REPUBLIQUE DU SENEGAL



Un peule -Un but -Une foi

Université Gaston Berger de Saint-Louis

UNIVERSITE GASTON BERGER

L'excellence au service du développement

UNITE FORMATION RECHERCHE DES SCIENCES APPLIQUEES ET DE TECHNOLOGIE

DEPARTEMENT D'INFORMATIQUE

……

MASTER SCIENCE ET TECHNOLOGIE

……

Réseaux Sécurité Système Distribué

……..

Mémoire

Mise en place d'un Network Operation Center(NOC) pour un réseau d'operateur

---

Présenté par :

Simon Sedar SENGHOR

Encadré par :

Pr Cherif DIALLO

Année académique 2021/2022

Dédicace

Je dédie ce mémoire à mes chers parents Grégoire waly SENGHOR et Abybatou DIALLO qui ont été toujours à mes côtés et m'ont toujours soutenu tout au long de ces longues années d'études. En signe de reconnaissance, qu'ils trouvent ici, l'expression de ma profonde gratitude pour tout ce qu'ils ont consenti d'efforts et de moyens pour me voir réussir dans mes études.

À mon frère Paul hamath SENGHOR et ma sœur Rose Anta SENGHOR pour leur encouragement et leur bonté qu'ils m'ont accordé, j'exprime ma profonde reconnaissance et mon grand respect.

À toute ma famille, mes amis je dédie ce travail, expression de toute ma gratitude et avec tous mes vœux de bonheur et de prospérité.

Remerciement

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais tout d'abord adresser toute ma reconnaissance au directeur de ce mémoire, Professeur Cherif DIALLO, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je désire aussi remercier les professeurs de l'université de Gaston BERGER de la formation en master, particulièrement ceux de la spécialité réseaux, sécurité et système distribué, qui m'ont fourni les outils nécessaires à la réussite de mes études universitaires.

Je voudrais exprimer ma reconnaissance envers ma famille les amis (14G2D et 8G2D)

- Monsieur Boubacar DIALLO, Monsieur Pierre henry Djiboune, Monsieur Jean Robert Ehemba, Monsieur Seydou BA, Monsieur Pape Bacary Michael FALL, Monsieur Arfang Ibrahima DIANE

Et collègues qui m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

Résumé

Le monde actuel du net est tellement connecté que les entreprises développent des réseaux plus complexes, fiables et conviviaux. C'est ainsi que le bon fonctionnement de l'architecture réseaux et des services sont d'une importance capitale pour une fiabilité de l'entreprise favorisant des recettes conséquentes. La migration du trafic web vers des services hébergés dans le Cloud, l'explosion de l'usage des appareils mobiles, la croissance des objets connectés : autant de facteurs qui vont apporter des changements structurels aux réseaux de communication des entreprises. Au final, de nombreux facteurs peuvent entraîner des pannes et des interruptions au bon fonctionnement notamment : coupures de câbles sous-marins, catastrophes naturelles, perturbations géomagnétiques, vols de cuivre et autres événements. À cela, on ajoute des vols de données à travers le piratage. Maintenant, face à ces nombreux facteurs, quelle est la meilleure manière de veiller à notre réseau afin d'anticiper ou de bien réagir à la protection du réseau le moment venu.

Pour répondre à cette difficulté nous allons dans un premier temps étudier le centre d'opération réseaux (NOC en anglais qui signifie Network Opération Center) qui est une zone centrale, l'architecture réseaux de l'entreprise. Il est question de savoir ce qu'un centre d'opération réseaux, mais de réfléchir à sa mise en place. Dans un second temps, de découvrir le réseau d'opérateur, c'est-à-dire comment il est structuré et les fonctionnalités qu'on trouve dedans. Et enfin mettre en place le NOC afin de bien surveiller notre réseau d'opérateur.

Dans la mise en place du centre d'opération nous avons pu faire des comparaisons dans le but de choisir les meilleurs outils pour mettre en pratique notre solution et atteindre nos objectifs. Au final, nous observons dans notre centre une surveillance de nos équipements du réseau d'opérateur avec l'ensemble des informations de nos appareils et une visualisation des données par rapport au mémoire, au réseau, et autre. Mais aussi la création de ticket pour un incident envoyé au niveau du centre d'opération réseau.

Abstract

Today's online world is so connected that companies are developing more complex, reliable and user-friendly networks. This is why the proper functioning of the network architecture and services is of capital importance for the reliability of the company, promoting substantial revenues. The migration of web traffic to services hosted in the Cloud, the explosion in the use of mobile devices, the growth of connected objects: all factors which will bring structural changes to business communication networks. Ultimately, many factors can cause outages and interruptions to proper operation, including: submarine cable cuts, natural disasters, geomagnetic disturbances, copper theft and other events. To this, we add data theft through hacking. Now, faced with these many factors, what is the best way to look after our network in order to anticipate or react well to protecting the network when the time comes?

To respond to this difficulty, we will first study the network operation center (NOC in English which means Network Operation Center) which is a central area, the network architecture of the company. It is a question of knowing what a network operations center is, but of thinking about its implementation. Secondly, to discover the operator network, that is to say how it is structured and the functionalities found in it. And finally set up the NOC in order to properly monitor our operator network.

In setting up the operations center we were able to make comparisons in order to choose the best tools to put our solution into practice and achieve our objectives. Ultimately, in our center we observe monitoring of our operator network equipment with all the information from our devices and visualization of the data in relation to memory, the network, and others. But also the creation of tickets for an incident sent to the network operations center.

Tables des matières

Université Gaston Berger de Saint-Louis i
Dédicace ii
Remerciement iii
Résumé iv
Abstract v
Liste des figures ix
Liste des tableaux xi
Liste des abréviations xii
INTRODUCTION GENERALE 1
CHAPITRE I : ETUDE DU CENTRE D'OPERATION RESEAUX 3
1-Introduction 3
2-Histoire de NOC 3
3-Qu'est qu'un NOC 3
4-Pourquoi un NOC 4
5-Les composants du NOC 4
5.1-Le système de supervision **5**
5.1.a-La supervision de système 6
5.1.b-La supervision réseaux 6
5.1.c-La supervision d'application 6
5.1.d-Les outils de supervision informatique 7
5.2-Le système de visualisation **7**
5.2.a-Définition 7
5.2.b-Pourquoi visualiser 7
5.3-Le système de ticketing (billetterie) **7**
5.4-Le système de gestion d'incident **9**
6-Sécurité du NOC 9
7-Comment bien mettre en place un NOC ? 10
7.1-Les bonnes pratiques **10**
8-Les outils pour un NOC 11
9-Conclusion 12
CHAPITRE II : PRESENTATION D'UN OPERATEUR RESEAUX 13
1-Introduction 13
2-Protocole et Modèle de communication 13
2.1-Protocole de communication **13**
2.2-Modèle de communication **13**

2.2.a-Modèle Open System Interconnection(OSI) 14
2.2.b-Modèle TCIP/IP 15
2.2.c-Transmission Control Protocol (TCP) 16
2.2.d-User Datagram Protocol (UDP) 17
2.2.e-IP (Internet Protocol) et routage 18
3-Réseaux d'operateur 19
3.1-Réseaux cœur **20**
3.2-Réseaux d'accès **21**
3.2.a-Réseaux d'accès mobile 21
3.2.b-Réseau d'accès fixe 21
4-Réseaux mobile 22
5-Qualité de service 24
5.1-Définition de la qualité de service **24**
5.2-QOS et QOE **25**
5.3-Paramètre QOS **25**
5.3.a-La bande passante 25
5.3.b-La latence 26
5.3.c-Le débit 26
5.3.d-Le taux de perte 26
5.3.e-La gigue 27
6-Conclusion 27
CHAPITRE III : MISE EN PLACE DU NOC POUR UN RESEAU D'OPERATEUR 28
1-Introduction 28
2-NOC d'un operateur 28
3-Les outils pour le NOC 29
3.1-Le système de supervision **29**
3.2-Système de ticketing **31**
3.3-Système de visualisation **33**
4-Environnement de travail 34
4.1-La solution locale **34**
4.2-Installation et configuration des outils choisis **34**
4.2.a-Installation l'outil de supervision : zabbix 34
4.2.a.1-Définition 34
4.2.b-Installation de l'outil Grafana 39
4.2.b.1-Définition 39
4.2.c-Installation l'outil de ticketing 41

4.3-Configuration du NOC 47
4.4-Résultat 60
5-Conclusion..... 62
CONCLUSION GÉNÉRALE..... 63

Liste des figures

Figure 1 : exemple de centre NOC [15] 4
Figure 2 : composants NOC 5
Figure 3 : Modèle OSI [16] 15
Figure 4 : modèle TCP/IP [17] 16
Figure 5 : TCP &UDP [18] 18
Figure 6 : Un réseau D'opérateur [21] 20
Figure 7 : Réseaux mobile [19] 22
Figure 8 : les Différents étapes [20] 23
Figure 9 : architecture du NOC d'un réseau operateur 29
Figure 10 : Mise en place d'un NOC locale 34
Figure 11: téléchargement de l'outil zabbix 36
Figure 12: désarchivage de zabbix 36
Figure 13: installation de zabbix serveur, agent zabbix, apache 36
Figure 14: création de la base de données 37
Figure 15:insertion nom utilisateur et mot de passe 37
Figure 16: redémarrer les services: zabbix, agent zabbix, apache 38
Figure 17: finalisation de l'installation 38
Figure 18: page d'accueil de l'outil zabbix 39
Figure 19:Ajout de la clé et dépôt du paquet grafana 40
Figure 20: installation des paquets nécessaires grafana 40
Figure 21: importation de la clé grafana 40
Figure 22:installation de GRAFANA 41
Figure 23: page d'accueil de GRAFANA 41
Figure 24: installation et lancement des services apache et PostgreSQL 42
Figure 25: installation des modules perl d'OTRS 42
Figure 26: activation des PERL 42
Figure 27: création de l'utilisateur: 42
Figure 28: création de la base de données 43
Figure 29: activation de l'utilisateur 43
Figure 30: téléchargement de l'outil OTRS 44
Figure 31: vérification des modules 44
Figure 32:copie des paramètres nécessaires OTRS 44
Figure 33: activation de la base de donné PostgreSQL 45
Figure 34: vérification des modules et dépendances 45
Figure 35: relancer le service web apache2 45
Figure 36: finalisation de l'installation 46
Figure 37:configuration des adresses ip au niveau du routeur 47
Figure 38: activation de SNMP 48
Figure 39: configuration agent zabbix 48
Figure 40: configuration de l'adresse serveur et du port 49
Figure 41:creation des utilisateurs 49
Figure 42: Activation de l'agent zabbix sur Windows 50
Figure 43: ajout d'un matériel sur zabbix 51
Figure 44: intégration zabbix sur grafana 52
Figure 45: Ajout du mail système 53
Figure 46: compte de messagerie 53

Figure 47:Ajout d'un groupe **54**
Figure 48: Enregistrement du client **54**
Figure 49:ajout des informations du client **55**
Figure 50: modification des relations **55**
Figure 51: Ajout d'operateur **56**
Figure 52: ticket hardware **57**
Figure 53: ticket software **58**
Figure 54: connexion de l'utilisateur **58**
Figure 55: Création et validation de ticket **59**
Figure 56: résultat de surveillance du réseau **60**
Figure 57: visualisation des données **61**
Figure 58: visualisation des tickets envoyés **62**

Liste des tableaux

Tableau 1 comparaison Zabbix et Nadios..... 30
Tableau 2 comparaison entre OTRS et Request Tracer 31
Tableau 3 comparaison entre Grafana & Kibana..... 33
Tableau 4 composant d'installation zabbix..... 35

Liste des abréviations

NOC : Network Operation Center

IT : Information Technologie

AT&T : l'American Téléphone & Telegraph

ITIL : Information Technology Infrastructure Library

SOC : Sécurité Operation Center

KPI: Key Indicator Performance

IEEE: Institute of Electrical and Electronics Engineers

RFC: Requests For Comments

LAN: Local Area Network

WAN: Wide Area Network

PAN: Personal Area Network

UIT : Union internationale des télécommunications

RIP : Routing Information Protocol

IGRP: Interior Gateway Routing Protocol

EIGRP: Enhanced Interior Gateway Routing Protocol

OSPF: Open Shortest Path First

IS-IS: Intermediate System to Intermediate System

VPN: Virtual Private Network

GPRS: General Packet Radio Service

UMTS : Universal Mobile Telecommunications System

INTRODUCTION GENERALE

Le monde du numérique d'aujourd'hui pousse les entreprises à développer des réseaux plus complexes, fiables et conviviaux. Pour les entreprises, la connectivité, que ce soit entre employés, entre systèmes autonomes, ou avec des clients et clients potentiels, reste un élément essentiel du bon fonctionnement de leur infrastructure. La migration du trafic web vers des services hébergés dans le Cloud, l'explosion de l'usage des appareils mobiles, la croissance des objets connectés autant de facteurs qui vont apporter des changements structurels aux réseaux de communication des entreprises. Au final, de nombreux facteurs peuvent entraîner des pannes et des interruptions de certaines ou de toutes les activités comme les coupures de câbles sous-marins, catastrophes naturelles, perturbations géomagnétiques, vols de cuivre et autres événements. Cependant, certaines industries nécessitent une connectivité ininterrompue, quelques soient les circonstances.

C'est ainsi que la surveillance de nos infrastructures informatiques a pris des échelons considérables pour le bien-être de nos entreprises. Il est aussi pertinent de s'intéresser à la meilleure manière de pratiquer la surveillance de tous les matériels du réseau afin de réduire certains facteurs dans le but d'offrir un service de qualité.

La sécurité est un moyen de protéger l'intégralité des technologies de l'information à savoir les systèmes, le réseau et les données dans le but d'offrir un service de qualité aux utilisateurs mais aussi d'avoir un sentiment de facilitateur afin que le monde du numérique puisse cliquer en toute aisance. Ce sentiment de bien servir et d'assurer une sécurité a soulevé des questionnements qui m'ont suscité mon intérêt face à la surveillance du réseau.

Les centres d'exploitation de réseau évoluent, mais toutes les transformations des centres d'exploitation de réseau se ressemblent. Certaines organisations modernisent leurs centres d'exploitation de réseau avec des outils d'automatisation et de visibilité, tandis que d'autres s'éloignent d'un centre d'exploitation de réseau autonome.

Le NOC s'oriente vers un centre d'opération unifié qui comprend une équipe chargée des réseaux, de la sécurité et de l'informatique en nuage.

Dans ce mémoire même si on ne peut pas avoir une sécurité totale et un service de qualité sans faille nous nous interrogeons sur les nouvelles stratégies de mise en place de NOC

pour un opérateur afin de maintenir un meilleur niveau de service de qualité mais aussi veiller à notre sécurité tout le temps.

Afin de traiter ce sujet et de répondre aux questionnements soulevés nous avons proposé un plan de recherche. D'abord des questions ont été postées en ligne durant quelques mois ensuite nous avons complété ces informations avec la lecture d'article scientifique et de mémoire de thèse.

Dans la suite nous voudrions comprendre en quoi la mise en place de NOC permettra une meilleure qualité de service d'un réseau d'opérateur dans ce monde ou les données sont en évolution d'année en année et la sécurité menacée.

Pour bien répondre à cette problématique nous verrons dans un premier temps qu'il est nécessaire de comprendre NOC afin de voir comment le mettre en place ensuite dans un second temps de faire l'étude d'un réseau d'opérateur et ces caractéristiques afin de voir comment veiller sur elle pour qu'il joue bien son rôle et finalement de mettre place la solution NOC pour notre réseau d'opérateur.

CHAPITRE I : ETUDE DU CENTRE D'OPERATION RESEAUX

1-Introduction

Dans cette partie, nous allons voir les notions de base du centre d'opération pour la mise en place d'un centre d'opération réseaux NOC (en anglais : Network Opération Center, abrégé NOC) qui est un service de surveillance des événements, d'analyse des données, des incidents. Puis nous parlerons de l'intérêt du NOC et enfin, nous allons présenter les objectifs, ce qui nous amène à identifier les possibilités de système NOC et les besoins qui nous permettront de bien mettre en place notre NOC pour un réseau d'opérateur.

2-Histoire de NOC

Les premières [1] versions du NOC existent depuis les années 1960. Un centre de contrôle du réseau a été ouvert à New York par AT&T (l'American Telephone & Telegraph) qui utilisait des tableaux d'état pour afficher en temps réel des informations sur les commutateurs et les itinéraires à partir des commutateurs à péage les plus importants, et ce centre s'est développé jusqu'à ce qu'il devienne le concept actuel du NOC.

3-Qu'est qu'un NOC

NOC qui signifie Network Opération Center [2] en anglais ou Centre d'Opération Réseaux est un lieu central de surveillance des événements, d'analyse des données, de gestion des incidents. Il est composé de personnels IT (Technologie de l'information) dans le but de protéger le réseau contre toute forme de dysfonctionnement. Le NOC sert de première ligne de défense contre les perturbations et les pannes du réseau. Le NOC peut nous faire voir l'infrastructure d'une entreprise, l'équipement, les systèmes sans fil, les bases de données, les pare-feu, les divers périphériques réseaux, les télécommunications. Ses services de gestion incluent également la supervision des appels des clients et des systèmes de tickets d'assistance clients, et ils s'intègrent aux outils de réseau des clients. On comprend donc que le NOC joue un rôle considérable pour la qualité de l'expérience client. Le NOC peut être sous-traité par une entreprise externe spécialisée dans la supervision et la gestion du réseau et des infrastructures, mais sinon on peut le mettre au niveau interne du Datacenter. La figure 1 illustre un exemple de NOC

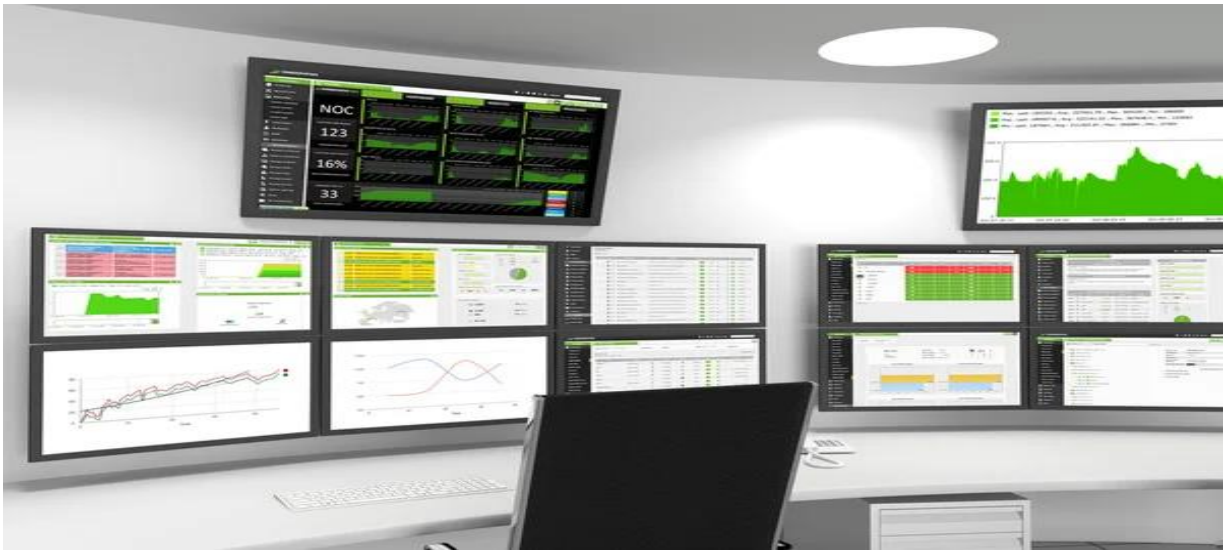


Figure 1 : exemple de centre NOC [15]

4-Pourquoi un NOC

Le volume d'utilisateurs, le trafic web et les logiciels malveillants peuvent nuire aux performances du réseau, et le risque peut venir de partout. Même des problèmes apparemment mineurs peuvent entraîner des interruptions désastreuses pour la productivité et votre capacité à répondre aux besoins des clients. C'est pour cela les organismes s'efforcent constamment d'adopter de nouvelles technologies, en mettant à profit l'infrastructure de pointe pour les fonctions informatiques critiques de l'entreprise telles que la ressource humaine, le marketing et les ventes. Dans la concurrence actuelle du marché, même un temps d'indisponibilité réduit (causé par des pannes d'infrastructure) a un énorme impact sur les revenus et la réputation de l'entreprise. Les fournisseurs de services informatiques ont reconnu ce défi et ont commencé à offrir un service plus fiable, évolutif et hautement disponible. Cela est assuré par le soutien de l'infrastructure sous l'acronyme « NOC », centre d'opérations du réseau qui permettra d'assurer les performances et la disponibilité du réseau pour un bon fonctionnement continu.

5-Les composants du NOC

Dans la mise en place d'un service efficace et fiable, un fournisseur de service internet est tenu de gérer son infrastructure avec une véritable discipline en utilisant une structure cohérente pour la gestion des informations recueillies. C'est pour cela que pour mettre en œuvre un NOC qui permet de maintenir les performances et la disponibilité du réseau à un niveau optimal de manière continue, il faut quatre éléments essentiels qui sont : système de supervision, un système de visualisation, un système de ticketing et un système ou guide de gestion d'incidents.

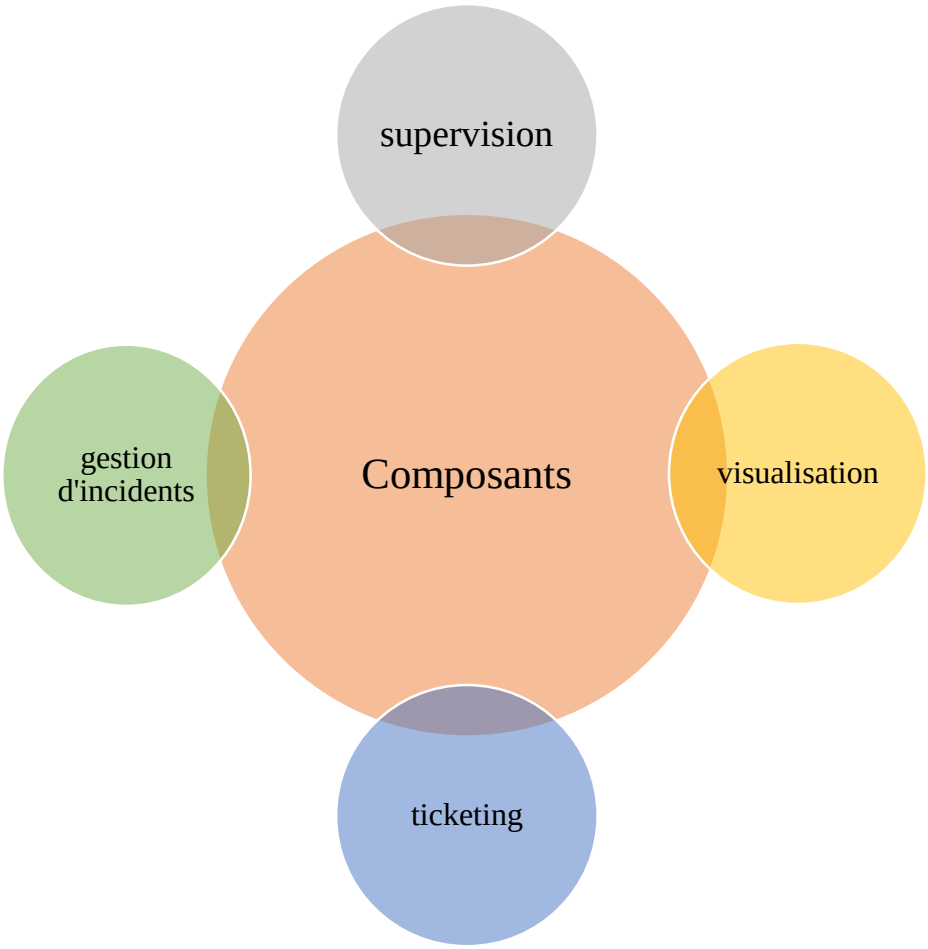


Figure 2 : composants NOC

5.1-Le système de supervision

La supervision est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. 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 aux préoccupations suivantes :

- Technique : surveillance du réseau, de l'infrastructure et des machines ;
- Applicative : surveillance des applications et des processus métiers ;
- Contrat de service : surveillance du respect des indicateurs contractuels ;
- Métier : Surveillance des processus métiers de l'entreprise.

On ajoutera les actions réflexes à cette surveillance du système. Ce sont les réactions automatisées en fonction d'alertes définies. En cas de dysfonctionnement, le système de

supervision permet d'envoyer des messages sur la console de supervision, ou bien d'envoyer un courriel à l'opérateur et ce 24h/24 et 7j/7 dans certaines entreprises. Mais si la supervision n'est pas active 24/7, le dysfonctionnement se produit en dehors des heures de bureau, et en l'absence de système approprié, l'alerte n'est pas reçue par l'opérateur, et les utilisateurs des applications ne sont pas prévenus du dysfonctionnement. C'est pourquoi il peut être utile de compléter le superviseur par un logiciel de gestion des alertes, qui envoie automatiquement un courriel, un SMS, ou un appel téléphonique à un opérateur sous astreinte.

5.1.a-La supervision de système

La supervision système porte principalement sur les trois types principaux de ressources système :

- Le processeur ;
- La mémoire ;
- Le stockage.
- Commutateurs : utilisation des ressources, métrologie.
- Serveurs : utilisation des ressources.

5.1.b-La supervision réseaux

La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité, mais également du contrôle des flux.

5.1.c-La supervision d'application

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs.

À titre d'exemple, un serveur informatique peut avoir une supervision système et réseau avec des signaux au vert, mais le site web qu'il héberge sera indisponible si l'application de serveur web n'est pas présente ou n'est pas en mesure de servir des pages Web.

La supervision applicative passe donc par des mesures faites aussi sur le flux de service. On parle alors de validation fonctionnelle. On utilise souvent un sous-ensemble des tests ayant permis la recette d'une application pour n'en prendre que les tests qui sont représentatifs de l'activité sans pour autant générer une charge trop importante ou modifier les données applicatives.

La supervision applicative ne peut se faire sans considérer la sécurité applicative.

5.1.d-Les outils de supervision informatique

Pour pouvoir réaliser une supervision industrielle ou informatique, il est possible d'utiliser des logiciels de supervision open source. Il en existe plusieurs à présent qui se sont développés par différentes communautés dont on peut citer : nagios, centreon, zabbix, zenos …

5.2-Le système de visualisation

5.2.a-Définition

La visualisation est un moyen de faire apparaitre des données sur un écran les résultats des traitements d'information. La visualisation des données est le processus d'utilisation d'éléments visuels tels que des diagrammes, des graphiques ou des cartes pour représenter les données. Elle traduit des données complexes, volumineuses ou numériques en une représentation visuelle plus facile à traiter. Les outils de visualisation des données améliorent et automatisent le processus de communication visuelle pour plus de précision et de détails. Vous pouvez utiliser les représentations visuelles pour extraire des informations exploitables des données brutes.

5.2.b-Pourquoi visualiser

La visualisation permet d'étudier, d'analyser les données afin de prendre des décisions stratégique, de voir les besoins du client pour une supervision plus efficace. Au niveau des outils de supervisions qui n'ont pas une visualisation très avancée (basique) on peut utiliser le système de visualisation quand il s'agit de tableaux de bord analytiques. Et NOC impose une solution de « dashbording » [1]

5.3-Le système de ticketing (billetterie)

Un système de billetterie est une application logicielle utilisée pour gérer et suivre les demandes d'assistance à la clientèle, les incidents et les demandes de renseignements. Il est couramment utilisé par les organisations pour gérer efficacement les demandes de service à la clientèle et pour s'assurer que les problèmes sont résolus en temps voulu et de manière organisée.

Le système de billetterie fonctionne en permettant aux clients de soumettre leurs demandes d'assistance ou leurs problèmes par le biais de différents canaux tels que le courrier électronique, le téléphone ou les formulaires web. Le système génère ensuite un numéro de

[1] **Dashboard** est la traduction anglaise du terme « tableau de bord ». Ainsi, **c'est** une représentation visuelle des informations importantes sur un même écran

ticket unique pour chaque demande et la classe en fonction du type de problème, du niveau de priorité et d'autres facteurs pertinents.

L'équipe d'assistance peut alors accéder au ticket, examiner les détails du problème et fournir des réponses appropriées en temps voulu. Le système de billetterie permet également aux membres de l'équipe de communiquer entre eux, de transmettre les problèmes aux autorités supérieures et de suivre l'évolution de chaque billet jusqu'à ce qu'il soit résolu.

Les systèmes de billetterie sont couramment utilisés dans divers secteurs, tels que l'assistance informatique, le service clientèle et les services d'assistances. En utilisant un système de billetterie, les organisations peuvent améliorer leurs temps de réponse, rationaliser leurs processus d'assistance et fournir un meilleur service à la clientèle dans l'ensemble.

« Ce type d'outils était conçu pour suivre les incidents ou anomalies d'un projet. Désormais, certains logiciels de suivi de problèmes sont configurables et permettent de gérer tous types de tickets ou alertes : tâches, demandes de support, exigences,...

Le système tickets permet de :

- Créer un ticket pour chaque problème signalé.
- Assigner le problème au 2ème niveau ou met à jour le statut des tickets.
- Favoriser l'archivage de tout dysfonctionnement sur du long terme.
- Donner des analyses statistiques (incidents/période, type, temps, moyen de résolution, etc...)
- Servir de base de connaissances (knowledge base)

L'équipe du centre d'opération se charge de :

- Détecter les anomalies et analyser les graphes et données (24x7)
- Ouvrir des tickets d'incidents pour suivre les problèmes
- Procéder au diagnostic préliminaire (1 st level)
- Assigner le problème à l'équipe, et met à jour le statut des tickets.
- Assure le suivi du problème jusqu'à sa résolution.»

5.4-Le système de gestion d'incident

La gestion des incidents (GDI) est un processus de gestion du cycle de vie de tous les incidents. Elle s'assure que l'exploitation normale des services soit rétablie le plus rapidement possible et que l'impact sur le business soit réduit au minimum.

L'exploitation normale des services est définie dans l'accord sur les niveaux de service (SLA : Le service-level agreement en anglais). Il décrit le service informatique, documente les cibles de niveau de service et spécifie les responsabilités du fournisseur de service informatique et du client.

Selon ITIL (Information Technology Infrastructure Library), l'objectif de la Gestion des Incidents est la suivante : « Restaurer aussi vite que possible le fonctionnement normal des services et minimiser l'impact négatif sur les activités métiers et s'assurer ainsi que les meilleurs niveaux de qualité de service et de disponibilité sont maintenus ». Un Incident est défini par ITIL comme étant : « Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.». Les incidents peuvent être classés en trois catégories : logiciel, matériel, et requête de service. La gestion des incidents est un moyen de mettre en place un système de gestion des incidents assurés par le centre NOC. Ce document définit les performances (KPI : Les KPI, Key Indicator Performance en anglais, sont les indicateurs d'une entreprise qui permettent de mesurer une performance. Autrement appelés ICP en français, Indicateurs Clés de Performance, ils sont nécessaires pour apprécier la situation réelle d'une entreprise et donc son état de santé à un instant T) ainsi que les éléments essentiels de la gestion des incidents.

6-Sécurité du NOC

Dans son rôle de veiller à la sante du réseau le NOC se doit d'avoir une sécurité optimale. Mais peut-il jouer ce rôle ?

NOC se charge des performances et de la disponibilité du réseau alors que SOC [3] par définition est le centre des opérations de sécurité qui rassemble des outils et professionnels qui supervisent, détectent et analyse le niveau de sécurité d'une entreprise. Dans leur fonctionnement les techniciens NOC recherchent les problèmes susceptibles de dégrader les réseaux tandis que ceux du SOC ont pour mission de repousser les menaces cybercriminels mais aussi de réagir aux attaques. NOC gère les évènements du réseau alors que le SOC gère que la sécurité. Hors mis leur différence les deux fonctionnent de manière similaire et partage la même approche de gestion des incidents. « Cela dit, les SOC et les NOC doivent collaborer

pour démêler les incidents majeurs et résoudre les crises, donc les deux équipes ne doivent pas être isolées l'une de l'autre. On sera surpris d'apprendre que près d'un tiers des entreprises n'indiquent que peu ou pas de contact entre le NOC et le SOC, et qu'elles soient 20 % à dire que les équipes ne coopèrent que pendant les urgences, selon une étude de SANS[14]. Les experts encouragent toutefois une meilleure intégration du NOC et du SOC. L'intégration des deux unités, même si elles restent essentiellement séparées au quotidien, commence par la mise en place de procédures opérationnelles, l'automatisation de certaines actions et l'adoption d'outils permettant la collecte et le partage des données de supervision du réseau entre le NOC et le SOC. »

NOC dans une situation qu'on peut mettre sur pied un NOC et un SOC, le NOC est capable de gérer [4] sa sécurité car il peut détecter les menaces de sécurité qui peuvent affecter la performance du réseau mais aussi avoir un personnel qualifie pour pouvoir apporter des solutions efficaces.

7-Comment bien mettre en place un NOC ?

7.1-Les bonnes pratiques

Dans la mise en place d'un NOC il faut prioriser la formation, s'appuyer sur les rôles clairement définis et établir les protocoles et moyen de communications.

- Priorité de la formation : les technicien du NOC doit avoir une expertise de haut niveau spécifiquement dans la supervision et la résolution des problèmes propres aux performances du réseau et à l'infrastructure IT. Renforcer la capacité sur les procédures et les protocoles associe à tous les évènements et mettre à jour la paysage technologique et de l'environnement informatique.
- Définissez des rôles clairs : Si les techniciens informatiques du NOC doivent avoir la liberté de faire leur travail et de proposer leurs éclairages il faut qu'un chef d'équipe répartisse le travail entre les techniciens selon leurs compétences, hiérarchise les tâches, prépare les rapports, veille à la bonne résolution des incidents et tienne les autres fonctions de l'entreprise informées des événements au besoin
- Protocole et moyens de communication : il n'est pas forcément simple de garder les lignes de communication ouvertes entre le NOC, le SOC et les autres équipes externes. Il faut bien plus qu'une poignée de réunions régulières. Au contraire, il faut un effort concerté pour former le personnel aux modalités de partage des informations, et pour veiller à ce qu'ils s'acquittent de ces obligations. Un Network Operation Center (NOC)

solide a impérativement besoin d'avoir des opportunités régulières de collaboration et de coordination. Mettez en place des directives et des protocoles clairs : assurez le bon déroulement des opérations en créant des politiques rigoureuses pour encadrer les activités suivantes :

- ❖ Gestion des incidents : documentez les étapes que les techniciens NOC doivent suivre pour gérer les incidents (par exemple, dans quelles circonstances le technicien peut prendre une décision, quand escalader la décision, quand informer ses collaborateurs, etc.).
- ❖ Solutions : décrivez les procédures de prise en charge des problèmes courants et fournissez des méthodes immédiates de gestion des urgences.
- ❖ Escalade : déterminez dans quelles conditions l'équipe doit escalader les problèmes, et à qui.
- ❖ Hiérarchisation : identifiez les types d'incidents qui doivent être traités en priorité et quel niveau de techniciens doit traiter les plus importants. Les incidents doivent être classés en fonction de l'impact qu'ils peuvent exercer sur les activités.

Disposer de protocoles établis garantit que toutes les parties prenantes sont sur la même longueur d'onde, assure la cohérence des opérations à l'échelle de l'entreprise et renforce la responsabilisation du personnel du Network Operation Center (NOC). Certes, du personnel compétent et des processus solides forment d'excellentes fondations, mais le véritable travail ne peut se faire sans les bons outils.

8-Les outils pour un NOC

L'outil dans lequel vous devez investir dépend largement des besoins de votre entreprise, mais votre Network Operation Center, ou centre d'opération du réseau, doit disposer d'un outil ou d'un groupe d'outils offrant :

Une image complète de votre infrastructure : qu'elle soit physique, virtuelle ou dans le Cloud.

L'automatisation : pour réduire les tâches répétitives, libérer le personnel de niveau 1 pour qu'il se concentre sur des problèmes plus importants et réduire le déluge d'alertes du NOC.

La gestion des tickets : pour voir les informations liées aux tickets ouverts, les tâches prioritaires et les techniciens NOC auxquels elles sont affectées, afin de résoudre rapidement les problèmes internes et externes.

Le signalement des incidents : un outil assurant des analyses visuelles et une représentation graphique des seuils, alarmes, indicateurs et tendances, facilite l'investigation des problèmes et leur documentation à des fins de référence future.

Une interface et un déploiement simples : vous voulez profiter des avantages de l'outil NOC sans attendre ni devoir traverser un déploiement long et complexe, doublé d'une courbe d'apprentissage ardue.

L'évolutivité : il faut que votre NOC puisse, en définition, gérer la croissance de votre entreprise. L'outil que vous choisirez doit vous donner une visibilité complète sur tout votre réseau et vous permettre d'analyser les données et les problèmes ainsi qu'améliorer votre réponse aux incidents au fur et à mesure.

9-Conclusion

Ce chapitre a permis d'étudier le NOC dans son ensemble qui permettra de mettre en place dans la suite notre centre NOC pour veiller à la sante du et au service du réseau. Le chapitre suivant se penchera sur le réseau d'opérateur.

CHAPITRE II : PRESENTATION D'UN OPERATEUR RESEAUX

1-Introduction

Dans cette partie, nous allons dans un premier temps comprendre les modèles conceptuels et les protocoles de communications modernes puis nous étudierons le réseau d'opérateur et ses différentes composantes. Par la suite nous nous arrêterons sur les réseaux mobiles et enfin nous parlerons de la qualité de service.

2-Protocole et Modèle de communication

2.1-Protocole de communication

Un protocole de communication est un ensemble de règles qui rendent la communication car les intervenants sont censés les respecter. C'est un langage commun que les intervenants utilisent pour se connecter l'un à l'autre afin d'échanger des informations. Ils peuvent définir une de série de paramètres dont : des paramètres physiques comme modulation, des types, de support physiques des connecteurs, le comportement de certains type de matériel, des commandes, des machines à état.

Ces protocoles sont discutés et développés par des organismes de normalisation, parmi lesquels on peut citer le protocole TCP/IP formalisé dans un document public par l'Internet Engineering Task Force (IETF) sous le nom de RFC ("Requests For Comments"). Ces documents sont désignés par un numéro de référence. Toutes les RFC ne sont pas nécessairement des normes. Leur statut dans le processus de normalisation peut être : informatif, expérimental, meilleures pratiques actuelles, voie standard ou historique. L'IETF s'appuie sur ISOC", le protocole LAN/WAN/PAN 2 mais est formalisé par d'autres organisations telles que l'IEEE (IEEE 802), et des organismes de réglementation tels que l'UIT, l'American National Standards Institute fixent les conditions d'utilisation des ondes en public Il s'agit d'organisations régies par des mandats nationaux convenus au niveau de l'Union internationale des télécommunications (UIT).Les consortiums commerciaux tels que la "Wi-Fi Alliance" assurent que des matériels de fournisseurs respectant un standard comme IEEE 802.11 soient compatibles entre eux.

2.2-Modèle de communication

Un modèle de communication en couches organise les communications entre les hôtes sous forme d'enveloppement hiérarchique. Chaque couche remplit une fonction spécifique à la communication et dispose de caractéristiques propres. Chaque couche utilise un protocole, soit un ensemble de règles de communication.

2.2.a-Modèle Open System Interconnection(OSI)

Le modèle OSI (Open Systems Interconnection) est la norme de communication réseau pour tous les systèmes informatiques. Il s'agit d'un modèle de communication entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation), qui décrit les fonctions nécessaires à la communication et la façon dont ces fonctions sont organisées, dans le but d'assurer l'interopérabilité des différents systèmes de communication grâce à des protocoles normalisés. Ce modèle divise le système de communication en couches d'abstraction. La version originale du modèle se composait de sept couches d'encapsulation, de la plus basse à la plus élevée. Chaque couche résoud certains problèmes liés à la transmission de données et fournit des services bien définis aux couches supérieures. Les couches supérieures sont plus proches de l'utilisateur et gèrent des données plus abstraites, utilisant les services des couches inférieures pour formater ces données en vue de leur transmission sur support physique. Parmi ces couches nous avons :

- La couche physique la plus basse chargée de la transmission de signaux sous forme numérique ou analogique. Son service est limité à l'émission et la réception d'un bit ou d'un train de bits continu
- La couche liaison gère l'adressage physique (adresse MAC : Media Acces Control)
- La couche Réseau se charge du parcours des données entre les équipements c'est-à-dire du routage, adressage des paquets
- La couche transport son rôle est de veiller à la communication de bout en bout entre processus. Les protocoles TCP et UDP appartiennent à cette couche
- La couche session quant à lui se concentre sur la synchronisation des échanges et les transactions, permet aussi l'ouverture et la fermeture des sessions.
- La couche présentation apporte des solutions de conversion et de chiffrement des données
- La couche application est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

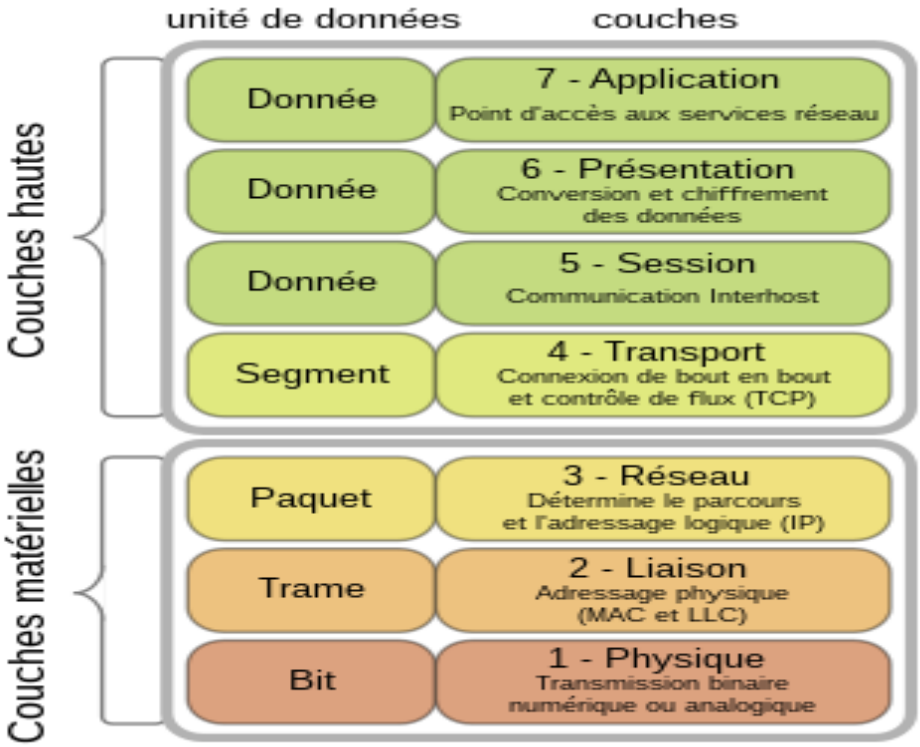


Figure 3 : Modèle OSI [16]

2.2.b-Modèle TCIP/IP

La suite de protocoles Internet est un ensemble de protocoles utilisés pour transmettre des données sur Internet. Elle est également connue sous le nom de suite TCP/IP. Il est souvent appelé TCP/IP, du nom de ses deux protocoles précédents : TCP (de l'anglais Transmission Control Protocol) et IP (de l'anglais Internet Protocol). Ils ont été inventés par Vinton G. Cerf et Bob Kahn, alors travaillant pour la DARPA, influencés par les travaux de Louis Pouzin. Le document de référence est la RFC 11222. Les trois couches supérieures du modèle OSI (Application, Présentation et Session) sont considérées comme une seule couche d'application dans TCP/IP. Étant donné que TCP/IP n'a pas de couche de session unifiée sur laquelle les couches supérieures peuvent s'appuyer, ces fonctions sont généralement exécutées par chaque application ou sont parfois ignorées.

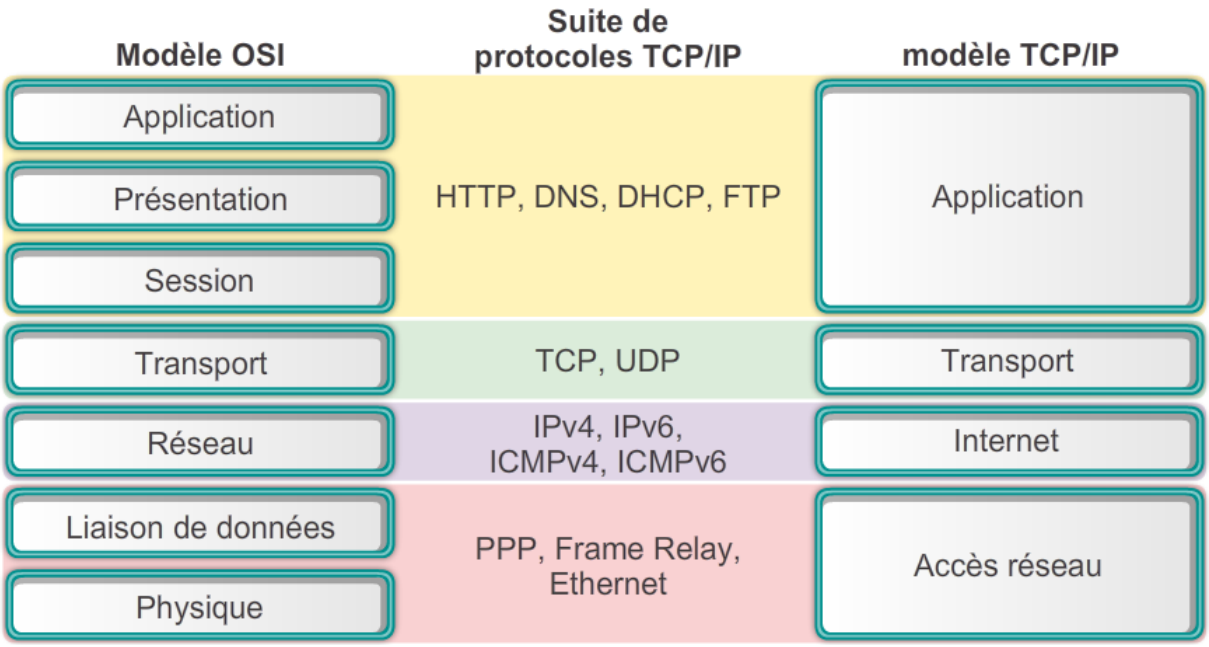


Figure 4 : modèle TCP/IP [17]

2.2.c-Transmission Control Protocol (TCP)

TCP est l'abréviation de Transmission Control Protocol (en français « Transmission Control Protocol »), et TCP est un protocole de transmission fiable en mode connexion. Dans le modèle Internet (également connu sous le nom de modèle TCP/IP), TCP se trouve au-dessus d'IP. Dans le modèle OSI, il correspond à la couche transport, avec la couche réseau et la couche session entre les deux. Les applications diffusent des données via des connexions réseau. TCP divise le flux d'octets en segments dont la taille dépend du MTU du réseau sous-jacent (couche liaison de données).

Dans son fonctionnement, TCP est constitué de trois phases : l'établissement de la connexion, les transferts de données, la fin de connexion. « La procédure de connexion suivie par TCP est composée de trois étapes connues sous le nom de « Three-way handshake »[2]. La source commence par envoyer une demande de connexion vers le destinataire. Si le destinataire accepte la connexion, elle envoie un message vers la source, qui lui répond enfin pour confirmer l'ouverture de la connexion. Une fois la connexion établie, les applications peuvent communiquer. Le protocole utilise des messages d'acquittement appelés « ACK », envoyés par la machine destinataire à la réception d'un paquet, pour détecter les erreurs de transmissions. Si le message d'acquittement correspondant à un message transmis précédemment n'est pas reçu après une certaine période de temps, le message est réémis. De la même manière, à la

[2] Three-way handshake signifie Poignée de main à trois

réception, TCP procède à un contrôle des paquets : les messages dupliqués sont ignorés et les messages désordonnés sont réordonnés avant leur transfert à l'application destinataire. Le protocole TCP adapte automatiquement le débit de transfert en procédant à un contrôle de congestion. Il utilise pour cela une fenêtre glissante de taille variable définissant le nombre maximal de paquets pouvant transiter sur le réseau avant qu'un paquet d'acquittement ne soit envoyé vers la source ».

2.2.d-User Datagram Protocol (UDP)

User Datagram Protocol (UDP) [5] est l'un des principaux protocoles de télécommunications utilisés par Internet. Il fait partie de la couche de transport du modèle OSI et, comme TCP, est la quatrième couche du modèle. Il a été défini par David P. Reed en 1980 et spécifié dans la RFC 7681.

Ce que fait ce protocole, c'est permettre de transférer des données de manière très simple (sous forme de datagrammes) entre deux entités, chacune définie par une adresse IP et un numéro de port. Contrairement à TCP (qui utilise un processus de prise de contact), aucune communication préalable n'est requise pour établir une connexion. UDP utilise la transmission sans connexion.

L'intégrité des données est assurée par une somme de contrôle sur l'en-tête. Cependant, l'utilisation de cette somme est facultative en IPv4 mais obligatoire en IPv6. Si l'hôte n'a pas calculé la somme de contrôle du datagramme transmis, la valeur de la somme de contrôle est mise à zéro. La somme de contrôle inclut également les adresses IP source et de destination.

En raison de l'absence d'un mécanisme de prise de contact, le protocole expose les programmes qui l'utilisent à d'éventuels problèmes de fiabilité du réseau ; par conséquent, il n'y a aucune garantie de protection contre la livraison, l'ordre d'arrivée ou la duplication possible des datagrammes. Si une correction d'erreur est nécessaire, les applications peuvent se tourner vers les protocoles TCP ou SCT[3]P conçus à cet effet. Par conséquent, UDP convient aux utilisations qui ne nécessitent pas de détection et de correction d'erreurs ou qui sont directement exécutées par l'application.

La nature du protocole UDP le rend adapté au transfert rapide de petites quantités de données, d'un serveur à de nombreux clients, ou dans des situations où des datagrammes sont susceptibles

[3] **protocole de transmission de contrôle de flux** (**SCTP**) est un protocole de communication de réseau informatique dans la couche de transport de la suite de protocoles Internet

d'être perdus plutôt que d'attendre une retransmission. Le DNS, la voix sur IP ou les jeux en ligne sont des utilisations typiques de ce protocole.

Comme tous les protocoles réseau, UDP est une méthode standardisée de transfert de données entre deux ordinateurs sur un réseau. Comparé à d'autres protocoles, UDP le fait d'une manière simple : il envoie des paquets (unités de transfert de données) directement à l'ordinateur cible sans établir de connexion au préalable, et sans lui demander d'être d'abord établi via un processus automatisé appelé " prise de contact ". Connexion. Ce n'est qu'une fois la prise de contact terminée qu'un ordinateur transmet réellement le paquet à l'autre ordinateur. La commande de ces colis ne vérifie pas non plus qu'ils arrivent comme prévu.

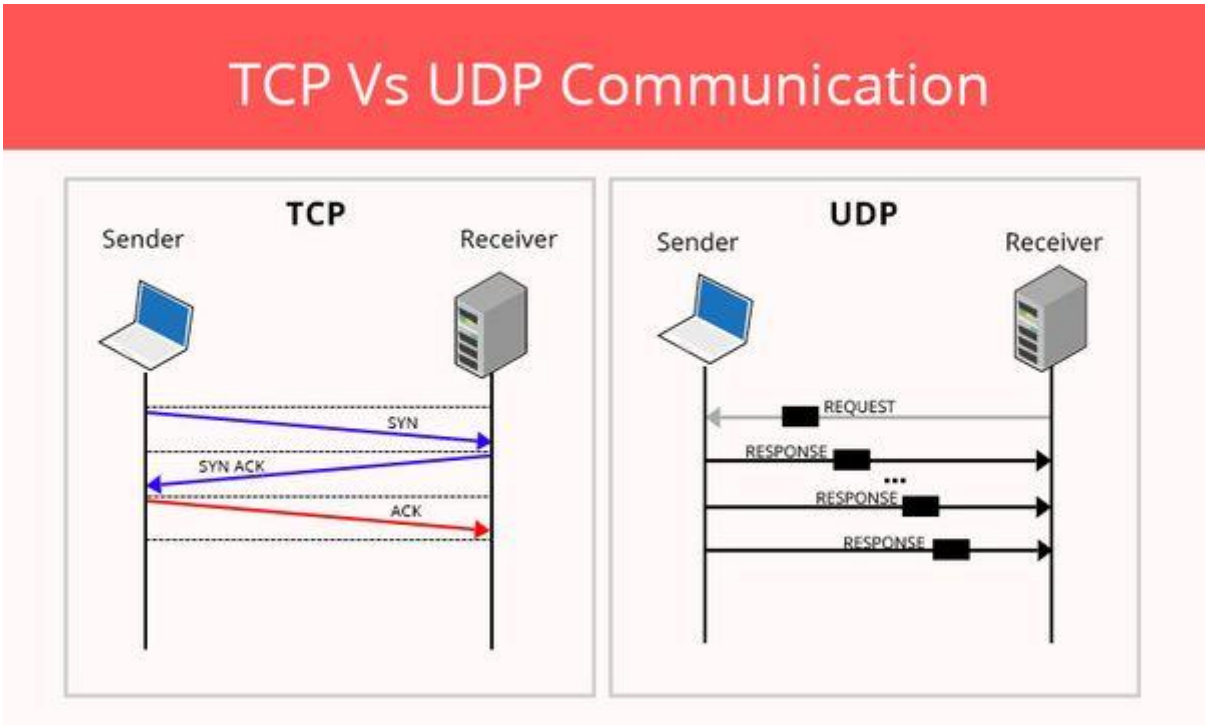


Figure 5 : TCP &UDP [18]

2.2.e-IP (Internet Protocol) et routage

Le routage IP désigne l'ensemble des méthodes de l'Internet Protocol utilisées pour router un paquet à travers un réseau. Par extension, cela désigne également l'ensemble des politiques internationales sur la configuration des réseaux, notamment internet.

Un réseau étant constitué d'une multitude de nœuds (routeurs) indépendants les uns des autres, le premier des objectifs est de permettre à deux machines de part et d'autre du réseau de communiquer en passant par un chemin raisonnablement court, si possible optimal. Il s'agit également de permettre à deux machines sur deux réseaux différents connectés via des passerelles de communiquer entre elles.

Chaque nœud du réseau possède une table de routage comportant l'adresse des autres nœuds directement connectés et éventuellement d'autres adresses (définies par l'administrateur, apprises par des protocoles de routage, etc.). Cette table permet à un routeur, à partir de l'en-tête IP, de savoir sur quel port rediriger un paquet2.

Les protocoles de routages diffèrent selon le type de réseau et la taille de ceux-ci, citons notamment :

- Protocoles à vecteur de distances (RIP, IGRP, EIGRP, Babel...) sont des protocoles permettant de construire des tables de routages où aucun routeur ne possède la vision globale du réseau, la diffusion des routes se faisant de proche en proche. Le terme « vecteur de distances » vient du fait que le protocole manipule des vecteurs (des tableaux) de distances vers les autres nœuds du réseau. La « distance » en question est le nombre de sauts (hops) permettant d'atteindre les routeurs voisins.
- Protocoles à état de liens OSPF et IS-IS, pour le routage au sein d'un système autonome.
- Protocole à vecteur de chemin : Border Gateway Protocol, pour le routage entre systèmes autonomes.

Lors de la réception d'un paquet, le routeur va lire l'en-tête de la troisième couche du modèle OSI afin d'en extraire l'adresse IP destination. À partir de sa table de routage, il affecte le paquet à la file d'attente de sortie associée au port correspondant à l'adresse IP ou au préfixe le plus proche / le plus spécifique s'il n'y a pas de correspondance exacte. Il effectue également d'autres opérations, tel que la décrémentation du TTL (si le TTL tombe à zéro, le paquet est supprimé et cette suppression est signalée à l'émetteur par un message ICMP).

3-Réseaux d'operateur

La nature [6] du protocole UDP le rend adapté au transfert rapide de petites quantités de données, d'un serveur à de nombreux clients, ou dans des situations où des datagrammes sont susceptibles d'être perdus plutôt que d'attendre une retransmission. Le DNS, la voix sur IP ou les jeux en ligne sont des utilisations typiques de ce protocole.

Comme tous les protocoles réseau, UDP est une méthode standardisée de transfert de données entre deux ordinateurs sur un réseau. Comparé à d'autres protocoles, UDP le fait d'une manière simple : il envoie des paquets (unités de transfert de données) directement à l'ordinateur cible sans établir de connexion au préalable, et sans lui demander d'être d'abord établi via un processus automatisé appelé " prise de contact " Connexion. Ce n'est qu'une fois la prise de contact terminée qu'un ordinateur transmet réellement le paquet à l'autre ordinateur. La

commande de ces colis ne vérifie pas non plus qu'ils arrivent comme prévu.

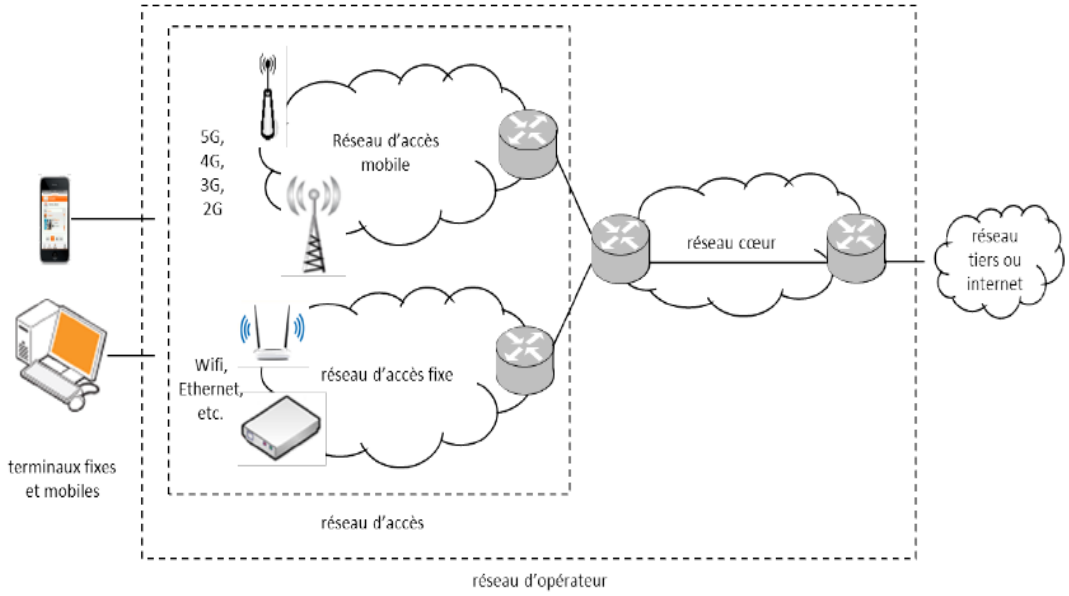


Figure 6 : Un réseau D'opérateur [21]

3.1-Réseaux cœur

Tous les réseaux [7] de télécommunications sont organisés autour d'un noyau central appelé réseau central. Les installations et équipements utilisés dans le réseau central (également appelé backbone) sont les routeurs et les commutateurs. Les technologies utilisées sur ces équipements centraux sont principalement celles opérant sur la couche réseau et la couche liaison de données. Il se compose de plusieurs auxquels nous pouvons nous référer

- **Agrégation** : Le plus haut niveau d'agrégation peut être observé dans le réseau d'un fournisseur de services. Ensuite, dans la hiérarchie des nœuds centraux, se trouve le réseau de distribution, puis le réseau périphérique. L'agrégation est une méthode permettant de combiner plusieurs connexions réseau en parallèle pour augmenter le débit au-delà de ce qu'une seule connexion peut prendre en charge. Il permet également d'assurer la redondance en cas de défaillance de la liaison du centre de données.
- **L'authentification** : Elle permet de déterminer si l'utilisateur qui demande un service à un réseau est autorisé à accomplir cette tâche dans le réseau. Les équipements du réseau central ont la capacité de décider si l'utilisateur dispose des privilèges nécessaires à son exécution. Le bon fonctionnement de l'authentification est au centre de la sécurité du réseau.
- **Facturation** : il traite et consolide les données de facturation créées par plusieurs nœuds de réseau. L'équipement de cœur de réseau est capable de gérer la collecte et le

traitement des données de charge générées par tous les différents nœuds du réseau. Chaque paquet de données passant par le réseau central est tarifé en conséquence.

- **Contrôle d'appel ou communication** : le contrôle d'appel ou les fonctions de commutation déterminent le déroulement futur d'un appel en fonction du traitement de la signalisation d'appel. Selon le numéro appelé, la fonction de commutation peut décider d'acheminer l'appel vers un utilisateur du réseau de cet opérateur avec un niveau de portabilité plus ou moins élevé. Cela augmente le niveau de qualité de service.
- **Invocation de service** : le réseau central effectue des tâches d'invocation de service pour ses utilisateurs. Cette exécution peut être effectuée par l'utilisateur dans le cadre d'une activité spécifique (renvoi d'appel) ou de manière inconditionnelle (appel en attente). L'exécution du service peut ne pas être une fonction exclusive du réseau central. Certains sous-réseaux ou nœuds tiers peuvent en effet participer à l'exécution du service.
- **Passerelles** : elles sont utilisées dans le réseau central pour accéder à d'autres réseaux. Les capacités des passerelles dépendent du type de réseau auquel elles sont connectées. La sécurité du réseau est une préoccupation importante lors de la configuration d'une passerelle. Il peut être amélioré en utilisant un VPN.

3.2-Réseaux d'accès

Le réseau d'accès [8] d'un opérateur est composé d'un réseau d'accès cellulaire pour gérer la communication des utilisateurs mobiles et le réseau d'accès fixe qui permet la connexion des réseaux résidentiels des clients.

3.2.a-Réseaux d'accès mobile

C'est un réseau qui permet la communication entre les utilisateurs mobiles. Appelé aussi RAN qui signifie Radio Access Network en anglais qui fournissent des services de radiocommunications. Il est charge de véhiculer les flux des utilisateurs mobiles jusqu'au réseau cœur mais aussi leur connectivite sur le réseau en toute mobilité.

3.2.b-Réseau d'accès fixe

Le réseau d'accès fixe contrairement aux réseaux d'accès mobile se charge d'offrir la connectivité aux clients à l'aide des équipements tels que câble Ethernet, wifi, fibre optique dont le but est d'acheminer les flux vers le réseau cœur. C'est le réseau filaire dont les extrémités en cuivre ou en fibre optique sont tirées jusqu'au plus proche de l'utilisateur, de manière à ce qu'il puisse y connecter ses propres points d'accès tels qu'un modem Wifi. Les technologies utilise pour ce réseau sont au niveau de la couche physique du modèle OSI avec Digital

Subscriber Line (DSL) pour les cuivres et Fiber to the Home/Building/Desktop/etc. (FTTx) pour la fibre.

4-Réseaux mobile

Les réseaux [9] mobiles reposent sur une variété d'appareils, qui remplissent tous des fonctions spécifiques. Les réseaux mobiles sont basés sur la division du territoire en zones appelées cellules. Au centre de la cellule, une antenne (ou ensemble d'antennes) assure la liaison entre le terminal mobile et le réseau. La communication entre le téléphone mobile et l'antenne s'effectue par ondes radio puis via un réseau filaire vers le réseau mobile, lui-même connecté à un réseau de téléphonie fixe ou mobile ou à un réseau de transmission de données (Internet, Intranet...).

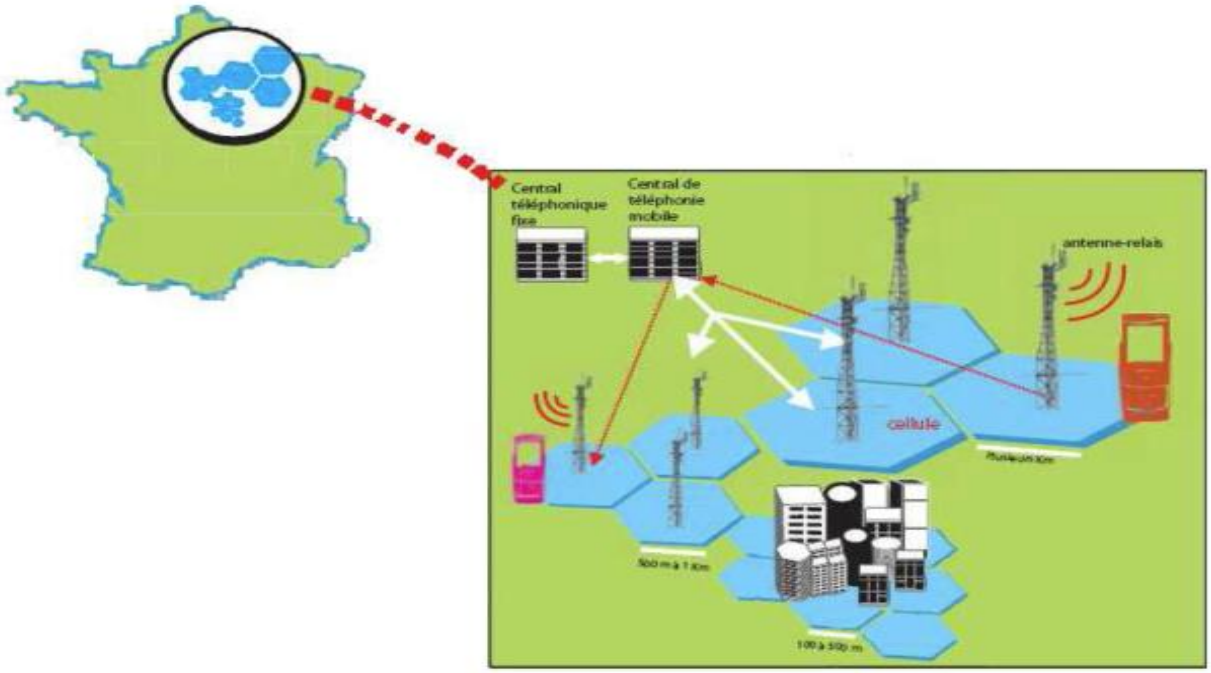


Figure 7 : Réseaux mobile [19]

« Chaque antenne-relais gère un nombre limité d'appels simultanés. Plus une zone est peuplée, plus il faut d'antennes pour absorber le trafic et assurer une bonne qualité de service. En ville, le maillage du réseau est donc plus serré : on trouve une antenne tous les 300 mètres environ, à la campagne tous les 2 km.

Quand une zone pavillonnaire ou un centre commercial se construit, le réseau mobile se déploie. La capacité du réseau mobile est augmentée aux abords des équipements qui subissent des pics ponctuels de fréquentation : stades, palais de congrès, gares, aéroports, etc. Un même site peut accueillir plusieurs antennes. La couverture réseau des axes de communication est une priorité,

notamment pour pouvoir donner l'alerte en cas d'accident de la route. Sur les lignes TGV la couverture réseau est stratégique : l'internet mobile est très apprécié par les travailleurs nomades.

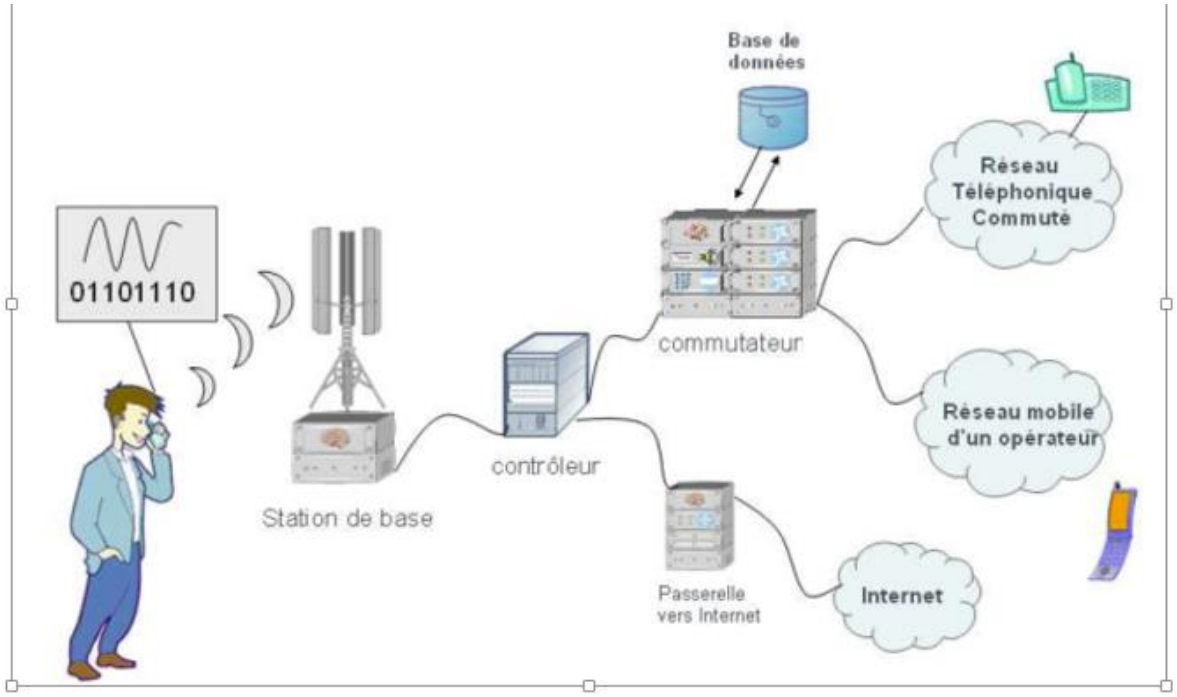


Figure 8 : les Différents étapes [20]

Station de base : équipement de transmission radio des réseaux mobiles. Elle est constituée d'une antenne-relais et d'une armoire électronique chargée de la gestion des communications par ondes radio.

Il y en une par cellule, et tous les mobiles situés dans la cellule y sont connectés. (BTS pour le GSM et le GPRS – Node B pour l'UMTS)

- Contrôleur : est l'organe intelligent : il alloue les canaux et gère les déplacements des clients entre les zones de couvertures cellulaires (BSC pour le GSM et le GPRS – RNC pour l'UMTS)
- Commutateur : assure les liaisons des communications. Il interagit avec une base de données dans laquelle sont enregistrées les infos liées aux abonnées (numéro, option, localisation…)
- Passerelle vers Internet : passerelle d'interconnexion entre le réseau de paquet mobile (GPRS UMTS) et les réseaux IP externes). La 4 G utilise le réseau IP ».

Plusieurs générations de réseau d'accès radio se sont succédé. De légères modifications de l'architecture et l'utilisation de bandes de fréquence différentes ont permis d'améliorer au fil des générations la qualité de service. Ainsi, on a connu la 1G, la 2G, la 3G, la 4G et maintenant la 5G qui comporte déjà des exigences plus fortes de qualité de service et de résilience permettant d'accueillir notamment les nouveaux réseaux d'objets communément appelés Internet of Things (IoT).

5-Qualité de service

5.1-Définition de la qualité de service

La Qualité de Service [10] est un élément important dans le fonctionnement des réseaux et des services, notamment aux yeux des utilisateurs. La qualité de service (QoS en anglais quality of service) fait référence à la capacité de fournir un type de trafic donné dans des conditions favorables, notamment la disponibilité, le débit, le nombre de transferts, la gigue, la perte de paquets, etc. La Qualité de Service est un concept de gestion visant à optimiser les ressources d'un réseau (gestion des systèmes d'information) ou d'un processus (logistique) et à garantir le bon fonctionnement des applications critiques d'une organisation. La qualité de service peut fournir aux utilisateurs une vitesse et des temps de réponses différenciés par application (ou activité) sur la base de protocoles appliqués au niveau de la structure. Ainsi, il permet aux prestataires de services (services réseaux des entreprises, opérateurs, etc.) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leur infrastructure IP.

« On a tendance à utiliser le mot « QoS » dans des situations différentes où elle ne représente pas exactement la même chose. Néanmoins, un modèle de QoS [ITU-T, 2001] proposé par l'UIT-T unifie les définitions et clarifie les différents types de QoS que l'on peut observer :

- QoS intrinsèque : La QoS intrinsèque correspond au type de QoS spécifié par la définition IETF. Il s'agit de la QoS dérivée de la capacité du réseau.
- QoS offerte : La QoS offerte correspond au niveau de service fourni par le fournisseur au client en fonction de la situation.
- QoS atteint : Malgré une certaine volonté et un cahier des charges pour fournir un certain niveau de qualité, la QoS peut être limitée dans certaines limites en raison de divers facteurs. Le niveau auquel tout est atteint est appelé QoS atteint.
- QoS Désirée : La QoS Désirée est la QoS qui répond aux besoins du client, dans ce cas la QoS établie dans son contrat de service ou Service Level Agreement (SLA) 3.

- QoS perçue : la QoS perçue, comme son nom l'indique, est ce que les clients perçoivent en fonction de la QoS atteinte, de la QoS requise et de divers facteurs externes qui affectent leur expérience. Par conséquent, il est similaire à la qualité d'expérience (QoE).

5.2-QOS et QOE

Le QOE peut être défini comme la mesure dans laquelle un utilisateur apprécie ou est fatigué d'une application ou d'un service. Elle est due à la satisfaction des attentes de l'utilisateur quant à l'utilité et/ou l'approbation de l'application ou du service, compte tenu de la personnalité de l'utilisateur et de son statut actuel. QOS est un moyen qui consiste en des mesures techniques objectives qui qualifient les performances du réseau, tandis que QOE consiste en des mesures subjectives qui dépendent de l'utilisateur et montrent la satisfaction de ce dernier.

5.3-Paramètre QOS

La qualité [11] de service peut être affectée avec certaines fonctionnalités qui dégradent la perception de l'utilisateur comme : Fiabilité, Sécurité, Politique de routage, Ingénierie de trafic. Mais la QOS est mesurée par des paramètres à savoir la bande passante, le débit, la latence, le taux de perte et la gigue.

5.3.a-La bande passante

La bande passante, passe-bande chez nos amis anglophones, désigne dans le monde de l'informatique le débit binaire d'une voie de transmission. Elle représente la quantité d'informations pouvant être transmises simultanément sur une voie de transmission, et s'exprime en bits/seconde.

Aujourd'hui, le terme de bande passante est principalement utilisé dans la mesure de la qualité et des performances des accès à Internet à haut débit. En choisissant de tester leur bande passante en ligne, les internautes peuvent identifier très facilement la qualité de leur accès à Internet et la rapidité avec laquelle ils accèdent à des informations en ligne.

Son seuil a été fixé à 8 Mb/s. On peut dire qu'il s'agit d'un minimum syndical : de quoi assurer une navigation correcte sur Internet ou regarder la télé ou des vidéos en streaming sur Netflix, Youtube ou MyCanal en haute définition (HD).

Une méthode de mesure de la bande passante consiste à transférer un ou plusieurs fichiers de taille connue et de mesurer le temps nécessaire au transfert. Le résultat est converti en bps, en divisant la taille des fichiers par le temps nécessaire au transfert.

5.3.b-La latence

En informatique, la latence (ou délai de transit, ou retard) est le délai de transmission dans les communications informatiques. Il désigne le temps nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau. Et on a une bonne qualité de service si le délai est inférieur à 150ms. La latence ou délai est composé du délai applicatif et du délai réseau

- Le délai applicatif est le délai introduit par le traitement applicatif
- Le délai réseaux qui est le temps qui s'écoulé entre la transmission sur le lien du premier bit et l'arrivé du dernier bit d'un paquet à la destination
- Le délai de transmission est temps nécessaire pour transmettre un paquet sur le médium (filaire ou sans fil)
- Délai de traitement des paquets : le temps écoulé à cause des traitements du paquet sur les équipements intermédiaires
- Délai de propagation : le temps de propagation du signal sur le réseau

5.3.c-Le débit

« C'est est la quantité de trafic maximale pouvant être transportée par un flux sur le lien considéré sur une période de mesure. C'est la raison pour laquelle on parle souvent de débit moyen sur une période. Cette notion est dépendante de plusieurs facteurs tels que le type de trafic transitant sur le lien (UDP ou TCP par exemple). S'il s'agit d'un trafic TCP, le débit peut aussi dépendre du nombre de connexions TCP, de la taille des buffers TCP, de la congestion le long du chemin de retour pour l'envoi des paquets ACK ou de l'algorithme utilisé pour l'implémentation de TCP. Un débit calculé sur une connexion TCP qui a saturé le lien sur la période de mesure va donc refléter la quantité de données que l'on peut faire transiter par unité de temps sur le lien quand il se trouve dans les mêmes conditions que lors de la période de mesure »

5.3.d-Le taux de perte

Le taux de perte en anglais PLR (Packet Loss Rate) est le pourcentage de de paquets perdus lors de la traversée du réseau de la source à la destination. Cela est cause par une congestion (dépassement de la capacité de traitement de l'interface par un flux d'arrive), échec d'acheminement d'un paquet sur un nœud, changement de la topologie. Comme pour le délai, le taux de perte influence négativement la qualité de service des applications temps réel comme la communication audio ou vidéo. Bien qu'ils intègrent ce problème dans leur conception, des taux de pertes élevées dégradent la qualité perçue par l'utilisateur (dégradation de la qualité

vidéo ou audio, coupures intempestives). En termes de qualité de service un taux de perte inférieur à 0,1% garantit une bonne QOS

Pour la mesure du taux de perte il est recommandé d'avoir :

- Intervalle maximal de calcul ➔ 5mn
- Intervalle moyen d'émission des paquets ➔ 200ms
- Les taux de pertes sont exprimés en pourcentage avec une précision de 0.1%
- Un taux de perte est capturé tous les périodes

5.3.e-La gigue

La gigue (en anglais jitter) est la variation de la latence au fil du temps. Il ne faut pas la confondre avec la gigue en électronique qui recouvre une notion différente. Plus précisément, la gigue est la différence de délai de transmission de bout en bout entre des paquets choisis dans un même flux de paquets, sans prendre en compte les paquets éventuellement perdus. Elle peut avoir plusieurs origines :

- Délai de traitement au niveau des files d'attentes
- Délai de traitement au niveau des équipements
- Chemins d'acheminement

Une gigue inférieure à 50ms donne une bonne QoS même pour des applications sensibles à la gigue.

6-Conclusion

En somme, cette partie a permis de comprendre les éléments et modèles de communications et des protocoles dans un réseau, mais également de voir comment est constitué un réseau d'opérateur afin de répondre aux besoins des clients en termes de qualité de service.

CHAPITRE III : MISE EN PLACE DU NOC POUR UN RESEAU D'OPERATEUR

1-Introduction

Dans ce chapitre, nous allons dans un premier temps définir une solution NOC pour un réseau d'opérateur, ensuite étudier les outils pour notre NOC, enfin de parler de notre environnement de travail avec une solution locale.

2-NOC d'un operateur

Un réseau dans ce monde actuel est en perpétuel danger. C'est pour cela qu'il est important de veiller sur ce réseau, plus particulièrement à celui des opérateur dont l'objectif est de mettre en place, de gérer et d'exploiter des infrastructures constituant une bonne partie des réseaux de télécommunication, en respectant certaines normes internationales et locales. Mais aussi de fournir une bonne qualité de service aux clients malgré les menaces dont peut citer la fiabilité, la sécurité, l'ingénierie du trafic et la politique de routage. Face à cela, il est important d'étudier les différentes solutions de protections qui puissent surveiller notre réseau en temps réel afin d'apporter une solution à chaque problème avec efficacité et efficient sans affecter notre réseau d'opérateur en terme qualité de service. Ainsi la mise en place d'un NOC (Network opération center) est un lieu central de surveillance d'analyse de données et gestion d'incident permettant de mieux gérer notre réseau d'opérateur contre les menaces empêchant d'atteindre les objectifs du réseau.

Un réseau d'opérateur est composé du réseau d'accès et du réseau de cœur qui est connecté à internet et pour surveiller ce réseau, nous allons mettre place notre NOC pour couvrir l'infrastructure de ce réseau de façon à être connecté au routeur d'intermédiaire entre internet et notre réseau d'opérateur comme illustrer dans notre schéma ci-dessous.

Pour notre architecture nous allons connecter notre NOC au niveau du routeur qui nous lie à internet pour surveiller les données qui entrent mais en même temps notre réseaux d'opérateur.

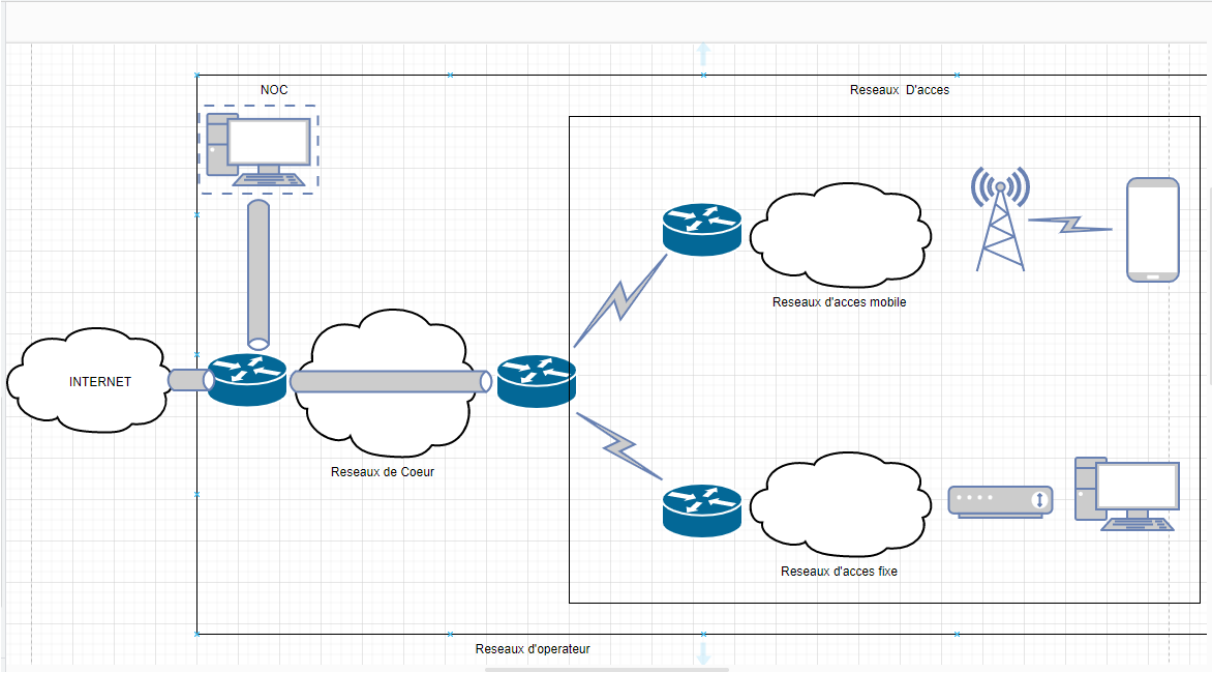


Figure 9 : architecture du NOC d'un réseau operateur

3-Les outils pour le NOC

La mise en place d'un NOC implique le déploiement et l'intégration des quatre composants à savoir le système de supervision qui permettra d'avoir une vue de notre réseau c'est à dire les différents équipements, le système de ticketing dont le but est informer à partir des tickets les incidents au technicien du NOC afin de réagir aux problèmes, le système de visualisation intégré à l'outil de de supervision afin d'afficher des données à l'écran et le système de gestion des incidents. Pour mettre en place un bon NOC il nous fait choisir pour chaque système un bon outil afin que le centre d'operation réseau puisse jouer so rôle à savoir de veiller à la disponibilité et à la santé du réseau.

3.1-Le système de supervision

Pour la supervision nous pouvons citer plusieurs outils qui sont zabbix, nadios, Opmanager, PRTG network monitor, Centreon … Parmi ces outils nous allons comparer nadios, zabbix qui sont les plus utilise afin d'en choisir une pour notre réseau d'opérateur.

Tableau 1 comparaison Zabbix et Nadios

	Zabbix	Nadios
Présentation	❖ Multiplateformes. ❖ Moteur en C, interface web utilisateur en PHP, base de données SQL (MySQL, Oracle…) ❖ Configuration centralisée sur une même Interface graphique. Peut monitorer de 3 manières : ❖ Lancement d'un processus sur les machines à monitorer pour collecter des données locales, grâce à l'agent Zabbix. ❖ Requêtes SNMP. ❖ Check externes qui sert à tester les services réseaux (tests limités à des pings ou test de protocoles).	❖ Conçu pour les plateformes Unix. ❖ Moteur en C, perl, sharp…, interface web en PHP, base de données SQL. ❖ Configuration plus ou moins complexe ❖ Peut monitorer de 2 manières : ❖ L'utilisation des journaux d'exploitation par l'envoie des évènements issus des fichiers log en temps réel vers un serveur central offrant les informations nécessaires à la supervision. ❖ Supervision active des services et Infrastructure qui nous permet de garder l'historique des performances
Fonctionnalité	❖ Offre une interface web de consultation et d'administration. ❖ Surveillance des ressources des serveurs (CPU, mémoire…). ❖ générer des graphes et des écrans ❖ Supervise des équipements SNMP. ❖ Gère les pannes et les performances ❖ capable de faire du monitoring SNMP et IPMI ainsi que de la découverte de réseau	❖ Offre une interface web basée sur les CGL avec gestion des droits pour la consultation. ❖ Génère des rapports de surveillance. ❖ Surveillance des ressources des serveurs (CPU, mémoire…). ❖ Surveillance des services réseaux.
Avantages	❖ Multiplateforme. ❖ Utilise peu de ressources ❖ Configuration et utilisation aisée. ❖ Interface vaste mais claire. ❖ Richesse des sondes et tests possibles (Supervision d'applications Web) ❖ Réalisation de graphiques, cartes ou screens ❖ Configuration par l'interface graphique. ❖ Mise à jour de la configuration via l'interface Web de Zabbix.	❖ Des plugins qui étendent les possibilités de Nagios. ❖ Des plugins permettent aux utilisateurs de développer facilement ses propres vérifications de services. ❖ La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (Alerte par courrier électronique, SMS, etc…).

	❖ Surveillances des sites web : temps de réponse, vitesse de transfert... ❖ les agents Zabbix sont assez légers (en C).	
Inconvénients	❖ L'agent Zabbix communique les données en claire nécessité de sécuriser les données. ❖ Peu d'interfaçage avec d'autres solutions commerciales.	❖ Difficile à installer et à configurer ❖ Dispose d'une interface compliquée ❖ Ne permet pas d'ajouter des hosts via Web ❖ Besoin d'un autre outil comme CACTI pour faciliter sa configuration ❖ Pas de représentations graphiques ❖ Les mises à jour de la configuration se font en mode « lignes de commandes » et doivent être réalisées côté supervision comme côté serveur à superviser.

Choix : la supervision est un élément important pour un NOC c'est pour cela à travers cette comparaison nous allons retenir zabbix comme outil de monitoring car étant facile à paramétrer et conçu pour les grandes infrastructures mais aussi il est puissant.

3.2-Système de ticketing

Un autre composant du NOC le ticketing qui permet de renseigner à l'équipe noc des diffèrent incident. Pour les outils de ticketing nous allons voir ceux qui ont plus de fonctionnalité en gestion d'incident et la possibilité d'avoir des rapports d'activité. Ainsi nous allons nous focaliser sur deux outils à savoir l'OTRS et le Request Tracer.

Tableau 2 comparaison entre OTRS et Request Tracer

	OTRS	RT (Request Tracer)
Présentation	Open source Ticket Request System est un système moderne et flexible de gestion des tickets	Une solution de ticketing éditée par Best Practical développée en perl
Fonctionnalité	❖ Possibilité d'ouvrir un ticket soit via l'interface soit par mail	❖ Création de tickets par mail, formulaire en ligne ❖ Création de requêtes de recherches avec possibilité de sauvegarde de celles-ci.

	❖ Personnalisation de l'interface via thème ❖ Gestion d'historique des tickets ❖ Gestion de priorités ❖ Gestion du temps et de la facturation ❖ Agent de création d'actions automatiques par actions planifiées ❖ Fonctionnalité de Workflow ❖ Multi langage dont le Français ❖ Répondeur automatique pour les tickets ouverts par mail	❖ Réponse automatique lors de l'ouverture d'un ticket, ou à la réception avec gestion de la personnalisation des mails via Template ❖ Possibilité d'ajout de champs personnalisés ❖ Gestion fines des permissions ❖ Gestion d'historique ❖ Gestion de la criticité
Avantages	❖ Centralité des demandes ❖ Chaque ticket a un numéro unique ❖ L'affectation d'un ticket à un service permet à l'équipe la plus qualifié de le résoudre.	❖ très flexible ❖ développement actif ❖ interface web ou pilotage par mail
Inconvénients	❖ C'est une application de base ❖ Une configuration très longue ❖ Des bugs parfois	❖ Difficile à installer ❖ Prend du temps pour comprendre le fonctionnement

Choix : A travers cette comparaison nous optons pour le choix d'OTRS du fait de sa gestion des priorités mais aussi la fonctionnalité statistique.

3.3-Système de visualisation

La visualisation est moyenne d'avoir en temps réel les données dans un écran en intégration avec l'outil de supervision. Parmi les outils de visualisations on peut citer Grafana, Kibana dont nous ferons l'objet d'une comparais afin de choisir celui qui nous convient.

Tableau 3 comparaison entre Grafana & Kibana

	Grafana	kibana
Présentation	Grafana est un logiciel libre sous licence GNU Affero General Public License Version 3 qui permet la visualisation de données. Il permet de réaliser des tableaux de bord et des graphiques depuis plusieurs sources dont des bases de données temporelles comme Graphite, InfluxDB et OpenTSDB	Kibana est un greffon de visualisation de données pour Elasticsearch publié sous la licence libre Apache version 2. Il fournit des fonctions de visualisation sur du contenu indexé dans une grappe Elasticsearch.
Fonctionnalité	❖ Une analyse de données avancée. ❖ Une visualisation des données dans une variété de types de tableaux, de tableaux et de cartes. ❖ La création un tableau de bord log analytique complet.	❖ Une présentation de graphes temporels basés sur des métriques spécifiques telles que l'utilisation des CPU et des E/S. ❖ Grafana prend en charge de nombreux backends de stockage différent. ❖ Grafana possède un éditeur de requêtes spécifique qui est personnalisé pour les fonctionnalités et les capacités qui sont incluses dans cette source de données
Avantages	Puissant, élégant très extensibles, riche par rapport aux options de visualisation	Surveillance sans agent des périphériques de réseau Outils de réduction du bruit configurables et système d'alerte
Inconvénients	Nécessite du temps pour comprendre et pouvoir visualiser les données	Fonctionnalités payantes (export PDF,...) Pas de Tableaux de bord prédéfinis prêts à l'emploi Coût supplémentaire pour avoir un stockage conséquent pour conserver la donnée

Choix : les deux outils se valent et sont très important dans le traitement des données mais nous allons opter Grafana afin d'enrichir notre représentation des données par des graphes et les écrans déjà configurés avec zabbix.

4-Environnement de travail

4.1-La solution locale

Pour illustrer notre NOC nous allons mettre en place au niveau local en utilisant l'outil gns3 (Graphical network simulator) avec 3 machines virtuels ou l'une est installé notre NOC et les deux autres seront les machines à surveiller dont l'une des machines est Linux ou est installé Asterisk (est un autocommutateur téléphonique privé (PABX) open source pour systèmes UNIX). Il permet, entre autres, la messagerie vocale, les files d'attente, les agents d'appels, les musiques d'attente, les mises en garde d'appels, la distribution des appels et la gestion de conférences) pour voir les résultats concernant la surveillance téléphonique et l'autre est une machine Windows ainsi que les routeurs qui les relient.

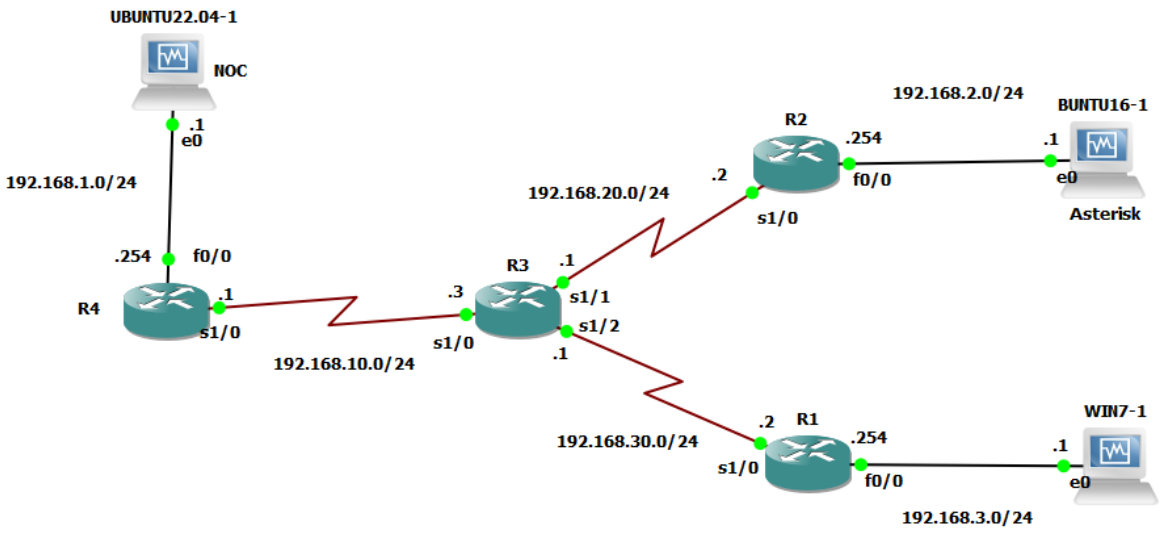


Figure 10 : Mise en place d'un NOC locale

4.2-Installation et configuration des outils choisis

4.2.a-Installation l'outil de supervision : zabbix

4.2.a.1-Définition

Zabbix a été créé par Alexei Vladishev, [12] et est actuellement activement développé et soutenu par ZABBIX SIA. Zabbix est une "entreprise-class open source Distributed monitoring solution". Zabbix est un logiciel qui supervise de nombreux paramètres réseaux ainsi que la santé et l'intégrité des serveurs. Zabbix utilise un mécanisme de notification flexible

qui permet aux utilisateurs de configurer une base d'alerte e-mail pour pratiquement tous les événements. Cela permet une réponse rapide aux problèmes serveurs. Zabbix offre un excellent reporting et des fonctionnalités de visualisation de données basées sur les données stockées.

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 Compagnie.

Installation de zabbix

Pour installer Zabbix il suffit d'aller au niveau site officiel de zabbix ou il y a plusieurs versions sont proposés et pour chaque version les systèmes disponibles. Mais nous allons choisir la version 6.2 et le système 22.04 d'ubuntu.

Tableau 4 composant d'installation zabbix

Version	Système	Version	Composant Zabbix	Base de données	Serveur web
Zabbix 6.2	Ubuntu	22.04 Jammy	Server, Front end, Agent	PostgreSQL	apache

Pour installer zabbix il faut préalable installer ubuntu 22.04 en mode virtuel mettre à jour le système Ubuntu avant de commencer les commandes d'installation de Zabbix

Nous allons télécharger le dépôt de zabbix avec la commande

#wgethttps://repo.zabbix.com/zabbix/6.2/ubuntu/pool/main/z/zabbix-release/zabbixrelease_6.2-4+ubuntu22.04_all.deb

 # dpkg -i zabbix-release_6.2-4+ubuntu22.04_all.deb

 # apt update

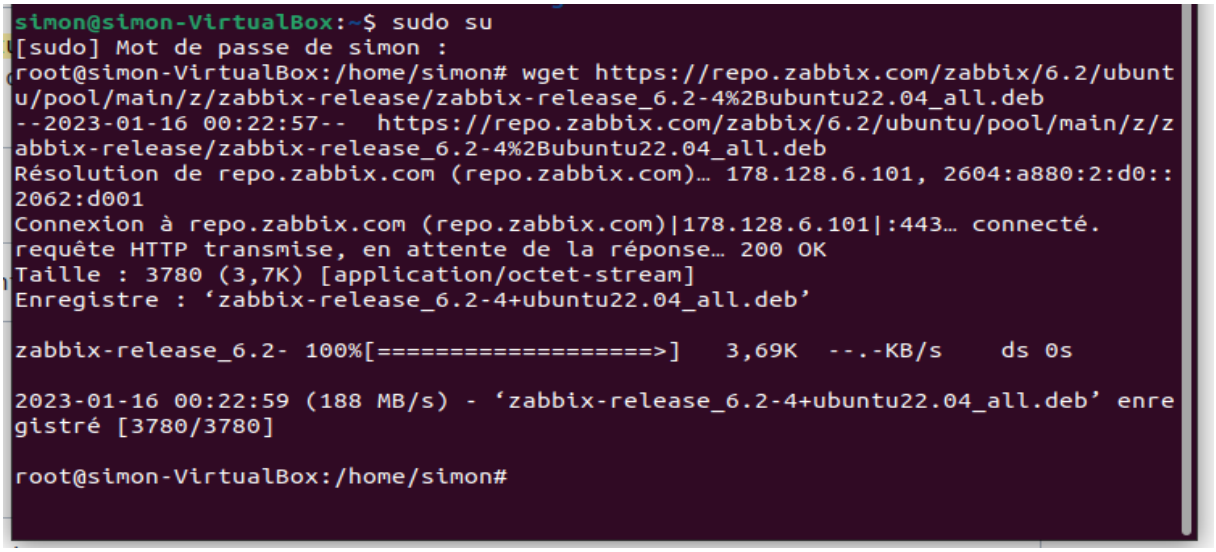


Figure 11: téléchargement de l'outil zabbix

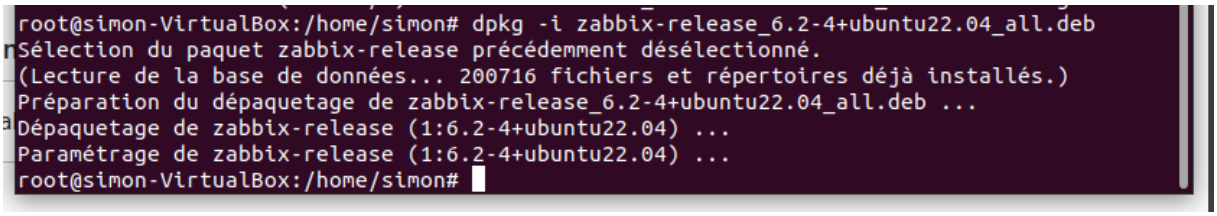


Figure 12: désarchivage de zabbix

Apres cela il faut télécharger les composants de Zabbix : **# apt install zabbix-server-pgsql zabbix-frontend-php php8.1-pgsql zabbix-apache-conf zabbix-sql-scripts zabbix-agent**

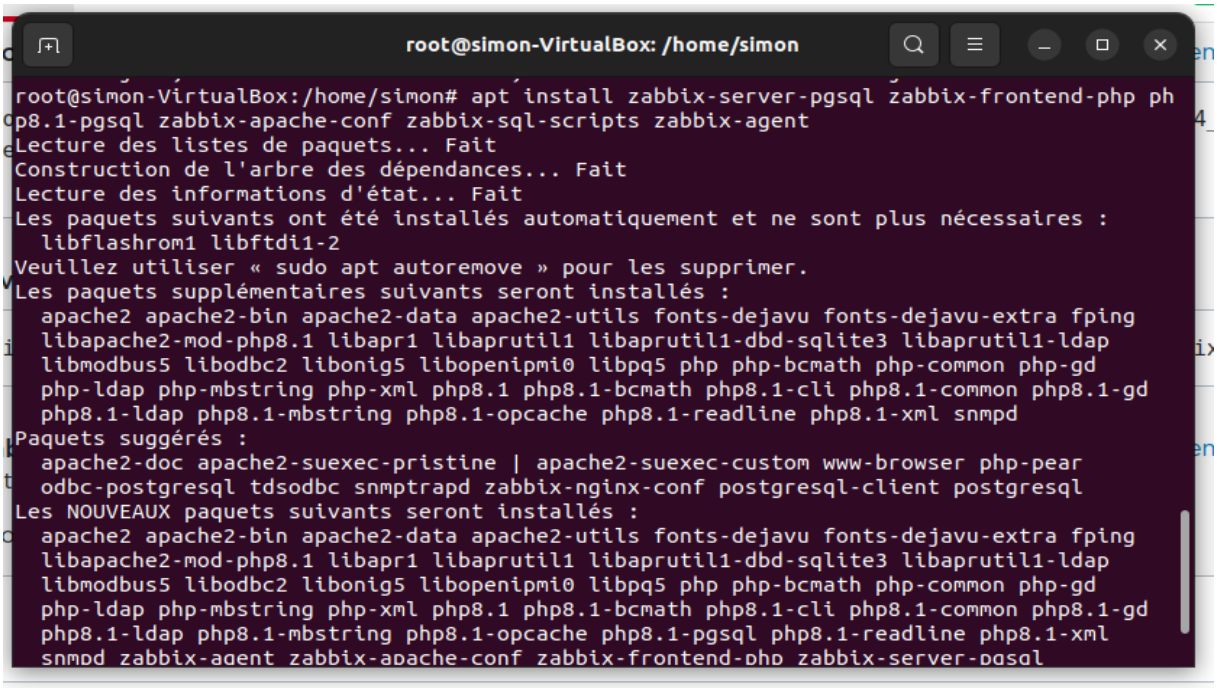


Figure 13: installation de zabbix serveur, agent zabbix, apache

Nous allons maintenant créer notre base de données

 # sudo -u postgres createuser --pwprompt zabbix

 # sudo -u postgres createdb -O zabbix zabbix

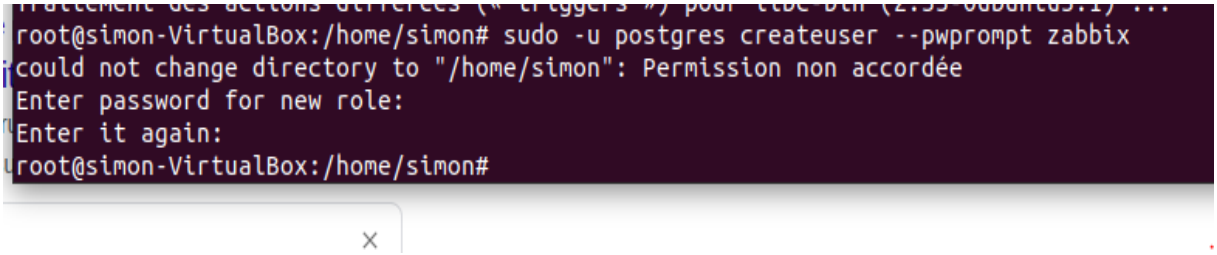
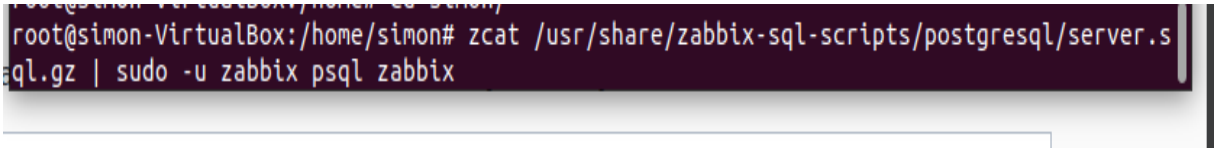


Figure 14: création de la base de données

Sur le serveur hôte de Zabbix, importez le schéma et les données initiales. Vous serez invité à saisir votre mot de passe nouvellement créé.

 # zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix



Configuration de la base de données pour éditer le fichier **/etc/zabbix/zabbix_server.conf**

On définit le mot de passe du serveur zabbix

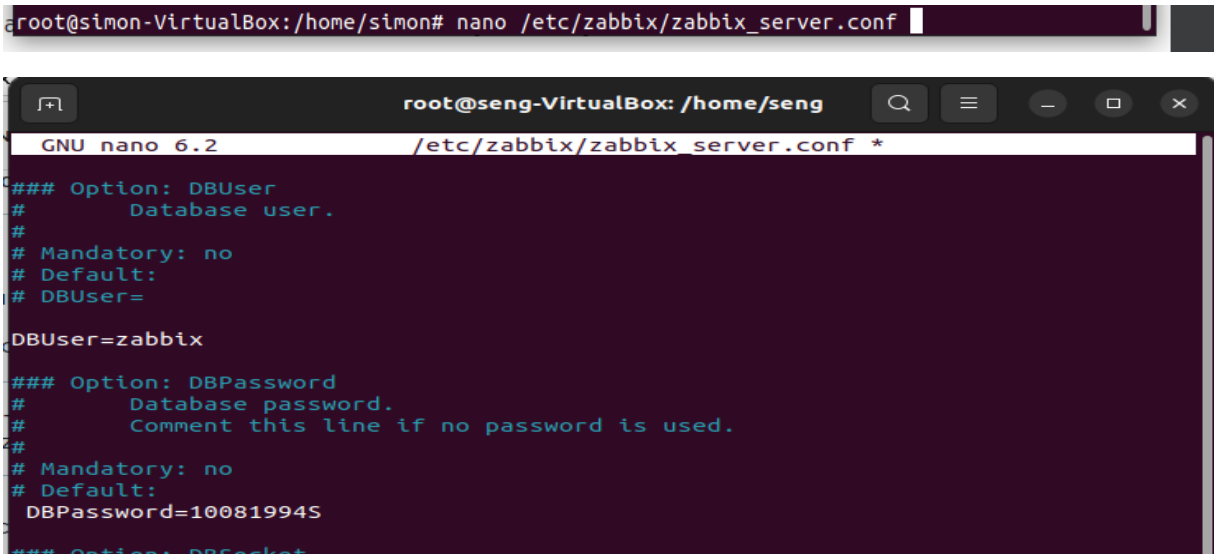


Figure 15:insertion nom utilisateur et mot de passe

Maintenant on redémarre les services :**# systemctl restart zabbix-server zabbix-agent apache2**

 # systemctl enable zabbix-server zabbix-agent apache2

```
root@simon-VirtualBox:/home/simon# nano /etc/zabbix/zabbix_server.conf
root@simon-VirtualBox:/home/simon# systemctl restart zabbix-server zabbix-agent apache2
root@simon-VirtualBox:/home/simon# systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/s
ystemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/sy
stemd-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@simon-VirtualBox:/home/simon#
```

Figure 16: redémarrer les services: zabbix, agent zabbix, apache

Suite à cela nous terminer l'installation en lançant notre navigateur

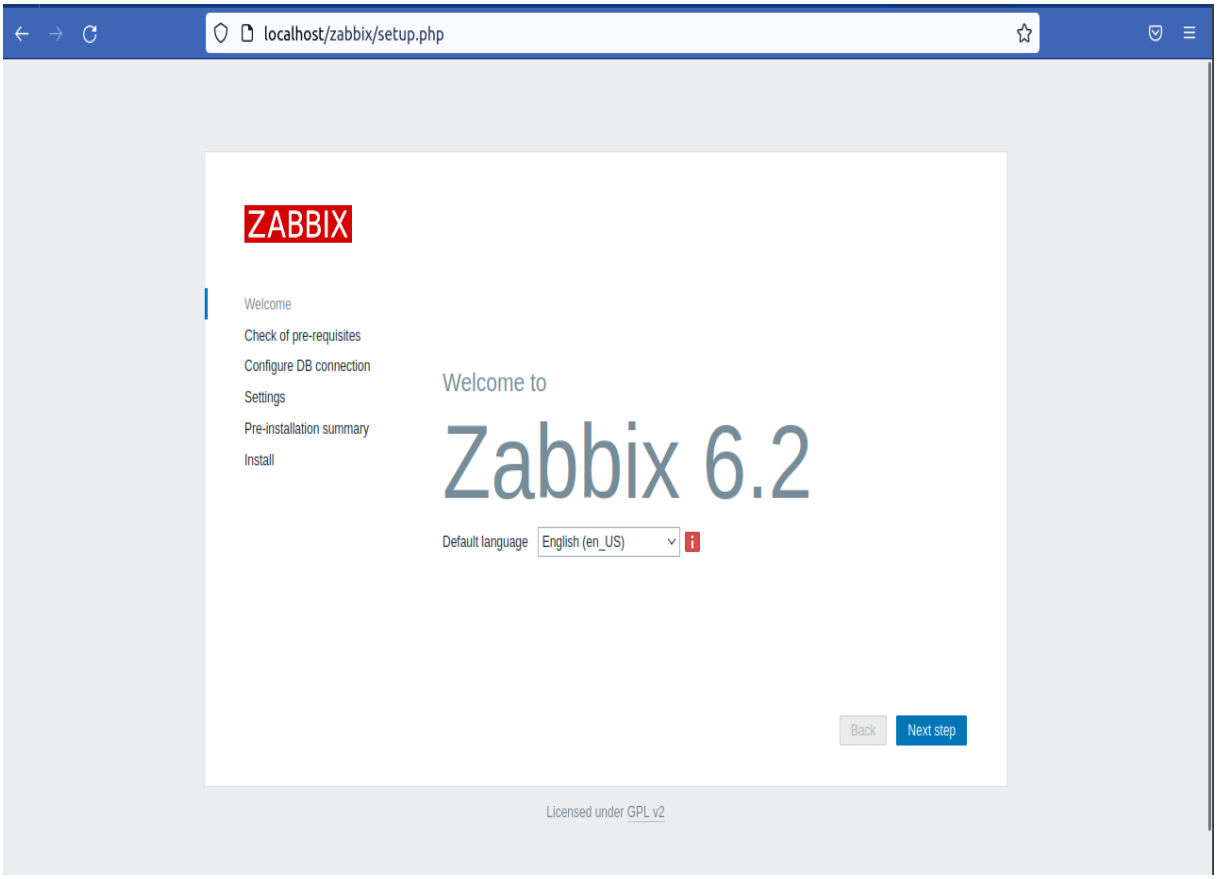


Figure 17: finalisation de l'installation

Ainsi nous avons fini l'installation de notre superviseur zabbix

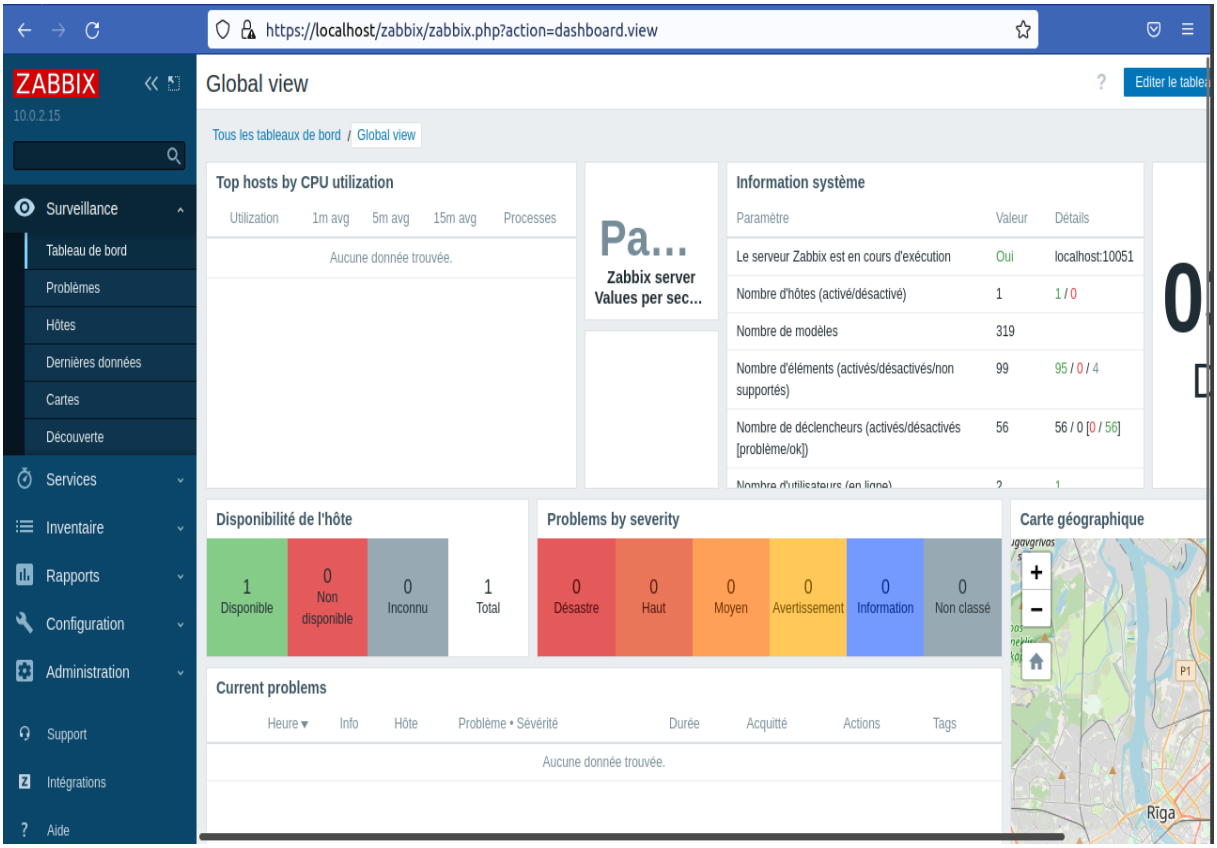


Figure 18: page d'accueil de l'outil zabbix

4.2.b-Installation de l'outil Grafana

4.2.b.1-Définition

Grafana Open Source Software [12] (OSS) est un outil de surveillance, d'analyse et de visualisation des données système en temps réel. A partir d'une série de données collectées, il fournit un aperçu graphique de la situation de l'entreprise ou de l'organisation. Il génère des graphiques et des tableaux de bord à partir de bases de données de séries chronologiques (Graphite, InfluxDB ou OpenTSDB). Il vous permet également de les partager avec d'autres utilisateurs en tant que sauvegarde instantanée.

Pour installer Grafana nous allons installer le paquet de Grafana qui ne se trouve pas dans le paquet par défaut d'Ubuntu en l'ajoutant. Il faut importer la Clé **GPG** (GNU Privacy Guard est un outil multifonction, libre et gratuit, qui permet de signer et de chiffrer à peu près tout ce qui se présente sous forme numérique). Puis on ajoute le dépôt

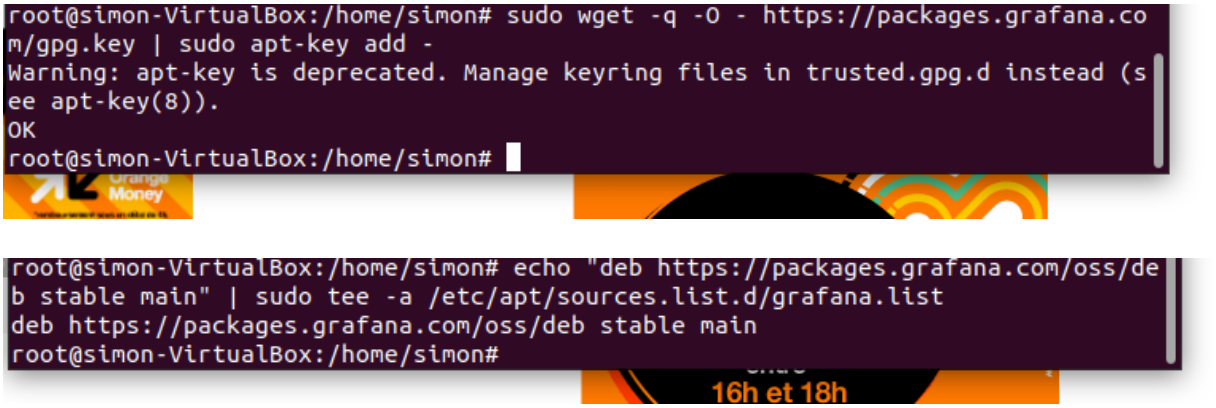


Figure 19:Ajout de la clé et dépôt du paquet grafana

Apres cela on installe les paquets nécessaires

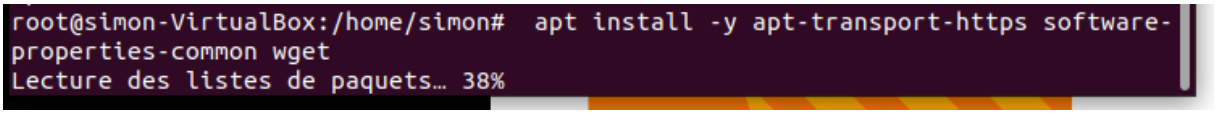


Figure 20: installation des paquets nécessaires grafana

Alors, il faut lister les clés présentes dans votre système afin d'importer celle de GRAFANA. Puis repérer cette dernière parmi celles listées et copier les 8 derniers chiffres qui seront utilisés pour l'importation

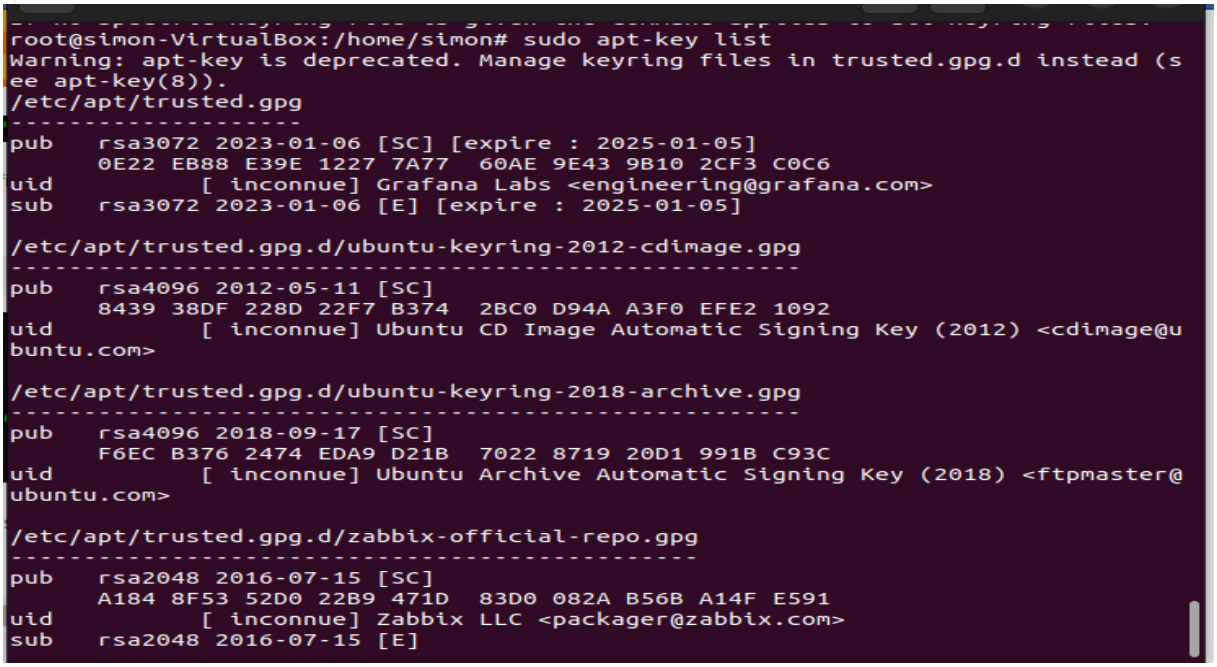


Figure 21: importation de la clé grafana

Enfin nous installons GRAFANA

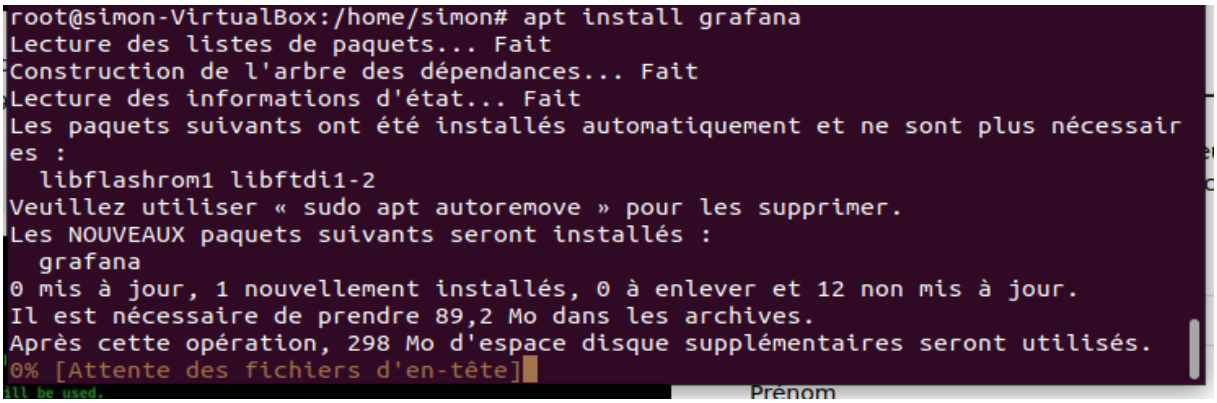


Figure 22:installation de GRAFANA

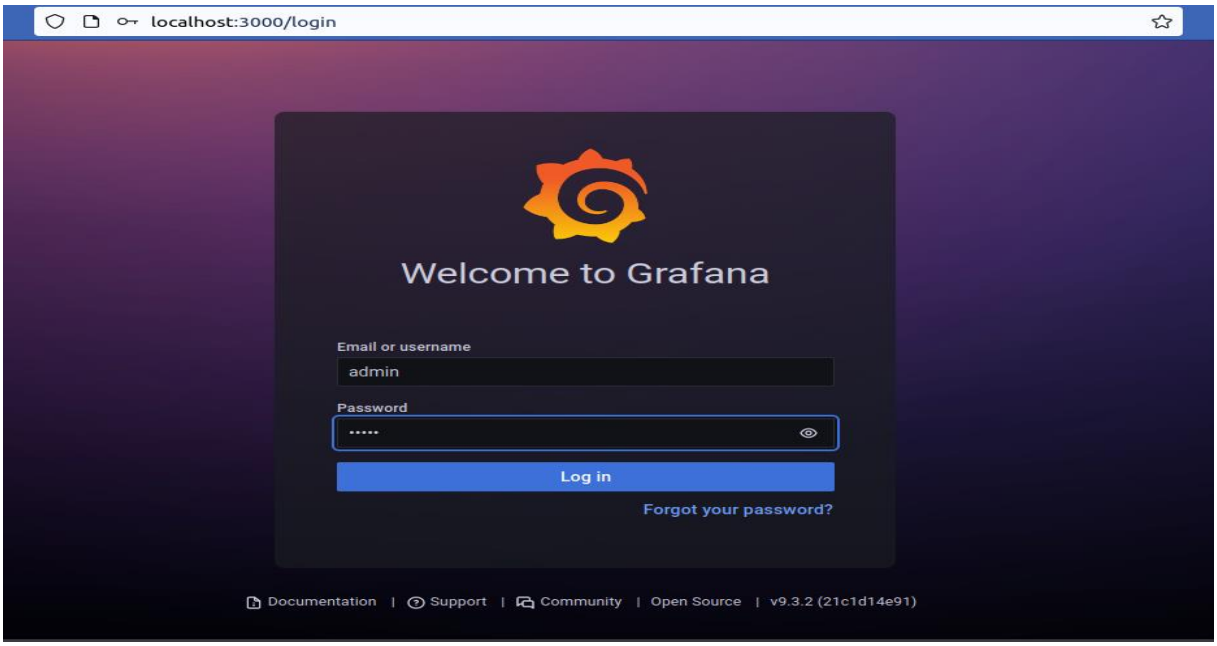


Figure 23: page d'accueil de GRAFANA

4.2.c-Installation l'outil de ticketing

OTRS [13] peut être installé sur différentes distributions GNU/LINUX et utiliser plusieurs gestionnaires de bases de données, la décision dépend donc de nos besoins. Nous utiliserons la combinaison Ubuntu, Apache et PostgreSQL. OTRS dispose d'une interface web très conviviale à partir de laquelle le système est contrôlé. Nous devons donc installer apache et postgreSQL comme système de gestion de base de données. Ensuite Nous lançons le service web apache2 et notre base de données posqtgresql

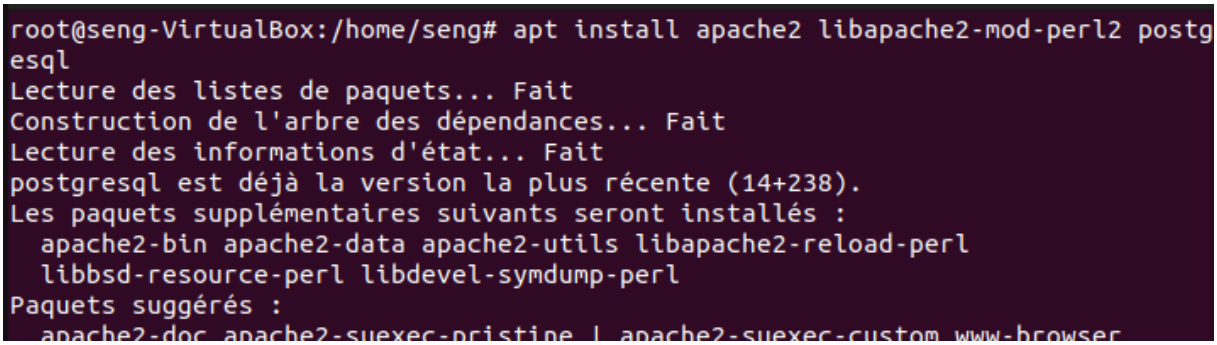


Figure 24: installation et lancement des services apache et PostgreSQL

Nous procédons maintenant à l'installation de quelques modules PERL afin que l'OTRS fonctionne correctement. C'est parce qu'il est construit avec Perl (langage de programmation). Nous allons activer perl

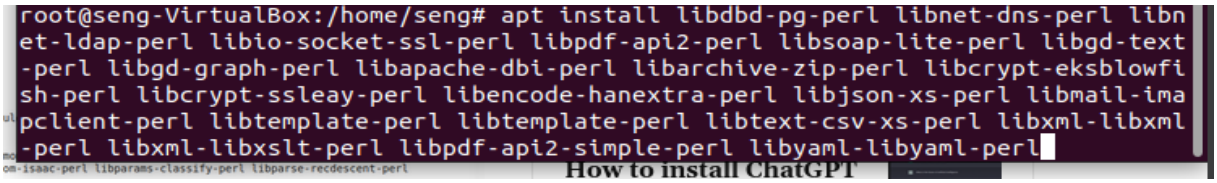


Figure 25: installation des modules perl d'OTRS

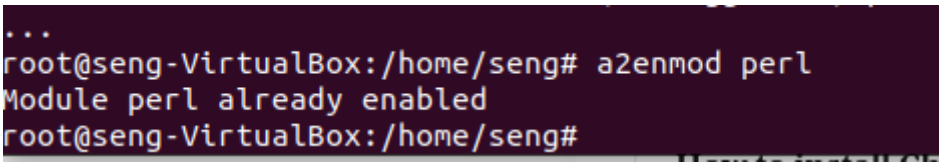


Figure 26: activation des PERL

Nous créons un utilisateur puis nous ajoutons maintenant au groupe www-data qui est le groupe qui a l'autorisation d'exécuter apache.

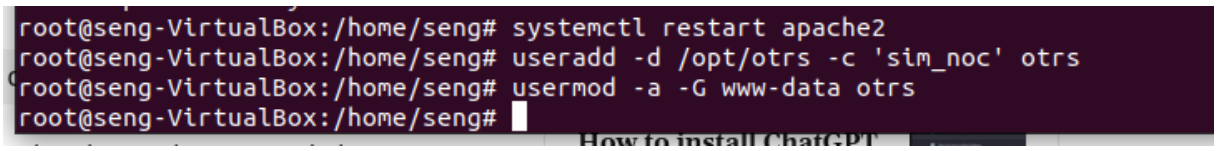


Figure 27: création de l'utilisateur:

Maintenant Nous allons maintenant créer l'utilisateur dédié à OTRS puis créer la base de données et donner des privilèges à l'utilisateur nouvellement créé sur celle-ci

```
root@seng-VirtualBox:/home/seng# sudo su  postgres
postgres@seng-VirtualBox:/home/seng$ psql
could not change directory to "/home/seng": Permission non accordée
psql (14.6 (Ubuntu 14.6-0ubuntu0.22.04.1))
Type "help" for help.

postgres=#
```

```
postgres=# create user otrs password 'otrspss' nosuperuser;
CREATE ROLE
postgres=# create database otrs owner otrs;
CREATE DATABASE
postgres=#
```

Figure 28: création de la base de données

Nous passons à l'activation du nouvel utilisateur en éditant le fichier pg_hba.conf **# nano /etc/postgresql/10/main/pg_hba.conf**

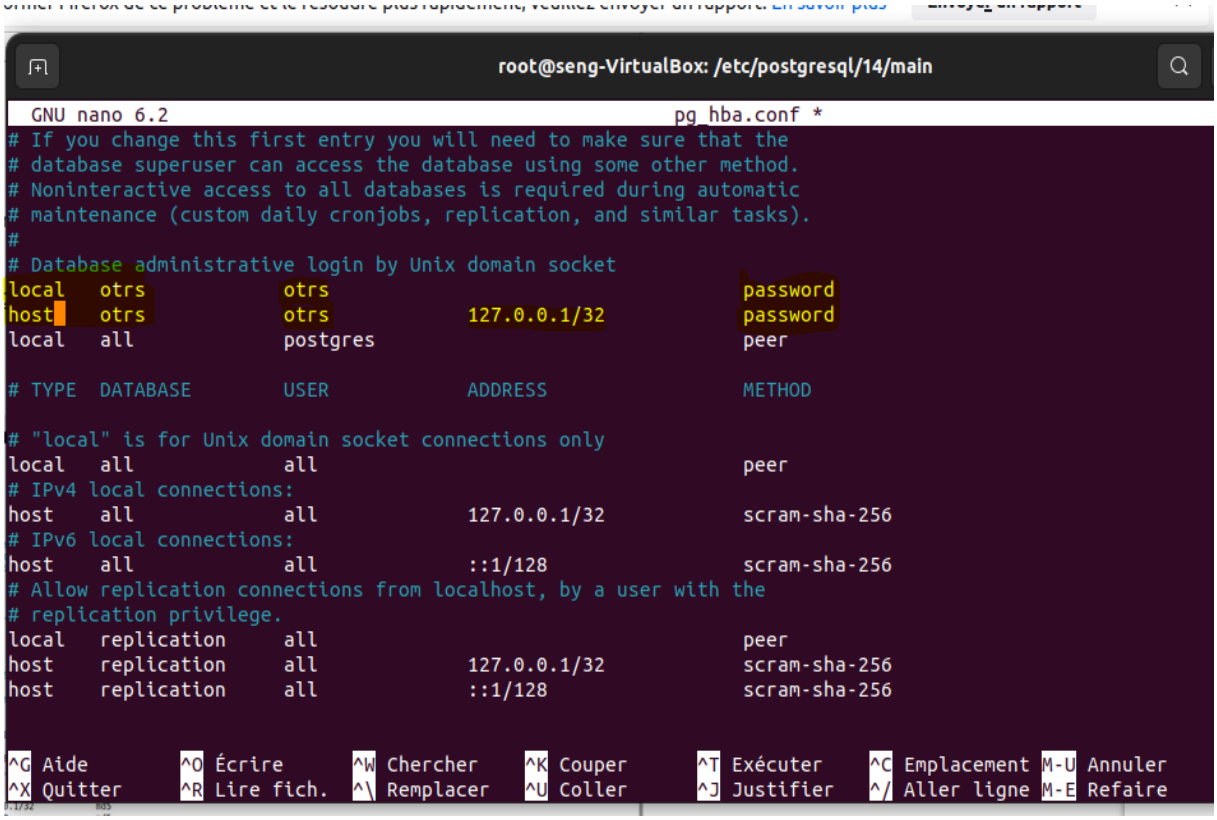


Figure 29: activation de l'utilisateur

Nous pouvons maintenant télécharger OTRS depuis leurs serveurs, leur dernière version stable est la 6.0. Une fois téléchargé, nous le décompressons, renommons le dossier en un nom court et enfin changeons le propriétaire du dossier.

```
otrs-community-edition-6.0.38.tar.gz
root@seng-VirtualBox:/opt# tar -xzvf otrs-community-edition-6.0.38.tar.gz
```

```
root@seng-VirtualBox:/opt# mv otrs-community-edition-6.0.38 otrs
root@seng-VirtualBox:/opt# chown -R otrs:otrs otrs
root@seng-VirtualBox:/opt#
```

Figure 30: téléchargement de l'outil OTRS

Avant de continuer, nous devons exécuter un script qui vérifiera si tous les modules sont disponibles.

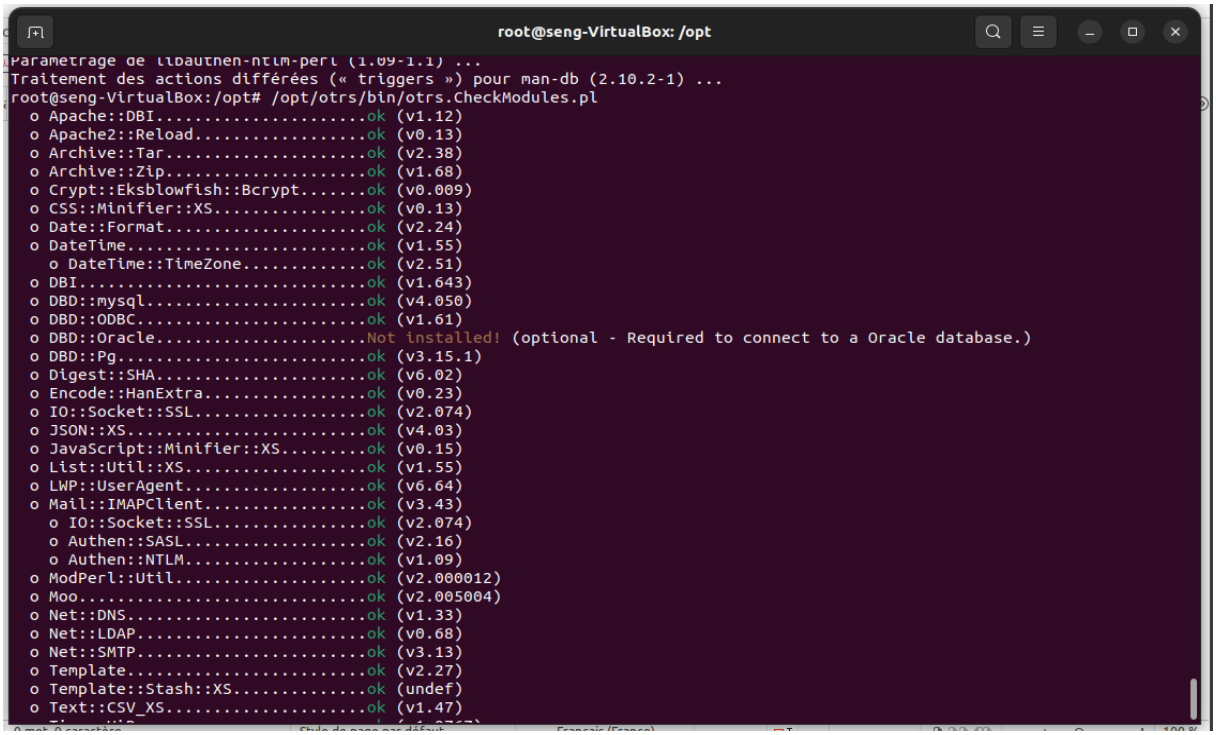


Figure 31: vérification des modules

Nous pouvons maintenant voir que nous répondons à toutes les exigences. Les modules manquants sont optionnels. Nous allons maintenant copier les paramètres nécessaires à l'exécution.

```
root@seng-VirtualBox:/opt# cd /opt/otrs/
root@seng-VirtualBox:/opt/otrs# cp Kernel/Config.pm.dist Kernel/Config.pm
root@seng-VirtualBox:/opt/otrs#
```

Figure 32:copie des paramètres nécessaires OTRS

Les étapes suivantes consistent à modifier le fichier de configuration et à changer la base de données, en supprimant le support de mysql et en supportant PostgreSQL. Ensuite, nous devons activer le support de PostgreSQL dans apache et perl.

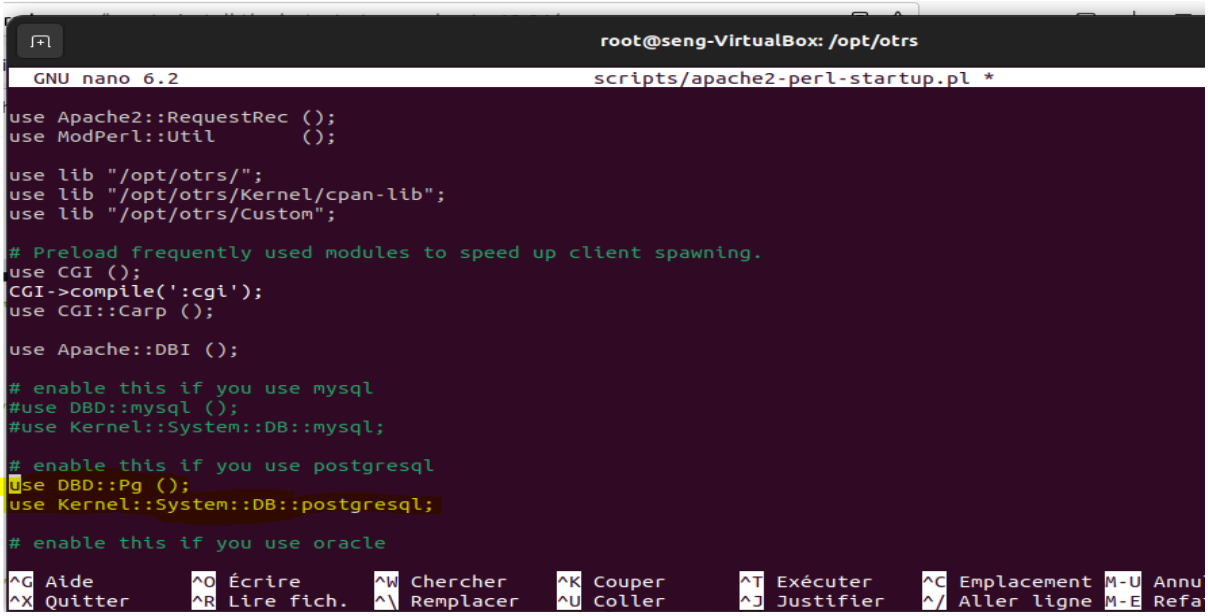


Figure 33: activation de la base de donné PostgreSQL

Nous vérifions maintenant que toutes les dépendances et tous les modules sont correctement chargés et configurés. Et si, lors de l'exécution de chacune des commandes, nous recevons une "Syntaxe OK". Tout va bien.

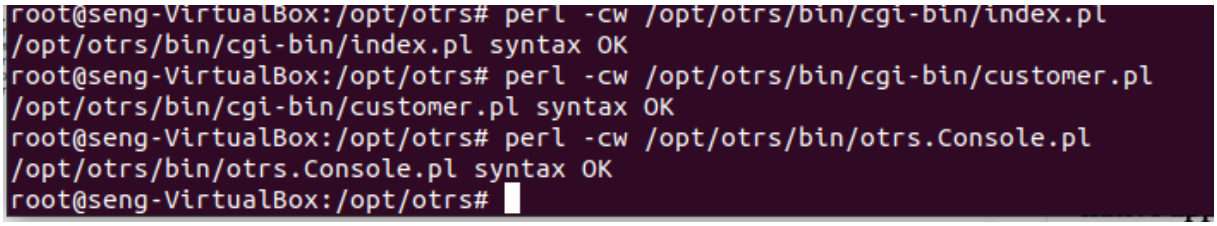
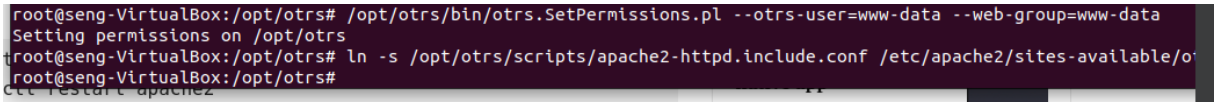


Figure 34: vérification des modules et dépendances

Faisons ensuite un lien symbolique depuis la configuration Virtual host créée vers le fichier de configuration d'apache. Nous avons enfin activé Virtual host et redémarré apache.



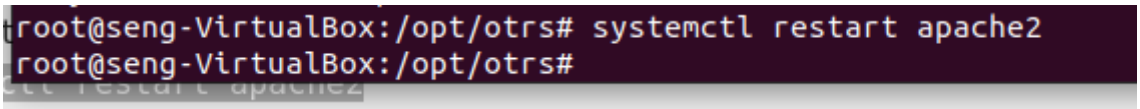


Figure 35: relancer le service web apache2

Maintenant nous connectons au niveau du navigateur pour finaliser l'installation

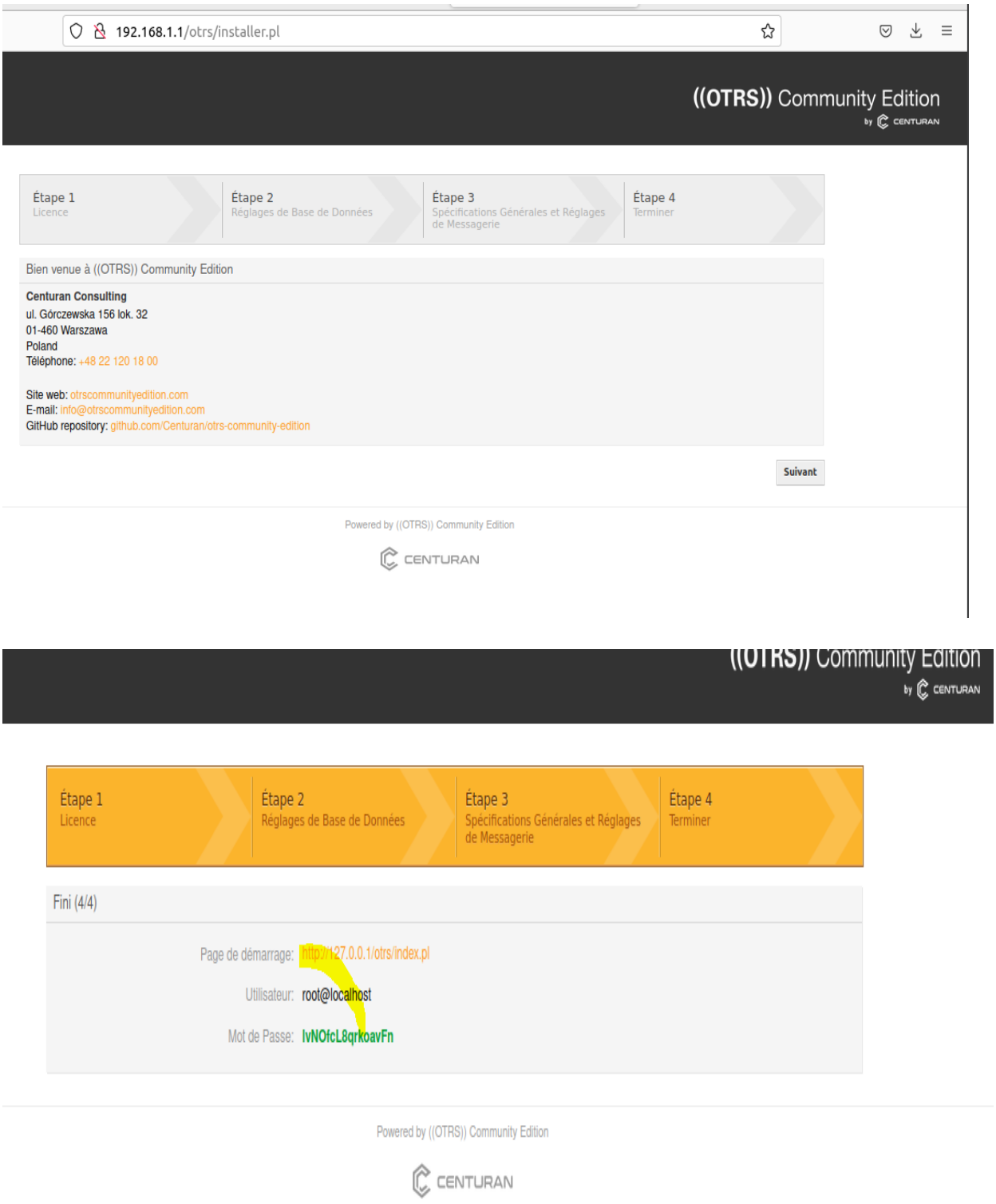


Figure 36: finalisation de l'installation

4.3-Configuration du NOC

Après avoir mis en place l'architecture de notre réseau et installé les logiciels choisis, nous allons faire de la configuration de notre NOC constitué du monitoring zabbix afin de surveiller tous les matériels du réseau, du GRAFANA afin de visualiser les données et le système des tickets avec OTRS mais aussi des routeurs et du réseau afin d'accéder aux différents nœuds dans le but de surveiller notre réseau d'opérateur.

Au niveau des routeurs on configure le nom les différentes interfaces par rapport aux réseaux auxquels ils appartiennent puis nous créons les routes en utilisant le routage statique et enfin on active pour surveiller les sauteurs SNMP (***Simple Network Management Protocol***) est un protocole de gestion de réseaux de protocole de communication permettant de gérer, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

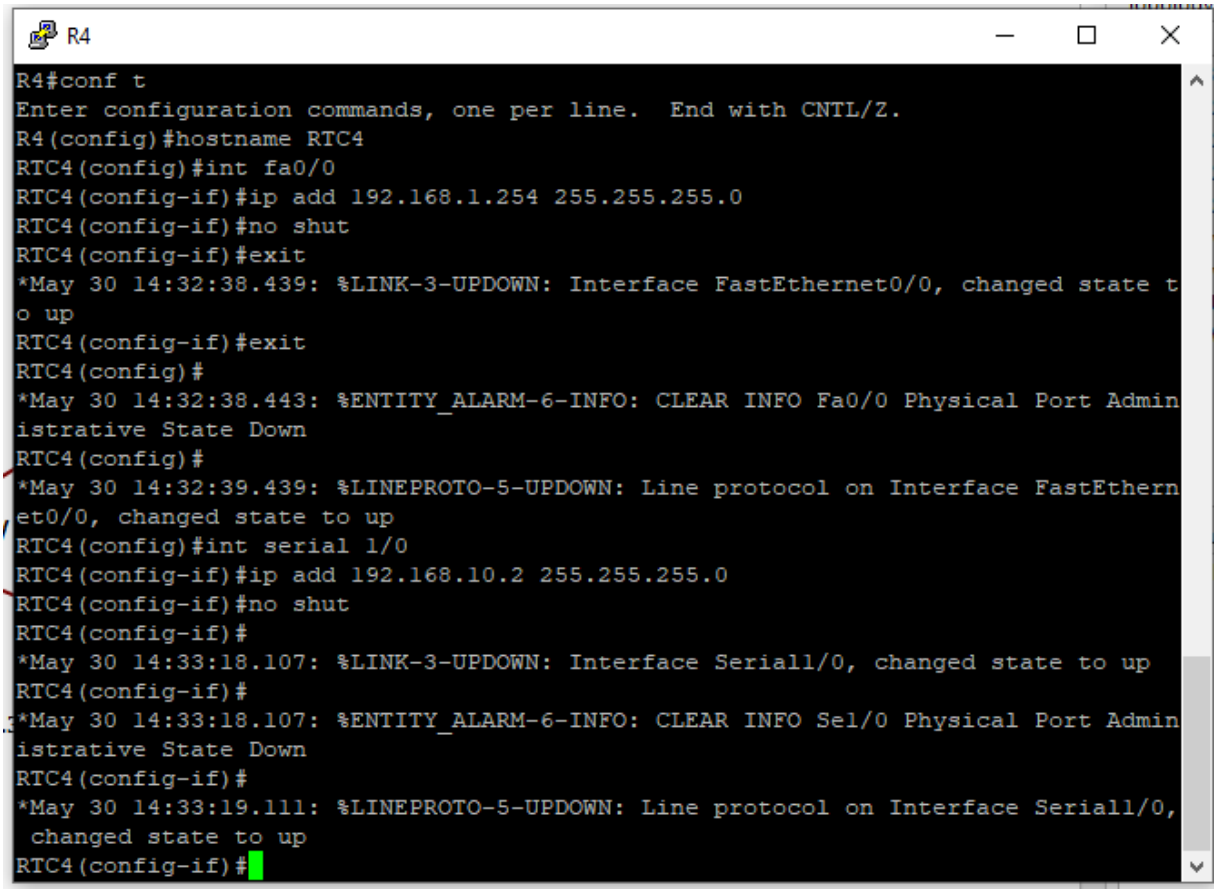


Figure 37:configuration des adresses ip au niveau du routeur

```
RTC4(config-if)#exit
RTC4(config)#snmp
RTC4(config)#snmp-ser
RTC4(config)#snmp-server comm
RTC4(config)#snmp-server community NOC1 RO
RTC4(config)#snmp-server community pr
RTC4(config)#snmp-server community priv
RTC4(config)#snmp-server community priva
RTC4(config)#snmp-server community private RW
RTC4(config)#do wr
Building configuration...
[OK]
RTC4(config)#
```

Figure 38: activation de SNMP

Au niveau de notre machine Ubuntu 16 il est possible de surveiller en installant l'agent zabbix ou le protocole SNMP au niveau mais aussi nous installons l'asterisk afin de connaître les résultats par rapport à la téléphonie.

SNMP : installation #apt install snmpd

Ensuite on configure adresse de l'agent en éditant le fichier snmpd.conf en y mettant l'adresse de la machine ubuntu-16

```
root@simon-VirtualBox: /etc/snmp
  GNU nano 2.5.3                Fichier : snmpd.conf

###############################################################################
#
# EXAMPLE.conf:
#   An example configuration file for configuring the Net-SNMP agent ('snmpd')
#   See the 'snmpd.conf(5)' man page for details
#
#  Some entries are deliberately commented out, and will need to be explicitly $
#
###############################################################################
#
#  AGENT BEHAVIOUR
#

#  Listen for connections from the local system only
agentAddress  udp:192.168.2.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
#agentAddress udp:161,udp6:[::1]:161


^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^J Justifier ^C Pos. cur.
^X Quitter    ^R Lire fich.^\ Remplacer   ^U Coller    ^T Orthograp.^_ Aller lig.
```

Figure 39: configuration agent zabbix

Puis on relance le service snmpd

#system restart snmpd

Agent-zabbix

#apt installe zabbix-agent

Puis on configure le fichier zabbix_agentd.conf en y mettant l'adresse du serveur zabix de notre NOC

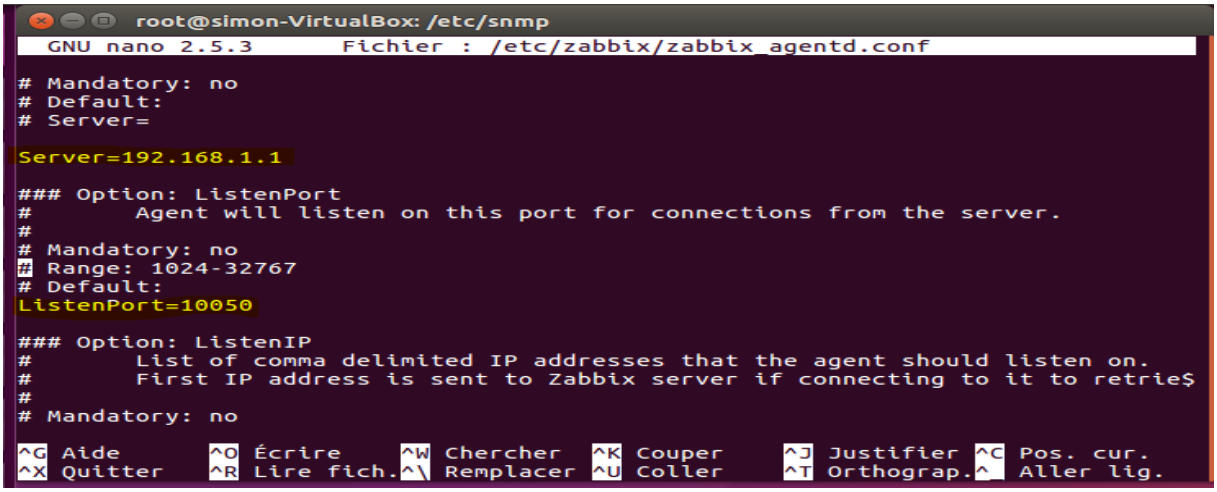


Figure 40: configuration de l'adresse serveur et du port

Enfin nous configurons l'asterisk pour la téléphonie.Nous ajoutons nos utilisateurs dans le fichier users.conf. Puis dans le fichier extension qui permet aux utilisateurs de pouvoir communiquer entre eux

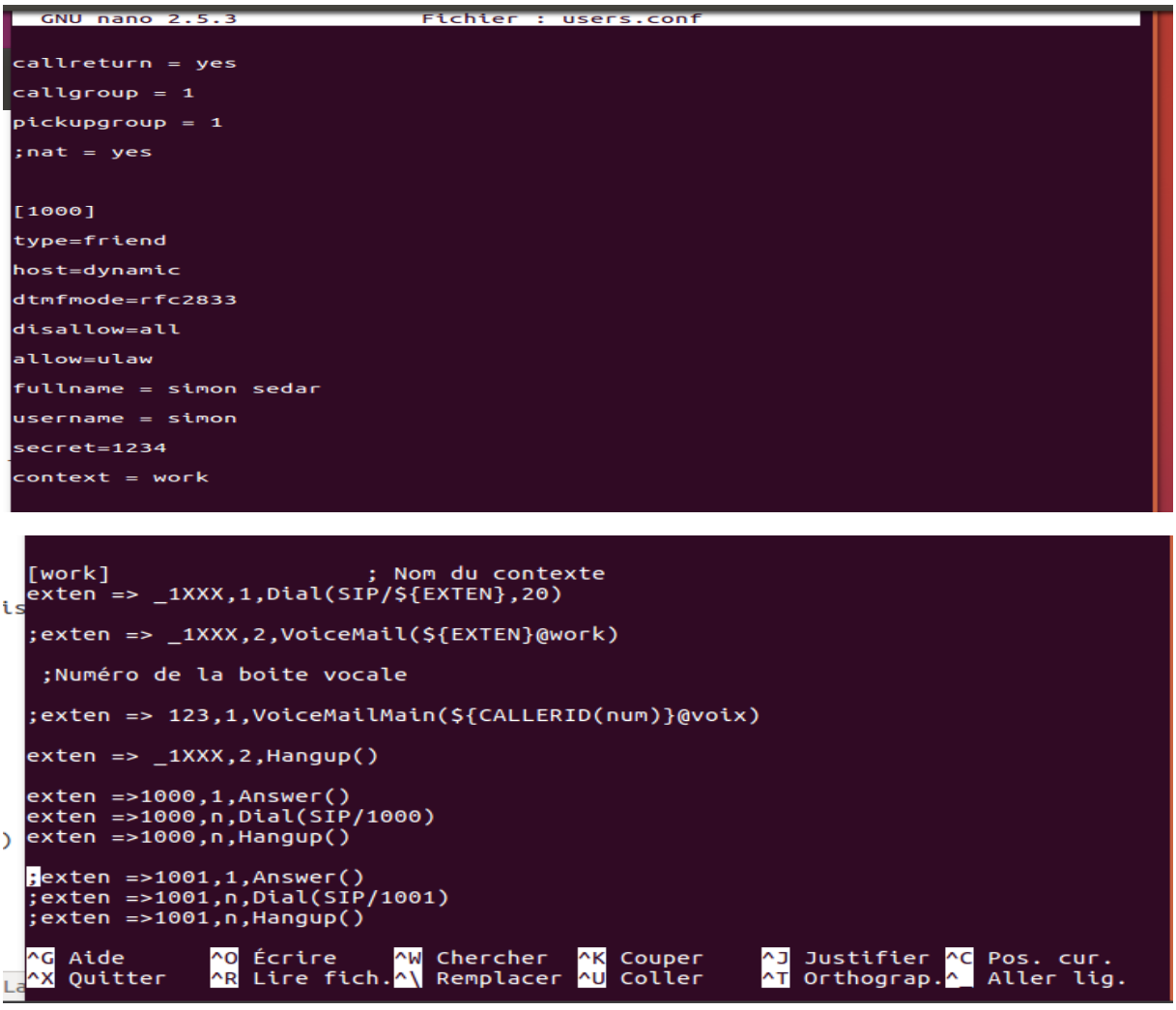


Figure 41:creation des utilisateurs

Au niveau de la machine Windows nous téléchargeons et installons l'outil zabbix agent

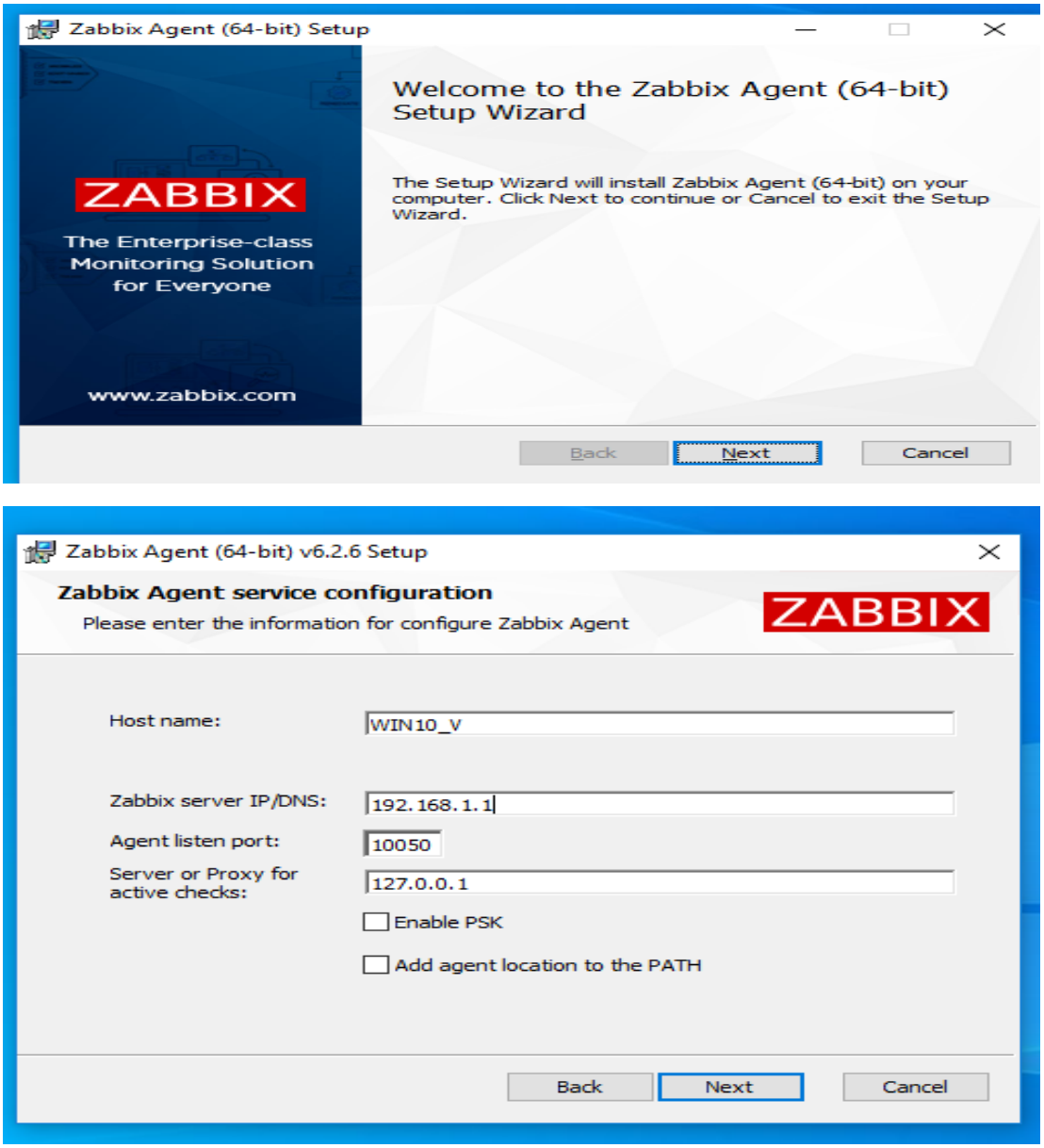


Figure 42: Activation de l'agent zabbix sur Windows

Au niveau de notre machine Ubuntu nous allons ajouter les matériels à superviser au niveau de zabbix ensuite visualisé les données sur GRAFANA et montrer l'émission de ticket au niveau OTRS en cas d'incident

Pour ajouter un matériel nous cliquons sur nouvel hôte puis nous enregistrons les différents éléments de la machine : le nom, le Template (modèle qu'il appartient), le groupe de machine, l'adresse du matériel (machine ou routeurs.) et la communauté de snmp

Routeur

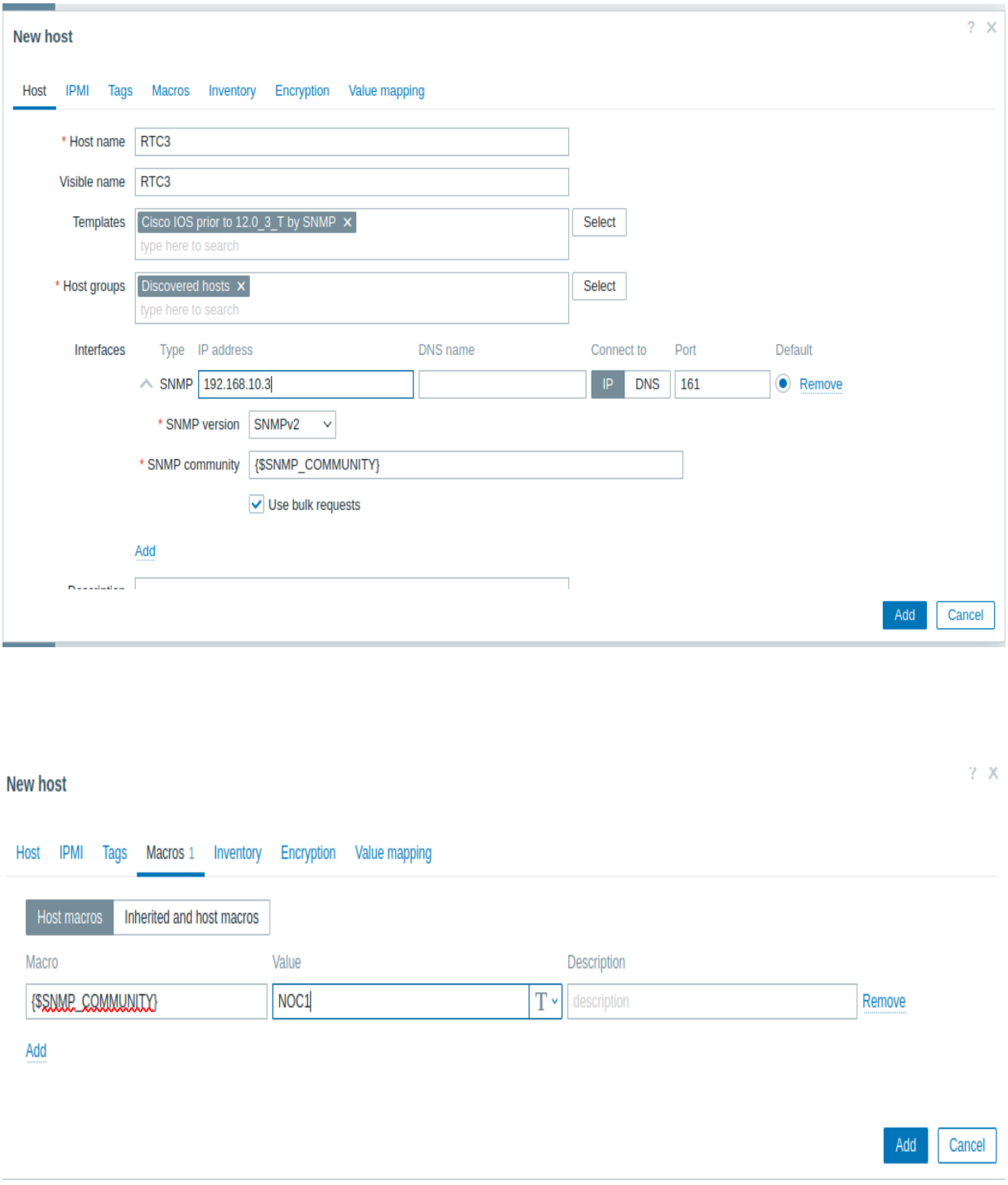


Figure 43: ajout d'un matériel sur zabbix

Au niveau de la visualisation nous intégrons zabbix au niveau de grafana et on choisit les données à visualiser

Au niveau de la configuration dans l'onglet Plugins on ajoute zabbix à GRAFANA

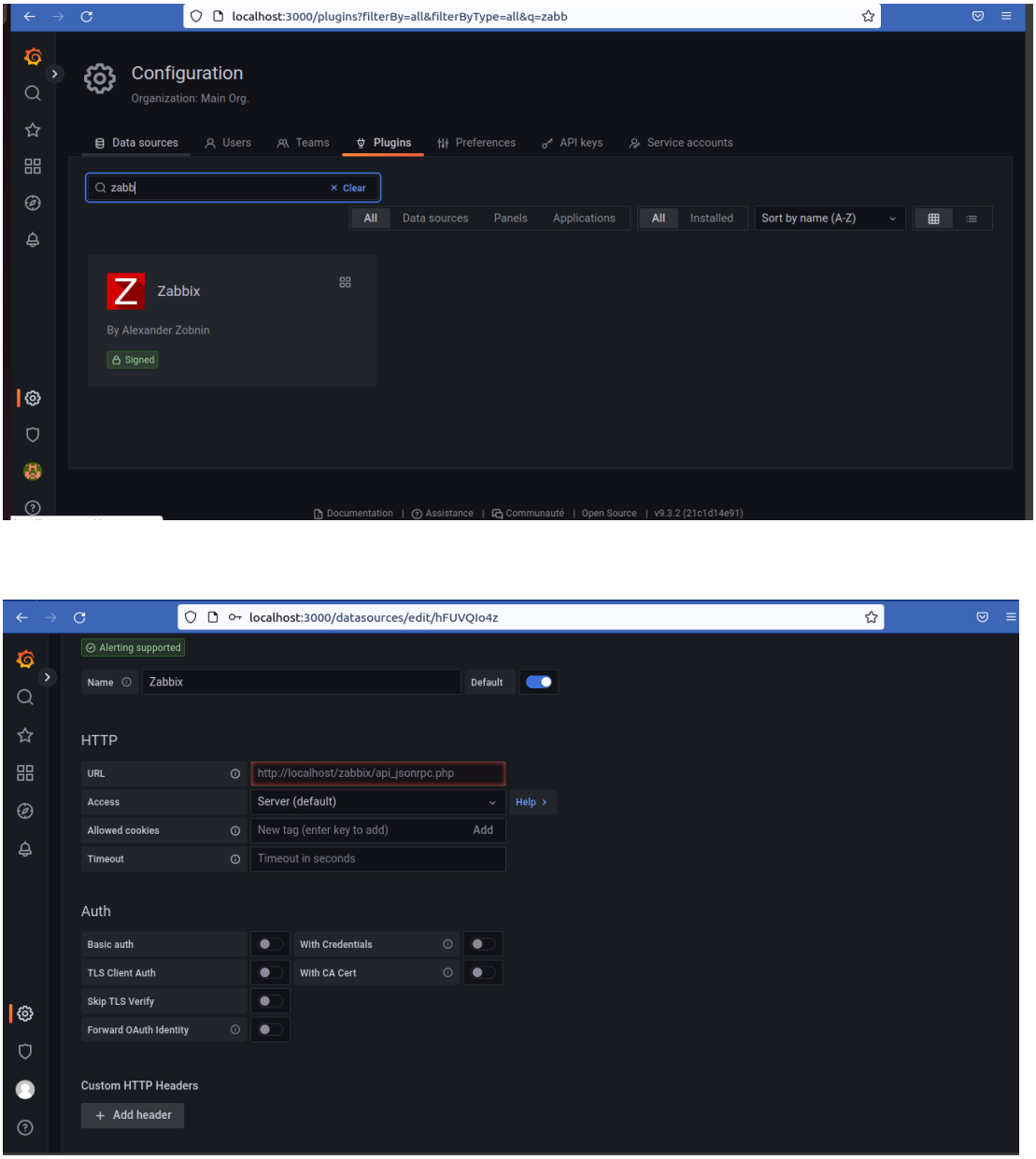


Figure 44: intégration zabbix sur grafana

Et maintenant le système de ticket ou dans un premier temps il faut configurer l'utilisateur au niveau du serveur OTRS puis l'utilisateur se connecte sur sa machine afin de créer un ticket en cas de besoins et cela sera reçu au niveau serveur qui sera prise en compte afin d'apporter une solution par rapport à ce ticket.

Nous débutons d'abord par créer un email du système

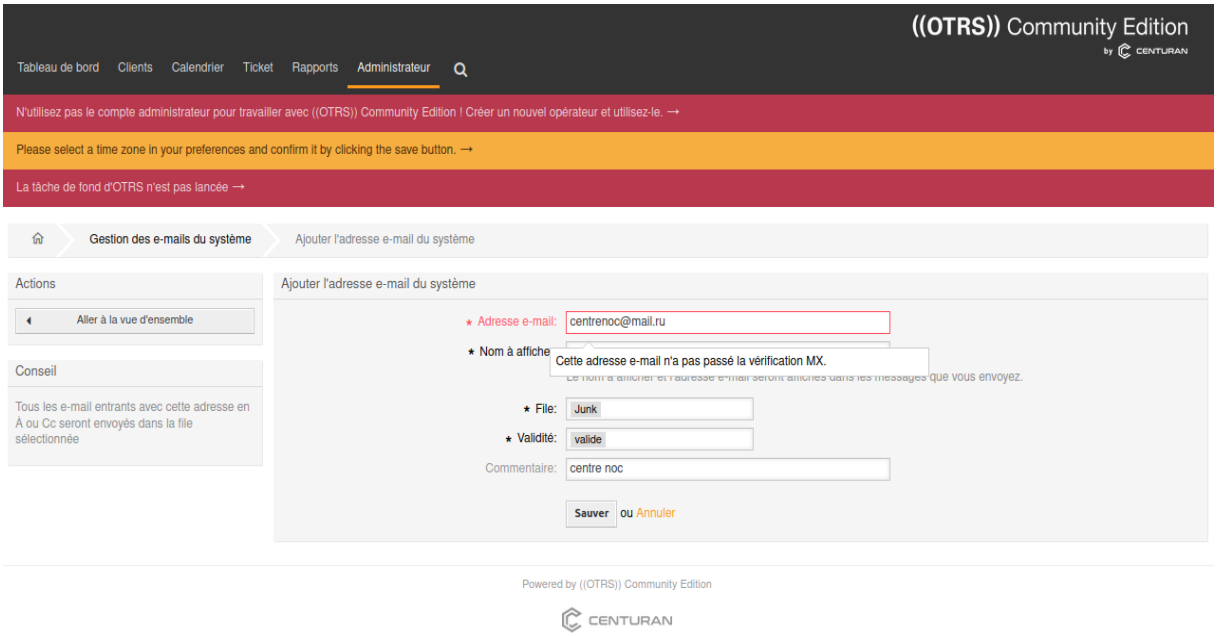


Figure 45: Ajout du mail système

Puis un compte de messagerie

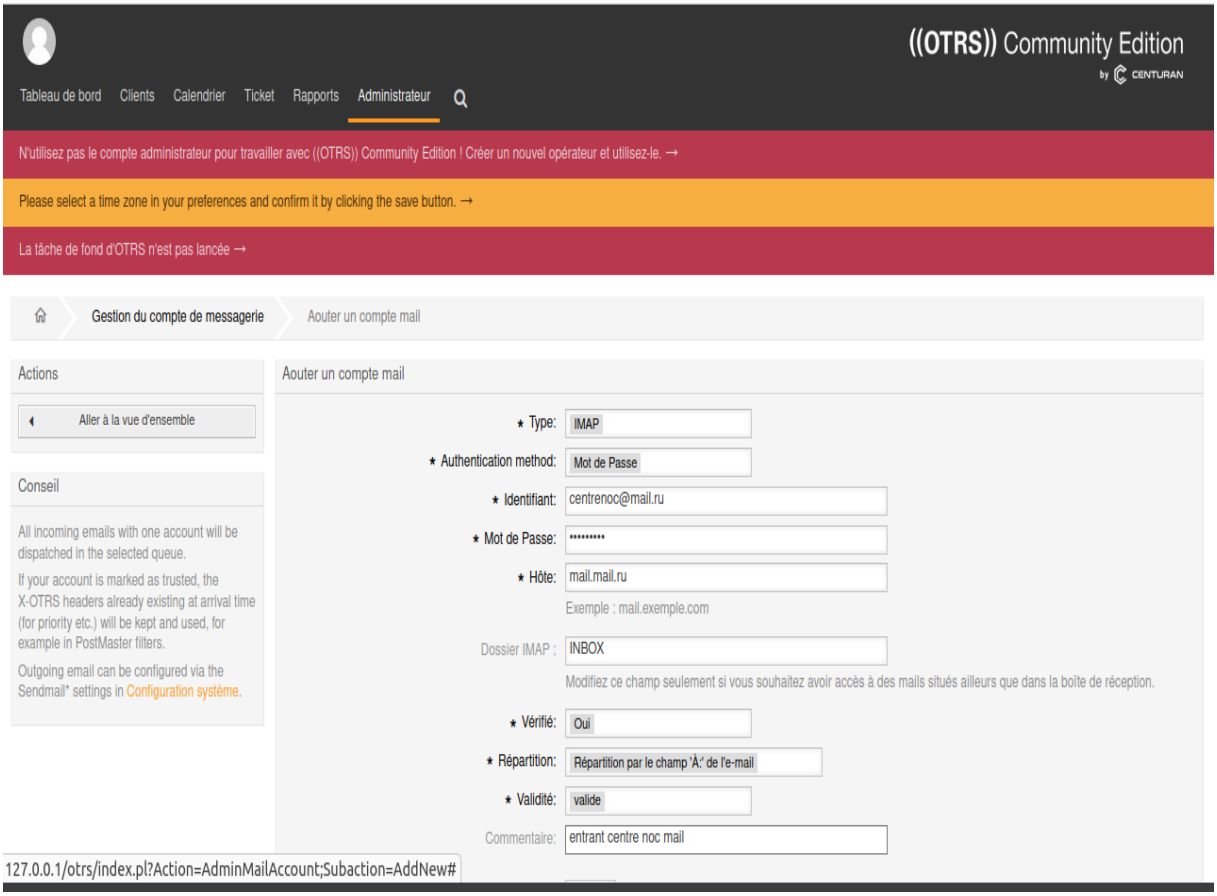


Figure 46: compte de messagerie

Nous ajoutons un groupe

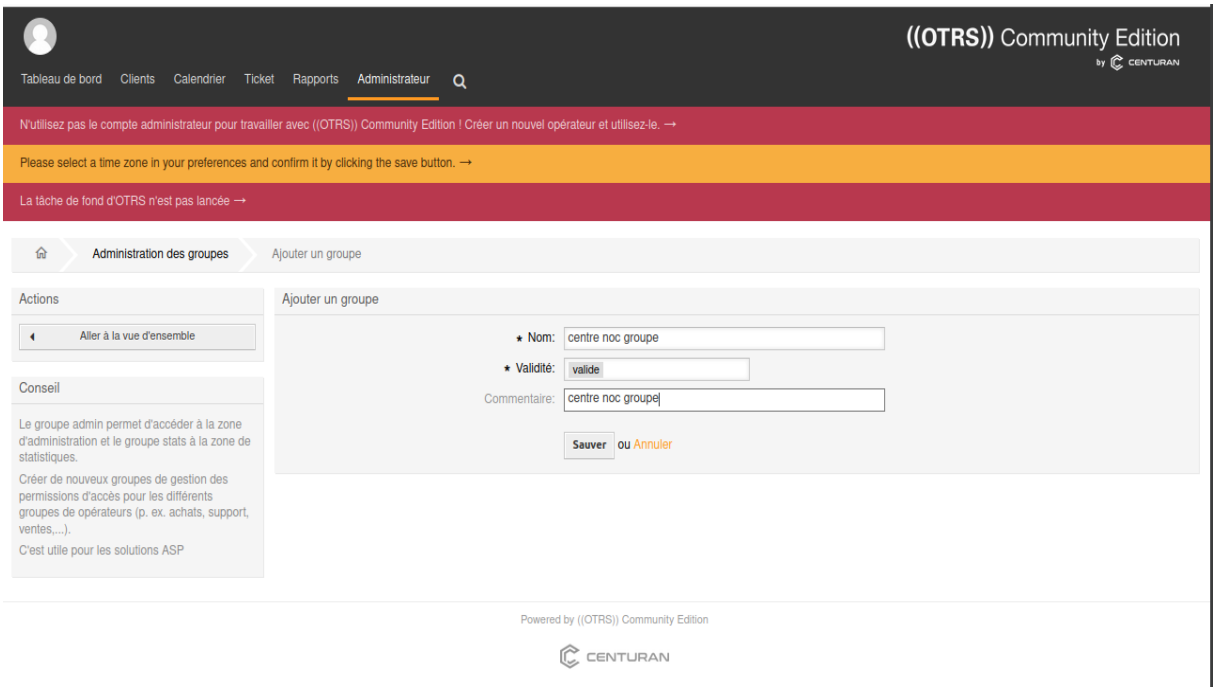


Figure 47:Ajout d'un groupe

Nous allons enregistrer le code client avec les informations du client

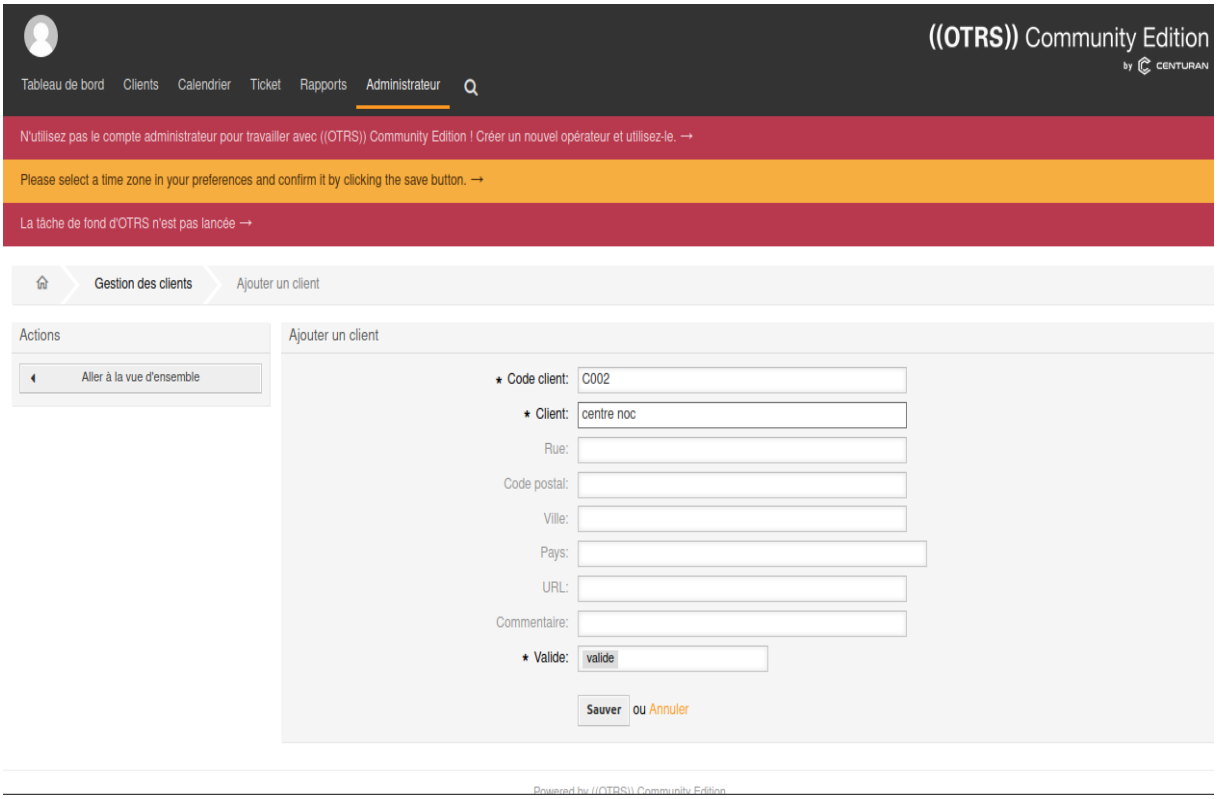


Figure 48: Enregistrement du client

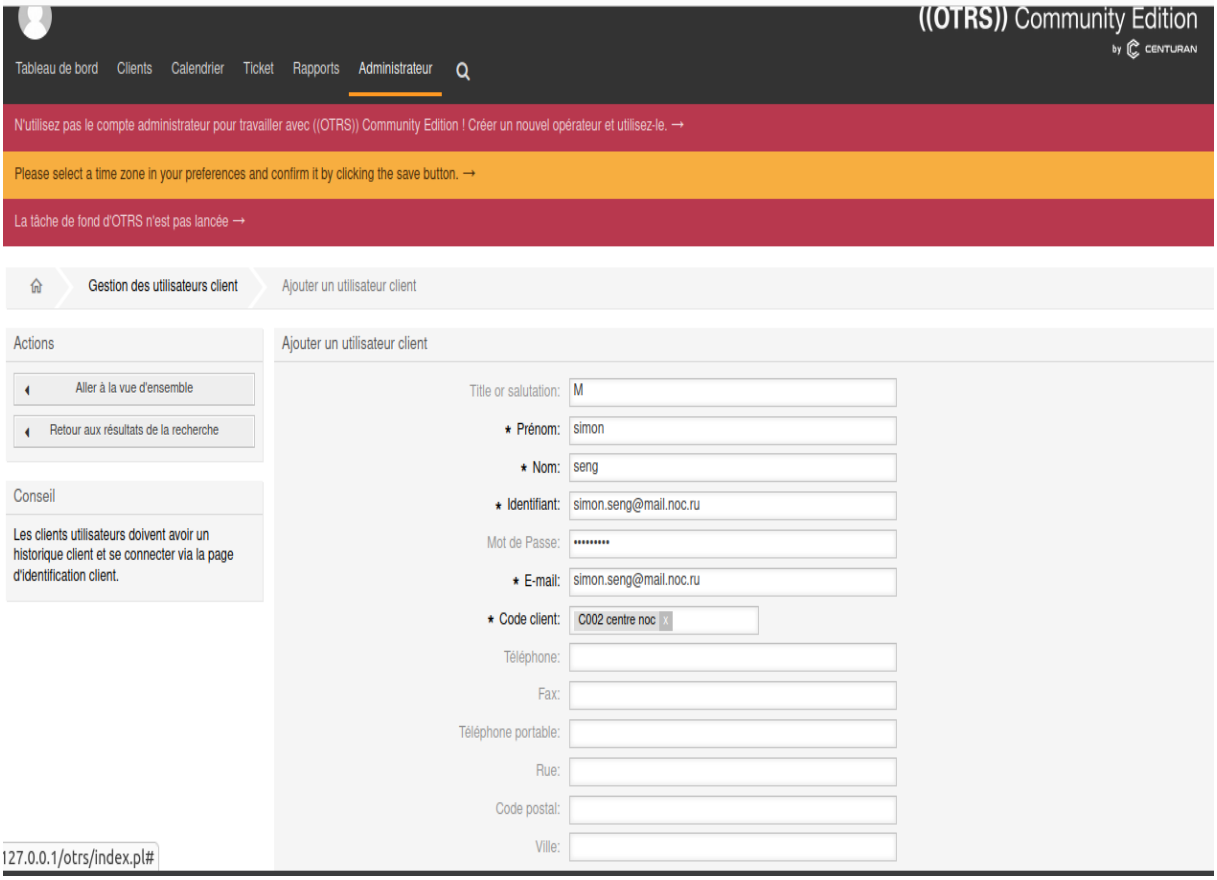


Figure 49:ajout des informations du client

Nous modifions les relations client et les groupes et utilisateur

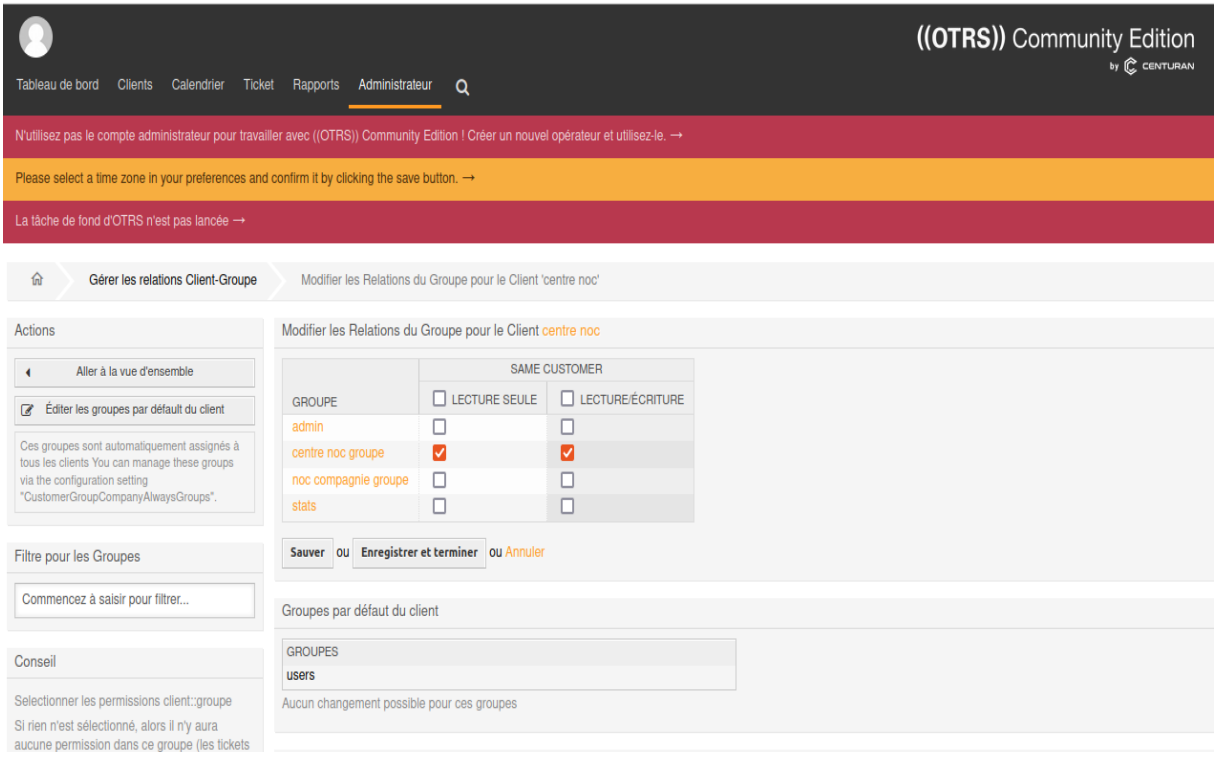
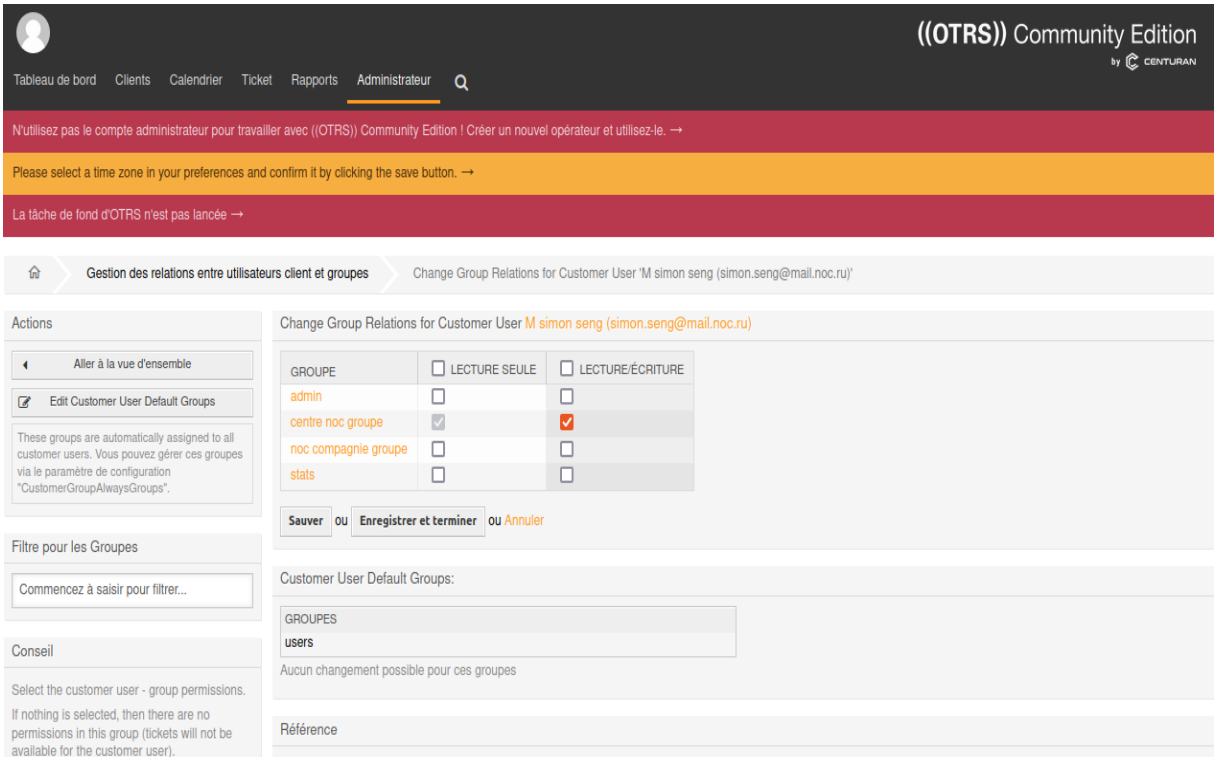


Figure 50: modification des relations



Nous allons créer un opérateur qui est moyen permettant de travailler simultanément sur les alertes entrées dans le système de lecture, le catalogage et répondre aux messages entrants

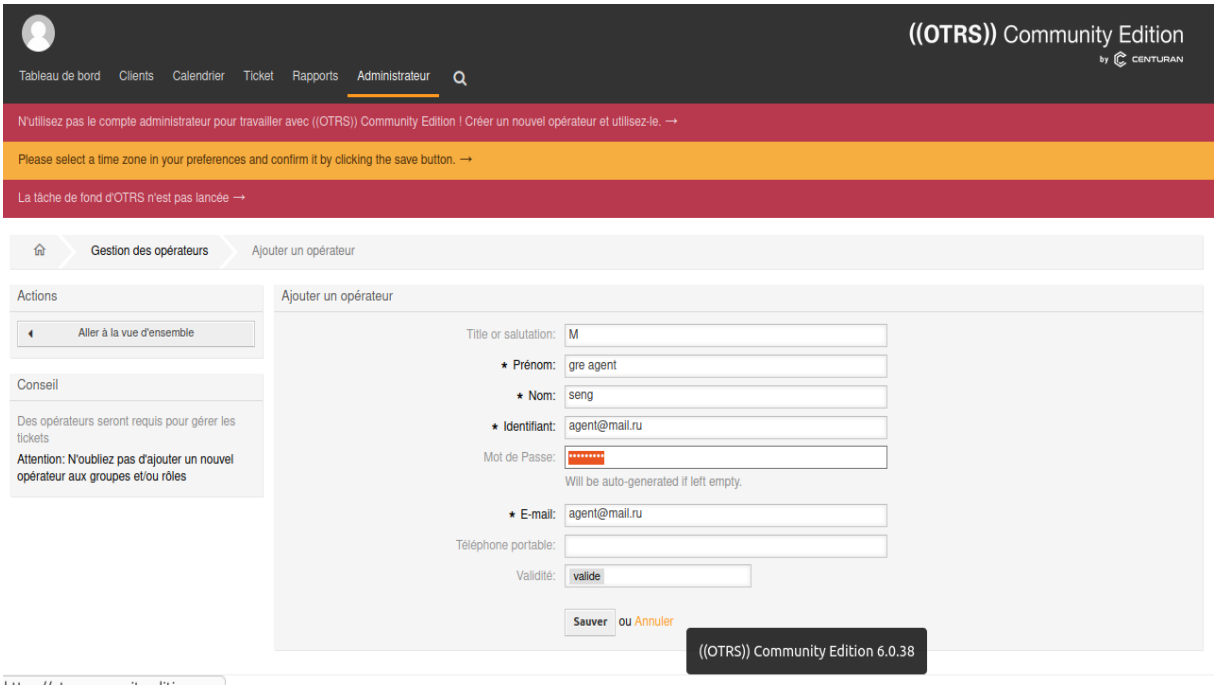


Figure 51: Ajout d'operateur

Maintenant nous éditons les files qui est moyen de gérer les types de ticket c'est-à-dire des problèmes logiciels ou matériel.



Figure 52: ticket hardware

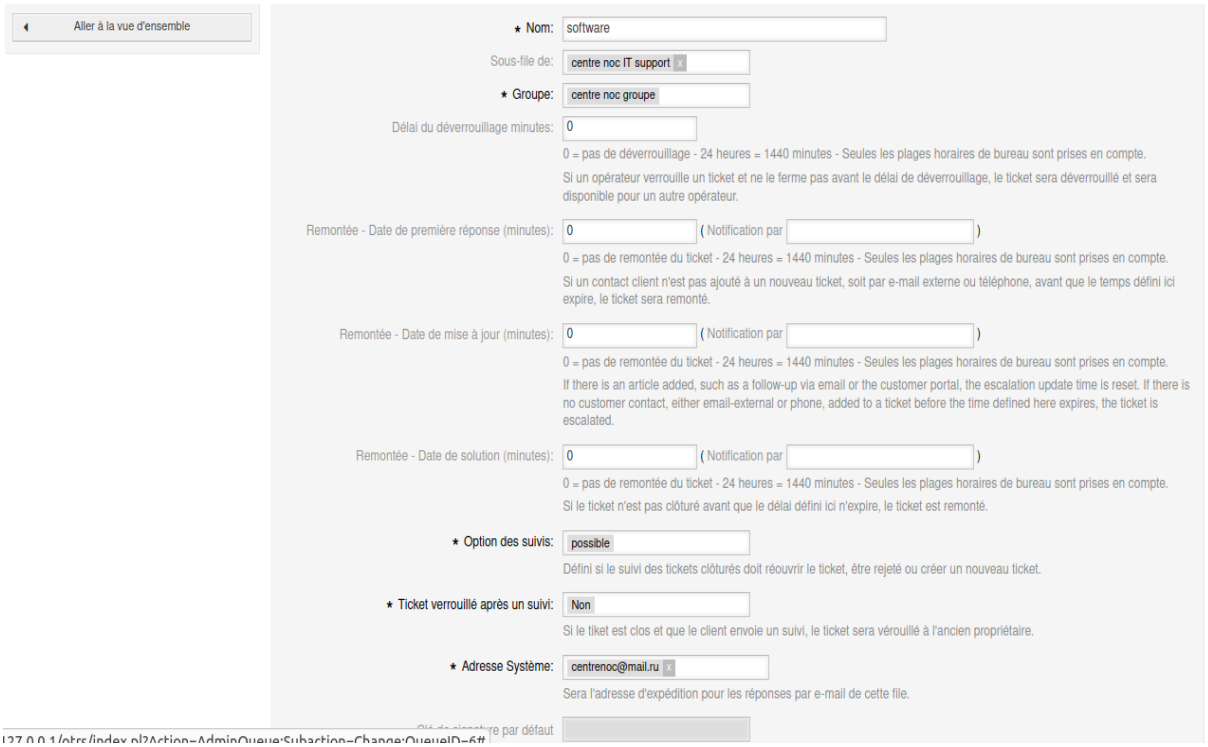


Figure 53: ticket software

A ce stade, l'utilisateur peut se connecter sur sa machine et créer un ticket afin de pouvoir mettre l'information concernant un incident ou problème. Alors au niveau de notre machine Ubuntu on se connecte afin de créer notre ticket pour illustrer

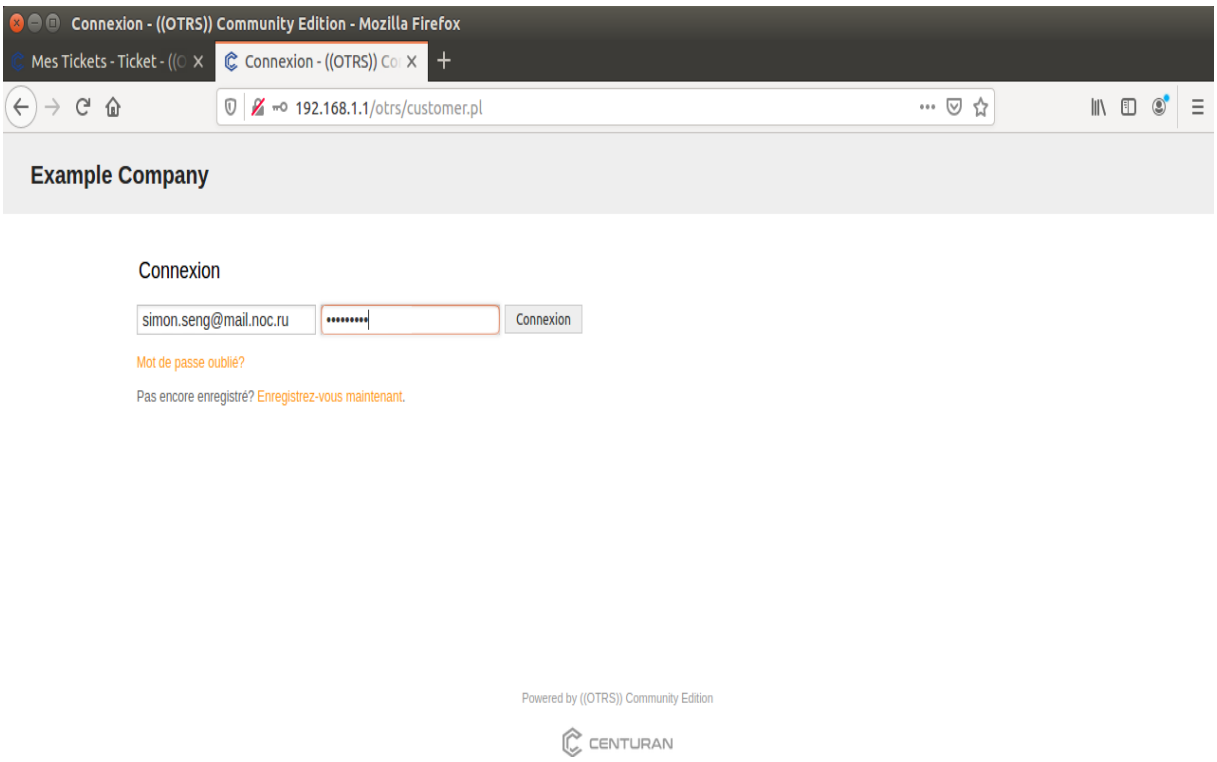


Figure 54: connexion de l'utilisateur

Création du ticket et Validation de la création de ticket

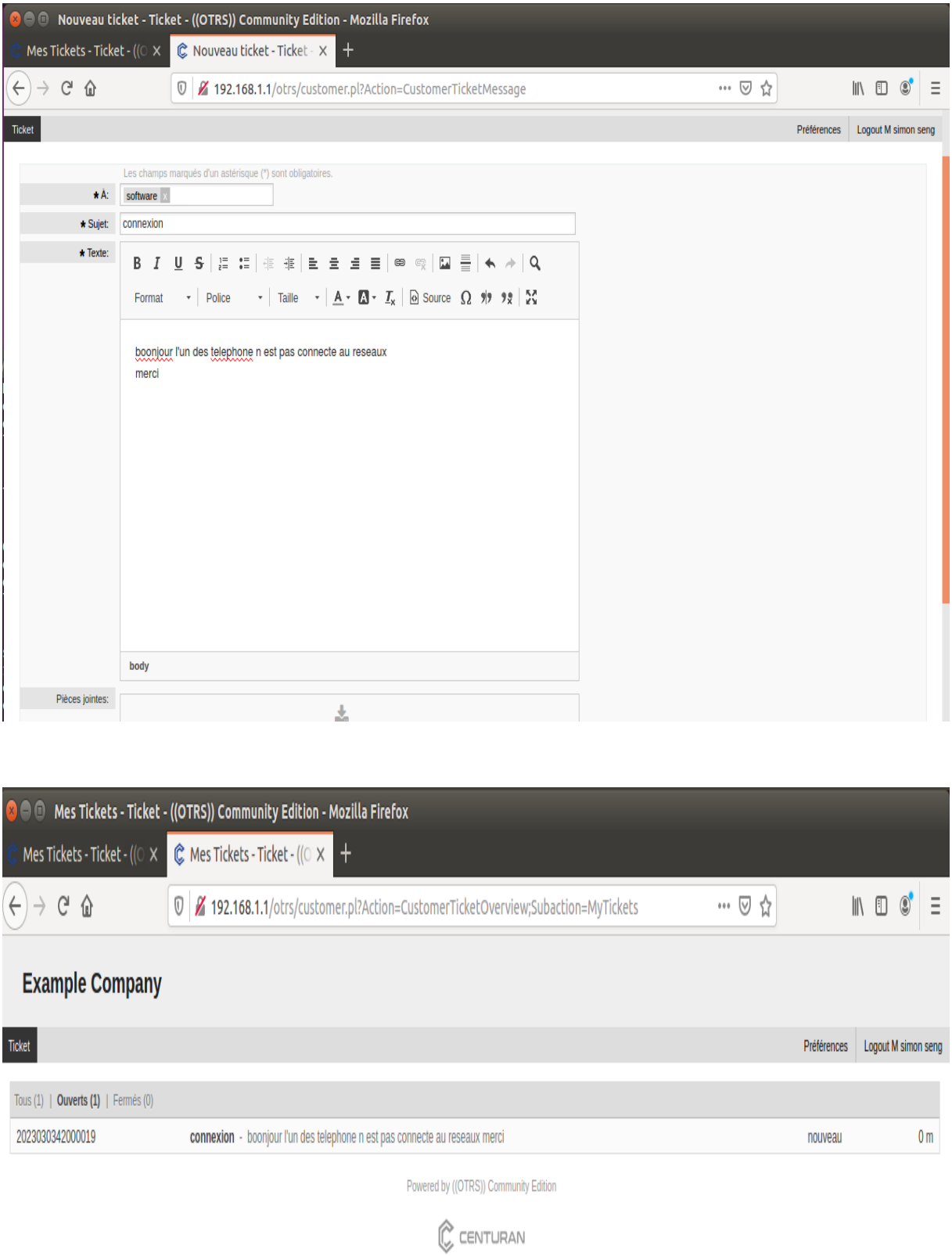


Figure 55: Création et validation de ticket

4.4-Résultat

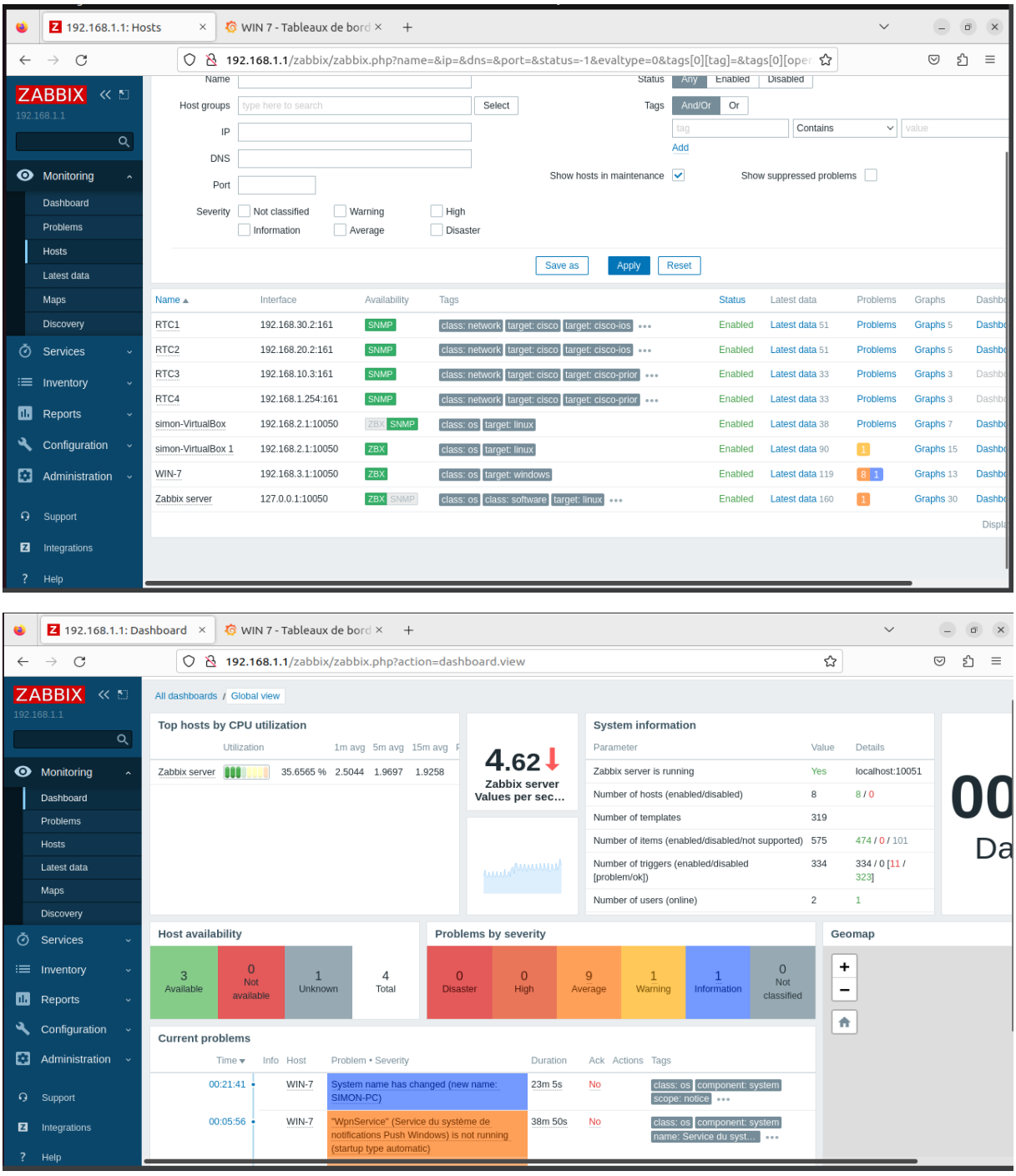


Figure 56: résultat de surveillance du réseau

Apres avoir configuré l'ensemble des machines nous observons au niveau de notre centre d'opération les résultats de la surveillance de notre architecture de simulation avec l'outil zabbix qui montre un ensemble d'information par rapport à la mémoire, le réseau mais des applications de la machine. Mais aussi le niveau par rapport au problème de sécurité.

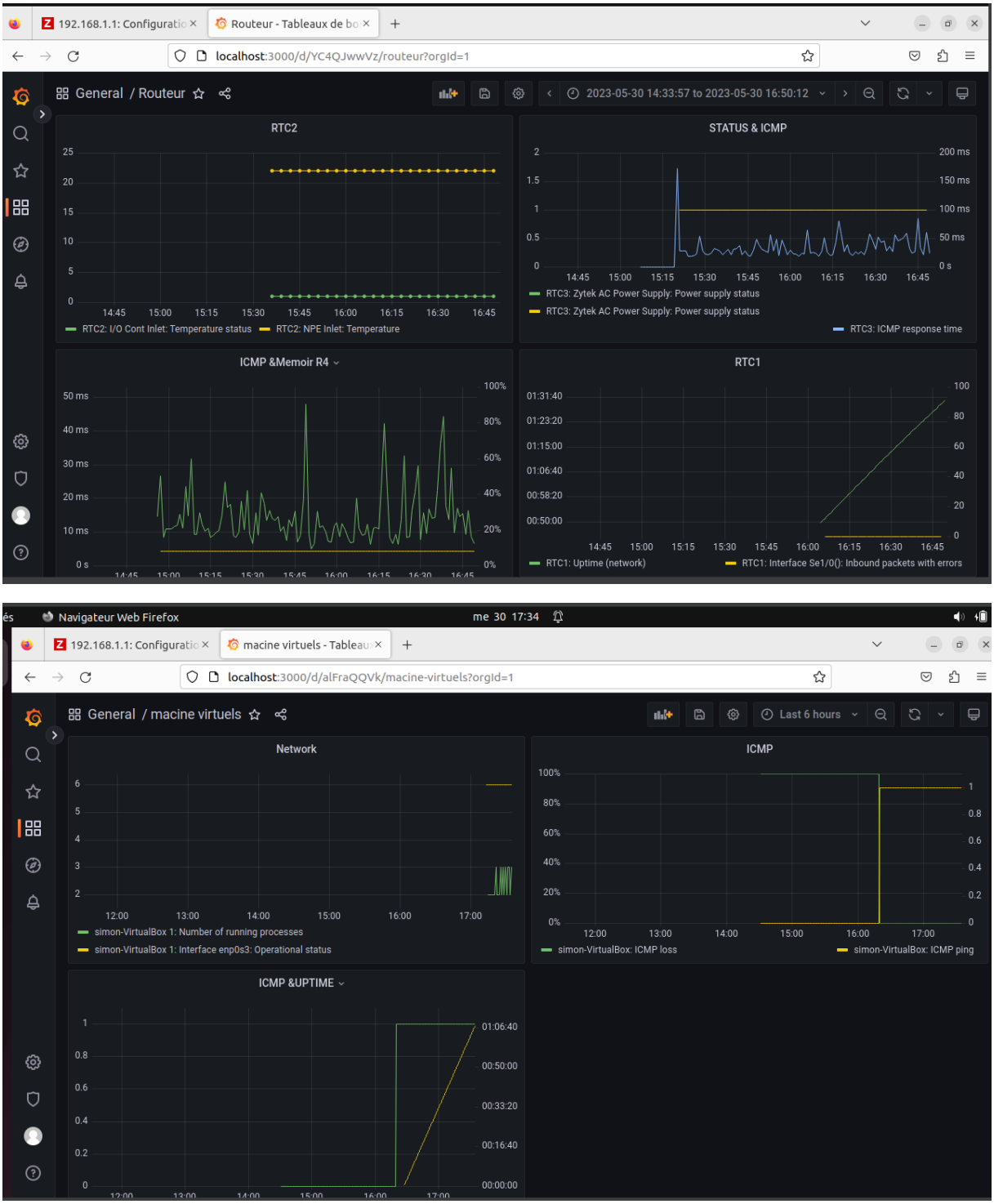


Figure 57: visualisation des données

L'autre facette de notre NOC est la visualisation qui à travers ces captures montrent les données en temps réel par rapport à une machine ou un routeur qu'on surveille. Par exemple au niveau du routeur on a une surveillance du réseau (situation de l'interface de la machine mais aussi le nombre de processus en cour).

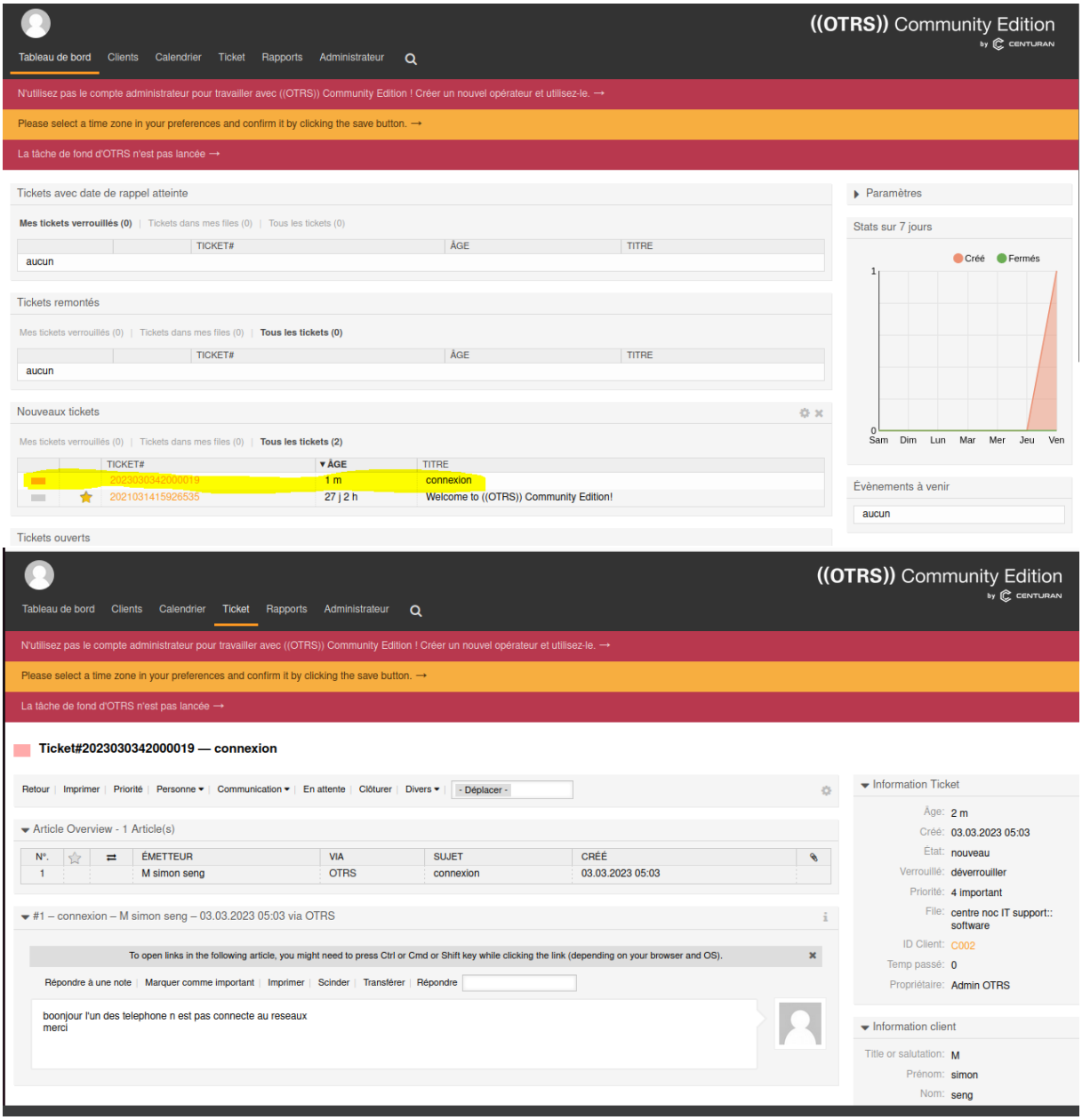


Figure 58: visualisation des tickets envoyés

L'autre partie de notre centre d'opération réseaux est la création de ticket envoyé au niveau de l'écran central afin d'étudier et d'ordonner les tickets par priorité et d'apporter des solutions à chaque problème soulevé au niveau du réseau.

5-Conclusion

En somme cette partie de mettre en pratique les informations reçues au niveau de la première et deuxième partie afin de bien configurer notre NOC pour un réseaux d'opérateur afin de proposer une solution à notre problématique.

Conclusion générale

Pour finir, ce mémoire a permis de réfléchir, d'étudier, d'appliquer et aussi de proposer une solution par rapport à la mise en place d'un NOC pour un réseau d'opérateur. On se demanda comment un NOC pourrait permettre de veiller à un réseau d'opérateur pour un service de qualité.

Il a fallu dans un premier temps comprendre le NOC ou il était question de voir de quoi, il s'agit puis d'étudier les composants d'un NOC et enfin de découvrir la démarche d'une bonne mise en place de NOC. Dans un second temps d'étudier un réseau d'opérateur compose d'un réseau d'accès constitue le réseau d'accès mobile et celle fixe, mais du réseau de cœur qui fait le lien entre le réseau d'accès et internet et enfin ces informations ont permis de bien choisir une solution avec laquelle nous avons proposé un réseau local composé de trois machines virtuels dont l'une nous a servi de NOC et les autres comme faisant partie de notre réseau d'opérateur, mais aussi des routeurs pour faciliter la communication au sein du réseau permettant d'atteindre notre objectif de mise en place de NOC pour un réseau d'opérateur.

Apres avoir mis en place NOC pour un réseau d'opérateur, même s'il joue le premier rôle de sécurité, cela n'est pas suffisant, alors nous proposerons d'inclure le soc (sécurité opération center est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance) mais aussi d'inclure le Cloud.

Webograph

[2] Publié le 01 Aout 2019 *C'est quoi un Network Operations Center (NOC) ? | Splunk*. (n.d.). Splunk. https://www.splunk.com/fr_fr/data-insider/network-operations-center.html

[3] *Qu'est-ce qu'un SOC ? - Définition du Security Operation Center*. (s. d.). Oracle France. https://www.oracle.com/fr/cloud/soc-security-operations-center/

[4] Awati, R. (2021). Network opérations center (NOC). *Networking* https://www.techtarget.com/searchnetworking/definition/network-operations-center

[5] Wikipédia contributors. (2023, 27 septembre). *User Datagram Protocol*. Wikipedia. https://en.wikipedia.org/wiki/User_Datagram_Protocol

[1],[6], [8], [10], [21] Alassane Samba le 29/10/2018. *Science des données au service des réseaux d'opérateur : proposition de cas d'utilisation, d'outils et de moyens de déploiement*. THESE DE DOCTORAT DE L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE BRETAGNE PAYS DE LA LOIRE - IMT ATLANTIQUE

[7] *Le Cœur de Réseau - Blog - SCC France*. (n.d.) https://france.scc.com/scc-france/blog/le-coeur-de-reseau

[9] Orange. (n.d.). *Le réseau mobile*. Cite Des Télecoms. https://www.cite-telecoms.com/accueil/musee-des-telecommunications/la-telephonie-mobile/le-reseau-mobile/

[11] *Download and install Zabbix*. (s. d.). https://www.zabbix.com/download?zabbix=6.4&os_distribution=alma_linux&os_version=9&components=server_frontend_agent&db=pgsql&ws=apache

[12] François, A. (2023). Installer et configurer Grafana OSS sur Ubuntu 22.04. *Lecoindunet*. https://www.lecoindunet.com/installer-configurer-grafana-oss-ubuntu

[13] Angeloma. (2018). How to install the latest OTRS on Ubuntu 18.04? *Linux Windows and Android Tutorials*. https://www.osradar.com/how-to-install-the-lastest-otrs-on-ubuntu-18-04/

[14] Wake, T. (2023, 26 novembre). NOC/SOC Integration : Opportunities for increased efficiency in incident response within Cyber-Security | SANS Institute. https://www.sans.org/white-papers/38290/

[15]CNO/COS - gros plan d'un centre : Illustration de stock 294087929 | Shutterstock. (s. d.). Shutterstock. https://www.shutterstock.com/fr/image-illustration/noc-soc-close-network-security-operations-294087929

[16], [17] Sery, N. (2015, 11 janvier). *Modèle OSI et TCP/IP*. Linux- notebook. https://linux-note.com/modele-osi-et-tcpip/

[18] Jiju, N. (2023, 6 mars). *TCP/IP vs UDP : What& # 8217 ; s the difference ?* Colocation America. https://www.colocationamerica.com/blog/tcp-ip-vs-udp

[19]Cité des télécoms : parc de loisirs dédié aux télécoms en Bretagne. (2023, 16 novembre). Cité des télécoms. https://www.cite-telecoms.com/voy_content/uploads/2015/02/Capture-d'ecran-2015-02-18-A0-16.22.00.png

[20]Cité des télécoms : parc de loisirs dédié aux télécoms en Bretagne. (2023b, novembre 16). Cité des télécoms. https://www.cite-telecoms.com/voy_content/uploads/2015/02/Capture-d'ecran-2015-02-18-A0-16.22.57-613x405.png