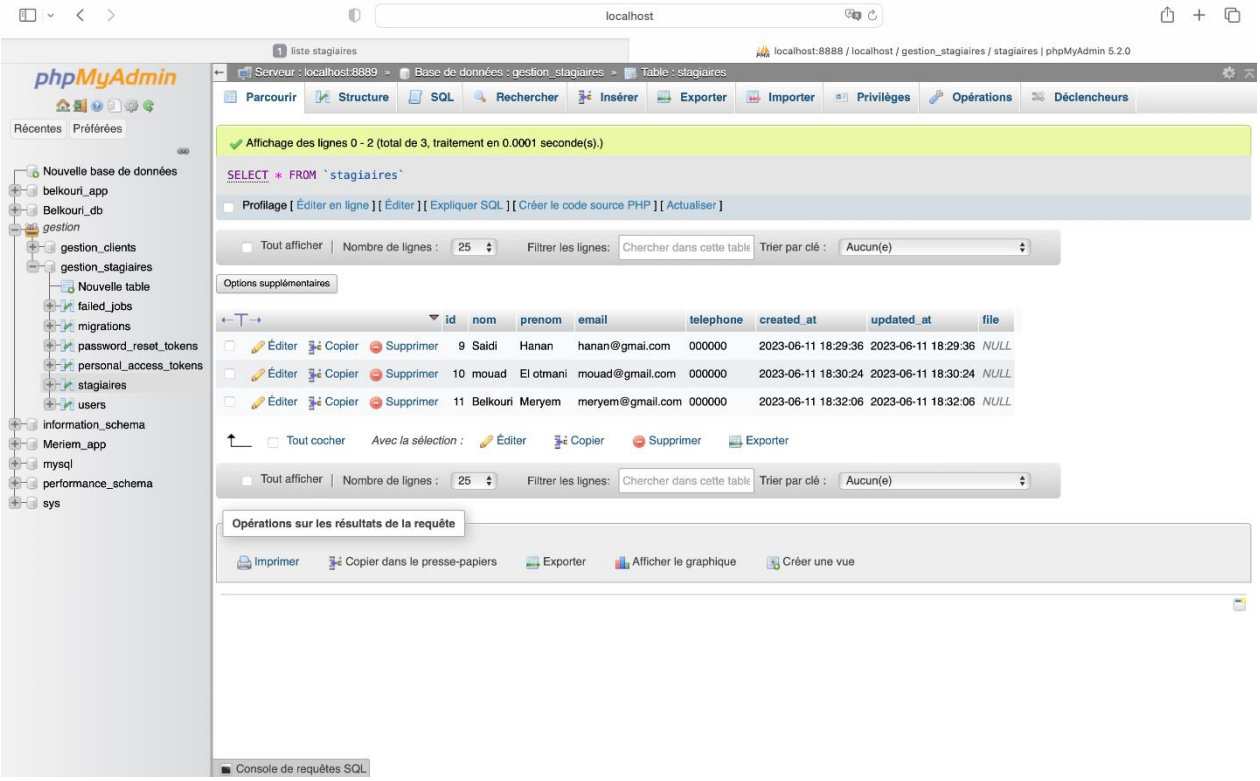


Figure 135: toutes les modifications sont appliquées dans DB

Conclusion générale :

En conclusion, notre stage au sein du Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation a été une expérience enrichissante et formatrice. Nous avons eu l'opportunité d'appliquer nos connaissances théoriques acquises au cours de notre formation et de développer de nouvelles compétences techniques et humaines.

Durant notre stage, nous avons été encadrés par une équipe compétente et dévouée, qui nous a guidés tout au long de notre mission. Nous avons travaillé sur des projets d'envergure, tels que la mise en place d'un réseau local sécurisé, la supervision avec Zabbix et le développement d'une application web avec le Framework Laravel. La réalisation de ces tâches nous a permis de mettre en pratique nos connaissances en matière de réseaux, de sécurité informatique, de supervision et de développement web. Nous avons pu découvrir et manipuler divers équipements et outils, et nous avons acquis une expérience concrète dans ces domaines.

Ce stage nous a également offert l'opportunité de développer des compétences non techniques, telles que la communication, la gestion de projet et le travail en équipe. Nous avons appris à collaborer efficacement avec nos collègues et à nous adapter à un environnement professionnel dynamique.

En conclusion, ce stage a été une étape clé dans notre parcours d'étudiant en nous permettant de mettre en pratique nos connaissances et de développer de nouvelles compétences. Nous sommes reconnaissants envers tous ceux qui nous ont soutenus et encadrés tout au long de cette expérience. IL nous a permis de grandir professionnellement et personnellement, et nous sommes désormais prêts à relever de nouveaux défis dans notre carrière future.

Résumé

Ce rapport présente en détail notre expérience de stage au sein du Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation. Durant notre stage, nous avons réalisé plusieurs tâches importantes, notamment la mise en place d'un réseau local sécurisé, la supervision avec l'outil Zabbix et le développement d'une application web utilisant le Framework Laravel.